NIVEL DE MADUREZ DE SEGURIDAD EN EL ÁREA DE REDES DE LA UNIVERSIDAD PEDAGOGÍCA Y TECNOLÓGICA DE COLOMBIA (U.P.T.C) TUNJA, BASADO EN NORMA ISO 27001.

ANTONIO LEONEL RODRIGUEZ BUSTOS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍAS (ECBTI)
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
TUNJA
2018

NIVEL DE MADUREZ DE SEGURIDAD EN EL ÁREA DE REDES DE LA UNIVERSIDAD PEDAGOGÍCA Y TECNOLÓGICA DE COLOMBIA (U.P.T.C) TUNJA, BASADO EN NORMA ISO 27001.

ANTONIO LEONEL RODRIGUEZ BUSTOS

Trabajo monografía de grado para optar el título de Especialista en Seguridad Informática

Director
Especialista. Daniel Felipe Palomo Luna

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍAS (ECBTI)
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
TUNJA
2018

Nota de aceptación:

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Tunja, noviembre de 2018

DEDICATORIA

“A DIOS, todo poderoso por ser mi guía darme fuerza, conocimiento, entendimiento y paciencia para culminar con esta nueva meta propuesta en mi vida”.

A mí querida esposa Yudi Mireya que con sus hermosos ojos verdes que inspiran alegría, ternura y amor, a nuestros hijos y a mi hija, por la paciencia, el amor, el apoyo y comprensión.

A mi princesa Sara Lucia, a mi fortachón Samuel Antonio y a mi gordo Leonel Alejandro, con la más hermosa, dulce, y tierna sonrisa alegran mi vida, mi hogar, y por todo el tiempo no compartido.

A mi Madre Ana Custodia, a mis hermanas y a mi sobrino que siempre me apoya y ayudan en todos los momentos de mi vida incondicional

AGRADECIMIENTOS

Quiero agradecer a DIOS y la virgen, a mi esposa, a mis hijos, a mi madre, a mis hermanas, a mi sobrino y a mi amigo y colega Ricardo Santamaría por su apoyo, paciencia y colaboración.

A la UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD, por su confianza y apoyo no sólo en especialización sino también en el cumplimiento de sus temáticas, a la ingeniera María Consuelo Rodríguez y al ingeniero Daniel Felipe Palomo Luna, por su valiosa orientación en el desarrollo de la tesis, también agradecer a todos los docentes de la Especialización por su conocimiento y experiencia que contribuye a mi crecimiento personal y profesional, a mis compañeros de la especialización de quienes aprendí y compartí todos contratiempos de esta nueva etapa de estudio.

TABLA DE CONTENIDO

pág.

LISTA DE FIGURAS

pág.

LISTA DE CUADROS

pág.

ANEXOS

pág.

RESUMEN

Con el uso de la internet y los servicios alrededor de esta como herramienta de comunicación, por las diferentes organizaciones sea cual sea su carácter o composición jurídica, la internet es la más utilizada para el intercambio de información y de problemas a medida que avanzan las tecnologías Con ella también se propagan el riesgo de pérdida de información, el robo de los datos, el ataque y violación de información por consiguiente se deben diseñar políticas que minimicen los riegos y/o fallas a la que se encuentre expuesta la información en el entorno empresarial, estas políticas deben ir dirigidas hacer tomar y/o a crear conciencias sobre el valor de la información del negocio.

El desarrollo del presente proyecto busca reconocer el nivel de madurez de seguridad de la información en el área de redes de la universidad Pedagógica y Tecnológica de Colombia (U.P.T.C) Tunja, basado en norma ISO 27001, mediante la recopilación, descripción, registro, análisis e interpretación de la información, y la comprensión de procesos y fenómenos de la realidad estudiada. Este análisis se realiza sobre el funcionamiento y manejo que actualmente se da a la información, permitiendo de esta manera detectar falencias, diseñar soluciones y resolver problemas con el propósito de evitar la pérdida de información y garantizar la seguridad, integridad, disponibilidad, confidencialidad, autenticidad en la información y la continuidad del negocio.

INTRODUCCIÓN

Desde principios del siglo XXI es común escuchar a diario la palabra brecha tecnológica en casi todas las culturas del mundo, sobre todo en los países Latinoamericanos; y se habla de las nuevas tecnologías de la información y las comunicaciones TIC, en los países latinos hoy en día se habla de agenda de conectividad, gobierno en línea, que no son más que políticas internacionales para poner en práctica; las TIC en todas las áreas del conocimiento, aplicaciones y actividades de una región o país. Con la aparición de la internet es realmente como la revolución industrial del siglo veinte, esto a razón que el mundo es uno antes y después de la aparición de la internet, con la aparición y masificación de la red más grande, hablamos de un mundo globalizado y con este el intercambio comercial en la sociedad de la información y el conocimiento tecnológico.

Con el uso de la internet y los servicios alrededor de esta como herramienta de comunicación, por las diferentes organizaciones sea cual sea su carácter o composición jurídica, la internet es la más utilizada para el intercambio de información, a medida que avanzan las tecnologías con ella también se propagan los riesgos de pérdida de información, el robo de los datos, el ataque y violación de información por consiguiente se deben establecer políticas que minimicen los riegos y/o fallas a la que se encuentra expuesta la información en el entorno empresarial, estas políticas deben ir dirigidas a crear conciencia sobre el valor de la información del negocio.

El área de educación no es ajena a los riesgos relacionados anteriormente, la U.P.T.C., es una universidad de carácter nacional, regulada por Ministerio de Educación Nacional, cuenta con seccionales en Chiquinquirá, Tunja, Duitama y Sogamoso. Con programas de educación profesional y disciplinar, en los niveles de pregrado, postgrado. Por consiguiente, es vital importancia velar por la no pérdida de información, la adulteración de notas en las planillas de profesores entre otros se convierte en un aspecto de inconformidad y causales de retiro de los clientes (estudiantes), y la mala imagen en la calidad de la atención y del servicio por falta de capacitación, actualización e implementación de un sistema de seguridad, además de poner en riesgo activos de alto valor institucional.

El desarrollo de este proyecto busca identificar el nivel de madurez de seguridad de la información en el área de redes de la universidad, tomando como referencia la Norma ISO 27001, con el propósito de ayudar a los encargados del área a evaluar la seguridad de la organización, y de igual forma, determinar el nivel o grado en que se encuentra ésta, con el fin de identificar las falencias que se tienen en un determinado nivel, y adoptar políticas de seguridad, que redunden en la prestación de un mejor servicio haciéndola más competitiva y segura, frente a las otras Universidades.

1. TÍTULO

Nivel de Madurez de Seguridad informática en el Área de Redes de la Universidad Pedagógica y Tecnológica de Colombia (U.P.T.C) Tunja, basado en norma ISO 27001.

2. DEFINICIÓN DEL PROBLEMA

La Universidad Pedagógica y Tecnológica de Colombia, UPTC, es una entidad universitaria autónoma, de carácter nacional, estatal y público, de régimen especial, vinculado al Ministerio de Educación Nacional en lo referente a las políticas y la planeación del sector educativo, con sedes seccionales en Duitama, Sogamoso y Chiquinquirá, y con domicilio en Tunja. Al tener una fusión social está comprometida a ofertar programas formales profesionales y disciplinares, en los niveles de pregrado, postgrado y de formación permanente, que hacen efectivos los derechos humanos individuales, colectivos y culturales pertinentes para el desarrollo económico y ecológico de la nación, y la permanente observación de los adelantos tecnológicos y su asimilación prioritaria para la consolidación de una sociedad con bienestar y desarrollo social.

Debe tenerse en cuenta que la pérdida de información, la adulteración de notas en las planillas de profesores entre otros, se convierte en un aspecto de inconformidad y causales de retiro de los clientes (estudiantes) y que pueden afectar a la Universidad, si se permite la ocurrencia de la pérdida, se genera entre otros, mala imagen en la calidad de la atención y servicio por falta de capacitación, actualización e implementación de un sistema de seguridad, además de poner en riesgo activos de alto valor institucional.

Actualmente, en la entidad, se presentan inconvenientes de seguimiento en los procesos de control, evolución y seguimiento a la información, por lo que se requiere establecer políticas de seguridad de la información, que redunden en la prestación de un servicio de calidad haciéndola más competitiva y segura, frente a otras Universidades de la región.

2.1. FORMULACIÓN DEL PROBLEMA.

¿Qué factores influyen en la pérdida de información en el Área de Redes de la Universidad Pedagógica y Tecnológica de Colombia. (U.P.T.C) Tunja y como se puede reducir este impacto?

3. OBJETIVOS

3.1. OBJETIVO GENERAL.

Evaluar el nivel de madurez de seguridad informática en el área de redes de la Universidad Pedagógica y Tecnológica de Colombia (U.P.T.C) sede Tunja conforme a lo señalado en la norma ISO 27001

3.2. OBJETIVOS ESPECÍFICOS.

- Identificar la estructura organizacional y funcional del área de redes de la Universidad Pedagógica y Tecnológica de Colombia (U.P.T.C) sede Tunja.

- Realizar un diagnóstico inicial de madurez en el área de redes de la Universidad Pedagógica y Tecnológica de Colombia (U.P.T.C) sede Tunja de conformidad con la norma ISO 27001.

- Trazar las políticas para la gestión de la seguridad de la información en el área de redes de la Universidad Pedagógica y Tecnológica de Colombia (U.P.T.C) sede Tunja.

- Sugerir un modelo en el área de redes de la Universidad Pedagógica y Tecnológica de Colombia (U.P.T.C) sede Tunja para reducir o eliminar los incidentes de seguridad relacionados con la pérdida de la información.

4. JUSTIFICACIÓN.

Con el nacimiento de ARPANET en los años 60 y el desarrollo de los primeros lenguajes de programación en los años 70, la aparición de la primera calculadora científica, la globalización del mundo, el intercambio comercial, la masificación de uso de internet y de las TIC, colocaron en ventaja a las organizaciones que le apostaron a la modernización sin olvidar que la tecnología va de la mano con el desarrollo social, político, económico y cultural de la organización tanto en la región como en el país, la educación en todas sus áreas del conocimiento no es ajena a la implementación de nuevas políticas y tecnologías del intercambio comercial y cultural.

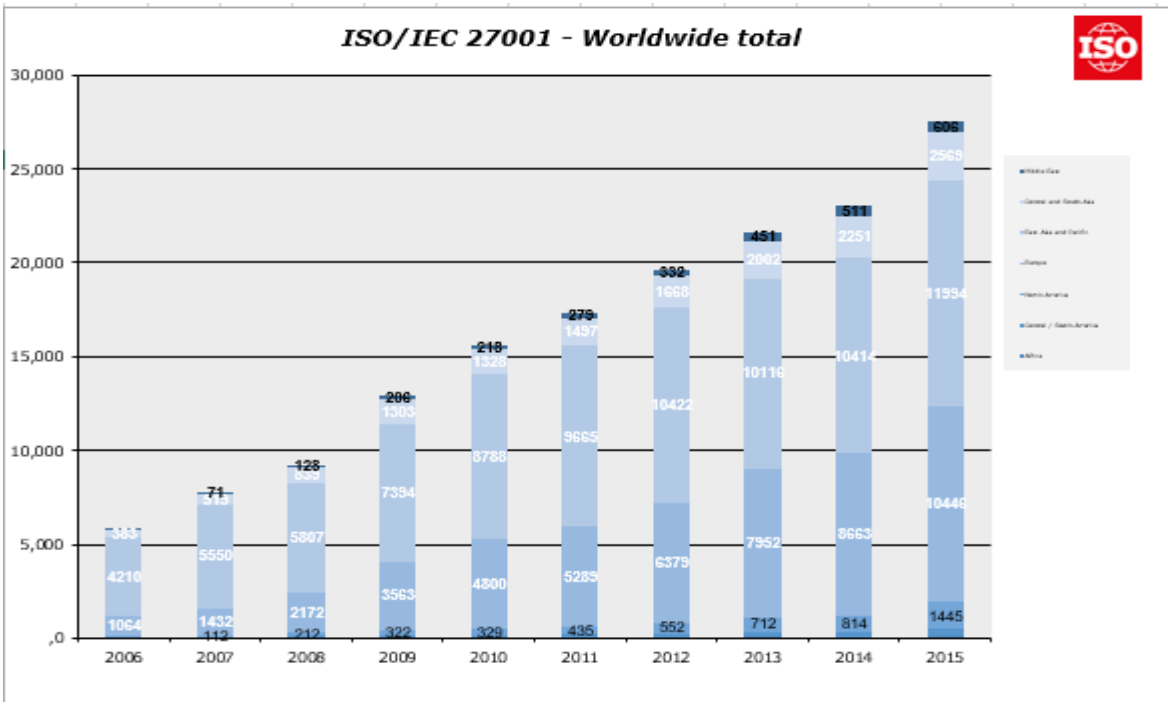
La gestión de la seguridad de la información es tan importante como la implementación de las nuevas tecnologías, que la Organización Internacional para la estandarización ISO, ha creado capítulos en cada país y regiones del mundo, para capacitar y certificar en la familia ISO 27000, y anualmente publica una serie de estadísticas que reflejan la concientización de los gerentes de las empresa en certificar y estandarizar sus procesos y estos a su vez ayudan a posicionar sus empresas y sus productos. Como podemos observar en la figura 1, en el año 2006 existían más de 5700 compañías en 64 países con la certificación ISO 27001.

El análisis de seguridad de la información hecho en Colombia, por ACIS[1] en su revista sistemas, demuestra que este no es un tema, relevante o una política de interés para la gran mayoría de las organizaciones, incluidas las Instituciones de Educación Superior, de igual manera, el tema de la seguridad informática está en un segundo plano y la inversión si la hay, no va dirigida a reforzar la unidad de redes de la organización.

Un gran porcentaje de las organizaciones en Colombia consideran prioritario e importante adquirir nuevo personal y/o sistemas de vigilancia, infraestructura física, que una política de mejoramiento, modernización, inversión e implementación de dispositivos de seguridad informática para proteger los sistemas de información alojados en los diferentes servidores de los intrusos informáticos; más sin embargo el crecimiento de organizaciones certificadas en ISO 27001:2005 en Colombia desde 2006 hasta el 2012, ha sido progresivo y positivo su crecimiento como se observa en la Figura 1, es importante resaltar que en la actualidad no hay una sola Institución de Educación Superior certificada, pero si hay varias en vía de Capacitación, preparación, mejoramiento de sus procesos y políticas de seguridad.

[1] Almansa, A. (Abril – Junio 2016) Encuesta Nacional de Seguridad Informática- Retos de la Ciberseguridad. Obtenido. http://acis.org.co/revista139/content/tendencias-2016-encuesta-nacional-de-seguridad-inform%C3%A1tica

Figura. 1. Adopción mundial de ISO 27001.



Fuente: http://iso27000.es/certificacion.html

El estado colombiano y el ministerio de las TIC, y su programa gobierno en línea, han desarrollado políticas para la masificación y buen uso las TIC, implementando el Nivel de Madurez de Seguridad de la información, para el manejo de la información por parte de las entidades de estado.

En el marco de la globalización, se ha generado la necesidad de estandarizar los procesos de Adopción de buenas prácticas sobre gestión y seguridad de TI, cuyo principal objetivo es la concientizar acerca de la integridad, confidencialidad y la disponibilidad de la información. Es así, que, en la actualidad las áreas de tecnología no son las únicas en la responsabilidad de gestionar la información, sino que es el colectivo de la organización, donde se hace necesario hacer modificaciones a su normatividad y conductas en el manejo de la información, involucrando a las personas a estar más comprometidas con la protección de la información, ya que la seguridad no es solo un tema de infraestructura sino un tema cultural. A nivel global, la tecnología está siendo definida por criterios unificados comprobados en un mercado, a través del establecimiento de estándares internacionales que permitan adoptar las buenas prácticas que certifican una mayor competitividad en el mercado. De esta forma, la adopción de estándares ofrece beneficios a las organizaciones que les permiten posicionamiento, confianza y satisfacción a los clientes, como también seguridad, eficiencia y productividad en la misma, minimizando los riesgos a los que están expuestos.

La Organización Internacional para la Estandarización (ISO), es una entidad que define un estándar como un acuerdo documentado que incluye especificaciones técnicas y criterios precisos para ser aplicados como guías de ciertas características que garanticen que todos aquellos productos, materiales, procesos o servicios están cumpliendo con su propósito. Dentro de este contexto, la ISO 27000, contiene un marco de Gestión de la Seguridad de la Información que puede ser utilizado por cualquier tipo de Organización, ya sea tipo privada o pública. Con el desarrollo de este proyecto se busca la adopción de las buenas prácticas en gestión de la Seguridad de la Información en el área de redes de la Universidad Pedagógica y Tecnológica de Colombia (U.P.T.C). Tunja, que no sólo les permita conocer y administrar adecuadamente sus activos de información, sino también, aquellos riesgos a los que se encuentran expuestos sean en factores Físicos, lógicos o de Recursos Humanos.

4.1 ALCANCES Y DELIMITACIÓN DEL PROYECTO

El presente proyecto abarca el Área de Redes de la Universidad Pedagógica y Tecnológica de Colombia, describiendo los requerimientos para establecer el nivel de madurez de seguridad de la Información dentro del contexto de los riesgos de administración de la Información en la organización, atendiendo a los controles de seguridad definidos.

Ramos (2009), comenta que ISO 27000 es la única norma en la cual se define todos aquellos requisitos para un Sistema de Gestión de la Seguridad de la Información, garantizando la elección de los controles de seguridad más adecuados, que ayudan a proteger los archivos de información y confiere confianza a las partes involucradas (clientes y usuarios).

Este proyecto tiene como finalidad, sugerir políticas en cuanto a la gestión de la seguridad de la información general para la U.P.T.C de acuerdo con las necesidades técnicas y humanas a que se enfrenta la institución en el día a día.

5. MARCO REFERENCIAL

5.1. MARCO CONTEXTUAL.

La Universidad Pedagógica y Tecnológica de Colombia (UPTC), cuenta con su sede principal en la ciudad de Tunja, es una institución de carácter oficial y de disposición nacional, fue creada mediante decreto 2655 del 10 de octubre de 1953, actualmente cuenta con seccionales en las ciudades de Sogamoso, Duitama, Chiquinquirá, Yopal y Bogotá D.C.

Por medio del Acuerdo 087 del 14 de diciembre de 1983 la universidad crea el Instituto de Educación Abierta y a Distancia (IDEAD), y consecutivamente por medio de convenio que se llevó a cabo con la Universidad de Antioquia, el Consejo Superior de la UPTC, crea el programa en la modalidad de Educación a Distancia estipulado en el Acuerdo 0116 del 19 de noviembre de 1998, el cual está adscrito al Instituto de Educación Abierta y a Distancia (IDEAD).[2]

La U.P.T.C, en el departamento de Boyacá es la institución de educación superior más importante y una de las más prestigiosas del país, haciendo presencia en 10 departamentos a lo largo del territorio nacional con 24 centros regionales de educación a distancia en los que funcionan 12 facultades, 79 programas académicos de pregrado presencial, 26 de pregrado a distancia y 89 de postgrado.

5.1.2. ESTRUCTURA ORGANIZACIONAL

El componente teleológico de la Universidad Pedagógica y Tecnológica de Colombia U.P.T.C., reza textualmente lo siguiente:

5.1.2.1. Misión. En la búsqueda de la excelencia educativa el Centro busca brindar a la comunidad upetecista y regional asesoría integral en las áreas psicopedagógica, psicoafectiva y de rehabilitación social desde la prevención e intervención, con el propósito de fortalecer el ejercicio de la libertad, la autonomía, la autoestima, el autoaprendizaje, y los valores fundamentales que propicien el equilibrio personal y favorezcan el desarrollo de las potencialidades en beneficio de una mejor calidad de vida.[3]

---

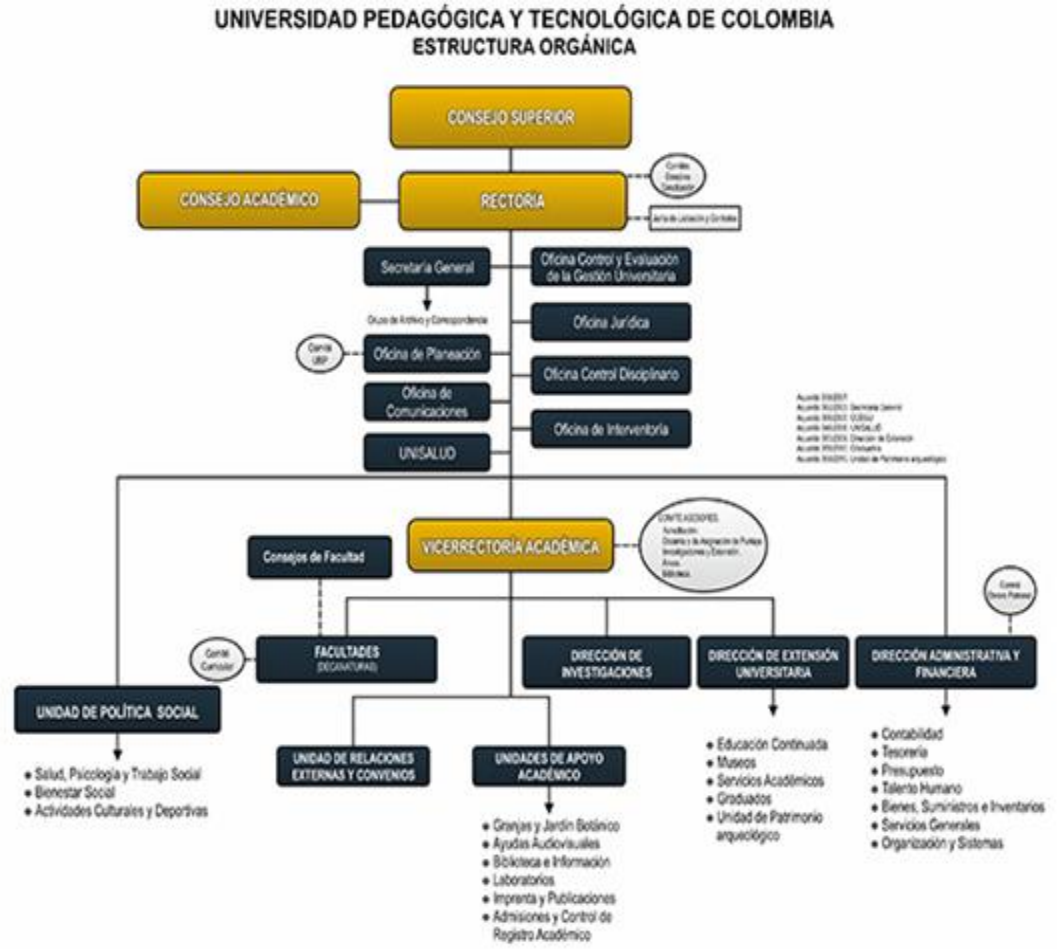
[2] Historia de la U.P.T.C. Obtenido. http://www.uptc.edu.co/facultades/fesad/regencia_farmacia/aspectos_misionales/Historia

[3] Filosofía institucional. Obtenido. http://www.uptc.edu.co/extension/cap/aspectos_misionales/

5.1.2.2. Visión. En el desarrollo de su misión y objetivos el Centro de Atención Psicopedagógica espera constituirse, en el próximo quinquenio, en el principal centro universitario de asesoría psicopedagógica que contribuya a la formación integral de los estudiantes, para lo cual formulará proyectos de investigación y programas de desarrollo social y comunitario y así apoyar los procesos académicos-institucionales para contribuir al mejoramiento de la calidad de vida. [4]

5.1.2.3. Organigrama. El siguiente es el organigrama de la Universidad:

Figura. 2. Organigrama de la Organización



Fuente: http://www.uptc.edu.co/export/sites/default/universidad/acerca_de/inf_institucional/doc/org_uptc_2017.pdf.

[4] UPTC. Filosofía institucional. Obtenido. http://www.uptc.edu.co/extension/cap/aspectos_misionales/

5.1.2.4 Políticas de calidad. La Universidad, al estar comprometida con la formación integral del ser humano, basa su desarrollo en la docencia, investigación y proyección social, establecido en una gestión ética y transparente de los recursos y en el continuo mejoramiento de cada uno de sus procesos; brindando la satisfacción de sus usuarios y proyección del desarrollo sostenible, tanto en la parte regional como nacional. La política de Calidad fue aprobada mediante la Resolución Nº 1850 de 15 de Mayo de 2008.[5]

5.1.2.5. Objetivos de la calidad. La alta dirección de la universidad en búsqueda de un mejoramiento continuo propone unos objetivos de calidad que van de la mano con las políticas de calidad, con el propósito de mejorar y capacitar de forma continua a todo el personal. A continuación, una breve descripción de los mismos:

- Mantener una formación y capacitación continua de su personal (servidores públicos).
- Fomentar el uso permanente de las nuevas tecnologías de información y comunicaciones.
- Expandir la proyección social de la Universidad por medio de Centros, Grupos de Investigación y programas de extensión generando un impacto tanto en el sector empresarial como en la comunidad en general.
- Fortalecer las relaciones con aliados de otras instituciones.
- Propender por un perfeccionamiento continuo del Sistema.[6]

5.1.2.6. Políticas de Sistema Integrado de Gestión. (SIG). Formar personas como profesionales integrales en diferentes niveles de educación superior, fortaleciendo las actividades de docencia, investigación, extensión e internacionalización, como aporte a la trasformación y al desarrollo de la sociedad, se compromete a:[7]

- Cumplir con aquellos requerimientos legales aplicables, relacionados a las actividades y otros requisitos de las partes interesadas.
- Prevenir la contaminación ambiental, por medio del control y la minimización de aquellas actividades de las labres diarias que generan impactos adversos en el planeta.

[5] Políticas de calidad obtenido de. http://www.uptc.edu.co/universidad/acerca_de/politica_calidad.html
[6] Ibíd.
[7] Información institucional obtenida de. http://www.uptc.edu.co/universidad/acerca_de/inf_institucional/

- Implementar programas que fomenten hábitos y conductas seguras, permitiendo reducir tanto los accidentes como las enfermedades ocupacionales en el personal (servidores públicos).
- Posicionarse como una institución de educación superior, que sea reconocida a nivel nacional como una de las mejores proyectándose a nivel internacional y conservando la identidad del contexto latinoamericano, formando profesionales con altas competencias que contribuyan a la innovación, el pensamiento crítico y la solidaridad, con alto grado de impacto social promoviendo la convivencia para la construcción de una nación con identidad, equidad y justicia.

5.1.2.7 Objetivos de Sistema Integrado de Gestión. (SIG).

- Lograr que, tanto la institución como los programas académicos ofertados, cuente con acreditación de alta calidad.
- Formar y capacitar de forma constate a todo su personal (servidores públicos).
- Promover el uso adecuado y permanente de las TIC.
- Mantener una proyección social que genere cambios positivos en el sector empresarial y la comunidad en general, por medio de Centros y Grupos de Investigación y programas de extensión.
- Crear y fortalecer los lazos con otras Instituciones, de igual manera contribuir en el mejoramiento continuo, logrando eficiencia, eficacia y efectividad en el Sistema Integrado de Gestión.
- Promover mecanismos de sensibilización y capacitación ambiental a todo el personal con el objetivo de lograr disminuir los efectos adversos derivados de actividades, proyectos, productos o servicios que se ejercen diariamente en pro del funcionamiento adecuado de la universidad.

Cuadro. 1. Estándares de Calidad que en la Actualidad tiene implementado la organización.

NTC GP 1000:2009	Norma Técnica de Calidad en la Gestión Pública
NTC-ISO 001:2008	Norma Internacional para los Sistemas de Gestión de Calidad
MECI 1000:2005	Modelo Estándar de Control Interno
GTC 180	Responsabilidad Social
SISTEDA	Sistema de Desarrollo Administrativo

Fuente: autor

Cuadro. 1 (Continuación)

NTC OHSAS 18001:2007	Sistemas de Gestión en Seguridad y Salud Ocupacional
NTC ISO 14001:2004	Sistemas de Gestión Ambiental
NTC-ISO/IEC 7025:2005	Requisitos Generales para la Competencia de los laboratorios de ensayo y calibración

Fuente: autor

5.1.3. Grupo Organización y Sistemas. El Grupo de Organización y Sistemas de la UPTC se enfoca en la innovación de la infraestructura informática, logrando mantener un adecuado funcionamiento y ofreciendo de esta manera un servicio eficiente a la comunidad educativa y contribuir en la construcción de la nueva Sociedad Colombiana. Facilitando la ejecución de actividades académicas, administrativas y de investigación, mediante el uso de estas herramientas[8].

5.1.3.1. Objetivos y responsabilidades del grupo de organización y sistemas en el manejo de seguridad de la información. En la actualidad el grupo de organización y sistemas de la Universidad tiene como objetivo principal el apoyo y funcionamiento de las Tecnologías de la información y las comunicaciones, en cabeza de su director para cumplir los siguientes objetivos[9].

- Tomar las decisiones acerca del Sistema de Gestión en Seguridad Informática
- Reportar las novedades a la Alta Dirección y al Comité de Seguridad.
- Validar y proponer los alcances y límites del SGSI, enfocados en las características del negocio, la organización, su ubicación, sus activos y la tecnología.
- Coordinar la implementación de la gestión de riesgo, es decir el análisis y la evaluación de los riesgos.
- Velar por una constante integración entre los dos sistemas de la universidad (Sistema de Gestión de Seguridad de la Información y Sistema de Gestión Integral).
- Definir y emplear las instrucciones de seguimiento y revisión del SGSI
- Aprobar los procesos del SGS tales como documentación, responsables, registros e indicadores.

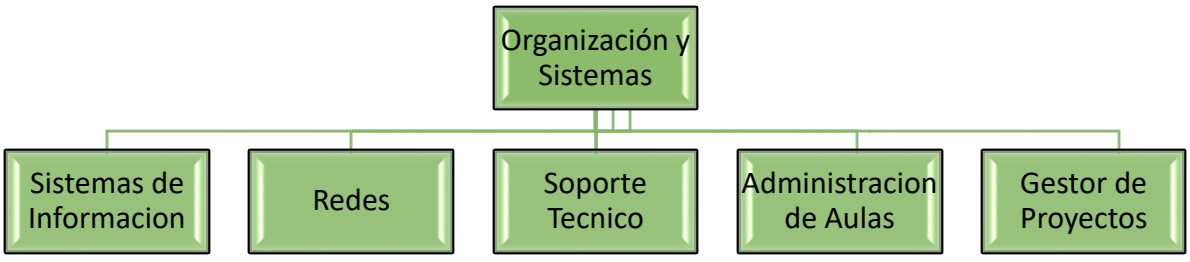
[8] http://www.uptc.edu.co/universidad/administracion/org_sistemas

[9]Grupo de organización y sistemas. Obtenido de. http://www.uptc.edu.co/universidad/administracion/org_sistemas

- Apoyar, participar y capacitar a la comunidad académica en los procesos de certificaciones de calidad y sistemas de seguridad de la información.
- Responsable del plan de adquisiciones y actualización de los sistemas de información y las bases de datos en las diferentes sedes.
- Realizar asesoramiento tecnológico para adquirir hardware y software de calidad.
- Realizar un constante seguimiento a las labores referentes al Sistemas de Información, las redes, el soporte técnico, la administración de aulas y el gestor de proyectos.
- Apoyar en las diferentes capacitaciones relacionadas con el área de TI, de acuerdo a las necesidades de cada sede universitaria.
- Capacitar y actualizar a la universidad, en las estrategias de las políticas de gobierno en línea.[10]

5.1.3.2. Estructura del grupo de organización y sistemas. El grupo de organización y sistemas de la Universidad, cuenta una infraestructura de cinco grandes áreas de trabajo para el apoyo y soporte a toda la organización como se observa en la figura 3.

Figura. 3. Organigrama del grupo de organización y sistemas



Fuente: Autor

[10] http://www.uptc.edu.co/sig/estruct/

5.1.3.3. Personal que labora en el grupo de organización y sistemas. Esta unidad es dirigida por un Profesional Universitario con título ingeniero de sistemas y Maestría en una de las áreas relacionadas directamente con las funciones de esta, adicionalmente cuenta con el siguiente grupo de trabajo:

Cuadro. 2. Personal del área de sistemas de información del grupo de organización y sistemas.

Áreas de Trabajo	Actividades	Recurso Humano	Capacidades	Nivel de Acceso a La Información	Acceso a SI
1. Sistemas de Información	Desarrollo de Sistemas de Información	4. Desarrolladores	Conocimiento en herramientas de desarrollo	Información Privada	Restringido
	Bases de datos.	DBA	Conocimiento y certificación en Oracle	Información confidencial e información Privada	Total con restricción
	Administración de Sistemas de Información	4 Ingenieros de sistemas	Diseñadores, analistas, auditores en Sistemas de información	información pública	Total con restricción

Fuente: autor

Cuadro. 3. Personal del área de redes del grupo de organización y sistemas.

Áreas de Trabajo	Actividades	Recurso Humano	Capacidades	Nivel de Acceso a La Información	Acceso a S.I
2.Redes	Administración redes Inalámbricas	2 ingenieros de sistemas	conocimientos y habilidades en gestión de redes	información privada, confidencial	restringido
	Administración Data Center	1 ingeniero de sistemas	Conocimientos y habilidades gestión de la seguridad.	información privada, confidencial	restringido

Fuente: autor

Cuadro. 3 (Continuación)

Áreas de Trabajo	Actividades	Recurso Humano	Capacidades	Nivel de Acceso a La Información	Acceso a S.I
2.Redes	Administración de la seguridad de las redes	1. Ingeniero de sistemas	Conocimiento y habilidades en administración de S. Operativos. Windows, REDHAT, Solaris.	información privada, confidencial y pública	restringido
	Diseñar actualizaciones de infraestructura	4. Ingenieros. de sistemas	Manejo de herramientas	información privada, confidencial y pública	restringido

Fuente: autor

Cuadro. 4. Personal del área soporte técnico del grupo de organización y sistemas.

Áreas de Trabajo	Actividades	Recurso Humano	Capacidades	Nivel de Acceso a La Información	Acceso a S.I
3. Soporte Técnico	Plataforma Computacional	1 Técnico electrónico para, PC´S, Impresos y videobeam	conocimiento y habilidades en de hardware, e instalación de aplicaciones	Información Publica	restringido
	Redes de Datos	3 técnicos para redes	Conocimiento y certificaciones en redes.	Información Publica	restringido
	Data Center	1 técnico para manejo de software especializado	Habilidad en la manipulación de hardware tipo servidor.	Información Publica	restringido

Fuente: autor

Cuadro. 4 (Continuación)

Áreas de Trabajo	Actividades	Recurso Humano	Capacidades	Nivel de Acceso a La Información	Acceso a S.I
3. Soporte Técnico	Capacitación a usuarios finales	1 Ingeniero de Sistemas para Data Center	habilidad en el manejo de equipos de protección, UPS, Aire acondicionado tipo precisión, Plantas de emergencias	Información Publica	restringido

Fuente: autor

Cuadro. 5. Personal del área de administración de aulas de informática del grupo de organización y sistemas

Áreas de Trabajo	Actividades	Recurso Humano	Capacidades	Nivel de Acceso a La Información	Acceso a S.I
4. Administración de Aulas de Informática.	Mantenimiento preventivo y correctivo.	6 técnicos	Operadores para la gestión de las salas	Información Publica	restringido
	Definir programación de clases y préstamo	1 Profesional	conocimiento en el manejo de las herramientas tecnológicas disponibles para la administración de salas	Información Publica	restringido

Fuente: autor

Cuadro. 6. Personal del área de Gestores de Proyectos del grupo de organización y sistemas.

Áreas de Trabajo	Actividades	Recurso Humano	Capacidades	Nivel de Acceso a La Información	Acceso a S.I
5.Gestores de Proyectos	Administrar proyectos	2 Profesionales	Gerentes de proyectos informáticos	Información Privada y Publica	restringido

Fuente: autor

5.1.3.4 Recursos con que cuenta el área de redes. Para la implementación, desarrollo, capacitación y mantenimiento, el grupo de organización y sistemas cuenta con los siguientes recursos:

- Recursos físicos (puestos de trabajo y elementos de trabajo).
- Recursos técnicos (computadores, impresoras, servidores, internet)
- Recursos lógicos (software libre, software licenciado).
- Recursos humanos. (ingenieros y técnicos de soporte, administrador de red y auditor)

5.2. MARCO TEORICO

5.2.1. Sistema de gestión de la seguridad de la información (SGSI). (En inglés *Information Security Managenement System*, ISMS) Es un conjunto de métodos para gestionar la información o activos de la organización, de forma eficientemente, buscando siempre asegurar los pilares de la seguridad de la información tales como la confidencialidad, la integridad y su disponibilidad, reduciendo los riesgos de seguridad y adaptándose a los constantes cambios tanto de la organización como su entorno.

5.2.2 En que ayuda los Sistemas de Gestión en General. Ayuda a las organizaciones a ser más, eficientes en sus procesos y procedimientos de la información, que a su vez aseguren una mejora continua a la organización.

5.2.3 Que Información Protege un SGSI. Los SGSI tienen como función proteger de los activos (tangibles e intangibles) de una organización, como: correos electrónicos, páginas web, documentos entre otros.

5.2.4 Que son las normas ISO. *(La International Organization Standardization - ISO e International Electrotechnical Commission HJL– IEC),* son las organizaciones de estandarización de carácter mundial que desarrollaron un conjunto de Normas ISO/IEC 27000, que entregan los lineamientos, procesos y procedimientos para la gestión de la seguridad en la información en todo tipo de empresa.

5.2.5 Que es ISO 27001. Es una norma internacional que compila todos los parámetros del Sistema de Gestión de Seguridad de la Información, disponible para ser implementada en cualquier tipo de institución ya sea de carácter pública o privada, grande o pequeña acreditada por auditores externos certificados. Éste estándar proporciona los lineamientos para la ejecución de controles de seguridad de acuerdo con las disposiciones particulares de las entidades.

EL SGSI está diseñado para elegir los controles de seguridad de acuerdo a las necesidades de protección de los activos (tangibles e intangibles) de la organización, para lo cual cuenta con 14 dominios para gestionar e implementar un SGSI, a saber:

- Política de Seguridad de la Información.
- Organización de la Seguridad de la Información.
- Seguridad de los recursos humanos.
- Gestión de Activos.
- Control de Acceso
- Criptografía.
- Seguridad Física y del entorno.
- Seguridad de las operaciones.
- Seguridad de las Comunicaciones.
- Adquisición, desarrollo y mantenimiento de sistemas.
- Relaciones con los proveedores.
- Gestión de incidentes de seguridad de la información.
- Aspectos de Seguridad de la información de la gestión de continuidad del negocio.

5.2.6. El Ciclo de Vida PHVA en inglés (PDCA). Para implementar y gestionar un Sistema de Gestión de la Seguridad de la Información, con base en el estándar ISO 27001, se utilizará el modelo o ciclo continúo PHVA, que permite a todos los

sistemas de gestión hacer una mejora continua del sistema. Como se representa en la figura 4.

Figura. 4. Ciclo de Vida PHVA

Fuente http://www.iso27000.es/sgsi_implantar.html

Plan: Establecer el SGSI[11]

- Definir los alcances del SGSI, enfocados en el negocio, su localización, la estructura organizacional, los activos y la tecnología con la que cuenta, justificando cualquier exclusión.
- Definir el alcance y los límites del SGSI, en este proceso no es obligatorio abarcar toda la organización, se puede realizar estipulando un alcance limitado.
- Definir una política de seguridad, en este paso se busca incluir el marco general y cada uno de los objetivos para dar cumplimiento a la seguridad de la información que se manejara en la organización.
- Revisar las obligaciones legales o contractuales referentes a la seguridad de la información.
- Alinear el contexto estratégico de gestión de riesgos de la institución en donde se debe establecer el SGSI y diseñar criterios para evaluar el riesgo.

Fijar una metodología que permita evaluar el riesgo y que a su vez sea apropiada tanto para el SGSI como para delimitar las necesidades reales de la organización.

[11] El portal de ISO 27001 en español obtenido. http://www.iso27000.es/articulos.html.

Es importante especificar los criterios de aceptación, el nivel mínimo de riesgo y determinar estrategias que eviten la perdida de información; lo fundamental de esta metodología es que los resultados alcanzados sean repetibles y aptos para realizar un proceso de confrontación, por lo que es necesario detllar una estrategia.

Reconocer los riesgos:

- Reconocer los responsables directos (propietarios), de los activos que están dentro del alcance del SGSI.
- Reconocer tanto las amenazas como las vulnerabilidades a las que se encuentran expuestos los activos.
- Reconocer los impactos en la integridad, confidencialidad y disponibilidad de los activos.

Analizar y evaluar los riesgos:

- Evaluar el impacto del negocio en cuanto a las fallas de seguridad, que puedan ocasionar problemáticas serias como la pérdida de confidencialidad, la integridad o en su caso la no disponibilidad de un activo de información.
- Determinar en tiempo real las posibles fallas de seguridad relacionadas con las amenazas, la vulnerabilidad, los impactos en los activos y los controles que ya estén puestos en marcha.
- Determinar el tipo de riesgo, es decir si es válido o es necesario realizar ajustes según los criterios establecidos.

Do: Implementar y utilizar el SGSI.[12]

- Definir los pasos para llevar a cabo el tratamiento de riesgos, identificando especialmente los recursos, actividades, las diferentes responsabilidades y las prioridades del SGSI.
- Implementar el plan referente al tratamiento de riesgos, el cual debe garantizar el alcance de los objetivos de control identificados con anterioridad, incluyendo de esta manera la asignación de recursos, responsabilidades y prioridades.
- Implementar los controles para asegurar el cumplimiento de los objetivos.
- Diseñar un sistema de métricas que permita obtener resultados reproducibles y que sean aptos para realizar comparaciones que permitan medir la eficacia de los controles o grupos de controles.
- Gestionar programas que se enfoquen en la capacitación del personal, mediante el desarrollo de manuales que garanticen la concientización de la seguridad de la información.
- Gestionar los recursos necesarios que permitan un continuo mantenimiento de la seguridad de la información.
- Implementar los procedimientos y controles que permitan detectar y dar una respuesta oportuna a los incidentes que se lleguen a presentar de seguridad.

[12] El portal de ISO 27001 en español obtenido. http://www.iso27000.es/articulos.html

***Check*: Monitorizar y revisar el SGSI**. [13]
La institución deberá cumplir con las siguientes recomendaciones:

- Identificar brechas e incidentes de seguridad.
- Establecer procedimientos que permitan realizar el monitoreo y la revisión con el fin de identificar errores en los resultados generados en el procesamiento de la información, para darles una solución oportuna.
- Asesorar a la dirección en el proceso evaluación de las actividades ejecutadas tanto por el personal como por los recursos tecnológicos y verificando de esta manera, el cumplimiento de las políticas estipuladas para garantizar la seguridad de la información.
- Revisar periódicamente la efectividad del SGSI, mediante la verificación del cumplimiento de las políticas y los objetivos propuestos para el SGSI, así mismo realizar un control y análisis de los resultados obtenidos en las auditorías internas y externas de seguridad, reconocer los incidentes, las sugerencias y las diferentes observaciones de todas las partes implicadas.
- Medir la efectividad de los controles, garantizando el cumplimiento de los requisitos de seguridad.
- Revisar periódicamente la planeación de evaluación de riesgos, (residuales y sus niveles de aceptación), teniendo en cuenta diversas variable y resultados obtenidos como lo son, aquellos posibles cambios en la organización, los recursos tecnológicos, los objetivos y los procesos de negocio, de igual forma la identificación de amenazas, la efectividad de los controles implementados, los requerimientos legales y las obligaciones contractuales, entre otras.
- Realizar auditorías internas del SGSI, en intervalos previamente establecidos.
- Evaluar regularmente el SGSI por parte de la dirección, con el objetivo de asegurar que el alcance definido es acertado y a su vez el SGSI se encuentra en continuo mejoramiento.
- Actualizar y realizar las respectivas modificaciones que permitan mejorar los planes de seguridad, a partir de los hallazgos encontrados durante las actividades revisión y verificación del SGSI

Act (Actuar): Mantener y mejorar el SGSI. [14]

La organización deberá regularmente:

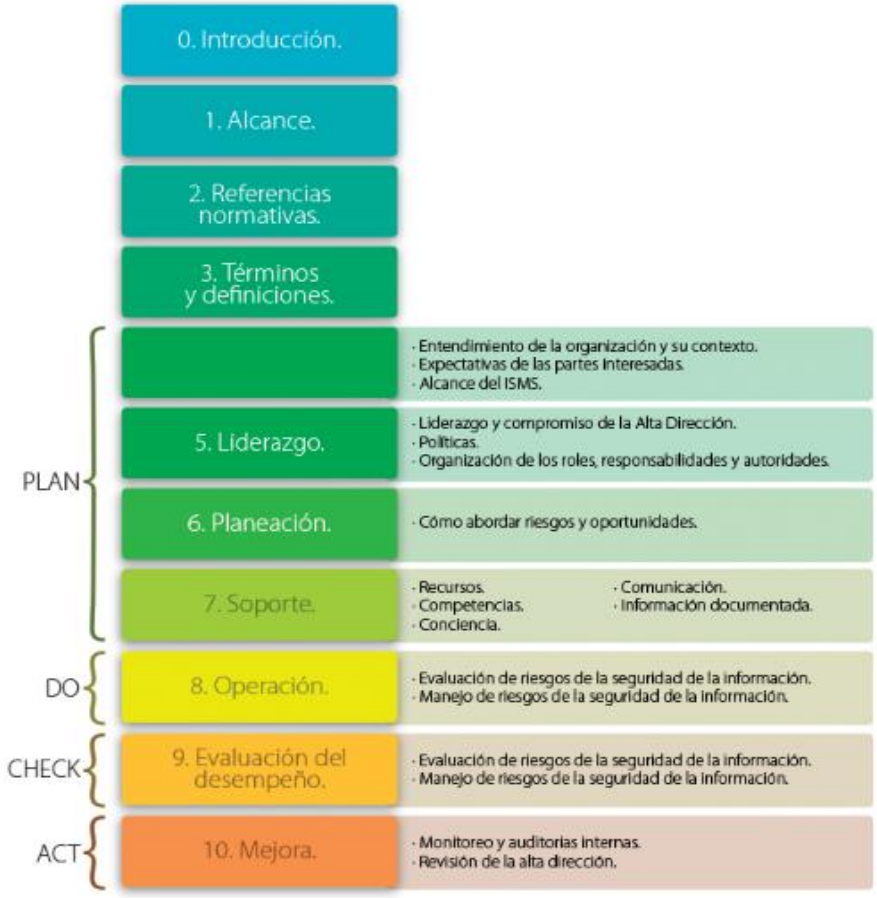
- Implementar mejoras identificadas al SGSI.
- Realizar acciones preventivas y correctivas adecuadas relacionadas con la cláusula 8 de ISO 27001 y a al aprendizaje adquirido de las experiencias propias y de otras organizaciones para dar soluciones a las no conformidades que han sido detectadas.

[13] El portal de ISO 27001 en español obtenido. http://www.iso27000.es/articulos.html
[14] El portal de ISO 27001 en español obtenido. http://www.iso27000.es/articulos.html

- Comunicar y capacitar con detalle las acciones y mejoras a todas las partes interesadas y la forma de actuar o implementar dichas mejoras.
- Certificar que todas aquellas mejoras que se implemente cumplan con los objetivos previstos por el SGSI.

5.2.7. Estructura De La Norma ISO 27001:2013. Esta norma internacional proporciona un conjunto de lineamientos bajo una misma estructura, a todas las organizaciones para el desarrollo y la ejecución de un Sistema de Gestión de Seguridad de la Información, facilitando la integración entre los sistemas. El objetivo de implementar y certificar SGSI es garantizar la confidencialidad, integridad y disponibilidad de la información de la organización. En la figura 5 que se encuentra a continuación, es posible identificar las secciones de la estructura de la Norma ISO 27001:2013.

Figura. 5. Estructura de la Norma ISO 27001:2013 Vida.



Fuente: http://www.magazcitum.com.mx/?p=2397#.W9-3FpNKjIW

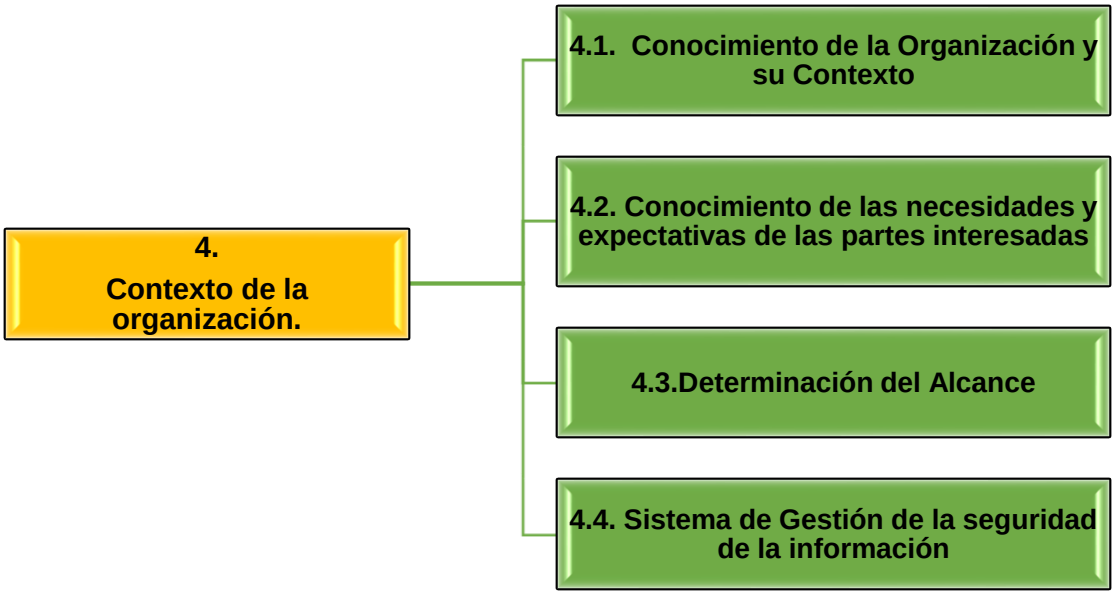
5.2.7.1. Sección 1 – Alcance. Esta Sección estipula, que es de carácter obligatorio el cumplimiento de los requisitos específicos de los capítulos del 4 al 10 del documento, para obtener de esta manera la conformidad de cumplimiento y lograr certificarse[15].

5.2.7.2. Sección 2 – Referencias normativas. Esta Sección, menciona la importancia de recurrir a aquellos documentos afines con la seguridad de información.[16]

5.2.7.3. Sección 3 – Términos y definiciones. Esta Sección describe la terminología de carácter obligatorio que se debe manejar a la hora de implementar la norma.

5.2.7.4. Sección 4 – Contexto de la Organización. Esta Clausula permite conocer e identificar el contexto interno y externo de la actividad de la organización y de esta manera adoptar políticas que permitan el mejoramiento para suplir estas necesidades. Esta Sección, se encuentra compuesta por cuatro partes como se puede observar en la siguiente figura.

Figura. 6. Estructura de la Sección 4 – ISO/IEC 27001:2013.

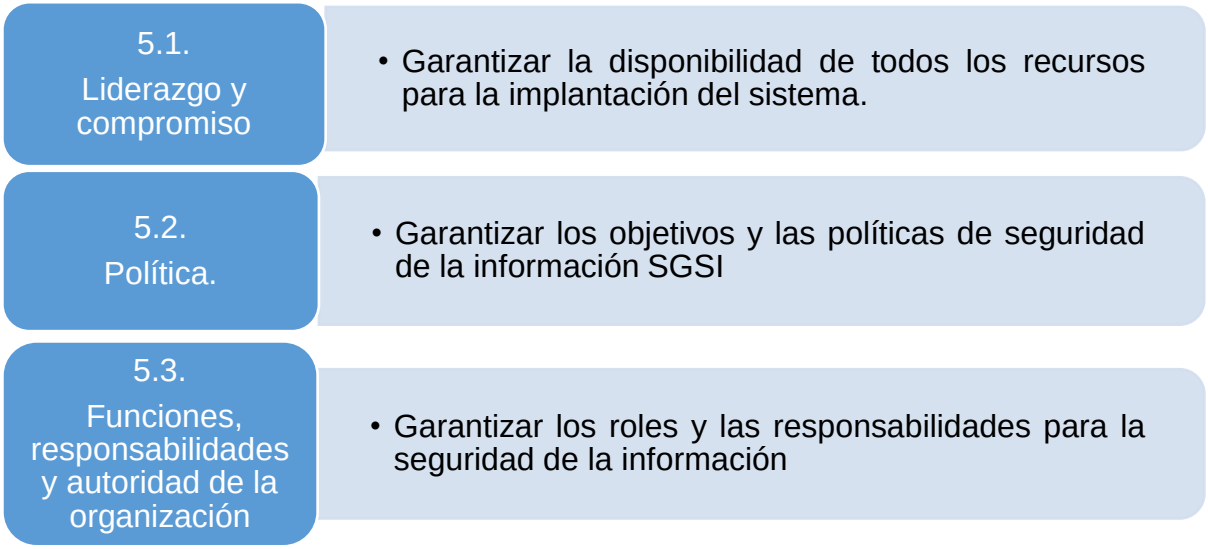


Fuente: ISO/IEC 27001:2013

[15] https://www.isotools.com.mx/la-estructura-la-nueva-norma-iso-27001-2013/
[16] https://www.isotools.com.co/normas/ntc-iso-27001/

5.2.7.5. Sección 5 – Liderazgo. Esta Sección hace referencia al liderazgo, compromiso y responsabilidad de la alta gerencia para con el SGSI, la sección de liderazgo está conformada por tres numerales como se observa en la figura a continuación (figura 7).

Figura. 7. Estructura de la Sección 5 – ISO/IEC 27001:2013



Fuente: ISO/IEC 27001:2013

5.2.7.6. Sección 6 – Planificación. Esta Sección busca identificar los riesgos y su planificación, así como definir los objetivos específicos de seguridad, y los planes que se van a emplear para alcanzar las metas. Las organizaciones deben tener presente que es de suma importancia realizar una valoración de los riesgos que se pueden presentar en la seguridad de la información, para ello se debe utilizar una metodología que permita:

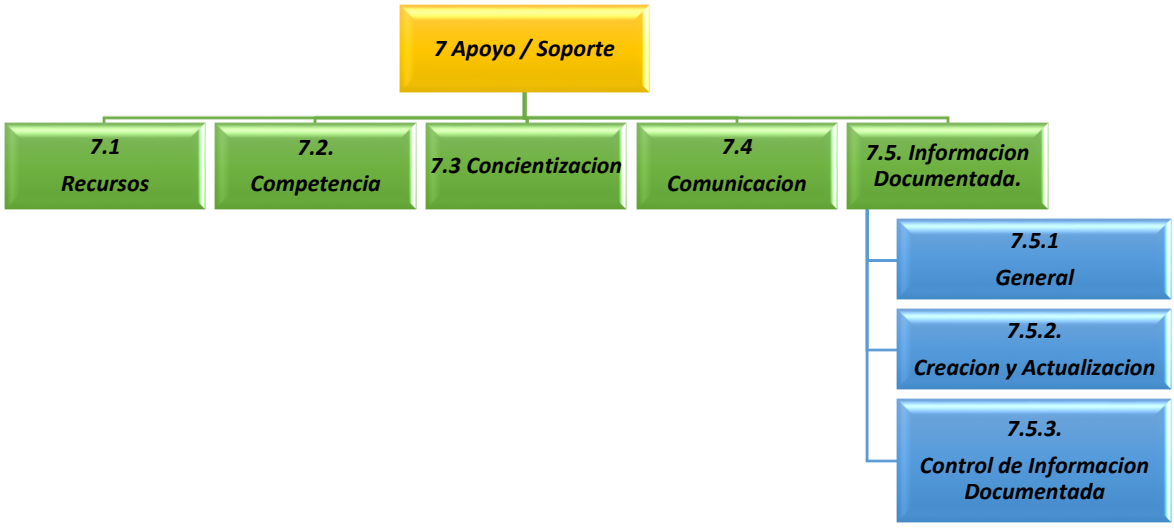
- Establecer los criterios de aceptación del riesgo.
- Fijar los pasos para realizar la evaluación del riesgo.
- Identificar los riesgos de la seguridad de la información.
- Identificar el origen del riesgo.
- Analizar los riesgos mediante la evaluación de las consecuencias y las posibles oportunidades de repetición.
- Determinar el nivel de riesgo.
- Priorizar los riesgos para proponer posibles soluciones y prevenciones.

Figura. 8. Estructura de la Sección 6 – ISO/IEC 27001:2013.

Fuente: ISO/IEC 27001:2013

5.2.7.7. Sección 7 – Apoyo/Soporte. Esta Sección, establece los requisitos del personal de soporte de la organización encargado de realizar el diseño, la implementación y el mejoramiento en el Sistema de Gestión de Seguridad de la Información según la norma ISO 27001:2013. Esta Sección consta de cinco subsecciones como se indica en la figura a continuación (figura 9).

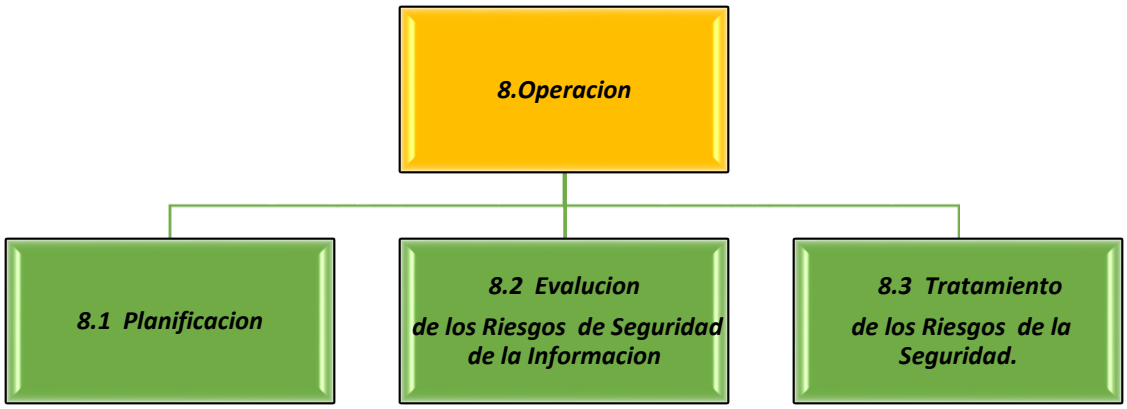
Figura. 9. Estructura de la Sección 7 – ISO/IEC 27001:2013



Fuente: ISO/IEC 27001:2013

5.2.7.8. Sección 8 – Operación. En esta sección se habla acerca del cumplimiento de los requisitos del SGSI y a la ejecución de lo planificado en la Sección 6, esto se logra por medio de una adecuada planificación, implementación y control de los procesos organizacionales, llevando a la par una valoración detallada de los riesgos a los que se somete la seguridad de la información y por supuesto, el posterior tratamiento[17]. En la figura 10. Se observa su estructura.

Figura. 10.Estructura de la Sección 8 – ISO/IEC 27001:2013



Fuente: ISO/IEC 27001:2013

5.2.7.9. Sección 9 – Evaluación del desempeño. Hace referencia a la importancia de realizar el seguimiento, medición, análisis y evaluación del desempeño del SGSI en la organización, lo anterior se lleva a cabo gracias a las auditorias internar y a la revisión por parte de la dirección del grupo de SGSI. Esta Sección consta de tres etapas como se muestra en la figura 11.

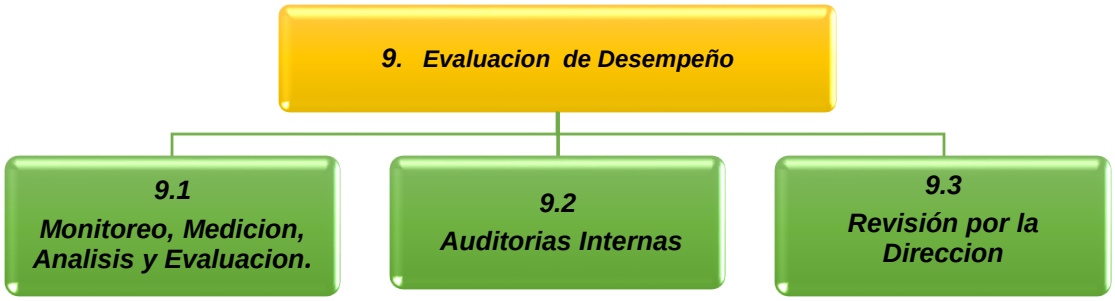
En la Sección 9.1, se expone la forma de hacer el Monitoreo, medición, análisis y evaluación de la efectividad del SGSI en la organización, para lo cual se debe analizar cada uno de los ítems expuesto a continuación:

- ¿Qué se debe monitorear?
- Métodos de monitoreo y medición.
- Frecuencia de ejecución.
- ¿Quién realiza monitoreo y medición?

[17] www.isotools.com.co/normas/ntc-iso-27001/

La información recolectada del monitoreo y medición, debe estar documentada y organizada, para que sirva como evidencia del SGSI.

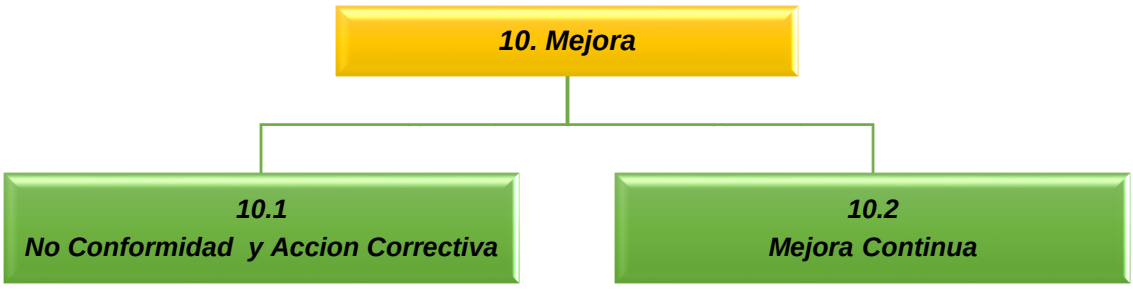
Figura. 11. Estructura de la Sección 9 – ISO/IEC 27001:2013.



Fuente: ISO/IEC 27001:2013

5.2.7.10. Sección 10 – Mejora. Esta Sección hace referencia a la estructura de alta gerencia que es la responsable de establecer las necesidades de la organización en pro de una mejora continua, es decir, que sean capaces de detectar las no conformidades y saber qué medida adoptar para darle solución y así, mejorar continuamente el Sistema de Gestión de Seguridad de la Información.[18]. Como se puede observar en la figura 12, esta sección se divide en dos partes, la primera habla de las no conformidades y acciones correctivas, y la segunda, acerca de la mejora constante del sistema.

Figura. 12.Estructura de la Sección 10 – ISO/IEC 27001:2013

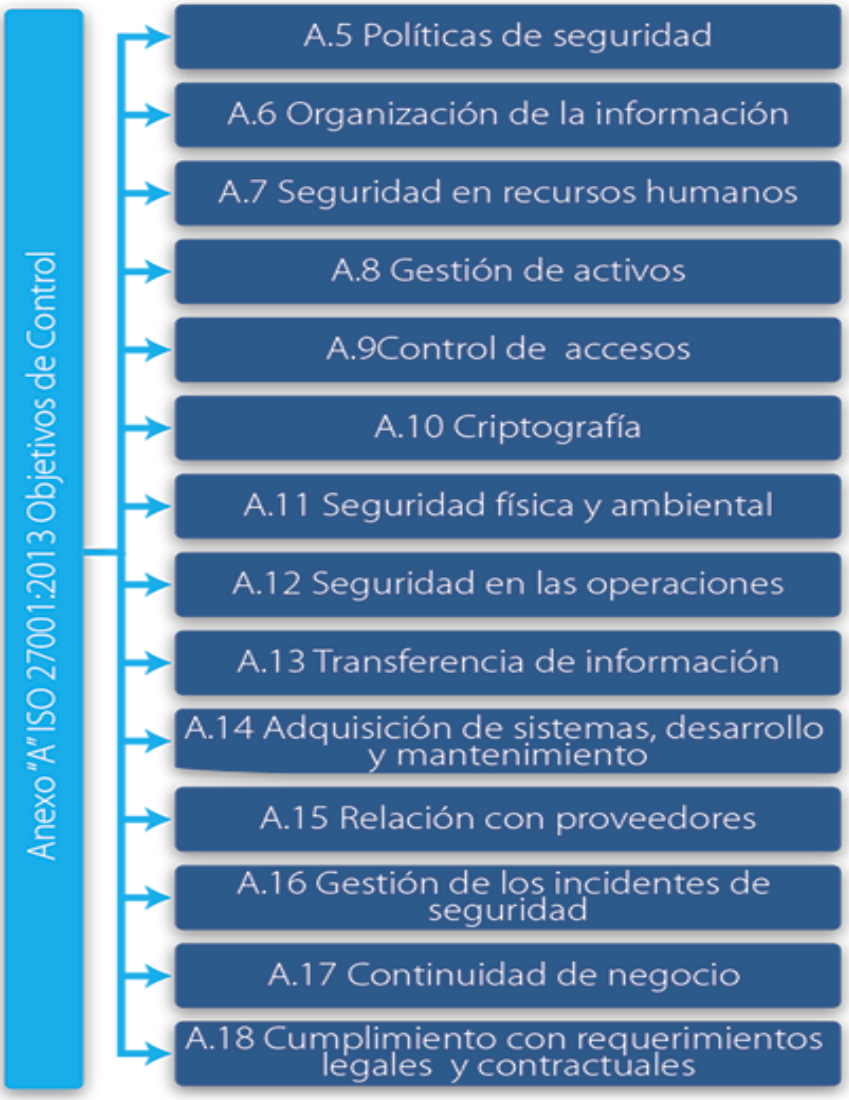


Fuente: ISO/IEC 27001:2013

[18] https://www.isotools.com.co/normas/ntc-iso-27001/

5.2.7.11. Anexo A – Objetivos de control y controles de referencia. El Anexo A, hace referencia a un listado de controles de seguridad, que pueden ser utilizados como una herramienta de gestión, para mejorar la seguridad de la información, dicho anexo, esta compuesto por un total de 114 controles mejor conocidos como medidas de seguridad, los cuales se encuentran distribuidos en 14 secciones que van de la A.5 a A.18, como representa en la en la Figura 13.

Figura. 14. Dominios de Seguridad - Anexo A - ISO/IEC 27001:2013

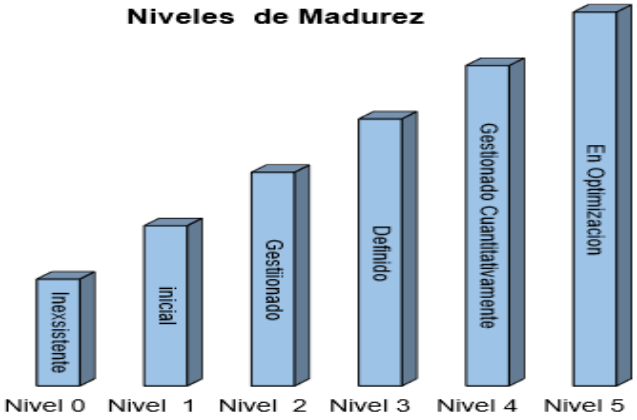


Fuente: http://www.magazcitum.com.mx/?p=2397#.WgW9T_nia1t

5.2.8. Nivel de madurez. Para los encargados de la seguridad de la información de una organización o institución, resulta de suma importancia establecer grados de madurez a través de la estratificación de la organización y la búsqueda de políticas de crecimiento de forma estructurada y planificada, y que a su vez, se encuentren estructuradas bajo las políticas de seguridad previamente diseñadas para un correcto funcionamiento de la organización. Para tal efecto, se establecen modelos para verificar el nivel de madurez, sin embargo, para este análisis, se referencia únicamente el modelo **CMMI**[19], que resulta ser una recopilación de buenas prácticas específicas y genéricas, relacionadas para un conjunto predefinido de áreas de proceso para el mejoramiento de éstos y los procedimientos utilizados en los productos o servicios de la organización.

Este modelo refleja niveles de madurez tanto en su diseño como en el contenido y es llevado a cabo por equipos de trabajo relacionados con el gobierno, la industria y del *Software Engineering Institute* (S.E.I, 2010) [20] En este orden, el nivel de madurez, es una plataforma evolutiva previamente definida para lograr una constante mejora de los procesos organizacionales, planteando de esta manera el desarrollo de procesos de suma importancia, con el fin de realizar una preparación que permita pasar de un nivel a otro, lo cual se logra únicamente con el cumplimiento de ciertas metas específicas y genéricas, relacionadas con cada conjunto predefinido de áreas de procesos. (S.E.I, 2010)[21], como se logra identificar en la figura 15.

Figura. 15. Niveles de Madurez



Fuente: *CMMI®, Software Engineering Institute, 2010.*

[19] *Capability Maturity Model® Integration*
[20] CMMI® para Desarrollo, Versión 1.3. Mejora de los procesos para el desarrollo de mejores productos y servicios. Obtenido. https://resources.sei.cmu.edu/asset_files/WhitePaper/2010_019_001_28782.pdf
[21] Ibíd.

5.2.8.1. Nivel de madurez 0: Inexistente. Hay total falta o ausencia de procesos y procedimientos de seguridad. En este nivel, la organización no ha logrado reconocer o no está enterada que existen problemas que deben ser resueltos lo más pronto posible.

5.2.8.2. Nivel de madurez 1: Inicial. En este nivel, generalmente los procesos son confusos, sin planificación, con actividades desconectadas y sin un orden definido, en este punto, para que las organizaciones que se encuentran en este nivel tengan éxito es necesario que cuente con un personal competente en la resolución de problemas, debido a que su entorno es poco estable y no proporciona un ambiente óptimo para dar un soporte a los procesos. Es importante tener claro que muchas de las organizaciones que se encuentran en este nivel de madurez, es decir en el Nivel 1, constantemente fabrican productos y ofrecen servicios de calidad con un buen funcionamiento, pero muchos de ellos se exceden tanto en el presupuesto como en el tiempo estipulado para su creación , por otro lado, en este nivel las organizaciones tienden a comprometerse en exceso ocasionado el abandono de sus procesos en los momentos de crisis y no cuentan con la capacidad para repetir sus éxitos. *(Software Engineering Institute, 2010)*[22]

5.2.8.3. Nivel de madurez 2: Gestionado. En este nivel, se garantiza que la planificación y la ejecución de los procesos deben estar bajo las políticas institucionales, así mismo, se debe contar con recursos propios y un personal calificado a la hora de iniciar cualquier proyecto para garantizar la producción de resultados controlados vinculando a todos los actores del proceso. Se debe realizar monitoreo, control, revisión y evaluación frente a la articulación de los lineamientos del proceso con el fin de mantener que las prácticas existentes en los periodos o etapas difíciles. Generalmente, los proyectos se realizan y gestionan de acuerdo a planes documentados. *(Software Engineering Institute,* 2010)[23]

5.2.8.4. Nivel de madurez 3: Definido. En este nivel las organizaciones cuentan con herramientas, procedimientos y metodologías que en un trabajo conjunto generaran procesos bien determinados y comprendidos, de igual manera se estipulan actualizaciones y/o mejoras a largo plazo. Estos procesos estándar contribuyen a establecer la integridad en toda la organización. (*Software Engineering Institute*, 2010) [24]

5.2.8.5. Nivel de madurez 4: Gestionado cuantitativamente. Aquí se gestiona y cuantifica la organización, se establecen objetivos cuantitativos de

[22] CMMI® para Desarrollo, Versión 1.3. Mejora de los procesos para el desarrollo de mejores productos y servicios. Obtenido. https://www.sei.cmu.edu/library/assets/whitepapers/Spanish%20Technical%20Report%20CMMI%20V%201%203.pdf
[23] Ibíd.
[24] Ibíd.

calidad y rendimiento de los procesos, basados en las necesidades del cliente. Las variables de calidad y el rendimiento se exponen y analizan de manera estaistica y se gestionan durante la vida de los proyectos. (*Software Engineering Institute*, 2010) [25]

5.2.8.6. Nivel de madurez 5: En optimización. Las organizaciones que alcanzan este nivel, se enfocan en perfeccionar de manera continua el rendimiento de los procesos fomentando la aplicación de la tecnología. Por otra parte, la organización se interesa por reconocer las causas frecuentes de variación del proceso, en realizar cambios y mejorar constantemente el rendimiento, garantizando el alcance de sus objetivos cuantitativos. Finalmente, en este nivel, se ve reflejado el rendimiento de la organización y los cambios en los objetivos del negocio; éstos se utilizan como criterios para gestionar la mejora de procesos. (S. E. I, 2010)[26].

A continuación, se describen los niveles de madurez y sus características en cada uno de sus niveles en el Cuadro 7.

Cuadro. 7. Niveles de Madurez para la seguridad de la información

	Descripción
Nivel 1 (Inicial)	Se deben reconocer los activos de la organización de manera general.
	Tanto los activos como la información, la seguridad, los equipos y la sede de la organización deben ser clasificados para implementar la mejor protección a cada uno de ellos.
	Se presentan diversas situaciones de amenazas contra la información, los activos y la continuidad del negocio, pero la organización no los considera como situaciones de alto riesgo.
	Los empleados tienen conductas de riesgo, por ejemplo, prestan las claves, dejan los equipos con las sesiones abiertas, entre otras, todo ello debido a la falta de conciencia y capacitación en cuanto a la seguridad informática.
	Se responde reactivamente a las amenazas de intrusión, virus, robo de equipos y de información.
	La organización no cuenta con el personal capacitado e interdisciplinario para abordar las diversas problemáticas referentes a la seguridad informática.
	Se cuenta con un proceso de desarrollo de software, pero este no tiene en cuenta las normas de la seguridad informática.

Fuente: autor

[25] Ibíd.
[26] Ibíd.

Cuadro7. (Continuación).

	Descripción
Nivel 2 (Gestionado)	Bajo la Norma ISO 27002, se procede a definir cada una de las Políticas de Seguridad de la Información de la organización, el interés por identificar las causas que originaron la ocurrencia de situaciones de alto riesgo para la información, los activos y la continuidad del negocio van aumentando y de igual manera se diseñan planes para dar a conocer las Políticas de Seguridad de la Información.
	Se identifican los riesgos y las vulnerabilidades a las se encuentran expuestos los equipos, la información y las sedes, por medio de las políticas.
	Se lleva un control por medio de informes en donde se plasman aquellas novedades e incidentes relacionados con la seguridad.
	Se cuentan con Planes de continuidad del negocio, es decir los planes que se desarrollaran en caso que el negocio este pasando por un momento crítico, garantizando de esta manera la continuidad del mismo, no obstante, se dejan otros procesos de la organización por fuera.
	Se crean los diferentes roles del área de Seguridad informática, así mismo se definen las actividades que desarrollara cada uno de ellos.
	La creación de un inventario tanto del hardware como del software es de suma importancia, este se realiza una vez se han clasificado todos los activos con los que cuenta la organización.
	Se va incluyendo la seguridad informática dentro del proceso de desarrollo de software, pero aún no es el momento de documentarla en la metodología de desarrollo de software de la organización.
	El personal empieza a mostrar una conciencia sobre la seguridad informática, aunque no tienen un compromiso solido con ella.
Descripción	
Nivel 3 (Definido)	Las Políticas de Seguridad de la Información son divulgadas en toda la organización.
	Se cuenta con un grupo interdisciplinario, el cual se encargara de la divulgación de las medidas de seguridad que deben tener en cuenta para garantizar la conservación de la información de la organización, este proceso se realiza en cada una de las áreas a las que representan.

Fuente: CMMI® para Desarrollo, Versión 1.3. Mejora de los procesos para el desarrollo de mejores productos y servicios. Obtenido https://www.sei.cmu.edu/library/assets/whitepapers/Spanish%20Technical%20Report%20CMMI%20V%201%203.pdf

Cuadro7. (Continuación).

Nivel 3 (Definido)	El personal está más comprometido con el tema de la seguridad informática.
	Se incluye dentro del proceso de desarrollo de software las normas de seguridad informática.
	Se crean e implementan procedimientos que capaciten al personal en temas tales como el manejo seguro de la información y los equipos de cómputo.
	La red de la organización cuenta con un monitoreo constante para prevenir ataques, intrusiones, o infecciones de virus.
Descripción	
Nivel 4 (Gestionado Cuantitativamente)	Los activos de la organización están más seguros gracias a las revisiones periódicas y/o monitoreos que se realizan.
	Se utiliza un indicador de cumplimiento para establecer si las Políticas de Seguridad de la Información y las cláusulas de seguridad establecidas por la organización.
	Se verifica el correcto funcionamiento por medio de pruebas de control las cuales se realizan de manera sistemática.
	Los simulacros de incidentes de seguridad, se implementan con el fin de para probar la efectividad de los planes de respuesta a incidentes.
	La realización de pruebas es más frecuente, debido a que permite verificar que las aplicaciones o software desarrollados están cumpliendo con los requisitos de seguridad estipulados en la metodología de desarrollo de software de la organización.
	Se llevan a cabo pruebas de intrusión a los equipos de la organización con el objetivo de detectar claves de bajo nivel (fáciles de adivinar) y los errores que permiten el ingreso al sistema por parte de usuarios no autorizados.
Nivel 5 (En Optimización)	**Descripción**
	El personal contribuye y apoya la modernización de la seguridad informática en la organización.
	Los incidentes y fallas en la seguridad que se presentan, sirven para tomar medidas y mejorar continuamente. Seguridad presentada.
	Los planes de respuesta e incidentes son competencia de todas las áreas de la organización (críticas y no críticas).

Fuente: CMMI® para Desarrollo, Versión 1.3. Mejora de los procesos para el desarrollo de mejores productos y servicios. Obtenido https://www.sei.cmu.edu/library/assets/whitepapers/Spanish%20Technical%20Report%20CMMI%20V%201%203.pdf

Cuadro. 8. Prácticas de Seguridad al Interior de Cada Nivel

Práctica de la Norma ISO/IEC 27000	
Nivel 1 (Inicial)	5.2 Clasificación de la Información.
Nivel 2 (Gestionado)	3.1 Políticas de Seguridad de la Información
	4.1.1 Foro Gerencial sobre la Seguridad de la Información
	4.1.2 Coordinación de la Seguridad de la Información
	4.1.3 Asignación de responsabilidades en materia de la seguridad de la información
	5.1.1 Catálogo de activos o recursos de información
	6.3 Respuesta a incidentes y anomalías en materia de seguridad
	10.1.1 Estudio y especificaciones de los requisitos de seguridad
	11.1.1 Proceso de administración de la continuidad del negocio
	11.1.3 Diseño e implementación de planes de continuidad del negocio
Nivel 3 (Definido)	6.2 Capacitación del usuario
	7. Seguridad Física y Ambiental
	8.1.3 Procedimiento y manejo de incidentes 8.5 Administración de la red
	9.5 Seguimiento de acceso al sistema operativo
	10.2 Seguridad en los sistemas de aplicación
Práctica de la Norma ISO/IEC 27000	
Nivel 4 (Gestionado Cuantitativamente)	9.2 Administración de acceso de usuario
	9.3 Responsabilidad del usuario
	9.5.4 Sistema de Administración de Contraseñas
	9.6 Controles de Acceso a las aplicaciones
	9.7 Monitoreo del acceso y uso de los sistemas
	10.3 Seguimientos criptográficos
	10.4 Seguridad de los archivos del sistema
	11.1.5 Prueba, mantenimiento y reevaluación de los planes de continuidad del negocio
	12.3.1. Controles de auditoría de sistemas
Nivel 5 (En Optimización)	11.1.5.1 Sostenimiento y reevaluación del plan

Fuente: Páez, C. Obtenido. http://www.academia.edu/6744740/5.niveles_de_madurez_para_el_proceso_de_seguridad_de

5.3. MARCO LEGAL.

Con el Nacimiento de las comunicaciones electrónicas, las situaciones sociales, económicas y políticas de la segunda guerra mundial, el descubrimiento de los circuitos integrados y el desarrollo y permeación de las Tecnologías de la información y las comunicaciones (TIC), han generado diversos cambios a nivel global, dando origen entre otros al comercio electrónico a mediados de los años 60, en E.E.U.U, lo que luego daría el paso mediante la resolución 2205 (XXI), de 17 de diciembre de 1966, por la cual se logra establecer la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional y en ese sentido la Ley Modelo de la CNUDMI sobre Comercio Electrónico, como directriz internacional en el intercambio comercial.

En Colombia la ley 527 de 1999, está orientada a definir y reglamentar el uso y acceso de los mensajes de datos, las firmas digitales, el comercio electrónico y los temas relacionados con las entidades que pueden hacer el ejercicio de certificación.

En este mundo globalizado, nadie se escapa a la influencia de las TIC, en casi todas las áreas de conocimiento y desarrollo social, político y comercial, y con esta influencia también han surgido una serie situaciones de riesgo y comportamientos ilícitos que pueden ser denominados como delitos informáticos, contemplados en Colombia mediante la expedición de la ley 1273 del 2009, dichos delitos pueden afectar directa e indirectamente a una organización y como contrarrestar o minimizar la perdida de información, mediante el diseño de políticas, estrategias y controles que certifiquen, avalen y/o garanticen la disponibilidad, confidencialidad e integridad, de la seguridad de la información dentro de las organizaciones. A continuación, se describe parte de la legislación colombiana relacionada con seguridad de la información.

5.3.1 Ley 527 de 1999 de comercio electrónico. En su Artículo 1. Describe entre otros el ámbito de aplicación de dicha normatividad, donde presume que puede aplicarse a todo tipo de información en forma de mensaje de datos, excepto en los casos descritos a continuación:

a) En aquellas obligaciones adquiridas por el Estado colombiano en el marco de tratados internacionales y convenios.[27]
b) En las advertencias y/o notificaciones escritas que por disposición de la normatividad legal deban ir necesariamente estampadas y/o impresas de productos en razón a los riesgos que implica su uso, consumo y comercialización[28].

[27] Propiedad de la Secretaría Jurídica Distrital de la Alcaldía Mayor de Bogotá D.C. ley 527 del 1999 obtenida. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276
[28] Ibíd. p51.

5.3.2. Mensaje de datos. Este ítem describe entre otros toda aquella información que ha sido creada, difundida recibida, guardada o comunicada por cualquier tipo de medio ópticos, electrónico o similares como pueden ser, por mencionar algunos, el internet, el correo electrónico, el Intercambio Electrónico de Datos (EDI), el telefax y el telegrama.[29]

5.3.3. Comercio electrónico. Se creó para la realización de intercambio comercial mediante el uso de los denominados mensajes de datos o cualquier medio electrónico, donde se pueda realizar compra de bienes y servicios; dependiendo la legislación de cada país

5.3.4. Firma Digital. En ese ítem se entiende como un valor numérico que es adherido a un mensaje de datos en el cual es utilizado un proceso matemático, que vinculado al cifrado del iniciador y al texto que se ha puesto en el mensaje permite establecer que este valor es un producto exclusivo obtenido con la clave del iniciador y que el mensaje que se ha desarrollado de forma inicial no haya sido alterado después de realizada la transformación[30]

5.3.5. Intercambio Electrónico de Datos (EDI). Se refiere a la transmisión electrónica de datos de un computador a otro, que está constituido bajo las normas técnicas pactadas al efecto.[31]

5.3.6. Sistema de Información. Se entenderá como todos aquellos sistemas que son usados para crear, recibir, enviar, guardar o procesar de alguna otra manera mensajes de datos.[32]

5.3.7. Ley 1273 de 2009 de la protección de la información y de los datos[33]. Mediante la cual se hacen modificaciones al Código Penal, y se permite la creación de un nuevo bien jurídico tutelado – titulado *"De la protección de la información y de los datos"*- y se resguardan de manera integral los sistemas que usan las TIC, entre otras disposiciones.

En su capítulo I se describen las disposiciones para regular los delitos y/o atentados que afecten o estén en contra de la integridad, confidencialidad y disponibilidad de los datos y de los sistemas informáticos, estos son castigados con pena de prisión

[29] Ibíd. P. 51
[30] Ley 527 de 1999, agosto 18, Obtenido. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276
[31] Ibíd.
[32] Ibíd.
[33] Obtenida de www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 SMLV, como se describe a manera de resumen en los siguientes artículos:

“Artículo 269A: Acceso abusivo a un sistema informático. Hace referencia a todas aquellas situaciones donde sin permiso o fuera de los términos acordados, se acceda de forma general o por partes a un sistema informático que se encuentre protegido o no con un régimen de seguridad, o se conserve dentro de este en contra de la voluntad de quien tenga todos los derechos a excluirlo, (…).”

“Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. Todo aquel que sin tener las facultades y/o derechos, imposibilite o genere obstáculos para el funcionamiento o uso normal a un sistema informático, a los que puedan estar allí almacenado, o a una red de telecomunicaciones, (…)”

“Artículo 269C: Interceptación de datos informáticos.

Todo aquel que sin ninguna orden de tipo judicial logré interceptar datos informáticos en su ligar de creación u origen, de destino, en las partes interna de un sistema informático, o en las emisiones electromagnéticas que son producto de un sistema informático que los movilice incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.”

“Artículo 269D: Daño Informático.

Todo aquel que, sin tener facultades genere daños, destruya, elimine, deteriore, modifique o aniquile datos de tipo informático o un sistema de manejo de información o sus partes o mecanismos lógicos (…).”

“Artículo 269E: Uso de software malicioso.

Todo aquel que, sin tener facultades, origine, adquiera, comercie de manera ilegal, distribuya, envíe, despache, ingrese o saque del territorio nacional cualquier tipo de software malicioso u otros programas computacionales con fines dañinos, (…).”

“Artículo 269F: Violación de datos personales.

Todo aquel que, sin tener facultades, de manera individual o con apoyo de un tercero logre obtener, compilar, ofrecer, sustraer, comercializar, canjear enviar, comprar, interceptar, divulgar, modificar o emplear códigos de tipo personal, datos personales guardados en ficheros, bases de datos, archivos, o medios similares (…).”

“Artículo 269G: Suplantación de sitios web para capturar datos personales. Todo aquel que con fines delictivos y sin tener las facultades para ello, logre crear,

desarrollar, comercializar ilegalmente vender, ejecutar, programar o enviar páginas electrónicas, enlaces o ventanas emergentes, (…)."

5.3.8. Ley 1581 de 2012 protección de datos personales. Esta ley reza en su Artículo 1o. el objeto, el cual busca desarrollar el derecho en el marco de la constitución que tienen las personas de estar al tanto, actualizar y reformar todas aquellas informaciones que hayan sido recolectadas en bases de datos o archivos, que sean sobre ellos, también describe los demás derechos, garantías y libertades de tipo constitucional a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.[34]

5.3.9. Ley 1341 del 30 de julio de 2009. En esta ley de describen los principios y conceptos relacionados a la sociedad de la información y la ordenación de las Tecnologías de la Información y las Comunicación TIC- donde se crea la Agencia Nacional del Espectro y se establecen otras disposiciones. [35]

5.4. MARCO CONCEPTUAL

En la sociedad digital, la sociedad informacional, la seguridad de la información es un conjunto de medidas preventivas que toman en las empresas (colectiva, individual, cooperativa, entre otras), si es pública o privada, todas buscan proteger los activos y minimizar la pérdida de información privilegiada, estas medidas buscan establecer políticas, procedimientos, seguridad lógica y física, para que solo pueda ser utilizada por personal autorizado, para mantener la confiabilidad, la integridad y la disponibilidad de la información.

Los datos informacionales "información" es procesada, enviada y almacenada en medios como equipos de cómputo, Smartphone, tabletas, lo cual la hace vulnerable. Por tanto, se hace importante contar con un sistema de seguridad de la información el cual debe contener:

Información documentada: Son los procedimientos que las empresas deben elaborar para implementar un sistema de gestión de seguridad de la información, teniendo en cuenta como controlar y mantener, así como el medio en que se encuentre contenida la información para su conservación y consulta. – ISO 9001, Sistemas de gestión de la calidad, términos y definiciones[36].

---

[34] Ley 1581 de 2012 Decreto 1377 de 2013, Obtenido. http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

[35]Ley 1341 de 2009. Obtenido de. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=36913

[36] ICONTEC, Instituto Colombiano de Normas Técnicas. NTC ISO 9001:2015. 2015. P33

Identificación y valoración de activos: Son las actividades que se deben realizar para medir las amenazas y vulnerabilidad que tienen los activos, de manera que se pueda determinar cuáles y como deben ser protegidos para mitigar el riesgo al que están expuestos[37]

Control de acceso: Controles que se establecen al interior de la empresa, para el acceso a la red y software seguro. Con la definición de este control se concede la autorización para el uso de un sistema, software o área de la empresa[38]

Evaluación y tratamiento de los riesgos: Son las actividades realizadas para identificar el impacto y probabilidad de los riesgos y validando lo efecticos que pueden ser los controles o tratamientos, a través de una metodología estándar que sea conocida y apropiada por todos los involucrados al interior de la empresa.[39]

Declaración de aplicabilidad: en estas líneas descritas en un documento se relacionan los 114 controles del anexo A de la norma NTC ISO 27001:2013[40]; para comprobar y contar con evidencia de que la empresa creó los controles establecidos por la Norma.

Continuidad de negocio: La empresa debe gestionar la continuación o trazabilidad de la seguridad de la información durante el uso de esta, pruebas, planes de contingencia y regreso a la normalidad de las operaciones. Se debe establecer un plan de pruebas para conocer el uso adecuado de la información[41]

Incidentes de seguridad de la información: las organizaciones empresariales están en la obligación de definir la gestión que llevara a cabo en los incidentes o eventualidades de seguridad de la información que se puedan presentar, con el fin de identificar los riesgos a los cuales se expone la información. Todos los

---

[38] ISO, *International Organization for Standardization Information technology --Security techniques. Information security management systems Overview and vocabulary. 2016*. P37

[39] NTC ISO 31000 de. 2009, disponible en https://calidadgestion.wordpress.com/2016/10/28/gestion-del-riesgo-iso-31000/

[40] Declaración de aplicabilidad. disponible en: <https://www.idu.gov.co/documents/20181/251887/FO-TI-27+Formato+Declaracion+de+Aplicabilidad++V_1.0+-+Diligenciado+Dic2015.pdf/1138b1b6-6f0c-41cf-85b1-7383c5f15f54>

[41] Contingencia TIC vs continuidad de negocio. disponible en https://www.incibe.es/protege-tu-empresa/blog/contingencia-vs-continuidad

[40] Metodología Magerit
. disponible en: <https://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionarriesgos/>

empleados deben estar en la facultad de reportar los incidentes al encargado de seguridad de la información[42]

Activo: Elementos físicos o lógicas, que pueda tener un valía e importancia para la organización.

Activos Intangibles: Son todas aquellas pertenencias identificables, inmateriales, de carácter no monetario, simbolizados en derechos, privilegios de competitividad, que en determinado momento son de alto valor, porque favorecen directa e indirectamente al acrecimiento de utilidades de la organización.

Activo de información: Son todos aquellos recursos como: bases de datos, contratos, sistemas de información, manuales, y todos sus recursos informáticos relacionados con el tratamiento de esta, que tenga valor para la universidad), que utiliza el Sistema de Gestión de Seguridad de la Información, para su funcionamiento y a la vez para cumplir con los objetivos propuesto por la alta dirección. Según [150/1EC 13 335-1:2004'], cualquier elemento que tiene cuantía, valía o valor para la empresa u organización.

Auditoría de seguridad de la información: Son las revisiones que se desarrollan al Sistema de gestión de seguridad de la información (SGSI) para determinar si es adecuado, si es acorde con lo establecido en la norma e identificar oportunidades de mejora

Autorización: Es la forma que tienen las organizaciones para garantizar que el personal pueda tener acceso de manera segura a la información y/o transacciones propias de la organización, dando cumplimiento al manual de políticas de seguridad de la información.

6 DISEÑO METODOLÓGICO

La presente monografía, se desarrolla en el marco de la Línea de investigación en Gestión de Sistemas, de la Universidad Nacional Abierta y a Distancia UNAD, cuyo objetivo está orientando a apoyar el desarrollo productivo, tecnológico y social empresarial mediante el análisis, diseño, implementación o administración de sistemas de información y las TIC que estén basados en la plantificación, dirección, control, evaluación y realimentación de actividades procedimentales.[43]

El proyecto busca analizar y evaluar el nivel de madurez de seguridad informática en el área de redes de la Universidad Pedagógica y Tecnológica de Colombia (U.P.T.C) Tunja, basado en norma ISO 27001, con el fin de minimizar la pérdida de información y sugerir políticas para la gestión de la seguridad de la información de la universidad, con el propósito de mejorar la prestación del servicio con mayor eficiencia y calidad.

Para tal fin se usaron diversos métodos de recopilación documental, dentro de cuales se resalta la aplicación de encuestas al personal del área de redes de la universidad y la observación directa de los procesos administrativos, organizacionales, funcionales y de infraestructura tecnológica, se busca desarrollar una investigación donde se puedan analizar los componentes necesarios, para hallar el nivel de madurez de área de redes, y sugerir unos protocolo o políticas de seguridad de la información, con el propósito de minimizar la pérdida de información de la institución educativa objeto de estudio.

6.1. Estratificación de la organización. La estratificación de la organización permite reconocer de forma general, el nivel de complejidad estimado para realizar la implementación, del sistema de gestión de seguridad de la información (SGSI), independiente de la estratificación la organización debe utilizar la aproximación mediante la gestión del riesgo para identificar el conjunto de controles mínimos sugeridos aplicables para cada uno de ellos.

Para la identificación de estratificación del proyecto se tiene como marco de referencia el modelo de seguridad de la información planteado por la estrategia del Gobierno en Línea 2.0 descritos en el Anexo 3: titulado “Estratificación de Entidades".

[43] ECBTI-Cadena de formación en sistemas Líneas de investigación. Obtenido de https://academia.unad.edu.co/images/escuelas/ecbti/Investigaci%C3%B3n/Grupos_por_cadena_de_formaci%C3%B3n/Cadena_de_formaci%C3%B3n_en_sistemas.pdf.

El documento define la estratificación de las empresas en tres nivéleles: bajo, medio y alto[44], el valor para su clasificación se obtiene a partir de una evaluación los siguientes criterios: el costo o precio para su operatividad, la infraestructura tecnológica definida en el número total de computadores, los servicios con los que cuenta en línea y si el tamaño y finalmente la capacidad de la dependencia de sistemas[45].

Para identificar la estratificación de la institución educativa UPTC, se tomó como referencia el documento estandarizado diseñado por gobierno en línea 2.0 la cual puede encontrarse en el Anexo A de la presente monografía.

El formato de estratificación relacionado en el anexo A. se observa en el Cuadro 10, que se relaciona a continuación, este se observa diligenciado y desarrollado de acuerdo a la recolección de información desarrollada en la universidad y las respectivas respuestas suministradas en esta institución. Siguiendo con el protocolo de gobierno en línea se asignó el respectivo puntaje a cada una de ellas, luego los puntajes fueron sumados y así se obtuvo el valor de estratificación de la organización.

Cuadro. 10. Estratificación de la organización.

Parámetros de Evaluación	**Opciones De Respuesta**	**Puntos**	**Observación**
Presupuesto	Menos de 3,000 millones de pesos	3	Para el 2016: $2.350.309.196 Fuente: acuerdo. 039_2016 de la Organización
	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	Datos suministrados administrador de la red
	Entre 100 y 500 computadores		
	Más de 500 computadores		
Número de Servidores	Menos de 4 Servidores	3	Datos suministrados administrador de la red
	Entre 4 y 20 Servidores		
	Más de 20 Servidores		
Parámetros de Evaluación	**Opciones De Respuesta**	**Puntos**	**Observación**

Fuente: Autor

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

Cuadro 10. (Continuación).

Parámetros de Evaluación	Opciones De Respuesta	Puntos	Observación
Número Empleados de Tecnología	Menos de 6 empleados	2	Datos suministrados dirección de tecnología
	Entre 6 y 50 empleados		
	Más de 50 empleados		
Existencia y función del área de sistemas (tecnología).	No hay área de sistemas o tecnología como tal	3	Datos suministrados por la dirección de tecnología
	Área de tecnología enfocada en la operación del día a día, que cumple labores en su mayoría REACTIVAS		
	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.	3	Datos suministrados dirección de tecnología
Parámetros de Evaluación	**Opciones De Respuesta**	**Puntos**	**Observación**
Existencia y objeto de la WAN.	WAN pública (p.ej. Internet) con servicios ofrecidos al ciudadano. Puede o no haber desarrollos sofisticados de transaccionalidad.	3	Datos suministrados por la dirección de tecnología
	Lo anterior más la existencia de una WAN privada (no incluye VPN a través de Internet)		
Transaccionalidad en la WEB.	Solo ofrece servicios de consulta (páginas WEB estáticas y correo electrónico)	3	Datos suministrados por la dirección de tecnología. Aplicación web para el pago de créditos por PSE
	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		

Fuente: Autor

Cuadro 10. (Continuación).

Parámetros de Evaluación	Opciones De Respuesta	Puntos	Observación
Transaccionalidad en la WEB.	Solo ofrece servicios de consulta (páginas WEB estáticas y correo electrónico)	3	Datos suministrados por la dirección de tecnología. Aplicación web para el pago de créditos por PSE
	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	Datos suministrados por la dirección de tecnología.
	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		**22**	

Fuente: Autor

El puntaje obtenido de la estratificación de la organización, se logra a partir de la sumatoria de los puntajes independientes obtenidos en cada una de las preguntas del instrumento, para este caso el resultado fue igual a 22 puntos.

La estratificación de la organización, de acuerdo con las sumatoria de los puntajes individuales obtenido, se establece con base en los rangos de valores descritos en el Cuadro11.

Cuadro. 11. Rangos de Estratificación de Entidades. [46]

Rango De Puntos	Estrato
Menor a 10 puntos	**Bajo**
Entre 11 y 22 puntos	**Medio**
Mayor a 22 puntos	**Alto**

Fuente: Estratificación de Entidades - Modelo seguridad de la información para la estrategia de Gobierno en Línea 2.0, Pág. 12.

Con el puntaje obtenido por la organización, con valor numérico de 22 puntos, la organización se clasifica en un nivel MEDIO, esto indica que de forma primaria se requiere de un importante esfuerzo, para implementar de manera pertinente el Sistema de Gestión de Seguridad de la Información. Teniendo como base la información recolectada y analizada, se realizó los siguientes análisis.

El presupuesto de la entidad para el año 2016 fue aproximadamente de $2.350.309.196, según lo expuesto en el acuerdo 039 del 2016, lo que facilitaría a la organización contar con los recursos económicos necesarios para la implementación del sistema de gestión de seguridad de la información de acuerdo a lo establecido en la norma ISO/IEC 27001:2013[47] La capacidad de equipos de cómputo y servidores, con que cuenta la organización, implica un mayor esfuerzo para garantizar la seguridad de los activos de información. En ese sentido se deben implementar en el proceso la valoración de los riesgos, donde se pueda identificar los niveles de protección y los protocolos de seguridad para poder salvaguardar dichos datos. Establecer estos protocolos se hace necesario para dar cumplimiento con requisitos establecidos en los controles "6.1.2 Valoración de riesgos de seguridad de la información"[48] y 6.1.3 Tratamiento de riesgos de la seguridad de la información' [49] de la norma ISO/IEC 27001:2013.

El Cuadro de estratificación de la organización, refleja el tamaño de la Organización y el número de empleados con que cuenta el grupo de organización y sistemas de la universidad, por consiguiente, lo que implica atender los requerimientos de los usuarios tanto internos como externos de la organización y la prestación de los

[46] Anexo 3: Estratificación de Entidades - Modelo seguridad de la información para la estrategia de Gobierno en Línea 2.0, Pág. 12.
[47] Norma ISO/IEC 27001:2013, Pág. 4
[48] Ibíd., Pág. 4
[49] Ibíd., Pág. 4

servicios TIC, el recurso humano con que cuenta la organización de sistemas, puede no ser suficiente para cubrir las necesidades tecnológicas de la organización.

El área de organización y sistemas es la responsable de administrar, coordinar y evaluar las necesidades de las diferentes dependencias, es importante mencionar que esta área forma parte de la junta de compras de almacén, de igual forma debe planear, desarrollar e implementar proyectos TIC.

7 RESULTADOS Y DISCUSIÓN

7.1. Nivel de madurez del área de redes. Para poder evaluar y/o determinar el nivel de madurez de la seguridad del área de redes del grupo de organización y sistemas de organización, se analizaron los dominios que se muestran a continuación correspondientes a la ISO / IEC 27002: 2013:

- Política de seguridad
- Organización de la seguridad de la información
- Gestión de activos
- Seguridad física y ambiental
- Seguridad a los recursos humanos
- Control de acceso
- Gestión de comunicaciones y operaciones
- Gestión de incidentes
- Adquisición, desarrollo y mantenimiento de Sistemas de Información
- Cumplimiento.
- Gestión de continuidad de negocio

7.2. Revisión de los controles de ISO / IEC 27001. Se revisaron los 114 controles diseñados por ISO / IEC 27001, con los diferentes objetivos de control. En el cuadro se aparece a continuación se puede observar el Modelo de Madurez de la Capacidad (CMM), definido en el marco conceptual del documento, de igual forma se describirá la metodología para verificar que los diferentes controles de la ISO / IEC 27001 se cumplieron a cabalidad.

Cuadro. 12. Metodología para verificar el cumplimiento de los diferentes controles de la ISO / IEC 27001.

Efectividad	CMM	Significado	Descripción
Cero por ciento (0%)	**A0**	**Inexistente**	Completa ausencia de cualquier proceso reconocible. No existe el más mínimo conocimiento o afán por conocer que existe alguna problemática por resolver.
Diez por ciento (10%)	**A1**	**Inicial / Ad-hoc**	El triunfo de todas las actividades y los procesos la mayoría de veces es resultado del esfuerzo personal. En algunos casos no existen los procedimientos o se localizan en áreas concretas.

Fuente Autor

Cuadro12. (Continuación)

Efectividad	CMM	Significado	Descripción
Cincuenta por ciento (50%)	**A2**	**Reproducible, pero intuitivo**	Los procesos similares se llevan en forma similar por diferentes personas con la misma tarea. Las buenas prácticas son producto de los conocimientos adquiridos en la experiencia de situaciones presentadas en el pasado. Cada individuo tiene sus respectivas responsabilidades y solo él se encargará de darles el cumplimiento. Cada persona cuenta con conocimientos únicos, haciendo que se dependa de su grado de conocimiento.
Noventa por ciento (90%)	**A3**	**Proceso definido**	Este es un proceso conjunto, es decir toda la organización participa en su desarrollo. Los procesos están implantados, documentados y comunicados por medio de una respectiva preparación.
Noventa y cinco por ciento (95%)	**A4**	**Gestionado y medible**	Se observa una evolución en los procesos, debido a que los indicadores son representados de manera numérica y estadística. La calidad y la eficiencia, se ven optimizados gracias a la disponibilidad de tecnología que ayuda a mejorar el flujo de trabajo.
Cien por ciento (100%)	**A5**	**Optimizado**	Se busca la excelencia y perfección en todos los procesos. Se determinan las desviaciones más comunes y se perfeccionan los procesos, basándose en los criterios cuantitativos.

Fuente: Autor

7.3. Evaluación del control de ISO / IEC 27001. Se evaluará el desempeño y alcance de los diferentes ítems de los controles de la norma, con los cuales se pretende identificará el nivel de cumplimiento del objeto de estudio, ítem a item, tomando como referencia la descripción de los controles que se encuentra en el cuadro a continuación:

Cuadro 13. Descripción de evaluación de los controles de ISO / IEC 27001.

Control	Objetivo a Evaluar de Cada Control
Política de seguridad	Objetivo: Proveer la orientación de gestión y soporte a la seguridad de la información tomando como base los requerimientos de la institución y la reglamentación vigente.
Organización de la seguridad de la información.	Objetivo 6.1: Construir un marco de gestión para emprender y vigilar la implementación y operación de seguridad de la información dentro de la institución. Objetivo 6.2: Asegurar las óptimas condiciones del teletrabajo y la implementación de dispositivos móviles.
(7) Seguridad de Recursos Humanos	Objetivo 7.1: Comprobar que el personal y los contratistas identifiquen y comprendan sus responsabilidades, y de igual manera verificar que son idóneos para dar cumplimiento a las funciones asignadas. Objetivo 7.2: Cerciorarse que tanto los empleados como los contratistas tienen pleno conocimiento y cumplan con sus responsabilidades de seguridad de la información. Objetivo 7.3: Salvaguardar los intereses de la institución, como parte del proceso de cambiar o finalizar el empleo.
Gestión de Activos	Objetivo 8.2: Confirmar que la información cuenta con protección de calidad de acuerdo al nivel de importancia para la organización. Objetivo 8.3: Evitar la transmisión no autorizada, el cambio, la anulación o destrucción de la información alojada en los medios de comunicación.
Control de Acceso	Objetivo 9.1: Restringir el acceso a las instalaciones encargadas del procesamiento de la información. Objetivo 9.2: Permitir el acceso oportuno de los usuarios autorizados y crear medidas de seguridad para restringir el acceso al sistemas y servicios, por parte de otras personas. Objetivo 9.3: Crear conciencia y responsabilidad en los usuarios respecto a la importancia de manejar la información de ingreso y autenticación de manera segura. Objetivo 9.4: Evitar el acceso no autorizado a los sistemas y aplicaciones propios de la organización.
Criptografía	Objetivo 10.1: Asegurar el uso correcto y efectivo de la criptografía para salvaguardar la confidencialidad, la autenticidad y / o integridad de la información.

Fuente: Autor

Cuadro13. (Continuación).

Control	Objetivo a Evaluar de Cada Control
Seguridad física y ambiental	Objetivo 11.1: Restringir el acceso a personal externo a la institución, a efectuar arreglos locativos a la infraestructura físicas que puedan ocasionar daños y obstrucción a la información y procesamiento de la misma sobre las instalaciones de la organización. Objetivo 11.2: Disminuir los riesgos de la pérdida, daño, robo o el compromiso de los activos y la obstrucción de las actividades que se llevan a cabo en la organización.
Operaciones de seguridad	Objetivo 12.1: Garantizar que las operaciones de instalación de procesamiento de información se realicen de manera correctas y seguras. Objetivo 12.2: Asegurar que tanto la información como su procesamiento se encuentran protegidos contra el malware. Objetivo 12.3: Disminuir los riesgos de pérdida de datos. Objetivo 12.4: Registrar todas las actividades y a su generar evidencia de todos los procesos. Objetivo 12.5: Garantizar la integridad de los sistemas operativos. Objetivo 12.6: Evitar la utilización de las vulnerabilidades técnicas. Objetivo 12.7: Reducir el impacto que generan las actividades de auditoría en los sistemas operativos.
Seguridad de las Comunicaciones	Objetivo 13.1: Garantizar el resguardo de la información en los espacios óptimos como las redes y sus instalaciones de apoyo de procesamiento de información. Objetivo 13.2: Conservar la seguridad de la información transferida de manera interna en la organización y con otras instituciones.
Sistema de adquisición, desarrollo y mantenimiento	Objetivo 14.1: Cerciorarse que la seguridad informática es una parte importante de los sistemas de información a través de todo el ciclo de vida. Esto también incluye los requisitos para los sistemas de información que suministran los servicios a través de redes públicas. Objetivo 14.2: Garantizar la seguridad de la información que se diseña e implementa dentro del ciclo de vida de desarrollo de sistemas de información.
Relaciones con los proveedores	Objetivo 15.1: Garantizar la protección y respaldo de los activos con los que cuenta la organización. Objetivo 15.2: Conservar un nivel adecuado de seguridad.

Fuente: Autor

Cuadro13. (Continuación).

Control	Objetivo a Evaluar de Cada Control
Información de gestión de incidentes de seguridad	Objetivo 16.1: Contar con un enfoque coherente y eficaz a la hora de gestionar los incidentes de seguridad de la información, incluyendo aquellos relacionados con la comunicación en los eventos de seguridad.
Los Aspectos de Seguridad de Información de la Gestión de la Continuidad del Negocio	Objetivo 17.2: Garantizar la disponibilidad permanente de instalaciones de procesamiento de la información.
Conformidad	Objetivo 18.1: Cumplir a cabalidad con las obligaciones legales, estatutarias o contractuales, referentes a las exigencias en la seguridad de la información. Objetivo 18.2: Garantizar que la seguridad de la información que se implementa está bajo los estándares de las políticas y procedimientos de la organización

Fuente: Autor

7.4. Cumplimiento de los controles ISO / IEC 27002: 2013. Mediante el análisis del cumplimiento de los controles de ISO / IEC 27002: 2013, con los valores de efectividad y el valor CMM estimado para cada uno de los controles, se determinará el nivel de madurez del área de redes de la universidad.

Cuadro. 14. Análisis del Cumplimiento de la norma ISO / IEC 27002: 2013.

CONTROL		Efectividad	CMM
5. POLITICA DE SEGURIDAD			
5.1 Dirección de la gestión de seguridad de la información.			
5.1.1	Políticas de la seguridad de la información	50%	A2
5.1.2	Revisión de las políticas de la seguridad de la información.	50%	A2
6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION			
6.1 Organización de la seguridad de la información.			
6.1.1	Funciones y compromisos de seguridad de información.	50%	A2

Fuente: Autor

Cuadro 14. (Continuación).

CONTROL		Efectividad	CMM
6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION			
6.1 Organización de la seguridad de la información.			
6.1.2	División y clasificación de las funciones.	50%	A2
6.1.3	Reunión con las autoridades.	10%	A1
6.1.4	Acercamiento con grupos de especial interés.	0%	A0
6.1.5	Seguridad de la información en la gestión y ejecución de proyectos.	10%	A1
6.2 Dispositivos móviles y teletrabajo			
6.2.1	Políticas de dispositivos móviles.	NA	
6.2.2	Teletrabajo	NA	
7. SEGURIDAD DE RECURSOS HUMANOS			
7.1 Antes de empleo.			
7.1.1	*Screening*	NA	
7.1.2	Términos y condiciones de empleo	NA	
7.2 Durante el empleo.			
7.2.1	Compromisos de gestión	20%	A1
7.2.2	Conocimiento de seguridad de la información y capacitación.	50%	A2
7.2.3	Procedimiento disciplinario	10%	A0
CONTROL		**Efectividad**	**CMM**
7.3 Terminación y cambio de empleo.			
7.3.1	Finalización o cambio de las obligaciones de empleo	90%	A3
8. GESTION DE ACTIVOS			
8.1 Responsabilidad de los activos			
8.1.1	Categorización de la información	60%	A2
8.1.2	Rotulado de la información	50%	A2
8.1.3	Administración de activos	50%	A2
8.2 Clasificación de la Información			
8.2.1	Lista de activos	95%	A4
8.2.2	Pertenencia de los activos	90%	A3
8.2.3	Retoma de los activos	90%	A3
8.3 Manejo de Medios			
8.3.1	Gestión de medios extraíbles	60%	A2
8.3.2	Exclusión de medios	60%	A2
8.3.3	Transferencia de medios físicos	60%	A2

Fuente: Autor

Cuadro 14. (Continuación).

CONTROL		Efectividad	CMM
9. CONTROL DE ACCESO			
9.1 *Business Requirements of Access control*			
9.1.1	Política de vigilancia de acceso	90%	A3
9.1.2	Acceso a las redes y servicios de red	90%	A3
9.2 Gestión de acceso de usuario			
9.2.1	Registro de usuario y anulación de registro	90%	A3
9.2.2	Acceso acumulado de usuario	90%	A3
9.2.3	Gestión de derechos de accesos privilegiados	90%	A3
9.2.4	Gestión de la información de autenticación secreta de los usuarios	90%	A3
9.2.5	Verificación de los derechos de ingreso de usuario	90%	A3
9.2.6	Exclusión o corrección de los derechos de acceso	90%	A3
9.3 Responsabilidades del usuario			
9.3.1	Uso de información confidencial de autenticación	90%	A3
9.4 Control de sistemas y acceso a las aplicaciones			
9.4.1	Limitación del acceso a la información	90%	A3
9.4.2	Modo de inicio de sesión seguro	95%	A4
9.4.3	Sistema de gestión de contraseñas	90%	A3
9.4.4	Aplicación de programas de servicios públicos privilegiados	NA	
9.4.5	Control de ingreso al código fuente del programa	NA	
10. CRIPTOGRAFIA			
10.1 Controles criptográficos			
10.1.1	Políticas relacionadas con el control criptográfico	50%	A2
10.1.2	Gestión de Claves	NA	
11 SEGURIDAD FISICA Y AMBIENTAL			
11.1 Áreas seguras			
11.1.1	Perímetro de seguridad física	90%	A3
11.1.2	Controles de ingreso físico	90%	A3
11.1.3	Certificar oficinas habitaciones e instalaciones	90%	A3
11.1.4	Defensa contra amenazas tanto como ambientales	60%	A2
11.1.5	Laborar en lugares seguros	90%	A3
11.1.6	Zonas especiales de entrega y carga	90%	A3
11.2 Equipo			
11.2.1	Ubicación y defensa del equipo	50%	A2
11.2.2	Soporte a los servicios públicos	10%.	A1

Fuente: autor

Cuadro 14. (Continuación).

CONTROL		Efectividad	CMM
11.2 Equipo			
11.2.3	Seguridad de cableado	90%	A3
11.2.4	Revisión y preparación constante de los equipos	90%	A3
11.2.5	Eliminación de los activos	90%	A3
11.2.6	Seguridad de equipo y activos cuando se encuentran fuera de las instalaciones	NA	
11.2.7	Anulación segura o reutilización de los equipos	60%	A2
11.2.8	Equipos de usuario desatendidos	NA	
11.2.9	Área de trabajo limpia (escritorio y pantalla del pc)	50%	A2
12 OPERACIONES DE SEGURIDAD			
12.1 Procedimientos y responsabilidades operacionales			
12.1.1	Instrucciones de operativos documentales	70%	A2
12.1.2	Gestión del cambio	70%	A2
12.1.3	Gestión de la capacidad.	50%	A2
12.1.4	Separación de desarrollo, pruebas y entornos operativos	50%	A2
122 Protección contra el malware			
12.2.1	Inspecciones contra el malware	70%	A2
12.3 Copias de seguridad			
12.3.1	Backups de la información	100%	A5
12.4 Registro y seguimiento			
12.4.1	Reporte de eventos	60%	A2
12.4.2	Respaldo de la información de los registros	60%	A2
12.4.3	Registros de dirección y operación	60%	A2
12.4.4	Sincronización del reloj	90%	A3
12.5 Control del software operativo			
12.5.1	Soporte a los servicios públicos	NA	
12.6 Técnico de gestión de vulnerabilidades			
12.6.1	Gestión de vulnerabilidades técnicas	90%	A3
12.6.2	Limitaciones de instalación de software	90%	A3
12.7 Sistemas de la información consideraciones de auditoria			
12.7.1	Sistemas de información inspecciones de auditoria	90%	A3
13. SEGURIDAD DE LAS C0MUNICACIONES			
13.1 Gestión de la Seguridad de Red			
13.1.1	Ocupaciones y obligaciones de seguridad de información.	90%	A3
13.1.2	Separación de funciones.	90%	A3
13.1.3	División en Redes.	90%	A3

Fuente: autor

Cuadro 14. (Continuación).

CONTROL		Efectividad	CMM
13. SEGURIDAD DE LAS C0MUNICACIONES			
13.2 Transferencia de Información			
13.2.1	Políticas y procedimientos de transmisión de información	80%	A2
13.2.2	Convenios sobre la transmisión de información	80%	A2
13.2.3	Mensajería electrónica	80%	A2
13.2.4	Pactos de reserva o de no divulgación	70%	A2
14 SISTEMA DE ADQUISICION, DE SARROLLO Y MANTENIMIENTO			
14.1 Requerimientos de seguridad de los sistemas de información			
14.1.1	Información de análisis de requerimientos de seguridad y su especificación	80%	A2
14.1.2	Certificar los servicios de aplicaciones en las redes publicas	80%	A2
14.1.3	Protección de las transacciones de servicios de aplicaciones	80%	A2
14.2 Seguridad en los procesos de desarrollo y de apoyo			
14.2.1	Política de desarrollo seguro	NA	
14.2.2	Procedimientos de revisión de cambio del sistema	NA	
14.2.3	Revisión técnica de las aplicaciones tras efectuar mejoras en la plataforma operativo	NA	
14.2.4	Restringir los cambios de los paquetes de software	NA	
14.2.5	Principios de ingeniería de sistemas seguros	NA	
14.2.6	Ambiente de desarrollo seguro	NA	
14.2.7	Desarrollo *Outsourcing*	NA	
14.2.8	Pruebas de seguridad del sistema	NA	
14.2.9	Pruebas de aprobación del sistema	NA	
14.3 Datos de prueba			
14.3.1	Protección de datos de prueba	NA	
15.RELACION CON PROVEEDORES			
15.1 Segundad en la información en las relaciones con proveedora			
15.1.1	Política de seguridad dé la información para relaciones con los proveedores	60%	A2
15.1.2	Abordar la seguridad a partir de los acuerdos con proveedores	100%	A5
15.1.3	Cadena de la información y tecnología de comunicación de abastecimiento	NA	
15.2 Gestión de la prestación de servicios de proveedores			
15.2.1	Política de mejora segura	NA	
15.2.2	Procedimientos de control de cambio del sistema	NA	

Fuente: autor

Cuadro 14 (Continuación).

CONTROL		Efectividad	CMM
16. INFORMACIÓN DE GESTIÓN DE INCIDENCIAS DE SEGURIDAD			
16.1 Gestión de incidencias de seguridad de la información y mejo			
16.1.1	Compromisos y procedimientos	90%	A3
16.1.2	Presentación de informes de programas de seguridad de información	90%	A3
16.1.3	Informes de las falencias de seguridad de información	50%	A2
16.1.4	Valoración y decisión sobre las actividades de seguridad de información	50%	A2
16.1.5	Respuestas a casos problemas de seguridad de la información	50%	A2
16.1.6	Aprendiendo de las dificultades presentadas en la seguridad de la información	10%	A1
16.1.7	Provisión de pruebas	0%	A0
17. ASPECTOS DE SEGURIDAD DE INFORMACIÓN DE LA GESTIÓN			
17.1 Información continuidad seguridad			
17.1.1	Planificación información continuidad seguridad	NA	
17.1.2	Implementación de la información, su continuidad y la seguridad	NA	
17.1.3	Confirmar, revisar y valorar la información de seguridad y continuidad	NA	
17.2 Redundancias			
17.2.1	Disponibilidad de instalaciones encargadas del procesamiento de información	90%	A3
18. CONFORMIDAD			
18.1 Cumplimiento de los requisitos legales y contractuales			
18.1.1	Reconocer la legislación aplicable y aquellos requisitos contractuales	90%	A3
18.1.2	Derechos de propiedad intelectual	90%	A3
18.1.3	Amparo de los registros	90%	A3
18.1.4	Confidencialidad y aseguramiento de datos personales	90%	A3
18.1.5	Reglamento de los controles criptográficos	70%	A2
18.2 Revisiones de seguridad de información			
18.2.1	Revisión independiente de seguridad de la información	NA	
18.2.2	Acatamiento de las políticas y modelos de seguridad	90%	A3
18.2.3	Revisión del alcance técnico	90%	A3

Fuente: autor.

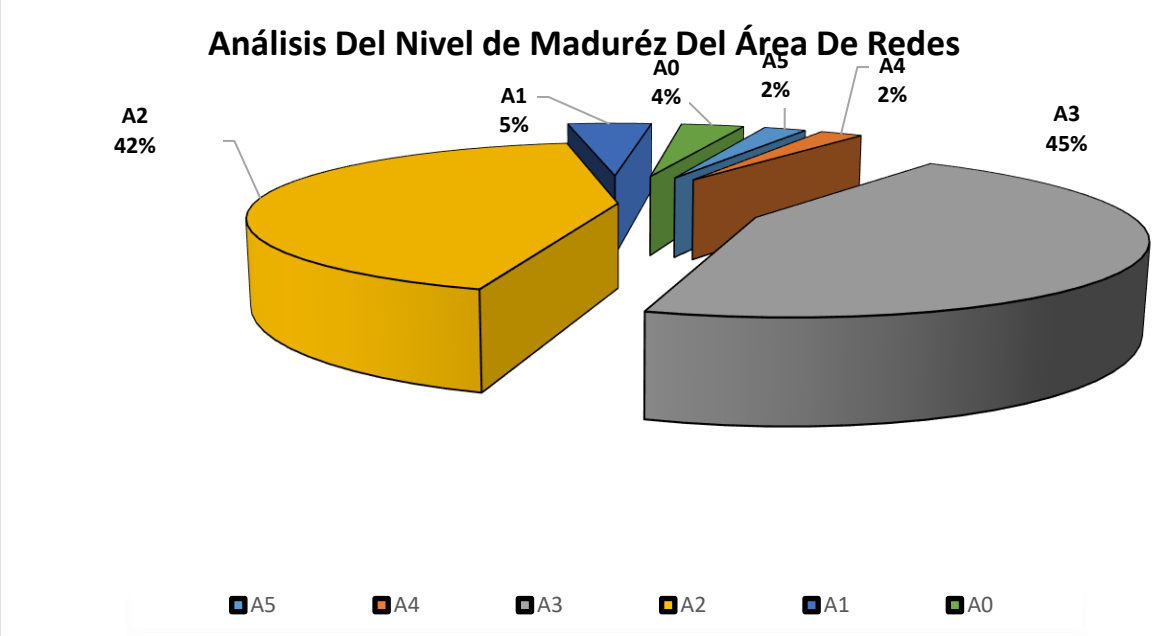
7.5 Resultados del nivel de madurez del área de redes. Mediante el análisis de los valores recolectados en el Cuadro que se presenta a continuación de la aplicación de comprobación de la norma ISO / IEC 27001: 2013, como resultado determinara el porcentaje del nivel de madurez del área de redes de la organización.

Cuadro. 15. Resultados del nivel de madurez del área de redes.

Nivel de madurez	Total, de CMM% por nivel
Nivel de madurez del nivel A0	4%
Nivel de madurez del nivel A1	5%
Nivel de madurez del nivel A2	42%
Nivel de madurez del nivel A3	45%
Nivel de madurez del nivel A4	2%
Nivel de madurez del nivel A5	1%

Fuente: Autor

Figura. 16. Análisis grafico del porcentaje del Nivel de Madurez del área de redes de la organización



Fuente: autor

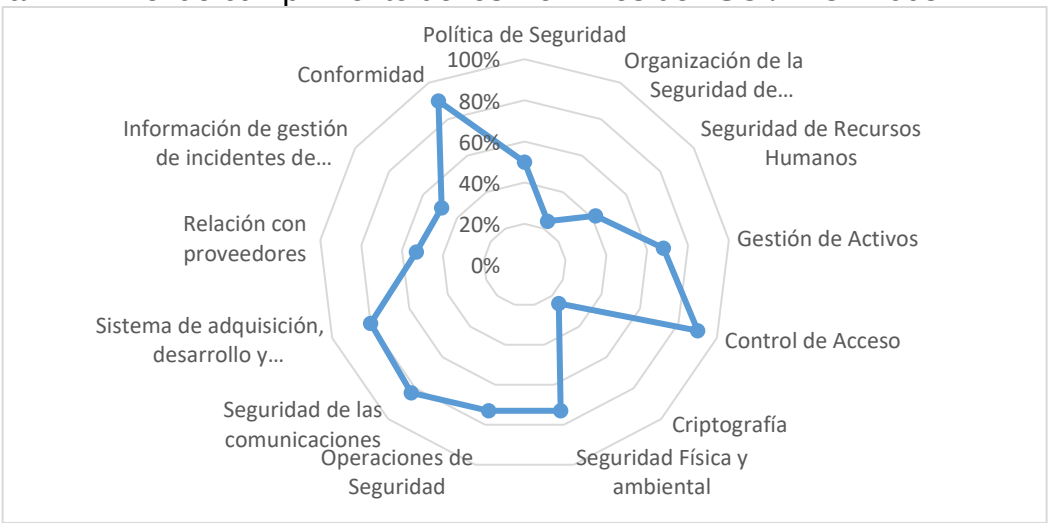
7.6. Nivel de cumplimiento. Mediante el uso del diagrama de radar, como se muestra en la Figura 18. Se puede tener una visión más detallada del análisis del nivel de cumplimiento en cada uno de los capítulos tratados en los dominios de la norma ISO / IEC 27003, en donde los niveles que se esperan, deberían ser los más aproximados al 100% de desempeño.

Cuadro. 16. Nivel de cumplimiento de los Dominios del ISO 2007/ IEC 27003.

Capítulos de los Dominios del ISO / IEC 27003		Nivel de Cumplimiento
5.	Política de Seguridad	**50 %**
6.	Organización de la Seguridad de Información	**24%**
7.	Seguridad de Recursos Humanos	**42%**
8.	Gestión de Activos	**68%**
9.	Control de Acceso	**90%**
10	Criptografía	**25%**
11.	Seguridad Física y ambiental	**73%**
12.	Operaciones de Seguridad	**73%**
13.	Seguridad de las comunicaciones	**83%**
14.	Sistema de adquisición, desarrollo y mantenimiento	**80%**
15.	Relación con proveedores	**53%**
16.	Información de gestión de incidentes de seguridad	**49%**
18.	Conformidad	**90%**

Fuente Autor

Figura. 17. Nivel de cumplimiento de los Dominios del ISO / IEC 27003



Fuente Autor

Se observa en el Cuadro16 y en la Figura. 17. Que todos los controles del área de redes de la organización excepto (Organización de la Seguridad de Información, Seguridad de Recursos Humanos y Criptografía), están por encima del 50%, y es de recalcar que los controles (Control de Acceso y Conformidad) cuenta con un 90%, lo que evidencia un trabajo importante por cuenta del grupo de seguridad de la información.

7.7. Modelo sugerido. Uno de los objetivos del desarrollo de este proyecto es sugerir un modelo de seguridad al área redes de la Universidad, esto con el objetivo de disminuir el riesgo de la pérdida de información de la universidad. Para lograr, desarrollar e implementar cualquier modelo de seguridad, como primera estrategia es contar con el soporte de la alta dirección o alta gerencia, en este caso más exactamente en el año 2011, se incluyó el Proyecto "Adopción de buenas prácticas bajo los estándares ISO 20000 e ISO 27001" dentro del Plan de Desarrollo de la Universidad Pedagógica y Tecnológica de Colombia; garantizando de esta manera tanto con el aval de alta calidad como con los diferentes recursos que permitirán llevar a cabo las actividades solicitadas para lograr la certificación con estas normas.[50]

Una vez se tiene el acompañamiento de la alta dirección para implementar o sugerir un modelo de seguridad, el segundo paso o estrategia es hacer el proceso de estratificación y análisis de madurez de la organización, este proceso se desarrolló con base a las normas de la familia ISO 27000 como: (ISO 27001:2005 y la ISO 27002:2005), la cual define unos controles, procesos y procedimientos mediante un listado detallado que garantiza la seguridad de la información.

El análisis del nivel de madurez de la organización busca planes para aportar en el fortalecimiento de los procesos y servicios que realiza la Oficina del área de redes, mediante la sugerencia o recomendación de un modelo para manejar y mejorar los aspectos de seguridad, según el análisis de madurez evitar la pérdida de información.

Este modelo de seguridad de la información que se sugiere es implementar la norma ISO 27000 plantea de manera adecuada las buenas prácticas para realizar la gestión de un área de Tic, permitiendo adelantar actividades que aseguren la información, a su vez implementen y/o ajusten los protocolos de seguridad mencionados y establecer la política de seguridad para apoyar la gestión de los peligros informáticos identificados por la organización y dar la debida seguridad a la información que circula por el área de redes de la organización.

[50] Estrategias Para La Implementación de ISO 20000 E ISO 27001 En Una Universidad Pública Colombiana. Plata. Diana. junio 2013

7.8. Definir las políticas para la gestión de la seguridad de la información.

Las políticas deben ser definidas por el grupo encargado de seguridad y avaladas por la alta gerencia de la organización, para tener el carácter institucional, se debe brindar capacitaciones y jornadas de sensibilización a todos los niveles de la organización acerca de la importancia de proteger la información, como los medios tecnológicos donde se guardan o reposa esta. Si no se cuenta con políticas adecuadas donde se definan los usos adecuados de las herramientas de seguridad con las que cuenta la organización, existe la posibilidad de que estos tiendan a ser vulnerables.

Para que estas herramientas funcionen adecuadamente, es conveniente la creación de políticas para la generación, cambio, recuperación de claves y contraseñas, para el acceso a los sistemas de información, por parte del personal de la organización, contribuyendo a que los empleados utilicen únicamente aquellos archivos necesarios para el cumplimiento de sus funciones diarias y permitan que las herramientas hagan su función con éxito.[51]

Objetivo: Identificar, evaluar y establecer los controles de propósito general, para proteger de forma apropiada la información de la universidad.

Aplicabilidad: Estas políticas van dirigidas, a todos los funcionarios, docentes, estudiantes, y en general a todos los usuarios (directos e indirectos), de la Universidad

Directrices:

- Definir, Implementar, verificar y actualizar las políticas de seguridad.
- La organización debe implementar o mejorar los dispositivos utilizados para la seguridad perimetral, y para la conexión a Internet.
- Todo el software utilizado al interior en la universidad (en la parte administrativa, como en la parte académica), debe ser aprobado por el área de redes, según las políticas y necesidades de la Universidad.
- Todos los jefes administrativos o jefes de área deben velar con absoluta responsabilidad, por el acatamiento de las políticas y estándares de seguridad de la información de la universidad.
- Definir protocolos para transferencia de archivos con organizaciones externas y coordinar las políticas y controles de seguridad de la información a seguir con estas entidades, según las políticas institucionales.
- El comité de seguridad de la organización debe clasificar la información, para facilitar la creación de reglas, implementar monitoreos (dispositivos a emplear, gestión de claves, políticas para el uso de sistemas de cifrado de datos).

[51] http://es.slideshare.net/luisrobles17/modelos-de-seguridad-de-la-informacin

7.8.1. Política para el manejo de la información. Esta política tiene como finalidad establecer las directrices para proteger la información contra uso no autorizado, divulgación, publicación, modificación, daño o pérdida de la información de la organización.

- **Acuerdos de Confidencialidad:** Los trabajadores (funcionarios y/o contratistas) de la universidad deben firmar un acta de compromiso de reserva de información al instante de legalizar su contrato laboral, donde se comprometen a no divulgar, usar y/o explotar la información institucional.
- Los proveedores de la universidad que requieran tener acceso a la información institucional, deberán firmar un acta de compromiso de confidencialidad. En caso de negarse el proveedor a la firma de éste, no se contará con los permisos para obtener la información solicitada.
- Propietario de la Información: Todos los empleados de la organización independiente de su forma de vinculación laboral, que generen: (artículos, revistas, contenidos de cursos, videos, fotos, información académica, sistemas de información entre otros), la organización es propietaria de los derechos de esta información.
- Derechos de Autor: La legislación colombiana y la organización prohíbe sacar copias no autorizadas de la información institucional. No se realizará copias de seguridad de software que no le esté permitido (sea adquirido o desarrollado por la organización).
- Publicaciones de Seguridad de la Información: Se deben aplicar las directrices publicadas y comunicadas en las diferentes campañas y capacitaciones institucionales ofrecidas a todos los usuarios de servicios de tecnologías de Información.
- El correo electrónico debe utilizarse únicamente para el cumplir con el desarrollo de las funciones asignadas dentro de la organización, de igual forma se podrá utilizar para el uso personal, siempre y cuando se utilice de forma responsable y ética, evitando poner en peligro la información de la organización, ni su productividad.
- Los funcionarios de la universidad deben guardar reserva total de la información de la Institución, es decir debe ser confidencial toda aquella información a la que tengan acceso para poder desempeñar su labor.
- Los mensajes enviados deberán contener tanto el formato de la imagen corporativa definido por universidad como el mensaje legal corporativo de confidencialidad.
- Es obligación de todos los funcionarios verificar la identidad de las personas (jurídicas o naturales), antes notificarlas o de entregar información por: cualquiera de estos medios fax, teléfono, correo electrónico, correo certificado, entre otros.

- Equipos de procesamiento de datos tipo servidor: Los administradores de los servidores y bases de datos que manejen información clasificada, deben garantizar la confidencialidad de la información y el uso de credenciales de administración (usuario y contraseña), sin excepción. La administración de los equipos de procesamiento de datos tipo servidor que soportan los servicios institucionales debe ser realizada por personal del Grupo Organización y Sistemas de la organización.

7.8.2. Políticas de uso de recursos tecnológicos.

- Instalación, Mantenimiento y Actualización de recursos tecnológicos: Solo el personal del área de redes es el autorizado para instalar y actualizar aplicaciones de software, como de hacer los mantenimientos preventivos y correctivos en los equipos.
- Uso de los recursos tecnológicos: los recursos de la organización como:(servidores, portátiles, computadores, tablas, impresoras, videobeam, equipos de video conferencia entre otros), el personal autorizado es el único que puede dar uso de estos recursos, para desarrollar sus funciones y las actividades asignadas.
- Todos los empleados (funcionarios, contratistas y/o docente) de la universidad serán responsables de los recursos tecnológicos fijados para el cumplimiento de sus funciones, y serán incluido a su inventario personal, de acuerdo con los procesos y procedimientos de egreso de bienes y suministros del almacén.
- Los recursos tecnológicos móviles como: (celulares, video cámaras, portátiles, Tablets, entre otros) propiedad de la universidad, son responsabilidad exclusiva del usuario y deberá tomar las medidas de seguridad necesarias, que le permitan garantizar la integridad y confidencialidad de la información.
- Artículos de decoración en los recursos tecnológicos: todos los recursos propiedad de la organización se deben mantener libres de fotos, calcomanías y cualquier otro elemento que lo pueda deteriorar o comprometer su integridad.
- Software en los recursos tecnológicos: En todos los recursos tecnológicos de la organización, se instalará solo el software que cuente con licencia legales. El software que no cuente con licencia se debe desinstalar de manera inmediata.
- Antivirus: Todos los recursos tecnológicos de la universidad (celulares, computadores, portátiles, Tablets, entre otros), se les instalará única y exclusivamente el software antivirus autorizado y aprobado por el área de redes.
- Todos los usuarios que realizan labores de escaneo o digitalización de archivos, cada uno de ellos debe tener claro que no está permitido cambiar o alterar la configuración del antivirus de equipo.
- Los funcionarios y empleados no pueden descargar archivos adjuntos que procedan de fuentes desconocidas, para garantizar que no se instalara software malicioso o contenga virus informáticos.
- Aplicaciones de Ofimática: Los equipos de cómputo pertenecientes de la universidad solo se permitirá la suite de ofimática versiones de Microsoft Office

licenciadas, para Windows y Mac, y el uso de las versiones libres de ofimática Open Office.

- Sistemas de información de entes de control: Es responsabilidad del ente de control, el licenciamiento de los sistemas de información por donde se reporta información.
- Acceso a Código Fuente de Aplicaciones: Se prohíbe manipular el código fuente de las aplicaciones desarrolladas por la universidad, sin el consentimiento, la autorización y el debido acompañamiento del Grupo Organización y Sistemas, para generar cambios o mejoras a la misma. De igual forma las aplicaciones desarrollas por los proveedores externos, quedan sujetas a la revisión de las condiciones del contrato.
- Gestión de Cambios: Todos los cambios que se realicen a los recursos tecnológicos de la organización, deben quedar documentados bajo los lineamientos estipulados en la gestión de modificaciones y entregas.
- Monitoreo de los recursos tecnológicos: La universidad se reserva el derecho de monitorear los recursos tecnológicos, que se encuentren acoplados a la red de datos de la organización.
- La Organización dispone de un Data Center, que satisfacen con todos los requisitos vigentes para el alojamiento de los equipos de procesamiento de datos tipo servidor.
- El área de redes de la organización anualmente realiza un plan de mantenimiento preventivo y correctivo con el objetivo de garantizar la integridad, disponibilidad y confidencialidad de los activos de información que se encuentran allí alojados.
- La instalación y/o modernización de un nuevo elemento en la red de datos debe ser autorizada y supervisada por la Coordinación del Grupo Organización y Sistemas.
- La adopción, actualización y uso de tecnologías de la información y la comunicación orientadas a la gestión de servicios institucionales, serán aprobados por el Grupo Organización y Sistemas.

7.8.3. Políticas de Acceso remoto. La presente política va dirigida al uso de las comunicaciones electrónicas y conexiones remotas de usuarios con permisos de ingreso a los servicios de la red de datos de la organización.

- El Servicio de acceso remoto permite el ingreso a la red de datos, a los usuarios externos e internos, expresamente autorizados por el área de redes, el acceso a la conexión desde una red interna o externa, están sujetas a la autenticación con un nivel adecuado de protección.
- Para el servicio de accesos remoto se realizará la conexión solo con los equipos tipo servidor y de comunicaciones. Para la conexión de acceso remoto con los

equipos tipo cliente quedan sujetos a la previa autorización e identificaciones de los mismos

7.8.4. Políticas de escritorios y pantallas limpias. Esta política se implementa a la hora de proteger la información institucional, ya sea en medio físico o digital, y que pueden estar localizada en diferentes lugares como lo son las estaciones de trabajo, el escritorio, los computadores portátiles, en medios magnéticos, documentos en físicos (papel) y en general cualquier tipo de información que se utiliza para apoyar la realización de las actividades laborales.

El objetivo de esta política es reducir al máximo las amenazas de acceso no autorizado, pérdida o daño a la información dentro y fuera de las horas laborales.

- Todas las terminales de trabajo de la organización deben usar el papel tapiz Institucional y el protector de pantalla corporativo, deben contar con bloqueo de sesión automática después de tres minutos de inactividad, el cual, debe mostrar la pantalla de inicio de sesión solicitando el ingreso del usuario y contraseña para su ingreso de nuevo.
- Cuando se imprime información sensible o confidencial de la universidad, se debe retirar de inmediato de la impresora.
- La información que se considere de suma importancia de la organización almacenada en los equipos y/o sistemas de información, no debe estar ubicada en el escritorio o ser de fácil acceso.
- Todo usuario que se ausente de su lugar de trabajo, deberá bloquear su equipo de trabajo o computador portátil, para proteger el acceso a la información, a las herramientas y servicios de la institución de los empleados no autorizado o ajeno a la dependencia.
- En los escritorios de los equipos de trabajo o computador portátil, no deben tener accesos directos a los archivos de información.
- Los usuarios de las estaciones de trabajo o computadores portátiles, al terminar su jornada laboral, debe asegurarse de cerrar la sesión y apagar los equipos de cómputo en su totalidad, no solo la pantalla.
- Al finalizar la jornada de laboral, el usuario debe almacenar o guardar en un lugar seguro los documentos físicos, medios y los dispositivos que contengan información confidencial o de uso interno.
- No se deben realizar publicaciones, divulgaciones, ni dejar de fácil acceso satos como contraseñas y nombres de usuario, Números de cuenta, aquellos datos de personas que tienen alguna relación de tipo laboral, contractual, académica, entre otras con la organización y Propiedad intelectual. (información de carácter contractual o legal).

7.8.5. Política de retención y archivo de datos. Esta política tiene como propósito: Conservar la integridad, garantizando la disponibilidad, los servicios y el tratamiento de la información.

Directrices:

- Implementar políticas y diseñar tablas de retención y conservación de los archivos, para establecer que tiempo deben permanecer almacenada la información de la organización.
- Reglamentar e Implementar políticas de archivística, según los lineamientos definidos por la ley 594 del 2000 de archivística nacional, y las políticas institucionales.
- Utilizar sistemas de información para la administración, conservación de archivos e implantar programas de gestión de documental.

7.8.6. Política de respaldo y restauración de información. El objetivo de esta política es garantizar la seguridad, la integridad y confiabilidad de la información de (bases de datos, sistemas de información y el software), en caso de sufrir fallas y/o pérdida de información, mediante la implementación e instalación de sistemas de respaldo.

Directrices:

- Se debe emplear medios magnéticos como: (cintas, CD, DVD.), para hacer copias periódicas de la información.
- El personal encargado de los servidores, los sistemas de información, las bases de datos y los equipos de comunicaciones (administradores), serán los encargados de definir la periodicidad, para hacer las copias de respaldo y los requerimientos o necesidades técnicas y de seguridad para hacer las mismas.
- El objetivo de sacar las copias de respaldo es el de restituir el sistema en caso de que sufra algún de virus informático, defectos o daño total en los discos de acopio, dificultades de hardware y software en los servidores o en los computadores personales, catástrofes, fallas eléctricas y por requerimiento legal).
- El personal administrador o encargado de infraestructura deberá hacer semanalmente, un proceso de *backup* y verificar su correcto funcionamiento y ejecución de los procesos, como de suministrar los medios magnéticos requeridos para tal fin.

7.8.7. Política de gestión de activos de información. El propósito de esta política es plantear la forma como se va a salvaguardar adecuadamente los activos de información.

Directrices:

- Se conservará un inventario actualizado y centralizado de todos los activos de información, el cual estará asignado como una de las responsabilidades del personal propietario de la información y se enviará copia al jefe de redes.
- La información, los procesos propios de cada dependencia, los sistemas de información, las bases de datos, las aplicaciones, la infraestructura, la tecnología, de la información y comunicaciones (TIC) es responsabilidad del personal del grupo de organización y sistemas de la organización.

7.8.8. Política de uso de los activos. El propósito de esta política es salvaguardar todos los activos de información de la organización, mediante la asignación de responsabilidades al personal (docente, admirativo, estudiantes y usuarios en general), según el rol y las funciones que desempeñe en la universidad.

Directrices:

- Los activos de información son propiedad única y exclusivamente de la universidad y deben emplearse para tal fin.
- Se realizará una visita periódica a las diferentes dependencias de la universidad por parte del área de redes, para verificar si los programas utilizados e instalados son los autorizados y licenciados por la institución.
- El personal de la universidad deberá hacer un uso óptimo tanto de los recursos tecnológicos como de los sistemas de información.
- No se realizará Instalación software o programas en ningún equipo de la universidad, sin previa autorización del área de redes.
- Queda prohibido realizar modificaciones de hardware y software, en los equipos de cómputo o de comunicaciones de propiedad de la universidad, sin previa autorización del área de redes.
- Todas las acciones efectuadas desde la “cuenta de usuario”, es responsabilidad única y exclusiva del propietario de la cuenta.

7.8.9. Política de uso de Internet. El objetivo es garantizar la seguridad de la navegación y el buen uso de la red por parte del personal de la universidad y del público en general

Directrices:

- Implementar medidas y controles que garanticen la prestación y el uso razonable, eficiente y seguro del servició de internet.
- Se debe monitorear continuamente el canal de por el cual se tiene acceso al internet y el ingreso a la información consultada.
- Restringir la navegación y la descarga de aplicaciones que representen peligro para la red y la información de la organización como (programas maliciosos, pornografía, música, juegos, terrorismo entre otros).

- Establecer mecanismos que permitan hacer seguimiento y generar reportes en tiempo real, del uso de la red por parte del personal y de usuarios en general.
- Para efectuar descargas de:(programas, archivos, videos, entre otros), por la red deben ser con propósitos institucionales, para evitar interferencias en el servicio de Internet o de la Intranet, por consiguiente, debe solicitar el permiso por correo electrónico institucional para tal fin al área de redes.

7.8.10. Política de uso de mensajería instantánea y redes sociales. El objetivo es garantizar la seguridad a la hora de utilizar servicios tales como el de mensajería instantánea y el de redes sociales, al personal de la universidad y al público en general

Directrices:

- El servicio de redes sociales solo estará autorizado y administrado por la oficina de comunicaciones.
- Toda información que sea publicada por las redes sociales como *Facebook®, Twitter®*, *YouTube® LinkedIn® o blogs*, entre otras, en un ambiente diferente al de la oficina de comunicaciones, no se considera institucional, y estarán fuera del alcance del grupo de redes, y de las políticas institucionales, por consiguiente, no se podrá garantizar su confiabilidad, integridad y disponibilidad

7.8.11. Política de uso de impresoras y del servicio de Impresión. El propósito es garantizar el servicio de impresión, con seguridad, calidad, velocidad y protección de la información.

Directrices:

- Las impresoras son de carácter institucional, para imprimir documentos de sus funciones o rol laboral.
- Es responsabilidad del personal del área de redes, capacitar al usuario de la universidad, sobre el uso adecuado, las técnicas y el funcionamiento de los equipos de escáner, impresión y fotocopiadora.
- Solo el personal del área de redes, o en su efecto el personal técnico contratado por la universidad es el único autorizado para efectuar labores tales como el mantenimiento y la reparación de las impresoras.

7.8.12. Políticas de seguridad física y del entorno.

- Todos los empleados (funcionarios, contratistas y/o docente) y estudiantes, que ingresan a las instalaciones de la universidad, deben hacer uso del Sistema de Control de Acceso mediante el uso del carnet o tarjeta de ingreso.
- Aquellas personas ajenas a la institución deben registrarse en la entrada de la universidad e informar a que dependencia se dirige.

- Únicamente ingresará a la data center los usuarios autorizado por la dirección del grupo organización y sistemas con los elementos necesarios para desarrollar sus labores.
- No se permiten las visitas al data center, las únicas visitas deben ser para llevar a cabo labores de mantenimiento o auditorias.
- Los empleados (funcionarios, contratistas y/o docente), no deben proporcionar información sobre la ubicación del datacenter, centros de cableado, o lugares críticos, como mecanismo de seguridad.
- El datacenter, los centros de cableado y los gabinetes deben estar siempre con las puertas cerradas y aseguradas.
- Todos los empleados (funcionarios, contratistas y/o docente), deben portar en un lugar visible el carnet de identificación (carnet universitario), durante el tiempo que permanezcan dentro de las instalaciones de la organización, y no prestarlo por ningún motivo.

7.8.13 Políticas de instalación de cableado. Esta política va dirigida a la planeación, diseño, construcción, instalación, administración, certificación y mantenimiento del cableado estructurado de la Institución, debe cumplir con todos los estándares, con el objetivo de dar cumplimento al principio de integridad, conservar la estética y la seguridad de las redes de telecomunicaciones de la universidad.

7.8.14. Políticas de seguridad del datacenter y centros de cableado. Esta política debe garantizar la protección y seguridad de la información en las redes, en los servidores y en la infraestructura tecnológica, por parte del personal de la universidad, como de los terceros que ingresan a estas instalaciones.

Directrices:

- Se prohíbe fumar, comer o beber; en las instalaciones del datacenter y los centros de cableado.
- Se prohíbe guardar en las instalaciones del datacenter y centro de cableado papelería o materiales con alto riesgo de incendio o propagación de fuego, se debe eliminar periódicamente estos materiales, y se debe conservar el orden y la limpieza del Data center y los centros de cableado
- Se prohíbe el ingreso de personal extraño al datacenter y centros de cableado, el personal externo a esta dependencia, debe estar autorizado por el área de redes. Y debe diligenciar la planilla de asignada para controlar tato el ingreso como la salida del personal.
- El control de ingreso del personal al datacenter y centros de cableado, se realizará mediante dispositivos electrónicos de control de acceso con autenticación (por huella, por tarjeta y control biométrico).

- El área de redes y la oficina de planeación, deberán garantizar a la universidad, que todos los equipos tecnológicos del datacenter y los centros de cableado deberán contar con U.P.S (sistema alterno de respaldo de energía).
- Deben estar provisto de señalización, elementos y equipos de emergencia, luces de emergencia y guías de evacuación, siguiendo la normatividad vigente de seguridad industrial y de salud ocupacional.
- El datacenter deben contar con pisos falsos, elaborados con materiales no combustibles.
- Deben estar acondicionados con sistemas de enfriamiento por aire acondicionado de precisión. Estos equipos deben ser redundantes para cuando este falle, se pueda continuar con la refrigeración, y no afecte los equipos tecnológicos del datacenter.
- el sistema de extinción de fuego y las alarmas de detección de humo, deben ser automáticos y deben estar conectados al sistema central.
- Los sistemas contra incendios (extintores deben estar cargados y no deben estar despresurizado), deben ser adecuados, y estar adecuadamente, ensayados y con la capacidad ideal para detener el fuego generado al interior.
- El cableado estructurado de la red debe estar certificado y cumplir con las normas y estándares internacionales.
- El mantenimiento preventivo y correctivo del datacenter y los centros de cableado, deben estar supervisados y debidamente autorizados por el personal del área de redes.

7.8.15. Políticas de seguridad de los Equipos. El proposito de esta política es garantizar la seguridad y la protección de la información en los equipos.

Directrices:

- Garantizar que el cableado estructurado cuente con una red de energía regulada para cada uno de los lugres de trabajo, permitiendo la conexión de equipos tales como computadores, pantallas y videobeam, las impresoras se deberán conectar a la red comercial no regulada.
- Seguridad del cableado: Los cables deben estar totalmente identificados y marquillados como lo exige la norma técnica y las políticas de redes de la universidad.
- Deben reposar en el área de redes y planeación, los planos de la red eléctrica comercial y red eléctrica regulada, como de la red lógica.

Mantenimiento de los Equipos:

- Se debe mantener contratos durante todo el año, realizar el mantenimiento preventivo y correctivo de los equipos en estados críticos.

- Programar mantenimientos preventivos y correctivos de los equipos críticos periódicamente, para evitar suspensiones no programadas del servicio y tener pérdida de información y de equipos.
- Los equipos tecnológicos lograran ser retirados de las instalaciones de la universidad, si cuentan con permiso de almacén y el visto bueno del área de redes.
- Para reasignar o retirar equipos de cómputo, se debe garantizar la eliminación total y definitiva de toda la información en la unidad de almacenamiento.

7.8.16. Política de uso de correo electrónico. El objetivo de esta es garantizar y garantizar la protección de la información, producto del intercambio de mensajes de comunicación entre la universidad y sus colaboradores**.**

Directrices:

- Definir políticas sobre el buen uso de correo electrónico lo que se considera apropiado e inapropiado y establecer lineamientos para dar un buen uso a esta herramienta institucional.
- Las cuentas de correo institucional pertenecen a la universidad y son asignadas al personal de la institución, que gocen de algún tipo de vinculación laboral o académica.
- El personal de la universidad es directamente responsable por la información que sea enviada desde sus respectivas cuentas de correo electrónico corporativo.
- El correo electrónico corporativo se debe emplear única y exclusivamente para enviar comunicaciones institucionales.
- Se prohíbe utilizar el correo institucional para el envío de materiales que no sean propios y de uso institucional (cadenas).
- Se prohíbe realizar envíos de correos masivos, con archivos adjuntos de gran tamaño debido a que pueden congestionar la red, se debe utilizar técnicas para reducir el peso del archivo adjunto.
- Los correos electrónicos de la organización deben contener el siguiente texto firma: *"El contenido de este mensaje y sus anexos son propiedad de la universidad, es únicamente para el uso del destinatario ya que puede contener información pública reservada o información pública clasificada (privada o semiprivada), las cuales no son de carácter público. Si usted no es el destinatario, se informa que cualquier uso, difusión, distribución o copiado de esta comunicación está prohibido. Cualquier revisión, retransmisión, diseminación o uso de este, así como cualquier acción que se tome respecto a la información contenida, por personas o entidades diferentes al propósito original de la misma, es ilegal."*

7.8.17. Política de control de acceso. Esta política tiene como principal propósito garantizar el acceso de forma segura y controlada a la información, de

forma física o de forma lógico, que reposa en la plataforma informática, así como el empleo de medios móviles.

Directrices:

- El seguimiento de acceso a los sistemas de información de la universidad, debe realizarse con ayuda de credenciales de acceso (Usuario y Contraseña), las cuales son de uso exclusivo e intransferible.
- La asignación de credenciales para el ingreso a los sistemas de información, para todos los empleados (funcionarios, contratistas y/o docentes), se harán de forma individual e intransferible de acuerdo al tipo de contrato laboral que se firme con la universidad.
- El acceso a las aplicaciones, herramientas, plataformas, servicios y/o a cualquier recurso de información de universidad, se hará con la cuenta de usuario y contraseña asignado por el área de redes de la universidad.
- El acceso a los equipos especializados como: (servidores, enrutadores, entre otros) conectado a la red de datos, este es controlado y administrado por el Grupo de Organización y Sistemas de la universidad.
- Cada persona que tenga un vínculo con la institución (docentes, administrativos, estudiantes), es responsable de todas las actividades llevadas a cabo con su identificación de usuario y contraseña.
- Está prohibido imprimir y colocar de forma visible, en el área de trabajo el usuario y contraseña, de tal forma que personas ajenas tenga acceso a la información.
- No se deben almacenar las contraseñas en ningún programa que sirva para tal fin.
- Las contraseñas deben estar compuesta al momento de su construcción de al menos ocho (8) caracteres. Estos caracteres deben ser caracteres alfabéticos, numéricos y símbolos o caracteres especiales.
- El usuario tiene la libertad de cambiar su contraseña cuantas veces quiera.
- En caso de tener conocimiento o sospecha que sus datos de ingreso al sistema son conocidos por otra persona, es obligación del usuario realizar el respectivo cambio de manera inmediata para proteger toda la información.
- La gestión de la contraseña asignada al usuario institucional, se realizará directamente por los usuarios a través del *portal* *http://miclave.uptc.edu.co* [52].
- Todos los usuarios que bloquee su cuenta debido a la superación del número máximo de intentos cinco (5), al ingresar a los sistemas de bases de datos de la universidad, debe reportarlo al grupo organización y sistemas, informando a que sistema de información, para restaurar y activar su usuario y contraseña.
- Cuando el fabricante proporciona (contraseñas por defecto), antes de poner en producción cualquier activo de información en la Institución se debe hacer cambio de clave

[52] http://miclave.uptc.edu.co/self/PasswordForgotten.do

7.8.18. Política de adquisición, desarrollo y mantenimiento de sistemas de información. El propósito es garantizar que la seguridad, integridad y confiabilidad, es parte fundamental de los sistemas de información.

Directrices:

- Desarrollar estrategias para analizar y asegurar la integridad y confiabilidad en todos los sistemas de información y aplicativos informáticos de la universidad.
- Toda nueva adquisición de hardware y software que se vayan, a instalar, configurar y enlazar a la plataforma tecnológica de la universidad, por parte cualquier dependencia o proyecto de la universidad, deberá ser autorizado, revisado y gestionado por el área de redes.
- La compra o adquisición de licencias legales, de uno o varios software o programa según las necesidades, permitirá a la universidad efectuar una copia de seguridad (a no ser que esté especificado de manera distinta), para ser empleada en caso de que el medio se averíe.
- El único personal autorizado para sacar copias de seguridad del software licenciado, será el del área de redes.
- El software suministrado por la universidad no puede ser compartido o suministrado a terceros.
- El software que se adquiera a través de los proyectos o programas, quedara como propiedad de la universidad.
- Se prohíbe la descarga, instalación y uso, de aplicaciones de entretenimiento (juegos, videos) en los computadores de la universidad.
- Se mostrarán para dar de baja el software bajo los lineamientos dados por la Entidad. [53]

[53] MANUAL DE LA POLÍTICA DE SEGURIDAD PARA LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - TICS Código: M-TI-01 Versión 06 Proceso asociado: Tecnologías de Información y Comunicaciones

8. CONCLUSIONES

- Analizadas la estructura organizacional y funcional del área de redes de la Universidad se identificaron los posibles problemas de seguridad de la información a los que están expuestos diariamente a falta de políticas de seguridad y capacitación del personal que allí se desempeña.

- En el mismo sentido, se logró identificar el nivel de madurez del área de redes, a través de la observación directa, entrevistas, encuestas y la aplicación del *Check list* o plantillas para la recolección y análisis de la información, referente al paso a paso de la norma ISO/IEC27001 siendo posible establecer la presencia de dominios de la norma con niveles de madurez muy bajos, por lo que se comprobó la necesidad de proponer al grupo encargado de la seguridad de la información, el establecimiento de políticas de mejoramiento para obtener un mejor nivel de madurez y a la vez mejores políticas de seguridad.

- Dados los análisis de madurez del área de redes de la universidad, se formularon una serie de políticas para mejorar la gestión de seguridad de la información con miras a crear cultura de protección a través de la concientización de la calidad que ostenta la información como activo importante de la entidad. Fue así como se construyó un documento que servirá de apoyo para mejorar continuamente y reorganizar los procesos, controles y salvaguardas de manera que se garantice de forma real, la integridad, confidencialidad y autenticidad de la información, con el propósito de obtener a mediano plazo, la certificación ISO/IEC 27001:2013

10. DIVULGACION

La presente monografía de proyecto de grado titulado “Nivel de Madurez de Seguridad en el Área de Redes de la Universidad Pedagógica y Tecnológica de Colombia (U.P.T.C) Tunja”, tendrá como único medio de divulgación el repositorio institucional de la Universidad Nacional Abierta y a Distancia UNAD, en donde quedará como referencia de consulta para las personas externas y estudiantes de la universidad de los diferentes programas académicos de pregrado y posgrado.

BIBLIOGRAFÍA

AGUILERA LOPEZ, purificación. Seguridad Informática y comunicaciones. España: Editex, 2010.240 p.

BELLO, Claudia, “Manual de Seguridad en Redes” {en línea}. {18 de marzo de 2017}. Disponible en:
< https://es.slideshare.net/csandovalrivera/manual-de-seguridad-en-redes >

CALDER, alán. Nueve claves para el éxito. Una visión general de la implementación de la norma NTC-ISO/IEC27001. Colombia: ICONTEC, 2008. 128 p.

CAMELO, Leonardo. Seguridad de la Información en Colombia. Marco Normativo (Normas y políticas) de un SGSI. {En línea}. {14 de octubre 2016]. Disponible en. <http://seguridadinformacioncolombia.blogspot.com.co/2010/02/marco-legal-de-seguridad-de-la.html >

COMUNIDAD INTERNACIONAL DE IMPLANTADORES DE ISO27000 DE ISO27001SECURITY.COM. Consejos de implantación y métricas de ISO/IEC 27001 y 27002. Traducido por www.iso27000.es. {En línea} Versión 1, 16 p. 2007. {14 de agosto 2016}. Disponible en:
<http://www.iso27000.es/download/ISO_27000_implementation_guidance_v1_Spanish.pdf>

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley Estatutaria de 2012. (17 octubre). Por la cual se dictan disposiciones generales para la protección de datos personales. {En línea}. Bogotá D.C. Alcaldía de Bogotá. 2012. {9 de septiembre 2015}. Disponible en: <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981>

COSTAS SANTOS, Jesús. Seguridad Informática. España: Rama, 2011. 308 p.

ECBTI. Cadena de formación en sistemas Líneas de investigación. {En línea}. Bogotá D.C. {9 de septiembre 2015}. Disponible en. <https://academia.unad.edu.co/images/escuelas/ecbti/Investigaci%C3%B3n/Grupos_por_cadena_de_formaci%C3%B3n/Cadena_de_formaci%C3%B3n_en_sistemas.pdf>

FERNÁNDEZ, Carlos. PIATTINI, Mario. Modelo para el Gobierno de las TIC basado en las normas ISO. Modelo para el Gobierno de las TIC basado en las normas ISO. Colombia: Aenor, 2012.

Gobierno en Línea, M. (21 de Noviembre de 2016). Anexo 3: Estratificación de Entidades. {en línea}. Disponible en: <http://css.mintic.gov.co/ap/geA4/images/SeguridaddelaInformacion2_0_Anexo3_Estratificacion.pdf >.

Guachi, T. (2012). Norma de Seguridad Informática ISO 27001 para mejorar la confidencialidad, integridad y disponibilidad de los sistemas de información y comunicación en el Departamento de Sistemas de la Cooperativa de Ahorro y Crédito —San Francisco Ltda. {en línea} Disponible en <http://repo.uta.edu.ec/handle/123456789/2361>.

KOSUTIC, dejan. (2 de Abril de 2010). Usar la ISO 9001 para implementar la ISO 27001. {en línea}. Disponible en: <http://advisera.com/27001academy/es/blog/2010/04/02/usar-la-iso-9001-para-implementar-la-iso-27001>

Min TIC. (26 de Diciembre de 2008). Entregables 3, 4, 5 y 6: informe final – el Nivel de Madurez de Seguridad de La información – sistema SANSI - SGSI - el Nivel de Madurez de Seguridad de la información para la estrategia de gobierno. {en línea}. Disponible en: <http://programa.gobiernoenlinea.gov.co/apc-aa-files/5854534aee4eee4102f0bd5ca294791f/ ModeloSeguridad_SANSI_SGSI.pdf>.

MINTIC. (Marzo de 2011). El Nivel de Madurez de Seguridad de la Información para la Estrategia de Gobierno en Línea. {en línea}. Disponible en: <http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html>

PEREZ, cesar. (20 de septiembre de 2014). 5. Niveles De Madurez Para El Proceso De Seguridad De La Información. {en línea}. Disponible en: <http://www.pmg-ssi.com/2015/02/iso-27001-el-modelo-de-madurez-de-la-seguridad-de-la-informacion/>.

RENDÓN, maría. (2015). MIGRACIÓN DE UN SGSI BASADO EN ISO/IEC 27001:2005 A LA VERSIÓN ISO/IEC 27001:2013. {en línea}. Disponible en:

<http://www.dspace.espol.edu.ec/xmlui/bitstream/handle/123456789/31352/D-84811.pdf?isAllowed=y&sequence=-1>

RINCÓN, Ernesto. (01 de marzo de 2014). Instrumentos Normativos de Ciberseguridad. {en línea}. Disponible en: <https://web.certicamara.com/media/58493/normativa-colombiana-en-materia-de-ciberseguridad-y-ciberdefensa-1-marzo-2014.pdf>.

SALLIS, ezequiel. CARACCIOLO, claudio. RODRÍGUEZ, Marcelo. Ethical Hacking. México: Alfa Omega, 2010.138 p.

SECRETARÍA GENERAL DE LA ALCALDÍA MAYOR DE BOGOTÁ, Régimen Legal de Bogotá D.C. {En línea}. {25 de marzo de 2017}. Disponible en: <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492>

TRELLEZ ARAUJO, pedro. Seguridad Informática. {En línea}. {11 de febrero de 2017}. Disponible en: <http://es.slideshare.net/Tcherino/seguridad-informatica-3143924?next_slideshow=2>.

UNIVERSIDAD DISTRITAL. Seguridad de la Información: Política para la seguridad de la información de la Universidad Distrital Francisco José de Caldas, {en línea}. Disponible en: <https://portalws.udistrital.edu.co/CIT/documentos/NORMATIVIDAD/politica_seguridad/archivos/Politica_para_Seguridad_Informacion_Version_0.0.1.0.pdf>.

UNIVERSIDAD PEDAGÓGICA Y TECNOLOGICA DE COLOMBIA - U.P.T.C, TUNJA (enero de 2010). Historia de la U.P.T.C. {en línea}. Disponible en: <http://www.uptc.edu.co/facultades/fesad/regencia_farmacia/aspectos_misionales/Historia. > .

ANEXOS

Anexo A: Resumen Analítico De Estudio Formato RAE

Título:	NIVEL DE MADUREZ DE SEGURIDAD EN EL ÁREA DE REDES DE LA UNIVERSIDAD PEDAGÓGICA Y TECNOLÓGICA DE COLOMBIA (U.P.T.C) TUNJA, BASADO EN NORMA ISO 27001.
Autor:	**RODRÍGUEZ,** Antonio
Palabras Claves:	Seguridad de La Información, Confidencialidad, Integridad, Disponibilidad, Estratificación de la organización, Nivel De Madurez, Estándar, ISO / IEC 27001.:2013, Modelo de Seguridad, Políticas de Seguridad
Tema central:	Seguridad de la información.
Problemas:	¿Qué factores influyen en la perdida de información en el Área de Redes de la Universidad Pedagógica y Tecnológica de Colombia (U.P.T.C) Tunja y como se puede reducir este impacto?
Resumen de Contenido:	Con el uso de la internet y los servicios alrededor de esta como herramienta de comunicación, por las diferentes organizaciones sea cual sea su carácter o composición jurídica, la internet es la más utilizada para el intercambio de información y de problemas tecnológicos a medida que avanzan las tecnologías Con ella también se propagan el riesgo de pérdida de información, el robo de los datos, el ataque y violación de información por consiguiente se deben crear medidas, para crear políticas que minimicen los riegos y/o fallas a la que se encuentre expuesta la información en el entorno empresarial, estas políticas deben ir dirigidas hacer tomar y/o a crear conciencias sobre el valor de la información del negocio.
	Para el desarrollo de este proyecto se realiza el método deductivo y una vez hecha la recolección y análisis de la información del área de redes de organización se concluye que el nivel de madurez de seguridad en el área de redes de la universidad Pedagógica y tecnológica de Colombia (U.P.T.C) Tunja, es del 62%, y una vez revisado la evaluación y cumplimiento de los controles del ISO/IEC 27001, se procede a sugerir una serie de políticas con el propósito de evitar la pérdida de información y garantizar seguridad, integridad y autenticidad en la información y la continuidad del negocio.

Fuente: Autor

ANEXO A: (continuación)

Principales Referentes Teóricos y Conceptuales.	• Kosutic, D. (2 de Abril de 2010). *Usar la ISO 9001 para implementar la ISO 27001*. Obtenido de http://advisera.com/27001academy/es/blog/2010/04/02/usar-la-iso-9001-para-implementar-la-iso-27001. • MinTIC. (26 de Diciembre de 2008). *Entregables 3, 4, 5 y 6: informe final – el Nivel de Madurez de Seguridad de La información – sistema SANSI - SGSI - el Nivel de Madurez de Seguridad de la información para la estrategia de gobierno. .* Obtenido de http://programa.gobiernoenlinea.gov.co/apc-aa-files/5854534aee4eee4102f0bd5ca294791f/ModeloSeguridad_SANSI_SGSI.pdf. • MINTIC. (Marzo de 2011). *El Nivel de Madurez de Seguridad de la Información para la Estrategia de Gobierno en Línea.* • RENDÓN, maría. (2015). MIGRACIÓN DE UN SGSI BASADO EN ISO/IEC 27001:2005 A LA VERSIÓN ISO/IEC 27001:2013. {en línea}. Disponible en: • <http://www.dspace.espol.edu.ec/xmlui/bitstream/handle/123456789/31352/D-84811.pdf?isAllowed=y&sequence=-1> • PEREZ, cesar. (20 de septiembre de 2014). 5. Niveles De Madurez Para El Proceso De Seguridad De La Información. {en línea}. Disponible en: • <http://www.pmg-ssi.com/2015/02/iso-27001-el-modelo-de- madurez-de-la-seguridad-de-la-información/>. • SECRETARÍA GENERAL DE LA ALCALDÍA MAYOR DE BOGOTÁ, Régimen Legal de Bogotá D.C. {En línea}. {25 de marzo de 2017}. Disponible en: <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492>
Metodología de la Investigación	Se utilizará el método deductivo por lo que la norma ISO/IEC 27002:2013 control y controles de seguridad nos plantea una guía de implementación general para ser aplicada en todo tipo de organización. Se utilizaran datos particulares de la organización en estudio para realizar políticas generales y detalladas.
Resultados y Conclusiones	Una vez finalizado el análisis de cumplimiento de la norma ISO/IEC 27002: 2013, se observa que la organización, y muy

Fuente: Autor

ANEXO A: (continuación)

	• especialmente el área de redes perteneciente al grupo de organización y sistemas de la organización en estudio, se encuentra en un constante mejoramiento en cuento el manejo, aplicación y puesta en marcha de políticas de seguridad de la información que tiene que ver, directa e indirectamente con el área de redes de la organización.
Resultados y Conclusiones	• Es importante al recalcar que, una vez hecho este análisis de madurez, del área de redes de la organización, se encuentran dominios de la norma con niveles de madurez muy bajos, en los que el grupo encargado de la seguridad de la información, debe trabajar y proponer políticas de mejoramiento para obtener un mejor nivel de madurez y a la vez mejores políticas de seguridad. • Como ya se indicó, el área de redes cuenta con los siguientes índices de nivel de madurez, demostrando con este análisis que, a la fecha, dicho nivel ha superado un 62% el cumplimiento de la norma ISO.
Comentarios:	EL asunto de la seguridad de la información es uno de los temas de más relevancia en siglo XXI, con el fin de proteger uno de los activos más importantes de una organización.
Elaborado por:	Antonio Leonel Rodríguez Bustos Correo electrónico: leonelbus@gmail.com
Fecha Elaboración.	Noviembre del 2018.

Fuente: Autor

Anexo B: Análisis de las encuestas

Para el desarrollo de la presente monografía se realizaron entrevistas con el personal del área de redes, personal docente, estudiantes, para verificar el estado actual y hacer el diagnóstico del nivel de madurez del área en estudio, como se nuestra a continuación el modelo de encuesta realizada al personal del área de redes, basada en la norma ISO 27000, como se observa en la siguiente tabla.

Encuesta sobre el conocimiento de políticas de seguridad de la información en el Área de Redes, del grupo de organización y sistemas de la Universidad Pedagógica y Tecnológica de Colombia UPTC			
Ítems	**Políticas de seguridad de la información**	**Si**	**No**
1	¿Se cuentan con políticas de seguridad de la información?		x
2	¿Se tienen implementados controles de cumplimiento de las políticas de seguridad de la información?		x
3	¿Las políticas de seguridad de la información son de conocimiento de todo el personal de la Institución?		x
Aspectos organizativos para la seguridad			
4	¿La Universidad cuenta con un área para labores exclusivas de seguridad de la información?		X
5	¿La Universidad ha contratado un asesoramiento en materia de seguridad de la información?		X
6	¿Al realizar contratos con empresas externas exige cláusulas de seguridad de la información?		X
7	Con relación a la clasificación y control de activos informáticos		
9	¿Se cuenta con un inventario de activos de información actualizado?	X	
10	¿Este inventario esta automatizado?	X	
11	¿El inventario de activos informáticos se lo actualiza periódicamente?	X	
Políticas del personal respecto a la seguridad Informática			
12	¿Los incidentes de seguridad de los sistemas de información son reportados brevemente por los usuarios?	X	
14	¿La Universidad cuenta con convenios de confidencialidad de la información?		X
Seguridad física y ambiental de los sistemas de Información			
15	¿Todas las áreas esta identificadas?	X	
16	¿Para áreas seguras se cuentan con controles de ingreso del personal?	X	

Fuente autor.

Anexo B (continuación)

Seguridad física y ambiental de los sistemas de Información			
17	¿En caso del alguna falla en el cableado de datos se está preparados para su pronta corrección?	X	
18	¿Se realiza mantenimiento periódico del hardware y software en la Universidad		X
Con relación a la gestión de las comunicaciones de datos y operaciones de los sistemas informáticos			
19	¿La Universidad cuenta con controles contra software malicioso (antivirus, antispyware, etc)?		x
20	¿La Universidad cuenta con registros de accesos y uso de los aplicativos y servicios de la red de los colaboradores?		x
21	¿Se cuentan con controles de seguridad de los medios de almacenamiento?	x	
22	¿La Universidad cuenta con compromisos de responsabilidades del uso de los recursos de la Institución?		x
Control de acceso			
23	¿Para las aplicaciones de la Universidad tienen políticas de control de acceso?	x	
24	¿Las políticas de control de acceso son aplicadas?	x	
25	¿Cuentan con un inventario actualizado para los accesos otorgados a los sistemas informáticos?		x
23	¿Para las aplicaciones de la Universidad tienen políticas de control de acceso?	x	
24	¿Las políticas de control de acceso son aplicadas?	x	
25	¿Cuentan con un inventario actualizado para los accesos otorgados a los sistemas informáticos?		x
26	¿Todas las aplicaciones de la Universidad cuentan con una contraseña para permitir el acceso a los usuarios?	x	
27	¿Para el acceso remoto se tienen establecidos mecanismos de autenticación de usuarios a la red interna de la Universidad?		x
28	¿Se cuenta con controles de monitoreo para los recursos de la Universidad? ?		x

Fuente: Autor

Anexo B (continuación)

Desarrollo y mantenimiento de sistemas informáticos			
29	¿Para el desarrollo de aplicaciones se cuenta con controles de validación de datos de entrada y de salida?	x	
30	¿La Universidad cuenta con controles criptográficos, como por ejemplo el uso de certificados digitales u otros programas para la encriptación de datos?	x	
31	¿Se tienen controles que impidan el acceso no autorizado a los programas fuente de las aplicaciones de la Universidad?	x	
32	¿Se cuenta con un procedimiento de control de los cambios para las aplicaciones, software y sistema operativo?	x	
33	¿Se validan los códigos fuentes desarrollados por personal externo antes de la puesta en producción?	x	
Gestión de incidentes de sistemas informáticos			
34	¿La Universidad cuenta con un procedimiento formal para reportes de incidentes?		x
35	¿Cuentan con una herramienta de registro de incidentes o *Help desk?*		X
Gestión de incidentes de sistemas informáticos			
36	¿Al reporta un incidente de seguridad se cuenta con un plan de respuesta?		x
37	¿Se investiga y recolectan evidencias sobre el incidente de seguridad?		x
Administración de la continuidad de los sistemas Informáticos			
38	¿La Universidad cuenta con planes de continuidad de las operaciones?		x
39	¿Realizan pruebas, mantenimiento y evaluación constante de los planes de continuidad de las operaciones?		x
40	¿Tienen identificada la normativa legal que aplican a las aplicaciones que usa la Universidad?		x
41	¿La Universidad cuenta con políticas de protección de datos y privacidad de la información de los colaboradores?	x	
Cumplimiento legal referido a los sistemas Informáticos			
42	¿Cuentan con controles del uso inadecuado de los recursos de la Universidad?		x
43	¿La Universidad cuenta con controles del cumplimiento de las políticas de seguridad de la información?		x
44	¿Realizan auditoria a los sistemas informáticos de su institución?	x	

Fuente: Autor