IDENTIFICACIÓN, ANÁLISIS Y DESARROLLO DE PROPUESTA PARA OPORTUNIDADES DE MEJORA EN LA GESTIÓN DE ESTACIONES DE TRABAJO CRÍTICAS EN LA DIVISION DE TECNOLOGIAS DE LA UNIVERSIDAD AUTONOMA DE OCCIDENTE

JOSE ESTRADA GONZALEZ

Pasantía institucional para optar el título de Ingeniero Informático

Director
MIGUEL JOSÉ NAVAS JAIME.
Maestría en Ingeniería Telemática

UNIVERSIDAD AUTONOMA DE OCCIDENTE
FACULTAD DE INGENIERIA
DEPARTAMENTO DE OPERACIONES Y SISTEMAS
PROGRAMA DE INGENIERIA INFORMATICA
SANTIAGO DE CALI
2012

Nota de aceptación:

Aprobado por el Comité de Grado en cumplimiento de los requisitos exigidos por la Universidad Autónoma de Occidente para optar al título de Ingeniero Informático

MARIO WILSON CASTRO

_____

Jurado

JUAN CARLOS VALENCIA

_____

Jurado

Santiago de Cali, 16 de octubre del 2012

Dedico este proyecto a la familia Estrada González, que desde el inicio de la carrera de profesionalización creyeron en este proceso y entregaron sus consejos, palabras de aliento, su apoyo incondicional y todas las herramientas necearías para ayudar a cumplir los objetivos que ayudaron a llegar a este punto de la vida, el cual es la presentación de este trabajo de grado, ellos son y serán siempre el motivo de seguir adelante con las metas personales propuestas por José Estrada González.

AGRADECIMIENTOS

Al primero que le debo dar las gracias es a Dios, pues él fue el que me entrego toda la sabiduría y entendimiento para afrontar todos los obstáculos y darme las fuerzas en los momentos más difíciles para seguir adelante en la carrera de ser un profesional, en él y por él pude llegar hasta este punto, brindándome la salud para lograr mis objetivos, además de su infinita bondad y amor.

A mi madre Carmen González. Por haberme apoyado en todos los momentos fáciles y difíciles, por sus consejos sus valores, que me ha permitido ser una persona de bien, pero más que nada, por su amor y compresión que han sido un pilar fundamental en mi vida.

A mi padre Luis Estrada, por los ejemplos de perseverancia y constancia que me ha infundado siempre, por el valor mostrado para salir delante de las situaciones más adversas, por regalarme la oportunidad de ser un profesional.

A mi hermano Álvaro Estrada G, por estar a mi lado apoyándome y bridándome su amistad, compañerismo y consejos que me han servido mucho para en mi vida.

Al ingeniero Jorge Rojas, Coordinador de seguridad informática de la división de tecnologías, por haber brindado todo el conocimiento que fue aplicado en este proyecto.

CONTENIDO

LISTA DE CUADROS

Pág.

LISTA DE FIGURAS

LISTA DE ANEXOS

RESUMEN

El presente trabajo toma las directrices propuestas por el sistema de administración de riesgos integral (SARI), directrices expuestas en el anexo 4, se inicia haciendo un análisis de los activos de información, una vez determinados éstos se realiza la identificación de las estaciones de trabajo, puesto que sobre ellas es que se ejecutan los procedimientos de los procesos que soportan los servicios que ofrece la División de Tecnologías en los departamentos de Redes y Telecomunicaciones y de Cómputo.

Se procede a valorar la criticidad de las estaciones de trabajo, con lo que se determina cuáles son críticas. A aquellos activos críticos se les aplica la metodología OCTAVE Allegro, la cual brinda la identificación, evaluación y tratamiento de los riesgos a los que están enfrentados los activos de información críticos de la División de Tecnologías.

La metodología OCTAVE Allegro se desarrolla mediante ocho pasos, los cuales fueron seguidos por el presente trabajo, para al final proponer oportunidades de mejora, representadas en controles que se deben implantar para reducir las vulnerabilidades y así aumentar los niveles actuales de seguridad informática de la División de Tecnologías de la Universidad Autónoma de Occidente

Palabras Claves: SARI, seguridad de la Información, Octave Allegro, administración de riesgos, activos de Información, mitigación de riesgos.

INTRODUCCIÓN

Desde 1964 la informática es un gran pilar del mundo moderno, dejando de ser un complemento y pasando a ser una base sólida y vital en donde las organizaciones hacen sus pilas de crecimiento operacional y estratégico. Con el pasar de los años la informática ha evolucionado, con el fin de ser una ciencia que brinde soluciones, automatice tareas rutinarias y logre brindar información necesaria y útil para la toma de decisiones dentro del contexto que generan las organizaciones. Hoy en día la informática se ha convertido en punto necesario y trascendente para el manejo o tratamiento de la información dentro de las organizaciones.

La informática, al asumir el rol de la administración de la información, requiere la creación de un esquema de seguridad, el cual debe vigilar dos aspectos fundamentales, el primero es salvaguardar toda la información de la organización (desde la operacional hasta la información estratégica de alta gerencia) asegurando la integridad, disponibilidad y confidencialidad de esta. El segundo aspecto es la minimización de los riesgos a los que está expuesta la información; este requerimiento se encuentra implícito en lo que se llama seguridad informática, la cual se enfoca en la protección de estos aspectos con la ayuda de estándares y metodologías con el fin de brindar un manejo adecuado de la información.

Con el desarrollo de este proyecto la Universidad Autónoma de Occidente, quiere identificar las fortalezas y debilidades, en el proceso de gestión de la seguridad informática de las estaciones de trabajo críticas en algunos de los procesos de la división de tecnologías que son de suma importancia para dicha división, con el fin de analizar dicha información y proponer soluciones aplicables a las oportunidades de mejora encontradas, pero siempre buscando entregar unos servicios a la comunidad con una alta calificación y aceptación de calidad y respaldo.

1. PLANTEAMIENTO DEL PROBLEMA

La División de Tecnologías de la Universidad Autónoma de Occidente, tiene la necesidad apremiante e inaplazable de tomar medidas de seguridad sobre la información sensible y los servicios que administra y transmite para la comunidad que la conforma.

1.1. DESCRIPCION DEL PROBLEMA

Con la creciente sofisticación de la tecnología dentro del ámbito de la educación, las universidades se convirtieron en focos de desarrollo tecnológico de innovación permanente, la Universidad Autónoma de Occidente ostenta la reputación de ser una de las universidades mejor dotadas con tecnología de punta en el suroccidente colombiano. Esto se traduce en actividades administrativas y académicas informáticas cada vez más complejas, tales como el soporte de aplicaciones del negocio, administración de servidores web, autenticación de usuarios y recursos, almacenamiento de información en red, servicios de comunicación, servicio de conectividad en red cableada e inalámbrica, entre otros.

Tales actividades hacen que la seguridad de la información sea más compleja de administrar; ya no basta con resguardar los documentos más importantes bajo llave y mantener seguros a los empleados que poseen el conocimiento. Hoy en día es más difícil lograr niveles óptimos en los pilares de la seguridad informática como los son la disponibilidad o accesibilidad, integridad o fidelidad y confidencialidad o reserva de la información sensible de la organización, debido a que todo el contexto que genera la utilización de tecnología en las diferentes actividades operacionales, estratégicas y gerenciales de una organización está en continuo proceso de mejora evolutivo, lo que conlleva a la creación y revisión periódica de un sistema de administración de riesgos que brinden tranquilidad y confianza a todos los recursos tecnológicos y las personas que utiliza o proveen los servicios informáticos.

Actualmente la Universidad Autónoma de Occidente cuenta con un esquema de seguridad informática en donde se plantea la necesidad de hacer una evaluación permanente sobre la información sensible que la organización maneja. Dentro de este esquema se encuentra el Sistema de Administración de Riesgos Integral SARI (ver Anexo 4), que plantea una metodología para la mitigación de riesgos en los activos de información de la Universidad.

Para la División de Tecnologías uno de los activos más importantes y que se debe analizar, son las estaciones de trabajo, ya que en ellas se administran los servicios prestados a la comunidad y por esta razón se les debe evaluar para determinar si son críticas en términos de los pilares de la seguridad, confidencialidad, integridad y disponibilidad.

1.2. ALCANCES

A la División de Tecnología de la Universidad Autónoma de Occidente, se ha delegado el control y la operación de la seguridad de todos los activos informáticos que de una u otra manera manejan la información sensible de la organización, los cuales pueden llegar a ser numerosos y, dado el carácter de pasantía institucional a través del cual se desarrollo este proyecto que supone un periodo de tiempo limitado, el alcance del proyecto se restringe únicamente a las estaciones de trabajo del departamento de Redes y Telecomunicaciones y del departamento de Cómputo, como activos de análisis.

Es decir el alcance del presente trabajo se refiere únicamente a los activos denominados estaciones de trabajo críticas de los departamentos mencionados. Los otros activos se proponen como recomendaciones para ser analizados en futuros proyectos.

2. JUSTIFICACIÓN

En la Universidad Autónoma de Occidente el flujo de información es bastante alto, lo que implica que exista la posibilidad de que haya más riesgos de agentes externos o internos quieran vulnerar, robar, dañar, alterar o simplemente sabotear cualquier parte de la información a la que tengan acceso.

Por esta razón se hace imprescindible, y por ende justificable, que se reduzcan los riesgos de manera oportuna, implementando y actualizando permanentemente planes de seguridad informática en los departamentos de la División de Tecnologías de la universidad.

Los resultados de este proyecto benefician directamente a la institución, porque brindan un análisis confiable de la situación actual de la institución en términos de seguridad informática, a la vez que propone soluciones a las posibles oportunidades de mejora encontradas.

En este proyecto se aplicó la metodología planteada por SARI (ver Anexo 4), lo que permitió identificar fortalezas y debilidades del esquema actual de la seguridad informática de las estaciones de trabajo que administran los servicios que soportan la operación diaria de la organización y que manejan la información sensible de la universidad.

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Proponer soluciones aplicables a las oportunidades de mejora identificadas en el esquema de seguridad informática de las estaciones de trabajo críticas de la División de Tecnologías de la Universidad Autónoma de Occidente.

3.2. OBJETIVOS ESPECÍFICOS

- Describir los lineamientos del Sistema de Administración de Riesgos Integral (SARI), planteado por la División de Tecnologías de la Universidad Autónoma de Occidente.

- Aplicar los lineamientos del Sistema de Administración de Riesgos Integral (SARI), a los servicios actuales que el departamento de Cómputo y Departamento Redes y Telecomunicaciones ofrece a la comunidad de la Universidad Autónoma de Occidente.

- Identificar estaciones de trabajo críticas en las que se soportan los servicios actuales que el departamento de Cómputo y el departamento Redes y Telecomunicaciones brindan desde la División de Tecnologías a la comunidad de la Universidad Autónoma de Occidente.

- Identificar fortalezas y debilidades en el esquema actual de seguridad informática de la División de Tecnologías de la Universidad Autónoma de Occidente.

- Proponer mejoras a los niveles actuales de seguridad informática de la División de Tecnologías de la Universidad Autónoma de Occidente

4. ANTECEDENTES

En el proyecto de ANDRÉS ARISTIZÁBAL Y HUGO ANDRÉS LÓPEZ titulado *USING PROCESS CALCULI TO MODEL AND VERIFY SECURITY PROPERTIES IN REAL LIFE COMMUNICATION PROTOCOLS* de la Pontificia Universidad Javeriana, Cali[1], se contextualiza la seguridad informática como una de las características más importantes en las comunicaciones actuales y la necesidad de transmitir información crítica de manera segura, utilizando canales públicos, cobrando especial importancia en el contexto de los sistemas de cómputo globales como Internet. Los autores plantean protocolos de seguridad basados en cálculo de procesos concurrentes que determinan esquemas de comunicación para la corrección de falencias de seguridad. Con este estudio se aclararon algunos conceptos sobre seguridad informática y protocolos de seguridad.

En la tesis de grado titulada SEGURIDAD INFORMATICA – IMPLICANCIAS E IMPLEMENTACION desarrollada por el Lic. Cristian Borghello de la universidad Tecnología Nacional de Argentina[2], se plantea todo un contexto que ha creado la seguridad informática y la gran necesidad del aplicar esta rama de la ingeniería a los procesos críticos que soportan la misión y visión de las organizaciones. La conclusión que aporta el autor en su trabajo es que se debe tener en cuenta la seguridad al diseñar un sistema, estableciendo una correspondencia entre las técnicas que implementan la seguridad con las de diseño y desarrollo de sistemas, sin que sean procedimientos aislados. Por lo tanto se debe articular la seguridad desde el mismo diseño del sistema. En el proyecto titulado ANÁLISIS DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN de Juan Manuel Matalobos de la Universidad Politécnica de Madrid[3], el autor basa su proyecto en la creación de un plan de seguridad de la información, realizando una comparación de las diferentes metodologías propuestas por las diferentes organizaciones expertas en el tema, con el fin de encontrar fortalezas y debilidades de cada una de ellas en el contexto de la seguridad informática. Después de comparar las metodologías el

[1] ARISTIZÁBAL, Andrés Y LÓPEZ, Hugo Andrés. USING PROCESS CALCULI TO MODEL AND VERIFY SECURITY PROPERTIES IN REAL LIFE COMMUNICATION PROTOCOLS. [En línea]. Trabajo de grado de Ingeniero de Sistemas y Computación. Santiago de Cali: Pontificia Universidad Javeriana. Facultad de Ingeniería. 2006. P3. [Consultado el enero 15 de 2012]. Disponible en http://cic.puj.edu.co/~halopez/stuff/Tesis-halopez-aaristizabal.pdf

[2] BORGHELLO, Cristian. Seguridad Informática – Implicancias E Implementación. [En línea]. Trabajo De grado Licenciatura en Sistemas. Buenos Aires, argentina, Universidad Tecnología Nacional de Argentina. Faculta de Ingeniería 320. 217 p. [Consultado el enero 15 de 2012]. Disponible en http://www.segu-info.com.ar/tesis/

[3] MATALOBOS, Juan Manuel. ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN. [En línea]. Título de grado para Ingeniero Informático. Universidad Politécnica de Madrid: Madrid España. 2009. 306 p. [Consultado el abril 5 de 2012]. Disponible en http://oa.upm.es/1646/1/PFC_JUAN_MANUEL_MATALOBOS_VEIGAa.pdf

autor encuentra pertinente la creación de su propia metodología que le brinda pautas completas en la creación del plan de seguridad, pero utilizando las directrices y lineamientos que más se ajustan al contexto en el que va a ser planteado el plan de seguridad e la información.

La Universidad Autónoma de Occidente desde la división de tecnologías, ha desarrollado un programa de fortalecimiento de la plataforma tecnológica que soporta procesos académicos y administrativos, el cual contempla revisiones periódicas que contienen procesos de identificación y análisis de vulnerabilidades. Este proceso se ha llevado a cabo en diferentes oportunidades, el último de ellos se desarrolló en el año 2008 por una entidad externa[4].

[4] Entrevista con el Ing. Jorge Armando Rojas Varela. Coordinador de Seguridad Informática de la Universidad Autónoma de Occidente.

5. MARCO DE REFERENCIA

5.1 MARCO TEÓRICO

En la actualidad la ingeniería informática tiene muchas especialidades tales como la telemática, desarrollo de software, gestión de las tecnologías de la información y seguridad informática, entre otras, esto se debe a que ésta se ha transformado en una ciencia fundamental en este mundo globalizado. Un mundo que ha creado la necesidad de un servicio de administración de la información, con la gran característica de estar disponible las veinticuatro horas de los siete días de la semana, a fin de lograr grandes beneficios dentro de un mercado competitivo para las organizaciones.

El auge de internet y la necesidad de compartir información hace que el tema de seguridad adquiera una relevancia de la cual poco se hablaba hace unos años. La base de este proyecto es precisamente la seguridad de la información cuyos principales temas se plantean a continuación.

5.1.1 Gestión de las tecnologías de información y comunicación – TIC. Para suplir la necesidad de la administración de la información es necesario tener la gestión de las tecnologías de la información y las telecomunicaciones como un gran aliado para las organizaciones.

Los sistemas de información en términos generales se diseñan para gestionar la información y el conocimiento en las organizaciones cuyo objetivo final es el permitir mejorar los procesos empresariales y de esta manera crear valor como lo plantea Carmen de Pablos Herederos[5], por tal motivo es necesario crean un plan que gestione los sistemas de información con los que cuenta la organización.

Por otro lado Solorzano[6] plantea como beneficios de la implantación de lineamientos de la gestión de las TIC en la organizaciones, la reducción de costos y el mejoramiento de la eficiencia de las operaciones; así mismo al reemplazar los procesos manuales se puede reducir los tiempos y la necesidad de movilizarse

[5] HEREDERO, Carmen de Pablos. Y LOPEZ-HERMOSO AGIUS, jose joaquin. Y ROMO ROMERO, Santiago Martin Dirección y gestión de los sistemas de información en la empresa.ESIC Editorial, Madrid España,2008 p104 (367 Paginas)

[6] SOLORZANO, Arturo J, Importancia de las tecnologías de la información y comunicación (TIC) para las PYMEs. [En línea]. TIC de UAM. p 3 [Consultado el 21 de Marzo del 2012]: Disponible en: http://ticdeuam.wikispaces.com/file/view/Importancia+de+las+TIC.pdf (3 Paginas)

para realizar trámites o buscar información; otro beneficio se refiere a la generación de los ingresos adicionales mediante el uso de los sitios WEB por ejemplo, para vender y ofrecer sus productos y servicios; la ampliación de nuevos mercados y capitales utilizando Internet, el cual ofrece una amplia posibilidad a un bajo costo.

Como puede verse el auge de Internet ha obligado a las organizaciones a estar a la par con el desarrollo de las tecnologías de información y comunicación, esto también representa un mundo más interconectado entre sí y por ende más inseguro. Las grandes ventajas que conllevan la gestión de las TIC y la necesidad de salvaguardar la información sensible hacen que el tema de seguridad adquiera una gran relevancia.

5.1.2 Seguridad informática. La ingeniera informática debe ofrecer una plataforma de acceso a los servicios diseñados por los Sistemas de Información, lo que implica una alta responsabilidad, trayendo a su vez grandes riesgos y, como se mencionó anteriormente, están expuestos por la interconectividad que se ofrece hoy en día. De una u otra manera la ingeniería informática debe manejar o mitigar tales riesgos a fin de brindar tranquilidad y respaldo para los procesos diseñados por los sistemas de información.

Es así como surge la Seguridad Informática como una rama de la ingeniería que busca brindar soporte y respaldo a las organizaciones. Para Aguilera[7] la seguridad informática es "la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable." Esta definición se complementa con la expuesta por Areitio[8] quien plantea que "la meta final de la seguridad es permitir que una organización cumpla con todos sus objetivos de negocio o misión". Por lo tanto en el contexto de este proyecto la seguridad informática debe brindar un respaldo adecuado dentro de la organización, con el fin de lograr que ésta se enfoque en las tareas para las cuales fue creada.

[7] AGUILERA, Purificación. Seguridad informática. Editorial Editex S.A. Madrid España 2009. p9 (240 Paginas).

[8] AREITO, Javier, Seguridad De La información. Redes, Informática y Sistemas de Información PARANINFO, Madrid España. 2008 p2 (592 Paginas)

5.1.3. Pilares de la seguridad informática. Los principales objetivos de la seguridad informática que generan la base de la rama de la ingeniería informática son la disponibilidad, confidencialidad e integridad de la información, los cuales constituyen los tres pilares fundamentales de la seguridad de la información.

La disponibilidad en seguridad informática se refiere al grado en que la información esté en el lugar, momento y forma cuando es requerido por un usuario autorizado, lo cual está asociado directamente a la confiabilidad técnica de los componentes de un sistema de información, tal como lo plantea Aguilera[9],es decir la información debe estar disponible para los usuarios autorizados cuando la necesiten.

La confidencialidad se refiere al hecho de que la información está únicamente al alcance del conocimiento de las personas, entidades o mecanismos autorizados, en los momentos autorizados y de una manera autorizada, tal como lo plantea Aguilera[10,] es decir que sólo las personas autorizadas pueden acceder a la información correspondiente.

La integridad se refiere a la garantía por parte del sistema de que la información no ha sido alterada, ni destruida por alguien no autorizado, es decir que los procesos y los datos son exactos en todo momento[11].

Todo sistema de información se ve amenazado por un conjunto de actividades internas o externas, que deben ser analizadas y crean una fragilidad en el sistema si no están debidamente diseñados, lo que constituye un riesgo que puede hacer tambalear el cumplimiento de los objetivos planteados por éstos tres pilares de la seguridad.

[9] Óp. Cit. AGUILERA Seguridad Informática. p10.
[10] Ibíd. p10.
[11] Ibíd. p10 (240 Paginas).

5.1.4. Amenazas. Un sistema de información se puede ver atacado por factores tanto internos como externos que lo obligan a estar permanentemente vigilante de ellos. Estos factores se constituyen en amenazas a la seguridad de dichos sistemas. Para Mora[12] una amenaza es un conjunto de situaciones o acontecimientos que puede afectar y hacer variar la cualidad benéfica de los sistemas de información. Es por esta razón que se debe hacer un estudio de las posibles amenazas a los que se puede ver enfrentado un sistema.

Las amenazas son todas las posibles actividades que se valen de las deficiencias de un sistema y que pueden llegar a convertirse en un riesgo de ataque y por ende ocasionar un problema de seguridad.

5.1.5. Vulnerabilidades. En muchas ocasiones los sistemas de información presentan deficiencias que los hacen vulnerables ante posibles ataques a la seguridad, sobre todo si en su diseño inicial no se tuvo en cuenta este aspecto[13].

Para Mora[14] una vulnerabilidad la define como el grado de facilidad con que pueden producirse daños a las personas, cosas o procesos que se deben proteger como consecuencia de las amenazas.

Es decir una vez determinadas las amenazas se debe hacer un análisis cuidadoso y sistemático de las deficiencias de los sistemas, lo que constituye un análisis de vulnerabilidades del mismo.

Al identificar una amenaza y determinar las posibles vulnerabilidades que pueden llegar afectar la seguridad, se evalúa el nivel de tolerancia que éste puede llegar a soportar sin afectar los pilares de la seguridad; en caso de existir una alta probabilidad de afectación se constituye en un riesgo para la seguridad del mismo.

[12] MORA, Héctor. Manual del Vigilante de seguridad. Tomo 1 . 2ª Edicion. Editorial: Club Universitario Alicante España, 2009 p15 (440 Paginas)
[13] BORGHELLO Óp. Cit. p 217.
[14] MORA Óp. Cit. p15

5.1.6. Riesgos. Los sistemas se ven afectados por un sinnúmero de acciones que se valen de las deficiencias o limitantes de ellos y que de una u otra manera pueden llegar a afectar los beneficios para los cuales fue creado.

Mora[15] determina el riesgo como la probabilidad de que un bien pueda sufrir un daño y por lo tanto se puede cuantificar como alto, medio o bajo.

Por otro lado la ISO 27002:2005[16] plantea que el riesgo es la combinación de la probabilidad de un evento y sus posibles consecuencias, esta definición es la que se tomó en cuenta para el desarrollo del presente proyecto.

5.1.7. Sistemas de gestión de la seguridad de la información. La ingeniería informática, al tomar el rol de administrador de la información sensible de la organización, debe propender por la aplicación de los lineamientos planteados por la gestión de las TIC, que amarrados a la seguridad informática, deben garantizar que se cumplan los tres pilares de la seguridad, para entregar un sistema seguro y confiable. Para ello debe implantar procesos que permitan analizar las amenazas, relacionándolas con sus vulnerabilidades para que, al realizar un análisis de impacto se minimice el riesgo de ataque a la seguridad a los que se enfrenta la organización en su quehacer diario. La conformación de estos procesos da lugar los sistemas de gestión de la seguridad de la información SGSI.

La organización Internacional para la estandarización (ISO) y la comisión electrónica internacional (IEC) en el marco de la norma ISO-27001[17] define un Sistema de Gestión de la Seguridad de la Información, como un sistema gerencial general, basado en un enfoque de riesgo comercial, cuyo objetivo es establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.

Para Areitio[18] un sistema de gestión de la seguridad de la información incluye además la estructura organizacional, políticas, actividades de planificación, responsabilidades, prácticas, procedimientos, procesos y recursos. Es así como

[15] Ibíd. p15.
[16] ISO/IEC 27002:2005. Tecnología de la información – técnicas de seguridad. Código de práctica para la gestión de la seguridad de la información [en línea]. p. 2 [Consultado el 26 de Julio del 2011] Disponible en: http://es.scribd.com/doc/46085176/Normas-ISO-27002 (133 paginas)
[17] ISO/IEC 27001:2005. Tecnología de la información – técnicas de seguridad – sistemas de gestión de seguridad de la información – requerimientos. Primera edición [en línea]. p. 5 [Consultado el 26 de Julio del 2011] Disponible en: http://mmujica.files.wordpress.com/2007/07/iso-27001-2005-espanol.pdf (40 paginas)
[18] Op Cit. AREITO, p200.

un SGSI hace referencia a los esfuerzos sistemáticos y organizados destinados a preservar la seguridad de la información en las organizaciones.
La norma ISO-27001[19] determina que los SGSI deben asegurar la selección adecuada y proporcionar controles de seguridad que protejan los activos de información y den confianza a las partes involucradas.

El Instituto Nacional de Tecnologías de la Comunicación de España en su página WEB[20] afirma que un Sistema de Gestión de la Seguridad de la Información – SGSI se origina debido a que la información, al ser uno de los activos más importantes de toda organización requiere, junto a los procesos y sistemas que la manejan, que sea protegidos frente a las amenazas que puedan poner en peligro la continuidad de los niveles de competitividad, rentabilidad y conformidad legal necesarias para alcanzar los objetivos de la organización.

De esta manera los SGSI deben reunir los lineamientos necesarios que se deben cumplir para brindar una tranquilidad y respaldo del activo más importante que posee una organización: la información.

5.1.8. Activo de información. Los sistemas de información en general poseen componentes valiosos para la organización y por lo tanto necesitan tener cierto grado de protección, la cual debe ser brindada por los Sistemas de Gestión de la Seguridad de la Información. Estos componentes se definen como activos de información[21].

El concepto de activo de información cubre los aspectos relacionados con hardware, software, información, empleados, instalaciones físicas, servicios de información, bases documentales, documentos en papel, entre otros.

Es decir la característica de dichos activos es la sensibilidad de la información valiosa para la empresa, por lo que deben ser debidamente protegidos por los SGSI. Actualmente han surgido una serie de metodologías y normas que al ser tenidas en cuenta por los SGSI brindan una tranquilidad y confianza sobre los activos de información.

[19] Op Cit. ISO/IEC 27001:200 p 8
[20] INTECO. Sistema de Gestión de La Seguridad de La Información [en línea]. [Consultado el 26 de Julio del 2011]. Disponible en http://cert.inteco.es/Formacion/SGSI/Conceptos_Basicos/Concepto_SGSI/
[21] AREITO, Javier, Seguridad De La información. Redes, Informática y Sistemas de Información PARANINFO, Madrid España. 2008 p 62 (592 Paginas)

5.1.9. Metodología OCTAVE – Allegro. La seguridad informática requiere de unas directrices, estándares y metodologías que brinden la guía del qué y cómo lograr obtener un sistema que ofrezca a las organizaciones la tranquilidad y confianza del buen trato de la información con el fin de enfocarse a cumplir la misión planteada.

Esto se logra con la utilización de metodologías, entre las que se encuentra OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), creada por la organización CERT[22] , con el fin de brindar un documento que reúna de forma estandarizada y ordenada, las diversas verificaciones y pruebas que debe realizar la persona encargada de la seguridad informática de una organización para identificar y mitigar riesgos, ayudando así a que la organización tenga un ambiente administrado y controlado de sus tecnologías de la información y comunicación.

Adicionalmente la Organización CERT plantea una variación de la metodología OCTAVE orientada a la identificación, evaluación y tratamiento de los riesgos a los que están enfrentados únicamente los activos de información, llamada OCTAVE Allegro[23].

Las metodologías utilizadas por los SGSI hacen uso de normas y protocolos que proponen lineamientos estandarizados que les ayudan a cumplir el objetivo principal para el cual fueron diseñados.

[22] CERT. Metodología OCTAVE Allegro [en línea]. [Consultado el 26 de Julio del 2011]: Disponible en: http://www.cert.org/octave/download/allegro_form.html Versión 1.0
[23] Metodología OCTAVE Allegro [en línea]. CERT. [Consultado el 26 de Julio del 2011]: Disponible en: http://www.cert.org/octave/allegro.html

5.1.10. Normas y protocolos de la seguridad informática. La Organización Internacional para la Estandarización (ISO) y la Comisión Electrónica Internacional (IEC) forman el sistema especializado para la estandarización universal. Los miembros de la ISO y la IEC participan en el desarrollo de estándares nacionales mediante comités técnicos que se establecen para tratar los campos particulares de la actividad técnica, colaborando en campos de interés mutuo[24].

Los estándares internacionales son desarrollados en concordancia con las reglas dadas en las directivas ISO/IEC. La tarea principal del comité técnico es preparar estándares internacionales los cuales son adoptados por los organismos nacionales miembros.

En relación con el análisis de la seguridad del presente proyecto se presenta las normas ISO 31000 que se refiere a la identificación de riesgos; la ISO 27001, que se refiere a la creación de un SGSI y la norma ISO 27002 que se refiere al manual de buenas prácticas de la seguridad de la información.

5.1.10.1. Norma ISO 31000[25]. Esta norma genera un aporte valioso para la seguridad informática, ya que proporciona un marco de gestión de los riesgos utilizable por cualquier tipo de organización.

La aplicación de este estándar trae consigo beneficios para las organizaciones que se acojan a sus directrices, pues recomienda el desarrollo, implementación y mejoramiento continuo de un marco de trabajo o estructura de soporte, cuyo objetivo es integrar el proceso de gestión de riesgos a la organización en su planificación y estrategia, gestión en los procesos de información, políticas, valores y su cultura organizacional. En términos generales esta norma plantea los lineamientos para la gestión de Riesgos.

El jefe del grupo de trabajo ISO que desarrolló el estándar[26] justifica a la aplicación de la norma dado que para él todas las organizaciones independientemente de si son grandes o pequeñas, se enfrentan a factores tanto internos como externos

[24] Op cit. ISO/IEC 27001:2005. P 4.
[25] CASTRO, Mauricio. El Nuevo Estándar ISO Para La Gestión Del Riesgo. [En línea]. SURLATINA CONSULTORES. [Consultado el 26 de Julio del 2011]: Disponible en: http://www.surlatina.cl/contenidos/archivos_articulos/13-el%20nuevo%20estandar%20iso%20para%20la%20gestion%20del%20riesgo.pdf
[26] KNIGHT, Kevin W., New ISO Standard for Effective Management of Risk. [En línea]. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. [Consultado el 21 de Marzo del 2012]: Disponible en: http://www.iso.org/iso/pressrelease.htm?refid=Ref1266

que crean incertidumbre sobre si éstas podrán alcanzar sus objetivos. El efecto de esta incertidumbre es el riesgo y es inherente en todas sus actividades.

Por lo tanto lo que plantea esta norma son las directrices y parámetros para identificación y administración de los riegos a los que está expuesta la organización en su operación del día a día.

5.1.10.2. Norma ISO 27001[27]**.** Esta norma ayuda al desarrollo del Sistema de gestión de la Seguridad de la Información (SGSI). Es decir este estándar se refiere a los requerimientos necesarios para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un sistema de gestión de seguridad de la información.

Según la norma[28] un SGSI en una organización está diseñado para asegurar la sección adecuada y proporcionar controles de seguridad que protejan los activos de información y den confianza a las partes interesadas.

Es decir la norma plantea las pautas para identificar qué es lo que tiene valor para la organización, con el fin de crear control y administración de los riegos a los que están expuestos los ítems valiosos para la empresa.

5.1.10.3. Norma ISO 27002[29]. Esta norma proporciona un manual de Buenas Prácticas de Seguridad de la Información, en donde establece directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización.

Mas específicamente la norma determina los objetivos de control y los controles que se deben aplicar con el fin de satisfacer los requisitos identificados por la evaluación de riesgos.

[27] ISO/IEC 27001:2005 [en línea]. ISO. [Consultado el 26 de Julio del 2011]: Disponible en: http://mmujica.files.wordpress.com/2007/07/iso-27001-2005-espanol.pdf
[28] ISO/IEC 27001:2005 [en línea]. ISO. [Consultado el 26 de Julio del 2011]: Disponible en: http://mmujica.files.wordpress.com/2007/07/iso-27001-2005-espanol.pdf
[29] ISO/IEC 27002:2005 [en línea]. [Consultado el 26 de Julio del 2011]: Disponible en: http://webstore.iec.ch/preview/info_isoiec27002%7Bed1.0%7Den.pdf

6. METODOLOGÍA DE LA INVESTIGACION

Este trabajo es de tipo descriptivo correlacional. Inicialmente se describe el Sistema de Administración de Riesgos Integral, SARI., el cual implanta la metodología OCTAVE Allegro, bajo los lineamientos de la ISO 31000, ISO27001 e ISO 27002, para ello se contó con la colaboración del Coordinador de Seguridad Informática de la División de Tecnología de la Universidad Autónoma de Occidente, el cual brindó la información necesaria plasmada en una propuesta de Sistema de Administración de Riesgos Integral, desarrollada por él mismo.

Una vez analizada la propuesta se identificaron los activos de información de los departamentos de redes y telecomunicaciones, con sus respectivos propietarios, responsables y custodios, basándose en sus procedimientos, lo que permitió limitar los activos a las estaciones de trabajo respectivas.

Una vez identificadas las estaciones de trabajo se validó la información obtenida mediante una entrevista con cada uno de los jefes de departamento, los cuales determinaron su veracidad.

Con esta información se procedió a cualificar las necesidades implantadas por los pilares de la seguridad como lo son confidencialidad, integridad y disponibilidad, para determinar cuáles de ellas eran críticas y deberían ser sometidas a un análisis más profundo con el fin de identificar los riesgos, mediante el uso de los lineamientos más relevantes para el contexto de este proyecto, propuestos por la ISO 31.000 y proponer mejoras mediante el uso de las normas ISO 27.001 y 27.002 en los aspectos igualmente relevantes al proyecto.

Se finaliza entonces con el diseño de la propuesta de mejora del esquema de seguridad informática sobre estas estaciones de trabajo críticas.

Para la ejecución de este proyecto se utilizó el método OCTAVE Allegro propuesto por SARI, el cual consta de ocho pasos que se describen a continuación:

Paso 1 - Establecer criterios de medición del riesgo.

Paso 2 - Desarrollar un perfil de Activos de Información.

Paso 3 - Identificar los contenedores de la información de activos.

Paso 4 - Identificar áreas de preocupación.

Paso 5 - Identificar las situaciones de amenaza.

Paso 6 - Identificar los riesgos

Paso 7 - Analizar los riesgos.

Paso 8 – Seleccionar el enfoque de mitigación.

Todos estos pasos fueron ejecutados a largo de este proyecto cuyos resultados se muestran en los diferentes capítulos de este proyecto y que responden a los objetivos planteados.

7. DESCRIPCIÓN DE SARI

La informática ha evolucionado desde la aparición del equipo de escritorio, pasando por ser una disciplina que proporcionaba comprobación de cálculos matemáticos, automatización de procesos en la industria, hasta el punto en la que la conocemos ahora, como una ciencia que proporciona el manejo, custodia y gestión de la información sensible para la organización, con el fin de proporcionar información estratégica o hasta operacional.

La Universidad Autónoma de Occidente no es ajena a esta tendencia, por lo que en los últimos años se ha planteado la necesidad de proteger sus activos mediante la creación de un Sistema de Gestión de la Información, cuyo primer paso ha sido la creación y adopción de un sistema que pretende brindar garantías en todas las actividades generadas en el contexto de seguridad en la información a fin de mitigar o minimizar riesgos, es así como surge el Sistema de Administración de Riesgos Integral (SARI). En este capítulo se describe el Sistema de Administración de Riesgos Integral (SARI), basado en la propuesta presentada por el señor Rojas a la Vicerrectoría Administrativa y Financiera[30] (Ver anexo 4).

7.1. SISTEMA DE SEGURIDAD DE LA INFORMACIÓN EN LA UAO.

La Universidad Autónoma de Occidente, al conocer la importancia y entender los beneficios de tener un sistema de gestión de la seguridad de la información, comienza una labor de su implantación. El primer paso en el proceso de implantación de un sistema de gestión de la seguridad de la información (SGSI), nace en el momento de establecer un sistema de la gestión de las tecnologías de la información y telecomunicaciones (TIC), como se ha expuesto en el marco teórico de este proyecto.

Basada en las ventajas que trae consigo la implantación de la gestión de las TIC en los procesos y procedimientos que sostiene a las organizaciones, decide tomar como aliado este marco de gestión y arrancar con la aplicación gradual de las directrices planteadas en la gestión de las TIC, para lo cual arranca con la descripción de su estructura organizacional.

[30] ROJAS, Jorge Armando. Propuesta Sistema de Administración de Riesgos Integral. Material institucional de la Universidad Autónoma de Occidente. 2010. p 1 (6 Paginas)

La estructura administrativa de la Universidad está conformada por diferentes departamentos y divisiones, cuyo objetivo es brindar la sostenibilidad en los procesos vitales de la organización con el fin de cumplir a cabalidad los propósitos trazados por la misión y visión de la institución.

La división de Tecnologías ha sido una de las divisiones pioneras de la organización, en la aplicación y constitución de la gestión de las TIC, implantándola dentro de cada uno de los servicios, procesos y procedimientos, logrando así entender claramente el rol que tiene esta división dentro la organización y para la comunidad que conforma la Universidad Autónoma de Occidente.

En el desarrollo de la gestión de las TIC la división de tecnologías entiende que el rol que cumple en la organización es brindar un sinnúmero de servicios tales como Telecomunicaciones, Computo, Redes, Bases de datos, entre otros, que a su vez se han convertido en base fundamental para el desarrollo pleno de las actividades que realiza la organización.

Por la continua evolución de las tecnologías, que cada día se ven más presentes en actividades rutinarias y hasta en actividades gerenciales, como lo son la toma de decisiones estratégicas a futuro, la universidad toma la decisión de entregarle a la División de Tecnologías la administración y custodia de la información de la organización. De esta manera se sientan las bases para la creación del Sistema de Gestión de la Información de la universidad.

Al asumir el rol de la administración de la información la División de Tecnologías, ve la necesidad de participar activamente en el tema de la seguridad informática en todos los servicios, procesos y procedimientos. Por lo tanto se plantea como objetivo el salvaguardar toda la información de la organización a fin de asegurar la integridad, disponibilidad y confidencialidad de la información sensible.

La División de Tecnologías también planea la necesidad de crear planes que minimicen los riesgos tanto internos como externos, a los que está expuesta la información y que tratan de vulnerar de alguna forma los pilares de la seguridad informática.

7.2. DESCRIPCIÓN DEL SISTEMA DE ADMINSITRACIÓN DE RIESGOS INTEGRAL (SARI).

La División de Tecnologías enfoca todo su potencial en la creación de planes que logren la protección de la información sensible con la ayuda de estándares y metodologías para brindar un manejo adecuado de la información.

Uno de estos planes liderado por la Coordinacion de Seguridad Informática de la División de Tecnologías es el Sistema de Administración de Riesgos Integral – SARI, cuyo objetivo principal es proveer un marco de gestión con el cual garantizar que todas las actividades que se adelanten con el respecto a la seguridad de la información institucional, minimizan o se mitigan riesgos reales con la implantación de controles acordes a las necesidades de la Universidad Autónoma de Occidente[31].

Según la propuesta del Sistema de Administración de Riesgos Integral presentada por el señor Rojas[32,] para dar cumplimento al objetivo principal de SARI es necesarios desarrollar las siguientes actividades:

- Diseñar, implementar y establecer lineamientos que mejoren los procesos actuales de gestión de riesgos en la Universidad Autónoma de Occidente.

- Dotar la Universidad Autónoma de Occidente con una estrategia de gestión de riesgos acorde a las necesidades de la misma con respecto a la seguridad de la información

- Permitir la implantación de controles a los activos de la Universidad Autónoma de Occidente teniendo en cuenta los riesgos a que estos se encuentran expuestos y los niveles de aceptación del riesgo definidos para los mismos."

De acuerdo con la propuesta, SARI se encuentra desarrollado en total cumplimiento de lo establecido en las normas ISO 31000:2009, ISO 27001:2005, ISO 27002:2005 y OCTAVE Allegro, los que se constituyen en sus componentes metodológicos.

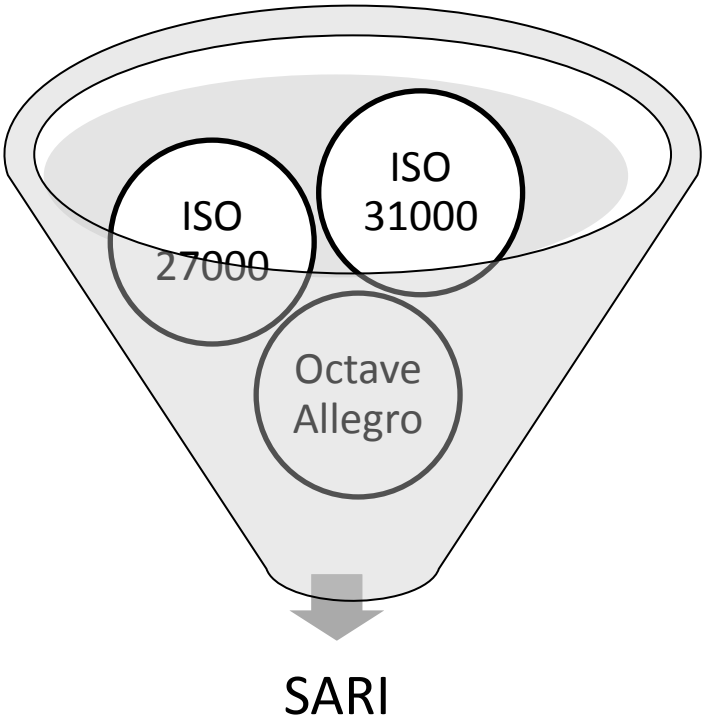
[31] Ibíd. p 1.

[32] Ibíd. p1.

7.3. COMPONENTES DE SARI

SARI se planteó con un marco de referencia y una metodología que le indica la guía de trabajo y a su vez le da cumplimento total de lo establecido en el mismo sistema de administración de riesgos integral, los componentes vitales de SARI son las normas ISO 31000:2009, ISO 27001:2005, ISO 27002:2005 y OCTAVE Allegro, los que se constituyen en sus componentes metodológicos como se puede ver en la figura 1.

Figura 1. Componentes que integran a SARI.



En el diseño de SARI se pensó en crear un sistema que gestione y administre de manera adecuada los riesgos a los que está expuesta la Universidad Autónoma de Occidente, fundamentándolo en los estándares internacionales ISO 31000, los cuales brindan unas directrices para la identificación de riesgos; ISO 27000 (27001 y 27002) los cuales establecen los lineamientos para la creación de un SGSI y los controles que se deben implementar y la metodología OCTAVE Allegro que le proporciona una secuencia de pasos válida y coherente para la identificación de oportunidades de mejora basa en al análisis y mitigación de riesgos enfocándose principalmente en los activos de información de la organización.

7.4. DIRECTRICES O LINEAMIENTOS PLANTEADOS POR SARI.

Las directrices o lineamientos planteados por SARI en la propuesta presentada por el señor Rojas[33] para el sistema de administración de riesgos integral se fundamentan en que cada uno de los pilares de seguridad se trata con igual criticidad respecto a la confidencialidad, integridad y disponibilidad. Es decir que cada pilar representa el 33,33% de la seguridad necesaria para el activo de información.

7.4.1. Valoración de los activos de información. La valoración de cada activo de información deberá ser realizada de acuerdo con la siguiente escala:

- Valor de 1 para la necesidad Mínima de presencia del correspondiente pilar
- Valor de 2 para la necesidad Baja de presencia del correspondiente pilar
- Valor de 3 para la necesidad Media de presencia del correspondiente pilar
- Valor de 4 para la necesidad Moderada de presencia del correspondiente pilar
- Valor de 5 para la necesidad Alta de presencia del correspondiente pilar.

7.4.2. Nivel de valoración del activo de información. La evaluación de los activos de información es de carácter institucional y se debe realizar con base en la valoración de los pilares de seguridad para el mismo. Los valores dados en cada pilar deberán ser promediados para dar la evaluación final al activo, constituyendo el nivel de valoración del activo de información, que servirán para medir el impacto.

7.4.3. Activos que se consideran en el SARI. Los activos de información que deberán ser contemplados en el SARI serán aquellos que, como resultado de la evaluación, obtengan un valor igual o superior a 3, los cuales posteriormente serán sujeto de análisis y valoración de riesgos.

7.4.4. Valoración de riesgos. Según SARI, los riesgos deberán ser calculados según la siguiente fórmula:

$$R = I \times (O.A) \times (O.V)$$

[33] Ibid. Pp 4 - 6

Dónde:

R = Riesgo
I = Impacto
O.A = Valoración de la Ocurrencia de la Amenaza
O.V = Valoración de la Ocurrencia de la Vulnerabilidad

7.4.4.1. Valor del impacto. La Valoración del Impacto (I) será la misma obtenida en el nivel de valoración del activo de información, según el promedio de la valoración de los tres pilares de la seguridad.

7.4.4.2. Valor de la Ocurrencia de la amenaza. La evaluación de la amenaza deberá ser realizada de acuerdo con la siguiente escala:

- Valor de 1 cuando la materialización de la amenaza sea rara
- Valor de 2 cuando la materialización de la amenaza sea poco probable.
- Valor de 3 cuando la materialización de la amenaza sea probable
- Valor de 4 cuando la materialización de la amenaza sea muy probable
- Valor de 5 cuando la materialización de la amenaza sea casi cierta.

7.4.4.3. Valor de la Ocurrencia de la vulnerabilidad. La valoración de la vulnerabilidad deberá ser realizada de acuerdo con la siguiente escala:

- Valor de 1 cuando la vulnerabilidad pueda ser aprovechada por la amenaza, sea rara.
- Valor de 2 cuando la vulnerabilidad pueda ser aprovechada por la amenaza, sea poco probable.
- Valor de 3 cuando la vulnerabilidad pueda ser aprovechada por la amenaza, sea probable.
- Valor de 4 cuando la vulnerabilidad pueda ser aprovechada por la amenaza, sea muy probable.
- Valor de 5 cuando la vulnerabilidad pueda ser aprovechada por la amenaza, sea casi cierta.

7.4.5. Nivel de criticidad. Según la propuesta el nivel de criticidad neta es resultado de evaluar el riesgo según los siguientes valores:

- Riesgo con valor entre 1 y 6 toma un valor neto y residual de bajo
- Riesgo con valor entre 7 y 12 toma un valor neto y residual de medio
- Riesgo con valor entre 13 y 18 toma un valor neto y residual de alto
- Riesgo con valor entre 19 y 25 toma un valor neto y residual de crítico.

El nivel de criticidad residual se calcula con el riesgo residual que se obtiene de dividir el riesgo neto entre la calificación de la gestión de los controles existentes, donde estos últimos son evaluados a criterio del responsable de los activos de información, aplicándosele los mismos criterios del riesgo.

7.4.6. Nivel de aceptación del riesgo. La aceptación del riesgo está determinada por el nivel que la alta dirección de la universidad está dispuesta a asumir y que no tenga ningún efecto adverso en la operación del negocio o proceso. Dicho criterio se fundamenta en la aplicación de controles a los riesgos netos con lo que se genera los riesgos residuales.

El riesgo neto es la oportunidad de que suceda algo que tendrá impacto en los objetivos institucionales, mientras que el riesgo residual es el remanente después de la implementación del tratamiento del riesgo (aplicación de controles).

A nivel de aceptación del riesgo, SARI hace relación a los valores de los riesgos tomados de acuerdo con su criticidad neta y residual. Este nivel es el establecido por la dirección de la universidad para adelantar actividades de mitigación de riesgos, donde su nivel de aceptación será dado con base en la siguiente escala:

- Riesgo con valor entre 1 y 5, no se adelantará ninguna actividad al respecto y será ubicado en la línea de Riesgo Aceptable.

- Riesgo con valor entre 6 y 14, no se adelantará ninguna actividad al respecto, pero de ser posible se monitoreará y será ubicado en la línea de Riesgo de Evaluación.

- Riesgo con valor entre 15 y 25, se adelantará actividades las cuales aporten en su mitigación y será ubicado en la línea de Riesgo Inaceptable.

7.5. DESCRIPCIÓN DE LA METODOLOGÍA.

SARI se basa en una metodología llamada OCTAVE Allegro, necesaria para la ejecución y aplicación de todos criterios planteados en él. La metodología consta de ocho pasos que se describen a continuación[34]:
Paso 1 - Se deben establecer los criterios de la medida del riesgo para definir el sistema cualitativo de las medidas (criterios de la medida de riesgo) contra las cuales se podrán evaluar los efectos de un riesgo sobre la misión de la organización y los objetivos del negocio.

Paso 2 – Consiste en desarrollar el perfil para cada activo de la información, que servirá como base en la identificación de amenazas y de riesgos que se realizará en pasos siguientes. El perfil del activo de la información es importante para asegurar que un activo está descrito clara y consistentemente, que hay una definición de los límites del activo y que los requisitos de seguridad para éste están definidos adecuadamente.

Paso 3 – En este paso se identifican los sitios donde la información es almacenada, transportada o donde se procesan los activos de la información, llamados contenedores de la información. Estos contenedores incluyen generalmente hardware, software, servidores, y redes, aunque también pueden incluir artículos tales como carpetas de archivo (donde la información se almacena en forma escrita) o gente.

Paso 4 – Consiste en identificar los motivos de preocupación que pueden llegar a representar las amenazas y sus resultados indeseables.

Paso 5 – Se identifican los panoramas de amenazas, desarrollando perfiles de riesgo del activo de la información, donde el riesgo es la combinación de una amenaza (condición) y del impacto resultante de la amenaza si está actuado sobre una vulnerabilidad (consecuencia).

Paso 6 – Consiste en identificar los riesgos mediante la aplicación de una ecuación, en donde se realiza la sumatoria de dos factores, el primero de ellos es la amenaza y el segundo es el impacto. La sumatoria de estos factores da como resultado el riesgo al que se expone el activo de información.

Paso 7 – Se analizan los riesgos para medir cualitativamente el grado al cual la organización puede verse afectada por una amenaza, evaluando cada riesgo que afecte a cada activo de la información. Esta información se utiliza para determinar

[34] CERT Metodología OCTAVE Op. Cit.. Pp. 3 - 29 (109 Paginas)

qué riesgos necesitan ser atenuados inmediatamente y así dar la prioridad a las acciones de mitigación.

Paso 8 – Finalmente se desarrolla una estrategia de mitigación del riesgo que sea eficaz y eficiente y según la priorización dada en el paso anterior.

Con el desarrollo de esta metodología de ocho pasos se obtiene un plan estratégico de mitigación del riesgo que debe ser aplicado para asegurar la protección de los activos de información analizados. Sin embargo este procedimiento debe ser aplicado en forma periódica, según el periodo determinado por la organización, que en el caso de la universidad se planteó que fuera anualmente.

7.6. CICLO DE APLICACIÓN DE SARI.

Con el rápido ritmo de evolución y surgimiento de nuevas tecnologías se aumenta el número de riesgos a los que se expone un sistema de información, lo que desencadena un proceso de revisión periódica de evaluación de los controles implantados en él.

Por esta razón SARI debe ser revisado y aplicado periódicamente para cumplir con el objetivo principal de garantizar que todas las actividades que se propone en el contexto de la seguridad de la información institucional, logren minimizan o mitigar los riesgos. Es decir SARI es una metodología que se debe aplicar en forma cíclica según el periodo determinado por la División de Tecnología, en este caso la propuesta plantea hacerla en forma anual.

8. APLICACION DE LOS LINEAMIENTOS DE SARI PARA DETERMINAR LOS ACTIVOS DE INFORMACIÓN.

La División de Tecnologías se constituye en un apoyo para el desarrollo de las directrices planteadas por la Vicerrectoría Administrativa y Financiera de la Universidad Autónoma de Occidente, para lo cual esboza la alineación de los objetivos de la organización con los objetivos de la división, a fin de lograr un engranaje óptimo entre las actividades operacionales que sostiene la organización con la tecnología de información y comunicación que soportan dichas actividades. Es así como de esta alineación surge SARI como se describió en el capítulo anterior.

En este capítulo se desarrollan los tres primeros pasos de la metodología planteada por SARI, que consisten en determinar los criterios de evaluación del riesgo en los activos de información, para después desarrollar un perfil en donde se relaciona para cada activo de información su tipo, ubicación, propietario, responsable y custodio (Ver anexo 1), por ultimo identificar los contenedores de información. Todo esto tiene como fin determinar qué es lo que tiene valor para la organización, lo que se constituye en los activos de información.

8.1. DESCRIPCIÓN DE LA DIVISIÓN DE TECNOLOGÍAS COMO PRESTADORA DE SERVICIOS.

Para lograr el engranaje entre las actividades operacionales que sostiene la organización, dadas por las directrices planteadas por la Vicerrectoría Administrativa y Financiera, con la tecnología de información y comunicación que soportan dichas actividades, la División de Tecnologías se presenta como una entidad prestadora de servicios.

La constitución de la división como una entidad prestadora de servicios se fundamenta en el marco de referencia llamado ITIL (Biblioteca de Infraestructura de Tecnologías de Información) [35], el cual propone un conjunto de directrices orientados a la identificación, planificación, entrega y mantenimiento de servicios de TI (Tecnologías de Información).

[35] ITIL: The Basics [en línea]. ITIL. p 3. [Consultado el 26 de Julio del 2011]: Disponible en: http://www.best-management-practice.com/gempdf/ITIL_The_Basics.pdf (5 Paginas)

La concepción de la División de Tecnologías como prestadora de servicios, basada en ITIL, permite que ésta se integre de manera transversal a las estrategias de la universidad, asegurando así que la entidad se dedique a la función específica para la cual fue concebida y se le permita a la división manejar los servicios ofrecidos como activos del negocio, constituyendo un portafolio de servicios.

El contar con este portafolio de servicios le permite a la División de Tecnologías alinearse con las necesidades del negocio; ofrecer niveles de servicio negociados alcanzables; establecer procesos fiables y constantes y brindar una eficacia en la entrega de servicio.

Desde la implantación del marco de referencia ITIL la División de Tecnologías ha tomado un rol dentro de la organización, que lo hace ver como un ente prestador de diferentes servicios tecnológicos y cuyo objetivo principal es el de satisfacer la demanda creada, para brindar un cimiento tecnológico a toda la comunidad que conforma la Universidad Autónoma de Occidente.

8.2. PORTAFOLIO DE SERVICIOS DE LA DIVISIÓN DE TECNOLOGÍAS.

La División de tecnologías diseñó y creó un catálogo de servicios para la comunidad administrativa y académica que conforma a la Universidad Autónoma de Occidente. Los servicios son ofrecidos por los diferentes departamentos en que está constituida la División de Tecnologías; los cuales son soportados por procesos que a su vez están constituidos por procedimientos, que determinan la dependencia, el responsable y el flujograma de todas las actividades que se deben realizar para prestar un servicio de calidad

Por efectos de confidencialidad de la División de Tecnologías solo permitió el acceso aun fragmento del portafolio de servicios, con el cual se logró conocer los servicios necesarios para este proyecto, según el alcance del presente proyecto, solo se tendrán en cuenta para el análisis, los servicios prestados por los departamentos de Redes y Telecomunicaciones y el de Cómputo, los cuales son relacionados en el Cuadro 1[36].

[36] ROJAS, Jorge Armando. Catálogo de servicios de la División de Tecnologías de la Universidad Autónoma de Occidente. Material institucional de la Universidad Autónoma de Occidente. 2010. p 2

Cuadro 1. Servicios ofrecidos por los departamentos de Redes y Telecomunicaciones y el de Cómputo.

Departamento	Servicios
Redes y Telecomunicaciones	• Mensajería Interna • Autentificación de Usuarios • Autogestión de Contraseñas • Autenticación de usuarios y recursos • Almacenamiento personal y por áreas • Almacenamiento de información en red • Servicio de Conectividad a la red cableada • Servicio de conectividad a la red inalámbrica • Servicio de extensiones telefónicas • Servicio de características y facilidades de extensiones • Servicio de correo de voz • Servicio de asignación de claves • Servicio de asignación de listas de abreviadas • Servicio de reporte telefónico por demanda • Servicio de instalación de cableado estructurado • Servicio de mantenimiento correctivo de cableado estructurado • Servicio de mantenimiento correctivo de networking.
Cómputo	• Soporte de aplicación de negocio • Mantenimiento de aplicaciones de negocio • Administración de Servidores Web • Asesorías de implementación de aplicaciones • Desarrollos Internos • Desarrollos Externos • Análisis y viabilidad tecnológica

8.3. RESPONSABLES DE LOS SERVICIOS PRESTADOS POR LA DIVISIÓN DE TECNOLOGÍAS.

Los Departamentos Redes y Telecomunicaciones y de Cómputo están conformados por equipos de trabajo que tienen la responsabilidad de crear el ambiente tecnológico ideal, que brinde la ayuda necesaria para llevar a cabo la tarea principal en cumplimento de las condiciones de continuidad para todos los servicios ofrecidos por estos departamentos, que se constituyen en la base de todas las actividades operativas, tácticas y gerenciales de la universidad.

Los grupos de trabajo están constituidos por los ingenieros, técnicos, auxiliares y jefes de los diferentes departamentos de la división de tecnologías que son los responsables de los servicios, lo que los hace elementos valiosos y como tal, deben ser considerados como activos de información, los cuales se tienen en cuenta en el segundo paso de la metodología planteada por SARI.

El primer lineamiento propuesto por SARI se refiere al primer paso de la metodología OCTAVE Allegro, el cual consiste en la definición de los criterios de la medida del riesgo. Ver capítulo 6. Descripción de SARI.

8.4. PRIMER PASO. DEFINICIÓN DE CRITERIOS DE MEDIDAS DEL RIESGO.

Para el cumplimiento del este primer paso se tomaron los criterios definidos para la valoración de los pilares de la seguridad informática planteados en el capítulo 6. Descripción de SARI también se puede encontrar el anexo 4.

8.4.1. Definición de criterios para la valoración de los activos de información.

El cuadro 2 muestra los criterios de valoración que se deben aplicar para considerar los activos de información que son tenidos en cuenta por SARI.

Cuadro 2. Definición de criterios para la valoración de los pilares de la seguridad informática

Nivel de necesidad de la característica de la seguridad			**Escala**	**Color**
Confidencialidad 33.3%	Integridad 33.3%	Disponibilidad 33.3%		
Mínima			1	
Baja			2	
Media			3	
Moderada			4	
Alta			5	

Para considerar la aplicación de un activo de información en SARI se promedia el valor dado en cada pilar de seguridad y se selecciona para su análisis si este valor es igual o superior a tres.

8.4.2. Definición de los criterios de valoración de riesgos. La valoración del riesgo responde a la fórmula dada en el capítulo 6.

$$R = I \times (O.A) \times (O.V)$$

8.4.2.1. Valoración del impacto. Este valor viene determinado por el promedio obtenido de la valoración de los pilares de seguridad para cada activo considerado.

8.4.2.2. Valoración de la ocurrencia de la **amenaza (O.A).** Los criterios definidos para la evaluación de la probabilidad de la materialización de la amenaza fueron planteados en el capítulo 6, éstos se resumen en el cuadro 3.

Cuadro 3. Definición de criterios para la evaluación de la materialización de la amenaza

Valoración de la ocurrencia de la amenaza	Escala
Materialización de la amenaza sea rara	1
Materialización de la amenaza sea poco probable	2
Materialización de la amenaza sea probable	3
Materialización de la amenaza sea muy probable	4
Materialización de la amenaza sea casi cierta	5

8.4.2.3. Valoración de la vulnerabilidad. (O.V). Los criterios definidos para la evaluación de ocurrencia de la que la vulnerabilidad pueda ser aprovechada por la amenaza, según lo planteado en el capítulo 6 (Descripción de SARI), se resumen en el cuadro 4.

Cuadro 4. Definición de criterios para la evaluación de la vulnerabilidad.

Valoración de que la vulnerabilidad sea aprovechada por una amenaza	Escala
Ocurrencia rara de que la vulnerabilidad pueda ser aprovechada por la amenaza.	1
Ocurrencia poco probable de que la vulnerabilidad pueda ser aprovechada por la amenaza.	2
Ocurrencia probable de que la vulnerabilidad pueda ser aprovechada por la amenaza.	3
Ocurrencia muy probable de que la vulnerabilidad pueda ser aprovechada por la amenaza.	4
Ocurrencia casi cierta de que la vulnerabilidad pueda ser aprovechada por la amenaza.	5

8.4.3. Definición del nivel de criticidad del riesgo. Como se mencionó en el capítulo 6 el riesgo neto es la oportunidad de que suceda algo que tendrá impacto en los objetivos institucionales, mientras que el riesgo residual es el remanente después de la implementación del tratamiento del riesgo (aplicación de controles).

8.4.3.1. Criticidad del riesgo neto. El riesgo neto (R_{NETO}) se calcula con el promedio de la valoración de la ocurrencia de una amenaza y una vulnerabilidad, multiplicada por el impacto, según la siguiente fórmula:

$$R_{NETO} = I * \frac{(O.A + O.V)}{2}$$

Una vez obtenido el riesgo neto, los criterios definidos para la evaluación de la criticidad de éste, según lo planteado en el capítulo 6 (Descripción de SARI), se resumen en el cuadro 5.

Cuadro 5. Definición de evaluación de la criticidad del riesgo neto.

Valoración del nivel de aceptación del riesgo	Escala	línea de ubicación	Color
Riesgo con valor entre	1-6	Riesgo Neto Bajo	
Riesgo con valor entre	7-12	Riesgo Neto Medio	
Riesgo con valor entre	13-18	Riesgo Neto Alto	
Riesgo con valor entre	19-25	Riesgo Neto Critico	

8.4.3.2. Valoración de los controles (V.C.). Es la calificación de la gestión respecto a la efectividad de los controles implantados, emitida mediante un acuerdo entre el evaluador y el director de la División de Tecnologías, este último como responsable de los activos de información. La valoración viene dada por el cuadro 6.

Cuadro 6. Escala de Valoración de Controles (V.C.).

Valoración de controles	Escala
Control no identificado	1
Control identificado	2
Control implantado (pero no necesariamente efectivo)	3
Control funcional (efectivo)	4
Control gestionado (mejoramiento continuo del SGSI)	5

8.4.3.3. Criticidad del riesgo residual. El riesgo residual se refiere al riesgo que aparece después de la evaluación de los controles existentes y su relación con el riesgo neto, este se calcula según la siguiente fórmula:

$$R_{RESIDUAL} = \frac{R_{NETO}}{V.C}$$

Una vez obtenido el riesgo residual, los criterios definidos para la evaluación de la criticidad del riesgo residual, según lo planteado en el capítulo 6 (Descripción de SARI), se resumen en el cuadro 7.

Cuadro 7. Definición de evaluación de la criticidad del riesgo residual.

Valoración del nivel de aceptación del riesgo	Escala	línea de ubicación	Color
Riesgo con valor entre	1-6	Riesgo Residual Bajo	
Riesgo con valor entre	7-12	Riesgo Residual Medio	
Riesgo con valor entre	13-18	Riesgo Residual Alto	
Riesgo con valor entre	19-25	Riesgo Residual Critico	

8.4.4. Definición del nivel de aceptación del riesgo. El nivel de aceptación del riesgo está dado por el análisis que se realiza sobre los riesgos residuales, toda vez que éstos implican designar nuevos controles. Los criterios definidos para la aceptación del riesgo residual o criterio de exposición, según lo planteado en el capítulo 6 (Descripción de SARI), se resumen en el cuadro 8.

Cuadro 8. Definición del nivel de aceptación del riesgo residual.

Valoración del nivel de aceptación del riesgo	Escala	línea de ubicación	Color
Riesgo con valor entre	1-5	Riesgo Aceptable. (A)	
Riesgo con valor entre	6-14	Riesgo de Evaluación. (M)	
Riesgo con valor entre	15-25	Riesgo Inaceptable (I)	

En el cuadro 9 resume el nivel de aceptación del riesgo adoptado por la División de Tecnologías de la Universidad Autónoma, con base a la probabilidad de ocurrencia del riesgo y su nivel de impacto.

Cuadro 9. Definición del nivel de aceptación del riesgo.

		Nivel de Impacto				
		1.Minimo	2.Bajo	2.Medio	4. Moderado	5. Alto
Probabilidad	5. Casi Cierta	A	M	I	I	I
	4. Muy Probable	A	M	M	I	I
	3. Probable	A	M	M	M	I
	2.Poco Probable	A	A	M	M	M
	1.Rara	A	A	A	A	A

8.5. SEGUNDO PASO. IDENTIFICACIÓN DE LOS ACTIVOS.

El segundo paso consiste en el desarrollo del perfil de los activos de información, según la metodología OCTAVE Allegro. Para el cumplimiento de este segundo paso se tomaron los criterios o lineamientos establecidos por SARI.

Para analizar, identificar y crear un perfil de los activos de los departamentos de Redes y Telecomunicaciones y de Cómputo, se tuvo en cuenta los procedimientos que soportan el proceso y que a su vez constituyen la base de los servicios prestados por cada uno de ellos.

Los procedimientos del Departamento de Redes y Telecomunicaciones que se tuvieron en cuenta son:

- 1.1 Solicitud de páginas laboratorio de idiomas
- 1.4 Respaldo de información
- 1.5 Recuperación de información
- 1.6 Plan de backup
- 1.7 Creación del nodo cliente
- 1.8 Creación de sitio sharepoint
- 1.13 Administración de políticas
- 1.20 Soporte de segundo nivel
- 1.21 Direcciones permitidas para el uso de envió de correo masivo

- 1.28 Creación de carpetas compartidas
- 1.30 Actualización de servidores
- 2.1 Configuración de equipos de sistema de voz
- 2.2 Instalación de equipos del sistema de voz
- 2.5 Configuración de switch de core y distribución
- 2.6. Instalación de equipos de transmisión de datos
- 2.7 Configuración de switch de acceso
- 2.8 Mantenimiento preventivo del cuarto de telecomunicaciones
- 2.9 Configuración de equipos de acceso inalámbrico
- 2.10 Control de acceso
- 2.11 Configuración de puntos de cableado
- 2.12 Instalación de puntos de cableado
- 2.13 Mantenimiento preventivo de cableado de comunicaciones
- 2.14 Mantenimiento correctivo de cableado de comunicaciones

Los procedimientos del Departamento de Cómputo que se tuvieron en cuenta son:

- 1.1. Soporte
- 1.2 Administración tecnológica
- 1.3 Desarrollo de software
- 1.4 Mantenimiento de aplicaciones

La identificación de los activos se hace teniendo en cuenta su nombre, su tipo, el propietario, el responsable y el custodio.

8.6. TERCER PASO. IDENTIFICACIÓN DE LOS CONTENEDORES DE INFORMACIÓN.

Este paso consiste en identificar los lugares donde los activos de información están almacenados, son transportados o son procesados y que pueden llegar a constituirse en puntos de vulnerabilidad y amenaza que ponen la información en riesgo.

Los contenedores típicamente pueden ser identificados como activos técnicos, tales como hardware, software o sistema, o pueden ser un objeto físico tales como una hoja de papel, o una persona que sea importante para la organización.

Los principales activos del Departamento de Redes y Telecomunicaciones están ubicados en las llamadas aulas 3 piso 2. Las personas que tienen que ver con este departamento en forma directa conforman el equipo de trabajo en el cual se encuentra el coordinador de intranet, coordinador de internet, coordinador de telecomunicaciones, auxiliar de cableado, auxiliar de soporte e infraestructura y por el jefe del dicho departamento.

Cada integrante de este equipo de trabajo cuenta con una estación de cómputo, excepto el coordinador de telecomunicaciones que tiene a su disposición una estación adicional móvil, la cual es transportada a diferentes sitios de la Universidad, según la necesidad y en la cual realiza los trabajos fuera del departamento. Alguna de las funciones del departamento son la administración de intranet, administración de comunicaciones (Mail, Chat, Telefonía IP), administración de redes, administración de servidores, respaldo de Información, entre otras.

El Departamento de Computo está ubicado en llamadas aulas 3 piso 3, el cual brinda el soporte del proceso de diseño y mantenimiento de sistemas de información. Está conformado por un equipo de trabajo en el que se encuentra el administrador de bases de datos, el jefe del departamento y cuatro analistas; donde cada uno de ellos cuenta con una estación de cómputo, excepto el jefe del departamento, que posee dos estaciones, las cuales son utilizadas para la administración, monitoreo y control de los servicios brindados. Algunas de sus funciones son la de dar soporte a las aplicaciones, administración tecnológica, desarrollo de software, mantenimiento preventivo y correctivo de aplicaciones, entre otras.

Ahora bien existen activos de información relacionados con los procedimientos de dichos departamentos que se encuentran ubicados en otras dependencias de la universidad, como por ejemplo las estaciones de cómputo de usuario final; personas como los jefes de los departamentos solicitantes de los requerimientos y los mismos usuarios de los diferentes aplicativos, que si bien no hacen parte de los departamentos mencionados son considerados dentro de sus procedimientos.

8.7. RESULTADO DEL DESARROLLO DE LOS PASOS DOS Y TRES DE LA METODOLOGÍA: PERFILES DE LOS ACTIVOS DE INFORMACIÓN.

El resultado final del desarrollo de los pasos dos y tres se consigna en los cuadros llamadas Activos de Información e Importancia Relativa, los cuales determinan la

creación de los perfiles de los activos de información. Para la creación de estos perfiles se diligenciaron los ítems descritos en el cuadro 10.

Cuadro 10. Descripción de ítems para la creación de los perfiles de los Activos de Información e Importancia Relativa.

Nombre del ítem	Descripción
Activo de Información	Cualquier persona o elemento que tenga valor para la Universidad desde el punto de vista del manejo, manipulación, gestión y/o custodia de información sensible.
Tipo de Activo	- Espacio Físico / Infraestructura - Persona - Dato - Documento - Sistema de Información - Sistema de Almacenamiento - Dispositivo - Servicio Tecnológico - Estación de trabajo - Sistema de Informático
Ubicación del Activo	Hace referencia al nombre del espacio Físico o Lógico
Propietario	Área Funcional que se encuentra definida por el Procedimiento del Sistema de Gestión de Calidad de cada una de las Divisiones.
Responsable	Determinado por el cargo del funcionario encargado de tomar decisiones frente a los activos de información, basado siempre en el cumplimiento de las expectativas de seguridad que se tienen sobre el mismo, generadas en función de proteger la Confidencialidad, Integridad y Disponibilidad del Activo de Información
Custodio	Hace referencia al cargo del funcionario encargado de adelantar labores, con base en las decisiones tomadas por el Responsable, en pro de garantizar el cumplimiento de las expectativas de seguridad que se tienen sobre el Activo de Información. Así mismo, es el encargado de hacer confluir las expectativas de seguridad del Responsable y las necesidades de usabilidad del activo por parte de los usuarios y/o clientes del mismo.

Para cada procedimiento que soporta los diferentes servicios brindados por la División de Tecnologías en los departamentos analizados, se elaboró una tabla con los ítems especificados que caracterizan cada uno de los activos identificados.

Las tablas, correspondientes al desarrollo del perfil de los activos de información de cada uno de los procedimientos de los departamentos de Redes y Telecomunicaciones y de Cómputo, se pueden ver en el anexo 1.

Una vez obtenidos los perfiles para los activos de información identificados en cada procedimiento se enfocó el análisis a las estaciones de trabajo de dichos departamentos, dado que todas las actividades de administración, monitoreo y control de los servicios brindados por ellos son realizadas desde sus estaciones de trabajo.

9. IDENTIFICACION DE LAS ESTACIONES DE TRABAJO

Como se mencionó anteriormente la División de Tecnologías pose un catálogo de servicios que son ofrecidos a la comunidad académica y administrativa, los cuales son emitidos y administrados desde departamentos que conforman esta División. Los servicios están soportados por procesos que a su vez están conformados por procedimientos, los cuales tienen un responsable y las correspondientes actividades que deben realizar cada uno de ellos; todo esto constituyen activos de información, cuya caracterización se planteó en el capítulo anterior.

Ahora bien, dado que todas estas actividades de administración, monitoreo y control de los servicios brindados por los departamentos de la División son realizadas desde sus estaciones de trabajo, se enfoca el análisis únicamente a este tipo de activos. Por tal razón se identifican en primer lugar las estaciones de trabajo que ejecutan las actividades de los procedimientos de los servicios de los departamentos de Redes y Telecomunicaciones y Cómputo. A continuación para cada una de ellas se les hace la evaluación respecto a sus necesidades de aplicación de los pilares de seguridad (confidencialidad, integridad y disponibilidad), con esto se determina cuáles de ellas son críticas y de acuerdo con SARI deben ser objeto de un análisis de seguridad informática más profundo.

Una vez identificadas estas estaciones de trabajo críticas se continúa con la aplicación de la metodología planteada por SARI, en la cual, en primer lugar, se identifican las áreas o motivos de preocupación que derivan en un panorama de amenazas. A este panorama de amenazas se le relaciona con las vulnerabilidades que presentan cada una de ellas, determinando los posibles riesgos a los que se ven expuestas, para finalmente crear la matriz de riesgos de estos activos de información críticos, con lo que se le daría cumplimiento a los pasos cuatro, cinco y seis de dicha metodología.

9.1. IDENTIFICACION DE LAS ESTACIONES DE TRABAJO.

Una vez definidos los perfiles de los activos de información se centra el análisis en las estaciones de trabajo por las razones anteriormente expuestas. La identificación de dichas estaciones fue validada con los correspondientes jefes de los departamentos de Redes y Telecomunicaciones y el de Cómputo, donde adicionalmente se identificó su responsable y su custodio.

9.1.1 Estaciones de trabajo de Departamento de Redes y Telecomunicaciones. A continuación se listan las estaciones de trabajo identificadas con su correspondiente responsable y custodio.

Cuadro 11. Estaciones de trabajo del Departamento de Redes y Telecomunicaciones.

Activo de Información	Cargo del usuario	Responsable	Custodio
Estación de trabajo # 1	Coordinador Intranet	Director División de Tecnologías	Jefe del Departamento de Redes y Telecomunicaciones
Estación de trabajo # 2	Coordinador de internet	Director División de Tecnologías	Jefe del Departamento de Redes y Telecomunicaciones
Estación de trabajo # 3	Jefe del Departamento	Director División de Tecnologías	Jefe del Departamento de Redes y Telecomunicaciones
Estación de trabajo # 4	Coordinador de Telecomunicaciones	Director División de Tecnologías	Jefe del Departamento de Redes y Telecomunicaciones
Estación de trabajo # 5	Coordinador de Telecomunicaciones	Director División de Tecnologías	Jefe del Departamento de Redes y telecomunicaciones
Estación de trabajo # 6	Auxiliar de Cableado	Director División de Tecnologías	Jefe del Departamento de Redes y telecomunicaciones
Estación de trabajo # 7	Ing. de Redes(Cargo que existe, pero no esta activo)	Director División de Tecnologías	Jefe del Departamento de Redes y telecomunicaciones
Estación de trabajo # 8	Admón. Backup (Cargo que existe, pero no esta activo)	Director División de Tecnologías	Jefe del Departamento de Redes y telecomunicaciones
Estación de trabajo # 9	Auxiliar de Soporte e infraestructura	Director División de Tecnologías	Jefe del Departamento de Redes y telecomunicaciones

9.1.2 Estaciones de trabajo del Departamento de Cómputo. En el cuadro 12 listan las estaciones de trabajo identificadas en los procedimientos que soportan los servicios ofrecidos desde el Departamento de Cómputo, con su correspondiente responsable y custodio.

Cuadro 12. Estaciones de trabajo del Departamento de Cómputo.

Activo de Información	Cargo del usuario quien la utiliza	Responsable	Custodio
Estación de trabajo # 1	Analista 1	Director División de Tecnologías	Jefe del Departamento de Redes y telecomunicaciones
Estación de trabajo # 2	Analista 2	Director División de Tecnologías	Jefe del Departamento de Redes y telecomunicaciones
Estación de trabajo # 3	Analista 3	Director División de Tecnologías	Jefe del Departamento de Redes y telecomunicaciones
Estación de trabajo # 4	Analista 4	Director División de Tecnologías	Jefe del Departamento de Redes y telecomunicaciones
Estación de trabajo # 5	Administrador de bases de Datos	Director División de Tecnologías	Jefe del Departamento de Redes y telecomunicaciones
Estación de trabajo # 6	Jefe del Departamento	Director División de Tecnologías	Jefe del Departamento de Redes y telecomunicaciones
Estación de trabajo # 7	Jefe del Departamento	Director División de Tecnologías	Jefe del Departamento de Redes y telecomunicaciones

En total se identificaron nueve estaciones de trabajo en el Departamento de Redes y Telecomunicaciones y siete en el de Cómputo. A estos activos de información se les evalúa su necesidad de aplicación de los pilares de seguridad, para determinar su criticidad.

9.2. EVALUACION DE LA CRITICIDAD DE LAS ESTACIONES DE TRABAJO.

Para esta evaluación se contó con el responsable de cada estación de trabajo, que en este caso es el Director de la División de Tecnologías, el cual emitió la calificación sobre la necesidad de aplicar en ellas los pilares de la seguridad informática (confidencialidad, integridad y disponibilidad).

Los valores dados a cada pilar de la seguridad son sumados y promediados (puesto que su peso por definición de SARI es igual) y el valor obtenido o Valor del Activo, es evaluado para determinar su nivel de criticidad, tal como se expuso en el capítulo 7. (Ver cuadro 2). Este valor también es utilizado como valor del impacto. (Ver 7.4.2.1.) A continuación se relacionan las estaciones de trabajo con los valores dados a los pilares de seguridad informática y el valor del activo obtenido.

9.2.1 Valor del activo de las estaciones de trabajo del Departamento de Redes y Telecomunicaciones. En el cuadro 13 muestra la calificación de los pilares de la seguridad, por parte del responsable de las estaciones de trabajo.

Cuadro 13. Valor del activo de las estaciones de trabajo del Departamento de Redes y Telecomunicaciones.

Activo de Información	Cargo del usuario quien la utiliza.	Necesidad de Confidencialidad	Necesidad de Integridad	Necesidad de Disponibilidad	Valor del activo
Estación de trabajo # 1	Coordinador Intranet	4	5	4	4
Estación de trabajo # 2	Coordinador de internet	4	5	4	4
Estación de trabajo # 3	Jefe del Departamento	4	5	4	4
Estación de trabajo # 4	Coordinador de Telecomunicaciones	4	5	4	4
Estación de trabajo # 5	Coordinador de Telecomunicaciones	4	5	4	4
Estación de trabajo # 6	Auxiliar de Cableado	4	5	4	4

Cuadro 13.(Continuación).

Estación de trabajo # 7	Ing. de Redes(Cargo que existe, pero no esta activo)	4	5	4	4
Estación de trabajo # 8	Admón. Backup (Cargo que existe, pero no esta activo)	4	5	4	4
Estación de trabajo # 9	Auxiliar de Soporte e infraestructura	4	5	4	4

9.2.2 Valor del activo de las estaciones de trabajo del Departamento de Cómputo. En el cuadro 14 muestra la calificación de los pilares de la seguridad, por parte del responsable de las estaciones de trabajo.

Cuadro 14. Descripción de las estaciones de trabajo, responsable y custodio identificadas en los procedimientos del departamento de cómputo.

Activo de Información	Cargo del usuario quien la utiliza	Necesidad De Confidencialidad	Necesidad De Integridad	Necesidad De Disponibilidad	Valor del activo
Estación de trabajo # 1	Analista 1	4	5	4	4
Estación de trabajo # 2	Analista 1	4	5	4	4
Estación de trabajo # 3	Analista 1	4	5	4	4
Estación de trabajo # 4	Analista 1	4	5	4	4
Estación de trabajo # 5	Administrador de bases de Datos	4	5	4	4
Estación de trabajo # 6	Jefe del Departamento	4	5	4	4
Estación de trabajo # 7	Jefe del Departamento	4	5	4	4

Como puede verse el valor del activo para todas las estaciones de trabajo, tanto del departamento de Redes y Telecomunicaciones, como para el de Cómputo es de cuatro, lo cual indica que todas ellas deben ser consideradas como críticas al aplicarles la tabla de nivel de criticidad (cuadro 2).

Si se observa la calificación dada en cada uno de los pilares de seguridad para cada estación de trabajo se puede ver que los valores son los mismos, es decir su comportamiento respecto a la necesidad de aplicar los pilares es igual para todas, por lo que se determinó, sin pérdida de generalidad, realizar una sola matriz de riegos para todas ellas.

Estos valores se pueden ver también en el anexo A.

9.3. APLICACIÓN DE LA METDOLOGIA PLANTEADA POR SARI A LOS ESTACIONES DE TRABJOS CRITICAS.

Una vez identificados los activos críticos, que para este caso, son todas las estaciones de trabajo de los departamentos de Redes y Telecomunicaciones y de Cómputo, se procede a aplicar los siguientes pasos de la metodología de SARI.

9.3.1 Paso cuarto. Identificación de los motivos de preocupación. En este paso se crea un panorama del mundo real de acciones externas e internas que preocupan al responsable del activo crítico, que en este caso es el director de la División de Tecnologías, basado en las acciones a las que se enfrenta día tras día, en el de cumplimiento del objetivo principal de dicha división.

De acuerdo con reuniones sostenidas con dicho responsable se determinaron los siguientes motivos de preocupación para estas estaciones críticas:

- Riesgos sociales
- Percepciones equivocadas de la seguridad
- El enemigo interno
- El enemigo externo
- Utilización de nuevas tecnologías
- Eventos Naturales
- Agresión a lo que tiene valor para la organización
- Fuga de información
- Falta de credibilidad a la gestión

- Administración inadecuada de la información sensible
- Errores humanos

Estos motivos de preocupación son la base para el desarrollo del panorama de amenazas.

9.3.2 Paso quinto. Panorama de amenazas. Basado en el panorama de preocupaciones expuesto, se creó un panorama de amenazas tanto de tipo externo como interno, el cual podría llegar a intranquilizar al responsable del activo y en el peor de los casos impedir la administración de los servicios desde las estaciones de trabajo.

El panorama de amenazas planteado es el siguiente:

9.3.2.1. Amenazas de origen externo.

- Agresiones Técnicas (Phishing, Ingeniería Social)
- Intervenciones humanas no autorizadas (Acceso a espacios restringidos)
- Acceso de terceros a información sensible.
- Obstaculización para la prestación del servicio.
- Robo y/o daño de activos de información.
- Eventos Naturales (Terremotos, Inundaciones, Incendios)

9.3.2.2. Amenazas de origen interno.

- Filtración de información a través de la estaciones de trabajo
- Encubrimiento de identidad por parte de un usuario o personal del grupo de trabajo
- Re-ruteo de comunicaciones por donde viaja información sensible
- Eliminación no controlada de información sensible
- Acceso no autorizado a las estaciones de trabajo
- Manipulación de software riesgoso en las estaciones de trabajo
- Error operacional por parte del personal
- llevarse de información al momento de ser desvinculado de la división
- intentos de Acceso a la red no autorizados
- Perdida de una estación de trabajo criticas
- instalar software en las estaciones de trabajo
- Fuga de información
- Perdida de la imagen institucional

Una vez determinado el panorama de amenazas internas y externas se le relacionan las vulnerabilidades que pueden favorecer la amenaza. En el cuadro 15 se realiza la asociación de las vulnerabilidades con las amenazas planteadas.

Cuadro 15. Descripción de panorama de amenazas con sus respectivas vulnerabilidades.

Amenazas	Vulnerabilidades
Ataque de Phishing	Falta de Política de correo seguro anti Phishing
	Falta de conciencia de los Integrantes de los departamentos involucrados en el proyecto
	Falta de Política de seguridad Informática en las estaciones de trabajo
	Falta de Política de utilización de servicios con certificados de seguridad
Ataque con Ingeniería Social	Falta de conciencia de los Integrantes de los departamentos involucrados en el proyecto
	Falta de directrices en la emisión de la información
Eventos Naturales (Terremotos, Inundaciones)	Falta de planes de contingencia o procedimientos de recuperación
	Ubicación en áreas susceptibles a desastres naturales (tormentas o vendavales)
Eventos Naturales (Incendios)	Falta de Sistema contra incendios
Intervenciones humanas no Autorizadas (Acceso a espacios restringidos)	Falta de controles físico
	Descuido del custodio de las áreas restringidas

Cuadro 15.(Continuación).

Acceso de Terceros a información sensible que se puede obtener desde estaciones de trabajo	Falta de controles Lógicos
	Falta de Política de acceso al información
Obstaculización para la prestación del servicios	Falta de controles Lógicos
Robo de activos de información	Falta de controles físico
Daño de activos de información	Falta de conciencia de los Integrantes de los departamentos involucrados en el proyecto
Filtración de información a través de la estaciones de trabajo	Falta de controles Lógicos
Encubrimiento de identidad por parte de un usuario o personal del grupo de trabajo	Falta de directrices en la gestión de acceso de los usuarios
Re-ruteo de comunicaciones por donde viaja información sensible	Falta de controles Lógicos
Eliminación no controlada de información sensible	Falta de controles Lógicos
Acceso no autorizado a las estaciones de trabajo	Falta de controles físico
	Falta de controles Lógicos
Manipulación de software riesgoso en las estaciones de trabajo	Falta lineamientos de Buen Uso de recursos tecnológicos
	Falta de controles Lógicos
Error operacional por parte del personal	Falta de plan de formación y capacitación
llevarse de información al momento de ser desvinculado de la división	Falta de controles Lógicos
	Falta de acuerdo de confidencialidad
intentos de Acceso a la red no autorizados	Falta de directrices en la administración de los servicios de red

Cuadro 15.(Continuación).

Perdida de una estación de trabajo criticas	Falta de un inventario
	Falta de controles físico
instalar software en las estaciones de trabajo	Falta de controles Lógicos
Fuga de información	Falta de directrices en la emisión de la información
	Falta de controles Lógicos
	Falta de controles físico
Perdida de la imagen institucional	Falta de Comunicación de eventos y debilidades en seguridad

Una vez definido este panorama de amenazas y vulnerabilidades se procede a valorar el riesgo aplicando la fórmula dada en el capítulo anterior (7.4.2.), donde es necesario valorar la probabilidad de ocurrencia de la amenaza, la probabilidad de ocurrencia de la vulnerabilidad y el impacto en cada estación de trabajo crítica. Es decir se procede a identificar los riesgos, generando la matriz de riesgos.

9.3.3. Paso sexto. Identificación de riesgos. Para el cumplimiento de este sexto paso se plantearon 35 vulnerabilidades, ligadas a las 22 amenazas a las que las estaciones de trabajo críticas están expuestas en las operaciones diarias en la ejecución de las actividades para la prestación de los servicios de la División de Tecnología. Para la generación de la matriz de riesgo se utilizaron los ítems descritos en el cuadro 16.

Cuadro 16. Descripción de ítems para la generación de la matriz de riesgos

Nombre del ítem	Descripción
Tipo de Activo	Clasificación de los tipos de activos.
Activo de información	Nombre de activo de información
Valoración del Impacto	Valoración del Activo de Información (Especificada en el documento Activos de Información e Importancia Relativa)

Cuadro 16.(Continuación).

Ubicación del Activo	Espacio físico o lógico en el que se encuentra el Activo de Información. Los riesgos varían de acuerdo con la ubicación.
Amenazas	Descripción de cada amenaza a la cual se encuentra expuesto el activo de información
Probabilidad Amenaza	Valoración de Probabilidad de Ocurrencia de la Amenaza utilizando la escala expuesta (Ver capítulo seis)
Pilar de la Seguridad Afectado	Característica de la seguridad de la información que se ve golpeado por la amenazas
Vulnerabilidades	Condiciones generadas por la universidad las cuales exponen a un peligro potencial el activo de información
Probabilidad Vulnerabilidad	Valoración de la Probabilidad de Ocurrencia que la vulnerabilidad pueda ser aprovechada por la amenaza en un periodo de un año, según la escala expuesta (Ver capítulo seis)
Posibilidad de Ocurrencia	Cálculo de la Probabilidad de Ocurrencia (Probabilidad Amenaza + Probabilidad Vulnerabilidad)/2
Cálculo de Riesgo Neto	Valoración del Riesgo Neto (Impacto x Probabilidad de Ocurrencia)
Criticidad Neta	Escala de Criticidad Neta de acuerdo con el valor calculado en el ítem de Cálculo de Riesgo Neto
Controles Existentes	Descripción de los Controles Existentes para la Mitigación del Riesgo Neto
Evaluación del Control	Calificación de gestión, de acuerdo con la efectividad de los controles implantados, (Ver capítulo siete)
Riesgo Residual	Calificación del Riesgo residual, (Riesgo Neto / Calificación de la Gestión)
Criticidad Residual	Escala de Criticidad residual, de acuerdo con el valor calculado en el ítem de Riesgo Residual (Ver capítulo siete)
Niveles de Aceptación del Riesgo	Criterio de Exposición (Aceptación del Riesgo), Ver capitulo siete.
Objetivos de Control	Fin con el que se plantea el nuevo control
Controles	Intervención que busca la mitigación del riesgo

Para la valoración de los ítems de probabilidad de ocurrencia de la amenaza y de probabilidad de ocurrencia de la vulnerabilidad, el responsable de las estaciones críticas asignó los valores correspondientes basados en su experiencia y conocimiento; al momento de evaluar la existencia de controles actuales, se

determinó que, para las vulnerabilidades encontradas, no existían controles, por lo que su calificación fue de uno (inexistencia de controles).
Con estos ítems se elaboró la matriz de riesgos para todas las estaciones de trabajo críticas, aplicando las fórmulas y directrices que se definieron en el primer paso de la metodología planteada por SARI (ver capítulo siete), esta matriz se puede ver en la tabla que se muestra en el anexo 2.

Esta matriz de riesgo sirve para hacer un análisis de éstos a fin de determinar las fortalezas y debilidades del esquema de seguridad informática con los cuales se plantean los correspondientes controles que mitiguen dichos riesgos.

10. FORTALEZAS Y DEBILIDADES

Una vez planteada la matriz de riesgos para todas las estaciones de trabajo críticas, se procede a hacer un análisis pormenorizado de los riesgos que pueden aparecer en el esquema de seguridad para dichos activos.

Como producto de este análisis se determinan las fortalezas y debilidades del esquema de seguridad informática con el que cuenta actualmente la División de Tecnologías, a fin de mitigar los riesgos a los que se exponen las estaciones de trabajo críticas, desde donde se administra la información sensible de la comunidad académica y administrativa de la Universidad Autónoma de Occidente.

En el análisis de los riesgos se aplicaron las directrices planteadas en el primer paso de la metodología SARI (ver capítulo siete), determinando el nivel de aceptación del riesgo y a continuación se establecieron las fortalezas y debilidades del esquema, dando cumplimiento al séptimo paso de la metodología planteada por SARI.

10.1 PASO SÉPTIMO. ANÁLISIS DE RIESGOS.

Como se mencionó anteriormente para el análisis del riesgo se utiliza la matriz de generada en el paso sexto (ver anexo dos). La información consignada en dicha matriz brinda la caracterización de todos los componentes que constituyen los riesgos a los que se expone la organización en la consecución de sus tareas diarias, el esquema también brinda los controles que propone la mitigación de cada riesgo identificado.

Para cada estación de trabajo crítica se determina la posible ocurrencia del riesgo, la cual viene dada por el promedio de la suma de la valoración de la ocurrencia de la amenaza con la valoración de la ocurrencia de la vulnerabilidad, esto permite determinar el riesgo neto, el cual es calculado multiplicando este valor con el valor obtenido por el impacto. (Ver fórmula en el capítulo siete). Con el valor obtenido por el riesgo neto se determina la criticidad neta, la cual es calculada según la tabla de valoración definida en el capítulo siete, esta criticidad permite determinar si el riesgo es alto, medio o bajo.

De acuerdo con el análisis de las estaciones de trabajo criticas consideradas se encontró que no existen controles para las vulnerabilidades planteadas (ver

capítulo ocho), por lo que la valoración (calificación) del control es de uno, por lo tanto el riesgo residual es el mismo riesgo neto (riesgo residual = riesgo neto / valoración del control), que como se mencionó anteriormente, el riesgo residual es el que determina la aplicación de nuevos controles como oportunidades de mejora; el riesgo residual es entonces el riesgo que aparece cuando los controles son deficientes o no existen. (En este caso no existen), ahora bien para el análisis de riesgos y determinación de fortalezas y debilidades se toman todos los riesgos. Aquellos riesgos cuya valoración es inaceptable se le proponen los controles correspondientes que determinan las oportunidades de mejora. A los otros riesgos (aceptable o moderado) se le proponen controles tendientes a contrarrestar las vulnerabilidades para anticiparse a que éstos se conviertan en inaceptables. La cantidad de vulnerabilidades referenciada por las amenazas se puede ver en la cuadro 17.

Cuadro 17. Cantidad de vulnerabilidades referenciadas por las amenazas.

Cantidad de vulnerabiliades referenciadas por la amenazas	
Tipo de Vulnerabilidad	**Cantidad**
Falta de controles Lógicos	10
Falta de controles físico	5
Falta de conciencia de los Integrantes de los departamentos involucrados en el proyecto	3
Falta de directrices en la emision de la informacion	2
Falta de Politica de seguridad Informatica en las estaciones de trabajo	1
Falta de acuerdo de confidencialidad	1
Falta de Political de acceso al informacion	1
Falta de directrices en la administracion de los servicios de red	1
Falta de Politica de correo seguro anti Phishing	1
Falta de Sistema contra incendios	1
Falta de Politica de utilizacion de servicios con certificados de seguridad	1
Falta de un inventario	1
Falta de Comunicación de eventos y debilidades en seguridad	1
Negligencia del custodio de las areas restrigidas	1
Falta lineamientos de Buen Uso de recursos tecnologicos	1
Falta de directrices en la gestion de acceso de los usuarios	1
Ubicación en áreas susceptibles a desastres naturales (tormentas o vendavales)	1
Falta de plan de formación y capacitación	1
Falta de planes de contingencia o procedimientos de recuperación	1
Total general	**35**

Como puede verse la principal vulnerabilidad se refiere a la falta de controles lógicos (10), seguido por la falta de controles físicos (5) y la falta de conciencia de los integrantes involucrados en el proyecto (3), la otra vulnerabilidad que se repite es la falta de directrices en la emisión de la información (2). El análisis se inició teniendo en cuenta éstos valores, bajo la premisa de que si una vulnerabilidad es recurrente, se debe priorizar su análisis para determinar la identificación de los controles, sin embargo no fue el único criterio que se tuvo en cuenta, puesto que después se analizaron los niveles de aceptación del riesgo.

De la matriz se puede observar que cada amenaza que se vale de las vulnerabilidades planteadas genera el mismo impacto sobre la seguridad informática en la organización, lo que constituye un riesgo, es decir todas las amenazas planteadas se constituyen en riesgos para la seguridad, como puede verse en el cuadro 18.

Cuadro 18. Lista de riesgos.

Cuadro de Riesgos	
Amenazas y Vulnerabilidades	**Impacto**
Acceso de Terceros a información sensible que se puede obtener desde estaciones de trabajo	
Falta de controles Lógicos	4
Falta de Política de acceso al información	4
Acceso no autorizado a las estaciones de trabajo	
Falta de controles físico	4
Falta de controles Lógicos	4
Ataque con Ingeniería Social	
Falta de conciencia de los Integrantes de los departamentos involucrados en el proyecto	4
Falta de directrices en la emisión de la información	4
Ataque de Phishing	
Falta de conciencia de los Integrantes de los departamentos involucrados	4
Falta de Política de correo seguro anti Phishing	4
Falta de Política de seguridad Informática en las estaciones de trabajo	4
Falta de Política de utilización de servicios con certificados de seguridad	4
Daño de activos de información	
Falta de conciencia de los Integrantes de los departamentos involucrados	4
Eliminación no controlada de información sensible	
Falta de controles Lógicos	4

Cuadro 18.(Continuación).

Encubrimiento de identidad por parte de un usuario o personal del grupo de trabajo	
Falta de directrices en la gestión de acceso de los usuarios	4
Error operacional por parte del personal	
Falta de plan de formación y capacitación	4
Eventos Naturales (Incendios)	
Falta de Sistema contra incendios	4
Eventos Naturales (Terremotos, Inundaciones)	
Falta de planes de contingencia o procedimientos de recuperación	4
Ubicación en áreas susceptibles a desastres naturales (tormentas o vendavales)	4
Filtración de información a través de la estaciones de trabajo	
Falta de controles Lógicos	4
Fuga de información	
Falta de controles físico	4
Falta de controles Lógicos	4
Falta de directrices en la emisión de la información	4
instalar software en las estaciones de trabajo	
Falta de controles Lógicos	4
intentos de Acceso a la red no autorizados	
Falta de directrices en la administración de los servicios de red	4
Intervenciones humanas no Autorizadas (Acceso a espacios restringidos)	
Falta de controles físico	4
Descuido del custodio de las áreas restringidas	4
llevarse de información al momento de ser desvinculado de la división	
Falta de acuerdo de confidencialidad	4
Falta de controles Lógicos	4
Manipulación de software riesgoso en las estaciones de trabajo	
Falta de controles Lógicos	4
Falta lineamientos de Buen Uso de recursos tecnológicos	4
Obstaculización para la prestación del servicios	
Falta de controles Lógicos	4
Perdida de una estación de trabajo criticas	
Falta de controles físico	4
Falta de un inventario	4
Perdida de la imagen institucional	
Falta de Comunicación de eventos y debilidades en seguridad	4
Re-ruteo de comunicaciones por donde viaja información sensible	
Falta de controles Lógicos	4

Cuadro 18.(Continuación).

Robo de activos de información	
Falta de controles físico	4

Como puede verse en el cuadro anterior la gravedad de todas las amenazas tienen un impacto de 4, lo cual indica que requiere un alto nivel de aplicación de los pilares de la seguridad, que de no ser empleado podría llegar a afectar de manera evidente la seguridad de las estaciones de trabajo.

Esto hace que se tenga que considerar todas las amenazas que pueden llegar a afectar el esquema de seguridad de las estaciones de trabajo, por tal motivo se hace un análisis de fortalezas y debilidades de dicho esquema, para determinar los controles que deben ser aplicados como oportunidades de mejora.

10.2. IDENTIFICACION DE FORTALEZAS Y DEBILIDADES SOBRE EL ESQUMA DE SEGURIDAD INFORMÁTICA.

A partir del análisis de los riesgos se identifican las fortalezas y debilidades que aplican sobre el esquema de seguridad de las estaciones de trabajo.

10.2.1. Fortalezas identificadas. De común acuerdo con el Director de la División de Tecnología de la universidad se propuso hacer el presente trabajo bajo un escenario del peor de los casos, en el cual no existen controles para ninguna de las vulnerabilidades identificadas, con el fin de proponer controles a todas las vulnerabilidades, pero haciendo énfasis en aquellas cuyo nivel de aceptación del riesgo es inaceptable según los lineamientos planteados por SARI (ver capítulo siete).

En este orden de ideas al esquema de seguridad informática se le identifica como fortaleza el hecho de ser capaz de identificar y valorar la probabilidad de ocurrencia de los riesgos.

Otra fortaleza que presenta el esquema es la forma de identificar el efecto que tendría el accionar de los riesgos en los activos de información, llamando la atención sobre aquellos que son más críticos para la División, esto permite que se enfoquen los esfuerzos de mitigar dichos riesgos sobre estos activos, pero sin

dejar de considerar los demás. Es decir permite jerarquizar los riesgos en forma tal que se prioricen aquellos más críticos o que más efectos nocivos tengan.

10.2.2. Debilidades identificadas. Al considerar un escenario del peor caso de no tener controles, la principal debilidad en el esquema de seguridad es el no tener la capacidad de proponer, aplicar y mejorar continuamente controles que brinden tranquilidad y confianza necesaria para prestación óptima de los servicios.

Otras debilidades encontradas en el esquema actual de seguridad informática se basan en las vulnerabilidades identificadas, dado que permiten la aparición de las consecuencias del riesgo por la mayor probabilidad de ocurrencia de la amenaza, Estas son:

- Falta de Política de correo seguro anti Phishing
- Falta de conciencia de los Integrantes de los departamentos involucrados en el proyecto
- Falta de Política de seguridad Informática en las estaciones de trabajo
- Falta de Política de utilización de servicios con certificados de seguridad
- Falta de conciencia de los Integrantes de los departamentos involucrados en el proyecto
- Falta de directrices en la emisión de la información
- Falta de planes de contingencia o procedimientos de recuperación
- Ubicación en áreas susceptibles a desastres naturales (tormentas o vendavales)
- Falta de Sistema contra incendios
- Falta de controles físico
- Descuido del custodio de las áreas restringidas
- Falta de controles Lógicos
- Falta de directrices en la gestión de acceso de los usuarios
- Falta lineamientos de Buen Uso de recursos tecnológicos
- Falta de acuerdo de confidencialidad
- Falta de directrices en la administración de los servicios de red
- Falta de Comunicación de eventos y debilidades en seguridad.

Continuando con el análisis de riesgos se procede a aplicar la directriz de SARI (ver capítulo 7) en la cual se determina si el riesgo es aceptable (valor de 1 a 5) moderado (valor de 6 a 14) e inaceptable (valor de 15 a 25). El resultado de esta valoración se puede ver en el anexo 3.

Una vez analizados los riesgos, fortalezas y debilidades del esquema actual de la seguridad informática y basada en el peor escenario planteado, se procede a proponer controles que se convierten en oportunidades de mejora del esquema actual de seguridad informática de la universidad.

Se determinó plantear los controles correspondientes a todas las vulnerabilidades o debilidades del esquema de seguridad buscando, para cada una de ellas, el control que debe ser aplicado, basados en la norma ISO 27002, como puede verse en el anexo 3, donde se muestran los controles propuestos sobre estas vulnerabilidades.

El análisis de los riesgos inaceptables y los controles propuestos se convierten en una oportunidad de mejora, en donde a cada control de dicho riesgo se le determinan recomendaciones que contribuyen a elevar la seguridad informática dentro de la División de Tecnologías, con el fin de cambiar el estado de los puntos débiles a fortalezas.

11. PROPUESTAS DE MEJORA AL ESQUEMA DE SEGURIDAD INFORMÁTICA

Las oportunidades de mejora se enfocan en proponer controles que mitiguen las consecuencias de los riesgos identificados como riesgos inaceptables, planteados en el capítulo anterior, con el fin de proponer soluciones aplicables sobre el esquema de seguridad informática abarcando la seguridad en las estaciones de trabajo críticas de la División de Tecnologías.

11.1 PASO OCTAVO. SELECCIÓN DEL ENFOQUE DE MITIGACIÓN.

En el cumplimiento de este paso se tomaron las vulnerabilidades de los riesgos inaceptables (valor entre 15 y 25) y los controles propuestos para mitigar dichos riesgos; a cada control se le determinó su objetivo y las actividades necesarias para su implementación, dando así como resultado la oportunidad de mejora del esquema de seguridad informática de la División de Tecnología.

Cabe notar que las oportunidades de mejora planteadas están relacionadas también con los componentes que de una u otra manera tienen que ver con las estaciones de trabajo. Es decir no se debe considerar la estación de trabajo como un ente físico o hardware, sino que a su vez incluye, procesos, información y recurso humano, con lo que se cubre un amplio porcentaje del esquema de seguridad informática en general.

A continuación se plantean las oportunidades de mejora a las debilidades o vulnerabilidades encontradas, cuyo nivel de aceptación del riesgo es inaceptable. Estas oportunidades se determinan basadas en los controles planteados por la norma ISO 27001[37] e ISO 27002[38], guía de implementación o buenas prácticas de la seguridad informática.

11.1.1. Falta de política de correo seguro anti-phishing. Para eliminar esta vulnerabilidad, la propuesta de mejora se basa en el objetivo de control A.5.1. Política de seguridad de la información, del cual se extrae el siguiente control:

[37] Referencia ISO 27001 Op. Cit. 15
[38] Referencia ISO 27002 OP. Cit. 38

- Documento de Política de seguridad de la información.

El control A.5.1.1. Documento de Política de seguridad de la información, propone definir en términos generales lo que se busca con la creación de la política de correo seguro. Para ello es necesario definir un documento en donde se consigne el objetivo general, alcance e importancia de crear una política de correo seguro Anti-Phishing.

Es necesario alinear de manera clara y objetiva esta política con las metas y los principios de seguridad informática, planteada por la División de tecnologías, con los objetivos de la organización.

En el documento también debe quedar consignada la estructura necesaria que asegure el cumplimento de esta política teniendo en cuenta las normas, directrices y principios de seguridad, exponiendo claramente las responsabilidades generales y específicas, para la gestión de la política de correo seguro Anti-Phishing.

Toda esta política debe ser comunicada a través de toda la división de manera pertinente, accesible y compresible para todos los integrantes del grupo de trabajo de los diferentes departamentos involucrados.

11.1.2 Falta de conciencia de los integrantes de los departamentos involucrados. Para eliminar esta vulnerabilidad la propuesta de mejora se basa igualmente en los objetivos de control A.5.1. Política de seguridad de la información, A.6.1. Organización Interna y A.8.2. Durante el Empleo. De ellos se extraen los siguientes controles:

- Documento de Política de seguridad de la información

El control A.5.1.1 Documento de Política de seguridad de la información, propone definir lo que se busca con la creación de la política de seguridad de la información para los departamentos de Redes y Telecomunicaciones y de Cómputo de la División de Tecnologías. Para ello es necesario desarrollar un documento en donde se consigne el objetivo general, alcance e importancia de crear una política de seguridad de la información, teniendo en cuenta las metas y los principios de seguridad informática planteada por la División de Tecnologías, los cuales deben estar alineados con los objetivos de la organización.

En el documento también debe quedar consignada la estructura necesaria que asegure el cumplimento de esta política, teniendo en cuenta las normas, políticas y principios de seguridad; planteando los requisitos de educación, formación y concientización que sobre seguridad deben tener equipo de trabajo; involucrando la forma en cómo se debe generar la gestión para la continuidad del negocio y exponiendo claramente las responsabilidades generales y específicas para la gestión de la política de seguridad de la información.

Toda esta política debe ser comunicada a toda la División de manera pertinente, accesible y compresible para todos los integrantes del grupo de trabajo de los departamentos de Redes y Telecomunicaciones y de Cómputo.

- Asignación de responsabilidades

El control A.6.1.3 Asignación de responsabilidades, propone definir claramente todas las responsabilidades en cuando a la seguridad de la información. En este caso la oportunidad de mejora recomienda definir claramente las responsabilidades para la protección de los activos individuales y para la ejecución de procesos específicos de seguridad.

También es necesario delegar a los integrantes de los grupos de trabajo las responsabilidades de seguridad, asignándoles las áreas sobre las cuales tiene las responsabilidades.

Se debe determinar claramente, en los activos y procesos de seguridad asociados con cada sistema, la entidad responsable y documentar dicha responsabilidad con sus respectivos niveles de autorización.

- Conciencia, formación y capacitación en seguridad de la información.

El control A.8.2.2 Conciencia, formación y capacitación en seguridad de la información, busca la formación y concientización del personal mediante la creación de un proceso formal de inducción, diseñado desde la Coordinación de Seguridad de la Información de la División de Tecnologías, en el que se presenten las políticas de seguridad de la organización y las expectativas, antes de otorgar el acceso a la información o los servicios, al personal del grupo de trabajo, buscando también la formación en el uso correcto de los servicios del procesamiento de la información.

Se recomienda que esta formación sea permanente e incluya los requisitos de seguridad, responsabilidades legales y controles que la Universidad ha planteado en sus políticas.

11.1.3 Falta de directrices en la emisión de la información. Para eliminar esta vulnerabilidad, la propuesta de mejora se basa en los objetivos de control A.6.1. Organización Interna y A.7.2. Clasificación de la Información (A.7.2), de los cuales se extraen los siguientes controles:

- Acuerdos de confidencialidad.

El control A.6.1.5 Acuerdos de confidencialidad, pretende crea unos acuerdos de no divulgación de la información sensible de la Universidad. En este acuerdo se debe abordar los requisitos para proteger la información confidencial, usando términos que se puedan cumplir legalmente.

Los requisitos deben tener en cuenta la definición de la información que se debe proteger, la duración esperada del acuerdo y las acciones requeridas cuando se termine el acuerdo.

Así mismo deben quedar consignadas las responsabilidades y acciones de los que suscriben el acuerdo para evitar divulgaciones no autorizas de información; se debe aclarar a quién pertenece y cuál es el uso permitido de la información confidencial y los derechos a los que se suscribe en el acuerdo de confidencialidad en el momento de usar dicha información sensible.

Debe quedar registrado el proceso para la notificación y el reporte de divulgación no autorizada o violación de la confidencialidad de esta información.

Igualmente se debe describir los términos para la devolución o destrucción de la información al finalizar el acuerdo y se debe aclarar las acciones esperadas que se deben tomar en caso de incumplimiento del acuerdo. Esto requisitos deben ser revisados periódicamente.

- Directrices de clasificación.

El Control A.7.2.1 Directrices de clasificación se aplica con el fin de generar una clasificación y aplicar los controles de protección con base en las necesidades de la Universidad relacionadas con el compartir o restringir la información sensible; las directrices de clasificación deben incluir convenciones para la clasificación inicial y la reclasificación necesaria al transcurrir un periodo de tiempo.

La responsabilidad de dicha clasificación debe recaer sobre el propietario del activo, donde éste debe definir la clasificación, revisarla permanentemente para asegurar que se mantiene actualizada.

Es necesario que los procedimientos para la identificación de la información comprendan tanto activos físicos como lógicos.

- Etiquetado y manipulado de la información

El control A.7.2.2 Etiquetado y manipulado de la información, crea un método de etiquetado de la información de los sistemas que contienen la información clasificada como sensible por el control anterior, reflejando las reglas de clasificación establecidas por éste último

Para cada nivel de clasificación se recomienda definir los procedimientos de manejo, incluyendo el procesamiento, almacenamiento, transmisión, desclasificación y destrucción segura de la información. También debe contener procedimientos para la cadena de custodia y el registro de cualquier evento de seguridad.

11.1.4 Falta de sistema contra incendios. Para eliminar esta vulnerabilidad, la propuesta de mejora se basa en los objetivos de control A.9.1. Áreas seguras, del cual se extrae el siguiente control:

- Protección contra amenazas externas y de origen ambiental.

El control A.9.1.4 Protección contra amenazas externas y de origen ambiental, busca recomendar directrices para evitar el daño debido a un destrate natural o artificial.

Se propone que el almacenamiento de materiales combustibles debe hacerse a una distancia prudente de las áreas que deben estar seguras; la instalación de los medios de soporte de seguridad se deben ubicar a una distancia prudente, para evitar el daño debido a algún desastre que afecte las instalaciones principales y se propone suministrar el equipo apropiado contra incendios ubicados adecuadamente.

11.1.5 Descuido del custodio de las áreas restringidas. Para eliminar esta vulnerabilidad, la propuesta de mejora se basa en los objetivos de control A.9.1. Áreas seguras, del cual se extrae el control:

- Perímetro de seguridad física

El Control A.9.1.1 Perímetro de seguridad física, propone crear las directrices para los perímetros de seguridad física, tales como definir claramente los perímetros de seguridad y ubicación y la fortaleza de los requisitos de seguridad de cada perímetro de los activos contenidos en dicha área.

También propone definir los perímetros del lugar que contenga los servicios de procesamiento y custodio de información, determinando que deberían ser robustos físicamente, como por ejemplo tener paredes externas de construcción sólida, que todas las puertas externas deben tener una protección adecuada contra el acceso no autorizado y contar con mecánicos de alarma, entre otros.

Se debe contar con una área de recepción que controle el acceso físico al lugar o edificación; contar con sistema de alarma para todas las puertas de evacuación, que se pueda monitorear y someterse a pruebas de control de acceso; se recomienda la instalación de sistemas adecuados de detención de intrusos, según las normas nacionales, regionales o internacionales.

Los servicios de procesamiento de información dirigido a la organización deben estar físicamente separados de aquellos que son dirigidos a terceras partes.

- Controles Físicos de Entrada

El control A.9.1.2 Controles Físicos de Entrada, propone la utilización de controles físicos de acceso que cumplan algunas directrices tales como el registro de la fecha y hora de entrada y salida de visitantes.

Todos los visitantes deben ser supervisados y su acceso debe estar relacionado únicamente para cumplir propósitos específicos y autorizados. También se debe controlar el acceso a las áreas en donde se procesa o almacena información sensible y restringir el acceso únicamente a personas autorizadas.

Se deben utilizar controles de autenticación (tarjetas de control) para autorizar y validar el acceso, exigiendo la utilización de identificación visible a todos los empleados, contratistas y usuarios de terceras partes, notificando si alguno de ellos no la usa.

También se plantea que para el personal de servicio de soporte de terceras partes, se le debe dar acceso restringido a las áreas seguras o los servicios de procesamiento de información sensible y únicamente cuando sea necesario; los derechos de acceso a áreas seguras se deben revisar y actualizar con regularidad.

- Seguridad de oficinas, despachos y recursos

El control A.9.1.3 Seguridad de oficinas, despachos y recursos, busca planear las directrices de seguridad que deben tener las oficinas, recintos y servicios. Directrices tales como los reglamentos y normas pertinentes a la seguridad y a la salud, claramente definidas, en donde en todas las oficinas, despachos y recursos deben contar con la instalación de claves que eviten el acceso al público.
Se debe procurar que las edificaciones sean discretas y no tener indicaciones sobre su propósito; así mismo se propone que los directorios o listados telefónicos internos, que indican las ubicaciones de los servicios de procesamiento de información sensible, no sean de fácil acceso por parte del público.

11.1.6. Falta de acuerdo de confidencialidad. Para eliminar esta vulnerabilidad, la propuesta de mejora se basa en los objetivos de control A.6.1 Organización Interna, del cual se extrae el control:

- Acuerdos de confidencialidad**.**

Con control A.6.1.5 Acuerdos de confidencialidad, se pretende crear acuerdos de no divulgación de la información sensible de la Universidad. En este acuerdo se debe abordar los requisitos para proteger la información confidencial, usando términos que se puedan cumplir legalmente, Dichos requisitos deben cumplir con

la definición de la información que se debe proteger, la duración esperada del acuerdo, las acciones requeridas cuando se termine.

También deben quedar consignadas las responsabilidades y acciones de los que suscriben el acuerdo para evitar divulgaciones no autorizas de información, se debe aclarar a quién pertenece y cuál es el uso permitido de la información confidencial y los derechos a los que suscribe en el acuerdo de confidencialidad, al momento de usar dicha información sensible.

Debe quedar registrado el proceso para la notificación y el reporte de divulgación no autorizada o violación de la confidencialidad de esta información, se deben describir los términos para la devolución o destrucción de la información al finalizar el acuerdo y aclarando las acciones esperadas a tomar en caso de incumplimiento del acuerdo.Todos estos requisitos deben ser revisados periódicamente.

11.1.7 Falta de directrices en la administración de los servicios de red. Para eliminar esta vulnerabilidad, la propuesta de mejora se basa en los objetivos de control A.10.6 Gestión de la seguridad de las redes y A.11.4 Control de acceso a la red, de los cuales se extraen los controles:

- Controles de Red.

El Control A.10.6.1 Controles de Red, busca garantizar la seguridad de la información sobre las redes y la protección de los servicios conectados, contra el acceso no autorizado, teniendo en cuenta los planteamientos que buscan dicha protección, tales como la segregación de la responsabilidad operativa de las redes con la responsabilidad de las operaciones operativas realizadas desde la estaciones de trabajo.

También es necesario establecer las responsabilidades y procedimientos para la gestión de los equipos remotos, incluyendo los quipos utilizados por los usuarios finales

Es necesario establecer controles especiales para salvaguardar la confidencialidad y la integridad de los datos que viajan por redes públicas o redes inalámbricas con el fin de proteger los sistemas y aplicaciones conectados. Se debe aplicar el registro y el monitoreo adecuado para permitir el registro de las acciones de seguridad.

Se recomienda coordinar todas las actividades de gestión para optimizar los servicios para la organización y para garantizar que los controles se aplican consistentemente en la infraestructura del procesamiento.

- Seguridad de los servicios.

El Control A.10.6.2 Seguridad de los servicios, propone lineamientos a la División de Tecnologías, tales que brinden capacidad de gestionar los servicios de red en forma segura, planteando acciones que se puedan encaminar a determinar, monitorear y realizar auditoria regularmente a los servicios prestados, para ello se debe identificar las disposiciones de seguridad, requisitos de gestión y niveles de servicio.

Se propone que para cada uno de los servicios principales de la división incluyan parámetros técnicos con el fin de logar la conexión segura a los servicios de red, según las reglas de seguridad y conexión; así mismo se deben plantear procedimientos para la utilización de los servicios de red y restringir su acceso a la red o a las aplicaciones cuando sea necesario.

- Política de uso de los servicios en red

Con el Control A.11.4.1 Política de uso de los servicios en red, se propone la creación de políticas que buscan plantear directrices relacionadas con el uso de las redes y de los servicios de red. Estas políticas deben contener las redes y los servicios a los cuales se le permite el acceso al equipo de trabajo de los departamentos involucrados, soportados por procedimientos de autorización.

Se deben proponer requisitos de seguridad para cada servicio, crear perfiles de acceso a los servicios de red por parte de los usuarios.

Toda esta política debe ser comunicada a toda la división de manera pertinente, accesible y compresible para todos los integrantes del grupo de trabajo de los departamentos involucrados.

- Identificación de los equipos en la redes

El control A.11.4.3 Identificación de los equipos en la redes, se pretende crear lineamientos de identificación de la estación de trabajo, en el momento en que

esté utilizando un recurso o servicio de red; estos identificadores deben indicar claramente a qué red tiene acceso permitido.

También debe aclarar los permisos dentro de las redes y si éstas tienen sensibilidad diferente.

- Segregación de las redes

El control A.11.4.5 Segregación de las redes, se determina para garantizar la seguridad de las redes, creando un método de control a partir de la división de la red en dominios lógicos, con el fin de crear perímetros diferentes de seguridad. Es decir lo que se busca es controlar el acceso y flujo de información entre diferentes dominios o equipos que se interconectan para compartir información.

También se propone aplicar un conjunto escalonado de controles en diferentes dominios lógicos de la red, para separar aún más los entornos de seguridad de la red, estos dominios se deben definir con base en la evaluación del riesgo a los que se enfrenta el acceso a información sensible por cada segmento de ella.

11.1.8 Falta de controles físicos. Para eliminar esta vulnerabilidad, la propuesta de mejora se basa en los objetivos de control A.9.1. Áreas Seguras y A.9.2. Seguridad de los equipos, de los cuales se extraen los controles:

- Perímetro de seguridad física**.**

Con este control A.9.1.1 Perímetro de seguridad física, se pretende crear las directrices relacionadas con los perímetros de seguridad física, en donde se deben definir claramente los perímetros de seguridad, la ubicación y la fortaleza de cada perímetro de acuerdo con los requisitos de seguridad de los activos contenidos en dicha área.

Los perímetros del lugar en donde se presten los servicios de procesamiento y la ubicación del custodio de información deben ser robustos físicamente, como por ejemplo tener paredes externas de construcción sólida, todas las puertas externas deben tener una protección adecuada contra el acceso no autorizado, se deben contar con mecánicos de alarma, entre otros.

Se debe contar con una área de recepción que controle el acceso físico al lugar o edificación; contar con sistema de alarma para todas las puertas de evacuación, que se pueda monitorear y someterse a pruebas de control de acceso; también se recomienda la instalación de sistemas adecuados de detección de intrusos según las normas nacionales, regionales o internacionales; los servicios de procesamiento de información dirigidos a la organización deben estar físicamente separados de aquellos que son dirigidos a terceras partes.

- Controles Físicos de Entrada

Con la aplicación del control A.9.1.2 Controles Físicos de Entrada, se propone la utilización de controles físicos de acceso que deben cumplir algunas directrices tales como la de registrar la fecha y hora de entrada y salida de los visitantes; todos los visitantes deben ser supervisados y su acceso se debe dar solo para cumplir propósitos específicos y autorizados.

También se debe controlar el acceso a las áreas en donde se procesa o almacena información sensible y se debe restringir el acceso únicamente a personas autorizadas.

Se deben utilizar controles de autenticación (tarjetas de control) para autorizar y validar el acceso, exigiendo la utilización a todos los empleados, contratistas y usuarios de terceras partes la identificación visible, en donde se debe notificar cuando alguno no use una identificación visible.

Al personal de servicio de soporte de terceras partes se le debe dar acceso restringido a las áreas seguras o a los servicios de procesamiento de información sensible únicamente cuando sea necesario, los derechos de acceso a áreas seguras se deberán revisar y actualizar con regularidad.

- Seguridad de oficinas, despachos y recursos

Con el control A.9.1.3 Seguridad de oficinas, despachos y recursos, se busca definir las directrices de seguridad que deben tener las oficinas, recintos y servicios, tales como la definición de reglamentos y normas pertinente a la seguridad y a la salud.

Todas las oficinas, despachos y recursos deben contar con la instalación de claves que eviten el acceso al público, se debe procurar que las edificaciones sean discretas y no tener indicaciones sobre su propósito. También se propone que los directorios o listados telefónicos internos, que indican las ubicaciones de los servicios de procesamiento de información sensible, no sean de fácil acceso por parte del público.

- Emplazamiento y protección de equipos

El control A.9.2.1 Emplazamiento y protección de equipos, busca la protección de las estaciones de trabajo, planteando que éstas estén en áreas en donde se minimice el acceso de personas no autorizadas.

Se exige que los servicios de procesamiento de información que manejan datos sensibles, deban estar ubicados de tal forma que se reduzca el riesgo para visualizar dicha información por parte de personas no autorizadas. Se sugiere que los activos que requieren protección especial deben estar aislados para reducir el nivel general de protección requerida de los demás activos.

Se recomienda dotar a las áreas donde se alojan estaciones de trabajo de sistemas que ayuden a minimizar el riesgo de amenazas físicas potenciales tales como robo, incendio, explosión, humo, tormenta eléctrica, agua, polvo, vibraciones, efectos químicos, interferencia con el suministro de electricidad, telecomunicaciones, entre otros.

Se debe proponer normas de comportamiento del personal que utiliza las estaciones de trabajo, donde es conveniente monitorear las condiciones ambientales (temperatura, humedad) que podrían llegar a afectar el funcionamiento adecuado de éstos.

- Seguridad de equipos fuera de los locales de la organización

Con control A.9.2.5 Seguridad de equipos fuera de los locales de la organización, se pretende crear una protección para la utilización de estaciones de trabajo fuera de la División de Tecnologías, en donde se plantea que, independientemente del propietario y custodio de las estaciones de trabajo, el director de la División de Tecnologías debe autorizar el uso y retiro de dichos equipos fuera de las instalaciones de la División.

También se plantea crear planes de conciencia del personal autorizado para utilizar estaciones de trabajo fuera de la división, en donde se recomienda establecer el cubrimiento del seguro, para proteger la estación de trabajo cuando esta por fuera de la División.

- Retirada de materiales propiedad de la empresa

El Control A.9.2.7 Retirada de materiales propiedad de la empresa, propone aplicar las directrices relacionadas con el retiro de activos de la División de Tecnologías, creando un mecanismo que autorice en forma previa el retiro de equipos de las instalaciones de la División de Tecnologías, identificando claramente aquellos empleados, contratistas y usuarios que tengan autoridad para retirar activos; se recomienda establecer y registrar límites de tiempo para el retiro y devolución de los equipos.

11.1.9 Falta de controles Lógicos. Para eliminar esta vulnerabilidad, la propuesta de mejora se basa en los objetivos de control A.10.4 Protección contra el código malicioso y descargable, A.10.6 Control de acceso a las aplicaciones y a la Información, A.10.7 Manejo de los medios, A.10.8 Intercambio de la Información, A.11.1 Requisitos del negocio para el control de acceso, A.11.2 Gestión de acceso de usuario, A.11.3 Responsabilidades del usuario, A.11.4 Control de acceso a la red, A.11.5 Control de acceso al sistema Operativo, A.11.6 Control de acceso a las aplicaciones y a la Información, A.12.3 Controles Criptográficos, A.12.4 Seguridad de los archivos del sistema, A.12.5 Seguridad en los procesos de desarrollo y soporte, de los cuales se extraen los controles:

- Controles contra el código malicioso

Con este control A.10.4.1 Controles contra el código malicioso se pretende detectar y reparar el accionar de los códigos maliciosos, para lograr la aplicación de controles contra este código es necesario crear conciencia de seguridad en el equipo de trabajo, también se debe brindar un acceso apropiado al sistema y una regulación de la gestión de cambios de la información, todas estas actividades deben quedar consignadas en una política formal que prohíba el uso de software no autorizado, en la cual se establezca unas directrices para la protección contra los riesgos asociados con la obtención de información sensible

Esta política debe incluir revisiones periódicas del software y de los datos de los sistemas que dan soporte a los procesos críticos de la División de Tecnologías, también es necesario plantear la regulación en la instalación y actualización del

software, que ayuda con la detección y reparación de códigos maliciosos, la política debe definir responsabilidades y procedimientos que ayuden con la protección contra códigos maliciosos y que de alguna manera queden consignaos para la creación de boletines de advertencia del accionar de dichos código, también es vital crear planes de recuperación adecuada para la continuidad de la organización, todas estas actividades se plantean con el fin de salvaguardar la información contra los ataques valiéndose del código malicioso.

- Controles de las redes

Con la aplicación del control A.10.6.1 Controles de las redes se plantea desea proteger las redes de las amenazas, buscando la seguridad de la información y de los servicios de red, contra el acceso no autorizado, para lograr este objetivo es necesario establecer las responsabilidades y los procedimientos para la gestión de quipos remotos, incluyendo las estaciones de trabajo en las áreas de los usuarios, es obligatorio establecer controles especiales para salvaguardar la confidencialidad y la integridad de los datos que viajan por las redes públicas o redes inalámbricas.

Es vital aplicar un monitoreo adecuado de las actividades en las redes para permitir el registro de acciones de seguridad pertinentes, tambien se recomienda coordinar las actividades de gestión tanto para la optimización en el servicio para la Universidad como para garantizar que se aplican los controles de seguridad consistentemente, todas estas actividades se plantean con el fin de mantener y controlar adecuadamente las redes por donde viaja la información.

- Seguridad de los servicios de la red

Con la implantación del control A.10.6.2 Seguridad de los servicios de la red se busca verificar la capacidad de la división de tecnologías para la gestión seguramente los servicios de red, este control busca identificar las directrices de seguridad necesarias para los servicios se presten de manera óptima a la comunidad de la Universidad, directrices tales como los requisitos de gestión, las características de seguridad para cada servicio, los niveles de servicio acordados, todas estas actividades se plantean con el fin de brindar unos servicios de red adecuados a la Universidad.

- Eliminación de los medios

Con este control A.10.7.2 Eliminación de los medios, se pretende plantear los procedimientos formales para la eliminación segura de los medios que contiene información sensible, buscando minimizar la fuga de información sensible a personas no autorizadas

Los procedimientos de almacenamiento y eliminación se debe realizar de forma segura e inocua, pero también se deben realizar acorde con la sensibilidad de la información contenida, por eso se hace necesario establecer procedimientos para la identificación de elementos que requieren eliminación segura, se proponer que cuando sea posible, se genere un registro de la eliminación de los elementos que contiene información sensible con el objetivo de mantener una prueba de auditoria. Todas estas actividades se plantean con el fin de minimizar la fuga de información.

- Procedimiento para el manejo de la información

Con la aplicación del control A.10.7.3 Procedimiento para el manejo de la información se propone la elaboración de procedimientos que indiquen el cómo manejar, procesar, almacenar y comunicar la información de acuerdo a su calcificación.

Se recomienda etiquetar todos los medios contenedores de información preferiblemente indicando el nivel de clasificación, también es necesario platear restricciones de acceso para evitar el acceso de personal no autorizado, se debe realizar mantenimiento de un registro formal de los receptores de la información autorizados.

Se pretende con todas estas directrices es garantizar que los datos se entrada de cualquier sistema tenga un alto grado de integridad y que su almacenamiento y mantenimiento de dichos datos se el óptimo, es neceario crear un rotulado claro de todas las copias de los medios para autenticación del receptor sea el autorizado, es vital plantear una revisión periódica de las listas de distribución y de receptores autorizados, todas estas actividades se plantean con el fin de brindar un manejo adecuado de la información.

- Políticas y procedimientos para el intercambio de información

Con el control A.10.8.1 Políticas y procedimientos para el intercambio de información, se deberían considerar la creación de procedimientos para proteger la interceptación, copiado modificación, enrutamiento inadecuado y destrucción la información sensible.

Se deben crear procedimientos para la detección y protección de la información adjuntada en correos y que esta protección se extienda también salvaguardar dicha información contra códigos maliciosos, lo que se pretende es la creación de políticas o directrices que enfaticen el uso aceptable de los servicios de comunicación electrónica que utiliza las redes cableadas o inalámbricas, también se debe hacer claridad en las responsabilidades de todo el equipo de trabajo, buscando exigir la utilización de técnicas criptográficas.

También se debe plantear que en estas políticas expongan directrices para la retención, eliminación y para prevenir la perdida de información sensible, debe quedar claro las restricciones asociadas con le envió de información sensible y por último se debe crear un plan de conocimiento y de concientización para el equipo de trabajo de cada departamento, todas estas actividades se plantean con el fin de diseñar procedimientos y controles para regular el intercambio de información

- Política de control de acceso

Con este control A.11.1.1 Política de control de acceso se desea plantear reglas y derechos que regulen acceso para cada usuario, para lograr esto se debe identificar todos los requisitos en el contexto de seguridad que las aplicaciones del Universidad requieran.

Es necesario platear políticas para la distribución y autorización del acceso a la información, esta política debe estar alienada con las políticas de clasificación de la información, esta política exige la creación de diferentes perfiles de usuario para controlar el acceso a la información y una forma de gestionar los derechos (autorización revisión y retiro) del acceso a la información. Todas estas actividades se plantean con el fin de regular el acceso de información.

- Registro de Usuario

Con la aplicación del control A.11.2.1 Registro de Usuario, se pretende crear un procedimiento formar para el registro y cancelación de usuarios que tendrían acceso a los sistemas o servicios de información.

Se propone el uso de identificaciones autorizadas solo por el responsable de cada activo, identificaciones únicas para cada uno de los usuarios para el acceso los sistemas o servicios de información con niveles de acceso, los niveles de acceso a la información deben ser verificados periódicamente y deben estar alineados con la política de seguridad de la División de Tecnologías, se debe brindar un declaración escritica de los derechos y accesos de cada usuario, donde cada usuario entienda y asuma la responsabilidad de cada acceso. Todas estas actividades se plantean con el fin controlar el acceso de usuarios a la información.

- Gestión de privilegios

Con la implantación del control A.11.2.2 Gestión de privilegios, lo que se busca es la protección contra el acceso no autorizado a la información, para lograr este objetivo se debe crear una la asignación autorizada de privilegios de acceso, para esta gestión se debe identificar todos los usuarios y sus privilegios de acceso asociado a cada sistema como sistema operativos, sistema de gestión de la bases de datos y aplicaciones.

También es necesario asignar los estos privilegios partiendo de la necesidad de uso de la información y de la política de acceso a la información, se recomienda promover el empleo de sistemas que eviten la necesidad de otorgar y operar con privilegios a los usuarios. Todas estas actividades se plantean con el fin controlar el acceso de usuarios a la información.

- Gestión de contraseñas para usuarios

Con este control A.11.2.3 Gestión de contraseñas para usuarios, se pretende recomendar la asignación de contraseñas, las cuales se debería controlar a través de un proceso formal de gestión y que debería exigir a los usuarios firmar una declaración de confidencialidad para mantener el secreto las contraseñas personales y grupales, esta declaración debe incluir términos y condiciones laborales

También se propone el establecer procedimientos formales y seguros para la entrega de contraseñas temporales pero donde se pueda verificar la identidad de un usuario antes de proporcionar una contraseña única y no descifrable, las contraseñas predeterminadas por el proveedor de cualquier sistema deben ser cambias inmediatamente a la instalación del sistema o del software. Todas estas actividades se plantean con el fin controlar el acceso de usuarios a la información.

- Revisión de los derechos de acceso de usuario

Con la aplicación del control A.11.2.4 Revisión de los derechos de acceso de usuario, se recomienda es una revisión de los derechos de acceso de los usuarios a la información sensible, se propone que los derechos de acceso sean revisados periódicamente.

Los derechos deben ser revisados y reasignados cada que se generen cambios en un cargo dentro de la División de Tecnologías, también es necesario plantear una revisión periódica corta de los cambios en las cuentas privilegiadas de cualquier sistema. Todas estas actividades se plantean con el fin controlar el acceso de usuarios a la información.

- Uso de Contraseñas

Con la implantación del control A.11.3.1 Uso de Contraseñas se busca, tener un mecanismo que genere una exigencia de cumplimiento de buenas prácticas de seguridad en la selección y uso de las contraseñas, se propone mantener la confidencialidad de las contraseñas, también se debe evitar el registro de las misma en una almacenamiento de fácil acceso.

Se debe crear una directrices de cambio de contraseñas que exijan el cambio periódico o por indicio de peligro en un sistema, las contraseñas deben cumplir con unas características de complejidad alta para no ser descifradas, se debe exigir el cambio de contraseñas temporales de forma inmediata, si los usuarios necesitan acceso múltiple a diferentes servicios, sistemas o plataformas deben tener diferentes contraseñas para cada uno de estos. Todas estas actividades se plantean con el fin controlar el acceso de usuarios a la información.

- Política de uso de los servicios en red

Con este control A.11.4.1 Política de uso de los servicios en red, se propone el crear una política que limite el acceso de los usuarios a los servicios cuyo uso están específicamente autorizados.

Se pretende crear directrices que dejen muy claro los procedimientos de autorización para determinar a qué se le permite el acceso a que redes y a que servicios, esta política también debe contener los controles y procedimientos de gestión de los servicios que se ofrecen, esta política debe ser consistente con la política de control de acceso de la organización. Todas estas actividades se plantean con el fin controlar el uso de los servicios de red de la Universidad.

- Identificación de los equipos en las redes

Con la aplicación del control A.11.4.3 Identificación de los equipos en las redes, lo que se busca es asegurar la comunicación entre dos partes específicas, lo que se propone es dotar cada equipo de un identificar único que le dará acceso a la comunicación en la red, estos identificadores deberían contener con claridad a que red está permitido conectar el equipo. Todas estas actividades se plantean con el fin controlar el uso de los servicios de red de la Universidad.

- Separación en las redes

El control A.11.4.5 Segregación de las redes, se propone con el fin de garantizar la seguridad de las redes, creando un método de control a partir de la división de la red en dominios lógicos, con el fin de crear perímetros diferentes de seguridad. Es decir lo que se busca es controlar el acceso y flujo de información entre diferentes dominios o equipos que se interconectan para compartir información.

También se propone aplicar un conjunto escalonado de controles en diferentes dominios lógicos de la red, para separar aún más los entornos de seguridad de la red, estos dominios se deben definir con base en la evaluación del riesgo a los que se enfrenta el acceso a información sensible por cada segmento de ella.

- Procedimientos seguro de inicio de sesión

Con este control A.11.5.1 procedimientos seguro de inicio de sesión, propone diseñar un el procedimientos de registro en un sistema operativo para minimizar la oportunidad de acceso no autorizado, por lo tanto lo que se busca es crear unas reglas que no muestre los el proceso de registro de inicio se ha completado exitosamente, también se exige no tener mensajes de ayuda durante el procedimiento de registro de inicio de cualquier sistemas.

Se debe dotar el sistema con una forma de validar la información de registro de inicio únicamente al terminar todos los datos de entrada, se debe proponer el limitar el tiempo y la cantidad de intentos permitidos para realizar el registro de inicio, se debería mostrar la información del último registro exitoso.

- Identificación y autentificación de usuario

Con la aplicación del control A.11.5.2 Identificación y autentificación de usuario se pretende controlar el accionar de los usuarios, se propone utilizar los identificadores de usuarios para rastrear las actividades de dicha persona en cada uno de los servicios donde hay información sensible, se pide que las actividades de usuarios regulares no se hagan desde cuentas con privilegios y en circunstancias excepcionales se puede un único identificador para diferentes usuarios y la autorización del uso de algún identificador debe estar documentada, también se requiere que si es necesario verificar la identidad y autenticación se utilice alguno de los métodos alternos a la contraseña como medios criptográficos, tarjetas inteligentes token o entre otros.

- Uso de las utilidades del sistema

Con el control A.11.5.4 Uso de las utilidades del sistema, se pretende restringir estrictamente el uso de programas utilitarios que puedan anular los controles del sistema, para estos propone el uso de procedimientos de identificación, autentificación y autorización para las utilidades del sistema, el crear una separación de las utilidades del sistema del software de aplicación, se propone también el limitar el uso y disponibilidad de las utilidades del sistema, se debe crear un registro de la instalación, uso y desinstalación de las utilidades del sistema.

- Restricción del acceso a la información

Con este control A.11.6.1 Restricción del acceso a la información, se desea crear limitaciones de acceso a la información basadas en los requisitos de las aplicaciones que administran información sensible, para lograr este cometido se debe proporcionar menús para controlar el acceso a las funciones del sistema de aplicación, también se deben controlar los derechos de acceso de cada usuario y se debe garantizar la integridad de toda la información sensible al que un usuario accede.

- Aislamiento de sistemas sensibles

Con la aplicación del control A.11.6.2 Aislamiento de sistemas sensibles, se pretende crear un entorno informático dedicado para los sistemas sensibles, en donde la sensibilidad del sistema debe estar calificada por el responsable de dicho sistema, se deben platear políticas para la utilización de sistemas que son lo suficientemente sensibles.

- Políticas sobre el uso de controles criptográficos

Con la Implantación del control A.12.3.1 Políticas sobre el uso de controles criptográficos, preténdete crear unas directrices para la protección de la información, enfocando esta política en el uso de controles criptográficos en toda la División de Tecnologías.

Se debe evaluar el nivel de protección requerido partiendo de los riesgos a los que se expone la información, también se propone utilizar métodos de encriptación para la protección de la información sensible transportada por redes o medios móviles o removibles, se debe crear un sistema de gestión para las calves y los diferentes métodos de encriptación, también en esta política debe describir claramente las funciones y responsabilidades de los responsables.

- Control del software operativo

Con este control A.12.4.1 Control del software operativo, se pretende controlar la instalación de software en los sistemas operativos con el fin de minimizar la posible corrupción dichos sistemas, para lograr esto es necesario crear directrices que vigilen la instalación y actualización del software operativo, aplicaciones y librerías utilizadas diariamente

La instalación de software debe ser autorizado y debería ser después de aplicar un conjunto de pruebas que aseguren un normal funcionamiento del software, el procedimiento de actualización solo debe ser realizado por personal autorizados, se propone la implantación de un sistema de control de configuración para el mantener estado adecuado del software, se debería conservar un registro para la auditoria de todas las actualizaciones de las librerías utilizadas y es de carácter obligatorio la creación de un plan de contingencia, que soporte la recuperación del sistema

- Fuga de Información

Con la aplicación del control A.12.5.4 Fuga de Información, se busca minimizar las oportunidades de que se produzca fuga de información, para controlar esto se debe plantear el uso de canales encubiertos, se debe proponer el enmascaramiento de las comunicaciones, se procurar el utilizar sistemas y software que se considere con alta integridad, también es necesario crear un sistema de monitoreo que regula las actividades del personal, de los sistemas y de los recursos utilizados.

11.2. OPORTUNIDADES DE MEJORA.

Todas estas actividades se constituyen en oportunidades de mejora al Sistema de Seguridad Informática de la División de Tecnologías, porque permiten de una u otra manera eliminar las vulnerabilidades que podrían ser utilizadas por los riesgos inaceptables para materializar un daño a la organización.

La aplicación de las oportunidades de mejora permite cumplir el objetivo principal del esquema de seguridad, toda vez que éste consiste en proponer controles que salvaguarden todas las actividades que se realizan desde las estaciones de trabajo, en la administración y prestación de los servicios ofrecidos por la División de Tecnologías a la Universidad

Si bien el análisis se realizó teniendo como base las estaciones de trabajo críticas, éste permitió plantear oportunidades de mejora en cinco aspectos generales relacionados con la Seguridad Informática, como lo son el recurso humano, administración de la información, el aspecto físico, los servicios de red y las políticas y directrices de la universidad.

11.2.1. Recurso Humano. Respecto al recurso humano se plantean mejoras relacionadas con la creación de conciencia respecto al tema de seguridad, mediante capacitaciones permanentes y formación de cada persona que conforma el equipo de trabajo, en el contexto de seguridad de la información; la definición clara de responsabilidades en cuando a la seguridad de la información; se proponen definir acuerdos de no divulgación de información sensible mediante actos que incluso tengan validez jurídica; el porte permanente y visible de carnets al interior de las áreas donde se encuentran los activos críticos; las restricciones de acceso a personal no autorizado o definición de accesos restringidos.

Se deben crear procesos formales de inducción diseñados desde la Coordinación de la Seguridad de la Información, mostrando las políticas de seguridad y formación en el uso correcto de los servicios del procesamiento de la información, incluyendo responsabilidades legales, normas de comportamiento del personal. En los planes de conciencia se debe incluir un capítulo especial para los usuarios que utilizan las estaciones de trabajo fuera de la división, estableciendo un cubrimiento seguro para proteger dicho activo fuera de la División. La formación debe ser permanente.

Se propone crear un mecanismo que autorice en forma previa el retiro de equipos de las instalaciones de la División de Tecnologías, identificando claramente aquellos empleados, contratistas y usuarios que tengan autoridad para retirar activos; se recomienda establecer y registrar límites de tiempo para el retiro y devolución de los equipos.

Al personal de servicio de soporte de terceras partes se le debe dar acceso restringido a las áreas seguras o a los servicios de procesamiento de información sensible únicamente cuando sea necesario, los derechos de acceso a áreas seguras se deberán revisar y actualizar con regularidad.

11.2.2. Administración de la información. Las oportunidades de mejora respecto a la administración de la información definidas por los controles propuestos se refieren a la clasificación de la información con el fin de restringir o compartir de manera adecuada la información; la definición de procedimientos de manejo, procesamiento, almacenamiento, transmisión y destrucción de la información.

Igualmente propone definir claramente las responsabilidades para la protección de los activos individuales y para la ejecución de procesos específicos de seguridad, es necesario delegar a los integrantes de los grupos de trabajo las responsabilidades de seguridad, asignándoles las áreas sobre las cuales tiene las responsabilidades.

Se debe determinar claramente, en los activos y procesos de seguridad asociados con cada sistema, la entidad responsable y documentar dicha responsabilidad con sus respectivos niveles de autorización.

Se deben definir los requisitos para proteger la información confidencial, usando términos que se puedan cumplir legalmente, teniendo en cuenta la definición de la

información que se debe proteger, la duración esperada del acuerdo y las acciones requeridas cuando se termine el acuerdo.

Así mismo deben quedar consignadas las responsabilidades y acciones de los que suscriben el acuerdo para evitar divulgaciones no autorizas de información; se debe aclarar a quién pertenece y cuál es el uso permitido de la información confidencial y los derechos a los que se suscribe en el acuerdo de confidencialidad en el momento de usar dicha información sensible

11.2.3. Áreas físicas. Respecto a las áreas físicas las oportunidades de mejora se refieren a la definición de los perímetros de seguridad y el acceso a ellos. Esto se hace implementando directrices para evitar el daño natural o artificial.

Se necesita tener reglamentos y normas pertinentes al acceso a todas las oficinas, despachos y recursos, se propone la protección de las estaciones de trabajo, ubicándolas en áreas en donde se minimice el acceso de personas no autorizadas, aplicando la autorización del responsable para la utilización de estaciones de trabajo fuera de la instalaciones físicas.

El almacenamiento de materiales combustibles debe hacerse a una distancia prudente de las áreas que deben estar seguras; la instalación de los medios de soporte de seguridad se deben ubicar a una distancia prudente, para evitar el daño debido a algún desastre que afecte las instalaciones principales y se propone suministrar el equipo apropiado contra incendios ubicados adecuadamente.

Se propone definir los perímetros del lugar que contenga los servicios de procesamiento y custodio de información, determinando que deberían ser robustos físicamente, como por ejemplo tener paredes externas de construcción sólida, que todas las puertas externas deben tener una protección adecuada contra el acceso no autorizado y contar con mecánicos de alarma, entre otros. Se debe procurar que las edificaciones sean discretas y no tener indicaciones sobre su propósito; así mismo se propone que los directorios o listados telefónicos internos, que indican las ubicaciones de los servicios de procesamiento de información sensible, no sean de fácil acceso por parte del público.

Se debe contar con un área de recepción que controle el acceso físico al lugar o edificación; contar con sistema de alarma para todas las puertas de evacuación, que se pueda monitorear y someterse a pruebas de control de acceso; se

recomienda la instalación de sistemas adecuados de detención de intrusos, según las normas nacional, regional o internacional.

Todos los visitantes deben ser supervisados y su acceso debe estar relacionado únicamente para cumplir propósitos específicos y autorizados. También se debe controlar el acceso a las áreas en donde se procesa o almacena información sensible y restringir el acceso únicamente a personas autorizadas, registrando la fecha y hora de entrada y salida de los visitantes; todos los visitantes deben ser supervisados y su acceso se debe dar solo para cumplir propósitos específicos y autorizados

Se deben utilizar controles de autenticación (tarjetas de control) para autorizar y validar el acceso, exigiendo la utilización de identificación visible a todos los empleados, contratistas y usuarios de terceras partes, notificando si alguno de ellos no la usa. Todas las oficinas, despachos y recursos deben contar con la instalación de claves que eviten el acceso al público.

11.2.4. Servicios de red. Básicamente están relacionadas con la garantía del acceso a las redes en forma segura y permanente. Para ellos se debe definir un documento en donde se consigne el objetivo general, alcance e importancia de crear una política de correo seguro Anti-Phishing, debe quedar consignada la estructura necesaria que asegure el cumplimento de esta política teniendo en cuenta las normas, directrices y principios de seguridad, exponiendo claramente las responsabilidades generales y específicas, para la gestión de la política de correo seguro Anti-Phishing.

Toda esta política debe ser comunicada a través de toda la división de manera pertinente, accesible y compresible para todos los integrantes del grupo de trabajo de los diferentes departamentos involucrados.

Se propone la creación de política que plantea la pautas para la prestación óptima de los servicios de red, creando lineamientos de identificación de los equipos que utilizan de algún modo la red y la creación de perímetro de seguridad en la red diferentes entre cada uno de ellos

Es necesario hacer la segregación de la responsabilidad operativa de las redes con la responsabilidad de las operaciones operativas realizadas desde la estaciones de trabajo. También es necesario establecer las responsabilidades y

procedimientos para la gestión de los equipos remotos, incluyendo los quipos utilizados por los usuarios finales

Es necesario establecer controles especiales para salvaguardar la confidencialidad y la integridad de los datos que viajan por redes públicas o redes inalámbricas con el fin de proteger los sistemas y aplicaciones conectados. Se debe aplicar el registro y el monitoreo adecuado para permitir el registro de las acciones de seguridad.

Se recomienda coordinar todas las actividades de gestión para optimizar los servicios para la organización y para garantizar que los controles se aplican consistentemente en la infraestructura del procesamiento. Se deben proponer requisitos de seguridad para cada servicio, crear perfiles de acceso a los servicios de red por parte de los usuarios.

Toda esta política debe ser comunicada a toda la división de manera pertinente, accesible y compresible para todos los integrantes del grupo de trabajo de los departamentos involucrados.

También se propone aplicar un conjunto escalonado de controles en diferentes dominios lógicos de la red, para separar aún más los entornos de seguridad de la red, estos dominios se deben definir con base en la evaluación del riesgo a los que se enfrenta el acceso a información sensible por cada segmento de ella.

11.2.5. Políticas y directrices. Hacia la división, se plantea mejoras como la creación de una política encaminada al cumplimiento de normas, directrices y principios de seguridad, tales como la creación de la política de seguridad de la información para los departamentos de Redes y Telecomunicaciones y de Cómputo de la División de Tecnologías. Para ello es necesario desarrollar un documento en donde se consigne el objetivo general, alcance e importancia de crear una política de seguridad de la información, teniendo en cuenta las metas y los principios de seguridad informática planteada por la División de Tecnologías, los cuales deben estar alineados con los objetivos de la organización.

En el documento también debe quedar consignada la estructura necesaria que asegure el cumplimento de esta política, teniendo en cuenta las normas, políticas y principios de seguridad

En este acuerdo se debe abordar los requisitos para proteger la información confidencial, usando términos que se puedan cumplir legalmente, Dichos requisitos deben cumplir con la definición de la información que se debe proteger, la duración esperada del acuerdo, las acciones requeridas cuando se termine.

11.2.6. Controles Lógicos. Respecto a los controles lógicos se plantean mejoras relacionadas con la creación de Controles contra el código malicioso, también se plantea proteger las redes de las amenazas y buscar la seguridad de la información y de los servicios de red, contra el acceso no autorizado, brindar seguridad en los servicios de red buscado la gestión segura de los servicios brindados, se propone mejoras planteando procedimientos formales para la eliminación segura de los medios que contiene información sensible, uno de las mejoras más delicadas que se propone es la elaboración de procedimientos que indiquen el cómo manejar, procesar, almacenar y comunicar la información de acuerdo a su calcificación, los departamentos involucrados necesitan considerar la creación de procedimientos para proteger la interceptación, copiado modificación, enrutamiento inadecuado y destrucción la información sensible, se debe plantear reglas y derechos que regulen acceso para cada usuario a cada sistema que contiene información sensible, se propone crear un procedimiento formar para el registro y cancelación de usuarios que tendrían acceso a los sistemas o servicios de información.

También se plantean mejoras con gestión de privilegios que lo que busca es la protección contra el acceso no autorizado a la información sensible, se recomienda también la asignación de contraseñas se debería controlar a través de un proceso formal de gestión, se propone la revisión de los derechos de acceso de parte de los usuarios a la información sensible, es necesario tener un mecanismo que genere una exigencia de cumplimiento de bunas prácticas de seguridad en la selección y uso de las contraseñas, se debe plantear una política que limite el acceso de los usuarios a los servicios cuyo uso están específicamente autorizados, implantado en las redes y en los servicios de red directrices que limiten el acceso. Es necesario crear la Identificación de los equipos en las redes, que lo que se busca es asegurar la comunicación entre dos partes específicas, se propone diseñar un el procedimientos de registro en un sistema operativo para minimizar la oportunidad de acceso no autorizado. También, es necesaria la Identificación y autentificación de usuario para controlar el accionar de los usuarios, lo que se propone es utilizar los identificadores de usuarios para rastrear las actividades de dicha persona en cada uno de los servicios donde hay información sensible, se propone restringir estrictamente el uso de programas utilitarios que puedan anular los controles del sistema También se propone crear limitaciones de acceso a la información basadas en los requisitos de las aplicaciones que administran información sensible, se pretende crear un entorno informático dedicado para los sistemas sensibles, se deben plantear unas

directrices para la protección de la información enfocando al dirección de esta política en el uso de controles criptográficos en toda la división de tecnologías, se propone como mejora el controlar la instalación de software en los sistemas operativos con el fin de minimizar la posible corrupción dichos sistemas y la última propuesta está enfocada en minimizar las oportunidades de que se produzca fuga de información.

12. CONCLUSIONES

Con la descripción de los lineamientos del Sistema de Administración de Riesgos Integral (SARI), se conocieron las todas las directrices planteadas para cumplir y garantizar que todas las acciones que se realizan en el contexto de seguridad de la información, logren mitigan y minimizan las consecuencias de los riesgos a los que se expone los activos de información de la Universidad Autónoma de Occidente. Con dicha descripción se logró entender de manera más precisa el proceso de administración de la seguridad de la información y determinar los pasos metodológicos que se deben hacer para plantear los lineamientos de seguridad de las estaciones de trabajo críticas.

Al aplicar los lineamientos del Sistema de Administración de Riesgos Integral (SARI), se logro apropiarse de manera adecuada del sistema que permite la identificación, valoración y mitigación de los riesgos inherentes al esquema de seguridad informática, también se pudo reconocer y valorar los artículos que tiene valor significativo para la organización, llamados activos de información de los cuales contienen personas, información, estación de trabajos y hasta a los servicios actuales que los departamentos involucrados prestan a la comunidad que conforma la Universidad Autónoma de Occidente.

Con la aplicación de los lineamientos del Sistema de Administración de Riesgos, se logró identificar las estaciones de trabajo criticas, desde las cuales se realiza la administración de los servicios actuales que el departamento de Cómputo y Departamento Redes y Telecomunicaciones ofrece a la Universidad Autónoma de Occidente, todo esto se hizo para poder de identificar el responsable y custodio de las estaciones de trabajo, con el fin de crear un panorama de amenazas y vulnerabilidades que podrían afectar drásticamente el esquema de seguridad informática de la División de Tecnologías de la Universidad Autónoma de Occidente.

A partir de un análisis de los riesgos a los que se expone las estaciones de trabajo criticas se logró la identificación de las fortalezas y debilidades en el esquema de seguridad informática de la División de Tecnologías, con las debilidades encontradas y se logró plantear las oportunidades de mejora, que al utilizar los controles acordes a las debilidades encontradas, logró aumentar los niveles de seguridad informática.

La aplicación de las oportunidades de mejora permitió cumplir el objetivo principal del esquema de seguridad, toda vez que éste consiste en proponer controles que

salvaguarden todas las actividades que se realizan desde las estaciones de trabajo, en la administración y prestación de los servicios ofrecidos por la División de Tecnologías a la Universidad Autónoma de Occidente. Si bien el análisis se realizó teniendo como base las estaciones de trabajo críticas, éste permitió plantear oportunidades de mejora en seis aspectos generales relacionados con la Seguridad Informática, como lo son el recurso humano, administración de la información, el aspecto físico, los servicios de red, controles lógicos y las políticas y directrices de la Universidad Autónoma de Occidente.

13. RECOMENDACIONES

Se recomienda desarrollar las oportunidades de mejora en términos de controles, planteadas en el presente proyecto para que el esquema de seguridad de las estaciones de trabajo críticas funcionen adecuadamente. Sin embargo es indispensable que, una vez colocados los controles, se repita nuevamente el ciclo para determinar e identificar nuevas oportunidades de mejora al esquema de seguridad informática de la División de Tecnologías.

Al tomarse como escenario el peor de los casos, donde no existían controles para ninguno de los riesgos identificados en este proyecto, se recomienda revisar la flexibilidad de la regla general del negoción, donde propone que solo los riesgos que tomen un nivel de aceptación del riesgo inaceptado serán tratados como oportunidades de mejora. A partir de la matriz consignada en el anexo 3 se puede identificar riesgos con niveles de aceptación medios que debiera ser tratado en próximo trabajo de grado para cambiarles esta valoración a aceptable.

Se recomienda también crear políticas y planes de capacitación para que todo el equipo de trabajo de la división de tecnologías entienda los roles y funciones dentro del esquema de seguridad informática con el que cuenta la División de Tecnologías

Se recomienda también crear un plan de contingencia, con el que se pueda contrarrestar las interrupciones en los procesos, procedimientos y servicios que soportan actividades “Core” de la Universidad Autónoma de Occidente, este plan debe velar por la protección y recuperación de los activos de información (Personas, Datos, Documentos, Sistema de Información, Servicio Tecnológico, Estaciones de trabajo, Sistemas de Informático) que son vitales para contra restar los efectos nocivos de incidente informático.

El plan de contingencia también debe minimizar el impacto y el tiempo de recuperación causado por la perdida de los activos en el momento de la aparición de incidentes tales como los desastres naturales, accidentes, fallas en los activos y hasta por acciones deliberadas de personas que lo único que quieren es generar daño, se propone que este plan contenga una metodología basada en la planeación de controles preventivos y de recuperación. También se recomienda identificar y acordar las responsabilidades, roles y funciones de cada uno de las personas principales y suplentes que actuaran en la aplicación del proceso de continuidad, por esta razón es necesario capacitar de manera adecuada a todos lo

integrantes de los diferentes equipos de trabajo que conforma a la División de Tecnologías.

Para continuar con la plan de dar a conocer oportunidades de mejoras, en el proceso de identificar los activos de información fue necesario la utilización de los procedimientos de cada uno de los departamentos involucrados en este proyecto, en dichos procedimientos también se encontraron oportunidades de mejora, que tomando acciones correctivas también dan un aporte valioso a la gestión de la información de la División de Tecnologías de la Universidad Autónoma de Occidente, estas oportunidades de mejora en los procedimientos son:

En el Departamento de Redes y Telecomunicaciones.

- El procedimiento 3.2.2 PD1.1 En Las sección de definiciones de términos que se utilizan en este procedimiento, falta claridad que ayude con la contextualización, es necesario plantear la definición de toda la terminología técnica que se utiliza en el procedimiento (Ej. Definición de Fortigate)

- El procedimiento 3.2.2 PD1.1 A Los pasos les hace falta claridad en la numeración, se debe realizar la enumeración de todos los pasos que conforman el flujo grama, con el fin de generar más claridad en el momento de buscar dependencias de actividades.

- El procedimiento 3.2.2 PD1.4 En Las sección de definiciones de términos que se utilizan en este procedimiento, falta claridad que ayude con la contextualización, es necesario plantear la definición de toda la terminología técnica que se utiliza en el procedimiento (Ej. Definición de TSM)

- El procedimiento 3.2.2 PD1.4 en el paso 4 es necesario deducir que el paso 5.1 es la respuesta al sí del momento de decisión, es ineludible crear el conector entre el momento de decisión y actividad

- En el procedimiento 3.2.2 PD1.5 el paso 6 hay un error de escritura dice “Servidos” y es “servidor”, se debe corregir este error de escritura para evitar ambigüedades.

- En el procedimiento 3.2.2 PD1.6 el paso 2 contiene un responsable llamado Usuario que la dependencia de este es el Departamento de Redes y

Telecomunicaciones, se debe corregir que los usuarios que envían este formato de solicitud, no pertenecen al Departamento de Redes y Telecomunicaciones si no a cualquier dependencia como se nombra en procedimiento 3.2.2 PD1.5 el paso 1

- En los procedimientos 3.2.2 PD1.4, 3.2.2 PD1.5, 3.2.2 PD1.6, 3.2.2 PD1.7 se habla de creación, administración y custodia de "NODOS" que ninguno de los procedimientos nombrados se le hace una definición y contextualización clara de este término, es necesario plantear la definición de toda la terminología técnica que se utiliza en el procedimiento.

- En el procedimiento 3.2.2 PD1.8 el paso 1 se habla de responsable llamado Usuario pero falta claridad al momento de indica de que dependencia a la que pertenece. Se debe corregir que los usuarios que envían este formato de solicitud pertenezcan a cualquier dependencia como se nombra en procedimiento 3.2.2 PD1.5 el paso 1

- En el procedimiento 3.2.2 PD1.8 falta definir un responsable en que recaiga los roles y actividades del procedimiento. Se debe asignar un responsable para que se deben realizar para cumplir satisfactoriamente el procedimiento.

- En el procedimiento 3.2.2 PD1.8 se habla de una dependencia llamada "Coordinación de Redes", pero en el organigrama de la División tecnologías de la Universidad Autónoma de Occidente no existe un departamento llamado de esa forma, se debe corregir indicando quien es el responsable y a que dependencia pertenece.

- En el procedimiento 3.2.2 PD1.20 el paso 1 se habla de responsable llamado Auxiliar de Soporte pero hay carecías al momento de indica de que dependencia a la que pertenece, se debe corregir indicando a que dependencia pertenece dicho responsable.

- El procedimiento 3.2.2 PD1.30 es ineficiente la claridad en le paso 1 cuando se habla de "equipo" se refiere y genera ambigüedad, es necesario plantear la definición de toda la terminología técnica que se utiliza en el procedimiento.

- El procedimiento 3.2.2 PD2.12 el paso 6 y 7 aparece un responsable llamado "Departamento de Suministros" enganchado al Departamento de Redes y

Telecomunicaciones cuando este responsable es del departamento de la planta física. Además, en el organigrama de la División Tecnologías no existe un departamento llamado de esa forma, se debe corregir indicando quien es el responsable y a que dependencia pertenece.

En el Departamento de Cómputo.

- El procedimiento 3.2.1 PD1.1 en el paso 2, se plantea que el responsable de la notificación de la solicitud de servicio es el responsable del proceso, es necesario hacer claridad en quien recae la responsabilidad de es dicha actividad, aclarando el rol y la función cumple el este responsable.

- El procedimiento 3.2.1 PD1.1 paso 5.4.1, se realiza la notificar la negativa del proveedor a un jefe, es necesario hacer claridad en quien recibir esa notificación.

- En el procedimiento 3.2.1 PD1.3 Carece de claridad a que departamento pertenecen los responsables que ejecutan las actividades, generando ambigüedad, es necesario enganchar cada responsable a una dependencia desde donde se ejecuta la actividad.

- En el procedimiento 3.2.1 PD1.3 se utilizan formatos estipulados para la definición de requerimientos, documentación de resultados, registro de capacitación, desarrollo de la capacitación, actualización de inventarios tecnológicos que no se utilizaron en ningún otro procedimiento, sabiendo que es el mismo departamento se debería proponer el utilizar estos formatos en los otros procedimientos que apliquen.

- En el procedimiento 3.2.1 PD1.4 falta claridad a que departamento pertenecen los responsables que ejecutan las actividades, generando ambigüedad, es necesario enganchar cada responsable a una dependencia desde donde se ejecuta la actividad.

Se recomienda hacer un análisis más profundo de dichos procedimientos.

BIBLIOGRAFIA

ADMINISTRACION Y SOPORTE DE TI - ITIL [en línea]. ITERA it & Busies Process . [En línea]. [Consultado el 26 de Julio de 2012]: Disponible en: http://www.iteraprocess.com/index.php?option=com_content&task=view&id=13&Itemid=32&limit=1&limitstart=1

AGUILERA, Purificación. Seguridad informática. Editorial Editex S.A. Madrid España 2009. 240 Paginas

AREITO, Javier, Seguridad De La información. Redes, Informática y Sistemas de Información PARANINFO, Madrid España. 2008. 592 Paginas.

ARISTIZÁBAL, Andrés Y LÓPEZ, Hugo Andrés. USING PROCESS CALCULI TO MODEL AND VERIFY SECURITY PROPERTIES IN REAL LIFE COMMUNICATION PROTOCOLS. [En línea]. Trabajo de grado de Ingeniero de Sistemas y Computación. Santiago de Cali: Pontificia Universidad Javeriana. Facultad de Ingeniería. 2006. 115 Paginas [Consultado el 15 de enero de 2012]. Disponible en http://cic.puj.edu.co/~halopez/stuff/Tesis-halopez-aaristizabal.pdf Paginas 115.

BORGHELLO, Cristian. Seguridad Informática – Implicancias E Implementación. [En línea]. Trabajo De grado Licenciatura en Sistemas. Buenos Aires, argentina, Universidad Tecnología Nacional de Argentina. Faculta de Ingeniería 320 Paginas. [Consultado el 15 de enero de 2012]. Disponible en http://www.segu-info.com.ar/tesis/

CASTRO, Mauricio. El Nuevo Estándar ISO Para La Gestión Del Riesgo. [En línea]. SURLATINA CONSULTORES. [Consultado el 26 de Julio del 2011]: Disponible en: http://www.surlatina.cl/contenidos/archivos_articulos/13-el%20nuevo%20estandar%20iso%20para%20la%20gestion%20del%20riesgo.pdf

HEREDERO, Carmen de Pablos. Y LOPEZ-HERMOSO AGIUS, jose joaquin. Y ROMO ROMERO, Santiago Martin Dirección y gestión de los sistemas de información en la empresa.ESIC Editorial, Madrid España,2008 367 Paginas

INTECO. Sistema de Gestión de La Seguridad de La Información [en línea]. [Consultado el 26 de Julio del 2011]. Disponible en http://cert.inteco.es/Formacion/SGSI/Conceptos_Basicos/Concepto_SGSI/
I

SO/IEC 27001:2005. . Tecnología de la información – técnicas de seguridad – sistemas de gestión de seguridad de la información – requerimientos. Primera edición [en línea]. 40 Paginas [Consultado el 26 de Julio del 2011] Disponible en: http://mmujica.files.wordpress.com/2007/07/iso-27001-2005-espanol.pdf

ISO/IEC 27002:2005. Tecnología de la información – técnicas de seguridad. Codigo de práctica para la gestión de la seguridad de la información [en línea]. p. 2 [Consultado el 26 de Julio del 2011] Disponible en: http://es.scribd.com/doc/46085176/Normas-ISO-27002 133 paginas

ITIL: The Basics [en línea]. ITIL. [Consultado el 26 de Julio del 2011]: Disponible en: http://www.best-management-practice.com/gempdf/ITIL_The_Basics.pdf 5 Paginas

KNIGHT, Kevin W., New ISO Standard for Effective Management of Risk. [En línea]. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. [Consultado el 21 de Marzo del 2012]: Disponible en: http://www.iso.org/iso/pressrelease.htm?refid=Ref1266

MATALOBOS, Juan Manuel. ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN. [En línea]. Título de grado para Ingeniero Informático. Universidad Politécnica de Madrid: Madrid España. 2009. 306 p. [Consultado el abril 5 de 2012]. Disponible en http://oa.upm.es/1646/1/PFC_JUAN_MANUEL_MATALOBOS_VEIGAa.pdf

METODOLOGÍA OCTAVE ALLEGRO [en línea]. CERT. [Consultado el 26 de Julio del 2011]: Disponible en: http://www.cert.org/octave/download/allegro_form.html Versión 1.0 109 Paginas

MORA, Héctor. Manual del Vigilante de seguridad. Tomo 1 . 2ª Edición. Editorial: Club Universitario Alicante España, 2009 440 Paginas

ROJAS, Jorge Armando. Propuesta Sistema de Administración de Riesgos Integral. Material institucional de la Universidad Autónoma de Occidente. 2010. 6 Páginas

ROJAS, Jorge Armando. Catálogo de servicios de la División de Tecnologías de la Universidad Autónoma de Occidente. Material institucional de la Universidad Autónoma de Occidente. 2010. p2

Solórzano, Arturo J, Importancia de las tecnologías de la información y comunicación (TIC) para las PYMEs. [En línea]. TIC de UAM. [Consultado el 21 de Marzo del 2012]: Disponible en: http://ticdeuam.wikispaces.com/file/view/Importancia+de+las+TIC.pdf 3 Paginas

ANEXOS

ANEXO A. TABLAS DE ACTIVOS DE INFORMACIÓN E IMPORTANCIA RELATIVA.

En medio digital, en la carpeta anexo 1, se pueden ver las tablas correspondientes al desarrollo del perfil de los activos de información de cada uno de los procedimientos de los departamentos de Redes y Telecomunicaciones y de Cómputo, organizadas en carpetas.

En la carpeta Departamento de Redes y Telecomunicaciones se encuentran 23 tablas de Excel, correspondientes a cada uno de los procedimientos analizados para este departamento.

En la carpeta Departamento de Cómputo se encuentran 4 tablas de Excel, correspondientes a cada uno de los procedimientos analizados para este departamento.

ANEXO B. TABLA DE MATRIZ DE RIESGOS PARA LAS ESTACIONES DE TRBAJO CRÍTICAS.

En medio digital, en la carpeta anexo 2, se puede ver la tabla correspondiente a la matriz de riesgos generada para las estaciones de trabajo críticas de los departamentos de Redes y Telecomunicaciones y de Cómputo.

ANEXO C. TABLA DE CONTROLES PROPUESTOS SOBRE LAS VULNERABILIDADES.

En medio digital, en la carpeta anexo 3, se puede ver la tabla correspondiente a la matriz de riesgos generada para las estaciones de trabajo críticas de los departamentos de Redes y Telecomunicaciones y de Cómputo con sus respectivos controles y objetivos de control propuesta.

ANEXO D. DIRECTRICES PLANTEADAS POR EL SISTEMA DE ADMINISTRACION RIESGO INTEGRAL.

En medio digital, en la carpeta anexo 4, se puede ver la propuesta del sistema de administración de riesgos integral (SARI), directrices planteadas por la coordinación de seguridad informática de la División de Tecnologías, con las cuales se desarrolló este trabajo.