# DISEÑO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA BASADAS EN LA NORMA NTC-ISO-IEC 27001:2013 PARA LA UNIVERSIDAD DE CARTAGENA CENTRO TUTORIAL MOMPOX BOLÍVAR.

MANUEL ESTEBAN URECHE OSPINO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
MAGANGUE BOLIVAR
2017

# DISEÑO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA BASADAS EN LA NORMA NTC-ISO-IEC 27001:2013 PARA LA UNIVERSIDAD DE CARTAGENA CENTRO TUTORIAL MOMPOX BOLÍVAR

MANUEL ESTEBAN URECHE OSPINO

PROYECTO PARA OBTENER EL TÍTULO DE ESPECIALISTA EN SEGURIDAD INFORMÁTICA

MSC ING. LORENA OCAMPO CORREA
ASESOR ENCARGADO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
MAGANGUE BOLIVAR
2017

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Magangué Bolívar 06-04-2017

## A Dios

Por haberme permitido llegar hasta este punto y haberme dado salud para lograr mis objetivos, además de su infinita bondad y amor. Que permitieron avanzar y seguir adelante en este proyecto profesional.

## A mi Esposa Carmen Chacón e Hija

Por haberme apoyado en todo momento, a superar cada uno de los obstáculos que se presentaron en el desarrollo y transcurrir de mis estudios, por su comprensión en los momentos que deje de compartir con ellas por dedicarle esfuerzo y dedicación a este proyecto.

## A mi Mama Nuris Ospino y Hermanos

Por los ejemplos de perseverancia y constancia que la caracterizan y que me ha infundido siempre, por el valor mostrado para salir adelante y por su amor.

## AGRADECIMIENTOS

El presente trabajo de Grado primeramente me gustaría agradecerte a ti Dios por tus maravillas que son infinitas y bendecirme para hacer realidad este logro, porque hiciste realidad este sueño anhelado. A la Universidad Nacional Abierta y A Distancia Unad por darme la oportunidad de estudiar y ser un Especialista en seguridad Informática.

A mi Asesora de tesis, MSC ING. Lorena Ocampo Correa por su esfuerzo y dedicación, quien con sus conocimientos, su experiencia, su paciencia y su motivación ha logrado en mí que pueda terminar mi proyecto con éxito. También me gustaría agradecer a mis profesores durante todo mi posgrado porque todos han aportado con un granito de arena a mi formación, su enseñanza y más que todo por su amistad.

A mi esposa Carmen Chacón e Hija que me han apoyado mucho en la consecución de este logro, las he visto en mis alegrías y mis tristezas, depositando toda su confianza y dedicación en cada uno de los sueños que nos hemos proyectado como familia.

A mi pastora Elka Pérez y José Pérez que  son como unos padres para mí, los cuales me han motivado y apoyado durante mi formación profesional. Son muchas las personas que han formado parte de mi vida profesional a las que me encantaría agradecerles su amistad, consejos, apoyo, ánimo y compañía en los momentos más difíciles de mi vida. Algunas están aquí conmigo y otras en mis recuerdos y en mi corazón, sin importar en donde estén quiero darles las gracias por formar parte de mí, por todo lo que me han brindado y por todas sus bendiciones.

**TABALA DE CONTENIDO**

Pág.

## LISTA DE TABLAS

Pág.

## LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

# RESUMEN

El presente trabajo de grado tiene como propósito diseñar las políticas de seguridad informática para Universidad de Cartagena Centro Tutorial Mompox, Teniendo en cuenta el análisis de riesgos y vulnerabilidades, tomando como referencia la norma NTC-ISO-IEC 27001:2013, es por ello que en este proyecto se platea el diseño de las políticas de seguridad informática. El propósito de este proyecto es proporcionar y garantizar la seguridad de la información de los recursos informáticos de la Universidad de Cartagena Centro Tutorial Mompox.

El proyecto se apoya en estudios realizados a los estudiantes de la Universidad de Cartagena Centro Tutorial Mompox y personal administrativo, donde se desarrollaron varias entrevistas al personal que administra el área de sistemas y recursos informáticos, de acuerdo a la información levantada se tomó una muestra de acuerdo a las necesidades de seguridad, utilizando estadística no probabilística donde se evidencia que no existen políticas de seguridad informática que se apliquen para este centro tutorial.

De acuerdo a lo anterior es importante destacar que la seguridad de la información y las políticas de seguridad informática tiene un papel importante en cualquier Universidad de estudios superior en el país, por ello es importante desarrollar las mejores prácticas de seguridad, con el fin de mantener un alto nivel de protección de la información.



Palabras claves: Seguridad informática, instituciones de educación superior, políticas, vulnerabilidades, amenazas, riesgo, norma NTC-ISO-IEC 27001:2013.

ABSTRACT

This degree work has the purpose designing security policies for University of Cartagena Center Tutorial Mompox, Considering the analysis of risks and vulnerabilities, with reference to the NTC-ISO-IEC 27001: 2013, which is why in this project the design of security policies silvers. The purpose of this project is to provide and ensure the information security of the information resources of the University of Cartagena Mompox Tutorial Center.

The project is based on studies students at the University of Cartagena Center Tutorial Mompox and administrative staff, where interviews were developed staff that manages the area of computer systems and resources, according to the information raised a sample was taken according to security needs, using statistical probabilistic no evidence where there are no security policies that apply to this tutorial center.

According to the above it is important to note that the security of information and security policies have an important role in any university higher studies in the country, so it is important to develop the best security practices in order to maintain a high level of protection of information.

Keywords: Computer Security, higher education institutions, policies, vulnerabilities, threats, risk, standard NTC-ISO-IEC 27001: 2013.

# 1. INTRODUCCIÓN

En nuestros días ya no es fácil trabajar sin estar a la vanguardia de la tecnología y lo que ella aporta para el funcionamiento de las empresas, con el uso del Internet, cada vez más compañías permiten a sus socios y proveedores acceder a sus sistemas de información. Por lo tanto, es fundamental saber qué recursos de la compañía necesitan protección para así controlar el acceso al sistema y los derechos de los usuarios del sistema de información. Los mismos procedimientos se aplican cuando se permite el acceso a la compañía a través de Internet.

Cada vez más empresas en el mundo capacitan a sus empleados en la formación tecnológica que busca mejorar cada uno de los procesos que se realizan dentro de las compañías Además, debido a la tendencia creciente hacia un estilo de vida nómada de hoy en día, el cual permite a los empleados conectarse a los sistemas de información casi desde cualquier lugar, se pide a los empleados que lleven consigo parte del sistema de información fuera de la infraestructura segura de la compañía.

Hoy en día hay empresas que han fracasado o dejado de funcionar por un descuido en el acceso al tesoro más valioso de ella la información, la seguridad informática es un tema al que mucha gente no le da la importancia, muchas veces por el hecho de considerar que es inútil o que jamás la utilizaran. Pero en el mundo moderno, cada día más y más personas mal intencionadas intentan tener acceso a los datos de nuestros ordenadores.

Con este proyecto se busca proponer políticas de seguridad para la Universidad de Cartagena Centro Tutorial Mompox Bolívar. Con el fin de que se realice una buena política de seguridad informática es necesario que se delegue por parte de la organización los usuarios que tendrán privilegios para acceder a la información, donde tendrán controles, restricciones e identificaciones de estos funcionarios, en lo posible que se establezca un protocolo para acceso a la información cuando se trate de personal ajeno a la organización.

## 2. TITULO

# DISEÑO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA BASADAS EN LA NORMA NTC-ISO-IEC 27001:2013 PARA LA UNIVERSIDAD DE CARTAGENA CENTRO TUTORIAL MOMPOX BOLÍVAR.

# 3. OBJETIVOS

## 3.1 OBJETIVO GENERAL

- Diseñar políticas de seguridad informática para la Universidad de Cartagena Centro Tutorial Mompox Bolívar, tomando como referencia la norma NTC-ISO-IEC 27001:2013.

## 3.2 OBJETIVOS ESPECÍFICOS

- Identificar la situación actual de los sistemas de la Universidad Cartagena Centro Tutorial Mompox.

- Levantar la información de los activos del departamento de Tecnología de la Universidad de Cartagena centro Tutorial Mompox.

- Realizar el Análisis de riesgos basado en la norma NTC-ISO-IEC 27001:2013.

# 4. PLANTEAMIENTO DEL PROBLEMA

## 4.1 DEFINICIÓN DEL PROBLEMA

Debido a las múltiples amenazas y riegos que se presentan con los constantes cambios tecnológicos en los sistemas informáticos de nuestros días, se hace necesario que en las universidades públicas y privadas cuenten con estrategias de seguridad, basadas en los riesgos detectados en el análisis de vulnerabilidad del sistema, que deben ir de la mano con las necesidades de las institución. Esto con el firme propósito de diseñar políticas de seguridad informática que apoyen y fortalezcan los objetivos estratégicos de la Universidad de Cartagena Centro Tutorial Mompox Bolívar.

Las políticas de seguridad informática representan una herramienta de gran utilidad Para la administración de la seguridad en las instituciones, ya que estas permiten establecer controles y procedimientos a cada uno de los procesos desarrollados en la entidad.

Con la implementación de las políticas de seguridad en la Universidad de Cartagena Centro Tutorial Mompox, se fomenta el sentido de pertenencia y empoderamiento en temas de seguridad, de tal forma que se logra la participación activa de todos los funcionarios en la identificación, definición, e implementación de medidas que busquen mejorar la seguridad de la información.

La implementación de políticas de seguridad informática requiere inicialmente que se realice un proceso de identificación de riegos y vulnerabilidades de seguridad que están vinculados con la información para que posteriormente se analicen los mecanismos que nos permitan preservarla y conservarla.

Con base en el diagnóstico que se ilustra a continuación en la figura 1. Identificación de la situación problema, apoyado en los resultados de las entrevistas que se le realizaron a cada uno de los funcionarios y estudiantes de la misma, la Universidad de Cartagena Centro Tutorial Mompox requiere implementar políticas de seguridad informática que permita mejorar la seguridad de la información que se produce en este centro tutorial, teniendo en cuenta que actualmente se presenta perdida de la información que se genera en este cread de la Universidad de Cartagena.

De acuerdo a lo anterior, se evidencia que el problema está asociado a:

- No se cuenta con una administración de seguridad informática en el centro Tutorial Mompox que lidere e identifique riesgos y vulnerabilidades que puedan afectar la seguridad de la información.

- Se denota falta de conocimiento, empoderamiento y concientización por parte del personal administrativo en temas relacionados con seguridad de la información.

- Se tiene problemas relacionados con integración activa de toda la universidad, para aplicar los debidos controles, apoyados en la evaluación de riesgos.

- No se tiene implementado un sistema que permita la gestión y valoración adecuada de riesgos y vulnerabilidades de seguridad.

- No existe una orientación desde la alta dirección para que las políticas de seguridad estén alineadas con los objetivos de la Institución.

- No se cuenta con formación e inducción a tutores sobre el manejo y conservación de los trabajos realizados por los estudiantes.

- El acceso al sistema presenta su mayor vulnerabilidad en los estudiantes, ya que no se aplica ninguna política de seguridad informática direccionada al personal que hace uso del centro tutorial.

## 4.2 DIAGNOSTICO SITUACION PROBLEMA

Teniendo en cuenta el análisis del estado de las políticas de la seguridad de la Universidad que incluye la identificación de aquellos riesgos que afectan la seguridad de la información, mediante la siguiente figura se ilustra la identificación de la situación problema en la entidad.

**Figura 1. Identificación de situación problema.**


**Fuente: El Autor**

En la siguiente tabla se muestra aquellos factores que se presentan en la universidad y que tiene que ver con aquellas situaciones que generan problema en la entidad.

Tabla 1. Factores Asociados a la Situación Problema

| Situación | Factores |
|---|---|
| No se cuenta con una administración adecuada de seguridad en la entidad. | ❖ No existe una instrucción por parte de la rectoría de la entidad en lo que respecta a seguridad de la información.<br>❖ Se evidencia poca participación de la rectoría de la entidad en temas de seguridad de la información. |
| Poca cultura de seguridad de la información | ❖ Los trabajadores de la entidad no tiene claro la diferencia entre seguridad de la información y seguridad informática.<br>❖ Se observa desinterés en los trabajadores en temas de seguridad<br>❖ No se aplica la mejora continua en lo que tiene que ver con seguridad de la información. |
| En la actualidad no se cuenta con un sistema de información que implique la gestión de riesgos de seguridad | ❖ No existe identificación de riesgos y controles de seguridad.<br>❖ Se tienen problemas para identificar y clasificar los activos y controles de información.<br>❖ La universidad no ha reglamentado a nivel de centro tutoriales el estado de seguridad para cada uno de ellos.<br>❖ No se tiene un sistema de información definido para la gestión de riesgos de seguridad. |
| No existen políticas de seguridad informática que estén alineadas a la misión y visión de la universidad. | ❖ Es necesario establecer las funciones de seguridad información y seguridad informática.<br>❖ Las políticas de seguridad informática son establecidas por la administración o dirección de tecnologías de la entidad. |

Fuente. Autor

## 4.3 INDICADORES DEL PROBLEMA

A continuación encontraremos los indicadores que se establecen con el propósito de identificar el estado actual de la situación problema:

Tabla 2. Indicadores del Problema

| **Indicador** | **Objetivo del Indicador** |
|---|---|
| Eficacia en tratamiento de riesgos. | Evidencia el grado de eficacia de la gestión de los tratamientos de los riesgos en la Universidad. |
| Nivel de responsabilidades y compromisos de seguridad informática. | Determina el grado de compromiso que tiene cada funcionario de la entidad y que quedan consignadas en el manual de políticas de información. |
| Establecer planes de tratamientos de riesgos de seguridad. | Muestra el nivel de cobertura que tienen los planes de seguridad de la información. |
| Concientización e importancia de las políticas de seguridad informática. | Evidencia el grado de cumplimiento de la sensibilización y capacitación en políticas de seguridad informática. |

Fuente. El Autor.

## 3.4 FORMULACIÓN DEL PROBLEMA

¿De qué manera la Universidad de Cartagena Centro Tutorial Mompox puede asegurar el manejo de la información apoyado en la norma NTC-ISO-IEC 27001:2013?

# 5. JUSTIFICACIÓN

La Universidad de Cartagena es una de las universidad públicas del país de gran prestigio y reconocimiento, certificada en calidad con gran reconocimiento nacional, por ende la importancia de la implementación de este proyecto, ya que busca mitigar los riesgos y vulnerabilidades que se presentan en uno de sus centro de formación; es importante decir o destacar que la seguridad de la información juega un papel importante dentro de las organizaciones, por medio de ella se protegen el activo más importante de la Institución que es la información.

Actualmente la información tiene mucha trascendencia, ya que una empresa que no tenga control de todo lo que genera sus sistemas informáticos, lo más seguro es que sea vulnerable y susceptible a cualquier pérdida o robo de la misma. Esto ha determinado que la seguridad informática tenga importancia en nuestros días, garantizando la disponibilidad, integridad y confidencialidad de la información cuando se cuenta con sistemas protegidos.

Para este proyecto se proponen políticas de seguridad informática buscando evitar posibles vulnerabilidades y riesgos de seguridad de la información al interior de la Universidad de Cartagena centro tutorial Mompox. Este proyecto se fundamenta en criterios y propuestas de solución en cuanto a políticas de seguridad se refiere donde se busca garantizar el correcto funcionamiento de los sistemas de información y bases de datos de la Universidad.

Con respecto a la Universidad de Cartagena Centro Tutorial Mompox, es importante que se establezcan e implementen las políticas de seguridad informática, ya que esto garantiza la confianza de cada uno de los estudiantes de municipio y de los pueblos ribereños, que han puesto su confianza en esta universidad para formarse profesionalmente en cada uno de los programas que el alma mater ofrece.

Es tan importante el tema de la seguridad de la información en las organizaciones que muchos pensadores como el señor George Beekman (1996) coinciden en decir que la información es la herramienta que hace fuerte a una empresa, por ello se dice que el tema seguridad informática constituye un tema de mucha importancia, en la medida en que avanza la tecnología y las investigaciones que presentan nuevos riesgos sobre los sistemas de cómputos. Las personas o usuarios utilizan la información para diferentes fines ya sean buenos o malos, por tal motivo se busca que las instituciones públicas como la Universidad de Cartagena tengan mayor preocupación por proteger sus sistemas informáticos.

Este proyecto es importante porque en la actualidad la seguridad no es un lujo de las organizaciones, es una necesidad, debido a que es el activo más valioso que tiene cada empresa para brindar una buena imagen y prestigio dentro de la sociedad; es por ello que se puede considerar que al implementar políticas de

seguridad en una organización se fortalece la seguridad delos sistemas informáticos ante accesos no deseados y lo más importante que cada uno de los usuarios de este campus Universitario se sientan seguros de que sus prácticas, proyectos, redes e información se le está dando el uso correcto dentro del alma mater.

# 6. MARCO REFERENCIAL

## 6.1 MARCO TEÓRICO

Con el avance y crecimiento que ha tenido la tecnologías de la información en los últimos tiempos, que obliga a las organizaciones a hacer un esfuerzo en cuanto a seguridad de la información se refiere, teniendo en cuenta que cada día son más complejas, especializadas y avanzadas, por otro lado la normatividad vigente exige y demanda mayor privacidad y protección sobre la información sensible que se produce en las organizaciones.

La elaboración de políticas de seguridad informática se desarrollan de acuerdo a los objetivos estratégicos de la entidad, orientado a una estructura organizacional que busca establecer responsabilidades dentro de las que se abordan procesos y procedimientos que permitan identificar de manera eficiente los riesgos y vulnerabilidades que atenten contra la seguridad de la información, destacando la disponibilidad, trazabilidad, integridad, autenticidad, no repudio entre otras.

Este proyecto está enfocado en realizar las Políticas de seguridad informática en una institución académica de educación superior en la ciudad de Mompox Bolívar. Actualmente la ciudad presenta un crecimiento comercial, generado por las construcciones de varios edificios, urbanizaciones, hoteles, por ser una de las ciudades turísticas que tiene la región de la mano con la orfebrería y costumbres culturales de la misma. Son muchos los estudiantes de los Municipios vecinos que le apuestan a esta ciudad para formarse profesionalmente en una de las mejores universidades de la costa atlántica.

Por esta razón es importante que instituciones como la Universidad de Cartagena centro tutorial Mompox, que desarrolla una labor académica importante en la región, en los diferentes programas ofertados por la misma y que tiene presencia en este Municipio de bolívar, diseñe las políticas de seguridad informática que garanticen el sostenimiento y confiabilidad de cada uno de los datos generados al interior del campus universitario.

### 6.1.1. ANTECEDENTES

Con el fin de dar cumplimiento a los objetivos a continuación se describe una serie antecedentes que servirán de apoyo para tener una mejor comprensión en cada uno de estos temas y alcances significativos evidenciados en otro u otros proyectos similares.

Las políticas y los procedimientos de seguridad informática surgen como una herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia y la sensibilidad de la información que favorecen el desarrollo y el buen funcionamiento de la empresa. Deben considerarse como reglas a cumplir que surgen para evitar problemas y que se establecen para dar soporte a los mecanismos de seguridad implementados en los sistemas y en las redes de comunicación.[1]

En el tema de políticas de seguridad en la actualidad se cuenta con las normas en seguridad informática como la ISO 27000 estas datan a partir de entidades normalizadores británicas como lo es la (British Standards Institution) fueron los primeros en publicar documentos sobre prácticas en Seguridad para empresas desde 1995, desde entonces esto se empezó a gestar la familia 27000 el año 2000 como requisito para un Sistema de gestión de la seguridad de Información o SGSI, que puede ser aplicado en el ámbito internacional, de allí se han presentado varios avances o cambios, dentro de ello complementos como la norma ISO 17000.[2]

### 6.1.2. NORMATIVA ISO 27001

El 15 de Octubre de 2005, revisada el 25 de Septiembre de 2013. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 (que ya quedó anulada) y es la norma con arreglo a la cual se certifican por auditores externos los SGSIs de las organizaciones. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados.[3]

---

[1]Citado el 19 de Octubre de 2015, Disponible en: http://repositorio.utp.edu.co/dspace/bitstream/11059/4117/1/0058A284.pdf

[2]Citado el 19 de Octubre de 2015, Disponible en: http://ribuc.ucp.edu.co:8080/jspui/bitstream/handle/10785/1731/CDMIST65.pdf?sequence=1

[3] Citado el 11 de Septiembre de 2016, Disponible en: http://www.iso27000.es/iso27000.html

### 6.1.3. NORMATIVA ISO 27000

La serie de normas ISO/IEC 27000 son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC). La serie contiene las mejores prácticas recomendadas en Seguridad de la información para desarrollar, implementar y mantener Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI). La mayoría de estas normas se encuentran en preparación e incluyen: ISO/IEC 27000 - es un vocabulario estándar para el PSI. Introducción y base para el resto. Tercera versión: enero de 2014.[4]

El logro del principal objetivo de este proyecto en la Universidad de Cartagena centro tutorial Mompox tiene su punto de partida en la norma ISO 27001, dado que la norma adopta temas como la mejora continua en la gestión de seguridad de la organización, dentro de las que está contenida el monitoreo, operación, seguimiento, revisión con el único fin de que cada uno de los procesos de la empresa se colaboren en mutuo acuerdo para cumplir el objetivo de la empresa u organización.

### 6.1.4. SEGURIDAD INFORMATICA.

El mundo se encuentra en tiempos de revolución tecnológica donde la manipulación correcta de la información generará buenas prácticas dentro de la organización. La seguridad informática genera un gran impacto en las empresas, porque representa una fortaleza y confianza para la organización que la implemente.

Con la aplicación de este proyecto es indispensable conocer por qué la seguridad informática es importante para la organización cuando el mayor activo es la información propiamente dicha.

Es claro que la idea principal de este proyecto es contribuir a solucionar un problema que tiene que ver con la seguridad informática de la Universidad de Cartagena centro tutorial Mompox, en cuanto a políticas de seguridad se refiere, este tema es importante para la organización y se le debe prestar mucha atención, ya que se requiere de la colaboración de todo el personal de la Universidad y de cada uno de los procesos implicados para implementar este tipo de políticas de seguridad en el alma mater.

[4] Citado el 11 de Septiembre de 2016, Disponible en: https://es.wikipedia.org/wiki/ISO/IEC_27000-series

### 6.1.5. GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

La gestión de la seguridad de la información es un proceso continuo que consiste en garantizar que los riesgos de la seguridad de la información sean identificados, valorados, gestionados y tratados por todos los miembros de la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.[5]

Es importante que en la administración de la seguridad de la información se involucre toda la institución, teniendo en cuenta la definición, identificación y planificación de cada uno de los controles a establecer para garantizar y proteger la información de la entidad, así como el acceso a cada uno de los recursos informáticos de la misma.

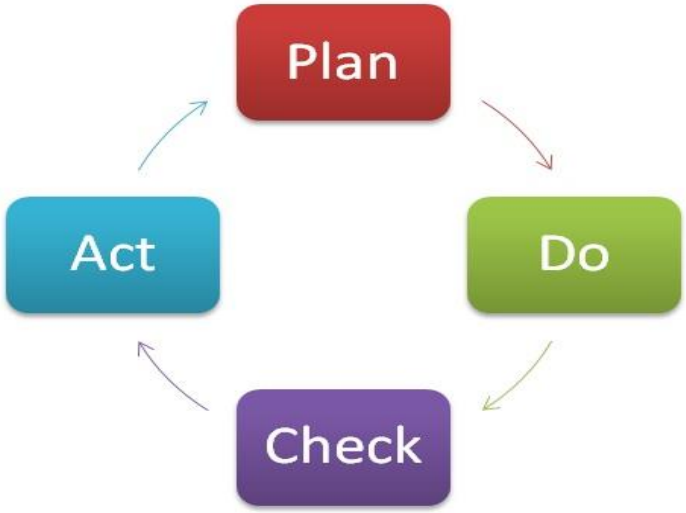
Toda buena gestión de la seguridad implica que se realice un proceso interno donde se clasifique cada uno de los activos de información con los que cuenta la institución de acuerdo a su valor con el objetivo de identificar qué tipo de riesgos que son nocivos para la organización, realizando controles que permitan prevenir accesos no autorizados a recursos informáticos o sistemas de información de la entidad.

### 6.1.6. CICLO DE MEJORA CONTINÚA VS NORMA ISO/IEC 27001:2013

El ciclo de mejora continua que se conoce como el ciclo PDCA (del inglés plan- do-check-act) o PHVA (planificar-hacer-verificar-actuar) o Ciclo de Deming por ser Edwards Deming su creador, en la actualidad es uno de los sistemas más utilizado y requerido por las organizaciones y empresas para mejorar cada uno de sus procesos, ya que establece cuatro pasos, que una forma organizada la empresa debe llevar a cabo con el único fin de alcanzar la mejora continua.

[5] http://www.iso27000.es/sgsi.html

Figura 2. Ciclo de mejora continua (ciclo deming)




Fuente: http://www.pdcahome.com/5202/ciclo-pdca/

Las cuatro etapas que componen el ciclo son las siguientes:

**PLANIFICAR (Plan):** En esta etapa se identifican las áreas susceptibles de mejora y se planifican los objetivos que se desean alcanzar. En el desarrollo de las actividades a alcanzar se buscan tecnologías mejores de las que se tienen.

**HACER (Do):** Corresponde a las actividades de cambios que se implementan en el sistema, para alcanzar la propuesta de mejora. En la mayoría de los casos se requiere establecer pruebas al sistema antes de operar los cambios definitivos.

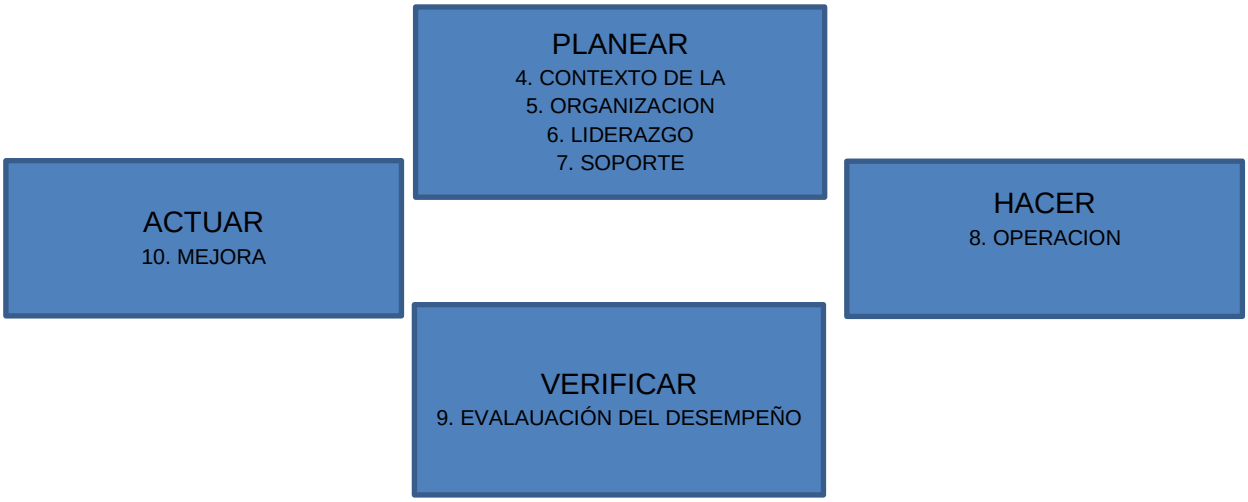
**CONTROLAR O VERIFICAR (Check):** Una vez que se implemente el nuevo sistema o mejora, debe realizarse una verificación que valide que el sistema opera correctamente. En la eventualidad en que el sistema no supere los objetivos proyectados se procede a ajustar o modificar de tal forma que se alcance lo proyectado o esperado.

**ACTUAR (Act):** Al finalizar el periodo de prueba definido, se estudian los resultados y se comparan con el funcionamiento incorporado antes de la mejora definitiva. Si se tienen resultados positivos se incorpora o implementa la mejora y si no proceder a ajustarlos de tal forma que se obtenga la meta propuesta, una vez culminado este

último paso se vuelve a realizar el ciclo en busca de estudiar cambios nuevos que mejoren el sistema.

En la norma ISO/IEC 27001:2013 encontramos el enfoque basado en proceso, este proceso brinda a las organizaciones mejoras continuas en un sistema de políticas de seguridad informática. De acuerdo a la versión de la norma se orientas los procesos de la siguiente forma:

Figura 3. Ciclo de mejora continua alineado a la norma ISO 27001:2013




Fuente: Elaborada con base en la información publicada en la página web http://www.welivesecurity.com/la-es/2013/10/09/publicada-iso-270002013-cambios-en-lanorma-para-gestionar-la-seguridad-de-la-informacion/

A continuación se muestra por medio de un cuadro la relación que se presenta entre las fases del ciclo de mejora continua 'PHVA' (planear, hacer, verificar y actuar) con respecto a los numerales y capítulos de la norma ISO 27001:2013.

Tabla 3. Fases PHVA vs Estructura ISO 27001:2013

| Fase PHVA | Capitulo ISO 27001:2013 |
|---|---|
| PLANEAR | 4. Contexto de la Organización<br>5. Liderazgos<br>6. Planificación<br>7. Soporte |
| HACER | 8. Operación |
| VERIFICAR | 9. Evaluación de desempeño |
| ACTUAR | 10. Mejora |

Fuente: Autor.

Fase PLANEAR en la norma ISO 27001:2013: En el capítulo 4[6] - Contexto de la organización14 de la norma ISO 27001:2013, Se establece la importancia de realizar un análisis de las partes internas y externas de la empresa, esto tiene como objetivo identificar las diferentes expectativas y necesidades de las áreas o departamentos de la empresa en el alcance de las PSI.

En el capítulo 5 - Liderazgo15[7], Hace referencia a los roles y compromisos que tiene la alta dirección con respecto al sistema de gestión de seguridad de la información, e implica el compromiso que adquiera una política de seguridad informática adecuada con el propósito de asignar la disponibilidad presupuestal para el sistema PSI, Para que se asignen los roles pertinentes y se comuniquen a toda la organización.

En el capítulo 6 - Planeación16[8], En este capítulo se hace una valoración y tratamiento a los riesgos de seguridad y se establecen los posibles objetivos y planes viables para la seguridad de la información de la empresa, y que se deben cumplir a cabalidad.

En el capítulo 7 - Soporte17[9] En este capítulo la administración de la entidad establece aquellos recursos necesarios para implementar y mejorar constantemente el sistema de gestión de seguridad de información implementado.

[6] NTC-ISO-IEC 27001:2013, Pág. 1-2
[7] Ibídem, Pág. 2-3
[8] Ibídem, Pág. 4-6
[9] Ibídem, Pág. 6

• Fase HACER en la norma ISO 27001:2013[10]. En el capítulo 8 - Operación18 de la norma ISO 27001:2013, se indica que la empresa debe realizar una planificación, luego debe proceder a implementar cada uno de sus procesos y posteriormente controlar todos los procesos que se generen en el sistema, para realizar la valorización y tratamiento de cada uno de los riesgos que se presenten con la seguridad de la información.

• Fase VERIFICAR en la norma ISO 27001:2013[11]. En el capítulo 9 - Evaluación del desempeño19, se establecen aquellos ítems que se deben evaluar con periocidad durante la ejecución y desempeño de la seguridad de la información evaluando la eficacia del mismo.

• Fase ACTUAR en la norma ISO 27001:2013[12]. En el capítulo 10 - Mejora20, Con la implementación del sistema de mejora continua en la organización y a partir de hallazgos de no conformidades, se establecen las acciones que permitan solucionar y mejorar con el propósito de que están no se vuelvan a presentar.

### 6.1.7 MARCO CONCEPTUAL (GLOSARIO DE TERMINOS)

**ACTIVO DE INFORMACIÓN:** Aquello que es de alta validez y que contiene información vital de la empresa que debe ser protegida.

**AMENAZA:** Es la causa potencial de un daño a un activo de información. Anexo SL: Nuevo esquema definido por International Organization for Standardization - ISO para todos los Sistemas de Gestión acorde al nuevo formato llamado “Anexo SL”, que proporciona una estructura uniforme como el marco de un sistema de gestión genérico.

**ANÁLISIS DE RIESGOS:** Utilización sistemática de la información disponible, para identificar peligros y estimar los riesgos.

**BACKUP:** Copia de la información en un determinado momento, que puede ser recuperada con posterioridad.

**COORDINACIÓN DE PLANEACIÓN E INNOVACIÓN:** Es el responsable de velar por el cumplimiento de esta Política, documentar el Manual de Seguridad de la Información, los procesos, procedimientos, instructivos y formatos específicos alineados al estándar internacional ISO 27001 y sus normas derivadas además de los otros marcos generalmente aceptados como: COBIT,

[10] Ibídem, Pág. 8-9
[11] Ibídem, Pág. 9-11
[12] NTC-ISO-IEC 27001:2013, Pág. 11-12

ITIL, NIST, ASNZ y DRII, así como liderar la implementación de los controles exigidos por la Ley y la Regulación Vigente.

**COMITÉ DE SEGURIDAD:** Equipo de trabajo conformado por el presidente ejecutivo, coordinador de tecnología o los funcionarios que hagan sus veces.

**CONTRASEÑA:** Clave de acceso a un recurso informático.

**CONTROL:** Medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal.

**CAUSA:** Razón por la cual el riesgo sucede. Ciclo de Deming: Modelo mejora continua para la implementación de un sistema de mejora continua.

**COLABORADOR:** Es toda persona que realiza actividades directa o indirectamente en las instalaciones de la entidad, Trabajadores de Planta, Trabajadores Temporales, Contratistas, Proveedores y Practicantes.

**CONFIDENCIALIDAD:** Propiedad que determina que la información no esté disponible a personas no autorizados.

**CONTROLES:** Son aquellos mecanismos utilizados para monitorear y controlar acciones que son consideradas sospechosas y que pueden afectar de alguna manera los activos de información.

**DIRECTRICES:** Descripción que aclara lo que se debería hacer y cómo hacerlo, para alcanzar los objetivos establecidos en las políticas.

**DISPONIBILIDAD:** Propiedad de determina que la información sea accesible y utilizable por aquellas personas debidamente autorizadas.

**DUEÑO DEL RIESGO SOBRE EL ACTIVO:** Persona responsable de gestionar el riesgo.

**IMPACTO:** Consecuencias de que la amenaza ocurra. Nivel de afectación en el activo de información que se genera al existir el riesgo.

**SERVICIOS DE PROCESAMIENTO DE INFORMACIÓN:** Cualquier servicio, infraestructura o sistema de procesamiento de información o los sitios físicos que los albergan.

**SEGURIDAD DE LA INFORMACIÓN:** Preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales

como autenticidad, responsabilidad, no-repudio y confiabilidad pueden estar Involucradas.

**EVENTO DE SEGURIDAD DE LA INFORMACIÓN:** Un evento de seguridad de la información es la presencia identificada de un estado del sistema, del servicio o de la red que indica un posible incumplimiento de la política de seguridad de la información, una falla de controles, o una situación previamente desconocida que puede ser pertinente para la seguridad.

**FIREWALL:** Conjunto de recursos de hardware y software que protegen recursos informáticos de accesos indebidos.

**INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN:** Evento no deseado o inesperado, que tiene una probabilidad de amenazar la seguridad de la información.

**INTEGRIDAD:** Propiedad de salvaguardar la exactitud y estado completo de los activos. Oficial de Seguridad: Persona encargada de administrar, implementar, actualizar y monitorear el Sistema de Gestión de Seguridad de la Información.

**PROBABILIDAD DE OCURRENCIA:** Posibilidad de que se presente una situación o evento específico. Responsables del Activo: Personas responsables del activo de información.

**INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN:** Está indicado por un solo evento o una serie de eventos inesperados o no deseados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

**INFORMACIÓN CONFIDENCIAL (RESERVADA):** Información administrada por La Cámara de Comercio en cumplimiento de sus deberes y funciones y que en razón de aspectos legales debe permanecer reservada y puede ser únicamente compartida con previa autorización del titular de la misma.

**INFORMACIÓN CONFIDENCIAL (CONFIDENCIAL):** Información generada por La Cámara de Comercio en cumplimiento de sus deberes y funciones y que debe ser conocida exclusivamente por un grupo autorizado de funcionarios por esta. El acceso a este tipo de información debe ser restringido y basado en el principio del menor privilegio. Su divulgación a Terceros requiere permiso del titular de la misma y de acuerdos de confidencialidad. Así mismo, su divulgación no autorizada puede causar daños importantes a la Entidad. Todo material generado durante la creación de copias de este tipo de información (ejemplo, mala calidad de impresión), debe ser destruido.

**INFORMACIÓN PRIVADA (USO INTERNO):** Información generada por La Cámara de Comercio en cumplimiento de sus deberes y funciones, que no debe ser conocida por el público en general. Su divulgación no autorizada no causa grandes daños a la Entidad y es accesible por todos los usuarios.

**INFORMACIÓN PÚBLICA:** Es la información administrada por La Universidad de Cartagena en cumplimiento de sus deberes y funciones que está a disposición del público en general.

**LAN:** Grupo de computadores y dispositivos asociados que comparten un mismo esquema de comunicación y se encuentran dentro de una pequeña área geográfica (un edificio o una oficina).

**LICENCIA DE SOFTWARE:** Es la autorización o permiso concedido por el dueño del programa al usuario para utilizar de una forma determinada y de conformidad con unas condiciones convenidas. La licencia precisa los derechos (de uso, modificación, o redistribución) concedidos a la persona autorizada y sus límites, además puede señalar el lapso de duración y el territorio de aplicación. [13]

**COPYRIGHT:** Son el conjunto de derechos de exclusividad con que la ley regula el uso de una particular expresión, de una idea o información. En términos más generalizados se refiere a los derechos de copia de una obra (poemas, juegos, trabajos literarios, películas, composiciones musicales, grabaciones de audio, pintura, escultura, fotografía, software, radio, televisión, y otras formas de expresión de una idea o concepto), sin importar el medio de soporte utilizado (Impreso, Digital), en muchos de los casos la protección involucra un periodo de duración en el tiempo. En muchos casos el copyright hace referencia directa a la protección de los derechos patrimoniales de una obra.

**PROPIEDAD INTELECTUAL:** Es una disciplina normativa que protege las creaciones intelectuales provenientes de un esfuerzo, trabajo o destreza humana, dignos de reconocimiento jurídico. [14]

**OPEN SOURCE (FUENTE ABIERTA):** Es el término por el que se conoce al software que es distribuido y desarrollado de forma libre, en el cual la licencia específica el uso que se le puede dar al software.

**SOFTWARE LIBRE:** Software que una vez obtenido puede ser usado, copiado, modificado, o redistribuido libremente, en el cual la licencia expresamente especifica dichas libertades.

---

[13] Tomado del diccionario Wikipedia. http://es.wikipedia.org/wiki/Licencia_de_software
[14] Tomado de http://www.derautor.gov.co/htm/preguntas.htm#01

**SOFTWARE PIRATA:** Es una copia ilegal de aplicativos o programas que son utilizados sin tener la licencia exigida por ley.

**SOFTWARE DE DOMINIO PÚBLICO:** Tipo de software en que no se requiere ningún tipo de licencia y cuyos derechos de explotar, usar, y demás acciones son para toda la humanidad, sin que con esto afecte a su creador, dado que pertenece a todos por igual. En términos generales software de dominio público es aquel en el cual existe una libertad total de usufructo de la propiedad intelectual.

**FREEWARE:** Software de computador que se distribuye sin ningún costo, pero su código fuente no es entregado.

**SHAREWARE:** Clase de software o programa, cuyo propósito es evaluar por un determinado lapso de tiempo, o con unas funciones básicas permitidas. Para adquirir el software de manera completa es necesario un pago económico.

**MÓDEM (Modulador - Demodulador de señales):** Elemento de comunicaciones que permite transferir información a través de líneas telefónicas.

**MONITOREO:** Verificación de las actividades de un usuario con respecto a los recursos informáticos de La Cámara de Comercio.

**OTP (One Time Password):** Contraseña entregada por el administrador de un recurso informático que permite el primer acceso a dicho recurso y obliga al usuario a cambiarla una vez ha hecho este acceso.

**PLAN DE CONTINGENCIA:** Plan que permite el restablecimiento ágil en el tiempo de los servicios asociados a los Sistemas de Información de La Cámara de Comercio en casos de desastres y otros casos que impidan el funcionamiento normal.

**POLÍTICA:** Toda intención y directriz expresada formalmente por la dirección.

**PROTECTOR DE PANTALLA:** Programa que se activa a voluntad del usuario, o automáticamente después de un tiempo en el que no ha habido actividad.

**PROXY:** Servidor que actúa como puerta de entrada a la Red Internet.

**RECURSOS INFORMÁTICOS:** Son aquellos elementos de tecnología de Información tales como: computadores servidores.

**RIESGO:** Grado de exposición de un activo que permite la materialización de una amenaza.

**RIESGO INHERENTE:** Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.

**RIESGO RESIDUAL:** Nivel de riesgo remanente como resultado de la aplicación de medidas de seguridad sobre el activo.

**PSE:** Proveedor de Servicios Electrónicos, es un sistema centralizado por medio del cual las empresas brindan a los usuarios la posibilidad de hacer sus pagos por Internet.

**PSI:** Siglas de políticas de seguridad informática.

**VULNERABILIDAD:** Debilidad de un activo o grupo de activos de información que puede ser aprovechada por una amenaza. La vulnerabilidad de caracteriza por ausencia en controles de seguridad que permite ser explotada.[15]

[15] Tomado del diccionario Wikipedia. http://es.wikipedia.org/wiki/Licencia_de_software

# 7. METODOLOGÍA PRELIMINAR

A continuación se describe, cada uno de los métodos que serán utilizados para obtener la solución del problema que se propone y que tiene que ver con la inexistencia de políticas de seguridad en la Universidad de Cartagena centro tutorial Mompox Bolívar, teniendo en cuenta el alcance y los objetivos que se proponen en este proyecto.

La metodología que se plantea en este proyecto busca dar cumplimiento al objetivo general que se definen en este proyecto. Dentro de esta metodología se tendrá en cuenta el marco de referencia de la norma ISO/IEC 27001:2013 que hace referencia entre otras cosas a las actividades y requisitos que se deben tener en cuenta para el desarrollo un buen diseño de políticas de seguridad informática.

## 7.1 FASES METODOLOGICAS

Tomando como base los requisitos de la norma ISO/IEC 27001:2013 para el diseño de políticas de seguridad informática, se establecieron las siguientes etapas para el desarrollo de este proyecto:

**Figura 4. Fases metodológicas para el diseño de las PSI**


Fuente: El autor

Para llevar a cabo las fases propuestas para el diseño de las políticas de seguridad informática, a continuación se muestran las actividades a realizar:

### 7.1.1 FASE I – DESCRIPCION DEL ESTADO ACTUAL

La descripción del estado actual tiene por objetivo realizar una descripción y análisis de los principales aspectos relacionados al problema encontrado en la Universidad de Cartagena Centro Tutorial Mompox. Para ello, se debe recopilar la información apropiada, de fuentes de origen primario y/o secundario.

En esta fase describe e identifica el estado real de la universidad con respecto a modelos de seguridad de la información de acuerdo a lo que propone la norma ISO/IEC 27001:2013.

### 7.1.2 FASE II – RECOLECCION DE LA INFORMACION

Esta fase describe todo el contexto de la organización que tienen que ver con los requerimientos que establece el "Capitulo 4.1 – Conocimiento de la organización y de su contexto"[16] de la norma ISO/IEC 27001:2013, tiene que ver con las determinación internas y externas de la Universidad que son necesarios para la implementación de políticas de Seguridad Informática.

Para el levantamiento de la información, se tuvieron en cuenta herramientas como:

- Diligenciamiento de encuestas, que permiten determinar el nivel de seguridad que tiene la Universidad con relación a los requisitos de la norma ISO/IEC 27001:2013.
- Documentos del sistema de calidad de la institución, con el objeto de verificar la documentación relacionada con la información de seguridad, que incluyen funciones, roles, que están involucrado en temas de seguridad.
- Fuentes Externas, tiene que ver con aquellas autoevaluaciones con encuestas, y lo que tiene que ver con las estrategias de gobierno que implementa el Ministerio de Tecnologías de Información y Comunicaciones.

[16] NTC-ISO-IEC 27001:2013, Pág. 1

### 7.1.3 FASE III – ANALISIS DE INFORMACION A TRAVES DEL ANALISIS DE RIESGOS.

En esta etapa se lleva a cabo un análisis de información que permita llevar a cabo un estudio general de todos los riesgos encontrados y que tienen relación con el proceso de tecnología de la Universidad. Dentro de los que están:

- Identificar los activos de información del proceso de gestión de tecnología y clasificarlos de acuerdo a su criticidad y protección.
- Desarrollar la valorización de los riesgos de seguridad de la información que se encuentren de acuerdo a lo establecido en los alcances de la PSI.
- Establecer los planes de acción que tenga en cuenta los controles a realizar cuyo objetivo es minimizar los riegos identificados durante el proceso de valorización, Para escoger los controles respectivos.

### 7.1.4 FASE IV – DISEÑOS DE POLITICAS.

Esta fase tiene que ver con todos los procesos que se desarrollan para establecer las políticas de seguridad informática, dentro de las que están:

- ❖ Definir los alcances que tiene la política de seguridad informática donde se establece la aplicabilidad y los límites de la política de seguridad informática.
- ❖ Establecer los límites que tiene las PSI, donde se establecerán la aplicabilidad de las políticas en la entidad, teniendo en cuenta hasta donde se pude llegar por temas de seguridad.
- ❖ Tener en cuenta la estructura organizacional de la universidad para determinar las responsabilidades tendientes a la seguridad de la información.
- ❖ Definir la política de seguridad de la entidad teniendo los riesgos encontrados.

Para desarrollar cada una de las fases que se proponen en la metodología, para diseñar las políticas de seguridad informática de la universidad, se describen a detalle a continuación.

## 8. DISEÑO DE POLITICAS DE SEGURIDAD INFORMATICA.

A continuación se muestra el desarrollo de las diferentes fases que se plantearon para el diseño de las políticas de seguridad informática de la Universidad de Cartagena Centro Tutorial Mompox, que incluyen cada una de las acciones que permitan lograr los objetivos específicos, que finalmente cumple con el objetivo general.

En el desarrollo de este documento encontramos los diferentes componentes, dentro de los que están valoraciones, datos levantados, insumos, y los diferentes cálculos que se han determinado en la definición de la metodología para el diseño de las políticas de seguridad informática de la Universidad de Cartagena Centro Tutorial Mompox.

A continuación se muestran algunos de estos componentes:

- El levantamiento de la información se obtuvo con la aplicación de técnicas de recolección de información, que nos permitieron realizar los respectivos diagnósticos y análisis de la entidad.
- Informe de cada uno de los análisis aplicados.
- Informe del proceso de valoración de riesgos.
- Incluir los puntos específicos de norma ISO/IEC 27001:2013 donde se establece aquellos requisitos de seguridad a los cuales se les debe dar cumplimiento.

## 8.1. FASE I. DESCRIPCIÓN DEL ESTADO ACTUAL

A continuación describimos el diagnostico que se realizó con el propósito de conocer la realidad que presenta la Universidad de Cartagena Centro Tutorial Mompox con respecto a políticas de seguridad informática con base a la norma ISO/IEC 27001:2013.

### 8.1.1 DIAGNOSTICO ESTADO ACTUAL DE LA SEGURIDAD

En el punto 1.1.3 DIAGNOSTICO SITUACIÓN PROBLEMA de este proyecto, se muestra un análisis que detalla los diferentes riesgos que afectan la seguridad de la Universidad que permite determinar que el problema está asociado a la “No existencia de políticas de seguridad informática”.

En términos general, las siguientes fueron las situaciones identificadas:

- No se cuenta con una administración de seguridad informática en el centro Tutorial Mompox que lidere e identifique riesgos y vulnerabilidades que puedan afectar la seguridad de la información.

- Se denota falta de conocimiento, empoderamiento y concientización por parte del personal administrativo en temas relacionados con seguridad de la información.

- Se tiene problemas relacionados con integración activa de toda la universidad, para aplicar los debidos controles, apoyados en la evaluación de riesgos.

- No se tiene implementado un sistema que permita la gestión y valoración adecuada de riesgos y vulnerabilidades de seguridad.

- No existe una orientación desde la alta dirección para que las políticas de seguridad estén alineadas con los objetivos de la Institución.

- No se cuenta con formación e inducción a tutores sobre el manejo y conservación de los trabajos realizados por los estudiantes.

- El acceso al sistema presenta su mayor vulnerabilidad en los estudiantes, ya que no se aplica ninguna política de seguridad informática direccionada al personal que hace uso del centro tutorial.

## 8.2 FASE II. RECOLECCION DE LA INFORMACION.

### 8.2.1 CONTEXTO DE LA ORGANIZACIÓN.

La norma ISO/IEC 27001:2013 hace énfasis en que hay que conocer la entidad por fuera y por dentro, y como pude afectar positiva o negativamente la implementación de las políticas de seguridad informática.

De acuerdo a lo anterior, la norma ISO/IEC 27001:2013 menciona en el capítulo “4. CONTEXTO DE LA ORGANIZACIÓN”, donde se debe identificar aquellas situaciones y aquellas factores internos y externos que se deben tener en cuenta para la implementación de las políticas de seguridad informática.

La Universidad de Cartagena es una universidad pública colombiana localizada en Cartagena de Indias. Fue fundada en 1827 por Francisco de Paula Santander y Simón Bolívar, y es reconocida por ser la más antigua del Caribe colombiano. El día 26 de marzo de 2014, la Universidad de Cartagena, recibió por parte del Ministerio de Educación Nacional la Acreditación Institucional de Alta Calidad convirtiéndose en la primera y única universidad pública de la región caribe con éste tipo de acreditación. En el 2015 estuvo en el Ranking de Scimago para Colombia catalogada como la décima mejor universidad del país y como la quinta mejor pública.[17]

[17] Tomado de: https://es.wikipedia.org/wiki/Universidad_de_Cartagena

### 8.2.2 CONOCIMIENTO DE LA ORGANIZACIÓN.

RESEÑA HISTÓRICA: La Universidad de Cartagena ha sido el espacio de formación de los jóvenes del Caribe colombiano desde el siglo XIX. Su historia e importancia se expresan desde los albores de la independencia y en el sueño de los libertadores Simón Bolívar y Francisco de Paula Santander, organizadores del novel Estado colombiano. Ellos visionaron la educación como el medio ideal para la formación de las nuevas generaciones que conducirían los destinos de la República.

En este contexto, se gestaron las universidades públicas. La Universidad del Magdalena e Istmo fue una de estas, creada por el Decreto de 6 de octubre de 1827. Abre sus puertas el 11 de noviembre de 1828 en su sede actual, el vetusto claustro del Convento de San Agustín. El primer nombre de la Universidad revelaba su cobertura, el Magdalena, territorio que comprendía en esa época todo el Caribe colombiano, incluida Panamá. Con el tiempo, la Universidad recibió otros nombres, entre ellos Universidad del Segundo Distrito, Colegio Provincial de Cartagena, Instituto Boliviano, Colegio del Departamento, Colegio Fernández de Madrid, Universidad de Bolívar y por último Universidad de Cartagena.

Durante el siglo XIX, y a medida que avanzaba la construcción del Estado, fue centro formativo del pensamiento político colombiano pues a ella asistían estudiantes de todas las regiones que terminaron desempeñando altos cargos públicos de representación nacional; entre ellos el cuatro veces presidente de la República y padre de la Constitución de 1886, Rafael Núñez Moledo.

Los primeros programas académicos con los que inició la Universidad, fueron la Escuela de Filosofía y Letras, la Escuela de Medicina y la Escuela de Jurisprudencia. Ya en el siglo XX, asumiendo las dinámicas de transformación de la educación superior, la Universidad inicia un proceso de modernización en respuesta a la realidad industrial que experimentaba el país y la región; expandiéndose, diversificándose y asumiendo el ingreso de nuevos grupos sociales como la mujer.

La Universidad de Cartagena en 2015, conmemora su aniversario 188 manteniendo su liderazgo, reconocimiento social y prestigio académico con programas en diferentes disciplinas y ciencias, institutos y 90 grupos de investigación que promueven la transformación social en la región, liderando proyectos educativos de maestrías y doctorados de las más altas calidades.

La Universidad ha comprendido que para estar a la altura de los tiempos, como reza su eslogan, hay que asumir los retos que le impone el tiempo. Por ello no solo forma a distancia a través de las tecnologías de la información sino que, además, se ha apropiado de las mismas desde la radio y la televisión; así, fomenta su desarrollo

para integrar a sus proyectos académicos a las comunidades.[18]

MISIÓN DE LA UNIVERSIDAD: La Universidad de Cartagena, como institución pública, mediante el cumplimiento de sus funciones sustantivas de docencia, investigación y extensión, y su proceso de internacionalización, forma profesionales competentes en distintas áreas del conocimiento, con fundamentación científica, humanística, ética, cultural y axiológica. Esto les permite ejercer una ciudadanía responsable, contribuir con la transformación social, y liderar procesos de desarrollo empresarial, ambiental y cultural en los contextos de su acción institucional.[19]

VISIÓN DE LA UNIVERSIDAD: En 2027, la Universidad de Cartagena continuará consolidándose como una de las más importantes instituciones de educación superior del país, y con una amplia proyección internacional. Para ello, trabaja en el mejoramiento continuo de sus procesos académicos, investigativos, administrativos, financieros, de proyección social, desarrollo tecnológico, internacionalización; con una clara vinculación al desarrollo social, político, cultural, ambiental y económico de Cartagena, Bolívar, la región Caribe y Colombia.[20]

OBJETIVOS: Para lograr su misión, la Universidad de Cartagena cumple con los siguientes objetivos:

- ✓ Impartir educación superior como medio eficaz para la realización plena del hombre colombiano, con miras a configurar una sociedad más justa, equilibrada y autónoma, enmarcada dignamente en la comunidad internacional.
- ✓ Elaborar y proponer políticas, planes, programas y proyectos orientados a resolver problemas regionales de la comunidad en su área de influencia y participar en ello.
- ✓ Establecer una política permanente de orientación docente y capacitación profesional, la cual debe fomentar el desarrollo personal, la práctica de la enseñanza y la investigación, en busca de un mejoramiento de la calidad institucional.

[18] Fuente: Pagina web de la entidad
[19] Fuente: Pagina web de la entidad
[20] Ibídem

- ✓ Propiciar el intercambio científico, tecnológico y cultural, con el propósito de mantener una actualización permanente que garantice la adecuada orientación del desarrollo de la región Caribe y del país.

- ✓ Armonizar su acción académica, administrativa, investigativa y de extensión con otras instituciones educativas y entidades de carácter público y privado a nivel nacional e internacional.

- ✓ Garantizar el cumplimiento de los programas de formación, en sus diversos niveles y modalidades, de acuerdo con lo establecido en las normas académicas.

- ✓ Impulsar en sus programas académicos el desarrollo del hombre, con base en sólidos componentes de formación humanística, instrucción cívica y en los principios y valores de la participación ciudadana.

- ✓ Fomentar, de conformidad con las necesidades y demandas de la región y del país, nuevas áreas del saber que permitan el desarrollo cualitativo y cuantitativo de las comunidades en su zona de influencia.

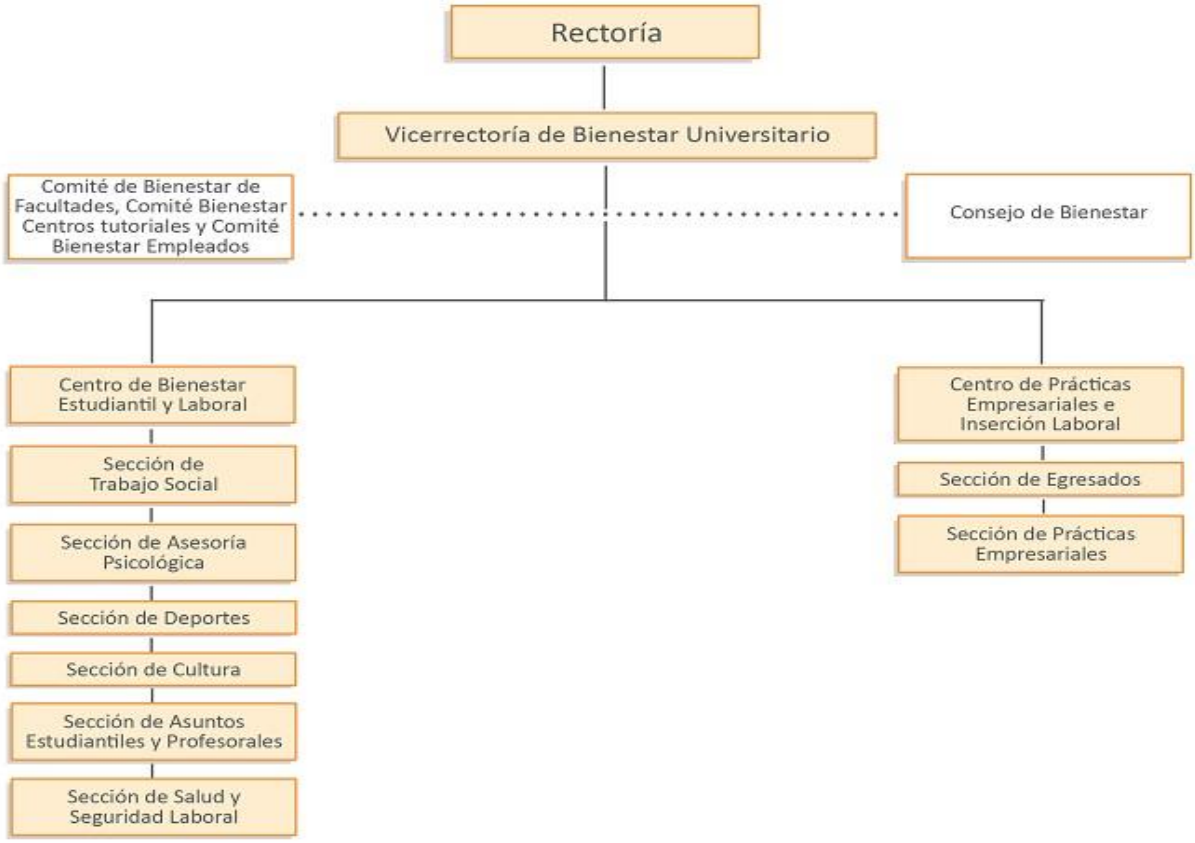
- ✓ Propender por la conservación del patrimonio histórico y cultural de Cartagena. De la región Caribe y del país, mediante acciones y programas educativos tendientes a ese fin.

- ✓ Promover un ambiente sano, mediante acciones y programas de educación y cultura ecológica. Ofrecer un adecuado servicio de información y documentación.[21]

[21] Tomado de: http://www.unicartagena.edu.co/index.php/universidad/institucion/item/155-mision-vision-y-objetivos#.WB_Fe-HhC8U

ESTRUCTURA ORGANIZACIONAL

Figura 6. Organigrama de la Entidad

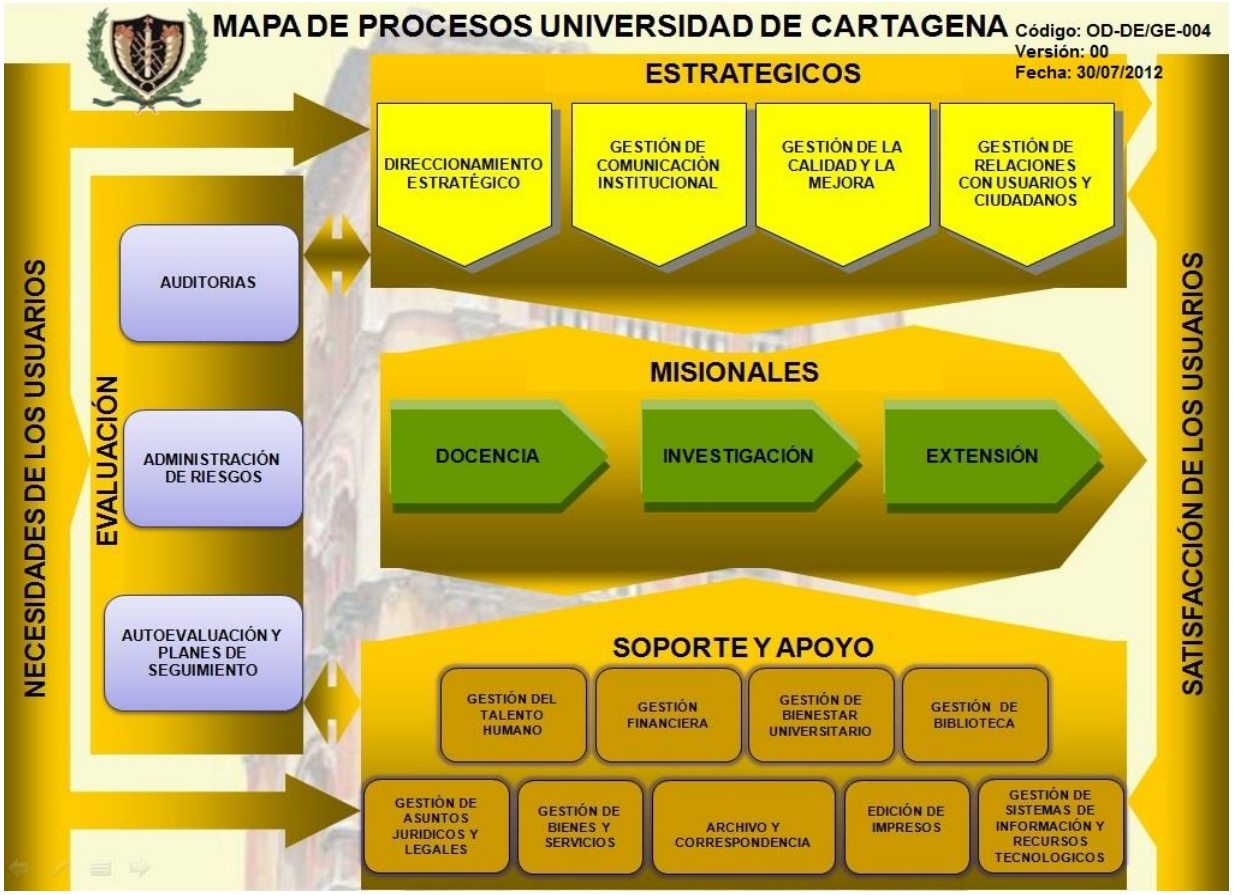



Fuente: La Entidad

MAPA DE PROCESOS

A continuación se muestra el mapa de procesos de la Universidad, en el cual se muestra el soporte y apoyo de gestión de sistemas de información y recursos tecnológicos:

Figura 7. Mapa de proceso de la Entidad




Fuente: La Entidad

## 8.3 FASE III. ANALISIS DE INFORMACION A TRAVES DE ANALISIS DE RIESGO.

### 8.3.1 IDENTIFICACION ESTRATIFICACION DE LA ENTIDAD.

En la identificación de nivel de estratificación de la Universidad, nos muestra en términos generales, lo complejo que es implementar un sistema de políticas de seguridad, en tal caso se toma como referencia la metodología planteada en el documento “TABLA 5: RANGO DE ESTRATIFICACIÓN DE ENTIDADES” apoyado en el modelo de seguridad de la información, este define tres tipos de estrato en las entidades como son: Alto, Medio, Bajo[22] estos valores resultan después de realizar un seguimiento tamaño y capacidad de la Universidad, el área de sistemas, los servicios que se ofrecen, el número total de equipos y lo referente al valor del presupuesto de funcionamiento.

Con el fin de establecer el nivel de estratificación se tomó como base el TABLA 4: ESTRATIFICACIÓN DE LA UNIVERSIDAD, de este trabajo que muestra las respuestas que se obtuvieron de acuerdo la información proporcionada por la entidad.

[22] Anexo 3: Estratificación de Entidades - Modelo seguridad de la información para la estrategia de Gobierno en Línea 2.0, Pág. 8

Tabla 4. Estratificación de la Universidad.

| PARAMETROS DE EVALUACION | OPCIONES DE RESPUESTA | PUNTOS | OBSERVACION |
|---|---|---|---|
| **Presupuesto** | Menos de 3,000 millones de pesos | 3 | Para el 2015 está fijado en 176 mil millones de pesos: Información publicada en la página web de la entidad |
| | Entre 3.000 millones y 50.000 millones de pesos | | |
| | Más de 50.000 millones de pesos | | |
| **Número total de computadores** | Menos de 100 computadores | 3 | Información suministrada por la división de sistemas |
| | Entre 100 y 500 computadores | | |
| | Más de 500 computadores | | |
| **Número Empleados de Tecnología** | Menos de 4 Servidores | 3 | Información suministrada por la división de sistemas |
| | Entre 4 y 20 Servidores | | |
| | Más de 20 Servidores | | |
| **Existencia y función del área de sistemas (tecnología).** | No hay área de sistemas o tecnología como tal | 3 | Información suministrada por la división de sistemas |
| | Área de tecnología enfocada en la operación del día a día, que cumple labores en su mayoría | | |
| | Punto anterior más área de sistemas que planea y desarrolla proyectos nuevos o de actualización, administra su presupuesto y desarrolla labores proactivas a través de comités y participación en decisiones corporativas | | |
| **Existencia y objeto de la WAN.** | WAN pública (p.ej. Internet) sólo para usar correo y navegar. Incluye servidores de correo y Web en hosting. | 2 | Información suministrada por la división de sistemas |
| | WAN pública (p.ej. Internet) con servicios ofrecidos al ciudadano. Puede o no haber desarrollos sofisticados de transaccionalidad | | |
| | Lo anterior más la existencia de una WAN privada (no incluye VPN a través de Internet) | | |
| **Transaccionalida d en la WEB.** | Solo ofrece servicios de consulta (páginas WEB estáticas y correo electrónico) | 3 | Información suministrada por la división de sistemas |
| | Transaccionalidad local. Generación de servicios y seguimiento de trámites, solo con base en datos y aplicativos propios. | | |
| | Lo anterior más interacción con aplicativos, datos y servicios de otras entidades y/o terceros | | |
| **Desarrollo de Software.** | No desarrolla software. Incluye aquellas entidades que tienen en hosting una página WEB básica e informativa y un servidor de correo. | 2 | Información suministrada por la división de sistemas |
| | Sí desarrolla software pero solo para aplicativos internos. Hay que aclarar que este desarrollo puede ser interno o en outsourcing (realizado por terceros). | | |
| | Sí desarrolla software para aplicativos externos. Sí publica información transaccional. | | |
| | **TOTAL PUNTOS** | **19** | |

Fuente: Autor

Para determinar la estratificación de la entidad, es necesario sumar los puntos obtenidos en cada una de las respuestas dadas, para este caso el total es **19 puntos.**

El nivel de estratificación está determinado en base a los rangos de valores establecidos en la siguiente tabla:

Tabla 5. Rango de Estratificación de Entidades[23]

| RANGO DE PUNTOS | ESTRATO |
|---|---|
| Menor a 10 puntos | BAJO |
| Entre 11 y 22 puntos | MEDIO |
| Mayor a 22 puntos | ALTO |

Fuente: El Autor

Teniendo en cuenta el puntaje obtenido por la Universidad, **19 puntos**, en este caso el nivel de estratificación la entidad clasifica en un nivel **MEDIO,** lo que representa un trabajo a largo de toda la Universidad para el diseño de políticas de seguridad informática.

Con base a la información proporcionada por la Universidad con el ánimo de determinar el nivel de estratificación, se hicieron los siguientes análisis:

- El presupuesto de la Universidad para el año 2015 fue de 176 mil millones de pesos, lo que supone que la entidad, debe tener establecido un rubro económico para la implementación de políticas de seguridad informática en cada uno de sus cread, basado en lo establecido en el numeral c) del capítulo 5.1 liderazgo y compromiso de la norma ISO/IEC 27001:2013[24]

- El número de equipos que tiene la universidad, hace indispensable que se garantice la seguridad de la información que reposa en cada una de estas máquinas, lo que hace necesario que se realice o desarrolle una valoración de los riesgos determinando los mecanismos de seguridad a implementar para minimizar riesgos y vulnerabilidades de seguridad. Lo expuesto

[23] Anexo 3: Estratificación de Entidades - Modelo seguridad de la información para la estrategia de Gobierno en Línea 2.0, Pág. 12.
[24] Norma ISO/IEC 27001:2013, Pág. 2

anteriormente es necesario para trabajar 'Valoración de riesgos de la seguridad de la información'[25] y 'Tratamiento de riesgos de la seguridad de la información'[26] de la norma ISO/IEC 27001:2013.

- El número de empleados que tiene que ver con la División de Sistemas y personal administrativo, muestra el tamaño de la misma y los recursos que son necesarios para el funcionamiento de cada una de sus dependencias. Muy a pesar de que se tiene un grueso número de trabajadores en la división de sistemas y personal administrativo, no se tiene control sobre la seguridad de la información, que permita establecer riesgos y vulnerabilidades asociados a toda información que tiene la entidad y se convierte en un activo significativo para la entidad.

- El área de tecnología de la entidad, además de administrar, planea y desarrolla proyectos, esto implica que la división de sistemas de la Universidad debe contemplar la implementación de proyectos tendientes a acciones y medidas de seguridad de la información que garanticen la minimización de brechas de seguridad.

### 8.3.2 NIVEL DE CUMPLIMIENTO CONTROLES ANEXO A ISO 27001:2013.

De acuerdo al análisis, se definió el nivel de cumplimiento que tiene la universidad con relación a los objetivos de control y controles establecidos en la FIGURA 5 NIVEL DE CUMPLIMIENTO CONTROLES ANEXO A ISO 27001:2013, ya que este resultado define una serie de pasos para minimizar los riesgos y vulnerabilidades de seguridad, permitiendo la disponibilidad, confidencialidad y la integridad de la información.

Para realizar este Proyecto fue necesario la utilización de una lista de verificación que incluían un conjunto de preguntas 'SI' o 'NO', que a su vez fueron respondidas por personal administrativo de la entidad, de acuerdo al objetivo de control que se estaba evaluando, teniendo en cuenta que los controles en la norma ISO/IEC 27001:2013, se orientan a la protección de la seguridad de las personas,

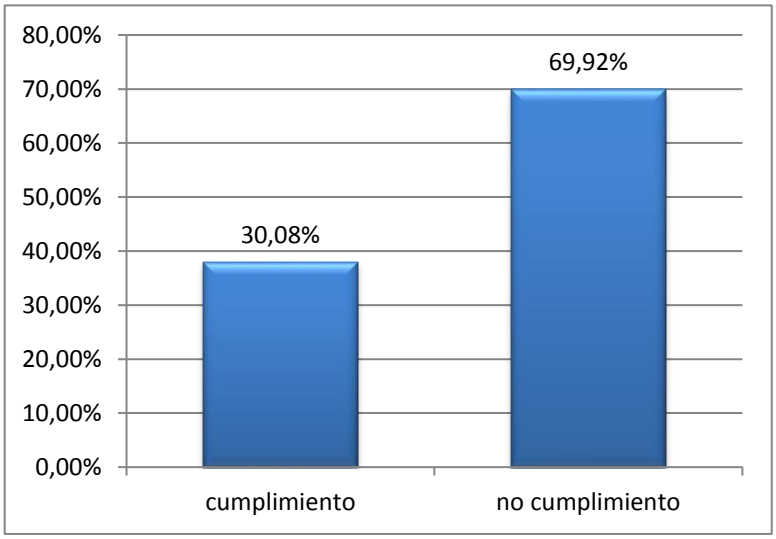
[25] Norma ISO/IEC 27001:2013, Pág. 4

[26] Ibídem, Pág. 5

infraestructura lógica y física, de los recursos tecnológicos y finalmente de la información.

Adicionalmente se muestra cada uno de los interrogantes que se plantearon para la evaluación de cada uno de los controles y preguntas contestadas por los funcionarios de la entidad. De acuerdo a lo anterior a continuación se muestra los resultados que se obtuvieron.

Figura 5. Nivel de cumplimiento controles Anexo A ISO 27001:2013




Fuente: El Autor

Lo anterior demuestra que se hace necesario la implementación del sistema de políticas de seguridad informática para la Universidad de Cartagena Centro tutorial Mompox, de acuerdo a los controles establecidos en la Figura 6. Nivel Cumplimiento Objetivos de Control Anexo A ISO 27001:2013, ya que esto obliga a la entidad a realizar un esfuerzo grande dado que no se cuenta con controles de seguridad, dado el bajo grado de cada uno de ellos. Para la ejecución de estos controles se requiere muchas mejoras en equipos y adecuaciones teniendo en cuenta herramientas y mecanismos tecnológicos que garantizan la efectividad del proceso e incluso la contratación de personal experto en el tema cuyos costos pueden ser altos, y requieren un tiempo considerable tendientes a la seguridad de la información.

El cumplimiento de dichos controles del Figura 6. Nivel Cumplimiento Objetivos de Control Anexo A ISO 27001:2013 muestra el nivel de madures que tiene la universidad frente a la administración de la seguridad de la información, sobre como protege los activos de información, el nivel de los riesgos y vulnerabilidades a partir de los controles y el cumplimiento de la normatividad vigente.

En el modelo de la seguridad de la información que presenta la estrategia de gobierno en línea, SISTEMA SANSI [7], que establece el nivel del riesgo de las entidades a partir del cumplimiento de los controles se clasifican en Alto, Medio, Bajo[27], con base a lo anterior se estableció la siguiente tabla de medición:

Tabla 6. Nivel de riesgos vs nivel cumplimiento controles.

| **Porcentaje cumplimiento controles** | **Nivel de riesgo e Implicaciones** | |
|---|---|---|
| Alto | Bajo | Se llevan a cabo los controles de seguridad y estos se implementan, se evidencia un grado de madures en la universidad con respecto a la seguridad de la información y mantiene la protección adecuada de los activos de información. Esta situación representa un riesgo bajo para la entidad. |
| Medio | Medio | La universidad aplica los controles de seguridad, un porcentaje de ellos no están debidamente documentados o no son los más indicados, se hace necesario una revisión a medio plazo, para mejorar el cumplimiento y la efectividad.<br><br>Esta situación representa un Riesgo Medio para la Universidad debido a la presencia de debilidades en algunos de sus controles que pueden ser aprovechadas por amenazas internas o externas para atentar contra la seguridad de la información. También es necesario revisar el nivel cumplimiento de la |

[27] Modelo de Seguridad de la Información, SISTEMA SANSI - SGSI – Modelo de Seguridad de la información para la estrategia de gobierno en línea, Pág., 47.

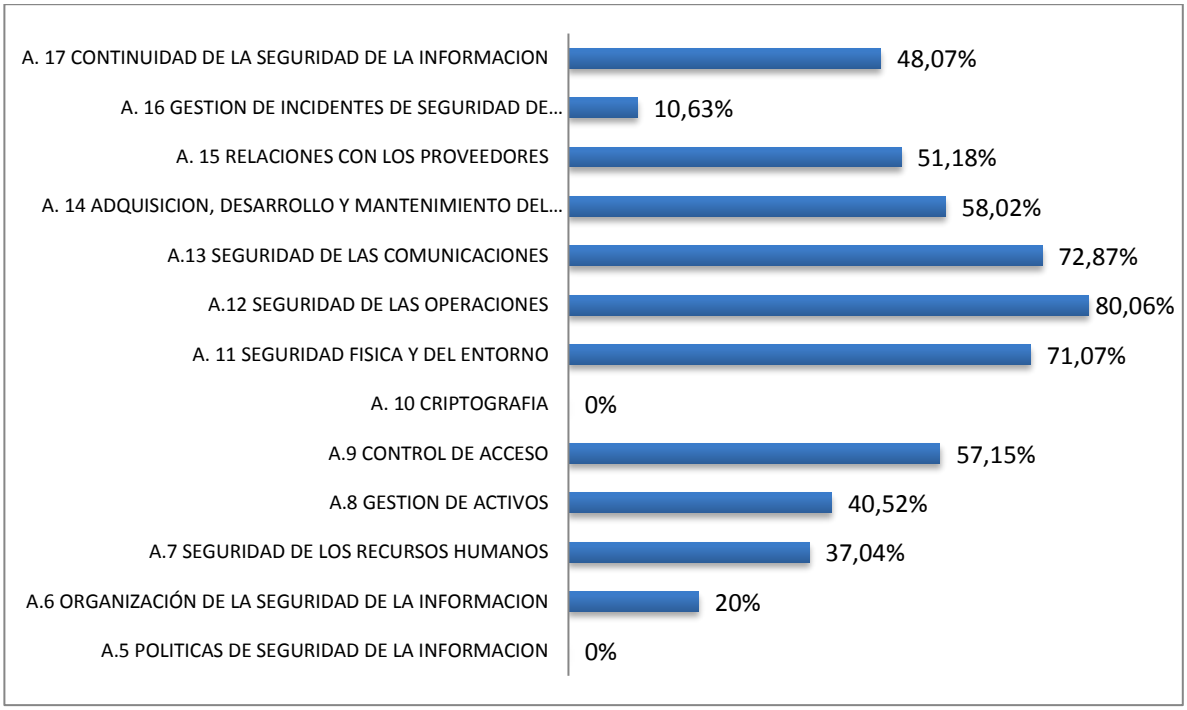
| | | |
|---|---|---|
| | | normatividad vigente relacionada con seguridad de la información. |
| Bajo | Alto | La no aplicación de controles o el poco grado de cumplimiento, muestra un riesgo ALTO para la entidad dado que el nivel de protección de sus activos y/o el cumplimiento de la normatividad vigente relacionado con la seguridad, no es el más adecuado.<br><br>Para este caso, es necesario que se implementen con carácter urgente las medidas de seguridad en un corto plazo con el objetivo de cerrar las brechas encontradas. |

Fuente: Autor

Teniendo en cuenta el nivel de cumplimiento con respecto al Anexo A de la norma ISO/IEC 27001:2013, la Universidad se encuentra en un grado MEDIO de implementación (30,08%) de los requerimientos establecidos en los objetivos de control y controles.

A continuación se muestra un informe de la verificación de cada uno de los objetivos de control del Anexo A de la norma ISO/IEC 27001:2013.

Figura 8. Nivel Cumplimiento Objetivos de Control Anexo A ISO 27001:2013




Fuente: Autor

OBJETIVOS DE CONTROL CON NIVEL DE CUMPLIMIENTO 'BAJO'

A continuación se muestran los objetivos del anexo A de la norma ISO/IEC 27001:2013 donde el nivel de cumplimiento por parte de Universidad es BAJO (menor o igual al 33%) en este caso representa un riesgo ALTO ya en este caso se carece o se han aplicado controles.

Los siguientes son los objetivos de control del Anexo A de la norma ISO/IEC 27001:2013 cuyo cumplimiento por parte de la entidad se encuentran en un nivel BAJO (menor o igual al 33%), lo que representa un riesgo ALTO para la entidad debido a la ausencia o inadecuada implementación de los controles que generan un nivel de bajo protección de sus activos de información y/o en algunos casos, el incumplimiento de la normatividad vigente relacionado con seguridad de la

información.

Tabla 7. Objetivos de control con nivel BAJO de cumplimiento

| OBJETIVO DE CONTROL | % CUMPLIMIENTO |
|---|---|
| A.10 CRIPTOGRAFIA | 0% |
| A.16 GESTIÓN INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN | 10.63% |
| A.6 ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACION | 20% |
| A.5 POLITICAS DE LA SEGURIDAD DE LA INFORMACION | 0% |

Fuente: Autor

**A.10 Criptográfica (0%).**

Tiene por objetivo asegurar el uso apropiado y eficaz de mecanismo criptográficos para proteger la confidencialidad, autenticidad e integridad de la información[28]. La universidad no cuenta con herramientas o mecanismos de cifrado para salvaguardar la información que reposa en cada una de sus equipos de cómputo, lo que evidencia un riesgo ALTO ya que no se puede garantizar la autenticidad, no repudio, integridad y confidencialidad de la información. Este hecho pone en riesgo la información sensible de la entidad, que puede implicarle perdida de información y/o sanciones de los entes de control por no proteger la información. De acuerdo a lo anterior la Universidad debe implementar cuanto antes herramientas de cifrado tales como: cifrado de correos, portal de intercambio seguro y cifrado del almacenamiento de dispositivos movibles y portátiles.

**A.16 Gestión de Incidentes de seguridad de la información (10.63%)**

La Universidad carece de un control de incidentes de seguridad de la información, por ello es necesario elaborar un proceso con el objetivo de determinar un dirección apropiada, para la correcta gestión de los incidentes de seguridad, proporcionando

[28] Norma ISO/IEC 27001:2013, Pág. 17

a la entidad herramientas que permitan generar reportes y evaluar los incidentes de seguridad que se presenten.

### A.6 Organización de la seguridad de la información (20%)

La Universidad no ha establecido las funciones y compromisos de la seguridad de la información, y este es uno de los roles que debe tener la rectoría de la institución especialmente para establecer un buen sistema de políticas de seguridad informática. Por lo tanto, es indispensables que la entidad comience a participar en eventos, foros, asociaciones y otros organizamos relacionados con seguridad de la información.

### A.5 Políticas de seguridad de la información (0%)

En la actualidad no se ha evidenciado un manual o procedimientos de políticas de seguridad informática en la división de sistemas de la entidad, tampoco en los centros tutoriales de la misma, los funcionarios de la entidad no tienen claro a que hacen referencia las políticas de seguridad informática. De acuerdo a lo anterior es urgente que se implemente las políticas de seguridad en la entidad y que a su vez esta sean aprobadas por la rectoría y concejo directivo de la Universidad.

Tabla 8. Objetivos de control con nivel MEDIO de cumplimiento

| **OBJETIVO DE CONTROL** | **% CUMPLIMIENTO** |
|---|---|
| A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DEL SISTEMA | 58.02% |
| A.8 GESTION DE ACTIVOS | 40.52% |
| A.7 SEGURIDAD DE LOS RECURSOS HUMANOS | 37.04% |
| A.15 RELACIONES CON LOS PROVEEDORES | 51.18% |
| A.17 CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACION | 48.07% |
| A.9 CONTROL DE ACCESO | 57.15% |

Fuente: Autor

## A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DEL SISTEMA (58.02%)

Los controles que se realicen se deben realizar teniendo en cuenta los siguientes controles:

La Universidad no tiene en cuenta los requisitos que tienen que ver con la seguridad de la información, teniendo en cuenta los requisitos y características específicas correspondientes con el desarrollo de sistemas de información, así como lo especifica el control A.14.1.1 del Anexo A de la norma ISO/IEC 27001:201335.

Tampoco se llevan a cabo verificaciones técnicas que tienen que ver con aquellas aplicaciones críticas, en el momento en que se desarrollen cambios a la plataforma tecnológica, esto es un riesgo alto ya que no permite seguridad, disponibilidad y el correcto funcionamiento de los servicios que se llevan a cabo en la división de sistemas de la entidad.

La institución carece de procedimientos que controlen el manejo de datos en los ambientes de producción, lo que representa un riesgo alto dado de que no se asegura la debida privacidad y protección de los datos sensibles de la Universidad.

## A.8 GESTION DE ACTIVOS 40.52%

La Universidad tiene problemas para identificar sus activos de información medio tecnológico con el cual se realiza la administración de la institución, este hecho representa un riesgo para la entidad ya que no tiene la realidad de todos activos de información. De acuerdo a lo anterior es importante desarrollar la identificación de activos teniendo en cuenta las prioridades y necesidad para la protección de la información, lo que genera que los usuarios desconozcan sus responsabilidades y consecuencia de sus acciones.

## A.7 SEGURIDAD DE LOS RECURSOS HUMANOS 37.04%

La Universidad no tiene una herramienta que garantice que su personal administrativo y contratistas que prestan servicios a la institución, conozcan las responsabilidades y funciones en lo referente a seguridad información. De acuerdo a lo anterior es necesario que la entidad organice su plan de capacitación anual o semestral para tener efectividad en los controles que se implementen.

## A.15 RELACIONES CON LOS PROVEEDORES 51.18%

Actualmente no se cuenta con políticas de seguridad informática donde se establezcan el reglamento de seguridad que tengan como objetivo evitar acceso no autorizados en la información de la Universidad.

Por otro lado, en lo que respecta a los contratos que se realizan con terceros no todos poseen el acuerdo de confidencialidad, lo que representa un riesgo, si una de estos terceros tengan acceso a la información sensible de la Universidad.

## A.17 CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACION 48.07%.

Teniendo en cuenta la continuidad del negocio se evidencia que no se tiene en cuenta los requisitos que garanticen la información en aquellos donde se presenten adversidades donde se ponga en riesgo la información. De acuerdo a lo anterior es urgente llevar a cabo procesos y procedimientos, que garanticen la seguridad de la información en casos donde se afecte la integridad de la información.

## A.9 CONTROL DE ACCESO 57.15%

El nivel de cumplimiento de este control se debe a los siguientes aspectos:

- La Universidad no tiene un procedimiento que involucre una restricción, control, y asignación de privilegios para acceso a los recursos tecnológicos de la entidad y cada una de sus aplicaciones.

- No se tiene un procedimiento para la gestión de contraseñas en los sistemas de acceso a la información de la entidad.

- No se tiene programado un plan de auditoria de manera regular para el acceso a la información.
- La parte administrativa de la Universidad no ha establecido una revisión al acceso de la información de cada uno de sus centros tutorial y usuarios respectivos.

De acuerdo a lo anterior se evidencia que existe un riesgo para la Universidad ya que carece de algunas medidas de seguridad para el control y acceso a la información, teniendo en cuenta que se puede materializar riesgos y vulnerabilidades dentro de las que están acceso no autorizados, abuso de privilegios entre otros que puede afectar drásticamente la información.

## OBJETIVOS DE CONTROL CON NIVEL DE CUMPLIMIENTO 'ALTO'

A continuación encontraremos aquellos objetivos de del Anexo A de la norma ISO/IEC 27001:2013 en donde el la entidad cumple y hace parte de un nivel ALTO (mayor al 70%), lo que representa un riesgo BAJO teniendo en cuenta que los medidas de seguridad aplicadas garantizan la protección de sus activos de información.

Tabla 9. Objetivos de control con nivel ALTO de cumplimiento

| **OBJETIVO DE CONTROL** | **% CUMPLIMIENTO** |
|---|---|
| A.13 SEGURIDAD DE LAS COMUNICACIONES | 72.87% |
| A.11 SEGURIDAD FISICA Y DEL ENTORNO | 71.07% |
| A.12 SEGURIDAD DE LAS OPERACIONES | 80.07% |

Fuente: Autor

## A.13 SEGURIDAD DE LAS COMUNICACIONES (72.87%)

Para este objetivo se evidencia que se encuentra en un nivel de cumplimiento ALTO lo que demuestra que la Universidad está administrando debidamente las redes. Teniendo en cuenta que este objetivo debe aumentar su nivel de cumplimiento de

acuerdo a lo establecido a la norma, la entidad debe

Este objetivo de control de encuentra en un nivel de cumplimiento ALTO debido a que las redes de la entidad son debidamente administradas y aseguradas. Con el objetivo de subir su nivel de cumplimiento y con esto cumplir a cabalidad los requerimientos establecidos en este objetivo de control de la norma, la entidad debe:

- ✓ Propender por la separación de los servicios de información, bases de datos y sistemas de información en la red, teniendo en cuenta el control A.13.1.3 del Anexo A de la ISO/IEC 27001:2013[29]

- ✓ Proteger la información que se incluye en los mensajes electrónicos, tal como lo menciona el control A.13.2.3 del Anexo A de la norma ISO/IEC 27001:2013[30]

- ✓ Definir y verificar en tiempos programados los requisitos para verificar los acuerdos de confidencialidad que reflejen lo que requiere la Universidad para la protección de la información, teniendo en cuenta el control A.13.2.4 del Anexo A de la ISO/IEC 27001:2013[31]

## A.11 SEGURIDAD FÍSICA Y DEL ENTORNO (71.07%)

Con el fin de aumentar el nivel de cumplimiento de este objetivo de control la Universidad debe:

Desarrollar áreas de trabajo seguras de acuerdo al control A.11.1.5 del Anexo A de la ISO/IEC 27001:2013[32]

Clasificar los riesgos que se deben trabajar fuera de la universidad, con el propósito de dar cumplir con el control A.11.2.6 ‘Seguridad de Equipos y activos fuera de las instalaciones’ del Anexo A de la ISO/IEC 27001:2013[33]

Teniendo en cuenta el total cumplimiento de la norma en lo referente al control A.11.2.6 ‘Seguridad de equipos y activos fuera de las instalaciones’ del Anexo A de la ISO/IEC 27001:2013[34]. La Universidad debe: (i) Diseñar estrategias de seguridad y verificación que validen la terminal de trabajo que se está conectando a la red

[29] NORMA ISO/IEC 27001:2013, pág. 20
[30] Ibídem
[31] Ibídem
[32] Ibídem, pág. 16
[33] Ibídem, pág. 18
[34] Ibídem

interna de la red segura y valida. (ii) Aplicar herramientas de monitoreo de las terminales que se conectan a la red.

- Desarrollar una política aplicada al escritorio con el propósito de salvaguardar la información sensible.

**A.12 SEGURIDAD DE LAS OPERACIONES (80.07%)**

Teniendo en cuenta que para incrementar el nivel de cumplimiento de este objetivo la universidad debe:

Propender para que los responsables de seguridad de la información establezcan mecanismos para el monitoreo de los log de eventos de seguridad y las actividades que realizan los administradores sobre la plataforma de procesamiento.

### 8.3.3 LEVANTAMIENTO DE LA INFORMACIÓN DE LOS ACTIVOS DEL DEPARTAMENTO DE TECNOLOGÍA.

En lo que respecta con la clasificación de los activos de información y la valorización de riesgos, se realizaron de acuerdo a los siguientes aspectos:

• **Alcance identificación de activos.** Para la identificación de activos de información se tuvo en cuenta el alcance de las Políticas de seguridad informática, dentro del cual solo se está contemplando el proceso de tecnología, de acuerdo a lo anterior solamente se tendrán en cuenta los activos que son administrados y utilizados por el proceso de tecnología, ya que esta es la materia prima en lo que respecta al proceso de valoración de riesgos de los activos de información.

• **Metodología para la clasificación de activos y valoración de sus riesgos.** La Metodología está enfocada con la identificación y clasificación de los activos de información del proceso de tecnología y como se lleva a cabo la valorización de estos riesgos.

• **Confidencialidad de la información.** Es importante aclara que dentro de este

proyecto no se mencionan las aplicaciones sino el objetivo, teniendo en cuenta la confidencialidad de la información por parte de la Universidad.

### 8.3.4 CLASIFICACION DE ACTIVOS DE TECNOLOGIA.

A continuación se encuentra un cuadro que evidencia los activos del proceso de tecnología de la Universidad, que muestra los parámetros, la formulación y los cálculos que se utilizaron para establecer el nivel de criticidad de los activos de información.

Tabla 10. Tipos de Activos de Información.

| **Tipo de activo** | **Descripción** |
|---|---|
| Servicios | Contempla servicios prestados por el sistema |
| Datos / información | Ficheros, copias de respaldo, datos de gestión interna, credenciales, datos de validación de credenciales, datos de control de acceso, registro de actividad. |
| Software | Programas, aplicativos, desarrollos, software base, sistema de información |
| Equipos informáticos | Hardware. Medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización |
| Personal | Personas relacionadas con los sistemas de información. |
| Redes de comunicaciones | Servicios de comunicaciones contratados a terceros; medios de transporte que llevan datos de un sitio a otro |
| Soportes de información | Dispositivos físicos que permiten almacenar información de forma permanente |
| Equipamiento auxiliar | Otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos. |

Fuente: El Autor

Lo primero que se realizó en esta etapa fue identificar, la cual establece la siguiente clasificación de tipos de activos:

En la siguiente tabla se muestra el inventario de cada uno de los activos de información que lograron identificar en el proceso de tecnología. A continuación se relaciona el inventario de los activos de información que se pudieron identificar en el proceso de tecnología:

Tabla 11. Inventario de activos de información de tecnología

| No | Nombre del Activo | Descripción del Activo | Tipo de activo | Contenedor |
|---|---|---|---|---|
| A1 | Servidores de aplicaciones de producción | Servidores de producción que soportan las aplicaciones y sistemas de información | Equipos informáticos | Data Center del proveedor |
| A2 | Plataforma de Correo | Servidores que soportan la plataforma y servicio de correo corporativo. | Equipos informáticos | Data Center del proveedor |
| A3 | Servidores de Pruebas | Servidores que soportan los ambientes de prueba de la entidad | Equipos informáticos | Data Center del proveedor |
| A4 | Servidores de Desarrollo | Servidores que soportan los ambientes de desarrollo de la Universidad | Equipos informáticos | Data Center del proveedor |
| A5 | SIMA | Unidades de almacenamiento donde reside la información de la plataforma virtual de la Universidad. | Equipos informáticos | Data Center del proveedor |
| A6 | Solución de Backup | Solución de Backup para el respaldo de información del negocio | Equipos informáticos | Data Center del proveedor |
| A7 | Dispositivos de red | Equipos y dispositivos de red activos (switch, router) | Equipos informáticos | Cuartos de rack |
| A8 | Computadores Administradores | Computadores que utilizan los administradores de plataforma | Equipos informáticos | Área administración de plataforma |
| A9 | Computadores de escritorio usuarios | Computadores de escritorio asignados a los colaboradores de la Universidad | Equipos informáticos | Computadores |
| A10 | Portátiles | Computadores portátiles de la Universidad | Equipos informáticos | Portátiles |
| A11 | Centro Principal de Procesamiento | Centro Principal de procesamiento donde reside la infraestructura para soporta la operación de la Universidad | Instalaciones | Data Center del proveedor |
| A12 | Centro Alterno de Procesamiento | Centro Alterno de procesamiento que contiene la infraestructura para la continuidad de la Universidad | Instalaciones | Data Center del proveedor |
| A13 | Cuartos de comunicaciones | Instalación física donde residen los rack de comunicaciones | Instalaciones | Cuartos de rack |
| A14 | Área administración de | Instalación física donde están ubicados los administradores de | Instalaciones | Área administración de plataforma |

| | | | | |
|---|---|---|---|---|
| | plataforma | plataforma | | |
| A15 | Red LAN | Red LAN corporativa de la Universidad | Redes de comunicaciones | Red LAN |
| A16 | Red WAN | Red WAN de la Universidad | Redes de comunicaciones | RED WAN |
| A17 | Red WIFI corporativa | Red Wifi utilizada por los equipos móviles para acceder a los recursos de la red corporativa de la Universidad | Redes de comunicaciones | Red LAN |
| A18 | Red WIFI estudiantes | Red Wifi para estudiantes | Redes de comunicaciones | Red LAN |
| A19 | Servidores de administración | Servidores que soportan los servicios bases de administración | Equipos informáticos | Data Center del proveedor |
| A20 | Servidores de bases de datos de producción | Servidores de producción que soportan los motores e instancias de bases de datos | Equipos informáticos | Data Center del proveedor |
| A21 | Impresoras | Impresoras de la entidad ubicada en diferentes áreas | Equipos informáticos | Impresoras |
| A22 | Aplicativo de nomina | Aplicativo para la gestión de recursos humanos | Software | Servidores de aplicaciones |
| A23 | Sistema de Gestión Documental | Sistema de Gestión documental de la Universidad | Software | Servidores de aplicaciones |
| A24 | Sistema de Gestión de Calidad | Aplicativo para el Sistema de Gestión de Calidad | Software | Servidores de aplicaciones |
| A25 | Aplicativo WEB transaccional | Aplicativo web para la consulta y pago de las obligaciones de cartera de los ex empleados | Software | Servidores de aplicaciones |
| A26 | Página WEB | Página Web de la Universidad | Software | Servidores de aplicaciones |
| A27 | Intranet | Página Web de la Universidad | Software | Servidores de aplicaciones |
| A28 | Aplicativos seguimiento proyectos | Página Web de la Universidad | Software | Servidores de aplicaciones |
| A29 | Equipos de seguridad perimetral | Equipos informáticos destinados a proteger la seguridad perimetral de la entidad. | Equipos informáticos | Equipos de seguridad perimetral |
| A30 | Aplicación Mesa | Aplicación utilizada por la mesa de ayuda para la gestión de | Software | Servidores de |

| | | | | |
|---|---|---|---|---|
| | de Ayuda | requerimientos e incidentes | | administración |
| A31 | Sistema Monitoreo de servicios | Aplicaciones utiliza para monitorear el rendimiento y disponibilidad de los servicios de TI | Software | Servidores de administración |
| A32 | Sistema de Control de Acceso | Sistema para controlar el acceso a las áreas de la Universidad | Software | Servidores de administración |
| A33 | Herramienta de Virtualización | Herramienta utilizada para la virtualización de servidores | Software | Servidores de administración |
| A34 | Sistema Gestor Base de Datos | Sistema de gestión y administración de las bases de datos de la entidad | Software | Servidores de bases de datos |
| A35 | Antivirus | Software de administración de seguridad para el control de virus | Software | Servidores de administración |
| A36 | Sistema administración de la SIMA | Sistema para administrar la SIMA | Software | Servidores de administración |
| A37 | Sistema de control de versiones | Sistema de administración para el control de versionamiento de software | Software | Servidores de administración |
| A38 | CRM | Aplicativo para gestión relación con clientes | Software | Servidores de aplicaciones |
| A39 | Terminales empresariales | Aplicativo para el pago de las obligaciones con terceros | Software | Otros bancos |
| A40 | Directorio activo | Servicio establecido donde están los objetos tales como usuarios, equipos o grupos, con el objetivo de administrar los inicios de sesión en los equipos conectados a la red | Servicios | Servidores de administración |
| A41 | Correo Electrónico | Correo electrónico corporativo de la Universidad | Servicios | Plataforma de Correo |
| A42 | Bases de datos | Bases de datos que almacenan la información de la Universidad. | Servicios | Servidores de bases de datos |
| A43 | FileServer | Almacenamiento de los documentos electrónicos que manejan las áreas de la Universidad | Servicios | Servidores de administración |
| A44 | Gestión de privilegios | Corresponde al mecanismo para la administración y asignación de privilegios de acceso a los recursos tecnológicos y aplicaciones. | Servicios | Directorio activo |
| A45 | Identidad del Usuario | Información que identifica a un funcionario (nombre, cedula, datos biométricos como la huella, código del usuario, etc.) | Datos / Información | Directorio activo |
| A46 | Datos de | Usuario y Contraseña que utiliza los usuarios para ingresar a los recursos | Datos / Información | Directorio activo |

| | | | | |
|---|---|---|---|---|
| | autenticación | tecnológicos y aplicaciones. | | |
| A47 | Usuarios genéricos | Usuario genéricos que utilizan las aplicaciones para conectarse a las bases de datos | Datos / Información | Bases de datos |
| A48 | Log de evento de seguridad | Log que contiene los registros de los eventos de seguridad y de los eventos de administración sobre las aplicaciones | Datos / Información | Log de eventos |
| A49 | Registro de incidentes de seguridad | Registro de incidentes de seguridad reportados por la herramienta de mesa de ayuda | Datos / Información | Bases de datos |
| A50 | Manuales técnicos de administración | Corresponde a los documentos, manuales y procedimientos relacionadas con la administración de la plataforma | Datos / Información | File Server |
| A51 | Bitácora de control de acceso al centro de computo | Registro de acceso al centro de computo | Datos / Información | Carpetas |
| A52 | Plan estratégico de tecnología | Documento que contiene el plan estratégico de tecnología | Datos / Información | File Server |
| A53 | Documentos del proceso | Corresponde a los documentos del proceso que están publicados en el sistemas de gestión de calidad | Datos / Información | Bases de datos |

Fuente: El Autor.

### 8.3.5 VALORACION RIESGOS ACTIVOS DE TECNOLOGIA.

En virtud de que se identificaron los activos de información se realizó la valorización de acuerdo a la lo activos crítico de la Universidad, para lo que se tuvo en cuenta el impacto y las pérdidas que le puede generar a la entidad, tanto en aspecto financieros, legales y de imagen, teniendo en cuenta que si se llega a materializar una amenazas, interrumpa la confidencialidad, integridad y disponibilidad, para lo que se desarrolló la siguiente valorización:

Tabla 12. Valoración activos de información

| Aspecto | Criterio de valoración | Criterio de valoración | Valor a asignar |
|---|---|---|---|
| **Financiero** | Pérdidas económicas para la empresa (porcentaje calculado sobre la utilidad operacional) | Menor o igual a 0.25% | 1 |
| | | Mayor a 0.25% y menor o igual a 5% | 2 |
| | | Mayor a 5% y menor o igual a 20% | 3 |
| | | Mayor a 20% y menor o igual a 50% | 4 |
| | | Mayor al 50% | 5 |
| **Legal** | Incumplimiento de normatividad y legislación | No tiene repercusión frente a normatividad y contratos. | 1 |
| | | Genera llamados de atención por parte de los entes de control. | 2 |
| | | Genera posibles sanciones menores por parte de los entes de control y/o reclamos por parte de terceros. | 3 |
| | | Genera sanciones económicas por parte de los entes de control y/o demandas por parte de terceros. | 4 |
| | | Genera sanciones mayores por parte de entes de control, cancelación de contratos, suspensión de licencias, cierre de líneas de negocios. | 5 |
| **Imagen** | Afectación de la imagen de la empresa | Conocido solo de manera interna de la empresa pero no de interés publico | 1 |
| | | Atención de algunas partes interesadas a nivel local que potencialmente puede afectar a la empresa | 2 |
| | | Media atención de las partes interesadas a nivel local y regional. | 3 |
| | | Alta Atención de las partes interesadas a nivel local, regional y nacional. | 4 |
| | | Conocimiento general a nivel nacional e internacional. | 5 |

Fuente: El Autor

Con el ánimo de establecer los activos más críticos se plantearon las siguientes preguntas:

Tabla 13. Preguntas para determinar la criticidad del activo.

| Criterio | Factor Afectado | Pregunta |
|---|---|---|
| **Disponibilidad** | **Financiero** | ¿Si el activo o la información que se gestiona a través de él no están disponibles puede generar pérdidas económicas para la Universidad? |
| | **Legal** | ¿Si el activo o la información que se gestiona a través de él no están disponibles puede generar sanciones legales de entes de control o demandas de terceros? |
| | **Imagen** | ¿Si el activo o la información que se gestiona a través de él no están disponibles puede afectar la imagen de la entidad? |
| **Integridad** | **Financiero** | ¿Si el activo o la información que se gestiona a través de él son alterados sin autorización puede generar pérdidas económicas para la Universidad? |
| | **Legal** | ¿Si el activo o la información que se gestiona a través de él son alterados sin autorización puede generar sanciones de entes de control? |
| | **Imagen** | ¿Si el activo o la información que se gestiona a través de él son alterados sin autorización puede afectar la imagen de la Universidad? |
| **Confidencialidad** | Financiero | ¿Su divulgación no autorizada puede relevar información sensible de la empresa requerida para la toma de decisiones estratégicas y financieras? |
| | Legal | ¿Su divulgación no autorizada puede afectar el cumplimiento de regulaciones impartidas por entes de control o puede generar demandas de terceros? |
| | Imagen | ¿Su divulgación no autorizada puede afectar la imagen de la Universidad? |

Fuente: El Autor

Con el fin de establecer el nivel crítico de cada activo se utilizó la siguiente tabla de valoración:

Tabla 14. Nivel de criticidad de los activo de información.

| Criterio de Evaluación | Valor Criticidad Activo | Nivel Criticidad |
|---|---|---|
| La gestión del activo compromete en un alto grado la integridad y/o confidencialidad y/o disponibilidad de la información de la Universidad. | >= 4 | ALTO |
| La gestión del activo compromete en un nivel medio la integridad y/o confidencialidad y/o disponibilidad de la información. | >2y<4 | MEDIO |
| La gestión del activo compromete en un nivel bajo la integridad y/o confidencialidad y/o disponibilidad de la información de la Universidad. | > 0 y <= 2 | BAJO |
| La gestión del activo no compromete la integridad, confidencialidad y disponibilidad de la información de la Universidad. | Igual a 0 | NO APLICA |

Fuente: El Autor

Tabla 15. Valoración nivel criticidad activos información de tecnología

| N | Nombre del Activo | Confidencialidad | | | Integridad | | | Disponibilidad | | | Confidencialidad | Integridad | Disponibilidad | Valor Total | Nivel de Criticidad |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Financiero | Legal | Imagen | Financiero | Legal | Imagen | Financiero | Legal | Imagen | | | | | |
| A1 | Servidores de aplicaciones de producción | 4 | 3 | 2 | 4 | 2 | 2 | 4 | 2 | 2 | 4 | 4 | 4 | 4 | ALTO |
| A2 | Plataforma de Correo | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | MEDIO |
| A3 | Servidores de Pruebas | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | BAJO |
| A4 | Servidores de Desarrollo | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | BAJO |
| A5 | SIMA | 4 | 4 | 3 | 4 | 4 | 3 | 4 | 4 | 3 | 4 | 4 | 4 | 4 | ALTO |
| A6 | Solución de Backup | 3 | 3 | 2 | 3 | 3 | 2 | 3 | 2 | 2 | 3 | 3 | 3 | 3 | MEDIO |
| A7 | Dispositivos de red | 4 | 4 | 3 | 4 | 4 | 3 | 3 | 3 | 2 | 4 | 4 | 3 | 4 | ALTO |
| A8 | Computadores Administradores | 4 | 4 | 3 | 5 | 4 | 3 | 5 | 4 | 3 | 4 | 5 | 5 | 5 | ALTO |
| A9 | Computadores de escritorio usuarios | 3 | 3 | 1 | 3 | 3 | 1 | 1 | 1 | 1 | 3 | 3 | 1 | 3 | MEDIO |
| A10 | Portátiles | 3 | 3 | 1 | 3 | 3 | 1 | 1 | 1 | 1 | 3 | 3 | 1 | 3 | MEDIO |
| A11 | Centro Principal de Procesamiento | 5 | 4 | 3 | 5 | 4 | 3 | 5 | 4 | 4 | 5 | 5 | 5 | 5 | ALTO |
| A12 | Centro Alterno de Procesamiento | 5 | 4 | 3 | 5 | 4 | 3 | 5 | 4 | 3 | 5 | 5 | 5 | 5 | ALTO |
| A13 | Cuartos de comunicaciones | 3 | 3 | 1 | 3 | 3 | 1 | 3 | 3 | 1 | 3 | 3 | 3 | 3 | MEDIO |
| A14 | Área administración de plataforma | 4 | 4 | 3 | 4 | 4 | 3 | 4 | 4 | 3 | 4 | 4 | 4 | 4 | ALTO |
| A15 | Red LAN | 4 | 4 | 3 | 4 | 4 | 3 | 2 | 1 | 1 | 4 | 4 | 2 | 4 | ALTO |
| A16 | Red WAN | 4 | 4 | 3 | 4 | 4 | 3 | 2 | 1 | 1 | 4 | 4 | 2 | 4 | ALTO |
| A17 | Red WIFI corporativa | 4 | 4 | 3 | 4 | 4 | 3 | 3 | 3 | 2 | 4 | 4 | 3 | 4 | ALTO |
| A18 | Red WIFI estudiantes | 3 | 2 | 1 | 3 | 2 | 1 | 3 | 3 | 1 | 3 | 3 | 3 | 3 | MEDIO |
| A19 | Servidores de administración | 4 | 3 | 2 | 4 | 3 | 2 | 4 | 3 | 2 | 4 | 4 | 4 | 4 | ALTO |
| A20 | Servidores de bases de datos de producción | 4 | 3 | 2 | 4 | 2 | 2 | 4 | 2 | 2 | 4 | 4 | 4 | 4 | ALTO |
| A21 | Impresoras | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | BAJO |
| A22 | Aplicativo de nomina | 3 | 3 | 1 | 3 | 3 | 1 | 2 | 1 | 0 | 3 | 3 | 2 | 3 | MEDIO |
| A23 | Sistema de Gestión Documental | 2 | 2 | 1 | 2 | 2 | 1 | 1 | 1 | 0 | 2 | 2 | 1 | 2 | BAJO |
| A24 | Sistema de Gestión de Calidad | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | BAJO |
| A25 | Aplicativo WEB transaccional | 0 | 3 | 2 | 0 | 3 | 2 | 0 | 0 | 1 | 3 | 3 | 1 | 3 | MEDIO |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A26 | Página WEB | 1 | 3 | 3 | 1 | 3 | 3 | 1 | 1 | 2 | 3 | 3 | 2 | 3 | MEDIO |
| A27 | Intranet | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | BAJO |
| A28 | Aplicativos seguimiento proyectos | 0 | 2 | 2 | 0 | 2 | 2 | 0 | 2 | 2 | 2 | 2 | 2 | 2 | BAJO |
| A29 | Equipos de seguridad perimetral | 4 | 4 | 3 | 4 | 4 | 3 | 3 | 3 | 2 | 4 | 4 | 3 | 4 | ALTO |
| A30 | Aplicación Mesa de Ayuda | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | BAJO |
| A31 | Sistema Monitoreo de servicios | 0 | 2 | 0 | 0 | 2 | 0 | 0 | 2 | 0 | 2 | 2 | 2 | 2 | BAJO |
| A32 | Sistema de Control de Acceso | 1 | 3 | 0 | 1 | 3 | 0 | 0 | 1 | 0 | 3 | 3 | 1 | 3 | MEDIO |
| A33 | Herramienta de Virtualización | 4 | 4 | 3 | 4 | 4 | 3 | 4 | 4 | 3 | 4 | 4 | 4 | 4 | ALTO |
| A34 | Sistema Gestor Base de Datos | 4 | 4 | 3 | 4 | 4 | 3 | 3 | 2 | 2 | 4 | 4 | 3 | 4 | ALTO |
| A35 | Antivirus | 0 | 2 | 0 | 0 | 2 | 0 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | BAJO |
| A36 | Sistema administración de la plataforma SIMA | 4 | 4 | 3 | 4 | 4 | 3 | 4 | 4 | 3 | 4 | 4 | 4 | 4 | ALTO |
| A37 | Sistema de control de versiones | 0 | 2 | 0 | 0 | 2 | 0 | 0 | 0 | 0 | 2 | 2 | 0 | 2 | BAJO |
| A38 | CRM | 0 | 3 | 1 | 0 | 2 | 1 | 0 | 0 | 0 | 3 | 2 | 0 | 3 | MEDIO |
| A39 | Terminales empresariales | 0 | 3 | 0 | 0 | 3 | 1 | 0 | 0 | 0 | 3 | 3 | 0 | 3 | MEDIO |
| A40 | Directorio activo | 4 | 4 | 0 | 4 | 4 | 0 | 0 | 0 | 0 | 4 | 4 | 0 | 4 | ALTO |
| A41 | Correo Electrónico | 3 | 3 | 2 | 3 | 3 | 2 | 0 | 0 | 2 | 3 | 3 | 2 | 3 | MEDIO |
| A42 | Bases de datos | 4 | 4 | 2 | 4 | 4 | 2 | 0 | 0 | 2 | 4 | 4 | 2 | 4 | ALTO |
| A43 | FileServer | 4 | 4 | 2 | 4 | 4 | 2 | 0 | 0 | 2 | 4 | 4 | 2 | 4 | ALTO |
| A44 | Gestión de privilegios | 4 | 4 | 0 | 4 | 4 | 0 | 0 | 0 | 0 | 4 | 4 | 0 | 4 | ALTO |
| A45 | Identidad del Usuario | 2 | 4 | 1 | 2 | 4 | 1 | 0 | 0 | 2 | 4 | 4 | 2 | 4 | ALTO |
| A46 | Datos de autenticación | 4 | 4 | 1 | 3 | 4 | 1 | 0 | 0 | 2 | 4 | 4 | 2 | 4 | ALTO |
| A47 | Usuarios genéricos | 4 | 4 | 1 | 3 | 4 | 1 | 0 | 0 | 2 | 4 | 4 | 2 | 4 | ALTO |
| A48 | Log de evento de seguridad | 3 | 4 | 0 | 3 | 4 | 0 | 0 | 0 | 0 | 4 | 4 | 0 | 4 | ALTO |
| A49 | Registro de incidentes de seguridad | 3 | 4 | 0 | 3 | 4 | 0 | 0 | 0 | 0 | 4 | 4 | 0 | 4 | ALTO |
| A50 | Manuales técnicos de administración | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | BAJO |
| A51 | Bitácora de control de acceso al centro de computo | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | BAJO |
| A52 | Plan estratégico de tecnología | 2 | 2 | 0 | 1 | 2 | 2 | 0 | 0 | 0 | 2 | 2 | 0 | 2 | BAJO |
| A53 | Documentos del proceso | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | BAJO |

Fuente: El Autor

Tabla 16. Activos seleccionados para valoración de riesgos.

| N | Nombre del Activo | Nivel de Criticidad |
|---|---|---|
| A1 | Servidores de aplicaciones de producción | ALTO |
| A2 | Plataforma de Correo | MEDIO |
| A5 | SIMA | ALTO |
| A6 | Solución de Backup | MEDIO |
| A7 | Dispositivos de red | ALTO |
| A8 | Computadores Administradores | ALTO |
| A9 | Computadores de escritorio usuarios | MEDIO |
| A10 | Portátiles | MEDIO |
| A11 | Centro Principal de Procesamiento | ALTO |
| A12 | Centro Alterno de Procesamiento | ALTO |
| A13 | Cuartos de comunicaciones | MEDIO |
| A14 | Área administración de plataforma | ALTO |
| A15 | Red LAN | ALTO |
| A16 | Red WAN | ALTO |
| A17 | Red WIFI corporativa | ALTO |
| A18 | Red WIFI estudiantes | MEDIO |
| A19 | Servidores de administración | ALTO |
| A20 | Servidores de bases de datos de producción | ALTO |
| A22 | Aplicativo de nomina | MEDIO |
| A25 | Aplicativo WEB transaccional | MEDIO |
| A26 | Página WEB | MEDIO |
| A29 | Equipos de seguridad perimetral | ALTO |
| A32 | Sistema de Control de Acceso | MEDIO |
| A33 | Herramienta de Virtualización | ALTO |
| A34 | Sistema Gestor Base de Datos | ALTO |
| A36 | Sistema administración de la plataforma SIMA | ALTO |
| A38 | CRM | MEDIO |

| | | |
|---|---|---|
| A39 | Terminales empresariales | MEDIO |
| A40 | Directorio activo | ALTO |
| A41 | Correo Electrónico | MEDIO |
| A42 | Bases de datos | ALTO |
| A43 | FileServer | ALTO |
| A44 | Gestión de privilegios | ALTO |
| A45 | Identidad del Usuario | ALTO |
| A46 | Datos de autenticación | ALTO |
| A47 | Usuarios genéricos | ALTO |
| A48 | Log de evento de seguridad | ALTO |
| A49 | Registro de incidentes de seguridad | ALTO |

Fuente: El Autor

Teniendo en cuenta la información anterior se llevó a cabo la valoración de los Riegos a los que se exponen los activos de información, que se referenciaron en el proceso de tecnología dentro de las cuales tenemos las siguientes Acciones:

• Identificación de riesgo
• Análisis del riesgo

### 8.3.6 IDENTIFICACION DE AMENAZAS

Teniendo en cuenta la implementación de las políticas de seguridad informática para la Universidad, para ellos se detectaron las siguientes amenazas a las cuales se exponen los activos de información de la entidad y que fueron seleccionados para la valorización de riesgo, para lo cual se plantearon los siguientes interrogantes:

• ¿Cuál es la probabilidad de ocurrencia de la amenaza?
• ¿Cuál sería el impacto en caso de que ocurriera?
• ¿Cuáles de los criterios de seguridad afectaría, si la confidencialidad, la integridad o la disponibilidad?

Con el ánimo de facilitar el levantamiento de la información, se desarrolló una lista de riesgos de seguridad, que pueden afectar a cualquier empresa y las políticas de seguridad que se relacionan con la integridad, confidencialidad y disponibilidad.

Tabla 17. Lista de riesgos y principios de seguridad afectados.

| | PRINCIPIOS AFECTADOS | | |
|---|---|---|---|
| **RIESGOS** | **C** | **I** | **D** |
| Abuso de privilegios de acceso | X | X | |
| Acceso no autorizado | X | X | |
| Cambio de privilegios sin autorización | X | X | X |
| Errores del administrador | X | X | X |
| Instalación de software no autorizado | | X | X |
| Interceptación no autorizada de información en tránsito | X | | |
| Manipulación de la configuración | X | | |
| Modificación sin autorización | | X | |
| Denegación de Servicio | | | X |
| Divulgación o robo de información de autenticación | X | | |
| Divulgación no autorizada de información del negocio | X | | |
| Ejecución de ingeniería social | X | | |
| Pérdida o robo de información | X | | X |
| Suplantación de identidad de usuarios | X | X | |
| Uso inadecuado de sistemas para generar fraudes | X | X | |
| Uso inadecuado de sistemas que generan interrupción | | | X |
| Auditorias débiles | | | |

Fuente: El Autor

De acuerdo a la información anterior se detectaron las siguientes amenazas a la cual se exponen los activos para el proceso de valoración de riesgos:

Tabla 18. Amenazas que pueden afectar los activos de tecnología.

| Amenazas | Activos de tecnología que pueden ser afectados |
|---|---|
| Interrupción en los servicios | Bases de datos<br>Data Center del proveedor<br>Directorio Activo<br>Red LAN<br>Red WAN<br>Servidores de Producción |
| Modificación sin autorización | Bases de datos<br>Directorio Activo<br>Servidores de Administración<br>Servidores de bases de datos de producción Servidores de aplicaciones de producción<br>Plataforma de Correo |
| Robo de equipos | Área administración de plataforma<br>Cuartos de Rack<br>Data Center del proveedor |
| Robo de información | Bases de datos<br>Directorio Activo<br>Servidores de Administración<br>Servidores de bases de datos de producción<br>Plataforma de Correo |
| Divulgación de información de autenticación | Bases de Datos<br>Directorio Activo<br>Servidores de Administración |
| Error del administrador | Bases de datos<br>Data Center del proveedor<br>Directorio Activo<br>Red LAN<br>Red WAN<br>Servidores de Administración<br>Servidores de bases de datos de producción<br>Servidores de aplicaciones de producción<br>Plataforma de Correo<br>Equipos de seguridad perimetral |

| | |
|---|---|
| Instalación de software no autorizado | Directorio Activo<br>Computadores<br>Portátiles |
| Interceptación no autorizada de información en tránsito | Red LAN<br>Red WAN<br>Servicio de Correo |
| Acceso no autorizado | Área administración de plataforma<br>Bases de datos<br>Cuartos de Rack<br>Data Center del proveedor<br>Directorio Activo<br>Equipos de seguridad perimetral<br>Servidores de Administración<br>Servidores de bases de datos de producción<br>Servidores de aplicaciones de producción<br>Plataforma de Correo |
| Ataques externos / internos (hacking no ético) | Bases de datos<br>Equipos de seguridad perimetral<br>Servidores de Administración<br>Plataforma de Correo<br>Servidores de bases de datos de producción<br>Servidores de aplicaciones de producción<br>Data Center del proveedor |
| Cambio de privilegios sin autorización | Directorio Activo<br>Servidores de aplicaciones de producción<br>Servidores de Administración Plataforma de Correo<br>Bases de Datos<br>Servidores de bases de datos de producción |
| Desastres naturales | Data Center del proveedor |
| Suplantación de identidad de usuarios | Directorio Activo<br>Servicio de Correo |
| Uso inadecuado de sistemas para generar fraudes | Bases de datos<br>Directorio Activo<br>Servidores de Administración<br>Servidores de bases de datos de producción<br>Servidores de aplicaciones de producción<br>Plataforma de Correo |

| | |
|---|---|
| Uso inadecuado de sistemas que generan interrupción | Bases de datos<br>Data Center del proveedor<br>Directorio Activo<br>Red LAN<br>Red WAN<br>Servidores de Administración<br>Servidores de bases de datos de producción<br>Servidores de aplicaciones de producción<br>Plataforma de Correo |
| Abuso de privilegios | Data Center del proveedor<br>Directorio Activo<br>Servidores de Administración<br>Servidores de bases de datos de producción<br>Servidores de aplicaciones de producción<br>Plataforma de Correo |

Fuente: El Autor

A continuación se muestran las vulnerabilidades que están relacionadas a las amenazas identificadas y que tienen que ver con los activos del proceso de tecnología.

Tabla 19. Vulnerabilidad asociados a las amenazas de los activos.

| AMENAZAS | ACTIVOS DE TECNOLOGÍA QUE PUEDEN SER AFECTADO | VULNERABILIDADES |
|---|---|---|
| Interrupción en los servicios | Bases de datos.<br>Data Center del proveedor.<br>Directorio Activo.<br>Red LAN.<br>Red WAN.<br>Servidores de Producción. | Inadecuada Configuración y Capacidad de los ambientes.<br>Ausencia o inadecuado procedimiento de control de cambios.<br>Falta de mantenimiento de equipos. |
| Modificación sin autorización | Bases de datos.<br>Directorio Activo.<br>Servidores de Administración.<br>Servidores de bases de datos de producción Servidores de aplicaciones de producción.<br>Plataforma de Correo. | Políticas no aplicadas o no existencia de seguridad Inadecuada.<br>Administración o Asignación de roles y permisos.<br>Inadecuado mecanismo de cifrado. |
| Robo de equipos | Área administración de plataforma.<br>Cuartos de Rack.<br>Data Center del proveedor. | Políticas no aplicada o no existencia de seguridad Ausencia o inadecuado.<br>Plataforma de vigilancia física.<br>Inadecuado inventario de activos físicos<br>Ubicación física de los equipos. |
| Robo de información | Bases de datos.<br>Directorio Activo.<br>Servidores de Administración.<br>Servidores de bases de datos de producción.<br>Plataforma de Correo. | Inadecuada Administración de Seguridad<br>Ausencia o Inadecuada plataforma de Seguridad Perimetral.<br>Políticas no aplicadas o no existencia de seguridad Inadecuada.<br>Administración o Asignación de roles y permisos.<br>Inadecuado mecanismo de cifrado.<br>Inexistencia de Log de eventos de seguridad. |
| Divulgación de información de autenticación | Bases de Datos.<br>Directorio Activo.<br>Servidores de Administración. | Inadecuada Administración de Seguridad<br>Contraseñas no seguras.<br>Políticas no aplicada o no existencia de seguridad<br>Inadecuada Administración o Asignación de roles y permisos.<br>Inadecuado mecanismo de cifrado. |

| | | |
|---|---|---|
| Error del administrador | Bases de datos.<br>Data Center del proveedor<br>Directorio Activo.<br>Red LAN.<br>Red WAN.<br>Servidores de Administración.<br>Servidores de bases de datos de producción.<br>Servidores de aplicaciones de producción.<br>Plataforma de Correo.<br>Equipos de seguridad perimetral. | Ausencia de capacitación permanente.<br>Ausencia o inadecuado procedimiento de control de cambios.<br>Desmotivación del personal. |
| Instalación de software no autorizado | Directorio Activo.<br>Computadores.<br>Portátiles. | Políticas no aplicadas o no existencia de seguridad.<br>Inadecuada Administración o Asignación de roles y permisos. |
| Interceptación no autorizada de información en tránsito | Red LAN.<br>Red WAN.<br>Servicio de Correo. | Políticas no aplicadas o no existencia de seguridad.<br>Inadecuado mecanismo de cifrado. |
| Acceso no autorizado | Área administración de plataforma.<br>Bases de datos.<br>Cuartos de Rack.<br>Data Center del proveedor.<br>Directorio Activo.<br>Equipos de seguridad perimetral.<br>Servidores de Administración.<br>Servidores de bases de datos de producción.<br>Servidores de aplicaciones de producción.<br>Plataforma de Correo. | Inadecuada Administración de Seguridad<br>Ausencia o Inadecuada plataforma de Seguridad Perimetral.<br>Inadecuada Administración o Asignación de roles y permisos.<br>Ausencia de una configuración segura de la red.<br>Contraseñas no seguras.<br>Configuración incorrecta de las cuentas de usuario.<br>Falta de seguridad de los puertos de red.<br>Políticas no aplicadas o no existencia de seguridad. |
| Ataques externos / internos (hacking no ético) | Bases de datos.<br>Equipos de seguridad perimetral.<br>Servidores de Administración.<br>Plataforma de Correo.<br>Servidores de bases de datos de producción.<br>Servidores de aplicaciones de producción.<br>Data Center del proveedor. | Inadecuada Administración de Seguridad.<br>Ausencia o Inadecuada plataforma de Seguridad Perimetral.<br>Ausencia de una configuración segura de la red.<br>Falla de seguridad en los componentes de red. |
| Cambio de privilegios sin autorización | Directorio Activo.<br>Servidores de aplicaciones de producción.<br>Servidores de Administración.<br>Plataforma de Correo.<br>Bases de Datos.<br>Servidores de bases de datos de producción. | Contraseñas no seguras.<br>Inadecuada Administración o Asignación de roles y permisos.<br>Inadecuada Administración de Seguridad<br>Políticas no aplicada o no existencia de seguridad. |

| | | |
|---|---|---|
| Desastres naturales | Data Center del proveedor. | Ausencia de un sistema de continuidad de negocio.<br>Ubicación física de los equipos.<br>Ubicación física del centro de cómputo.<br>Políticas no aplicadas o no existencia de seguridad física. |
| Suplantación de identidad de usuarios | Directorio Activo.<br>Servicio de Correo. | Contraseñas no seguras.<br>Cuentas de usuario sin auditar.<br>Ausencia o inadecuado plataforma de vigilancia física.<br>Inadecuado mecanismo de cifrado. |
| Uso inadecuado de sistemas para generar fraudes | Bases de datos.<br>Directorio Activo<br>Servidores de Administración.<br>Servidores de bases de datos de producción.<br>Servidores de aplicaciones de producción.<br>Plataforma de Correo. | Inadecuada Administración de Seguridad<br>Cuentas de usuario sin auditar.<br>Inexistencia de Log de eventos de seguridad.<br>Inadecuada Administración o Asignación de roles y permisos.<br>Políticas no aplicadas o no existencia de seguridad. |
| Uso inadecuado de sistemas que generan interrupción | Bases de datos.<br>Data Center del proveedor.<br>Directorio Activo.<br>Red LAN.<br>Red WAN.<br>Servidores de Administración.<br>Servidores de bases de datos de producción.<br>Servidores de aplicaciones de producción.<br>Plataforma de Correo. | Inadecuada Administración de Seguridad<br>Cuentas de usuario sin auditar.<br>Inexistencia de Log de eventos de seguridad.<br>Inadecuada Administración o Asignación de roles y permisos.<br>Políticas no aplicadas o no existencia de seguridad. |
| Abuso de privilegios | Data Center del proveedor.<br>Directorio Activo.<br>Servidores de Administración.<br>Servidores de bases de datos de producción.<br>Servidores de aplicaciones de producción.<br>Plataforma de Correo. | Cuentas de usuario sin auditar.<br>Contraseñas no seguras.<br>Inexistencia de Log de eventos de seguridad.<br>Inadecuada Administración o Asignación de roles y permisos.<br>Políticas no aplicadas o no existencia de seguridad. |

Fuente: El Autor

### 8.3.7 ANALISIS DEL RIESGO

Una vez realizado el análisis de los riesgos se estableció la ocurrencia probable de los riesgos y el impacto que representan los mismos en la entidad, lo que nos llevó a obtener el nivel de riesgo inherente, basado en las medidas y controles de seguridad que se llevan a cabo en la Universidad, lo que permite minimizar los riesgos.

Con el ánimo de tener la ocurrencia de una amenaza en cada uno de los activos de información se desarrollaron los siguientes criterios de valoración:

Tabla 20. Valoración probabilidad de ocurrencia.

| **Probabilidad de ocurrencia en un (1) años** | **Valor Cualitativo** | **Valor Asignado** |
|---|---|---|
| Una vez cada año | Raro | 1 |
| Una vez cada seis (6) meses | Baja (Improbable) | 2 |
| Una vez cada tres (3) meses | Media (Posible) | 3 |
| Una vez cada mes | Alta (Probable) | 4 |
| Más de una vez al mes | Muy Alta | 5 |

Fuente: El Autor

Con el ánimo de determinar el impacto que puede tener la perdida de disponibilidad, confidencialidad e integridad en los activos de información se trabajó en los siguientes criterios de valoración:

Tabla 21. Valoración del Impacto.

| IMPACTO | IMPACTO CUANTITATIVO (PORCENTAJE SOBRE UTILIDAD OPERACIONAL) | IMPACTO CUALITATIVO (UNO O MÁS FACTORES) | VALOR |
|---|---|---|---|
| INSIGNIFICANTE | Genera pérdidas financieras pequeñas no significativas. (Perdida Menor o igual a 0.25%) | No afecta la seguridad de la información de la entidad.<br>No afecta la imagen de la entidad ante las partes interesadas.<br>Genera reprocesos insignificantes.<br>La información se puede recuperar.<br>Rápidamente con la misma calidad. | 1 |
| MENOR | Genera pérdidas financieras menores no significativas. (Perdida Mayor a 0.25% y menor o igual a 5%) | No afecta la seguridad de la información de la entidad.<br>Afecta en menor grado la imagen de la entidad ante las partes interesadas.<br>Genera reprocesos menores.<br>La información se puede recuperar en un Tiempo moderado con la misma calidad. | 2 |
| MODERADO | Genera pérdidas financieras moderadas. (Mayor a 5% y menor o igual a 20%) | Afecta en menor grado la seguridad de la información de la entidad.<br>Afecta medianamente la imagen de la entidad ante las partes interesadas.<br>Genera reprocesos moderados.<br>La información se puede recuperar pero no con la misma calidad | 3 |
| MAYOR | Genera pérdidas financieras mayores. (Perdida mayor o igual a 20% y menor a 50%) | Afecta en mayor grado la seguridad de la información de la entidad.<br>Afecta altamente la imagen de la entidad ante las partes interesadas.<br>Genera reprocesos mayores.<br>Es difícil recuperar la información | 4 |
| CATASTRÓFICO | Genera pérdidas financieras críticas. (Perdidas Mayores a 50%) | Afectar seriamente la seguridad de la información de la entidad.<br>Afecta gravemente la imagen de la empresa ante las partes interesadas.<br>Puede generar pérdida masiva de clientes.<br>Genera alto nivel de reprocesos.<br>Es difícil y costoso recuperar la Información.<br>Afecta la continuidad del negocio | 5 |

Fuente: El Autor

Teniendo en cuenta que el riesgo inherente es igual al valor de la probabilidad X valor del impacto, se puede clasificar el riesgo ya sea inherente o residual dependiente de su nivel de riesgo, para ello se utilizaron los siguientes criterios de valoración que permiten determinar el riesgo:

Tabla 22. Valoración de los Riesgos.

| Tipo de riesgo | Valor Nivel Riesgo | Acción requerida |
|---|---|---|
| **Riesgo Extremo** | Nivel Riesgo mayor o igual a 15 puntos | Requiere acciones inmediatas que permitan reducir y compartir el riesgo, transferirlo o incluso evitarlo |
| **Riesgo Alto** | Nivel Riesgo mayor o igual a 10 y menor a 15 puntos | Requieren atención urgente e implementar medidas para reducir el nivel del riesgo |
| **Riesgo Medio** | Nivel Riesgo mayor o igual a 5 y menor a 10 puntos | Requiere de medidas prontas y adecuadas que permitan disminuir el riesgo a nivel bajo o inusual |
| **Riesgo Bajo** | Nivel Riesgo mayor o igual a 3 y menor a 5 puntos | El riesgo se mitiga con actividades propias y por medio de algunas medidas preventivas para reducir el riesgo |
| **Riesgo Inusual** | Nivel Riesgo Menor a 3 puntos | Se puede aceptar el riesgo sin necesidad de tomar otras medidas de control diferentes a las existentes. |

Fuente: El Autor

Tabla 23. Valoración de riesgos de la Dirección de Tecnología.

| | VALORACION IMPACTO | | | | ESTIMACION DE RIESGO | | | |
|---|---|---|---|---|---|---|---|---|
| **RIESGOS** | **D** | **I** | **C** | **Probabilidad** | **D** | **I** | **C** | **Nivel de Riesgo** |
| R1. Acceso no autorizado | | Mayor | Catastrófico | Alta | | Riesgo Extremo | Riesgo Extremo | Riesgo Extremo |
| R2. Ataques externos / internos (hacking no ético) | Mayor | | Mayor | Alta | Riesgo Extremo | | Riesgo Extremo | Riesgo Extremo |
| R3. Cambio de privilegios sin autorización | Moderado | Moderado | Moderado | Alta | Riesgo Alto | Riesgo Alto | Riesgo Alto | Riesgo Alto |
| R4. Desastres naturales (Terremotos, Incendios, Inundaciones, etc.) | Mayor | | | Raro | Riesgo bajo | | | Riesgo bajo |
| R5. Divulgación de información de autenticación | | | Moderado | Media | | | Riesgo Medio | Riesgo Medio |
| R6. Error del administrador | Moderado | | | Alta | Riesgo Alto | | | Riesgo Alto |
| R7. Instalación de software no autorizado | | Menor | | Media | | Riesgo Medio | | Riesgo Medio |
| R8. Interceptación no autorizada de información en tránsito | | Mayor | Mayor | Alta | | Riesgo Extremo | Riesgo Extremo | Riesgo Extremo |
| R9. Interrupción en los servicios | Moderado | | | Media | Riesgo Medio | | | Riesgo Medio |
| R10. Modificación sin autorización | | Moderado | | Media | | Riesgo Medio | | Riesgo Medio |
| R11. Robo de equipos | Moderado | | | Media | Riesgo Medio | | | Riesgo Medio |
| R12. Robo de información | Mayor | | Mayor | Media | Riesgo Alto | | Riesgo Alto | Riesgo Alto |
| R13. Suplantación de identidad de usuarios | | | Moderado | Baja | | | Riesgo Medio | Riesgo Medio |
| R14. Uso inadecuado de sistemas para generar fraudes | | | Mayor | Baja | | | Riesgo Medio | Riesgo Medio |
| R15. Uso inadecuado de sistemas que generan interrupción | Mayor | | | Baja | Riesgo Medio | | | Riesgo Medio |
| R16. Abuso de privilegios | | Mayor | Mayor | Alta | | Riesgo Extremo | Riesgo Extremo | Riesgo Extremo |

Fuente: El Autor

**D: Disponibilidad, I: Integridad, C: Confidencialidad**

## 8.4 DISEÑO DE POLITICAS

Con la constante exposición que presenta la información que se produce todos los días en el centro tutorial Mompox bolívar de la Universidad de Cartagena a través de las herramientas, tanto software como de hardware buscando minimizar el impacto con respecto a una eventual materialización de amenaza a la que está expuesta la universidad, en lo que respecta a Seguridad Informática.

Por lo anterior no solo se trata de la implementación de controles, debido a que la información aunque se procesa por medio de hardware y software, son los usuarios quienes la manejan, ingresando documentos, intercambiando información, convierten informes, para este caso es pertinente que la Universidad de Cartagena implemente políticas de seguridad informática, que deben estar dirigidas a funcionarios y estudiantes en determinados procesos, con el objetivo de proteger el activo más importante del alma mater la información.

A continuación se plantean Políticas de Seguridad Informática cuyo propósito, como se mencionó anteriormente, es salvaguardar los activos de información de la Universidad de Cartagena Centro Tutorial Mompox:

### 8.4.1 INTRODUCCIÓN

Con el ánimo de mejorar la estrategia de Seguridad de la información de Universidad de Cartagena Centro Tutorial Mompox Bolívar, surge la necesidad de buscar un modelo base que permita alinear los procesos hacia un mismo objetivo de seguridad en el manejo de la información.

Para tal fin, se establece una Política de la Seguridad de la Información, como marco de trabajo de la organización en lo referente al uso adecuado de los recursos, buscando niveles adecuados de protección y resguardo de la información, definiendo sus lineamientos, para garantizar el debido control y minimizar los riesgos asociados.

### 8.4.2 OBJETIVO

Este documento formaliza el compromiso de la dirección frente a la gestión de la seguridad de la información y presenta de forma escrita a los usuarios de sistemas de información el compendio de acciones con las cuales la Universidad de Cartagena Centro Tutorial Mompox Bolívar establece las normas para proteger de

posibles riesgos de daño, pérdida y uso indebido de la información, los equipos y demás recursos informáticos de la Entidad, los cuales están en constante cambio y evolución de acuerdo con el avance de la tecnología y los requerimientos de la Entidad.

El presente documento define los lineamientos que debe seguir la Universidad de Cartagena Centro Tutorial Mompox Bolívar, con relación a la seguridad de la Información. Estos lineamientos están escritos en forma de políticas.

### 8.4.3 ALCANCE

El documento de Política de Seguridad de la Información reglamenta la protección y uso de los activos de información de la Universidad de Cartagena Centro Tutorial Mompox Bolívar, y por tanto está dirigido a todos aquellos usuarios que posean algún tipo de contacto con estos activos. Los usuarios de los activos de información de la Entidad deberán diligenciar un acuerdo de confidencialidad, que los compromete con el cumplimiento de las políticas de seguridad aquí descritas. Los usuarios de los activos de información de la Entidad se han clasificado así:

Colaboradores de Planta: se definen como colaboradores de planta aquellas personas que han suscrito un contrato laboral con la Entidad.

Funcionarios de la Universidad de Cartagena Centro Tutorial Mompox Bolívar: Se definen como los empleados de la Universidad que son susceptibles de manipular sistemas de información.

Contratistas: se definen como contratistas a aquellas personas que han suscrito un contrato con la Entidad y que pueden ser:
Colaboradores en Misión;
Colaboradores por Outsourcing: son aquellas personas que laboran en la Entidad y tienen contrato con empresas de suministro de servicios y que dependen de ellos, Personas naturales que prestan servicios independientes a la Entidad, Proveedores de recursos informáticos. Entidades de Control Procuraduría; Revisoría Fiscal; Contraloría General de la República; Ministerio de Educación Nacional. Otras Entidades.

### 8.4.4 REQUISITOS LEGALES Y/O REGLAMENTARIOS

Para la implementación de la estrategia de seguridad de la información, la Universidad de Cartagena Centro Tutorial Mompox Bolívar, debe regirse por lo

dispuesto en el marco jurídico y normativo aplicable a las Universidades Publicas o entidades que las regulan y aglutinan.

### 8.4.5 RESPONSABLE

#### 8.4.5.1 COMPROMISO DE LA DIRECCIÓN

La dirección debe brindar evidencia de su compromiso con el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de los mecanismos para asegurar información:

- Mediante el establecimiento de una política de seguridad de la información;
- Asegurando que se establezcan objetivos y planes de seguridad de la información;
- Estableciendo funciones y responsabilidades de la seguridad de la información;
- Comunicando a la organización la importancia de cumplir los objetivos de seguridad de la información, las responsabilidades legales, y la necesidades de la mejora continua;

Asegurando que se realizan auditorías internas.

#### 8.4.5.2 GESTIÓN DE LOS RECURSOS

- Asegurar que las políticas de seguridad de la información brindan apoyo al cumplimiento de la misión y visión de La Universidad.
- Identificar y atender los requisitos legales y reglamentarios, así como las obligaciones de seguridad contractuales;
- Mantener la seguridad suficiente mediante la aplicación correcta de todos los controles implementados;
- Asegurar que todo el personal tiene conciencia de la importancia de la seguridad de la información.

#### 8.4.5.3 PROCEDIMIENTO

##### COMUNICACIÓN DE LAS POLITICAS DE SEGURIDAD:

Los miembros del Comité de Seguridad, conscientes que los recursos de información son utilizados de manera permanente por los usuarios que acceden a diferentes servicios, definidos en este documento, han considerado oportuno transmitir a los mismos las normas de comportamiento básicas en la utilización de los equipos de cómputo y demás recursos tecnológicos y de información.

##### APLICACIÓN DE LAS POLITICAS DE SEGURIDAD

Las políticas de seguridad informática se orientan a reducir el riesgo de incidentes de seguridad y minimizar su efecto. Establecen las reglas básicas con las cuales la organización debe operar sus recursos informáticos. El diseño de las políticas de seguridad informática está encaminado a disminuir y eliminar muchos factores de riesgo, principalmente la ocurrencia.

### 8.4.6 POLÍTICA DE SEGURIDAD DE LA UNIVERSIDAD DE CARTAGENA CENTRO TUTORIAL MOMPOX.

La Universidad de Cartagena reconoce abiertamente la importancia de la seguridad de la información así como la necesidad de su protección para constituir un activo estratégico de la organización y todas las partes interesadas, el no uso adecuado de los activos de información puede poner en peligro la continuidad del negocio o al menos suponer daños muy importantes que afecten el normal funcionamiento de los procesos.

Los funcionarios, terceros y usuarios en general deberán conocer el presente documento, normas, reglas, estándares y procedimientos que apliquen según las funciones que realicen para la organización, el desconocimiento que conlleve a la violación de lo anteriormente mencionado representará para la persona involucrada las sanciones disciplinarias que apliquen según el incidente presentado.

Igualmente se implementarán los controles de seguridad encaminados a garantizar la confidencialidad, integridad y disponibilidad de los activos de información de La Universidad con el objetivo de lograr un nivel de riesgo aceptable de acuerdo con la visión, misión, planeación y estrategia de la compañía, y dando cumplimiento al marco jurídico aplicable a los estándares nacionales.

### 8.4.7 POLÍTICAS GENERALES DE SEGURIDAD INFORMÁTICA

Estas normas son de obligatorio cumplimiento por parte de todos los usuarios de recursos informáticos y se han clasificado en:

- ✓ Políticas de Cumplimiento y Sanciones
- ✓ Políticas de uso de recursos informáticos.
- ✓ Políticas de contraseñas.
- ✓ Políticas de uso de la información.
- ✓ Políticas del uso de Internet y correo electrónico.
- ✓ Políticas de uso de la Intranet y Sitio Web de La Universidad de Cartagena
- ✓ Políticas Generales de la Rectoría.
- ✓ Políticas para Desarrolladores de Software.
- ✓ Políticas para Administradores de Sistemas.
- ✓ Políticas de Copias de respaldo.
- ✓ Políticas de Uso de Firewall.
- ✓ Políticas para Usuarios previstos en el numeral tercero.
- ✓ Políticas de Acceso Físico.

#### 8.4.7.1 POLÍTICAS DE CUMPLIMIENTO Y SANCIONES

##### 8.4.7.1.1 Cumplimiento con la seguridad de la información.

Todos los colaboradores de la organización, así como los contratistas, deben cumplir y acatar el manual de políticas y los procedimientos en materia de protección y seguridad de la información. Corresponde velar por su estricto cumplimiento a la Rectoría de La Universidad y al comité de seguridad.

##### 8.4.7.1.2 Medidas disciplinarias por incumplimiento de políticas de seguridad

Todo incumplimiento de una política de seguridad de la información por parte de un funcionario o contratista, así como de cualquier estándar o procedimiento es causa

para iniciar acciones disciplinarias, las cuales de acuerdo a su gravedad pueden suponer la terminación de la vinculación laboral del empleado o contratista.

Si el incumplimiento se origina en alguna sede de La Universidad, esta podrá suspender la prestación de cualquier servicio de información.

#### 8.4.7.2 POLÍTICAS DE USO DE RECURSOS INFORMÁTICOS

##### 8.4.7.2.1 Instrucciones para el uso de recursos informáticos.

El uso de cualquier sistema de información y demás recursos informáticos por parte del empleado, trabajadores o usuarios de los sistemas de la Universidad, debe someterse a todas las instrucciones técnicas, que imparta el comité de seguridad.

##### 8.4.7.2.2 Uso personal de los recursos

Los recursos informáticos de La Universidad, dispuestos para la operación, solo deben ser usados para fines laborales. El producto del uso de dichos recursos tecnológicos será de propiedad de la Entidad y estará catalogado como lo consagran las políticas de la Entidad. Cualquier otro uso está sujeto a previa autorización de la Presidencia.

##### 8.4.7.2.3 Acuerdo de confidencialidad

Para el uso de los recursos tecnológicos de La Universidad, todo usuario debe firmar un acuerdo de confidencialidad y un acuerdo de Seguridad de los sistemas de información antes de que le sea otorgado su Login de acceso a la red y sus respectivos privilegios o medios de instalación.

- Prohibición de instalación de software y hardware en los computadores de La Universidad.

La instalación de hardware o software, la reparación o retiro de cualquier parte o elemento en los equipos de computación o demás recursos informáticos solo puede ser realizada por los funcionarios de sistemas autorizados por la Universidad.

##### 8.4.7.2.4 Uso del aplicativo entregados

La Universidad ha suscrito con los fabricantes y proveedores un contrato de “LICENCIA DE USO” para los aplicativos que utiliza. Está terminantemente prohibido copiar cualquiera de los aplicativos que se aloja en los computadores de

la Entidad, esto se asegura con la firma del Acuerdo de Confidencialidad para los usuarios y con la firma del contrato realizado con los proveedores que maneje información de uso restringido a La Universidad Adicional a esto cada usuario, dependiendo de las actividades que realice sobre las aplicaciones maneja un perfil limitado, de esta forma es controlado el acceso.

8.4.7.2.5 El usuario es responsable por toda actividad que involucre su identificación personal o recursos informáticos asignados.

Todo usuario es responsable por todas las actividades relacionadas con su identificación. La identificación no puede ser usada por otro individuo diferente a quien esta le fue otorgada. Los usuarios no deben permitir que ninguna otra persona realice labores bajo su identidad. De forma similar, los usuarios no deben realizar actividades bajo la identidad de alguien más. La utilización de los recursos informáticos por parte de terceras personas con conocimiento o consentimiento del usuario, o por su descuido o negligencia, lo hace responsable de los posibles daños que estas personas ocasionen a los equipos o a la propiedad de La Universidad.

8.4.7.2.6 Declaración de reserva de derechos de La Universidad

La Universidad usa controles de acceso y otras medidas de seguridad para proteger la confidencialidad, integridad y disponibilidad de la información manejada por computadores y sistemas de información. Para mantener estos objetivos La Universidad se reserva el derecho y la autoridad de:
1. Restringir o revocar los privilegios de cualquier usuario;
2. Inspeccionar, copiar, remover cualquier dato, programa u otro recurso que vaya en contra de los objetivos antes planteados; y,
3. Tomar cualquier medida necesaria para manejar y proteger los sistemas de información de La Universidad. Esta autoridad se puede ejercer con o sin conocimiento de los usuarios, bajo la responsabilidad del comité de seguridad siempre con el concurso de la Rectoría o de quién él delegue esta función.

8.4.7.2.7 Recursos compartidos.

Está terminantemente prohibido compartir los discos duros o las carpetas de los computadores de escritorio, aunque estén protegidos por contraseña. Cuando exista la necesidad de compartir recursos esto se debe hacer con autorización previa y restringir por Dominio.

8.4.7.2.8 Todo monitoreo debe ser registrado e informado al jefe inmediato del usuario.

Un usuario puede ser monitoreado bajo previa autorización del comité de seguridad.

8.4.7.2.9 Acceso no autorizado a los sistemas de información de la Entidad.

Está totalmente prohibido obtener acceso a sistemas de información a los que no se tiene privilegios y de alguna forma dañar o alterar la operación de dichos sistemas. Esto implica la prohibición de capturar contraseñas, llaves de encripción y otros mecanismos de control de acceso que le puedan permitir obtener ingreso a sistemas no autorizados.

8.4.7.2.10 Posibilidad de acceso no implica permiso de uso.

Los usuarios no deben leer, modificar, copiar o borrar información perteneciente a otro usuario sin la debida autorización de este.

8.4.7.2.11 Prohibición a la explotación de vulnerabilidades de seguridad de los recursos informáticos.

A no ser que exista una aprobación por escrito para ello o sea parte de su función laboral, los usuarios no deben explotar las deficiencias de seguridad de los sistemas de información para dañar los sistemas o la información contenida en ellos, obtener acceso a recursos a los cuales no se le ha dado acceso. En el caso de encontrar vulnerabilidades, estas deben ser reportadas de inmediato al comité de seguridad.

8.4.7.2.12 Manejo de sesiones en sistemas informáticos.

Si el usuario está conectado a un sistema que contiene información sensible, éste no debe dejar el computador desatendido sin cerrar primero la sesión iniciada.

8.4.7.2.13 Notificación de sospecha de pérdida, divulgación ó uso indebido de información.

Cualquier incidente de Seguridad debe reportarse por escrito al correo electrónico del comité de seguridad.

8.4.7.2.14 Etiquetado y presentación de información de tipo confidencial a

los usuarios de computadores.

Toda la información que sea crítica para la organización debe ser etiquetada de acuerdo a los niveles establecidos en el presente documento: USO INTERNO y CONFIDENCIAL.

8.4.7.2.15 Traslado de equipos debe estar autorizado.

Ningún equipo de cómputo debe ser reubicado o trasladado dentro o fuera de las instalaciones de La Universidad sin previa autorización. Así mismo, ningún equipo de cómputo debe ser reubicado o trasladado de las instalaciones de la sede a la cual fue asignado. El traslado de los equipos se debe hacer con las medidas de seguridad necesarias, por el personal de sistemas autorizado.

8.4.7.2.16 Control de recursos informáticos entregados a los usuarios.

Cuando un usuario inicie su relación laboral con La Universidad se debe diligenciar el documento de entrega de inventario.

Cuando un empleado termine su vinculación laboral con la Entidad, sea trasladado a otra dependencia o por alguna otra circunstancia deje de utilizar el computador personal o el recurso tecnológico suministrado con carácter permanente, deberá hacerse una validación de lo entregado por el usuario contra lo registrado en el formato de descargue de inventario (Firmado). El empleado será responsable de los deterioros o daños que por su negligencia haya ocasionado a los equipos de hardware.

Cuando un funcionario de La Universidad inicie su relación laboral se debe diligenciar el documento de entrega de inventario.

8.4.7.2.17 Configuración de sistema operativo de las estaciones de trabajo.

Solamente los funcionarios del área técnica de sistemas están autorizados para cambiar la configuración del sistema operativo de las estaciones de trabajo de los usuarios.

8.4.7.2.18 Uso restringido de módems en las estaciones de trabajo.

Queda prohibido el uso de módems en las estaciones de trabajo que permitan obtener una conexión directa a redes externas como Internet a menos que se cuente con aprobación escrita por parte de Comité de Seguridad.

#### 8.4.7.2.19 Protección por Defecto de Copyright

Todos los colaboradores de La Universidad deben revisar, e investigar los derechos de propiedad intelectual para todo material como libros, artículos, informes, imágenes, software y/o sitio Web encontrado en Internet antes de ser usado para cualquier propósito con el fin de asegurar el cumplimiento de las leyes que aplican para este tipo de información.
Regularmente se deben realizar actividades de monitoreo sobre el software instalado en cada uno de los equipos de la organización, lo anterior para asegurar que los programas instalados correspondan correctamente con las licencias adquiridas por la empresa.

#### 8.4.7.2.20 Custodia de Licencias de Software.

Las licencias deben ser custodiadas y controladas por el área de tecnología. Esta área debe realizar auditorías de licencia de software como mínimo una vez al año generando las evidencias respectivas, lo anterior para garantizar que los funcionarios solo tienen instalado software legal y autorizado por el jefe de cada área.

#### 8.4.7.2.21 Apagado de equipos en la noche.

Con fin de proteger la seguridad y distribuir bien los recursos de la empresa, los equipos de cómputo deben quedar apagados cada vez que no haya presencia de funcionarios en la oficina durante la noche.

#### 8.4.7.2.22 Tiempo limitado de conexión en aplicaciones de alto riesgo.

Si el usuario está conectado a un sistema que contiene información sensible, y este presenta un tiempo de inactividad corto la aplicación deberá cerrar la sesión iniciada por el usuario.

### 8.4.7.3 POLÍTICAS DE USO DE LAS CONTRASEÑAS.

#### 8.4.7.3.1 Confidencialidad de las contraseñas.

La contraseña que cada usuario asigna para el acceso a los sistemas de información, debe ser personal, confidencial e intransferible. Cada usuario debe velar porque sus contraseñas no sean vistas y aprendidas por otras personas.

#### 8.4.7.3.2 Uso de diferentes contraseñas para diferentes recursos informáticos.

Para impedir el compromiso de múltiples recursos informáticos, cada usuario deberá utilizar diferentes contraseñas para cada recurso al que tiene acceso. Esto involucra así mismo a los equipos de comunicación (firewall, routers, servidores de control de acceso) y a los administradores de los mismos.

#### 8.4.7.3.3 Identificación única para cada usuario.

Cada usuario tendrá una identificación única en cada sistema al que tenga acceso (usuario), acompañado de un elemento para su autenticación (contraseña) de carácter personal y confidencial para la utilización de los recursos tecnológicos necesarios para sus labores. Esta política rige para aplicativos implementados hasta la fecha de liberación de este documento. Los funcionarios contarán con una identificación única personal y su respectiva contraseña asignada por el encargado por el área de tecnología de La Universidad.

#### 8.4.7.3.4 Cambios periódicos de contraseñas.

Todos los usuarios deben ser automáticamente forzados a cambiar su contraseña por lo menos una vez cada 30 días.

#### 8.4.7.3.5 Longitud mínima de contraseñas.

Todas las contraseñas deben tener una longitud mínima de OCHO (8) caracteres que debe cumplir con algunas de las siguientes características: Incluir combinación de números, letras mayúsculas, minúsculas y caracteres especiales. Este tamaño debe ser validado por el sistema en el momento de generar la contraseña para impedir un tamaño menor.

#### 8.4.7.3.6 Contraseñas fuertes.

Las contraseñas no deben ser nombres propios ni palabras del diccionario, debe ser una mezcla de números, letras y caracteres especiales.

8.4.7.3.7 Prohibición de contraseñas cíclicas.

No se debe generar contraseñas compuestas por una combinación fija de caracteres y una combinación variable pero predecible. Un ejemplo de este tipo de contraseñas prohibidas es “Enero-2004” que según la política “Contraseñas fuertes”, es una contraseña válida, pero al mes siguiente pasa a ser “Febrero-2004” y así sucesivamente.

8.4.7.3.8 Las contraseñas creadas por usuarios no deben ser reutilizadas.

El usuario no debe generar una contraseña idéntica o sustancialmente similar a una que ya haya utilizado anteriormente. Esta política es complementada por la política “Prohibición de contraseñas cíclicas”.

8.4.7.3.9 Almacenamiento de contraseñas.

Ninguna contraseña debe ser guardada de forma legible en archivos “batch”, scripts, macros, teclas de función de terminal, archivos de texto, en computadores o en otras ubicaciones en donde personas no autorizadas puedan descubrirlas o usarlas. Ningún usuario bajo ninguna circunstancia está autorizado para tener su contraseña en cualquier medio impreso, con excepción de lo contemplado en la política “Almacenamiento de contraseñas de administrador”.

8.4.7.3.10 Sospechas de compromiso deben forzar cambios de contraseña.

Toda contraseña deberá ser cambiada de forma inmediata si se sospecha o se conoce que ha perdido su confidencialidad.

8.4.7.3.11 Revelación de contraseñas prohibida.

Bajo ninguna circunstancia está permitido revelar la contraseña a empleados o a terceras personas. La contraseña personal no debe ser digitada en presencia de terceras personas, así sean funcionarios de la Entidad. Ningún usuario deberá intentar obtener contraseñas de otros usuarios, excluyendo lo contemplado en la política “Auditoria periódica a las contraseñas de los usuarios”.

8.4.7.3.12 Bloqueo estación de trabajo.

Todas las estaciones de trabajo de los usuarios deben tener activado el bloqueo automático de estación, el cual debe activarse luego de un período de ausencia o inactividad de 3 min. Por otra parte el escritorio del equipo de trabajo debe estar despejado y ordenado, de tal forma que la información que se encuentre en el puesto de trabajo o en la pantalla (escritorio) del equipo sea estrictamente la suficiente y necesaria para la labor desempeñada.

#### 8.4.7.3.13 Reporte de cambio en las responsabilidades de los usuarios al Administrador del Sistema.

El ingeniero en soporte y web master debe reportar por medio de un correo electrónico, de manera oportuna al área de sistemas, todos los cambios significantes en las responsabilidades de un usuario, de su estado laboral, de su ubicación dentro de la organización, con el fin de mantener el principio de seguridad de la información.

### 8.4.7.4 POLÍTICAS DE USO DE LA INFORMACIÓN

#### 8.4.7.4.1 Divulgación de la información manejada por los usuarios de La Universidad

La Universidad podrá divulgar la información de un usuario almacenada en los sistemas de acuerdo con la autorización suscrita por él mismo, por disposición legal, por solicitud de autoridad judicial o administrativa salvo las excepciones indicadas en este documento y las disposiciones legales de protección de datos personales. Se deja claridad que la información pública proveniente de la función registral es administrada exclusivamente para los fines propios de los registros públicos de acuerdo con las normas legales y reglamentarias vigentes sobre la materia. La información proveniente de las demás funciones de la Universidad es administrada y conservada, observando las disposiciones propias del régimen de protección de datos personales, garantizando la privacidad de la información, previamente clasificada, salvó autorización del titular de la misma para su divulgación.

#### 8.4.7.4.2 Transferencia de datos solo a organizaciones con suficientes controles.

La Universidad puede transmitir información privada solamente a terceros que por escrito se comprometan a mantener dicha información bajo controles adecuados de

protección. Se da una excepción en casos en los que la divulgación de información es forzada por la ley.

8.4.7.4.3 Registro de las compañías que reciben información privada.

El personal de La Universidad que liberó información privada a terceros debe mantener un registro de toda divulgación y este debe contener qué información fue revelada, a quién fue revelada y la fecha de divulgación.

8.4.7.4.4 Transferencia de la custodia de información de un funcionario que deja la Universidad.

Cuando un empleado se retira de La Universidad, su jefe inmediato debe revisar tanto los archivos magnéticos, correo electrónico como documentos impresos para determinar quién se encargará de dicha información o para ejecutar los métodos para la destrucción de la información.

8.4.7.4.5 Transporte de datos sensibles en medios legibles.

Si se transporta información sensible en medios legibles por el computador (disquetes, cintas magnéticas, CD´s, memorias USB), la información deberá ser encriptada, siempre y cuando el receptor acepte el intercambio de datos cifrados. Para equipos portátiles este tipo de información es asegurada mediante una aplicación de cifrado.

8.4.7.4.6 Datos sensibles enviados a través de redes externas deben estar encriptados.

Si se ha de transmitir datos sensibles a través de cualquier canal de comunicación externo, dichos datos deben ser enviados en forma encriptada, siempre y cuando el receptor tenga los recursos necesarios y acepte el intercambio de datos cifrados.

8.4.7.4.7 Clasificación de la Información

- Todos los activos deben estar claramente identificados y se debe elaborar y mantener un inventario de todos los activos importantes.

- Toda la información y los activos asociados con los servicios de procesamiento de la información deben ser “propiedad” de una parte designada de La Universidad.
- Se deben identificar, documentar e implementar las reglas sobre el uso aceptable de la información y de los activos asociados con los servicios de procesamiento de la información.
- Cualquier uso de servicio de procesamiento de información debe ser autorizado por el Jefe de TI de las Universidad según el caso, por lo anterior cualquier acceso a un servicio no autorizado es prohibido y de esto deben tener conocimiento todos los usuarios involucrados.

#### 8.4.7.4.8 Eliminación Segura de la Información en Medios Informáticos

Todo medio informático reutilizable de terceros como equipos rentados, discos externos, memorias USB, etc. utilizados por La Universidad, antes de su entrega se les realizara un proceso de borrado seguro en la información.

#### 8.4.7.4.9 Eliminación segura de la información en medios físicos.

Cualquier documento físico que haya sido considerado y clasificado de carácter confidencial y que necesite ser destruido, debe realizarse en la respectiva máquina destruye papel o cualquier otro método seguro de destrucción aprobado por el comité de seguridad.

### 8.4.7.5 POLÍTICAS DEL USO DE INTERNET Y CORREO ELECTRÓNICO

#### 8.4.7.5.1 Prohibición de uso de Internet para propósitos personales.

El uso de Internet está limitado exclusivamente para propósitos laborales. Los usuarios de Internet deben ser advertidos sobre la existencia de recursos tecnológicos que generan registros sobre las actividades realizadas. Esta política se complementa con la política “Instrucciones para el uso de recursos informáticos”.

#### 8.4.7.5.2 Formalidad del correo electrónico.

Toda comunicación a través del correo electrónico interno se considera una comunicación de tipo laboral y formal, por tanto podrá ser supervisada por el superior inmediato del empleado.

#### 8.4.7.5.3 Preferencia por el uso del correo electrónico.

Debe preferirse el uso del correo electrónico al envío de documentos físicos siempre que las circunstancias lo permitan.

#### 8.4.7.5.4 Uso de correo electrónico.

La cuenta de correo asignada es de carácter individual por lo cual ningún empleado bajo ninguna circunstancia debe usar la cuenta, El término “propietario” identifica a un individuo o una entidad que tiene responsabilidad aprobada de la dirección por el control de la producción, el desarrollo, el mantenimiento, el uso y la seguridad de los activos. El término “propietario” no implica que la persona tenga realmente derechos de propiedad de los activos.

#### 8.4.7.5.5 Revisión del correo electrónico.

Todos los usuarios que dispongan de correo electrónico están en la obligación de revisarlo al menos tres veces diarias. Así mismo, es su responsabilidad mantener espacio libre en el buzón.

#### 8.4.7.5.6 Mensajes prohibidos.

Se prohíbe el uso del correo electrónico con fines religiosos, políticos, lúdicos o personales o en beneficio de terceros ó que vulnere los derechos fundamentales de las personas. Por tanto, está prohibido el envío, reenvío o en general cualquier otra conducta tendiente a la transmisión de mensajes humorísticos, pornográficos, en cadena, publicitarios y en general cualquier otro mensaje ajeno a los fines laborales sin importar si son de solo texto, audio, video o una combinación de los tres.

#### 8.4.7.5.7 Acciones para frenar el SPAM.

En el caso de recibir un correo no deseado y no solicitado (también conocido como SPAM), el usuario debe abstenerse de abrirlo y avisar inmediatamente al área de sistemas.

#### 8.4.7.5.8 Todo buzón de correo debe tener un responsable.

Todo buzón de correo asignado debe tener una persona responsable de su administración, incluidos los buzones de las aplicaciones.

#### 8.4.7.5.9 Enviando software e información sensible a través de Internet.

Software e información sensible de La Universidad que requiera ser enviado por Internet debe transmitirse con la mayor seguridad posible acordada entre las partes.

#### 8.4.7.5.10 Intercambio de información a través de Internet.

La información interna puede ser intercambiada a través de Internet pero exclusivamente para propósitos laborales, con la debida aprobación y usando los mecanismos de seguridad apropiados.

### 8.4.7.6 POLÍTICAS DE LA INTRANET Y SITIOS WEB DE LA UNIVERSIDAD

#### 8.4.7.6.1 Reglas de uso de la Intranet.

La Universidad utiliza la intranet como un recurso de publicación de los documentos que rigen la relación entre ésta y el empleado o trabajador. Por lo tanto, el empleado debe consultar la intranet permanentemente, así como todos los documentos que en ella se encuentran publicados.

#### 8.4.7.6.2 Prohibición de publicitar la imagen de La Universidad en sitios diferentes a los institucionales.

La publicación de logos, marcas o cualquier tipo de información sobre La Universidad o sus actividades en Internet solo podrá ser realizada a través de las páginas institucionales de la misma y previa autorización de la Rectoría. En consecuencia, se encuentra terminantemente prohibido el manejo de esta información en páginas personales de los empleados.

#### 8.4.7.6.3 Prohibición establecer conexiones a los sitios Web de La Universidad.

Está prohibido igualmente establecer enlaces o cualquier otro tipo de conexión a cualquiera de los sitios Web de La Universidad por parte de los empleados y de sus sitios Web o páginas particulares, salvo previa autorización de la Rectoría, dependiendo del caso. Particularmente se encuentra prohibido el establecimiento de links o marcos electrónicos, y la utilización de nombres comerciales o marcas de propiedad de la Entidad en sitios diferentes a los institucionales o como meta-etiquetas.

#### 8.4.7.6.4 Prohibición de anuncios en sitios Web particulares.

Está terminantemente prohibido anunciarse en los sitios Web particulares como empleados de La Universidad o como sus representantes, o incluir dibujos o crear diseños en los mismos que lleven al visitante del sitio Web a pensar que existe algún vínculo con La Universidad.

### 8.4.7.7 POLÍTICAS GENERALES DE LA RECTORIA

#### 8.4.7.7.1 Evaluación y tratamiento del riesgo

La evaluación de riesgos debe identificar, cuantificar y priorizar los riesgos frente a los criterios de aceptación del riesgo y los objetivos pertinentes para la Universidad. Los resultados deben guiar y determinar la acción de gestión adecuada y las prioridades tanto para la gestión de los riesgos de seguridad de la información como para implementar los controles seleccionados para la protección contra estos riesgos.

El alcance de la evaluación de riesgos puede abarcar a toda la organización, partes de la organización, un sistema individual de información, componentes específicos del sistema o servicios, cuando es factible, realista y útil.

Se debe realizar una evaluación de riesgos a los recursos informáticos de La Universidad por lo menos una vez al año utilizando el procedimiento Interno: “Análisis de riesgos”

#### 8.4.7.7.2 Restricción por acceso telefónico e Internet sobre recursos tecnológicos de uso interno a clientes externos.

No se otorgarán privilegios de acceso telefónico o Internet a terceros a no ser que la necesidad de dicho acceso sea justificada y aprobada. En tal caso se deben habilitar privilegios específicos para ese usuario, con vigencia solamente del período de tiempo necesario para la actividad justificada y mediante el uso de los mecanismos de control de acceso aprobados por la Rectoría.

8.4.7.7.3 Los computadores multiusuario y sistemas de comunicación deben tener controles de acceso físico apropiados.

Todos los computadores multiusuario, equipos de comunicaciones, otros equipos que contengan información sensible y el software licenciado de propiedad de la Entidad deben ubicarse en centros de cómputo con puertas cerradas y controles de acceso físico apropiados.

8.4.7.7.4 Entrenamiento compartido para labores técnicas críticas.

Al menos dos personas deben tener la misma capacidad técnica para la adecuada administración de los sistemas de información críticos de La Universidad.

8.4.7.7.5 Preparación y mantenimiento de planes para la recuperación de desastres y para respuesta a emergencias.

Todo sistema o recurso informático debe tener definido un plan de contingencia para la restauración de la operación. Se debe preparar, actualizar y probar periódicamente un plan para la recuperación de desastres que permita que sistemas y computadores críticos puedan estar operativos en la eventualidad de un desastre. De igual forma se debe crear planes de respuesta a emergencia con el fin de que se pueda dar una pronta notificación de problemas y solución a los mismos en la eventualidad de emergencias informáticas. Estos planes de respuesta a emergencias pueden llevar a la formación de un equipo dedicado a esta labor. La contingencia de sistemas que se acuerdan con terceros deberá disponer de una infraestructura y de un modelo de soporte acorde a las necesidades de la Universidad.

8.4.7.7.6 Personal competente en el Centro de Cómputo para dar pronta solución a problemas.

Con el fin de garantizar la continuidad de los sistemas de información, La Universidad deben contar con personal técnico competente que pueda detectar problemas y buscar la solución de una forma eficiente.

#### 8.4.7.7.7 Chequeo de virus en archivos recibidos en correo electrónico.

La Universidad debe procurar y disponer de los medios para que todos los archivos descargados de Internet sean chequeados por un software de detección de virus informático, antes de ser transferidos a los computadores de los usuarios.

#### 8.4.7.7.8 Contacto con grupos especializados en seguridad informática

El personal involucrado con la seguridad de la información deberá tener contacto con grupos especializados o foros relacionados con la seguridad de la información. Esto con el objetivo de conocer las nuevas medidas en cuanto a seguridad de la información se van presentando.

### 8.4.7.8 POLÍTICAS PARA DESARROLLADORES DE SOFTWARE

#### 8.4.7.8.1 Ambientes separados de producción y desarrollo.

Todo sistema o aplicativo debe contar con ambiente de desarrollo y ambiente de producción. Así mismo para la realización de pruebas no se deben utilizar datos de producción.

#### 8.4.7.8.2 Cumplimiento del procedimiento para cambios y/o actualizaciones.

Todo cambio y/o actualización en los sistemas de información que se encuentren en producción, serán evaluados en ambientes de prueba cuya función es determinar el correcto funcionamiento y compatibilidad con las herramientas base. Una vez determinado el correcto funcionamiento y compatibilidad con las herramientas base se debe crear un plan de trabajo para la migración del ambiente de producción a la nueva versión.

#### 8.4.7.8.3 Documentación de cambios y/o actualizaciones.

Todo cambio y/o actualización en los sistemas de información que se encuentren en producción, debe tener la documentación respectiva.

#### 8.4.7.8.4 Catalogación de programas.

Debe cumplirse con el procedimiento establecido para pasar programas del ambiente de desarrollo al ambiente de producción previa prueba por parte del área encargada.

8.4.7.8.5 Medidas de seguridad deben ser implantadas y probadas antes de entrar en operación.

Todos los controles de seguridad para los sistemas de información deben ser implantados y probados sobre ambientes de pruebas o desarrollo y antes que dicho sistema entre en operación.

8.4.7.8.6 Dependencia de la autenticación de usuario en el sistema operativo.

Los desarrolladores de aplicaciones no deberán crear su propio sistema de control de acceso a la aplicación en desarrollo, esta labor deberá recaer en el sistema operativo o en un sistema de control de acceso que mejora las capacidades del sistema operativo. Esta política debe empezar a cumplirse desde la liberación de este documento.

8.4.7.8.7 Incorporación de contraseñas en el software.

Ninguna contraseña deberá ser incorporada en el código de un software desarrollado o modificado por La Universidad o sus proveedores, para permitir que las contraseñas sean cambiadas con la regularidad establecida en la política “Cambios periódicos de contraseñas”.

8.4.7.8.8 Acceso del usuario a los comandos del sistema operativo.

Después de haber iniciado una sesión, el usuario debe mantenerse en menús que muestren solo las opciones habilitadas para dicho usuario y de esta manera impedir la ejecución de comandos del sistema operativo y la divulgación de las capacidades del sistema.

8.4.7.8.9 Se requieren registros de auditoria en sistemas que manejan información sensible.

Todo sistema que maneje información sensible para La Universidad debe generar registros de auditoria que guarden toda modificación, adición y eliminación de dicha información.

8.4.7.8.10 Registros para los usuarios privilegiados en los sistemas en producción que lo permitan.

Toda actividad realizada en los sistemas por usuarios con privilegios de administración debe ser registrada, si los mismos lo permiten, o de lo contrario debe existir un procedimiento alterno de control.

8.4.7.8.11 Los registros del sistema deben incluir eventos relevantes para la seguridad.

Los sistemas de computación que manejan información sensible deben registrar todos los eventos de seguridad relevantes. Ejemplos de eventos de seguridad relevantes son: intentos de adivinación de contraseñas, intentos de uso de privilegios no otorgados, modificaciones a la aplicación y modificaciones al sistema.

8.4.7.8.12 Resistencia de los registros contra desactivación, modificación y eliminación.

Los mecanismos para detectar y registrar eventos de seguridad informática significativos deben ser resistentes a ataques, en los sistemas que permitan dicha configuración. Estos ataques incluyen intentos por desactivar, modificar o eliminar el software de registro y/o los registros mismos.

8.4.7.8.13 Procesos controlados para la modificación de información del negocio en producción.

La modificación de información en producción debe darse únicamente mediante procesos con privilegios dentro de la aplicación que maneja dicha información. Esto con el fin de evitar que la información pueda ser modificada por medios diferentes a los canales establecidos. Se excluyen los casos de emergencia, previa autorización de la Rectoría.

8.4.7.8.14 Validación de entradas en los desarrollos.

El desarrollador debe tener en cuenta durante la elaboración de la aplicación, la validación de las entradas de código con el objeto de evitar la ejecución de comandos que pongan en riesgo la seguridad de los sistemas.

8.4.7.8.15 Diseño de seguridad para aplicaciones.

El esquema de seguridad de aplicación, debe elaborarse de acuerdo con las definiciones establecidas para La Universidad.

8.4.7.8.16 Personas autorizadas para leer los registros de auditoria.

Los registros de sistemas y aplicaciones no deben estar disponibles para personal no autorizado. Personal no autorizado es aquel que no pertenece a auditoria interna, personal de seguridad informática, personal de administración de sistemas o administradores de bases de datos.

8.4.7.8.17 Archivo histórico de contraseñas.

En todo sistema multiusuario, software del sistema o software desarrollado localmente se debe mantener un archivo histórico encriptado de las contraseñas anteriores. Este archivo deberá ser usado para prevenir que un usuario seleccione una contraseña ya usada (ver política “Las contraseñas creadas por usuarios no deben ser reutilizadas”) y debe contener como mínimo las últimas cinco (5) contraseñas de cada usuario.

8.4.7.9 POLÍTICAS PARA ADMINISTRADORES DE SISTEMAS

8.4.7.9.1 Soporte para usuarios con privilegios especiales.

Todos los sistemas y computadores multiusuarios deben soportar un usuario con privilegios superiores a un usuario normal con el fin de poder ejercer las correspondientes labores administrativas y por lo cual estos privilegios deben ser asignados únicamente a los administradores.

8.4.7.9.2 Los privilegios de acceso a los sistemas de información otorgados a un usuario terminan cuando el usuario finaliza su vínculo contractual con la Entidad.

Todos los privilegios sobre los recursos informáticos de La Universidad otorgados a un usuario deben eliminarse en el momento que éste abandone la Entidad y la información almacenada queda en manos de su jefe inmediato para aplicar los procedimientos de retención o destrucción de información.

8.4.7.9.3 Cuando y como pueden asignar contraseñas los administradores

Las contraseñas iniciales otorgadas por el administrador deben servir únicamente para el primer ingreso del usuario al sistema. En ese momento el sistema debe obligar al usuario a cambiar su contraseña.

8.4.7.9.4 Límite de intentos consecutivos de ingreso al sistema.

El sistema debe limitar el número de intentos consecutivos de introducir una contraseña valida. Después de tres (3) intentos el usuario debe pasar a alguno de los siguientes estados: a) ser suspendido hasta nueva reactivación por parte del administrador; b) ser temporalmente bloqueado (no menos de 5 minutos); c) ser desconectado si se trata de una conexión telefónica.

8.4.7.9.5 Cambio de contraseñas por defecto.

Todas las contraseñas por defecto que incluyen equipos y sistemas nuevos deberán ser cambiadas antes de su utilización siguiendo los lineamientos de la política “Contraseñas fuertes”.

8.4.7.9.6 Cambio de contraseñas después de compromiso detectado en un sistema multiusuario.

Si un sistema multiusuario utiliza contraseñas como su sistema de control de acceso principal, el administrador del sistema debe asegurarse de que todas las contraseñas del mismo sean cambiadas de forma inmediata si se conoce evidencia de que el sistema ha sido comprometido. En este caso los usuarios deben ser advertidos de cambiar su contraseña en otros sistemas en los que estuvieran utilizando la misma contraseña del sistema en cuestión.

8.4.7.9.7 Administración de los buzones de correo.

Los administradores deben establecer y mantener un proceso sistemático para la creación y mantenimiento de los buzones de correo electrónico, mensualmente se realizará una revisión de control sobre cada uno de los buzones creados para determinar cuáles requieren una depuración para que no alcancen su límite de espacio asignado.

8.4.7.9.8 Brindar acceso a personal externo.

El ingeniero de soporte y web master velará porque individuos que no sean empleados, contratistas o consultores de la Universidad no tengan privilegio alguno sobre los recursos tecnológicos de uso interno de la entidad a menos que exista una probación escrita de la rectoría o el comité de seguridad.

8.4.7.9.9 Acceso a terceros a los sistemas de la Entidad requiere de un contrato firmado.

Antes de otorgarle acceso a un tercero a los recursos tecnológicos de La Universidad se requiere la firma de un formato, acuerdo o autorización de la Rectoría. Es obligatoria la firma del acuerdo de confidencialidad.

8.4.7.9.10 Restricción de administración remota a través de Internet.

La administración remota desde Internet no es permitida a menos que se utilicen mecanismos para encriptación del canal de comunicaciones.

8.4.7.9.11 Dos usuarios requeridos para todos los administradores.

Administradores de sistemas multiusuarios deben tener dos identificaciones de usuario: una con privilegios de administración y otra con privilegios de usuario normal.

8.4.7.9.12 Privilegios por defecto de usuarios y necesidad de aprobación explícita por escrito.

Sin autorización escrita Jefe de TI de la Universidad, los administradores no deben otorgarle privilegios de administración a ningún usuario.

8.4.7.9.13 Negación por defecto de privilegios de control de acceso a sistemas cuyo funcionamiento no es apropiado.

Si un sistema de control de acceso no está funcionando adecuadamente, el administrador debe negar todo intento de acceso hasta que su operación normal se haya recuperado.

8.4.7.9.14 Remoción de software para la detección de vulnerabilidades cuando no esté en uso.

Las herramientas de detección de vulnerabilidades usadas por los administradores se deben desinstalar cuando no estén operativas o implementar un mecanismo de control de acceso especial basado en contraseñas del software como tal.

8.4.7.9.15 Manejo administrativo de seguridad para todos los componentes de la red.

Los parámetros de configuración de todos los dispositivos conectados a la red de La Universidad deben cumplir con las políticas y estándares internos de seguridad.

8.4.7.9.16 Información a capturar cuando un crimen informático o abuso es sospechado.

Para suministrar evidencia para investigación, persecución y acciones disciplinarias, cierta información debe ser capturada inmediatamente cuando se sospecha un crimen informático o abuso. Esta información se deberá almacenar de forma segura en algún dispositivo fuera de línea. La información a recolectar incluye configuración actual del sistema, copias de backup y todos los archivos potencialmente involucrados.

8.4.7.9.17 Sincronización de relojes para un registro exacto de eventos en la red.

Los dispositivos multiusuario conectados a la red interna de La Universidad deben tener sus relojes sincronizados con la hora oficial.

8.4.7.9.18 Revisión regular de los registros del sistema.

El área de sistemas debe revisar regularmente los registros de cada uno de los diferentes sistemas para tomar acción oportuna sobre los eventos relevantes de seguridad informática.

8.4.7.9.19 Confidencialidad en la información relacionada con investigaciones internas.

Hasta que no se hayan presentado cargos o se haya tomado alguna acción disciplinaria, toda investigación relacionada con abusos de los recursos tecnológicos o actividad criminal debe ser confidencial para mantener la reputación del empleado.

8.4.7.9.20 Información con múltiples niveles de clasificación en un mismo sistema.

Si un sistema o computador maneja información con diferentes niveles de sensibilidad, los controles usados deben ser los adecuados para proteger la información más sensible.

8.4.7.9.21 Segmentación de recursos informáticos por prioridad de recuperación.

Se debe establecer y usar un marco lógico para la segmentación de recursos informáticos por prioridad de recuperación. Esto hará que los sistemas más críticos sean recuperados primero. Todos los departamentos deberán usar el mismo marco para preparar los planes de contingencia a los sistemas de información.

8.4.7.9.22 Software de identificación de vulnerabilidades.

Para asegurar que el equipo técnico de La Universidad ha tomado las medidas preventivas adecuadas, a todos los sistemas conectados a Internet se les debe correr un software de identificación de vulnerabilidades por lo menos una vez al año; adicionalmente en las estaciones de trabajo se cuenta con un software de Cortafuegos y Antivirus que cuente con una consola de administración en la cual se visualizan los reportes de eventos relacionados con vulnerabilidades. A nivel Corporativo se cuenta con un firewall que proporciona un software de IDS (Instrusion Detection System), detección de virus y bloqueo de correo no deseado.

8.4.7.9.23 En dónde usar controles de acceso para sistemas informáticos.

Todo computador que almacene información sensible de La Universidad, debe tener un sistema de control de acceso para garantizar que esta información no sea modificada, borrada o divulgada.

8.4.7.9.24 Mantenimiento preventivo en computadores, sistemas de comunicación y sistemas de condiciones ambientales.

Se debe realizar mantenimiento preventivo regularmente en todos los computadores y sistemas para que el riesgo de falla se mantenga en un nivel bajo.

#### 8.4.7.9.25 Habilitación de Log en Sistemas y Aplicaciones.

Se debe habilitar la gestión de log (archivos de transacción) en los sistemas y aplicaciones críticas de La Universidad.

#### 8.4.7.9.26 Monitoreo de Sistemas.

Se debe mantener una adecuada aplicación de monitoreo configurada que identifique el mal funcionamiento de los sistemas controlados.

#### 8.4.7.9.27 Mantenimiento de los Sistemas.

Se debe realizar periódicamente el mantenimiento en las bases de datos, antivirus, servidores de correo y servicios de La Universidad.

#### 8.4.7.9.28 Verificación física de equipos críticos.

Se debe verificar periódicamente el estado físico de los equipos de cómputo críticos.

#### 8.4.7.9.29 Servicios de Red.

Se debe garantizar que el servicio de red utilizado por La Universidad se encuentre disponible y operando adecuadamente, el administrador del sistema o una persona autorizada por el comité de seguridad puede efectuar escaneos de la red con la finalidad de: resolver problemas de servicio, como parte de las operaciones normales del sistema y del mantenimiento, para mejorar la seguridad de los sistemas o para investigar incidentes de seguridad.

#### 8.4.7.9.30 Revisión de accesos de usuarios

Se debe realizar por control de auditoría la revisión de los accesos de los usuarios a las aplicaciones utilizadas, por lo menos dos veces por año.

### 8.4.7.10 POLÍTICAS DE BACKUP

#### 8.4.7.10.1 Período de almacenamiento de registros de auditoria.

Registros de aplicación que contengan eventos relevantes de seguridad deben ser almacenados por un período no menor a tres (3) meses. Durante este período los registros deben ser asegurados para evitar modificaciones y para que puedan ser vistos solo por personal autorizado. Estos registros son importantes para la corrección de errores, auditoría forense, investigaciones sobre fallas u omisiones de seguridad y demás esfuerzos relacionados.

8.4.7.10.2 Tipo de datos a los que se les debe hacer backup y con qué frecuencia.

A toda información sensible y software crítico de La Universidad residente en los recursos informáticos, se le debe hacer backup con la frecuencia necesaria soportada por el procedimiento de copias de respaldo. Se deben hacer pruebas periódicas para garantizar el buen estado de la información almacenada.

8.4.7.10.3 Copias de información sensible.

Se deben elaborar una copia de cada backup con el fin de minimizar el riesgo por daño del medio de almacenamiento en disco y cinta, según procedimiento de copias de respaldo.

8.4.7.11 POLÍTICAS DE USO DE FIREWALL

8.4.7.11.1 Detección de intrusos.

Todo segmento de red accesible desde Internet debe tener un sistema de detección de intrusos (IDS) con el fin de tomar acción oportuna frente a ataques.

8.4.7.11.2 Toda conexión externa debe estar protegida por el firewall.

Toda conexión a los servidores de La Universidad proveniente del exterior, sea Internet, acceso telefónico o redes externas debe pasar primero por el Firewall. Esto con el fin de limitar y controlar las puertas de entrada a la organización.

8.4.7.11.3 Toda conexión hacia Internet debe pasar por el Firewall.

El firewall debe ser el único elemento conectado directamente a Internet por lo cual toda conexión desde la red interna hacia Internet debe pasar por el firewall.

8.4.7.11.4 Filtrado de contenido activo en el Proxy.

La dirección de TI de la Universidad, debe asegurar que dentro de las definiciones de políticas de Proxy, se filtre todo contenido activo como applets de java, adobe flash player, controles de ActiveX debido a que estos tipos de datos pueden comprometer la seguridad de los sistemas de información de La Universidad.

8.4.7.11.5 Firewall debe correr sobre un computador dedicado o appliance.

Todo firewall debe correr sobre un computador dedicado o modelo appliance para estos fines. Por razones de desempeño y seguridad no debe correr otro tipo de aplicaciones.

8.4.7.11.6 Inventario de conexiones.

Se debe mantener un registro de las conexiones a redes externas con el fin de tener una imagen clara de todos los puntos de entrada a la organización, lo anterior se cumple con el diagrama de red.

8.4.7.11.7 El sistema interno de direccionamiento de red no debe ser público.

Las direcciones internas de red y configuraciones internas deben estar restringidas de tal forma que sistemas y usuarios que no pertenezcan a la red interna no puedan acceder a esta información.

8.4.7.11.8 Revisión periódica y reautorización de privilegios de usuarios.

Los privilegios otorgados a un usuario deben ser reevaluados una vez al año con el fin de analizar sí los privilegios actuales siguen siendo necesarios para las labores normales del usuario, o si se necesita otorgarle privilegios adicionales. Esta política debe ser ejecutada por el área de sistemas con la participación de cada uno de los jefes de área, quienes harán la revisión y solicitud de cambios a la Presidencia.

8.4.7.12 POLÍTICAS PARA USUARIOS EXTERNOS

8.4.7.12.1 Términos y condiciones para clientes de Internet.

La Universidad asume que todos los clientes que usan Internet o realizan operaciones aceptan los términos y condiciones impuestos por La Universidad en sus términos y condiciones de uso del portal de internet, antes de realizarse cualquier transacción.

#### 8.4.7.12.2 Acuerdos con terceros que manejan información o cualquier recurso informático de La Universidad.

Todos los acuerdos relacionados con el manejo de información o de recursos de informática de La Universidad por parte de terceros, deben incluir una cláusula especial que involucre confidencialidad y derechos reservados. Esta cláusula debe permitirle a La Universidad ejercer auditoría sobre los controles usados para el manejo de la información y específicamente de cómo será protegida la información de La Entidad.

#### 8.4.7.12.3 Definición clara de las responsabilidades de seguridad informática de terceros.

Proveedores, estudiantes y otros asociados a las transacciones de la Universidad deben tener conocimiento de sus responsabilidades relacionadas con la seguridad informática y esta responsabilidad se debe ver reflejada en los contratos con La Universidad y verificada por la Rectoría, el responsable del manejo de estos terceros deberá realizar un acompañamiento controlado durante su estadía en las instalaciones de La Universidad, y de esta manera podrá verificar la calidad en la entrega de los servicios contratados.

### 8.4.7.13 POLÍTICAS DE ACCESO FÍSICO

#### 8.4.7.13.1 Reporte de pérdida o robo de identificación.

Todo empleado debe reportar con la mayor brevedad, cualquier sospecha de pérdida o robo de carnés de identificación y tarjetas de acceso físico a las instalaciones.

#### 8.4.7.13.2 Orden de salida para equipos electrónicos.

Ningún equipo electrónico podrá salir de las instalaciones de La Universidad sin una orden de salida otorgada por el personal adecuado o sin haber sido registrado en el momento de su ingreso.

#### 8.4.7.13.3 Orden de salida de activos

Todos los activos que afecten la seguridad de la información de La Universidad como medios de almacenamiento, CDs, DVDs., entre otros, y que necesiten ser retirados de la entidad, se debe realizar la autorización de salida por medio del formato de Autorización de salida de activos dispuesto para estos casos.

#### 8.4.7.13.4 Cuando se da una terminación laboral, los privilegios de acceso a la sede de La Universidad deben ser revocados.

Cuando exista una terminación laboral, el usuario deberá devolver los objetos de acceso físico a las instalaciones (carnés, tarjetas de acceso, etc.) y a su vez todos sus privilegios de acceso deberán ser revocados enviando (funcionarios autorizados) correo electrónico al área de Sistemas.

#### 8.4.7.13.5 Ingreso de equipos de grabación y fotografías al Cuarto de servidores.

Cualquier miembro de La Universidad y/o tercero debe estar autorizado por el área de seguridad de la información para ingresar con equipos donde puedan obtener información, estos pueden ser (video cámaras, celulares, cámaras fotográficas etc.).

### 8.4.7.14 POLITICA DE USO DE PORTATILES

#### 8.4.7.14.1 Protección de la información

- ✓ El antivirus siempre debe estar activo y actualizado
- ✓ No permitir que personas extrañas lo observen mientras trabaja en el equipo portátil, especialmente si esta fuera de las instalaciones de La Universidad.
- ✓ Seguir las políticas de acceso remoto
- ✓ Toda la información que es confidencial debe ir cifrada.

- ✓ Cuando el equipo deba ser devuelto a La Universidad para reparación, mantenimiento etc. La información confidencial deberá ser borrada y respectivamente guardada en una copia de respaldo

- ✓ De la información de usuario debe generarse copia de respaldo, por solicitud del usuario al área de sistemas.

#### 8.4.7.14.2 Protección del equipo portátil

- ✓ No dejar el computador móvil en lugares públicos

- ✓ Cuando viaje el computador portátil no debe ir dentro de su maletero siempre debe llevarse en su mano.

- ✓ Cuando vaya en su carro este debe ir en el baúl.

- ✓ No prestar el computador portátil a familiares y/o amigos

### 8.4.8 ACTUALIZACIÓN, MANTENIMIENTO Y DIVULGACIONDE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN.

Éste documento se debe revisar a intervalos planificados o cuando se produzcan cambios significativos, para garantizar que sigue siendo adecuada, suficiente y eficaz.

El Jefe de Riesgos o la persona designada por la presidencia debe aprobar el documento, es responsable por su publicación y comunicación a todos los empleados y partes externas pertinentes. El mecanismo de notificación y divulgación de los cambios realizados a la política de seguridad de la información será mediante correo electrónico.

#### 8.4.8.1 COMITÉ DE SEGURIDAD

El Comité de Seguridad de la información está conformado por un equipo de trabajo interdisciplinario encargado de garantizar una dirección clara y brindar apoyo visible a la Rectoría con respecto al programa de seguridad de la información dentro de la organización.

El comité debe estar a cargo de promover la seguridad de la organización por medio de un compromiso apropiado y contar con los recursos adecuados.

Las siguientes son las principales responsabilidades a cargo del Comité de Seguridad De la información, dentro de la Entidad:

- Revisión y seguimiento al modelo de gobierno de seguridad de la información a implementar en la organización.

- Revisión y valoración de la Política de Seguridad de la Información.

- Alineación e integración de la seguridad a los objetivos de la Universidad.

- Garantizar que la seguridad de la información forma parte integral del proceso de planeación estratégica de la organización.

- Establecer las funciones y responsabilidades específicas de seguridad de la información para toda la compañía.

- Reportar, a través de reuniones semestrales a la Rectoría el estado de la seguridad y protección de la información en la entidad y la necesidad de nuevos proyectos en temas de seguridad de la información

- Establecer y respaldar los programas de concientización de la Universidad en materia de seguridad y protección de la información

- Establecer, evaluar y aprobar el presupuesto designado para el tema de seguridad de la información

- Evaluar la adecuación, coordinación y la implementación de los controles de seguridad específicos para nuevos servicios o sistemas de información.

- Promover explícitamente el apoyo institucional a la seguridad de la información en toda la organización.

- Supervisar y controlar de los cambios significativos en la exposición de los activos de información a las principales amenazas.

- Revisar y seguir los incidentes de seguridad de la información.

- Analizar y autorizar cualquier tipo de movimiento o traslado de equipos de misión crítica para la Universidad.

Adicionalmente, el comité tiene la responsabilidad de tratar los siguientes temas (por demanda):
Mejoras en las actividades inherentes a la Seguridad de La Universidad y sus procesos.

- ❖ Seguimiento a la aplicación de las políticas, programas y planes adoptados para la protección de los sistemas, recursos informáticos y servidores de la Red Interna y Centro de Cómputo de La Universidad.
- ❖ Decisiones de carácter preventivo y proactivo que apunten a la optimización de la seguridad de los procesos y sus procedimientos.

- ❖ Cambio en los roles del ciclo de certificación.

- ❖ Participación activa en la revisión, evaluación, mantenimiento, recomendaciones, mejoras y actualizaciones de la presente política de La Universidad El Presidente Convoca al comité de seguridad con el propósito de evaluar los cambios a la presente política y autorizar su publicación. De este comité se deja Acta como constancia de su evaluación y aprobación.

- ❖ Las decisiones del comité de seguridad son protocolizadas mediante un Acta de Comité de Seguridad firmada por todos su miembros.

- ❖ Las Actas de comité de seguridad podrán ser Anuladas por el comité de Seguridad mediante el uso de un Acta que invalide el contenido siempre y cuando no se haya(n) ejecutado la(s) acción(es) relacionadas.

#### 8.4.8.2 OFICIAL DE SEGURIDAD DE LA INFORMACIÓN.

- ✓ Oficial de Seguridad de la Información (Jefe de Riesgos o persona designada para los temas de seguridad de la Entidad):

- ✓ Identificar y satisfacer las necesidades de capacitación en temas de seguridad de la información a los funcionarios de la compañía.

- ✓ Actualización y seguimiento periódico al mapa de riesgos de la compañía, validando con cada proyecto que se implemente como afecta el mapa de riesgos y tomando siempre como base este mapa para cualquier proyecto nuevo que se implemente.

- ✓ Dirigir el programa de manejo y seguimiento de incidentes.

- ✓ Crear y establecer una metodología de clasificación de la información según su importancia e impacto dentro de la compañía. Igualmente debe informarla a la compañía y validar que se cumpla. La metodología debe establecer niveles de acceso a la información.

- ✓ Crear y mantener un Programa de Concientización en seguridad de la información.

- ✓ Evaluar en forma continua la efectividad de la seguridad de la información de la organización con el propósito de identificar oportunidades de mejoramiento y necesidades de capacitación.

# 9. CONCLUSIONES

Con el desarrollo de este proyecto se evidencia que instituciones de formación superior, no aplican correctamente la norma ISO 27001 que permita el correcto funcionamiento e implementación de las políticas de seguridad informática.

Se evidencia la falta de procedimientos normativos, prácticos que garantice la evaluación de desempeño aplicado a los sistemas informáticos dentro de los que se encuentran auditorías y estudios de todo su sistema para establecer amenazas, vulnerabilidades y riesgos presentes en los mismos.

Se hace evidente la falta de controles orientados a preservar la información que se intercambia con terceros, estos pueden generar consecuencias graves para la Universidad de Cartagena Centro Tutorial Mompox e impactar de manera negativa la imagen institucional y corporativa en cada una de sus sedes a nivel nacional, se hace necesario que la Universidad diseñe e implemente mecanismos de cifrado con el propósito de garantizar la autenticidad, integridad, y confidencialidad de la información.

Se requiere la implementación de controles adecuados y acertados, o mejorar los existentes, con el propósito de contribuir a que la seguridad de la información sea parte del ciclo de vida del desarrollo de aplicaciones de la Universidad y con ello garantizar que los cambios que se realizan en las aplicaciones o software no afecten el funcionamiento ni la seguridad de la información.

El centro Tutorial Mompox de la Universidad de Cartagena, debe implementar los mecanismos de control de acceso necesarios a los dispositivos de la red de la Universidad, con el propósito de asegurar que solo pueden acceder los dispositivos autorizados.

El Oficial de seguridad debe diseñar un mecanismo que permita el monitoreo de los Log de eventos de seguridad y las funciones que realizan los funcionarios sobre la plataforma de la Universidad, igualmente el oficial de seguridad debe organizar a su equipos de trabajo, teniendo en cuenta que no se aplican lineamientos para el uso adecuado de los activos de información relacionados con la información e instalaciones de procesamiento de información, lo que conlleva que los funcionarios o estudiantes desconozcan sus responsabilidades y consecuencia de sus acciones.

Con el fin de fortalecer los conocimientos de cada uno de los funcionarios de la Universidad de Cartagena Centro Tutorial Mompox, se hace necesario desarrollar un cronograma anual de formación y socialización en seguridad de la información, con el objetivo de mejorar la cultura de seguridad en los funcionarios y contratistas que laboran para la Universidad.

# BIBLIOGRAFIA


[1] ICONTEC, GUIA TECNICA COLOMBIA GTC-ISO/IEC 27035, 2012.

[2] iso27000.es, «ISO 27000.es,» [En línea]. Available: http://www.iso27000.es/sgsi.html. [Último acceso: 16 Junio 2016]. Normas ISO

[3] 27000, 2012 Disponible en: http://www.iso27000.es/

[4] Norma ISO 27000 Consultado el 19 de Octubre de 2015, Disponible en: http://repositorio.utp.edu.co/dspace/bitstream/11059/4117/1/0058A284.pdf

[5] Políticas de Seguridad informática Consultada el 19 de Octubre de 2016, Disponible en: http://ribuc.ucp.edu.co:8080/jspui/bitstream/handle/10785/1731/CDMIST65.pdf?sequence=1.

[6] Wikipedia. http://es.wikipedia.org/wiki/Licencia_de_software

**Anexo 1. ACUERDO DE CONFIDENCIALIDAD**

Ciudad y Fecha:_____

Yo,_____ me comprometo a acatar y dar cumplimiento a cada una de las políticas establecidas en el documento POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN y así mismo mantener estricta confidencialidad sobre toda información que por una u otra razón deba conocer como producto del trabajo que actualmente realizo o realizaré.

Firma: _____

Documento de identificación: _____

Empresa: _____

Área de La Universidad: _____

_____

Vo. Bo. Recursos Humanos