DISEÑO DE POLÍTICAS DE SEGURIDAD PARA LA RED DE DATOS DE LA INSTITUCIÓN UNIVERSITARIA TECNOLÓGICA DE COMFACAUCA POPAYÁN A TRAVÉS DE ANÁLISIS, GESTIÓN DE RIESGOS Y VULNERABILIDADES

WILMAR ANDRÉS DUARTE ORTIZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESPECIALIZACION SEGURIDAD INFORMATICA
POPAYAN
2018

DISEÑO DE POLÍTICAS DE SEGURIDAD PARA LA RED DE DATOS DE LA INSTITUCIÓN UNIVERSITARIA TECNOLÓGICA DE COMFACAUCA POPAYÁN A TRAVÉS DE ANÁLISIS, GESTIÓN DE RIESGOS Y VULNERABILIDADES

WILMAR ANDRÉS DUARTE ORTIZ

TRABAJO DE GRADO PARA OPTAR AL TÍTULO DE
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

DIRECTOR DE PROYECTO
MARTIN CAMILO CANCELADO TUIZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS E INGENIERÍA
ESPECIALIZACION SEGURIDAD INFORMATICA
POPAYAN
2018

Nota de aceptación

_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del presidente del jurado

_____
Firma del presidente del jurado

POPAYÁN, MAYO DE 2018

DEDICATORIA

Este proyecto de grado está dedicado en primer lugar a Dios por ser tan bondadoso conmigo al permitirme haber llegado hasta esta el final de este proceso, a mi familia y en particular a mi madre y abuela materna quienes son el motor de mi vida. También agradezco a las demás personas que en algún momento me brindaron su apoyo y con sus buenos deseos me impulsaron para poder alcanzar mis metas propuestas y de esta manera continuar creciendo como ser humano y como profesional.

AGRADECIMIENTOS

Ingeniero Salomón González por su apoyo y orientación durante el proceso de culminación del proyecto.

Ingeniero Martín Camilo Cancelado Tuiz por el valioso aporte con sus conocimientos y sugerencias para el desarrollo del proyecto.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

FORMATO DE POLÍTICAS DE SEGURIDAD

Pág.

GLOSARIO

Ataque
Evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema. [1]

Amenaza
Causa peligrosa que puede generar un incidente no deseado, produciendo daños materiales o pérdidas inmateriales en sus activos.

Impacto
Calcular la consecuencia al materializarse una amenaza.

Riesgo
Posibilidad de que se produzca un impacto determinado en un Activo, en un Dominio o en toda la Organización. [2]

Vulnerabilidad
Posibilidad de ocurrencia de la materialización de una amenaza sobre un Activo.

Confidencialidad
Es una propiedad de la información que limita el acceso a la información debido a la importancia o valor que se ha asignado dentro de una organización y que solo puede estar disponible al personal autorizado para prevenir algún tipo de riesgo.

Disponibilidad
Es la propiedad que se le asigna a la información en determinado momento y para determinado fin.

Seguridad de la información
Es un estado de cualquier tipo de información (informático o no) que indica que ese sistema está libre de peligro, daño o riesgo. Se entiende como peligro o daño todo aquello que pueda afectar su funcionamiento directo o los resultados que se obtienen del mismo.[3]

---

[1] Universidad Nacional Autónoma de México. Seguridad informática. (Consultado el 15 de Septiembre de 2017). Disponible en http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/Ataques.php

[2] Galeon.com. seguridad informática. (Consultado el 15 de Septiembre de 2017). disponible en http://audisistemas2009.galeon.com/productos2229098.html

[3] Ecured. Seguridad informática. (consultado el 15 de Septiembre de 2017). disponible en disponible en https://www.ecured.cu/Seguridad_Inform%C3%A1tica

RESUMEN

El presente proyecto tiene como propósito la realización del diseño de políticas de seguridad para la red de datos de la Institución Universitaria Tecnológica de Comfacauca Popayán, a través del análisis, gestión de riesgos y vulnerabilidades ya que la información que se maneja en la institución es muy valiosa y requiere de protección de posibles eventualidades u amenazas que puedan llegar a ocurrir en la organización.

Se pudo evidenciar que al no tener buenas prácticas de seguridad informática en cuanto a la red, existe vulnerabilidad en la seguridad de los activos, lo que conlleva a generar daños y pérdidas de información así como también pérdidas económicas para la institución.

Es por eso que en el presente proyecto se realizó el proceso de diseño de políticas de seguridad para la red de datos de la Institución Universitaria Tecnológica de Comfacauca Popayán, basándose en la norma ISO 27001:2013 y en la metodología NIST SP 800-30. El diseño de las Políticas de Seguridad Informática se desarrolló a través de cuatro (4) fases:

En la primera fase se realizó un análisis de los activos de la Institución Universitaria con el fin de identificar cuáles son los activos más importantes en la red de datos de la Institución.

En la segunda fase se realizó el diagnóstico del estado de los activos en la red de la Institución Universitaria donde se utilizó la metodología NIST SP 800-30 y de acuerdo a ello se clasificó según su tipo de riesgo así: alta, media o baja; con el fin de verificar cuales son los activos con mayor riego de vulnerabilidad en cuanto a la seguridad informática.

Después de esto se procede a tomar como referencia los Controles del Anexo A del estándar ISO 27001:2013 y dominios a los que pertenece, esto con el fin de tener un Sistema de Gestión de Seguridad de la Información acorde a lo que dice esta norma y teniendo en cuenta los resultados obtenidos en la matriz de riesgos de la metodología NIST SP 800-30

En la tercera fase se procede al diseño de políticas de seguridad informática basadas en la Norma ISO 27001:2013; con la finalidad de proteger los activos de la Institución Universitaria para evitar su robo, pérdida, modificación o también el mal uso de su información.

En la cuarta fase se procede al desarrollo e implementación de las políticas de seguridad con el fin de minimizar las vulnerabilidades encontradas en el estudio realizado a la red de datos de la Institución Universitaria Tecnológica de Comfacauca. En estas políticas se encontrarán el adecuadamente uso y controles que se pueden utilizar en un determinado activo o recurso de la red para proteger así la información de posibles amenazas a las que está expuesta la red de datos en la institución.

INTRODUCCIÓN

En la actualidad, las instituciones de educación superior en el Departamento del Cauca tienden a apoyarse en las tecnologías de la información y las comunicaciones para realizar los procesos más importantes de sus labores diarias, a medida que la gestión de la información sobre la red se hace más crítica, las instituciones tienen el deber de reforzar la seguridad de sus recursos y sus activos informáticos implementando correctamente mecanismos de seguridad en las redes de computadores, en busca de evitar el mal funcionamiento de los procesos y disminución en la eficiencia de los mismos, además de pérdidas sustanciales de dinero, credibilidad del buen nombre de la institución y tiempo de ejecución de proyectos.

Teniendo en cuenta lo anterior, es importante mencionar que con el paso del tiempo la información se ha convertido en el activo más importante de las instituciones y organizaciones, por lo tanto, debe existir en estos sitios, técnicas que aseguren más allá de la parte física de los equipos en donde es almacenada la información. Estas técnicas son brindadas por la seguridad lógica (software) que consiste en la aplicación de barreras y procedimientos que resguardan el acceso a los datos y sólo permiten acceder a ellos a las personas autorizadas para hacerlo.

Al no tener políticas establecidas en la Institución Universitaria, se puede llegar a exponer la información a diferentes tipos de amenazas, lo que conlleva a generar que la información pierda su integridad y disponibilidad. Ésta es una problemática que se puede presentar en cualquier organización, y donde se debe involucrar a la alta dirección, haciendo notar la importancia del manejo y uso de la información, a fin que se comprometa con apoyar el proceso y poder de esta manera llevar acabo la implementación. Adicionalmente, se debe involucrar la asignación de recursos físicos y de personal que apoye con el conocimiento, la agilidad con que se llegue a realizar la implementación de las políticas para la protección de la red de datos de la institución.

Es así como durante el desarrollo del proyecto se podrá evidenciar la clasificación de los activos de la información mediante la metodología NIST SP 800-30, la cual permite identificar las posibles amenazas que puedan ocurrir en la Institución Universitaria y con base en este diagnóstico se pueden proponer políticas de prevención y control para la protección de los activos y a su vez, permitirá mitigar la perdida de información de la Institución Universitaria Tecnológica Unicomfacauca.

1. PROBLEMA DE INVESTIGACIÓN

1.1. DESCRIPCIÓN DEL PROBLEMA

Actualmente, la Institución Universitaria Tecnológica Comfacauca Popayán, dentro de su planta interna cuenta con el departamento de las tic´s el cual tiene asignada la administración de herramientas informáticas que permitan fortalecer los procesos y procedimientos que se desarrollan de forma virtual en la institución. Sin embargo, actualmente no cuentan con el establecimiento de políticas de seguridad, controles, estándares y herramientas vigentes que realicen un diagnóstico real de la red y a sus servicios lo cual se presenta como vulnerabilidad y riesgos de incidentes de seguridad informática como ataques cibernéticos, hacheó de cuentas y de la información y otros que se presentan ocasionalmente.

Es por ello que en el presente proyecto, se busca establecer los mecanismos de prevención, protección y como factor importante, también busca que el personal de las tic´s de la Institución, sea sensibilizado y capacitado acerca de la importancia de la implementación de políticas y mecanismos que permitan asegurar, gestionar y mejorar la integridad de la información en la División de Tecnologías de la Información y las Comunicaciones, dependencias de la institución y también de los usuarios que utilicen la red.

1.2. FORMULACIÓN DEL PROBLEMA

¿El diseño de políticas de seguridad para la red de datos de la Institución universitaria disminuirá la pérdida o mala manipulación de la información en la Institución Universitaria?

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Proponer políticas de seguridad para el Departamento de Tic´s en la Institución Universitaria Tecnológica de Comfacauca usando la norma ISO 27001:2013 implementando la metodología NIST SP 800-30 de evaluación de riesgos basado en la identificación de los activos, en el cálculo de las amenazas y vulnerabilidades.

2.2 OBJETIVOS ESPECÍFICOS

- Identificar los requerimientos sobre seguridad de la información almacenada y transmitida a través de las redes de datos en la Institución Universitaria Tecnológica de Comfacauca.

- Realizar el diagnóstico sobre el estado actual de seguridad de la información en la red de datos de la Institución Universitaria Tecnológica de Comfacauca a través del panorama de riesgos, utilizando los controles establecidos en la norma ISO 27001:2013 y la metodología NIST SP 800-30 y así seguir las recomendaciones vigentes que estas proporcionan, para poder controlar los recursos de la institución.

- Diseñar formatos de control y administración de acuerdo a las políticas de seguridad de la información que apoyen el cumplimiento y verificación dentro de la red de datos de la Institución Universitaria Tecnológica de Comfacauca.

- Implementar estrategias, mecanismos de control y gestión de riesgos en busca de minimizar las vulnerabilidades encontradas en el estudio de la red de datos de la Institución Universitaria Tecnológica de Comfacauca.

3. JUSTIFICACIÓN

Debido a los múltiples ataques de hackers, virus y otros tipos de vulnerabilidad como desastres naturales, atentados terroristas y demás de tipo informático a los que se encuentra expuesta actualmente el área de las Tic´s de la institución universitaria Tecnológica de Comfacauca, además de la poca inversión y preparación del personal encargado del área de tecnología, se pone en riesgo un activo valioso de toda organización, como lo es la Información, de no concienciar y capacitar al personal acerca del correcto uso de los recursos tecnológicos, la institución podrá perder miles de millones de pesos por la mala manipulación de su información, por lo tanto, se hace necesaria la creación de políticas de seguridad mediante la implementación de metodología de evaluación de riesgos, la cual permite la verificación de riesgos en lo referente a la seguridad de la información almacenada y transmitida a través de las redes de datos en la Institución Universitaria Tecnológica de Comfacauca. Para ello, es importante inicialmente realizar un diagnóstico detallado utilizando los controles establecidos en la norma ISO 27001:2013 y la metodología NIST SP 800-30 y así seguir las recomendaciones vigentes que esta proporciona, para poder controlar los recursos de la institución y de esta manera diseñar de controles propios que apoyen el cumplimiento y verificación dentro de la red de datos de la Institución Universitaria Tecnológica de Comfacauca y de esta manera se disminuyan las vulnerabilidades encontradas.

Por otra parte y como factor importante dentro de la implementación de políticas de seguridad se deberá proceder a realizar el proceso de sensibilización y capacitación de los colaboradores de la institución acerca de la importancia del uso de herramientas y la aplicación de las futuras políticas de seguridad expuestas en el presente proyecto, direccionadas a facilitar y proteger los datos y de esta manera prevenir la pérdida o daño de la información de la Institución Universitaria Unicomfacauca Popayán.

4. ALCANCE Y DELIMITACIÓN DEL PROYECTO

En la actualidad la Institución Universitaria Tecnológica de Comfacauca no cuenta con políticas de seguridad formalmente implementadas para el área de tic´s. En este momento la universidad cuenta con un lugar centralizado para los servidores, respaldados por una seguridad la cual no se encuentra documentada.

El proyecto se realizará para la creación de políticas de seguridad para el área de red datos de la universidad. Para poder realizar dichas políticas de seguridad que se debe trabajar involucrando a los colaboradores de la Institución, los procesos y los recursos de tecnología existentes. El presente proyecto tiene como objetivo fundamental el estudio de vulnerabilidades, que afectan la seguridad de la rede de datos de la Institución Universitaria Tecnológica de Comfacauca, con el fin de garantizar la integridad, disponibilidad y accesibilidad de la información para así proveer un servicio de calidad a los usuarios finales (Alumnos, Administrativos, Docentes etc.)

El proyecto está delimitado al área de las tic´s de la institución, mediante la creación de políticas de seguridad para la Institución, con el fin de que estas políticas sean aplicadas y de esta manera se mejoren los servicios a los usuarios.

Para ello se considera importante la tener en cuenta los siguientes elementos:

- Análisis de riesgos de los recursos tecnológicos de la Institución Universitaria Tecnológica de Comfacauca
- Realizar la implementación de políticas de seguridad de la información para el buen funcionamiento de los servicios tecnológicos de Unicomfacauca
- Organización física del área de TI de Unicomfacauca.
- Estudio del recurso Humano para el área de TI de Unicomfacauca.
- Controlar y verificar los activos más críticos.

5. MARCO REFERENCIAL

5.1. ANTECEDENTES

Se llevó a cabo una investigación de proyectos, tesis y estudios realizados con la temática de seguridad informática a nivel nacional, con el propósito de identificar los avances y los hallazgos encontrados referentes al tema mencionado.

En primer lugar se tiene el trabajo llamado “Modelo para la implementación del sistema general de seguridad informática y protocolos de seguridad informática en la oficina tic de la Alcaldía Municipal de Fusagasugá, basados en la gestión del riesgo informático” [4]elaborado por Ana Milena Pulido Barreto y Jenith Marsella Mantilla Rodríguez, publicado en Abril de 2016, como Tesis de grado de la especialización en seguridad informática de la Universidad Nacional Abierta y a Distancia ,el cual se encuentra en la Biblioteca Virtual de la Universidad; en este documento se puede observar los beneficios que traerá este a la Alcaldía del Municipio de Fusagasugá, con un Modelo que le permitirá implementar un Sistema Gestión de Seguridad de la información y protocolos de Seguridad que contribuyan a la Oficina TIC a realizar una mejor gestión y control de los riesgos informáticos que han sido identificados en la entidad.

Otro trabajo investigado fue El trabajo llamado “Diseño de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/iec 27001 para la dirección de sistemas de la gobernación de Boyacá.”[5], elaborado por Lidia Constanza Contreras Esguerra, como tesis de grado de la especialización en seguridad informática de la Universidad Nacional Abierta y a Distancia ,el cual se encuentra en la Biblioteca Virtual de la Universidad; documento en el cual se demuestra que es indispensable para cualquier organización implementar procesos y procedimientos necesarios para un Sistema de Gestión de Seguridad de la Información (SGSI) que es una herramienta que le permite a una organización realizar una completa gestión de los riesgos que se presentan en la producción, procesamiento, almacenamiento y análisis de la información, buscando mantener siempre las características de Confidencialidad, Integridad y Disponibilidad con las que ésta debe contar. La implementación de un SGSI en cualquier compañía conlleva realizar una serie

[4] Pulido Barreto, Ana Milena Mantilla y Rodríguez, Jenith Marsella. Modelo para la implementación del sistema general de seguridad informática y protocolos de seguridad informática en la oficina TIC de la alcaldía municipal de Fusagasugá, basados en la gestión del riesgo informático. Tesis de grado Especialista en Seguridad Informática. Arbeláez: Universidad Nacional Abierta y a Distancia. 2016. (consultado el 05 de Noviembre de 2017). disponible en http://hdl.handle.net/10596/6327

[5] Contreras Esguerra, Lidia Constanza. Diseño de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/iec 27001 para la dirección de sistemas de la gobernación de Boyacá. Tesis de grado Especialista en Seguridad Informática. Tunja: Universidad Nacional Abierta y a Distancia. 2016. (consultado el 05 de Noviembre de 2017). disponible en http://hdl.handle.net/10596/11895

de actividades que deben ceñirse a lo señalado por el grupo de normas ISO/IEC 27000, siendo la ISO/IEC 27001 la que establece los requisitos para la certificación, pero teniendo en cuenta las recomendaciones y mejores prácticas descritas en las demás

Según el proyecto de "implementaciones un sistema de gestión de seguridad de la información para una empresa de consultoría, aplicando la norma ISO/IEC 27001"[6], por Tola. Diana, publicado como tesis de grado para licenciado en sistemas de Información, en Guayaquil – Ecuador, en el 2015. Se requiere de la aplicación de medidas preventivas dentro de las organizaciones e instituciones, que tienen para el cumplimiento de su objetivo y misión, el uso de herramientas tecnológicas y por lo tanto, el uso de datos que deben ser protegidos, en busca de mantener la confidencialidad, integridad y disponibilidad oportuna de la información, entendiéndose esto, como impedir la divulgación de datos privados.

Finalmente, "el análisis de riesgos según la norma ISO 27001:2013 para las aulas virtuales de la Universidad Santo Tomas modalidad presencial", [7] por García, Viviana y Ortiz, Jhon publicado como proyecto de especialización en Seguridad en Redes, en Bogotá D.C, 2017. Donde se manifiesta la necesidad de la aplicación de mecanismos de seguridad y control de la información dentro de las instituciones educativas universitarias, para evitar el daño o perdida de la información, especialmente lo relacionado con el departamento financiero, académico y de las ti, por lo tanto, se propone el cumplimiento y aplicación de controles y políticas de seguridad, de acuerdo con la normatividad vigente, en este caso, menciona la norma ISO 27001: 2013, para contribuir con la estabilidad de información académica y administrativa de la institución.

[6] Tola Franco, Diana Elizabeth. implementaciones un sistema de gestión de seguridad de la información para una empresa de consultoría, aplicando la norma ISO/IEC 27001. Tesis de grado. Escuela Superior Politécnica del Litoral (ESPOL).Quito–Ecuador (consultado el 05 de Noviembre de 2017). disponible en http://www.dspace.espol.edu.ec/xmlui/handle/123456789/31114

[7] García Balaguera, Vivian Andrea y Ortiz González, Jhon Jarby. Análisis de riesgos según la norma ISO 27001:2013 para las aulas virtuales de la Universidad Santo Tomás modalidad presencial. Tesis de grado Especialista en Seguridad Informática. José Acevedo Gómez: Universidad Nacional Abierta y a Distancia. 2016. (consultado el 05 de Noviembre de 2017). disponible en http://hdl.handle.net/10596/12028

5.2. MARCO CONTEXTUAL

5.2.1 INSTITUCIÓN UNIVERSITARIA TECNOLÓGICA DE COMFACAUCA

Misión

La Institución Universitaria Tecnológica de Comfacauca tiene como misión contribuir a la formación de personas emprendedoras, con calidad humana y alta competencia e impulsar la tecnología y la productividad, apoyándose en la ciencia, mediante las funciones de docencia, investigación y proyección social, en la búsqueda constante de la excelencia y con un compromiso ineludible con la equidad social y el mejoramiento de las condiciones de vida de caucanos y colombianos, especialmente de los afiliados de la Caja de Compensación Familiar del Cauca.

Visión

La Institución Universitaria Tecnológica de Comfacauca será una institución universitaria adecuada al contexto social y económico regional, que impacta el suroccidente Colombiano por la cobertura con equidad, por su excelencia académica, por su articulación con el sector productivo y por el nivel de competencia y emprendimiento de sus egresados. Igualmente, será reconocida por la calidad de la gestión tecnológica y de la investigación orientada a la solución de problemáticas sociales y productivas y por la proyección social de sus programas.

Política de Calidad

Propender por la eficiencia y eficacia de nuestros servicios, a través de la mejora continua de nuestros procesos, fundamentados en la docencia, la investigación y la proyección social, articulados con el sector productivo y encaminado a exceder la satisfacción de la comunidad.

Reseña

La Institución Universitaria Tecnológica de Comfacauca es una universidad joven que ingresa a participar en el ambiente académico en el año 1999, denominándose en aquel entonces como Instituto Tecnológico de Educación Superior de Comfacauca, el cual se crea con el fin de fundar una nueva universidad que contribuyera a cumplir, en ese entonces, con las necesidades de la región y del país y complementara áreas docentes que no se ofrecían como opción de educación superior en la región.

Fue así como, del estudio de factibilidad presentado ante el Instituto Colombiano para el Fomento de la Educación Superior ICFES, se aprobó la creación del Instituto Tecnológico de Educación Superior de COMFACAUCA y gestada por iniciativa de la Caja de Compensación Familiar del Cauca, entidad privada, sin ánimo de lucro, cuya misión consiste en "mejorar la calidad de vida del trabajador afiliado, su familia y de la comunidad en el Departamento del Cauca mediante el pago de Subsidio Familiar Monetario, la prestación de servicios de calidad en el campo de la seguridad social y mercadeo de productos competitivos que nos permitan ser líderes del sector...". La Caja de Compensación ha ampliado sus objetivos enmarcados en la misión para propiciar el desarrollo empresarial con criterio social y el mejoramiento de la calidad de vida en el Departamento del Cauca y la región sur-occidental, mediante la formación de personas integrales con capacidad para vincularse al entorno mediante prácticas positivas que incidan en el crecimiento social y económico de la región.

Ya en el año 2008, el Instituto Tecnológico de Educación Superior de Comfacauca, vio la necesidad de establecer un proceso de profesionalización de sus programas y cubrir las nuevas necesidades de la comunidad educativa, por lo cual realiza los procedimientos respectivos ante el Ministerio de Educación Nacional, para lograr cambiar su carácter académico y pasar a ser la actual INSTITUCIÓN UNIVERSITARIA TECNOLÓGICA DE COMFACAUCA, carácter otorgado mediante resolución 8210 del 2008.

Así, La Institución Universitaria Tecnológica de Comfacauca tiene como tarea prioritaria en el Sur Occidente la educación para el desarrollo regional y local. Su existencia y funcionamiento es el resultado de diversas capacidades y recursos en interacción. Consciente de su propio compromiso, la institución busca cultivar la ciencia, la tecnología y el espíritu, bajo los principios de la democracia participativa, con responsabilidad histórica de contribuir mediante soluciones concretas a las necesidades del actual desarrollo de la región.

Las actividades institucionales materializan los conceptos, procesos y directrices establecidos en el Proyecto Educativo Institucional, garantizando la formación de personas competentes en los diversos campos profesionales, de sujetos autónomos capaces de impactar el entorno con valores y prácticas positivas, contribuyendo al desarrollo económico y social mediante la aplicación, adaptación y creación de técnicas contemporáneas a los diversos modelos de la producción y los servicios, así como la investigación aplicada a las condiciones, necesidades y potencialidades regionales. Los programas y las actividades de la Institución se formulan para materializar los criterios y procedimientos de la educación, los que la hacen o convierten en factor imprescindible de socialización y el medio indispensable para cultivar en el hombre la comprensión mutua y su realización existencial.

La Institución Universitaria Tecnológica de Comfacauca constituye en sí misma un entorno educativo abierto en el que confluyen muchos actores participando en múltiples procesos. El entorno educativo no solo está compuesto por los actores sino también por los productos culturales que sirven de interfaz para el desempeño de esos actores: espacios físicos, tiempo, instrumentos y equipos, estructura organizativa, normas, etc.

Así, la Institución se establece en la región como una organización privada, de utilidad común, sin ánimo de lucro, que articula la ciencia con la técnica y vincula la educación al saber práctico para atender los requerimientos del mundo laboral y productivo.

Recorrido

La Institución Universitaria Tecnológica de Comfacauca es una Institución joven, que ha logrado posicionarse en el departamento del Cauca gracias al importante desempeño de sus egresados en el sector productivo, a su significativa labor en el campo de la investigación, por la amplia infraestructura física y tecnológica con la que cuenta y por el alto nivel académico que brinda a sus estudiantes.

En este sentido, desde el año 2001, Unicomfacauca ofrece programas relacionados con la industria, tales como electrónica, producción industrial y aseguramiento de calidad, entre otros, inicialmente en el nivel tecnológico y posteriormente universitario. De este modo, ha ampliado su portafolio de programas académicos de pregrado en las áreas de ingeniería de sistemas, comunicación social y periodismo, gastronomía, producción agrícola y de alimentos, desarrollo de software y contaduría. Igualmente, ofrece programas de especialización y maestría en educación, en convenio con otras instituciones colombianas.

La institución cuenta con infraestructura física y tecnológica consolidada en cuatro ciudades del Departamento del Cauca.

Un ejemplo es el desarrollo de laboratorios de acceso remoto sobre redes de alta velocidad en el área de robótica, proyecto cofinanciado por Colciencias y que integra laboratorios tele-operados en cuatro universidades en colaboración.

Grupos y docentes investigadores desarrollan proyectos en áreas como comunicación social, educación superior, tecnologías en sistemas de información, control e instrumentación industrial, tecnologías agroambientales y cadenas productivas de valor.

En proyección social y cooperación técnica nacional e internacional, la universidad ha desarrollado proyectos y alianzas para la ampliación de

cobertura educativa, equidad, mejoramiento de la calidad y fortalecimiento del vínculo universidad-empresa, cofinanciados por el gobierno nacional (Ministerios de Educación con recursos del Banco Interamericano de Desarrollo (BID) y la Banco de Desarrollo de América Latina (CAF); Ministerio de Agricultura, Colciencias, Instituto de Investigación Alexander von Humboldt e Icetex) y organizaciones internacionales como la Fundación Panamericana, Youth Foundation y la Agencia Española de Cooperación Internacional.

Estos proyectos involucran alianzas de colaboración con otras universidades, gremios productivos y gobiernos locales.

Cuenta además con una Unidad de Emprendimiento, que le permite a la comunidad académica gozar de asesoramiento desde la formulación de una idea de negocio hasta la creación de la propia empresa. Esta dinámica ha permitido la generación de ideas de negocio exitosas relacionadas con el campo de la gastronomía y los sistemas, las cuales han obtenido reconocimientos por parte de Impulsarte y el Fondo Emprender respectivamente.

De igual manera, es importante resaltar que la Institución Universitaria fue la primera en recibir, por parte del ICONTEC, la certificación de calidad nacional ISO 9001:2008 e internacional IQNet para siete de sus programas académicos.

En una política de internacionalización, la Institución ha venido desarrollando convenios y alianzas de cooperación interinstitucionales para intercambio académico, desarrollo conjunto de programas y proyectos de formación e investigación y doble titulación. Ha suscrito convenios con universidades extranjeras tales como Halmstad University (Suecia), Universidad San Ignacio de Loyola -USIL (Perú), Universidad de Barcelona y Universidad Politécnica de Valencia (España). La Institución se proyecta así como una institución de educación superior joven, que crece con calidad y pertinencia.

En este sentido, la Institución Universitaria Tecnológica de Comfacauca busca que cada uno de sus procesos y dinámicas formativas evolucione de acuerdo con las necesidades del Cauca y del país, estableciendo actividades que le permitan al estudiante enfrentar los retos profesionales que se le presenten en un mercado laboral cambiante y globalizado.

Unicomfacauca ofrece más de 20 programas académicos en sus diferentes sedes en el departamento, ubicadas en Popayán, Santander de Quilichao, Puerto Tejada y El Bordo, las cuales cuentan con una excelente planta física y la mejor tecnología para el desarrollo de prácticas y procesos de investigación.

Entre sus programas de formación superior Unicomfacauca ofrece programas Universitarios, Tecnológicos y Técnicos Profesionales así:

Programas Universitarios

- Ingeniería de Sistemas (10 semestres)
- Contaduría Pública (10 semestres)
- Comunicación Social y Periodismo (9 semestres)

Programas Tecnológicos

- Sistemas Empresariales de Información (6 semestres)
- Maquinaria e Instrumentación Industrial (6 semestres)
- Gestión de Empresas Agrícolas (6 semestres)
- Comunicación Social y Periodismo (6 semestres)
- Aseguramiento de la Calidad (6 semestres)
- Realización Audiovisual (6 semestres)
- Electrónica (6 semestres)
- Electricidad (6 semestres)
- Agroambiental (6 semestres)
- Gastronomía (6 semestres)
- Producción Industrial (6 semestres)
- Publicidad (6 semestres)

Programas Técnicos Profesionales

- Desarrollo de Software (4 semestres)
- Procesamiento de Alimentos (4 semestres)
- Producción de Frutas y Hortalizas (4 semestres)
- Fabricación de Papel (4 semestres)
- Impresión Gráfica (4 semestres)
- Repostería Gráfica (4 semestres)
- Periodismo (4 semestres)[8]

[8]Unicomfacauca (2017).Inicio. Corporación. Quienes Somos. (consultado el 20 de Agosto de 2017). disponible en http://www.unicomfacauca.edu.co/index.php/institucion/2013-05-09-23-07-45#rese%C3%B1a-hist%C3%B3rica

5.3 MARCO TEORICO

Con el crecimiento de las nuevas tecnologías en las últimas décadas, se hace necesario investigar ,indagar y documentarnos en temas relacionados con la seguridad informática y la seguridad de la información, metodologías para el análisis de riesgos en seguridad informática como por ejemplo la metodología NIST SP 800-30 , normas internacionales como la ISO 27001 la cual describe cómo gestionar la seguridad de la información en un organización, poder identificar y clasificar las posibles vulnerabilidades o amenazas informáticas y por último plasmar el documento que nos permita realizar una adecuada estructuración del sistema de gestión de seguridad informática con sus respectivas etapas.

5.3.1 Seguridad de la Información

La información, en todas sus formas (automatizada o no automatizada, formalizada o no formalizada, pública o reservada, entre otras), es uno de los principales activos dentro de todas las organizaciones ya que se hace necesaria para el normal funcionamiento y para el logro de los objetivos que se tengan programados o que se deseen aplicar.

Teniendo en cuenta la importancia de la información, las organizaciones necesitan que exista una protección para la misma, con el objetivo de asegurar que se encuentre disponible en el momento que se requiera, además de ello, también es necesario que esta información sea confiable y que su distribución sea controlada; se requiere de esta información debido a que la cantidad y complejidad de información que manejan las organizaciones crece exponencialmente dificulta que se apliquen mecanismos para la protección. Es por ello que la seguridad que se debe aplicar a los sistemas de información debe actualizarse constantemente, por tal motivo se puede inferir que cada día hay una evolución y avance en ella y la meta o finalidad que se requiere alcanzar con la seguridad, es permitir el desarrollo de la organización así como también brindar seguridad a los socios, colaboradores, estudiantes, clientes, proveedores, administradores y demás personal involucrado en ellas

Los principales objetivos de la seguridad de la información son los siguientes:

I. Disponibilidad y accesibilidad de los sistemas y datos: Este objetivo, Comúnmente es uno de los objetos de seguridad más importantes dentro de las organizaciones, pues es únicamente para uso autorizado ya que es un requisito importante y es necesario ya que permite garantizar el trabajo específico y puntual del sistema, además de ello, se requiere de que este sea oportuno. La disponibilidad y accesibilidad se encarga de la protección del sistema frente a problemas determinados, como por ejemplo: intentos accidentales o intencionados de eliminar datos no autorizados, de causar

cualquier tipo de rechazo de algún servicio u acceso a datos o también del uso del sistema o los datos con fines no autorizados.

II. Integridad: se encarga vigilar y garantizar que toda la información del sistema continúe íntegra y no haya sido modificada por usuarios que no se encuentren autorizados; de este objetivo se despliegan dos facetas:

1. Integridad de datos. Esta faceta, hace referencia a la propiedad donde los datos no hayan sido alterados por usuarios no autorizados, durante el tiempo de su procesamiento, almacenamiento o transmisión.

2. Integridad del sistema. Se puede decir que esta faceta, es el objetivo más importante después de la disponibilidad, pues asume la característica que posee un sistema durante la ejecución de una función deseada, de manera no deformada y libre de manipulación o tratamiento de usuarios no autorizados. La integridad, normalmente es el objetivo de seguridad más importante después de la disponibilidad.

III. Confidencialidad de datos y de la información del sistema. Algunas organizaciones consideran que la confidencialidad se encuentra después del segundo objetivo disponibilidad en términos de “extrema importancia”, pues en algunos sistemas y algunos tipos de datos específicos como los autenticadores, este objetivo es de extrema importancia ya que es el requisito que busca que la información privada, secreta o exclusiva no se revele a usuarios no autorizados, esta confidencialidad es aplicada a los datos de almacenamiento durante el procesamiento, transmisión y tránsito de los mismos.

IV. Responsabilidad a nivel individual (registro de auditoría). Este objetivo, es la exigencia o requisito que permite que en la organización se puedan diseñar acciones de forma única, teniendo en cuenta que ocasionalmente debe existir políticas que soporten la retractación, aislamiento de fallas y detección de intrusiones además de la prevención de estas actividades, también debe contener información acerca de las acciones de recuperación y demás acciones legales que la organización considere pertinente.

V. Confiabilidad (aseguramiento). Hace referencia a la garantía de que los objetivos anteriormente descritos, se han cumplido de manera adecuada. Es la base que genera la confianza de que las medidas de seguridad, técnicas y operacionales, funcionan de tal manera como se plantearon inicialmente o se idearon con el fin de proteger el sistema y la información que en él se procesa.

La gestión de seguridad de la información se concibe como un proceso no aislado, por medio del cual, las organizaciones delimitan y logran mantener niveles de confidencialidad ventajosos y convenientes frente a la autenticidad

de la información que la organización opera, manteniendo la información integra y autentica.

Dentro del proceso de gestión de seguridad de la información, se incluyen los aspectos principales descritos a continuación:

- Determinación de objetivos, estrategias y políticas de seguridad de la información.
- Determinación de las obligaciones y requerimientos de seguridad de la información.
- La identificación y análisis de los riesgos y posibles peligros eventuales de seguridad.
- Especificación de protecciones convenientes teniendo en cuenta las amenazas, riesgos y vulnerabilidades que se identifiquen.
- Supervisión de la ejecución, implementación o el funcionamiento de las salvaguardas especificadas.
- Asegurar la concienciación de todo el personal en materia de seguridad de la información.
- Detección de las posibles incidencias de seguridad para reaccionar ante ellas.

En los últimos años, la disciplina en la seguridad de la información ha experimentado un rápido desarrollo, impulsado por la necesidad de formalizar todas las medidas de seguridad necesarias para proteger la información. De esta forma, el enfoque de la seguridad puramente basado en la tecnología (Seguridad Informática) ha pasado a un enfoque de la seguridad más global (abarcando aspectos tecnológicos, pero también legales, organizativos, culturales, etc.) planteando como un problema de negocio.

Con el enfoque global y de negocio de la seguridad de la información, se requiere de la implementación de herramientas de gestión que permitan facilitar la toma de decisiones a los responsables, con estas herramientas de gestión, el análisis que se realiza frente a los riesgos permite que se identifique y valoren las principales amenazas que existen para la seguridad de la información, esto analizado desde el punto de vista de negocio por lo tanto, es la eficiencia de la protección la que se establece para mitigar y/o eliminar los riesgos asociados.

5.3.2 **Norma ISO/IEC 27000**

Es un conjunto de estándares que fue creado por la ISO International Organization for Standardization) e IEC (International Electrotechnical Commission), esta norma proporciona las pautas para realizar la gestión de la seguridad de la información en cualquier organización de tipo pública o privada a nivel mundial.

5.3.3 **Normas relacionadas con las Norma ISO 27000**

- **ISO/IEC 27000:** Esta norma facilita y permite ver los sistemas de gestión de seguridad de la información y sus contenidos en cuanto a términos y definiciones que se utilizan en las diferentes normas de la 27000.

- **ISO/IEC 27001:** La última revisión hecha de esta norma fue el 25 de septiembre de 2013. Es la norma principal de la serie 2700 y en esta se encuentran todos los requisitos del sistema de gestión de seguridad de la información. En esta norma es donde se certifican todos los auditores que quieran realizar los SGSIs de las organizaciones.

- **ISO/IEC 27002:** Guía de buenas prácticas donde se detallan las tareas que deben tenerse en cuenta para el establecimiento e implementación de los objetivos de control y también la implementación de los controles recomendables para la seguridad de la información.

- **ISO/IEC 27003:** Guía donde se encuentra todo lo necesario para el diseño e implementación de un Sistema de Gestión de Seguridad de la Información de acuerdo a los requerimientos establecidos en la norma ISO/IEC 27001

- **ISO/IEC 27004:** Guía que especifica las métricas y técnicas de medición para determinar la eficacia de un SGSI y de sus controles.

- **ISO/IEC 27005**: Provee directrices para la gestión del riesgo en la seguridad de la información.

- **ISO/IEC 27006:** Detalla los requisitos que deben cumplir las organizaciones para la acreditación de entidades en auditoría y certificación de Sistemas de Gestión de Seguridad de la Información.

5.3.4 **Ciclo Deming en Iso 27001**

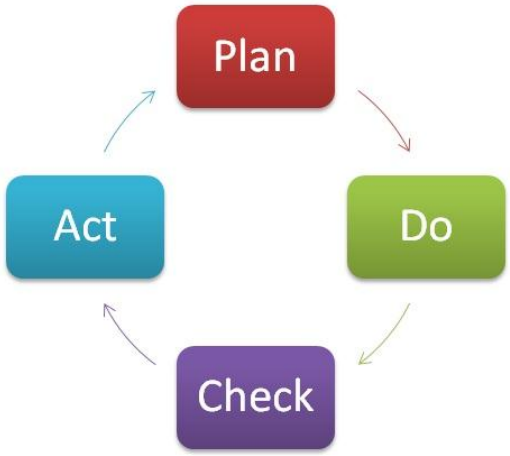
Para establecer y gestionar un Sistema de Gestión de Seguridad de la Información en base a la norma ISO 27001, se utilizará el ciclo continuo PHVA (del inglés Plan – Do - Check - Act), PHVA o también conocido como "Círculo de Deming", es uno de los métodos más utilizados para la implementación de estrategias continuas y de mejora de calidad en cuatro (4) pasos.

Las siglas PDCA significan:

- Plan (Planificar)
- Do (Hacer)
- Check (Verificar)
- Act (Actuar)

El ciclo Deming se representa en la siguiente figura:

FIGURA 1. CICLO DEMING-PDCA



Fuente: BERNAL Jorge Jimeno. Ciclo PDCA (Planificar, Hacer, Verificar y Actuar): El círculo de Deming de mejora continúa (en línea). España: el autor, 2013 (Consultado el 20 de noviembre de 2017). Disponible en: http://www.pdcahome.com/5202/ciclo-pdca/

- **Plan:** Es donde se define el alcance del SGSI en términos del área TI de la Institución Universitaria tecnológica de Comfacauca como la localización de los activos y tecnologías, incluyendo detalles y justificación de cualquier exclusión.

- **Hacer:** Donde se va a definir, Implementar y gestionar el plan de tratamiento de riesgos

- **Verificar:** En este punto se realiza los procedimientos de monitorización implementados en el Sistema de gestión de Seguridad informática.

- **Actuar:** Es donde se implementarán las mejoras identificadas en el sistema de gestión de seguridad de la información de la institución universitaria

5.3.5 **Metodología Nist Sp 800-30[9]**

La metodología National Institute of Standards and Technology (NIST), está compuesta por un conjunto de documentos cuyo contenido se centra en la aplicación de procedimientos y normas enfocados en la seguridad de la

[9] NIST. Risk Management Guide for Information Technology Systems Julio de 2002. (Consultado EL 02 DE noviembre de 2017). Disponible en: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

información. Desde 1990 ha venido realizando una serie de publicaciones entre las que se destaca la (SP 800), dedicada exclusivamente al análisis y gestión de riesgos de los sistemas informáticos.

La guía de evaluación de riesgos de NIST (9/18/2012), describe lo siguiente:

La NIST SP 800-30, está compuesta por 9 tareas o procesos que se deben seguir de manera ordenada para obtener los resultados previstos, esos procesos son:

- Caracterización de Sistemas.
- Identificación de amenazas.
- Identificación de vulnerabilidades.
- Análisis de controles.
- Determinación de probabilidades.
- Análisis de impacto.
- Determinación del riesgo
- Recomendación de controles.
- Documentación de resultados

5.4 MARCO CONCEPTUAL

Algunos de los aspectos que se deben tener en cuenta dentro del marco conceptual que se va a manejar en el siguiente proyecto está relacionado directamente con algunos conceptos que derivan de la seguridad informática y de la información, especialmente la temática que aborda las vulnerabilidades que pueden presentarse en los sistemas informáticos y que pueden afectar de manera significativa el correcto funcionamiento de cada uno de los procesos que se desarrollan en una organización.

Por ello, es importante tener en cuenta que el enfoque del presente proyecto es la protección de datos y el control de los recursos tecnológicos de la Institución Universitaria Tecnológica de Comfacauca mediante el uso y aplicación de los controles establecidos en la Norma ISO 27001:2013 y la metodología NIST SP 800-30 la cual puede utilizarse para evaluar los sistemas y analizar la probabilidad de eventos que pueden llegar a presentarse como son amenazas, pérdida de datos y otros tipos de vulnerabilidades con el fin de crear o fortalecer las políticas, normas y procedimientos propios que deben aplicarse para proteger los activos de información de la organización. Adicionalmente, se considera importante y necesario que los directivos y colaboradores de la Institución conozcan los procesos y demás aspectos relevantes acerca de las buenas prácticas para la protección de datos para así evitar la pérdida, alteración o mala manipulación de la información.

Dentro de los aspectos más relevantes que se deben conocer se encuentra principalmente la seguridad de la información haciendo referencia a un “estado de cualquier tipo de información (informático o no) que indica que dicho sistema se encuentra libre de peligro, daño o riesgo. A su vez, se entiende como peligro o daño todo aquello que pueda afectar su funcionamiento directo o los resultados que se obtienen del mismo”[10]. Por otra parte, también se considera importante conocer el significado de amenaza, concibiendo esta como una causa peligrosa que puede llegar a generar un incidente no deseado, produciendo daños materiales y pérdidas en los activos inmateriales como son los datos de la Institución.

[10] Ecured. Seguridad informática. (Consultado el 10 de Octubre de 2017). disponible en https://www.ecured.cu/Seguridad_Inform%C3%A1tica

5.5 MARCO LEGAL

Dentro de la normatividad aplicable para la Corporación Universitaria Comfacauca – UNICOMFACAUCA se relacionan las siguientes leyes:

5.5.1 Ley 1273 de 5 de enero de 2009 [11]

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

5.5.2 Ley 1581 de 2012 [12]

“Por la cual se dictan disposiciones generales para la protección de datos Personales.”

5.5.3 Decreto 1377 de 2013[13]

“Por el cual se reglamenta parcialmente la Ley 1581 de 2012”

[11] Alcaldía de Bogotá. Ley 1273 de 2009 Nivel Nacional. (consultado el 14 de Noviembre de 2017). disponible en http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

[12] Alcaldía de Bogotá. Ley 1581 de 2012 Nivel Nacional. (consultado el 14 de Noviembre de 2017). http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

[13] Alcaldía de Bogotá. DECRETO 1377 DE 2013. (consultado el 14 de Noviembre de 2017). http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646

6. DISEÑO METODOLOGICO

La investigación se llevará a cabo con la metodología cuantitativa, la cual supone un planteamiento, un acercamiento a la realidad objeto de estudio y a la teoría, así como también unos fines característicos de la investigación.

6.1.1 TIPO DE INVESTIGACION

La investigación que se llevará a cabo es de tipo cuantitativo, inicialmente es de carácter exploratorio, parte de la hipótesis de la situación considerada problema en el presente proyecto, la recolección de datos e información se realiza bajo la técnica de observación directa y se plasma de manera descriptiva es así como se aborda la seguridad informática identificando los principales riesgos de seguridad informática que tiene la institución; también podemos decir que es una investigación aplicada, orientada hacia la gestión de sistemas y en busca de generación de soluciones a los problemas que se presentan actualmente en la Institución Universitaria Tecnológica Unicomfacauca.

6.1.2 UNIVERSO Y MUESTRA

Para la Implementación la generación de políticas de seguridad a la red de datos, se establece como muestra al 100% de los procesos responsables del manejo de la información y a los sistemas utilizados en la Institución Universitaria Tecnológica de Comfacauca Popayán.

6.1.3 INSTRUMENTOS DE RECOLECCION

Para la recolección de la información se tienen establecidos los siguientes instrumentos de recolección:

Elaboración de Plantilla Diagnóstico esta se realiza para saber cuál es el estado actual de la Institución universitaria frente a la seguridad de la información, se aplicará este instrumento a cada uno de los responsables de los procesos según los requerimientos de la norma ISO 27001.

El diseño de instrumento de recolección se realizará para la aplicación de entrevistas personalizadas, las cuales serán aplicadas con cada equipo de trabajo de la institución: Según agenda programada y productos a obtener.

Establecer la estructura de la documentación acorde a las necesidades de la Institución Universitaria Unicomfacauca y lo establecido en la ISO 27001.

De acuerdo a la necesidades y el ambiente de trabajo se aplicaran las siguientes Técnicas para la recopilación de la información, con estas técnicas es posible identificar la situación actual de la Institución y así identificar posibles inconsistencias y realizar mejoras oportunas.

- Entrevista: se realizará esta para obtener información importante para la aplicación del proyecto, se utilizara una entrevista no estructurada, ya que esta técnica permitirá obtener los datos más relevantes y significativos e importantes para el proyecto, utilizando esta técnica vamos a obtener una opinión personalizada de los Profesionales de la institución Universitaria quienes son los encargados de todo lo relacionado con el departamento de las tic´s

- Observación: se utilizará esta técnica en el proyecto para que se lleve a cabo el registro del comportamiento de los usuarios (estudiantes, profesores y administrativos).

- Encuestas: se realizarán encuestas con el fin de comprender el nivel de dominio y conocimiento que tienen los usuarios de la Institución Universitaria Tecnológica Unicomfacauca acerca de amenazas, riesgos informáticos, vulnerabilidades y políticas de seguridad informática.

6.1.4 METODOLOGIA DE DESARROLLO

Para el desarrollo del presente proyecto se ejecutarán las siguientes etapas:

Etapa 1. Establecer un diagnóstico del estado actual de la seguridad de la información en el área de las TIC´s de la universidad, esto con el fin de saber si en la institución se lleva algún proceso o algún tipo de protocolo de políticas o alguna documentación, acerca de la seguridad de la información.

Para realizar esta etapa se procederá a:

- Indagar y examinar si existe alguna documentación respecto a la seguridad de la información.
- Tener una reunión con el encargado del área de las tic’s para determinar si existe o no alguna documentación sobre políticas, procesos de seguridad de la información de la institución universitaria

Etapa 2: verificar todos los activos que existen en el área de las TIC´s actualmente en la institución universitaria, esto con el fin de realizar la identificación de las vulnerabilidades, amenazas y riesgos de seguridad del área informática de los activos informáticos. Durante esta etapa se procedió a implementar la metodología NIST SP 800-30

Los pasos para realizar esta etapa son:

- Identificar, y clasificar los activos del área tecnológica de la universidad.
- Implementar la metodología NIST SP 800-30
- Analizar, recomendaciones y posibles vulnerabilidades encontradas en la universidad

Etapa 3: Elaborar y presentar las políticas de seguridad de la Institución Universitaria Unicomfacauca. Elaborar el resultado de la compilación, análisis de la información de las diferentes etapas desarrolladas para el presente proyecto.

7. APLICACIÓN E IMPLEMENTACION DE LOS OBJETIVOS

En esta fase del proyecto se inicia con la identificación, diagnostico, diseño e implementación de los mecanismos de control a la red de datos de la Institución Universitaria Tecnológica de Comfacauca para el cumplimiento de los objetivos planteados.

7.1 IDENTIFICAR LOS REQUERIMIENTOS SOBRE SEGURIDAD DE LA INFORMACIÓN ALMACENADA Y TRANSMITIDA A TRAVÉS DE LAS REDES DE DATOS EN LA INSTITUCIÓN UNIVERSITARIA TECNOLÓGICA DE COMFACAUCA.

Con el fin de establecer procesos de mejora en el Departamento de las Tic´s de la Institución Universitaria Tecnológica de Comfacauca, se procede a realizar una visita técnica a la Institución para la identificación de vulnerabilidades de la seguridad física, este proceso se realizó por medio de la norma ISO 27002:2013 en su Dominio número 11, siguiendo y evaluando el cumplimiento de cada uno se los subcontroles de la norma con su respectivo análisis para tener en cuenta en la elaboración de políticas de seguridad

A continuación se muestra el análisis de los procesos verificados y establecidos en la Norma ISO/IEC 27002:2013. Dominio numero 11 “Seguridad Física y Ambiental”

Tabla 1. Norma ISO/IEC 27002:2013

Dominio	Objetivo de Control	Controles	Cumple		Observaciones
			Si	No	

11. Seguridad física y ambiental	11.1 Áreas seguras.	11.1.1 Perímetro de seguridad física.		x	Estos controles se deberían utilizar para proteger las áreas que contengan información y recursos. La Institución Universitaria de Comfacauca no cuenta con mecanismos de control de acceso para el ingreso exclusivo de personal autorizado a determinadas zonas dentro de sus instalaciones. Como se evidencia en la siguiente imagen. **FIGURA 2. INGRESO AL DEPARTAMENTO DE LAS TIC´S**  Fuente: El Autor **FIGURA 3. INGRESO AL CORE**  Fuente: El Autor
		11.1.2 Controles físicos de entrada.		X	Cuando son mencionados los centros de datos y recursos, es muy conveniente pensar en la seguridad física y del entorno de estos, debido a que son ellos los que proveen la información crítica para el correcto funcionamiento de Unicomfacauca, dentro de esto se debe tener en cuenta, el robo de información, el sabotaje y el espionaje de datos. La necesidad de contrarrestar estas vulnerabilidades es más que obvia, la protección contra intrusos y el daño intencional podrían ocasionar los riesgos en la actividad ordinaria del personal que labora en estos centros de datos y recursos de procesamiento. Mantener a las personas no autorizadas o mal intencionado de lugares de donde no pertenecen, es el primer paso hacia el control físico y de los recursos. La definición de reglas de acceso puede producir un modelo de capas no tan complejo y mucho menos

					difícil de manejar pero con grandes ventajas para la seguridad de estas locaciones. El segundo paso es decidir la mejor manera para aplicar estos controles, entre ellos se pueden considerar, tarjetas inteligentes, escaneo de iris, huellas digitales, geometría facial, control de acceso manual, en busca de responder dos simples preguntas ¿quién es usted y porque está aquí? **Zonas de seguridad: Métodos de Identificación** En la seguridad de acceso juegan diversos métodos de identificación con diferentes niveles de seguridad basados en la norma ISO 27002, donde se encuentran tres categorías generales • **Lo que usted tiene:** Es un sistema menos confiable que los demás, debido a que es algo que se puede llevar de forma física como llaves, tarjetas u otros objetos, y por lo tanto siempre estará latente el riesgo de ser compartido o robado. El principal problema que esto genera es que no hay garantía de la identificación y utilización por parte de la persona correcta. • **Lo que usted sabe:** Sistema más confiable ya que no se puede robar a menos de que sea compartido o escrito, por lo general son códigos memorizados de acceso, contraseñas o PINs, pero para garantizar un nivel de confiabilidad más o menos bueno se deben tener ciertas consideraciones, si es fácil de recordar, es probable que también sea fácil adivinar y si es difícil de recordar probablemente también sea difícil de adivinar. Lo que sabes es más confiable que lo que tienes pero aun así este tipo de seguridad se reduce cuando son compartidas o escritas y que corren el riesgo de ser descubiertas. • **¿Quién es usted?:** Referido a la identificación mediante el reconocimiento de características físicas únicas donde los usuarios pueden registrarse y ser identificados con una certeza casi total. Existen diversos mecanismos tecnológicos para este tipo de seguridad; la biometría es una técnica de escaneo en donde se han desarrollado una serie de características humanas para el reconocimiento facial, huellas dactilares, e iris, tomando el patrón de colores de la vista, posición y patrón de los vasos sanguíneos de los ojos, retina, la nariz y boca, geometría de la mano, entre otros. Dentro de la organización existen diversos nodos o puntos críticos en donde la implementación de medidas de seguridad adecuadas es fundamental. Dos de ellas son muy importantes, los cuales se describen a continuación. **CORE / Redes de Computadores** Esta es la principal en donde convergen todos los accesos a los diversos sistemas informáticos ya sean físicos o lógicos, y la conexión a internet. El CORE contiene los enrutadores de acceso a internet, interconexiones en cable Utp 6e y fibra óptica

					para la comunicación entre los edificios, equipos de red. **Estado de la Seguridad** El acceso físico a esta zona es relativamente sencillo y fácil de penetrar, debido a que no cuenta con mecanismos de seguridad medianamente seguros. A continuación se exponen las posibles vulnerabilidades encontradas en el CORE. • Las llaves de la puerta para el ingreso al CORE están en un estantes colgadas, con un único mecanismo de seguridad de entrada (una chapa). • todo Cds y Dvs de instalación de programas y herramientas software son almacenados en esta ubicasion **FIGURA 4. EVIDENCIA LAS LLAVES DE LA PUERTA**  Fuente: El Autor **FIGURA 5. CDS, DVS DE INSTALACIÓN**  Fuente: El Autor División de Tic´s es el área en donde se concentran los servicios, sistemas de monitoreo de comunicaciones, equipos de ruteo y servidores de la organización.

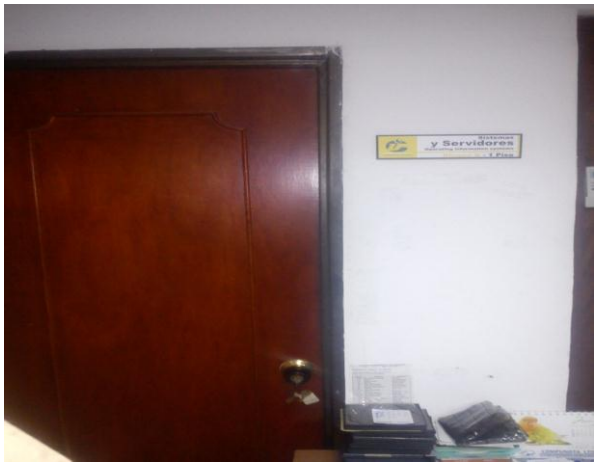
FIGURA 6. DIVISIÓN DE TIC Y SERVIDORES

Fuente: El Autor

Estado de la Seguridad

El acceso físico a estas instalaciones y su seguridad de ingreso está en un bajo nivel, las posibles vulnerabilidades encontradas se encuentran al acceso hacia los servidores está restringido por 2 puerta, la 1 de ellas es el acceso a Tic´s y la otra puerta es de los servidores, el otro control es una persona que se encuentra ubicada al ingresar a esta departamento (jefe se tic´s).

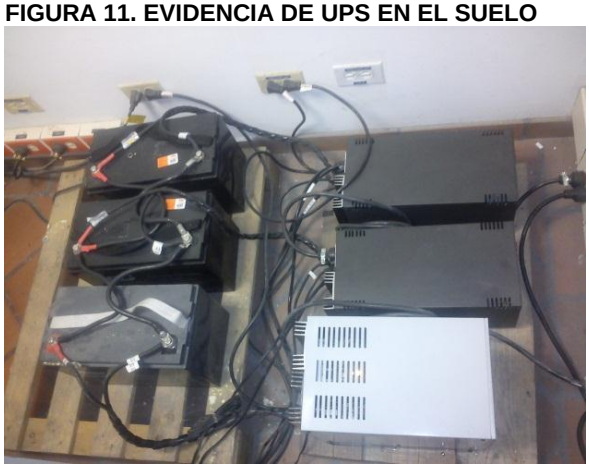
FIGURA 7. EVIDENCIA CONTROL ACCESO A DIVISIÓN DE TIC Y SERVIDORES

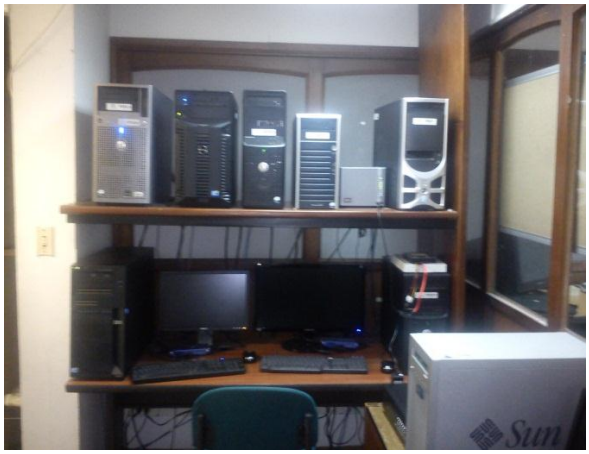


Fuente: El Autor

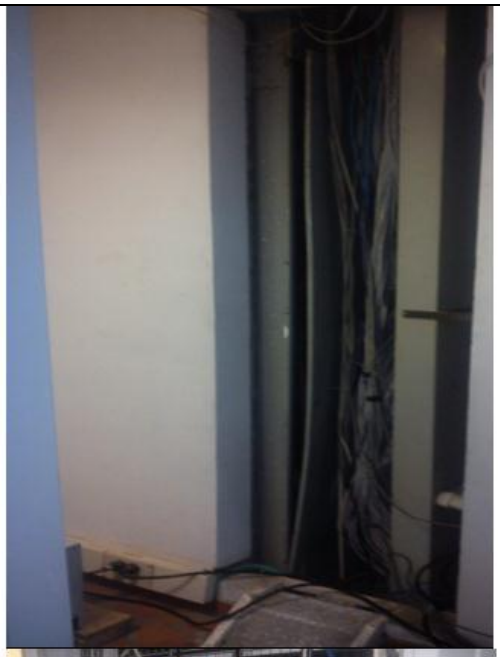
Existe una persona encargada de verificar el acceso del personal hacia este departamento y por consiguiente hacia los servidores (jefe del área tic´s).

					FIGURA 8. PERSONA ENCARGADA DEL DE ACCESO A DIVISIÓN DE TIC´S Y SERVIDORES  Fuente: El Autor
		11.1.3 Seguridad de oficinas, despachos y recursos.		X	Las oficinas son abiertas a todo el publico
		11.1.4 Protección contra las amenazas externas y ambientales.		X	Dentro de las instalaciones de la Unicomfacauca se logran identificar las siguientes amenazas: **Estado de la Seguridad:** Materiales inflamables y de alta combustión son almacenados en la sala de servidores y sala de Tic´s. **FIGURA 9. EVIDENCIAS DE MATERIAL INFLAMABLE DENTRO DE DEL ÁREA DE LAS TIC´S.**  Fuente: El Autor

					Cableado sin organizar, e instalaciones eléctricas sin tapas de protección, son grandes amenazas de producir un incendio por corto. **FIGURA 1. EVIDENCIAS DE UN POSIBLE INCENDIO POR CORTO CIRCUITO**  Fuente: El Autor UPS en el suelo sin ninguna protección. **FIGURA 11. EVIDENCIA DE UPS EN EL SUELO**  Fuente: El Autor No existen etiquetas de señalización que prohíban fumar dentro de estas locaciones. Muebles y ventana de madera dentro de Tic´s y servidores son grandes generadores de riesgos para un incendio. **FIGURA 12. EVIDENCIAS DE MUEBLES Y VENTANA EN MADERA**

					 Fuente: El Autor
		11.1.5 El trabajo en áreas seguras.		X	No existe
		11.1.6 Áreas de acceso público, carga y descarga.		X	Casi toda la oficina tiene acceso al publico
	11.2 Seguridad de los equipos.	11.2.1 Emplazamiento y protección de equipos.		X	Unicomfacauca no cuenta con controles para el acceso a la división de Tic´s en donde se hace necesario el uso de tarjetas inteligentes de control de puertas y cámaras para evitar el ingreso de personal no autorizado a las instalaciones. **FIGURA 13. ÁREA DE SERVIDORES**  Fuente: El Autor
		11.2.2 Instalaciones de suministro.	X		En la mayoría de los centros de datos, es necesario el uso grandes cantidades de electricidad para suministrar la potencia necesaria a todos los equipos informáticos que ahí se encuentran, debido a esto se hace necesario planificar, medir y mejorar la eficiencia de consumo eléctrico del centro de datos, para aprovechar de la mejor manera los recursos con los que se disponen. Unicomfacauca cuenta con una protección de respaldo

					de energía utilizando UPS de gran capacidad en el área (CORE división de TI) como se puede observar en la siguientes imágenes. **FIGURA 14. RESPALDO DE ENERGÍA**   Fuente: El Autor
		11.2.3 Seguridad del cableado.	X		En el área de sistemas se observa que los cables o Patch Cord se encuentran en el suelo y no cumplen con las normas (EIA/TIA 568 B), donde cualquier persona sin conocimiento de la ubicación de estos puede soltar, pisar o cortar algún cable generando la interrupción de algún servicio. La norma (EIA/TIA 568 B) consta de una serie de buenas prácticas donde recomienda del uso de las canaletas y la distancia de reserva de las mismas por si es necesario en algún futuro cambiarlos de sitio los equipos. Nota: se recomienda realizar un chequeo general de toda la red cableada para el definir el estado actual de la misma respecto a las normas anteriormente mencionadas, y realizar los cambios pertinentes en base a dichas normas según sea necesario. **FIGURA 15. EVIDENCIA DE VULNERABILIDAD POR CABLES**

					  Fuente: El Autor
		11.2.4 Mantenimiento de los equipos.	X		Actualmente la Universidad realiza dos tipos de mantenimiento, tanto software como hardware en los equipos. La parte de mantenimiento hardware se realiza mínimo cada seis meses, o en épocas de bajo tráfico en la red. Por otro lado la parte software no se tiene tiempo definido ya que los servidores son de distribución libre solo se hacen actualizaciones de los programas cada cierto tiempo y según las necesidades de la institución. En caso de presentarse un fallo o daño en un equipo, se procede a reemplazarlo inmediatamente para evitar la interrupción del servicio. Nota: se debe definir un tiempo determinado para hacer mantenimiento en los equipos, de ser posible buscar que todas los mantenimientos y actualizaciones de los

					servidores se programen en la misma fecha, en busca de llevar un registro de actualizaciones más controlado.
		11.2 .5 Salida de activos fuera de las dependencias de la empresa.		X	No existe
		11.2.6 Seguridad de los equipos y activos fuera de las instalaciones		X	No existe
		11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.	X		Solo se formatean a bajo nivel
		11.2.8 Equipo informático de usuario desatendido.	X		Solo se bloquea la sesión pasados unos minutos desatendido
		11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.	X		Depende de los empleados

7.2 DIAGNÓSTICO SOBRE EL ESTADO ACTUAL DE SEGURIDAD DE LA INFORMACIÓN EN LA RED DE DATOS DE LA INSTITUCIÓN UNIVERSITARIA TECNOLÓGICA DE COMFACAUCA A TRAVÉS DEL PANORAMA DE RIESGOS

A continuación se realizó una clasificación de los activos de la institución universitaria para obtener el resultado de los activos más importantes y utilizables teniendo como base en un estudio de recolección de información para el desarrollo del proyecto. Las tablas 2, 3, 4 ,5 categorizan los diferentes activos:

Tabla 2. Activos de Información

Activos De Información				
Datos Digitales	**Información Tangible**	**Información Intangible**	**Aplicaciones**	**Sistemas Operativos**
Bases de Datos - Mysql **Backup** - Nas **Correo Electrónico** Encriptación De Claves - SSL - SSH	**Personal** - División de Tecnología y Sistemas **Compartimiento de Seguridad** - Llaves De Oficina	- Información - Licencias - Buen Nombre De La Universidad	**Propietarias** - Siga **Adquiridas** **-** Sigo **Open Source** - Open Office - Zimbra - Osc Interventory **Aplicaciones De Escritorio** - Easy Calendar - Filezilla	- Fedora 26 - Debían 9.1.0 - Centos 7 - Ubuntu - Windows 7 - Windows 8

Fuente: El autor

Tabla 3. Activos Físicos TI

Activos Físicos Ti		
SOPORTE DE INFRAESTRUCTURA TI	**Controles De Entorno Ti**	**Hardware Ti**
- Cuarto de Telecomunicaciones - Rack - Oficinas	- Detector de incendios (censor de humo) - Alarmas y cámaras - Aire Acondicionado - Sistemas de UPS Servidores - Cableado Eléctrico Regulado	**Enrutadores** - Router Cisco Renata 1900 (Emtel) - 2 ROUTER Cisco Linksys E4200 **Switches** - 3 Switch's Power Connect 354/ 24 Puerto's Programables - Módulo De Fibra Óptica - Tranceiver De Fibra A Utp 10 A 100 Tplink

		- 5 Patch Panel De 48 Puertos - 5 Ordenadores - 1 Switch ZTE CX EV10 - Switch 2818S De Tarjeta De Fibra (Emtel) - Switch Dlink 10/100 De 24 Puertos - Switch De 48 Puertos Administrable DELL **Servidores** - Servidor Web (Ubuntu) - Servidores De Correo - Servidor Zimbra(Centos) - Osc Interventory (Centos) - Snies (Fedora 26) - Aplicaciones (Centos 7) - Proxy (Debian) - Directorio activo (Windows server) **Equipos Terminales** - Estaciones de trabajo - Portátiles **Impresoras** - HP F4180 **Teléfono** - **Cámara de video**

Fuente: El autor

Tabla 4. Activos de Servicios TI

Activos De Servicio De Ti		
Servicios De Red	**Servicios Web**	**Contratos De Soporte**
- Proxy - Dhcp - Ftp - Correo - Dns	- Apache - IIS	- Emtel S.A - ESET - Microsoft

Fuente: El autor

Tabla 5. Activos del Área informática

Activos de Información de Personal
Empleados División De Sistemas
- Jefe de sistemas - Pasante

Fuente: El autor

Dentro de la etapa de caracterización del sistema, luego de la identificación y clasificación de los activos por categorías se realiza la evaluación de estos. Este diagnóstico se hace teniendo inicialmente y como punto de partida los pirales de la seguridad informativa y para cada uno de ellos se definen diferentes niveles de cumplimiento como se consigna en la tabla 5. (MUY ALTO (5), ALTO (4), MEDIO (3), BAJO (2), MUY BAJO (1) el nivel más alto indicaría que se cumple a cabalidad con un determinado pilar de la seguridad informática.

Tabla 6. Puntuación para la Evaluación de Activos

Evaluación de Activos	
Muy Alto	5
Alto	4
Medio	3
Bajo	2
Muy Bajo	1

Fuente: El autor

Los Criterios para la valuación de activos observados en la tabla 7 son la confidencialidad, integridad, disponibilidad.

Tabla 7. Criterios para Evaluación de Activos

Criterios Para La Evaluación De Activos		
Confidencialidad	**Integridad**	**Disponibilidad**
- Los componentes del sistema TI serán accesibles sólo por aquellos usuarios autorizados.	- Los componentes del sistema TI sólo pueden ser creados y modificados por los usuarios autorizados.	- Los usuarios deben tener disponibles todos los componentes del sistema TI cuando así lo deseen.

Fuente: El autor

Considerando los criterios de la tabla 7, los niveles de puntuación y la categorización anteriormente creada de los activos se realiza la valuación plenamente, donde se obtiene un valor total que sirve para la escogencia de los activos más importantes dentro de la Empresa. En las tablas 8 al 18 se encuentra los valores asignados para cada uno de los activo. El criterio para la colocación de los valores se hizo teniendo en cuenta un primer estudio de afectación de la continuidad del negocio.

Tabla 8. Evaluación de Datos Digitales

Activos Datos Digitales				
Datos Digitales	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Valor De Activos**
Bases de datos	5	5	4	15
Backup	5	5	3	13

Encriptación de llaves	3	3	3	9
Correo electrónico	3	2	1	6

Fuente: El autor

Tabla 9. Evaluación de activos información tangible

Activos Información Tangible				
Información Tangible	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Valor De Activos**
División de tecnología y sistemas	5	3	4	12
Compartimiento de seguridad	5	4	4	13

Fuente: El autor

Tabla 10. Evaluación de Información Intangible

Activos de Información Intangible				
Información Intangible	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Valor De Activos**
Información	5	5	5	15
Licencias	2	1	2	5
Buen Nombre de la Universidad	1	2	3	6

Fuente: El autor

Tabla 11. Evaluación de Aplicaciones

Aplicaciones				
	Confidencialidad	**Integridad**	**Disponibilidad**	**Valor De Activos**
Propietarias				
SIGA	5	5	5	15
Adquiridas				
SIGO	5	5	5	15
Open Source				
Open Office	4	4	5	13
Zimbra	5	4	5	14
Osc Interventory	4	4	2	10
De escritorio				
Filezilla	4	3	2	9
Easy Calendar	3	2	2	7

Fuente: El autor

Tabla 12. Evaluación de Sistemas Operativos

Sistemas Operativos				
Servidores	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Valor De Activos**
Ubuntu (Servidor Web)	5	5	4	14

centos (Servidor base de datos)	5	5	5	15
Centos (Correo Zimbra y aplicaciones)	5	5	4	14
Debian (Osc Inventori y proxy)	5	5	4	14
Fedora 26 (Snies)	5	5	5	14
Windows server 2012	4	4	3	11
Windows 7 (Sigo)	4	3	2	9

Fuente: El autor

Tabla 13. Evaluación de Soporte de Infraestructura

Activos Físicos Ti				
	Confidencialidad	**Integridad**	**Disponibilidad**	**Valor De Activos**
Cuarto de Telecomunicaciones	5	5	5	15
Racks	4	3	3	10
Oficinas	3	2	3	8

Fuente: El autor

Tabla 14. Evaluación de Controles Entorno TI

Controles Entorno Ti				
	Confidencialidad	**Integridad**	**Disponibilidad**	**Valor De Activos**
Detector de incendios (censor de humo)	3	2	5	10
Alarmas y cámaras	3	3	5	11
Aire Acondicionado	3	3	4	10
Sistemas de UPS Servidores	4	5	5	14
Cableado Eléctrico Regulado	3	2	5	10

Fuente: El autor

Tabla 15. Evaluación de Hardware TI

Hardware TI				
	Confidencialidad	**Integridad**	**Disponibilidad**	**Valor de Activos**
Servidor web	5	5	4	14
Servidor base de datos	5	5	5	15
Servidor de aplicaciones	5	5	5	15
Servidor correo	5	5	3	13
Servidor ftp	5	5	5	15
Servidor directorio activo	4	4	4	12
Portátiles	3	3	3	9
Estación de trabajo	2	3	3	8
Router proveedor	5	5	3	13
Router´s	5	5	5	15

Switch´s	3	3	3	9
Impresora	1	2	2	5
Teléfono	3	2	1	6
Cámara de video	1	1	1	3

Fuente: El autor

Tabla 16. Evaluación de Activos de Servicio TI

Activos de Servicio TI				
Servicios de Red	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Valor De Activos**
Proxy	5	5	2	12
DHCP	4	4	2	10
FTP	5	5	5	15
CORREO	5	5	3	13
DNS	5	4	3	12

Fuente: El autor

Tabla 17. Evaluación de Servicios Web

Servicios Web				
Servicios Web	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Valor De Activos**
Apache 2.4.27	5	5	4	14
IIS	5	3	2	10

Fuente: El autor

Tabla 18. Evaluación de Contratos de Soporte

Contratos de Soporte				
Contrato de Soporte	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Valor De Activos**
EMTEL S.A	4	4	4	12
ESET	4	4	4	12
MICROSOFT	4	4	3	12

Fuente: El autor

Los activos importantes de acuerdo a la Puntuación dada anteriormente fueron aquellos que obtuvieron un valor entre 15 y 14, siendo este resultado la suma CID (Confidencialidad, Integridad, Disponibilidad) por cada activo. Después de realizar la evaluación se determina que los siguientes activos son de mayor importancia dentro de la empresa como se establece en la tabla 19 y 20.

Tabla 19. Activos de Información

Activos de Información				
Datos Digitales	**Información intangible**	**Información tangible**	**Aplicaciones**	**Sistemas Operativos**
Bases de Datos	Información	**Personal** **-**División de Tecnología	**Propietarias** - Siga **Adquiridas**	- Ubuntu (servidor web) - Centos (servidor

		y Sistemas	- Sigo	base de datos , correo)
Backups		**Compartimiento de Seguridad** -Llaves de Oficina	**Open Source** - Zimbra	- Debian (proxy) - fedora

Fuente: El autor

Tabla 20. Activos Físicos TI

Activos Físicos Ti		
Soporte de Infraestructura Ti	**Controles de Entorno Ti**	**Hardware Ti**
- Cuarto de Telecomunicaciones	- Sistemas de UPS Servidores	- Router´s cisco - Servidor Web - Servidor base de datos - Servidor Aplicaciones - Servidor Ftp

Fuente: El autor

Evaluación de Amenazas

Una vez identificados los activos más importantes, se procede a considerar los criterios de las posibles causas potenciales de un incidente no relacionado que pueden ocasionar alguna falla dentro de la Institución Universitaria. En la tabla 21 se realizó una categorización de las posibles causas o amenazas.

Tabla 21. Criterios para La Evaluación de las Amenazas

Criterios para la Valuación de las Amenazas		
Amenazas Naturales	**Amenazas Humanas**	**Amenazas Del Entorno**
- Terremoto - Tormentas Eléctricas - Vendavales - Inundaciones	- Acceso no autorizado a sistemas - Explotación de errores (usuario y administrador) - Ingeniería Social - Phishing - Interceptación de datos - Código malicioso - Abuso de la informática. - Virus	- Fallas eléctricas - Polución - Sustancias químicas - Temperatura - Incendios - Control de humedad - Edificaciones Cercanas - Accidente de tránsito. - Protección de los Equipos en el sitio - Fuentes de Potencia - Seguridad de cableados - Mantenimiento de Equipos - Ingreso no autorizado - Aseguramiento de oficinas, recintos Y espacios físicos. - Fallas de equipos

Fuente: El autor

Posteriormente y una vez categorizadas las amenazas, se procede a definir niveles para encontrar los activos más vulnerables y amenazados, lo que significa que a mayor puntuación, el activo puede estar más afectado por una amenaza. La tabla 22 define la puntuación para la evaluación de activos con relación a las amenazas.

Tabla 22. Puntuación para la Valuación de Amenazas

Puntación para la Evaluación de Activos	
Muy Alto	5
Alto	4
Medio	3
Bajo	2
MUY BAJO	1

Fuente: El autor

La utilización de niveles de evaluación permite identificar y ponderar cuantitativamente los activos con la finalidad de encontrar aquellos que pueden ser afectados en mayor medida por las diferentes amenazas presentes en la Institución Universitaria Tecnológica de Comfacauca. En las tablas de la 23 a la 33 se obtiene un valor de amenaza, dependiendo de las amenazas según su categoría (Natural, Humana y de Entorno) con relación a un activo.

Tabla 23. Evaluación de Amenazas de Datos Digitales

Amenazas de los Activos				
Activos de Información				
Datos Digitales				
	Amenaza Natural	Amenaza Humana	Amenaza Del Entorno	Valor De La Amenaza
Base de datos	1	5	2	8
Backup	1	3	4	8
Correo Electrónico	1	3	1	5
Encriptación de llaves	1	2	1	4

Fuente: El autor

Tabla 24. Evaluación de Amenazas de Información tangible

Información Tangible				
	Amenaza Natural	Amenaza Humana	Amenaza Del Entorno	Valor de la Amenaza
División de tecnología y sistemas	1	3	1	5
Compartimiento de seguridad	1	3	1	5

Fuente: El autor

Tabla 25. Evaluación de Amenazas de Información Intangible

Información Intangible				
	Amenaza Natural	Amenaza Humana	Amenaza Del Entorno	Valor de la Amenaza
Información	1	4	1	6
Licencias	1	2	1	4
Buen Nombre de la	1	2	1	4

Universidad				

Fuente: El autor

Tabla 26. Evaluación de Aplicaciones

Aplicaciones				
	Amenaza Natural	Amenaza Humana	Amenaza Del Entorno	Valor De La Amenaza
Propietarias				
SIGA	1	4	1	6
Adquiridas				
SIGO	1	4	1	6
Open Source				
Open Office	1	3	2	6
Zimbra	1	3	2	6
Osc Interventory	1	3	2	6
De escritorio				
Filezilla	1	2	1	4
Easy Calendar	1	2	1	4

Fuente: El autor

Tabla 27. Evaluación de Sistemas Operativos

Sistemas Operativos				
Servidores	Amenaza Natural	Amenaza Humana	Amenaza Del Entorno	Valor de la Amenaza
Servidor Web (Ubuntu)	1	4	2	7
Servidor base de datos (centos)	1	4	2	7
Centos (Correo Zimbra y aplicaciones)	1	4	2	7
Debian (Osc Inventori y proxy)	1	4	2	7
Fedora 26 (Snies)	1	4	2	7
Windows server 2012	1	3	2	6
Windows 7 (Sigo)	1	3	2	6

Fuente: El autor

Tabla 28. Evaluación de Soporte de Infraestructura

Activos Físicos Ti				
	Amenaza Natural	Amenaza Humana	Amenaza del Entorno	Valor de la Amenaza
Cuarto de Telecomunicaciones	1	3	2	6
Racks	1	3	2	6
Oficinas	1	3	2	6

Fuente: El autor

Tabla 29. Evaluación de Controles Entorno TI

Controles Entorno Ti				
	Amenaza Natural	Amenaza Humana	Amenaza del Entorno	Valor de la Amenaza
Detector de incendios (censor de humo)	1	2	1	4

Alarmas y cámaras	1	2	1	4
Aire Acondicionado	1	2	1	4
Sistemas de UPS Servidores	1	2	2	5
Cableado Eléctrico Regulado	1	2	2	5
Cableado de red	1	2	3	6

Fuente: El autor

Tabla 30. Evaluación de Hardware TI

Hardware Ti				
	Amenaza Natural	Amenaza Humana	Amenaza del Entorno	Valor de la Amenaza
Servidor web	1	3	2	6
Servidor base de datos	1	3	2	6
Servidor de aplicaciones	1	3	2	6
Servidor correo	1	3	2	6
Servidor ftp	1	3	2	6
Servidor directorio activo	1	3	2	6
Portátiles	1	3	2	6
Estación de trabajo	1	3	2	6
Router proveedor	1	1	2	4
Router´s	1	3	2	6
Switch´s	1	1	2	4
Impresora	1	3	2	6
Teléfono	1	2	1	4
Cámara de video	1	1	1	3

Fuente: El autor

Tabla 31. Evaluación de Activos de Servicio TI

Activos De Servicio Ti				
Servicios de Red	Amenaza Natural	Amenaza Humana	Amenaza del Entorno	Valor de la Amenaza
Proxy	1	3	2	6
DHCP	1	3	2	6
FTP	1	3	2	6
CORREO	1	3	2	6
DNS	1	3	2	6

Fuente: El autor

Tabla 32. Evaluación de Servicios Web

Servicios Web				
Servicios Web	**Amenaza Natural**	**Amenaza Humana**	**Amenaza del Entorno**	**Valor de la Amenaza**
Apache 2.4.27	1	5	2	8
IIS	1	3	2	6

Fuente: El autor

Tabla 33. Evaluación de Contratos de Soporte

Contratos De Soporte				
Contrato De Soporte	**Amenaza Natural**	**Amenaza Humana**	**Amenaza del Entorno**	**Valor de la Amenaza**

EMTEL S.A	2	4	2	10
ESET	1	1	1	3
MICROSOFT	1	1	1	3

Fuente: El autor

Una vez realizada la evaluación de amenazas se procede a identificar los activos que se encuentran amenazados actualmente en la institución universitaria.

Activos más Amenazados según la puntación de evaluación

En la tabla 34 se evidencian las amenazas de acuerdo a un estudio previo realizado en la Empresa sobre los activos dependiendo del tipo de Amenaza.

Tabla 34. Descripción de los Activos Amenazados

Activos más Amenazados según la Puntuación de Evaluación		
Activos	Tipo de Amenazas	Amenaza
Base de Datos	Amenaza humana	- Acceso no autorizado (Ingeniería Social y Phishing). - Errores del programador por falta de capacitación en el área.
Backup	Amenaza del entorno	- ingreso físico no autorizado por terceras personas - No se encuentran en un sitio confiable - No existen copias externas custodiadas
Información	Amenaza Humana	- Información impresa no está segura y controlada - Acceso físico no Autorizado por terceras personas
Aplicaciones propietarias y adquiridas	Amenaza humana	- Acceso no autorizado (Ingeniería Social y Phishing)
Sistemas operativos Linux	Amenaza humana	- Errores de seguridad, por mala administración.
Cuarto de telecomunicaciones	Amenaza Entorno	- Control de humedad - Polución
Oficinas	Amenaza humana	- Acceso no autorizado físico
Cableado de red	Amenaza de entorno	- Falta de cumplimiento de la normatividad de cableado estructurado
Estaciones de trabajo	Amenaza humana	- Ingeniería Social
Rack	Amenaza Entorno	- Falta de cumplimiento de la normatividad de cableado estructurado
Servidor Apache	Amenaza humana	- Spoofing Web - Errores de seguridad

Fuente: El autor

Probabilidades de amenazas de la Institución Universitaria

Las probabilidades de las amenazas determinan si un ataque es inminente, es decir, que podría causar perjuicio en la disponibilidad, confidencialidad, integridad y autenticidad de la información institucional.

Los criterios para la probabilidad de amenaza se definen en la tabla 35, clasificados en 4 niveles ALTA, MEDIA, BAJA, MUY BAJA.

Tabla 35. Criterios para probabilidad de Amenaza

Alta	La realización del ataque es inminente. No existen condiciones internas y externas que impidan el desarrollo del ataque.
Media	Existen condiciones que hacen poco probable un ataque en el corto plazo pero que no son suficientes para evitarlo en el largo plazo.
Baja	Existen condiciones que hacen muy lejana la posibilidad del ataque.
Muy Baja	No existen condiciones que impliquen riesgo/ataque.

Fuente: El autor

Los criterios de la probabilidad de amenazas anteriormente descritos permitirán la recolección de información y así poder identificar el nivel de probabilidad de una amenaza en la Institución Universitaria.

A continuación en las siguientes tablas 36 y 37, se utilizan las divisiones de la columna Probabilidad de Amenaza, marcando con una "X" la opción que se consideró aplicable a la Institución Universitaria dependiendo de los tipos de amenazas identificadas con su respectivo análisis.

Tabla 36. Probabilidad de Amenazas Humanas

Tipo de Amenaza	**Probabilidad de Amenaza**			
Amenaza Humana	**Alta**	**Media**	**Baja**	**Muy Baja**
acceso no autorizado por ingeniería social y Phishing (base de datos)	X			
errores del programador por falta de capacitación en el área (base de datos)	X			
información impresa no está segura y controlada (información)		X		
acceso físico no autorizado por terceras personas (información)		X		
acceso no autorizado por ingeniería social y Phishing (aplicaciones propietarias y adquiridas, open source)	X			
errores de seguridad por mala administración (s.o Linux)	X			
ingeniería social (estaciones de trabajo)	X			
spoofing web (servidor apache)	X			
errores de seguridad (servidor apache)	X			
acceso no autorizado físico (oficinas)	X			

Fuente: El autor

Tabla 37. Probabilidad de Amenazas de Entornos

Amenaza De Entorno	Alta	Media	Baja	Muy Baja
Ingreso físico no autorizado por terceras personas **(BACKUP)**		X		
No se encuentran en un sitio confiable **(BACKUP)**	X			
No existe copias externas custodiadas **(BACKUP)**	X			
control de humedad **(cuarto de telecomunicaciones)**	X			
polución **(cuarto de telecomunicaciones)**		X		
falta de cumplimiento de la normatividad de cableado estructurado **(rack principal)**	X			
falta de cumplimiento de la normatividad de cableado estructurado **(cableado de red)**	X			

Fuente: El autor

Identificación de Vulnerabilidades

Las debilidades pueden ocasionar que una amenaza cause daños a un activo y se afecte el normal funcionamiento de los procesos que se llevan a cabo en la Institución Universitaria por este motivo se procedió a la identificación de las vulnerabilidades, para ello se consideraron tres áreas que determina la metodología SP 800-30:

- Administración
- Operacional
- Técnica

En las tablas de la 38 a la 40 se describen las vulnerabilidades asociadas en las áreas de administración, operacional y técnica con relación a una serie de criterios establecidos por la metodología SP800-30. Además para cada uno de los activos más críticos (servidores) se identifican las vulnerabilidades como se indica en las tablas 41 a la 43.

Tabla 38. Vulnerabilidades del Área de Administración de sistemas

Criterios de la Área de Administración de Sistemas	
Criterios	**Vulnerabilidades Asociadas**
Asignación de responsabilidades	La asignación de responsables de los activos del área de sistemas no está muy bien definida.
Revisión periódica de controles de seguridad.	La existencia de controles de seguridad que protejan los activos es muy baja
Continuidad	No se maneja una política clara y específica para la continuidad del negocio. Actividades relacionadas con los controles de cambios en las aplicaciones críticas es susceptible a mejoras.
Evaluación de Riesgos	Algunos riesgos sobre los activos más críticos de la Institución Universitaria no están plenamente identificados y documentados.
Seguridad y capacitación técnica	No se posee un documento donde se estipulen los incidentes y las mejoras en seguridad.
	No se manejan roles para la gestión de vulnerabilidades

Plan de seguridad del sistema	Claramente no se tiene definido un plan de seguridad del sistema, aunque se realizan algunas actividades en lo relacionado a seguridad. El manejo de aplicaciones está más enfocado a lo funcional y no se tienen controles adecuados de seguridad.
Sistemas de autorización y re-autorización	El manejo de claves secretas por parte de los usuarios se realiza de manera informal. Falta de procedimiento formal para la revisión de los accesos a los sistemas para mirar usuarios y permisos asignados.

Fuente: El autor

Tabla 39. Vulnerabilidades del Área Seguridad Operacional

Seguridad Operacional	
Criterios	**Vulnerabilidades Asociadas**
Medios de acceso y eliminación de dato	Proceso formal de eliminación de datos no se tiene.
Facilidad de protección (Sala de computadores, Data center, oficinas)	Las actividades relacionadas con la seguridad física son susceptible de mejora para el control de acceso a la dependencia, cuarto de equipos y manejo de activos presentes en esta.
Control de humedad	No se maneja un mecanismo de control de humedad

Fuente: El autor

Tabla 40. Vulnerabilidades del área Técnica

Criterios en el Área de Seguridad Técnica	
Criterios	**Vulnerabilidades asociadas**
Comunicaciones (Interconexión se sistemas, Enrutadores).	No se puede determinar adecuadamente las rutas y espacios horizontales utilizados.
	Falta etiquetado de cableado horizontal.
	Falta de etiquetas adecuados de equipos activos y servidores.
	Existencia de derivaciones en cableado horizontal.
	No se tiene una plano adecuado para mirar distancias de puntos de red
	No existen barras de puesta a tierra dentro del cuarto de comunicaciones y en rack.
	El medio de trasporte de cable se encuentra deteriorado
	Equipos activos dentro de cuarto de comunicaciones no están aterrizados.
	El manejo de métodos criptogramas dentro de la organización es susceptible a mejoras.
Criptografía Control de acceso discrecional	En algunos servidores Linux no se maneja archivos para el control de longitud contraseñas, tiempos de expiración y cambios de estas.
	La falta documentación formal para la gestión de identificadores de usuarios únicos (ID´s).
Sistema de auditoria	Muchos de los servidores tienen instalados servicios innecesarios
	No se maneja un endurecimiento de servidores apropiado en los servidores (Hardening).
	Se permite conexión por ssh a root directamente.
	Documentos formales para registro de ingreso de personas al área no se tiene.
Identificación y autenticación	La gestión de Logs para control de accesos no está muy bien automatizada.

	No se manejan controles de autenticación para el ingreso al sitio de procesamiento de información (tarjetas de control con códigos etc.).
	Para el ingreso al área de sistemas no se exige portar documento de identificación en un lugar visible a personal ajeno a esta.

Fuente: El autor

Tabla 41. Vulnerabilidades del servidor de Directorio Activo

Criterios en el Área de Servidor de Aplicaciones	
Servidor de Aplicaciones	**Vulnerabilidades**
	Se permite autenticación al servidor como root por medio de ssh
	No hay un plan de contingencia establecido a nivel de Hw para este servidor.
	No se tienen herramientas de monitoreo de Logs automatizadas para este servidor.
	Explícitamente de se tiene asignado una persona responsable de este servidor.
	Es susceptible de mejora tener una política definida de control de cambios.
	No se tiene un documento de registro de incidentes y de soluciones de estos.
	No se tiene plenamente identificado cables de red ni el cableado eléctrico para el servidor.

Fuente: El autor

Tabla 42. Vulnerabilidades del servidor Web

Criterios del Servidor Web	
Servidor Web	Vulnerabilidades
	El Hardening utilizado en el servidor es susceptible de mejoras
	Backup para este servidor no se maneja
	Se tiene instalado software innecesario en este servidor.
	No se tiene plenamente identificado los cables, puntos red y el cableado eléctrico para el servidor.

Fuente: El autor

Tabla 43. Vulnerabilidades de Servidor de Base de Datos

Criterios del Servidor de Base de Datos (Mysql)	
Servidor Mysql	**Vulnerabilidades asociadas**
	El manejo de cambio de contraseñas por defecto durante la instalación es susceptible a mejoras
	La aplicación de Mysql es susceptible a mejoras en lo que se refiere a proceso de autenticación remota.
	No se posee explicita mente una documento formal de consignación de errores y fallas
	No se tiene dentro del servidor programas de chequeo de integridad para gestión de archivos del S.O
	No se maneja adecuadamente la gestión de contraseñas en el relacionado al tiempo para cambio de estas.
	El manejo de banners para el S.O del servidor es susceptible de mejoras

	Las diferentes conexiones de red y eléctricas que tiene el servidor no están plenamente etiquetadas.

Fuente: El autor

Probabilidad de Vulnerabilidades

Dentro de la Institución Universitaria existen una serie de vulnerabilidades que pueden ser exploradas por las amenazas por lo tanto se hace necesario definir criterios que permitan determinar el nivel de probabilidad de las vulnerabilidades.

Tabla 44. Nivel de Probabilidad de Vulnerabilidades

Nivel de Probabilidad	Definición de Probabilidad
Alta	La amenaza es altamente motivado y suficientemente capaz, y los controles para evitar la vulnerabilidad de ser ejercidas son ineficaces
Media	La amenaza es motivado y capaz, pero los controles están en el lugar que pueden impedir el ejercicio exitoso de la vulnerabilidad.
Baja	La amenaza carece de motivación o capacidad, o los controles existen para prevenir, o al menos obstaculicen de manera significativa la vulnerabilidad de ser ejercida.

Fuente: El autor

En la tabla 45 se asocian las amenazas y su probabilidad de acuerdo a los tres niveles anteriores para la Institución Universitaria.

Tabla 45. Probabilidad de amenazas Generales

Vulnerabilidad	Alta	Media	Baja
La asignación de responsables de los activos del área de sistemas no está definida.		X	
La existencia de controles de seguridad que protejan los activos es escasa.		X	
No se maneja una política clara y específica para la continuidad del negocio.	X		
Actividades relacionadas con los controles de cambios en las aplicaciones críticas es susceptible a mejoras.		X	
Algunos riesgos sobre los activos más críticos de la Institución Universitaria no están plenamente identificados y documentados.	X	X	
No se posee un documento donde se estipulen los incidentes y las mejoras en seguridad.	X		
No se manejan roles para la gestión de vulnerabilidades		X	
No hay exigencia continua de identificación en lugar visible para personas que ingresan al área.		X	
Claramente no se tiene definido un plan de seguridad del sistema, se realizan algunas actividades en lo relacionado a seguridad		X	
EL manejo de aplicaciones está más enfocado a lo funcional y no se tienen controles adecuados de seguridad.	X		
No se maneja una política clara de registro y des-registro de los usuarios en sistema		X	

Explícitamente no se posee documentación en cuanto a criterios de confidencialidad y criticidad de las aplicaciones	X		
EL manejo de claves secretas por parte de los usuarios se realiza de manera informal.		X	
Falta de procedimiento formal para la revisión de los accesos a los sistemas para mirar usuarios y permisos asignados.	X		
Falta maquillado de tableros e identificación de circuitos que alimentan las ups		X	
Proceso formal de eliminación de datos no se tiene. La eliminación de datos digitales no se realiza con herramientas adecuadas		X	
Los medios de acceso al cuarto de comunicaciones es susceptible a mejoras)		X	
Las paredes del cuarto de equipos falta un adecuando tratamiento.			X
Las actividades relacionadas con la seguridad física son susceptible de mejora para el control de acceso a la dependencia, cuarto de equipos y manejo de activos presentes.		X	
No se maneja un mecanismo de control de humedad		X	
No se puede determinar adecuadamente las rutas y espacios horizontales utilizados en el cableado de red.		X	
Falta etiquetado de cableado horizontal.	X		
Falta de etiquetas adecuados de equipos activos y servidores.		X	
Existencia de derivaciones en cableado horizontal.		X	
Cableado de red y eléctrico junto en algunos sitios.		X	
Equipos activos dentro de cuarto de comunicaciones no están aterrizados.	X		
La distribución dentro de rack no es la adecuada.		X	
El manejo de métodos criptogramas dentro de la organización es susceptible a mejoras.		X	
El algunos servidores Linux no se maneja archivos para manejo de longitud de contraseñas, tiempos de espiración de contraseñas y cambios de contraseñas.		X	
Las gestión de ID's únicos falta documentación.		X	
No se maneja un Hardening apropiado en los servidores.	X		
Se permite conexión por ssh a root directamente.		X	
Documentos formales para registro de ingreso de personas al área no se tiene.	X		
La gestión de Logs para gestión de accesos está muy bien automatizada.		X	
Herramientas de monitoreo para gestión de equipos conectados a determinado servicio no se tiene implementado.	X		
No se manejan controles de autenticación para en sitio de procesamiento de información (tarjetas de control con códigos etc.)			X
Para el ingreso al área de sistemas no se exige portar documento en un lugar visible para el personal que ingresa ajeno al área.		X	
Un diagrama lógico de conexión de equipos no se tiene			X

Fuente: El autor

Anteriormente se menciona que los servidores y su información son los activos más críticos e importantes de la institución universitaria motivo por el cual se hace necesaria una clasificación por niveles de la probabilidad de las vulnerabilidades.

Clasificación de la probabilidad de las vulnerabilidades para servidores

En las siguientes tablas, de la 46 hasta la 48 se determinará las diferentes vulnerabilidades encontradas en los diferentes servidores.

Tabla 46. Probabilidad de Vulnerabilidades del Servidor de Directorio Activo

Servidor de Aplicaciones			
Vulnerabilidad	**Alta**	**Media**	**Baja**
Hardening en para el sistema operativo que manejo este servidor es susceptible mejoras.	X		
Se permite autenticación al servidor como root por medio de ssh		X	
El plan de contingencia establecido para este servidor es susceptible de mejoras.	X		
No se tienen herramientas de monitoreo de Logs automatizadas para este servidor.	X		
Explícitamente se tiene asignado una persona responsable de este servidor.	X		
Es susceptible de mejora tener una política definida de control de cambios.	X		
El php instalado el servidor esta propenso a muchos ataques			X
No se tiene un documento de incidentes y ni de soluciones		X	
No se tiene plenamente identificado cables de red ni el cableado eléctrico para el servidor		X	
No se maneja software de chequeo de integridad	X		
Herramienta de monitorio para este servidor no se tiene			X

Fuente: El autor

Tabla 47. Probabilidad de Vulnerabilidades del Servidor Web

Servidor Web			
Vulnerabilidad	**Alta**	**Media**	**Baja**
El Hardening utilizado en el servidor es susceptible de mejoras		X	
El servicio de samba esta propenso a ataques.			X
No se posee un adecuado control de cambios para este servidor.	X		
No se tiene plenamente identificado los cables, los puntos red ni el cableado eléctrico para el servidor.	X		

Fuente: El autor

Tabla 48. Probabilidad de vulnerabilidades del servidor de bases de datos MYSQL

Servidor de Base de Datos (Mysql)			
Vulnerabilidad	**Alta**	**Media**	**Baja**
El manejo de cambio de contraseñas por defecto durante la instalación es susceptible a mejoras		X	
La base de datos esta propensa a ganancia de privilegios por accesibilidad de diccionario.		X	
La información de los parámetros para conexión remota es susceptible a mejoras.		X	
La aplicación de Mysql es susceptible a mejoras en lo que se refiere a proceso de autenticación remota.	X		
No se posee explicita mente una documento formal de consignación de	X		

errores y fallas			
No se tiene dentro del servidor programas de chequeo de integridad para gestión de archivos del S.O	X		
No se maneja adecuadamente la gestión de las contraseñas en el relacionado al tiempo para cambio de estas.	X		
El hardenig en el servidor es susceptible de mejoras.	X		
Las diferentes conexiones de red y eléctricas que tiene el servidor no están plenamente maquilladas	X		
Política de control de cambios no se tiene plenamente definida.	X		

Fuente: El autor

Análisis de Impacto

En el análisis de riesgos para la determinación de los impactos negativos derivados de la materialización de una amenaza es necesario medir las consecuencias que afectan la integridad, confidencialidad y disponibilidad. Los criterios tomados para el análisis de impacto se encuentran a continuación:

- Se pierde la información/conocimiento
- Terceros podrían tener acceso a la información/conocimiento
- La información ha sido manipulada o está incompleta
- La información/conocimiento o persona no está disponible.

En este análisis de impactos se considera en la siguiente escala descrita en la siguiente tabla:

Tabla 49. Escala de Impactos

MUY BAJO	No causa ningún tipo de impacto o daño a la organización.
BAJO	Causa daño aislado, que no perjudica a ningún componente de la organización.
MEDIO	Provoca la desarticulación de un componente de la organización. Si no se atiende a tiempo, a largo plazo puede provocar la desarticulación de la organización.
ALTO	En el corto plazo desmoviliza o desarticula a la organización.

Fuente: El autor

Para esta clasificación se tuvo en cuenta los principios de la seguridad informática y la magnitud de daño que sufre los activos, que corresponden a la realidad de la Institución Universitaria, como consecuencia de un impacto causado por un ataque exitoso como se observa en la siguiente tabla.

Tabla 50. Impacto a partir de los principios de Seguridad Informática en los Activos

Activos Amenazados	**Principios de la Seguridad Informática**			**Impacto**			
	Confidencialidad	Integridad	Disponibilidad	Alto	Medio	Bajo	Muy Bajo
Base de Datos	X	X	X	X			
Backup	X	X	X		X		
Información	X	X	X	X			

Aplicaciones propietarias y adquiridas	X	X	X	X			
Aplicaciones de Código Abierto	X	X	X			X	
Sistemas operativos Linux	X	X	X		X		
Cuarto de telecomunicaciones	X	X	X		X		
Oficinas			X			X	
Cableado de red			X		X		
Estaciones de trabajo					X		
Rack			X			X	
Servidor Apache	X	X	X		X		

Fuente: El autor

Análisis de riesgos

El riesgo es el efecto negativo cuando se produce un impacto sobre un activo, teniendo en cuenta tanto la probabilidad de la amenaza y el impacto de esta. Una efectiva administración de riesgos se necesita para evaluar y mitigar los riesgos identificados en la Institución Universitaria.
Dentro de este ámbito la probabilidad de amenaza e impacto de las amenazas, están considerados por medio de los siguientes niveles o escalas:

1 = Muy baja

2 = Baja

3 = Mediana

4 = Alta

Para calcular los riegos de amenaza del producto se realiza una multiplicación de la probabilidad de amenaza por el Impacto de la amenaza está agrupado en tres rangos, y para su mejor visualización se aplican diferentes colores.

Tabla 51. Tabla de conversión

Nivel Amenaza	Rango	Color
Bajo Riesgo	6 – 9	(Azul)
Medio Riesgo	10-12	(Naranja)
Alto Riesgo	13– 16	(Rojo

Fuente: El autor

En la siguiente tabla se especifican el impacto y la probabilidad de amenaza con relación a los activos más amenazados de Unicomfacauca.

Tabla 52. Análisis de riesgos

ANÁLISIS DE RIESGOS																		
IMPACTO		**PROBABILIDAD DE AMENAZA (alto=4, medio=3, bajo=2, muy bajo=1)**																
		HUMANA										**ENTORNO**						
	escala para impacto (alto=4, medio=3, bajo=2, muy bajo=1)	acceso no autorizado por ingeniería social y Phishing (base de datos)	errores del programador por falta de capacitación en el área (base de datos)	información impresa no está segura y controlada (información)	acceso físico no autorizado por terceras personas (información)	acceso no autorizado por ingeniería social y Phishing (aplicaciones propietarias y adquiridas, código abierto)	errores de seguridad por mala administración (s.o Linux)	ingeniería social (estaciones de trabajo)	spoofing web (servidor apache)	errores de seguridad (servidor apache)	acceso no autorizado físico (oficinas)	ingreso físico no autorizado por terceras personas (backup)	no se encuentran en un sitio confiable (servidores)	No existen copias externas custodiadas (BACKUP)	control de humedad (cuarto de telecomunicaciones)	polución (cuarto de telecomunicaciones)	falta de cumplimiento de la normatividad de cableado estructurado (rack principal)	falta de cumplimiento de la normatividad de cableado estructurado (cableado de red)
		4	**4**	**3**	**3**	**4**	**4**	**4**	**4**	**4**	**4**	**3**	**4**	**4**	**4**	**3**	**4**	**4**
Base de Datos	**4**	**16**	**16**	**12**	**12**	**16**	**16**	**16**	**16**	**16**	**16**	**12**	**16**	**16**	**16**	**12**	**16**	**16**
Backup	**2**	**8**	**8**	**6**	**6**	**8**	**8**	**8**	**8**	**8**	**8**	**6**	**8**	**8**	**8**	**6**	**8**	**8**
Información	**4**	**16**	**16**	**12**	**12**	**16**	**16**	**16**	**16**	**16**	**16**	**12**	**16**	**16**	**16**	**12**	**16**	**16**
Aplicaciones propietarias y adquiridas	**4**	**16**	**16**	**12**	**12**	**16**	**16**	**16**	**16**	**16**	**16**	**12**	**16**	**16**	**16**	**12**	**16**	**16**
Aplicaciones de Código Abierto	**2**	**8**	**8**	**6**	**6**	**8**	**8**	**8**	**8**	**8**	**8**	**6**	**8**	**8**	**8**	**6**	**8**	**8**
Sistemas operativos Linux	**4**	**16**	**16**	**12**	**12**	**16**	**16**	**16**	**16**	**16**	**16**	**12**	**16**	**16**	**16**	**12**	**16**	**16**
Cuarto de telecomunicaciones	**4**	**16**	**16**	**12**	**12**	**16**	**16**	**16**	**16**	**16**	**16**	**12**	**16**	**16**	**16**	**12**	**16**	**16**
Oficinas	**2**	**8**	**8**	**6**	**6**	**8**	**8**	**8**	**8**	**8**	**8**	**6**	**8**	**8**	**8**	**6**	**8**	**8**
Cableado de red	**4**	**16**	**16**	**12**	**12**	**16**	**16**	**16**	**16**	**16**	**16**	**12**	**16**	**16**	**16**	**12**	**16**	**16**
Estaciones de trabajo	**4**	**16**	**16**	**12**	**12**	**16**	**16**	**16**	**16**	**16**	**16**	**12**	**16**	**16**	**16**	**12**	**16**	**16**
Rack	**3**	**12**	**12**	**9**	**9**	**12**	**12**	**12**	**12**	**12**	**12**	**9**	**12**	**12**	**12**	**9**	**12**	**12**
Servidor Apache	**4**	**16**	**16**	**12**	**12**	**16**	**16**	**16**	**16**	**16**	**16**	**12**	**16**	**16**	**16**	**12**	**16**	**16**

Fuente: El autor

7.2.1 Tratamiento de los riesgos encontrados en la Institución Universitaria Tecnológica Unicomfacauca Popayán

Teniendo en cuenta el anexo A (que se encuentra al final del presente documento) y la matriz de riegos elaborada con la metodología NIST SP 800-30, se pudo establecer los riesgos y vulnerabilidades encontradas en el departamento de las TIC´s de La Institución Universitaria Tecnológica Unicomfacauca Popayán y de la misma manera, se procede a determinar los controles y acciones para mitigar la situaciones encontradas.

Tabla 53. Determinación de Controles

Activo	Causas	Consecuencia	Riesgo	Acciones A Tomar	Responsable
base de datos	acceso no autorizado por ingeniería social y Phishing	perdida , modificación de la información	alto	El personal del área de las TIC´s no debe informar, dar o decir ningún acontecimiento o información de esta área ya que con esto se está vulnerando la seguridad de la información, se debe capacitar al personal de la organización sobre la importancia de la seguridad informática en una organización.	Área de las tic´s
	errores del programador por falta de capacitación en el área	perdida, modificación o alteración de información que es vital para la organización	alto	Se deben implementar controles de detección, prevención y recuperación para proteger contra códigos maliciosos, así como procedimientos apropiados de concientización de los usuarios.	Área de las tic´s

	no se encuentran en un sitio confiable	alteración , modificación o daños a los servidores	alto	El sitio donde se encuentra este servidor debe estar protegido con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.	Área de las tic´s y Gerencia
backup	ingreso físico no autorizado por terceras personas	alteración , modificación o daños a los servidores	medio	El área de las tic´s deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado	Área de las tic´s y Gerencia
	No existen copias externas custodiadas	Ausencia de copias de seguridad	medio	se debe realizar copias de seguridad diariamente esto para contrarrestar pérdidas o daños de la información	Área de las tic´s
	no se encuentran en un sitio confiable	alteración , modificación o daños a los servidores	alto	El sitio donde se encuentra este servidor debe estar protegido con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado	Área de las tic´s
información	información impresa no está segura y controlada	perdida o mala manipulación de la información	medio	La integridad de la información que se pone a disposición en un sistema de acceso público debe estar protegida para evitar la	Área de las tic´s y Gerencia

				modificación no autorizada.	
	acceso físico no autorizado por terceras personas	perdida o mala manipulación de la información	medio	Las áreas deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado	Área de las tic´s y Gerencia
Aplicaciones propietarias y adquiridas	acceso no autorizado por ingeniería social y Phishing	Se deben implementar controles de detección, prevención y recuperación para proteger contra códigos maliciosos, así como procedimientos apropiados de concientización de los usuarios.	alto	El personal del área de las TIC´s no debe informar, dar o decir ningún acontecimiento o información de esta área ya que con esto se está vulnerando la seguridad de la información , se debe capacitar al personal de la organización sobre la importancia de la seguridad informática en una organización	Área de las tic´s
	no se encuentran en un sitio confiable	desastre naturales o mala manipulación de las aplicaciones	alto	Se debe diseñar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, y mayor seguridad en el área de las TIC´s	Área de las tic´s y Gerencia
Aplicaciones de Código Abierto	acceso no autorizado por ingeniería social y Phishing	Se deben implementar controles de detección, prevención y recuperación	alto	El personal del área de las TIC´s no debe informar, dar o decir ningún acontecimiento	Área de las tic´s

		para proteger contra códigos maliciosos, así como procedimientos apropiados de concientización de los usuarios.		o información de esta área ya que con esto se está vulnerando la seguridad de la información , se debe capacitar al personal de la organización sobre la importancia de la seguridad informática en una organización	
	no se encuentran en un sitio confiable	desastre naturales , modificación, eliminación o daño en la aplicación	alto	Se debe diseñar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, y mayor seguridad en el área de las TIC´s	Área de las tic´s y Gerencia
Sistemas operativos Linux	errores de seguridad por mala administración	acceso a la red de la organización que puede llevar al secuestro , perdida o modificación de la información	alto	Las redes se deben mantener y controlar adecuadamente para protegerlas de las amenazas y mantener la seguridad de los sistemas y aplicaciones que usan la red	Área de las tic´s
	no se encuentran en un sitio confiable	desastre naturales o mala manipulación de las aplicaciones	alto	Se debe diseñar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, y mayor seguridad en el área de las TIC´s	Área de las tic´s y Gerencia
Cuarto de telecomunicaciones	polución	daño en los equipos eléctricos	medio	Esta área debe contar con todas las	Área de las tic´s y Gerencia

				normas ambientales que estén el actualidad para contrarrestar esta	
	control de humedad	daño en los equipos eléctricos	alto	Esta área debe contar con todas las normas ambientales que estén el actualidad para contrarrestar esta	Área de las tic´s y Gerencia
Oficinas	acceso no autorizado físico	robo, perdida o daño en los equipos del área de la tic´s	bajo	Se debe implementar controles de seguridad en el área de la TIC´s como barra eléctricas, biométricos, cámaras de seguridad	Área de las tic´s y Gerencia
Cableado de red	falta de cumplimiento de la normatividad de cableado estructurado	perdida o caída de la red en la organización	alto	La organización deben tener las normas y estándares que estén en la actualidad	Área de las tic´s
Estaciones de trabajo	ingeniería social	perdida , modificación de la información	alto	El personal del área de las TIC´s no debe informar, dar o decir ningún acontecimiento o información de esta área ya que con esto se está vulnerando la seguridad de la información , se debe capacitar al personal de la organización sobre la importancia de la seguridad informática en una organización	Área de las tic´s
Rack	falta de cumplimiento de la normatividad de cableado	perdida o caída de la red en la organización	medio	La organización deben tener las normas y estándares que estén en la	Área de las tic´s

	estructurado			actualidad	
Servidor Apache	spoofing web	robo de la información , suplantación y modificación de la información	alto	El servidor debe tener los últimos parches de actualización que salgan esto para tener una seguridad fuerte y segura	Área de las tic´s
	errores de seguridad	robo de la información , suplantación y modificación de la información	alto	El servidor debe tener los últimos parches de actualización que salgan esto para tener una seguridad fuerte y segura	Área de las tic´s
	no se encuentran en un sitio confiable	desastre naturales , modificación, eliminación o daño en el servidor	alto	Se debe diseñar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, y mayor seguridad en el área de las TIC´s	Área de las TIC´s y Gerencia

Fuente: El autor

7.2.2 **DECLARACIÓN DE APLICABILIDAD**

En este punto se va a tomar como referencia los Controles del Anexo A del estándar ISO 27001:2013 y dominios a los que pertenece, esto con el fin de tener un Sistema de Gestión de Seguridad de la Información acorde a lo que dice establece dicha norma y teniendo en cuenta los resultados obtenidos en la anterior matriz de riesgos

Tabla 54. Declaración de Aplicabilidad

Dominio	**Objetivo de Control**	**Controles**	**Cumple**		**Observaciones**
			Si	No	
5. Políticas de seguridad de la información	5.1 Directrices de la Dirección en seguridad de la información.	5.1.1Conjunto de políticas para la seguridad de la información.	X		Hay un documento inicial de políticas de seguridad ligado al Plan Estratégico de Tecnologías de la Información de la Organización, ya paso por una revisión y aprobación inicial, pero no se han concretado algunas observaciones
		5.1.2 Revisión de las políticas para la seguridad de la información.		X	Solo se realizó la aprobación inicial de las políticas. Aún no se ha decidido cómo va a ser la revisión de estas, ni tampoco su frecuencia
6. Aspectos organizativos de la seguridad de la información	6.1 Organización interna.	6.1.1 Asignación de responsabilidades para la seguridad de la información.		X	No hay participación por parte de la dirección para la asignación de responsabilidades, creen que solo le compete a al área de Informática
		6.1.2 Segregación de tares.		X	Si existe una distribución parcial de funciones, pero no se aplica en todos los casos
		6.1.3 Contacto con las autoridades.	X		La organización tiene contacto directo con la policía ambiental que se encarga del acompañamiento y accionar en caso de algún desastre
		6.1.4 Contacto con grupos de interés especial.		X	No se comparte información con grupos de interés, ni se reciben notificaciones de seguridad, parches y vulnerabilidades. Solo se recibe un boletín de la policía nacional.
		6.1.5 Seguridad de la información en la gestión de proyectos.		X	No se incluye el componente de seguridad en el proceso de planeación y administración de proyectos
	6.2 Dispositivos para movilidad y	6.2.1 Política de uso de dispositivos para movilidad.		X	Está restringida la conexión a las redes wifi de los dispositivos móviles.

	teletrabajo.	6.2.2 Telegrama.			No aplica
7. Seguridad ligada a los recursos humanos.	7.1 Antes de la contratación.	7.1.1 Investigación de antecedentes.		X	Cuando se nombran funcionarios no se verifican, y a los contratistas se les exige los certificados judiciales
		7.1.2 Términos y condiciones de contratación.		X	No existen responsabilidades acerca de la seguridad de la información en los contratos
	7.2 Durante la contratación.	7.2.1 Responsabilidades de gestión.		X	No hay exigencia por parte de la dirección ni concienciación.
		7.2.2 Concienciación, educación y capacitación en seguridad de la información		X	No se imparte formación adecuada sobre políticas o procedimientos de seguridad de la información
		7.2.3 Proceso disciplinario.	X		Si existen procesos disciplinarios. El procedimiento es: Empezar una investigación con proceso disciplinario y enviarla al comité de procesos disciplinarios para evaluar y tomar decisiones al respecto.
	7.3 Cese o cambio de puesto de trabajo.	7.3.1 Cese o cambio de puesto de trabajo.		X	Después de finalizar el contrato, el contratista debe entregar un informe final de sus actividades y firmar el acta final del contrato, pero no se atiende ninguna otra responsabilidad o deber
8. Gestión de activos.	8.1 Responsabilidad sobre los activos.	8.1.1 Inventario de activos.	X		Existe, pero la información existente necesita ser revisada y filtrada; la información se actualiza cada que un nuevo activo es adquirido y se encuentra actualizado
		8.1.2 Propiedad de los activos.	X		Cada activo tiene asignado un responsable que es el encargado de velar por su custodia
		8.1.3 Uso aceptable de los activos.	X		En el documento de políticas actuales se encuentran consignadas algunas reglas para la utilización de equipos e información dentro de la entidad
		8.1.4 Devolución de activos.	X		Existen procedimientos para la devolución de activos en general al término de la contratación laboral, pero nada especifico
	8.2 Clasificación de la información.	8.2.1 Directrices de clasificación.	X		La información se encuentra parcialmente clasificada de acuerdo a un cuadro facilitado por gobierno en línea, pero solo se clasifico en el cuadro y no se ha empleado ninguna actividad con la información.
		8.2.2 Etiquetado y		X	No existe

		manipulado de la información.			
		8.2.3 Manipulación de activos.		X	No existe
	8.3 Manejo de los soportes de almacenamiento.	8.3.1 Gestión de soportes extraíbles.	X		Existen algunos controles para el préstamo de expedientes y documentos almacenados en el centro de documentación
		8.3.2 Eliminación de soportes.		X	No hay control o procedimiento definido para la eliminación de medios
		8.3.3 Soportes físicos en tránsito.	X		Existen algunos controles por ejemplo para el préstamo de expedientes hay una aplicación para el control de estos y para los documentos alojados en el centro de documentación hay otra aplicación y una persona encargada de administrar esa información
9. Control de accesos.	9.1 Requisitos de negocio para el control de accesos.	9.1.1 Política de control de accesos.		X	No hay políticas bien definidas o documentadas para el acceso y revisión periódica de la información
	9.2 Gestión de acceso de usuario.	9.2.1 Gestión de altas/bajas en el registro de usuarios.	X		Hay un registro y cancelación de usuarios a los sistemas y servicios de información, pero no hay un proceso o procedimiento definido, normalmente se recibe un comunicado interno por parte del jefe inmediato informando la cancelación del acceso al empleado
		9.2.2 Gestión de los derechos de acceso asignados a usuarios.	X		Hay una serie de roles y controles de acceso en la mayoría de aplicaciones
		9.2.3 Gestión de los derechos de acceso con privilegios especiales.	X		Si hay en la mayoría de aplicaciones
		9.2.4 Gestión de información confidencial de autenticación de usuarios.		X	No existe
		9.2.5 Revisión de los derechos de acceso de los usuarios.	X		Se realiza una revisión para la conexión a internet de los equipos y direcciones IP dentro de la organización

		9.2.6 Retirada o adaptación de los derechos de acceso	X		El supervisor o interventor del contrato debe informar a las dependencias la restricción al acceso de la información de la entidad como correo, software, expedientes, etc.
	9.3 Responsabilidades del usuario.	9.3.1 Uso de información confidencial para la autenticación.	X		Se solicita el uso de contraseñas seguras con ciertas normas para la autenticación solo en algunas aplicaciones
	9.4 Control de acceso a sistemas y aplicaciones	9.4.1 Restricción del acceso a la información.	X		Se realiza la restricción a través de un usuario y contraseña
		9.4.2 Procedimientos seguros de inicio de sesión.	X		Si algunos procedimientos seguros de inicio de sesión principalmente en el domino
		9.4.3 Gestión de contraseñas de usuario.	X		Existen ciertas restricciones para algunas contraseñas, así mismo pueden ser actualizadas a través del usuario administrador por requerimiento
		9.4.4 Uso de herramientas de administración de sistemas.	X		Se restringe el uso de estas herramientas
		9.4.5 Control de acceso al código fuente de los programas.		X	No está restringido en la mayoría de casos
10. Cifrado.	10.1 Controles criptográficos	10.1.1 Política de uso de los controles criptográficos.		X	No existe
		10.1.2 Gestión de claves.		X	No existe
11. Seguridad física y ambiental.	11.1 Áreas seguras.	11.1.1 Perímetro de seguridad física.	X		Para el acceso a la organización hay un control por biométrico donde se registra el usuario que ingresa, además se debe registrar los bolsos y se hace ingreso de los equipos de cómputo.
		11.1.2 Controles físicos de entrada.		X	Los controles físicos efectuados son los realizados en la entrada, la sala de servidores no cuenta con un control adecuado de acceso y registro
		11.1.3 Seguridad de oficinas, despachos y recursos.		X	Las oficinas son abiertas a todo el publico

		11.1.4 Protección contra las amenazas externas y ambientales.		X	Existe un plan de evacuación donde cada dependencia tiene brigadistas que conocen las instrucciones para las emergencias que se presenten. También tiene alarmas contra incendios, detectores de humo y conexión de mangueras
		11.1.5 El trabajo en áreas seguras.		X	No existe
		11.1.6 Áreas de acceso público, carga y descarga.		X	Casi toda la oficina tiene acceso al publico
	11.2 Seguridad de los equipos.	11.2.1 Emplazamiento y protección de equipos.		X	No hay protección específica para los equipos más que el usuario y contraseña de dominio
		11.2.2 Instalaciones de suministro.	X		Los equipos están conectados a electricidad regulada
		11.2.3 Seguridad del cableado.	X		Hay electricidad regulada, ups y planta eléctrica
		11.2.4 Mantenimiento de los equipos.	X		Hay contrato de mantenimiento
		11.2 .5 Salida de activos fuera de las dependencias de la empresa.		X	No existe
		11.2.6 Seguridad de los equipos y activos fuera de las instalaciones		X	No existe
		11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.	X		Solo se formatean a bajo nivel
		11.2.8 Equipo informático de usuario desatendido.	X		Solo se bloquea la sesión pasados unos minutos desatendido
		11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.	X		Depende de los empleados

12. Seguridad en la operativa.	12.1 Responsabilidades y procedimientos de operación	12.1.1 Documentación de procedimientos de operación.		X	No existe
		12.1.2 Gestión de cambios.		X	No existe
		12.1.3 Gestión de capacidades	X		Se realiza parcialmente y por accionar propio del empleado
		12.1.4 Separación de entornos de desarrollo, prueba y producción		X	No existe
	12.2 Protección contra código malicioso.	12.2.1 Controles contra el código malicioso.	X		Existen licencias de antivirus para cada equipo y una consola de administración, así como también hay un servidor de seguridad perimetral
	12.3 Copias de seguridad	12.3.1 Copias de seguridad de la información.	X		Si existen procesos de respaldo realizados de forma periódica a la información
	12.4 Registro de actividad y supervisión.	12.4.1 Registro y gestión de eventos de actividad.	X		En algunas ocasiones se hace, pero no es un procedimiento o una actividad que siempre se realice.
		12.4.2 Protección de los registros de información.	X		Se realiza una protección parcial
		12.4.3 Registros de actividad del administrador y operador del sistema.	X		Solo se aplica en algunas aplicaciones
		12.4.4 Sincronización de relojes.		X	No existe
	12.5 Control del software en explotación.	12.5.1 Instalación del software en sistemas en producción.	X		Se controla
	12.6 Gestión de la vulnerabilidad técnica.	12.6.1 Gestión de las vulnerabilidades técnicas.		X	No existe
		12.6.2 Restricciones en la instalación de software.	X		Parcialmente

	12.7 Consideraciones de las auditorías de los sistemas de información	12.7.1 Controles de auditoría de los sistemas de información.		X	No existe
13. Seguridad en las telecomunicaciones.	13.1 Gestión de la seguridad en las redes.	13.1.1 Controles de red.	X		El control por el servidor de seguridad perimetral
		13.1.2 Mecanismos de seguridad asociados a servicios en red.	X		El software y hardware del servidor de seguridad perimetral
		13.1.3 Segregación de redes.	X		Hay una segregación de red por vlan
	13.2 Intercambio de información con partes externas	13.2.1 Políticas y procedimientos de intercambio de información.	X		Cuando existe solicitud de información se entrega únicamente con el aval del jefe inmediato
		13.2.2 Acuerdos de intercambio.	X		Existen algunos acuerdos de intercambio con otras entidades
		13.2.3 Mensajería electrónica.	X		Se contrata el servicio de correo con un tercero
		13.2.4 Acuerdos de confidencialidad y secreto.		X	No existe
14. Adquisición, desarrollo y mantenimiento de los sistemas de información.	14.1 Requisitos de seguridad de los sistemas de información.	14.1.1 Análisis y especificación de los requisitos de seguridad.		X	No existe
		14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.		X	No existe
		14.1.3 Protección de las transacciones por redes telemáticas.		X	No existe
	14.2 Seguridad en los procesos	14.2.1 Política de desarrollo seguro de software.		X	No existe

	de desarrollo y soporte.	14.2.2 Procedimientos de control de cambios en los sistemas.		X	No existe
		14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	X		Se realiza en algunas ocasiones
		14.2.4 Restricciones a los cambios en los paquetes de software.	X		Solo en algunas aplicaciones
		14.2.5 Uso de principios de ingeniería en protección de sistemas.		X	No existe
		14.2.6 Seguridad en entornos de desarrollo.		X	No existe
		14.2.7 Externalización del desarrollo de software.	X		Se aplica parcialmente
		14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.		X	No existe
		14.2.9 Pruebas de aceptación.		X	No existe
	14.3 Datos de prueba	14.3.1 Protección de los datos utilizados en pruebas.		X	No existe
15. Relaciones con suministradores	15.1 Seguridad de la información en las relaciones con suministradores.	15.1.1 Política de seguridad de la información para suministradores.		X	No existe
		15.1 .2 Tratamiento del riesgo dentro de acuerdos de suministradore	X		Se trata parcialmente, se incluyen unas pólizas de cumplimiento

		s.			
		15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.		X	No existe
	15.2 Gestión de la prestación del servicio por suministradores.	15.2.1 Supervisión y revisión de los servicios prestados por terceros.	X		Se hace una evaluación a los proveedores, pero no se realizan auditorias periódicamente
		15.2.2 Gestión de cambios en los servicios prestados por terceros.		X	No existe
16. Gestión de incidentes en la seguridad de la información	16.1 Gestión de incidentes de seguridad de la información y mejoras	16.1.1 Responsabilidades y procedimientos.		X	No existe
		16.1.2 Notificación de los eventos de seguridad de la información.		X	No existe
		16.1.3 Notificación de puntos débiles de la seguridad.		X	No existe
		16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.		X	No existe
		16.1 .5 Respuesta a los incidentes de seguridad.	X		Se resuelven los incidentes, pero no hay procedimientos debidamente documentados
		16.1.6 Aprendizaje de los incidentes de seguridad de la información.		X	No existe
		16.1.7 Recopilación de evidencias.		X	No existe
17. Aspectos de seguridad de la	17.1 Continuidad de la	17.1.1 Planificación de la	X		Hay definido un procedimiento inicial de continuidad

información en la gestión dela continuidad del negocio.	seguridad de la información.	continuidad de la seguridad de la información.			
		17.1.2 Implantación de la continuidad de la seguridad de la información.	X		Si se tienen planes
		17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.		X	No existe
	17.2 Redundancias.	17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.	X		Solo hay redundancia en algunos de sistemas y servicios
18. Cumplimiento.	18.1 Cumplimiento de los requisitos legales y contractuales.	18.1.1 Identificación de la legislación aplicable.	X		Se tienen identificadas la siguiente legislación: Documento Compes 3072 de 2000, Ley 962 de 2005, Ley 1151 de 2007 art 6, Decreto 1151 de 2008, Documento Compes 3650 de 2010, Ley 1450 de 2011 art. 227, Ley 1450 de 2011 art. 230, Ley 1450 de 2011 art. 232, Decreto 2693 de 2012, Manual 3.1 Gobierno en línea, Acuerdo Carder 005 de 2013, Ley 527 de 1999, Decreto 1747 de 2000 art 9, Ley estatutaria 1266 de 2008, Ley 1273 de 2009, Ley 1581 de 2012, LEY 23 DE 1982, LEY 44 DE 1993
		18.1.2 Derechos de propiedad intelectual (DPI).	X		Se controla
		18.1.3 Protección de los registros de la organización.		X	No existe
		18.1.4 Protección de datos y privacidad de la información personal.		X	No existe
		18.1.5		X	No existe

		Regulación de los controles criptográficos.			
	18.2 Revisiones de la seguridad de la información	18.2.1 Revisión independiente de la seguridad de la información.		X	No existe
		18.2.2 Cumplimiento de las políticas y normas de seguridad.		X	No existe
		18.2.3 Comprobación del cumplimiento	X		Se hace verificación

Fuente: El autor

8. DISEÑO DE FORMATOS DE CONTROL Y ADMINISTRACIÓN DE ACUERDO A LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA INSTITUCIÓN UNIVERSITARIA TECNOLOGICA UNICOMFACAUCA POPAYAN

La generación de políticas de seguridad en el área de TIC´s de cualquier organización, son la estructura principal para el buen control y funcionamiento de todos los procesos internos que se manejen en ella.

El tener bien definido que procesos se manejan en el área de TIC´s de la Organización, facilita tener claro la creación de las políticas de seguridad. Dichas políticas deben ser claras y concretas para poder realizarse un buen diligenciamiento y Seguimiento.

A continuación se nombran las políticas de seguridad de la información recomendadas para la División de TI de Unicomfacauca.

1. Política de Seguridad de La Información.
2. Política de Monitoreo a la Seguridad.
3. Política de uso de Internet.
4. Política de administración de contraseñas
5. Política de Administración de Cuentas
6. Política de Administración y seguridad en Servidores.
7. Política de Licenciamiento de Software.
8. Política de Respaldo y Recuperación de Información.
9. Política de administración de reporte de Incidentes (tickets)
10. Política de Detección de Intrusiones.
11. Política de buen uso de los recursos de la universidad
12. Política de acceso físico a los recursos
13. Política de acceso a la red
14. Política de entretenimiento y capacitación en seguridad
15. Políticas de detección de virus

Fecha de Creación:	**19-10/2017**	Fecha de Actualización:	
Numero Documento :	Política 1	Departamento:	**TIC´S**
Nombre Documento:	**POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN**		
Elaborado Por:	**Wilmar Andrés Duarte Ortiz**		
Aprobado por:			
observaciones:			
Política	Unicomfacauca aplicará políticas, prácticas, procedimientos y guías, para proteger los datos internos, y así prevenir errores de programación, mal manejo por individuos dentro o fuera de la Universidad. Esto con la finalidad de proteger a la Universidad de riesgos que comprometan la integridad de los programas, estos serán responsables y adaptables a los cambios tecnológicos que afecten los Recursos de Información.		
Normatividad	▪ El departamento de TIC´s está dirigida a establecer la responsabilidad de políticas para el manejo de las actividades de los recursos de información, proveer una mejor coordinación de las actividades de la información para asegurar una mejor orientación de tales actividades. ▪ La división de TIC´s tiene la autoridad y responsabilidad de implementar políticas, prácticas, procedimientos y guías para proteger los recursos de Información de Unicomfacauca **Administrador:** Es el usuario directamente responsable de las funciones que tiene que ver con el manejo y soporte de los recursos, es la persona a la cual se le responsabiliza de gestionar los programas que utilizan los recursos de información. El administrador es responsable de establecer los controles que provean la seguridad. Dependiendo sea el caso, la propiedad puede ser compartida por		

	gerentes o administradores de diferentes áreas. **Usuario:** Tiene la responsabilidad de (1) usar los recursos sólo para los propósitos establecidos por el administrador y la Universidad, (2) cumplir con los controles establecidos por el propietario y Unicomfacauca, y (3) prevenir declaraciones de información confidencial o sensible. El usuario es la persona que ha sido autorizada por el administrador para leer, ingresar, modificar o actualizar la información. El usuario cumple el más simple control efectivo para proveer adecuada seguridad. **Controles:** Asegura que los recursos de información de Unicomfacauca estén adecuadamente resguardados, basado en un manejo de riesgos, dirigido por el Jefe de la división de TIC´s, actuando con autoridad delegada para la toma de decisiones de manejo de riesgos. ➢ Los controles de Seguridad no deben ser evadidos o inutilizados. ➢ La conciencia de seguridad del personal debe ser continua, reforzada, actualizada y validada. ➢ Todo el personal es responsables por los actos relacionados a la seguridad. El personal es igualmente responsable de reportar cualquier sospecha o confirmación de violaciones o manejo inapropiado de la política de seguridad de información. ➢ Las contraseñas, números de identificación de personal (PIN), claves de seguridad (tarjeta inteligente de seguridad), y otros procedimientos y dispositivos de seguridad en los sistemas de información que deben ser protegidos por el usuario. Toda violación de seguridad debe ser reportada al responsable, administrador, encargado y/o a la división de TIC´s. ➢ El acceso, el cambio y el uso de los recursos de Información deben ser estrictamente seguros. La autorización de acceso a la información para cada usuario debe ser revisada regularmente, así como el cambio de status del usuario como: transferencia, baja o culminación de sus

	actividades. ➢ El uso de los recursos de Información debe ser oficialmente autorizado, los mismos que son sólo para propósitos de la empresa. No existe garantía de privacidad personal o acceso a herramientas que se encuentran dentro de los recursos, pero no se limitan a: e-mail, navegación en Internet, web, ftp, y otras herramientas de comunicación electrónica. El uso de estas herramientas pueden ser monitoreadas para realizar o esclarecer reclamos o procesos de investigación. Los departamentos o áreas que tienen a cargo el manejo de computadores, deben ser responsable de la adecuada utilización de los recursos de Información, el efectivo manejo, estado y reporte del mismo. ➢ Cualquier información, debe ser mantenida con confidencialidad y seguridad por el usuario. El hecho de que la información sea almacenada electrónicamente no cambia el requerimiento de mantener la información segura y confiable. El tipo o clasificación de la información por sí misma es la base para determinar si la información debe guardarse en forma confidencial y segura. Adicionalmente, si esta información es almacenada en un papel o un formato electrónico, o si la información es copiada, impresa o trasmitida electrónicamente debe ser protegida como confidencial y segura.

Fecha de Creación:	**19-10/2017**	Fecha de Actualización:	
Numero Documento :	**Política 2**	Departamento:	**TIC´S**
nombre documento:	**Política de monitoreo a la seguridad**		
Elaborado Por:	**Wilmar Andrés Duarte Ortiz**		
Aprobado por:			
observaciones:			

Política	El propósito de este procedimiento es establecer los lineamientos básicos para la elaboración de los archivos y manuales de gestión de evaluación del buen uso de la red.
Normatividad	El jefe de la división de TIC´s y el Administrador directamente estarán encargados de: **Control del Acceso:** • Almacenar los archivos generados de forma persistente en un disco duro y realizar las copias de seguridad necesarias para su evaluación • Realizar el análisis diario de los eventos de tráfico de red, envío de correo electrónico y acceso en horario no común. • Hacer seguimiento a los eventos no comunes encontrados en los análisis realizados. • Poner en marcha el plan de incidentes en caso de encontrar una vulnerabilidad. **Tráfico de la Red:** • Realizar semanalmente el gráfico que me permita analizar el tráfico de la red. • Hacer uso del software especializado para realizar el análisis de tráfico de la red. • Monitorear los recursos más importantes a través del software de gestión de red. **Volúmenes de correo:** El personal autorizado de la generación de reportes de correo debe estar en capacidad para definir si existen cambios en el monitoreo de correo o mails en tránsito, con el propósito de verificar el uso de los medios de comunicación. **Monitoreo de conexiones activas:**

	• El personal autorizado de la vigilancia y monitoreo en tiempo real debe estar pendiente de la inactividad de los terminales. • Un terminal en estado inactivo por más de 30 minutos será dado de baja en la red. • El usuario que no tenga un terminal seguro será dado de baja en la red entendiéndose como inseguro un equipo sin antivirus. • De tener un terminal con antivirus desactualizado el sistema le exigirá actualización, de no realizarse, el sistema le dará de baja al terminal. **Modificación de archivos:** • El director de la división de TI será el encargado de autorizar la modificación de archivos generados de ser necesario. • De ser modificado un archivo sin autorización, se debe penalizar al actor de dicho cambio y recuperar el archivo a través de su copia de seguridad de forma inmediata. **Copias de Seguridad:** Las copias de seguridad realizadas diaria, semanal o mensualmente deben almacenarse junto con todos los Backups **Puertos en la Red:** El personal autorizado del monitoreo en tiempo real debe estar monitoreando los puertos activos y la seguridad de los mismos. Si el puerto no es seguro debe cerrarse de inmediato.

Elaborado Por:	**Wilmar Andrés Duarte Ortiz**
Aprobado por:	
observaciones:	
Política	El propósito de esta Política es colocar límites para el acceso y el uso de Internet, esto con el fin de garantizar la navegación por internet de manera segura y confiable y de esta manera contrarrestar y evitar algún virus o código malicioso en la red de la institución universitaria y así proteger la información de los procesos de la organización.
Normatividad	• El servicio de internet es ofrecido para el personal administrativo, docentes y estudiantes de la Institución que lo solicite, el uso de este recurso por personas ajenas a la misma queda terminantemente prohibida sin previa autorización. • El acceso a Internet se realiza por medio de servidores Proxy, los cuales permiten a la comunidad educativa acceder a Internet de una manera rápida y eficiente, dicho servicio puede ser empleado por cualquier miembro del estamento educativo de manera anónima, el servicio como tal tiene configurada políticas de seguridad que generan restricciones de acceso a lugares o puertos específicos que pueden causar una vulnerabilidad. • El acceso a la información en internet debe ser de carácter institucional, no puede tener contenido pornográfico o contenido lesivo contra la integridad de una institución o una persona. • Para la navegación los usuarios cuentan con acceso a través de Proxy por tal motivo las aplicaciones p2p, Torrens, para descarga información no pueden ser empleadas. • La descarga de información debe ser controlada, esta información debería tener un carácter educativo. • No se puede emplear el acceso a Internet para realizar actividades que entorpecen el normal

	funcionamiento de redes externas

Fecha de Creación:	**19-10/2017**	Fecha de Actualización:	
Numero Documento:	**Política 4**	Departamento:	**TIC´S**
Nombre Documento:	**POLÍTICA DE ADMINISTRACIÓN DE CONTRASEÑAS**		
Elaborado Por:	**Wilmar Andrés Duarte Ortiz**		
Aprobado por:			
observaciones:			

Política	El propósito de la política para la administración de contraseñas es establecer las reglas para la creación, distribución, protección y terminación de los mecanismos de autenticación del usuario para ejecutar los recursos de información.
Normatividad	• El jefe de las TIC´s es el responsable de la creación, eliminación y administración de las cuentas. La contraseña se debe cambiar la primera vez que el usuario ingrese al equipo. • Se debe mantener un historial de contraseñas para evitar la reutilización de las mismas. • Las contraseñas almacenadas deben estar cifradas. • Las contraseñas asignadas a cada usuario no deben ser divulgadas o compartidas con nadie. • Si la seguridad de una contraseña está en duda, la contraseña debe ser cambiada inmediatamente. • Todas las contraseñas creadas por los usuarios no deben utilizar palabras que se encuentren en el diccionario, como tampoco debe llevar información de los datos personales del usuario. • Los dispositivos electrónicos como computadores , portátiles o tables siempre deben tener habilitado el protector de pantalla, esto para proteger la

	información del usuario y de la organización • Todas las contraseñas deben ser como mínimo de 8 caracteres y en su contenido deben llevar letras mayúsculas, minúsculas, números u otros caracteres especiales es decir alfanuméricos. • Las contraseñas deben ser cambiadas, pues su vigencia máxima debe ser de tres meses.

Fecha de Creación:	**19-10/2017**	Fecha de Actualización:	
Numero Documento :	**Política 5**	Departamento:	**TIC´S**
Nombre Documento:	**POLÍTICA DE ADMINISTRACIÓN DE CUENTAS**		
Elaborado Por:	**Wilmar Andrés Duarte Ortiz**		
Aprobado por:			
observaciones:			
Política	El propósito de la política de administración de la cuentas es establecer las reglas para la creación, seguimiento, control y eliminación de cuentas de usuario.		
Normatividad	• El administrador de cuentas o personal autorizado: • Son responsables de crear, modificar o eliminar las cuentas de las personas que trabajan dentro de la división de TI, que cambian de puesto o de los roles de trabajo, o pierden relación con la división de TI. • Deben de documentar la modificación de los parámetros de las cuentas de usuario. • Deben tener un proceso documentado para la revisión y validación periódica de las cuentas existentes.		

	• Están sujetas a revisión de auditoría independiente. • Deben proporcionar una lista de cuentas de usuario con los sistemas que administran y el acceso que poseen cuando sea solicitado por la administración. • Deben cooperar con la administración de la división de TIC´s y con Unicomfacauca con la investigación de los incidentes de seguridad relacionados con las cuentas de acceso. • Todas las cuentas creadas deben tener una solicitud asociada y la aprobación por el jefe de la división de TIC´s. • Todas las cuentas deben tener un número único de identificación con el nombre de usuario asignado. • Todas las contraseñas por defecto para las cuentas de usuario deben ser creadas de acuerdo a las políticas de administración de contraseñas. • Todas las contraseñas de las cuentas deben tener una caducidad de acuerdo a las políticas de administración de contraseñas. • Los usuarios no deben compartir la(s) cuenta(s) de usuario, o contraseñas con ninguna persona. • Cuentas de personas sin uso (más de 30 días) se desactivará. • Todas las nuevas cuentas de usuario que no se hayan accedido en un periodo de 30 días desde su creación se desactivarán. • Todo usuario que requiere una cuenta temporal, deberá solicitarla formalmente al jefe de la división de TIC´s indicando los motivos de la solicitud.

Creación:			
Numero Documento :	**Política 6**	Departamento:	**TIC´S**
Nombre Documento:	**POLÍTICA DE ADMINISTRACIÓN Y SEGURIDAD EN SERVIDORES**		
Elaborado Por:	**Wilmar Andrés Duarte Ortiz**		
Aprobado por:			
observaciones:			
Política	Esta política tiene como propósito proporcionar un nivel de seguridad y control sobre el acceso y gestión de los servidores de Unicomfacauca. Se define quién tendrá acceso al servidor, y quienes tendrán acceso a modificar su contenido y su respectiva documentación, también se define quien será notificado cuando se realizan cambios en los servidores.		
Normatividad	Se debe diseñar una hoja de vida para llevar un control de administración del servidor, en el que se incluya la siguiente información: • Documentaciones de seriales y características equipo. • Nombre y contacto del responsable directo del equipo. • Documentación de necesidades del entorno de operación (sistema de alimentación ininterrumpida, aire acondicionado, etc.) y ubicación del equipo. • Se deberá llevar la documentación sobre la configuración, instalación y actualización del sistema operativo, así como de las aplicaciones requeridas y de los programas propios de la institución, de acuerdo a los requisitos que prestar el nuevo equipo. • Se Llevara la documentación sobre todo lo relacionado con la creación, publicación de solicitudes de creación, eliminación y modificación de cuentas de usuarios, también se llevara la documentación de las instalaciones de programas y de mejora de recursos, etc. • Todo lo que corresponde sobre la administración de los servidores se llevara a cabo por una solo persona que esta lo decidirá el jefe de TIC´s de la institución • Se llevara a cabo el monitoreo continuamente sobre		

	todos los servidores, para verificar que todo los servicios que estén instalados se encuentren operando, funcionando correctamente y estén disponibles para el acceso controlado de usuarios. • Tener las instalaciones donde se encuentre la infraestructura de la red informática en óptimas condiciones con acceso cómodo. • Llevar documentado los registros de los eventos periódicamente de los monitoreos que la red y de los servidores como también se tendrá que llevar los registros históricos de incidencias, sincronizar los relojes.

Fecha de Creación:	**20-06/2012**	Fecha de Actualización:	
Numero Documento :	**Política 7**	Departamento:	**TIC´S**
Nombre Documento:	**POLÍTICA DE LICENCIAMIENTO DE SOFTWARE**		
Elaborado Por:	**Wilmar Andrés Duarte Ortiz**		
Aprobado por:			
observaciones:			
Política	Esta política se crea como marco regulatorio en donde se definen los procedimientos para instalación manipulación y uso responsable de las herramientas software licenciadas, adquiridas por Unicomfacauca y da a conocer a los usuarios el alcance de lo permitido y lo prohibido de las licencias software a su disposición.		
Normatividad	Esta política se crea como marco regulatorio en donde se definen los procedimientos para instalación manipulación y uso responsable de las herramientas software licenciadas, adquiridas por Unicomfacauca y da a conocer a los usuarios el alcance de lo permitido y		

	lo prohibido de las licencias software a su disposición. **Normatividad** La división de TIC´s de Unicomfacauca es la única área autorizada para llevar a cabo la administración del software de la institución, por lo que dentro de sus responsabilidades se encuentran: • Mantener bajo resguardo las licencias de uso de software. • Llevar un control detallado de las licencias en operación y los equipos en los cuales se encuentra en uso. • Organizar la inspección de los equipo ofimáticos de la institución en intervalos regulares. • Difundir a los usuarios las políticas de licenciamiento de software en busca de dar a conocer la normatividad existente. • Analizar las necesidades y requerimientos de software de la institución. • Instalar, prestar soporte o guiar en el proceso de instalación de software en todos los equipos ofimáticos de la institución. Se debe llevar un registro documentado de todas las licencias que adquiere Unicomfacauca, realizada por el personal autorizado en donde se debe incluir los siguientes datos: Acta de Registro de Licencias Software: • Nombre del software • Empresa desarrolladora. • Versión. • ID Institucional. • Fecha de adquisición. • Fecha de vencimiento. • Tipo de Garantía. • Tiempo de Garantía. • Contacto.

Fecha de Creación:	**20-10/2017**	Fecha de Actualización:	
Numero Documento :	**Política 8**	Departamento:	**TIC´S**
Nombre Documento:	**POLÍTICA DE RESPALDO Y RECUPERACIÓN DE INFORMACIÓN**		
Elaborado Por:	**Wilmar Andrés Duarte Ortiz**		
Aprobado por:			
observaciones:			
Política	El propósito principal de este procedimiento es certificar que al acceder a algún recurso por parte de personal ajeno a la administración del mismo, este solo pueda modificar los archivos, aplicaciones y/o servicios que previamente hayan sido autorizados.		
Normatividad	• El administrador directo de recurso después de aprobar las modificaciones que se le realizarán al mismo, creara una cuenta de usuario y contraseña determinados, para la persona que va ingresar al recurso. • Cada cuenta que se utiliza para el acceso especial a los recursos, debe cumplir con las políticas de administración de cuentas y contraseñas vigentes estipuladas por la división de TIC´s de Unicomfacauca. • La cuenta del usuario para la persona que ingresara al recurso deberá tener limitaciones, solo podrá acceder a los Archivos, Aplicaciones y/o Servicios necesarios para las modificaciones autorizadas. • Dicha cuenta proporcionada tendrá un tiempo límite de actividad, luego de este tiempo la cuenta será cancelada. • Para cuentas de acceso especial compartido, la contraseña debe ser cambiada cuando alguna persona		

	es dada de baja o reubicada dentro de la división de TI de Unicomfacauca, Así mismo se aplica en caso de cambio en el personal de algún proveedor. • Se debe mantener siempre el Backups de la configuración del recurso previa a las modificaciones, para garantizar una restauración rápida y eficiente en caso de fallas. • En el caso de que un recurso sólo tenga un administrador, debe haber un procedimiento de traspasó de contraseña, para que alguien que no sea el administrador (Acceso especial) puede acceder al sistema en una situación de emergencia. • Se debe establecer un manual o documentación detallada de las modificaciones, configuraciones, actualizaciones que se realicen al recurso, por si existe algún problema en el futuro

Fecha de Creación:	**20-10/2017**	Fecha de Actualización:	
Numero Documento :	**Política 9**	Departamento:	**TIC´S**
Nombre Documento:	**POLÍTICA DE ADMINISTRACIÓN DE REPORTE DE INCIDENTES (TICKETS)**		
Elaborado Por:	**Wilmar Andrés Duarte Ortiz**		
Aprobado por:			
observaciones:			
Política	La Política de Administración de Incidentes (tickets) tiene como propósito resolver cualquier incidente que cause una interrupción en el servicio de la manera más rápida y eficaz posible.		

Normatividad	• Se debe documentar cualquier incidente, así como su solución, almacenándolos en una base de datos para dar solución fácil a los futuros incidentes similares. • Se debe designar personal responsable para la gestión de incidentes reportados • Se debe realizar la divulgación de la política de la creación de incidentes para todo el personal de la organización sin excepción. • Ejecutar procedimientos de administración de incidentes para contener y mitigar el incidente. • Se debe documentar y clasificar los incidentes que ocurra en la organización. • El personal responsable de la administración de los incidentes es el responsable de la integridad de la información de la organización. • Se procederá al aprendizaje, conocimiento con los incidentes de seguridad de la información creados y solucionados, para prevenir nuevas ocurrencias. • Se implementara actividades post-incidente, como es la generación de mejoras a los procesos operativos de gestión de incidentes de seguridad de la información o asegurar la evidencia de los incidentes.

Fecha de Creación:	**20-10/2017**	Fecha de Actualización:	
Numero Documento :	**Política 10**	Departamento:	**TIC´S**
Nombre Documento:	**POLÍTICA DE DETECCIÓN DE INTRUSIONES**		
Elaborado Por:	**Wilmar Andrés Duarte Ortiz**		
Aprobado por:			
observaciones:			
	La finalidad de esta política es garantizar o minimizar al		

Política	máximo los riesgos, fallas, o robo de información que se puedan llegar a presentar por el acceso no autorizado de un intruso durante el proceso normal de funcionamiento de los equipos en general (Hardware y software).
Normatividad	• Guardar un reporte documentado y físico en discos de almacenamiento de intrusiones y Backups por parte del departamento de TIC´s y respaldarlos con una segunda copia guardada en una segunda sede de ser posible. • Todos los procesos relacionados con los servicios informáticos de Unicomfacauca deben contar con diversos sistemas de seguridad que protejan al máximo nivel los mismos. • Los registros de acceso en los sistemas de control físico deben ser controlados /revisados diariamente por el analista de seguridad encargado. • Se debe contar con funciones de alarma y alerta en los servidores de seguridad y en los cuales siempre debe de estar habilitado. • Todo registro de control de acceso físico o lógico debe mantenerse siempre activo. • Hacer comprobaciones de integridad del sistema en todos y cada uno de los servidores para el correcto funcionamiento de trabajo en Unicomfacauca sobre una base diaria. (La integridad del sistema se refiere a la estabilidad y accesibilidad del servidor que patrocina la fuente de trabajo). • Los registros de auditoría para los servidores y maquinas internas de la red protegida deben ser revisados una vez por semana. El administrador del sistema debe proporcionar un informe al analista de seguridad. • Todos los informes que presenten problemas deben ser revisados en búsqueda de síntomas que podrían contener actividad intrusiva. • Los usuarios deben ser precavidos para reportar cualquier anomalía en el funcionamiento del sistema o signos de mala conducta en el mismo.

Fecha de Creación:	**20-10/2017**	Fecha de Actualización:	
Numero Documento :	**Política 11**	Departamento:	**TIC´S**
Nombre Documento:	**POLÍTICA DE BUEN USO DE LOS RECURSOS DE LA UNIVERSIDAD**		
Elaborado Por:	**Wilmar Andrés Duarte Ortiz**		
Aprobado por:			
observaciones:			
Política	Los recursos son bienes estratégicos de la Universidad tecnológica de Comfacauca que deben ser manejados como recursos valiosos, por tal razón se hace necesario generar una serie de regulaciones y normas que busquen orientar a toda la comunidad universitaria sobre el buen uso que se le debe de dar teniendo en cuenta la disposición de los usuarios en Unicomfacauca.		
Normatividad	Los alumnos, profesores y personal administrativo no deben tratar de acceder a cualquier información o programa de los sistemas de la Universidad a los que no han sido autorizados o cuenten con consentimiento explícito. • El uso incidental no deben significar costos directos a la Universidad. • El uso incidental no debe interferir con las actividades normales de los deberes de los estudiantes, profesores o personal administrativo. • El uso incidental no deben significar costos directos a la Universidad. • El uso incidental no debe interferir con las		

	actividades normales de los deberes de los estudiantes, profesores o personal administrativo. • Los alumnos y profesorado no deben compartir sus cuentas, contraseñas, números de identificación (PIN), claves de Seguridad o información similar o dispositivos usados para propósito de identificación y autorización. • Los usuarios no deben hacer copias no autorizadas de software.

Fecha de Creación:	**20-10/2017**	Fecha de Actualización:	
Numero Documento :	**Política 12**	Departamento:	**TIC´S**
Nombre Documento:	**POLÍTICA DE ACCESO FÍSICO A LOS RECURSOS**		
Elaborado Por:	**Wilmar Andrés Duarte Ortiz**		
Aprobado por:			
observaciones:			
Política	La Política de acceso fisco a los recursos tiene como propósito definir la responsabilidad de los actores que tienen algún vínculo con los activos de información y el acceso a ella, tanto interna como externamente.		
Normatividad	• Los equipos deben ser protegidos ante fallas de potencia • Se deben tener UPS para el correcto funcionamiento de servidores y equipos en general. • Se deben tener interruptores eléctricos		

	adicionales. • El mantenimiento del cableado y de los equipos debe ser realizado por personal calificado y autorizado. • El sitio en donde se ubiquen los recursos debe ser físicamente sólido y protegido de factores naturales y acceso de no autorizados. • Debe existir un área de recepción que permita el acceso de personal autorizado. • Todas las salidas de emergencia del perímetro deben estar protegidas con alarmas. • Se debe separar físicamente la operación de terceros de la estructura encargada del procesamiento informático. • Equipos como impresoras, faxes, fotocopiadoras usados por el personal deben estar en una zona definida que evite el acceso a los activos de información. • La información confidencial de la Universidad solo puede ser enviada a través de fax o Modem cuando no existan otros medios que confieran una mejor seguridad. • La información considerada como confidencial NUNCA debe enviarse a una impresora de red sin que exista una persona autorizada para cuidarla durante y después de la impresión. • Todas las personas deben estar pendientes del personal extraño sin identificación visible dentro de las instalaciones físicas, en caso de saber de alguno, se debe informar inmediatamente a seguridad. • En cuanto a la seguridad de los equipos se debe tener en cuenta: • Robo • Fuego • Explosivos

	• Humo • Inundación o falta de suministro • Interferencia eléctrica • No se permite fumar dentro del área de los recursos ni en el área de recepción. • Los equipos deben ser protegidos ante fallas de potencia • Se deben tener UPS para el correcto funcionamiento de servidores y equipos en general. • Se deben tener interruptores eléctricos adicionales. • El mantenimiento del cableado y de los equipos debe ser realizado por personal calificado y autorizado.

Fecha de Creación:	**20-10/2017**	Fecha de Actualización:	
Numero Documento :	**Política 13**	Departamento:	**TIC´S**
Nombre Documento:	**POLÍTICA DE ACCESO A LA RED**		
Elaborado Por:	**Wilmar Andrés Duarte Ortiz**		
Aprobado por:			
observaciones:			
Política	El propósito de esta política es establecer las reglas para el acceso y uso de la infraestructura de la red. Estas reglas son necesarias para preservar la		

	integridad, disponibilidad y confidencialidad de la información de la Unicomfacauca.
Normatividad	• Los usuarios no deben instalar hardware o software de red que proporcione servicios de red sin autorización. • Los usuarios no deben descargar, instalar o ejecutar programas de seguridad o utilidades que revelen debilidades en la seguridad de un sistema. • Los usuarios no pueden modificar el hardware de red en modo alguno sin previa autorización. • Los usuarios y sistemas informáticos que requieran conectividad de red deben ajustarse a las normas ya descritas en esta política y siempre con la autorización. • Los usuarios están autorizados a utilizar solo las direcciones de red que les sean asignadas por la división de sistemas y redes de datos. • Todos los accesos remotos hacia los recursos de información de la Unicomfacauca, solo se podrán establecer a través de protocolos aprobados por la misma. • Los usuarios no deben extenderse o retransmitir los servicios de la red en cualquier forma, incluyendo la instalación de cualquier tipo de router, Switch, o punto de acceso inalámbrico sin la debida autorización por parte de Unicomfacauca.

Elaborado Por:	**Wilmar Andrés Duarte Ortiz**
Aprobado por:	
observaciones:	
Política	La política de Entrenamiento y Capacitación en Seguridad se diseña con el fin de asegurarse de que el personal que este en contacto con el área TIC´s reciban un adecuado entrenamiento sobre el comportamiento de los recursos computacionales.
Normatividad	• Coordinar la disponibilidad horaria con el personal de la división de TIC´s para realizar capacitaciones. • Establecer los procedimientos y normas internas relacionadas con la capacitación en seguridad necesaria para el personal de división de TIC´s • Desarrollar un banco de recursos internos y externos para proveer capacitaciones de seguridad. • Preparar anualmente informes de logros e informes estadísticos relacionados con las capacitaciones realizadas sobre seguridad. • Desarrollar guías sobre las capacitaciones que pueden requerirse al personal de nueva capacitación, en nombramiento provisional y personal con funciones de supervisión. • Desarrollar instrumentos de evaluación para medir la utilidad y alcance de las capacitaciones. • Evaluar periódicamente las necesidades de capacitación. • Se debe elaborar un plan de capacitación y calendario anual de actividades a realizar, que responda a las necesidades reales del personal para proveer conocimiento y el desarrollo de destrezas y habilidades con el fin de mejorar el desempeño y seguridad en el uso de los activos de información.

	• Se debe atender a las necesidades de capacitación mediante la planificación, organización, coordinación y ofrecimiento de actividades educativas de desarrollo personal, desarrollo tecnológico y profesional.

Fecha de Creación:	**20-10/2017**	Fecha de Actualización:	
Numero Documento :	**Política 15**	Departamento:	**TIC´S**
Nombre Documento:	**POLÍTICA DE DETECCIÓN DE VIRUS**		
Elaborado Por:	**Wilmar Andrés Duarte Ortiz**		
Aprobado por:			
observaciones:			
Política	El propósito de la política de detección de virus es prevenir que los usuarios pierdan información por causas de los virus que vienen en los correos que nos envían desde internet.		
Normatividad	• El personal de la institución universitaria no debe abrir correo que no sean de personas o contactos conocidos • El antivirus de la institución universitaria debe actualizarse cada día, se debe llevar un reporte de los virus maliciosos si este encuentra en la red para así llevar un proceso de control y eliminación de este. • No se deben utilizar memorias usb o medios magnéticos en los equipos de la institución universitaria que no sean de la organización, si por algina razón se debe implementar una de estas se deberá informar al área de las tic´s para que hagan su respectiva análisis y determinar si se puede o no usar esta esto con el fin de prevenir de algún virus en la red de la organización.		

9. IMPLEMENTACION DE ESTRATEGIAS, MECANISMOS DE CONTROL Y GESTIÓN DE RIESGOS

La generación de políticas de seguridad en el área de Tic´s de cualquier organización, son la estructura principal para el buen control y funcionamiento de todos los procesos internos que se manejen en ella.

El tener bien definido que procesos se manejan en el Departamento de las Tic´s de la institución, facilita tener claro la creación de las políticas de seguridad. Dichas políticas deben ser claras y concretas para poder realizar un buen diligenciamiento y Seguimiento.

Las políticas de Seguridad de Unicomfacauca son un gran apoyo en el proceso de Gestión de Calidad que se lleva dentro de la organización (ISO 9001).

A continuación se describe el seguimiento que se ha realizado a las políticas de Seguridad, sugeridas al departamento de Tic´s de Unicomfacauca.

Política 1

Unicomfacauca aplicará políticas, prácticas, procedimientos y guías, para proteger los datos internos, y así prevenir errores de programación, mal manejo por individuos dentro o fuera de la Universidad. Esto con la finalidad de proteger a la Universidad de riesgos que comprometan la integridad de los programas, estos serán responsables y adaptables a los cambios tecnológicos que afecten los Recursos de Información.

Verificación Política 1

Esta Política se está ejecutando en los desarrollos generados para el proceso de la Universidad pro no se está Documentando, Los desarrollos principales como el SIGA son verificados por las empresas que los venden, por medio de cláusulas de cumplimiento

Política 2

El propósito de este procedimiento es dar los lineamientos básicos para la elaboración de los archivos y manuales de gestión de evaluación del buen uso de la red.

Verificación Política 2

Este Procedimiento ya se está efectuando con software específico como IPTRAF y el SQUID y las copias de seguridad con CRONTAB. Los registros encontrados se almacenan para verificar y comprar, mas no se está documentando.

Política 3

El propósito de la Política de Uso de Internet es establecer lineamientos de acceso y uso de Internet para: proporcionar, buscar e intercambiar información de todas las áreas y así dar apoyo con la calidad y el nivel que requiere la continuidad operativa de la Institución, aprovechando eficaz y eficientemente la infraestructura de red conforme a la normatividad aplicable y las políticas institucionales.

Verificación Política 3

Esta política se realiza mediante control de acceso al servicio de internet tanto como para Administrativos, Docentes y Alumnos, para realizar dichas restricciones se utiliza el software SQUID Y UNTANGLE, pero no se está documentando.

Política 4

El propósito de la política para la administración de contraseñas es establecer las reglas para la creación, distribución, protección y terminación de los mecanismos de autenticación del usuario para ejecutar los recursos de información.

Verificación Política 4

Para la creación y custodia de las contraseñas se generan de la siguiente forma.

a. Para la creación de contraseñas se utiliza patrones generados por combinación de palabras, números y eventos.

b. Las custodias de las contraseñas se almacenan en caja Fuerte.

Si está documentado este proceso.

Política 5

El propósito de la política de administración de la cuentas es establecer las reglas para la creación, seguimiento, control y eliminación de cuentas de usuario.

Verificación Política 5

Este control de usuarios se está realizando en las creaciones de cuentas en el sistema SIGA y ZIMBRA, pero no hay directorios activos, para el control de los administrativos y Docentes.

Política 6

Esta política tiene como propósito proporcionar un nivel de seguridad y control sobre el acceso y gestión de los servidores de Unicomfacauca. Se define quién tendrá acceso al servidor, y quienes tendrán acceso a modificar su contenido y su respectiva documentación, también se define quien será notificado cuando se realizan cambios en los servidores.

Verificación Política 6

Se tiene claro quién es la persona encargada del acceso a los servidores y quienes tienen acceso limitado, algunos servicios. Pero no se ha documentado.

Política 7

Esta política se crea como marco regulatorio en donde se definen los procedimientos para instalación manipulación y uso responsable de las herramientas software licenciadas, adquiridas por Unicomfacauca y da a conocer a los usuarios el alcance de lo permitido y lo prohibido de las licencias software a su disposición.

Verificación Política 7

Se está realizando documentos informativos para Administrativos, Docentes y Alumnos para que tengan claro que es lo que se puede instalar y que uso se puede dar. Si se está documentando.

Política 8

El propósito principal de este procedimiento es certificar que al acceder a algún recurso por parte de personal ajeno a la administración del mismo, este solo pueda modificar los archivos, aplicaciones y/o servicios que previamente hayan sido autorizados.

Verificación Política 8

Se está realizando en el área contable y copias de seguridad, hay personal que tiene diferentes tipos de acceso a esta información.

El los servidores también tienen diferente tipo de acceso. No se ha documentado.

Política 9

La Política de Administración de Incidentes (tickets) tiene como propósito resolver cualquier incidente que cause una interrupción en el servicio de la manera más rápida y eficaz posible.

Verificación Política 9

No se tiene un sistema de Help Desk, pero tienen un sistema de correo para la solicitud de soporte, se deja la recomendación para implementar un sistema de Tickets.

Política 10

La finalidad de esta política es garantizar o minimizar al máximo los riesgos, fallas, o robo de información que se puedan llegar a presentar por el acceso no autorizado de un intruso durante el proceso normal de funcionamiento de los equipos en general (Hardware y software).

Verificación Política 10

Se tienen registro del Hardware y Software en medios físicos (Hojas) y también los controles de mantenimientos. Se recomienda sistematizar este servicio para un mejor desarrollo del proceso.

Política 11

Los recursos son bienes estratégicos de la Universidad tecnológica de Comfacauca que deben ser manejados como recursos valiosos, por tal razón se hace necesario generar una serie de regulaciones y normas que busquen orientar a toda la comunidad universitaria sobre el buen uso que se le debe de dar teniendo en cuenta la disposición de los usuarios en Unicomfacauca.

Verificación Política 11

Si se está realizando esta política de seguridad, cuando el funcionario es contratado se le hace firmar un contrato, el cual le indica que los bienes informáticos son parte de la organización y como tal tiene que velar por el buen uso de ellos. Si se encuentra documentado.

Política 12

La Política de acceso fisco a los recursos tiene como propósito definir la responsabilidad de los actores que tienen algún vínculo con los activos de información y el acceso a ella, tanto interna como externamente.

Verificación Política 12

Los equipos de la Universidad se encuentran protegidos con garantías con el proveedor de venta ante bajones de energía, daños físicos y lógicos.

La Universidad tiene póliza de seguro contra los equipos de cómputo ante catástrofes. Los servidores tienen sistemas de UPS. Si se encuentra documentado.

Política 13

El propósito de esta política es establecer las reglas para el acceso y uso de la infraestructura de la red. Estas reglas son necesarias para preservar la integridad, disponibilidad y confidencialidad de la información de la Unicomfacauca.

Verificación Política 13

Nadie en la Universidad tiene el derecho de hacer modificaciones internas en los equipos informáticos, sin la autorización del Coordinador del área de Tic´s. No se encuentra documentado.

Política 14

La política de Entrenamiento y Capacitación en Seguridad se diseña con el fin de asegurarse de que el personal que este en contacto con el área Tic´s reciban un adecuado entrenamiento sobre el comportamiento de los recursos computacionales.

Verificación Política 14

Se están realizando capacitaciones al personal de Tic´s, para el buen uso de las herramientas informáticas de la Universidad. Si se encuentra documentado.

Política 15

El propósito de la política de detección de virus es prevenir que los usuarios pierdan información por causas de los virus que vienen en los correos que nos envían desde internet.

Verificación Política 15

Se tiene control de los virus con software licenciado y se tiene control de los equipos por medio de una consola centralizada y con complementos para minimizar posibles daños en la información y las maquinas.

10. RESULTADOS

Al desarrollar este proyecto de grado, la Institución Universitaria Tecnológica de Unicomfacauca, tendrá una guía que les brindara las herramientas para la construcción, implementación de políticas de seguridad y procedimientos del SGSI.

El área de las TIC´s de la institución universitaria tendrá en conocimiento las matrices de los activos identificados, clasificados y valorados, posteriormente tendrá a su disposición la matriz con las amenazas y riesgos que presentan en la actualidad la institución universitaria.

11. CONCLUSIONES

Teniendo en cuenta el proceso de estudio que se llevó a cabo, el cual fue realizado con la metodología SP-830 al área de TIC´s de Unicomfacauca, se logró como resultado del proceso de diagnóstico, identificando factores de riesgo los cuales se consideran muy importantes ya que permitieron realizar un análisis y evaluación acerca del estado actual que se presenta en cuanto la seguridad de la información en la red de datos de la Institución Universitaria Tecnológica de Comfacauca.

Dentro de los factores encontrados y haciendo referencia a posibles amenazas de las bases de datos, información, aplicaciones adquiridas y de propiedad de la institución y de conformidad con lo establecido en la norma ISO 27001:2013, hay que tener en cuenta que se debe cumplir la norma indicada para trabajar con cableado estructurado en los centros de cableados principales y secundarios de la institución, para no tener percances ni traumatismos en el tránsito de la información y ampliaciones en la red. Las normas a tener en cuenta son:

ANSI/TIA/EIA-568-B: Cableado de Telecomunicaciones en Edificios Comerciales. (Cómo instalar el Cableado)

- ✓ TIA/EIA 568-B1: Requerimientos generales
- ✓ TIA/EIA 568-B2: Componentes de cableado mediante par trenzado balanceado
- ✓ TIA/EIA 568-B3: Componentes de cableado, Fibra óptica

ANSI/TIA/EIA-569-A: Normas de Recorridos y Espacios de Telecomunicaciones en Edificios Comerciales.
ANSI/TIA/EIA-570-A: Normas de Infraestructura Residencial de Telecomunicaciones
ANSI/TIA/EIA-606-A: Normas de Administración de Infraestructura de Telecomunicaciones en Edificios Comerciales
ANSI/TIA/EIA-607: Requerimientos para instalaciones de sistemas de puesta a tierra de Telecomunicaciones en Edificios Comerciales.
ANSI/TIA/EIA-758: Norma Cliente-Propietario de cableado de Planta Externa de Telecomunicaciones.

En cuanto a los mecanismos de control y gestión de riesgos que permiten disminuir los riesgos encontrados, se evidencia que se requiere dentro de la institución el establecimiento de políticas de seguridad de la información a fin de controlar, mitigar y prevenir los riesgos que puedan presentarse, adicionalmente, es importante y necesaria, la adecuación de los espacios físicos, teniendo en cuenta la normatividad vigente. Es así como se hizo necesaria la creación de formatos de control y administración de las políticas de seguridad de la Institución Universitaria, basándose en el anexo A del estándar ISO 27001:2013 cuyo objetivo fue verificar si la institución cumplía o

no con los controles y los dominios de este anexo encontrando un incumplimiento en varios de los controles aplicados.
De esta manera y según el resultado obtenido, se realizó la creación y consolidaron de los mecanismos de control y las políticas de seguridad de la información, las cuales serán entregadas a la institución y servirán como insumo necesario para fortalecer el área de las TIC´S mediante acciones de control, mitigación y prevención de vulnerabilidades en la red de datos.

Recomendaciones

Para la aplicación de las políticas de seguridad planteadas en el presente documento, se recomienda capacitar a todos los usuarios que hacen parte de la institución Universitaria puesto que la seguridad de la información es responsabilidad de todos.

Se recomienda a la institución, adecuar los espacios físicos especialmente del área de las Tic´s donde se encuentran los equipos tecnológicos, de acuerdo a la normatividad vigente, con el fin de contrarrestar alteraciones, daños y demás situaciones de riesgo que puedan presentarse.

Es importante implementar las políticas de seguridad propuestas, ya que estas buscan ayudar a la institución a mitigar y prevenir riesgos de la información de la institución.

Se recomienda que los colaboradores del área de las Tic´s cumplan con un perfil profesional apropiado para el área, con el fin de ser bien administrada el área.

Finalmente se recomienda que dentro de la Institución Universitaria se realicen constantes actualizaciones tecnológicas en cuanto al software y hardware teniendo en cuenta derechos de autor y respetando el uso de software legal para prevenir vulnerabilidades en los sistemas.

DIVULGACIÓN

La divulgación del presente proyecto se realizará por los medios dispuestos por la UNAD y será entregado a la organización, con el fin de ser un recurso que permita la consulta del área de las TIC´s y los usuarios de la institución en lo referente al desarrollo, resultados y recomendaciones obtenidos durante su proceso.

BIBLIOGRAFÍA

ALBERTO G. Alexander. Implantación de la ISO 27001:2005 Sistema de Gestión de Seguridad de la Información. 2014. Disponible en http://www.iso27000.es/download/Implantacion_del_ISO_27001_2005.pdf

Alcaldía de Bogotá. Ley 1273 de 2009 Nivel Nacional. (Consultado el 14 de Noviembre de 2017). Disponible en http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

Alcaldía de Bogotá. Ley 1581 de 2012 Nivel Nacional. (Consultado el 14 de Noviembre de 2017).Disponible en http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

Alcaldía de Bogotá. DECRETO 1377 DE 2013. (Consultado el 14 de Noviembre de 2017). Disponible en http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646

ARDILA NAVARRETE, Julián Andrés. Diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001 para Positiva Compañía de Seguros S.A en la ciudad de Bogotá. 2016. Universidad Nacional Abierta y a Distancia de Colombia. Disponible en http://hdl.handle.net/10596/11980

ABALCO MAILA, David Elías y RUILOVA SANDOVAL, Romel Ruperto. Elaboración del plan de seguridad de la información para el fondo de cesantía y jubilación del mdmq. Disponible en http://bibdigital.epn.edu.ec/bitstream/15000/10391/1/CD-6182.pdf

BENÍTEZ, Moisés. Políticas de Seguridad Informática. 2013. Disponible en http://www.gestionintegral.com.co/wp-content/uploads/2013/05/Pol%C3%ADticas-de-Seguridad-Inform%C3%A1tica-2013-GI.pdf

BERNAL Jorge Jimeno. Ciclo PDCA (Planificar, Hacer, Verificar y Actuar): El círculo de Deming de mejora continúa (en línea). España: el autor, 2013 (citado el 20 de noviembre de 2017). Disponible en: http://www.pdcahome.com/5202/ciclo-pdca/

Contreras Esguerra, Lidia Constanza. Diseño de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/iec 27001 para la dirección de sistemas de la gobernación de Boyacá. Tesis de grado Especialista en Seguridad Informática. Tunja: Universidad Nacional Abierta y a

Distancia. 2016. (consultado el 05 de Noviembre de 2017). Disponible en http://hdl.handle.net/10596/11895

Ecured. Seguridad informática. (Consultado el 15 de Septiembre de 2017). Disponible en https://www.ecured.cu/Seguridad_Inform%C3%A1tica

Galeon.com. seguridad informática. (Consultado el 15 de Septiembre de 2017). Disponible en http://audisistemas2009.galeon.com/productos2229098.html

García Balaguera, Vivian Andrea y Ortiz González, Jhon Jarby. Análisis de riesgos según la norma ISO 27001:2013 para las aulas virtuales de la Universidad Santo Tomás modalidad presencial. Tesis de grado Especialista en Seguridad Informática. José Acevedo Gómez: Universidad Nacional Abierta y a Distancia. 2016. (consultado el 05 de Noviembre de 2017). Disponible en http://hdl.handle.net/10596/12028

GÓMEZ, Á. (2014). Auditoría de seguridad informática. Recuperado de Universidad Nacional Abierta y a Distancia de Colombia: http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/detail.action?docID=11046412

ISO/IEC 27001:2005 Information technology — Security techniques — Information security management systems – Requirements

ISO/IEC 27005:2008 Information technology — Security techniques — Information security risk management

ISO/IEC 27006:2007 Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems

ISO/IEC 27002:2005 Information technology — Security techniques — Code of practice for information security management (anterior ISO/IEC 17799:2005)

ISO/IEC 13335-1:2004, Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management

ISO/IEC TR 13335-3:1998, Information technology — Guidelines for the management of IT Security — Part 3: Techniques for the management of IT security

ISO/IEC TR 13335-4:2000, Information technology — Guidelines for the management of IT Security — Part 4: Selection of safeguards

ISO 14001:2004, Environmental management systems — Requirements with guidance for use

ISO/IEC TR 18044:2004, Information technology — Security techniques — Information security incident management

ISO 19011:2002, Guidelines for quality and/or environmental management systems auditing

MAYA ARANGO, Paula Andrea. (06 de junio de 2016). Plan de implementación del SGSI basado en la norma ISO 27001:2013. Recuperado de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/53466/8/pmayaaTFM0616memoria.pdf

Metodoss. Metodología PDCA – Ciclo Deming. Disponible en https://metodoss.com/metodologia-pdca-ciclo-shewhart-deming/

Ministerio De Tecnologías De La Información Y De Las Telecomunicaciones. Ley 1273 de 2009. (Citado el 14 de noviembre de 2017). Disponible en: http://www.mintic.gov.co/portal/604/w3-article-3705.html

Ministerio De Comercio Industria Y Turismo. Decreto 1377 del 27 de junio de 2013. (Citado el 14 de noviembre de 2017). Disponible en: http://www.mintic.gov.co/portal/604/articles-4274_documento.pdf

NIST. Risk Management Guide for Information Technology Systems Julio de 2002. (Consultado EL 02 DE noviembre de 2017). Disponible en: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

OCAMPO GARCIA, Darley. (2015). Modelo de Seguridad de la Información para las Entidad Publicas del Estado Colombiano. Recuperado de Universidad Piloto de Colombia: http://polux.unipiloto.edu.co:8080/00002024.pdf

Pulido Barreto, Ana Milena Mantilla y Rodríguez, Jenith Marsella. Modelo para la implementación del sistema general de seguridad informática y protocolos de seguridad informática en la oficina TIC de la alcaldía municipal de Fusagasugá, basados en la gestión del riesgo informático. Tesis de grado Especialista en Seguridad Informática. Arbeláez: Universidad Nacional Abierta y a Distancia. 2016. (consultado el 05 de Noviembre de 2017). Disponible en http://hdl.handle.net/10596/6327

REINA GARCÍA, Elkin y MORALES RAMÍREZ, José Raúl. Modelamiento de proceso basado en el grupo de normas internacionales ISO/IEC 27000 para gestionar el riesgo y seleccionar controles en la implementación del sistema de gestión de seguridad de la información. 2014. Recuperado de Universidad Tecnológica de Pereira: http://hdl.handle.net/11059/4894

REYES SILVA, Eudrey Didney. (2013) .Metodología para realizar una auditoría de sistemas a la seguridad de la información bajo la norma Iso/iec 27002:2007, como modelo para ser aplicada por empresas de desarrollo de software. Recuperado de Universidad Antonio Nariño de Colombia: http://www.uan.edu.co/images/programas-posgrados/Esp_Auditoria_sistemas/documentos/2013_II/METODOLOGIA_PARA_REALIZAR_UNA_AUDITORIA_DE_SISTEMAS_A_LA_SEGURIDAD_DE_LA_INFORMACION_BAJO_LA_NORMA_ISO.pdf

ROMERO USSA, Katherine Astrid. (2015). Gestión de la seguridad y el riesgo de TI. Recuperado de Universidad Piloto de Colombia: http://polux.unipiloto.edu.co:8080/00002222.pdf

SOLARTE SOLARTE, Francisco Nicolás (06 de julio de 2016).). Sistema de gestión de la seguridad de la informática. Disponible en http://blogsgsi.blogspot.com.co/2016/07/sgsi.html

Tola Franco, Diana Elizabeth. Implementaciones un sistema de gestión de seguridad de la información para una empresa de consultoría, aplicando la norma ISO/IEC 27001. Tesis de grado. Escuela Superior Politécnica del Litoral (ESPOL).Quito–Ecuador (consultado el 05 de Noviembre de 2017). Disponible en http://www.dspace.espol.edu.ec/xmlui/handle/123456789/31114

Unicomfacauca (2017).Inicio. Corporación. Quienes Somos. (Consultado el 20 de Agosto de 2017). Disponible en http://www.unicomfacauca.edu.co/index.php/institucion/2013-05-09-23-07-45#rese%C3%B1a-hist%C3%B3rica

Universidad Nacional Autónoma de México. Seguridad informática. (Consultado el 15 de Septiembre de 2017). Disponible en http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/Ataques.php