SISTEMAS DE GESTIÓN EN SEGURIDAD INFORMÁTICA SGSI EN UNIVERSIDADES PÚBLICAS DEL EJE CAFETERO – COLOMBIA

RUBY ESPERANZA BUITRAGO GIRALDO

Monografía de grado para optar al título de especialista en Seguridad Informática

Directora: Yenny Stella Núñez Álvarez – Ingeniero de Sistemas, Especialista en Seguridad Informática

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SE-GURIDAD INFORMÁTICA.
DOSQUEBRADAS, RISARALDA
2020

NOTAS DE ACEPTACIÓN

_____
_____
_____
_____
_____

_____
Presidente del Jurado

_____
Jurado

_____
Jurado

DOSQUEBRADAS, RISARALDA, MAYO 2020

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

Pág.

SIGLAS USADAS

BD: Bases de Datos, Bodega de Datos

CEAD: Coordinación de Educación a Distancia

CIA: Confidentiality, Integrity and Availability (Confidencialidad, Integridad y Disponibilidad)

CVE: Lista Common Vulnerabilities and Exposures

GIDT: Gerencia de Innovación y Desarrollo Tecnológico de la UNAD

GTHUM: Gerencia de Talento Humano de la UNAD

ICFES: Instituto Colombiano para la Evaluación de la Educación

IDEA: Instituto de Estudios Ambientales, Universidad Nacional de Colombia

IEC: International Electrotechnical Commission

IoT: Por sus siglas en inglés o Internet de las Cosas

ISO: International Organization for Stardarization

MECI: Modelo Estándar de Control Interno (Colciencias)

NTC: Norma Técnica Colombiana

OTIC: Oficina de las Tecnologías de la Información y las Comunicaciones, en este caso en las universidades públicas del Eje Cafetero.

SGC: Servicio Geológico Colombiano

S.G.C.: Sistemas de Gestión de Calidad

SGSI: Sistema de Gestión de la Seguridad Informática

SI: Sistema de Información

SIG: Sistema Integrado de Gestión

SUE: Sistema Universitario Estatal (Colombia)

TI: Tecnología(s) de la Información

TIC: Tecnología de la Información y las Comunicaciones

UNAD: Universidad Nacional Abierta y a Distancia

UNESCO: Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura

UTP: Universidad Tecnológica de Pereira

UNISUR: Unidad Universitaria del Sur de Bogotá

USA: United States of América (Estados Unidos de América)

GLOSARIO

ALMACENAMIENTO EN LA “NUBE”: En inglés cloud storage. Es un modelo de almacenamiento de información, el cual es basado en redes de computadores. Dichos datos se encuentran alojados en espacios de almacenamiento virtualizados, por lo general aportados por terceros.

AMENAZA: Es todo aquello que, de darse desde el interior o desde el exterior de las organizaciones, pueda causar daños a la información, o pérdida de ella, o alterar el normal desarrollo de las actividades a partir de esa información.

ANTIVIRUS: Son programas informáticos que han sido creados para la prevención, el bloqueo, la detección y la eliminación de ciertos archivos o ejecutables que son dañinos para los sistemas informáticos y que se descargan en el computador, sin previo aviso, con el solo hecho de navegar en internet.

ATAQUE(S) INFORMÁTICO(S) O CIBERATAQUE: Es un intento de causar algún tipo de daño o problemas a un sistema informático o red, por parte de una o más personas, de manera organizada e intencional. Adicionalmente, consiste en aprovechar alguna debilidad o falla en el software o en el hardware para obtener un beneficio.

CONFIDENCIALIDAD: Es la forma de prevenir la propagación de la información a personas o sistemas que no se encuentran autorizados.

DISPONIBILIDAD: Es el acceso que se tiene a la información y a los sistemas por personas que son autorizadas para tal y que pueden consultar la información en el momento que así lo requieran, sin que se presenten contratiempos para ello.

INTEGRIDAD: Se refiere a que los datos de una entidad deben permanecer intactos todo el tiempo, libres de modificaciones o de cualquier tipo de alteración que pueda ser generado por un tercero. Se hace necesario a toda costa proteger la información para que sólo sea modificada por una misma persona, evitando de esta manera que se pierda la integridad de esta.

ISO/IEC 27000: Es una familia de normas a la cual se la conoce también como serie ISO 27000, desarrollada y publicada por la ISO y la IEC para facilitar un marco reconocido de forma mundial a las prácticas de gestión de la seguridad de la información.

MALWARE: Es cualquier tipo de programa que ha sido diseñado y elaborado para generar daños; también, puede introducirse sin autorización en algún SI.

PHISHING: Delito cibernético donde el objetivo es contactado vía correo electrónico (pueden ser varios los objetivos – personas contactadas), teléfono o por mensaje de texto por alguien que se hace pasar por una institución legítima para atraer a las personas; lo que buscan estos atacantes es obtener información confidencial, como información de identificación personal, datos bancarios y de tarjetas de crédito, y contraseñas, entre otros.

POLÍTICAS DE SEGURIDAD: Conjunto de normas, reglas y protocolos de acción que se encargan de velar por la seguridad de la información de una empresa.

SISTEMA DE INFORMACIÓN: Conjunto de datos conectados entre sí de forma que, ante una entrada generada por un mundo exterior, produce una respuesta llamada salida.

SISTEMA OPERATIVO – S.O.: Es un programa que, después de cargarse inicialmente en el computador por un programa de arranque, se encarga de gestionar los demás programas que se ejecutan en el mismo.

RIESGO: Lo constituye, para la información, la ligazón entre amenaza y vulnerabilidad.

VULNERABILIDAD: se define así al nivel de exposición a las amenazas a que se somete la información.

RESUMEN

Se busca con este documento conocer el estado de cosas de la gestión de la información que poseen y manejan las universidades públicas del denominado en Colombia Eje Cafetero, en procura de indagar en detalle lo relacionado con la aplicación de normas nacionales e internacionales que rigen en el país la necesidad o conveniencia de contar con un adecuado Sistema de Gestión de la Seguridad Informática (SGSI por su sigla) por parte de empresas, entidades y organizaciones en general, sean públicas o privadas, ante la realidad de vulnerabilidades frente al riesgo de ataques informáticos que comprometan la confidencialidad, autenticidad e integridad de la información. El incremento acelerado de dichos ataques en el mundo obliga a pensar en cuáles serían los mecanismos y acciones a utilizar para enfrentar tal situación y mitigar los riesgos de pérdidas cuantiosas en tangibles e intangibles del patrimonio de las universidades. Se desarrolla entonces una monografía que aporta en la exploración de los adelantos que pudieran tener las universidades públicas del eje cafetero hacia la implementación o consolidación de un SGSI en ellas, basados en normas como la ISO 27001 y metodologías probadas como MAGERIT.

PALABRAS CLAVE: Seguridad informática, sistema de gestión, universidad pública, Eje Cafetero, SGSI.

1. INTRODUCCIÓN.

El panorama de la implementación de sistemas de gestión de seguridad informática en infinidad de organizaciones en Colombia no aparece muy claro, por lo novedoso del asunto, porque tal vez no hay plena conciencia de su importancia y porque se pudiera estar considerando un gasto inoficioso.

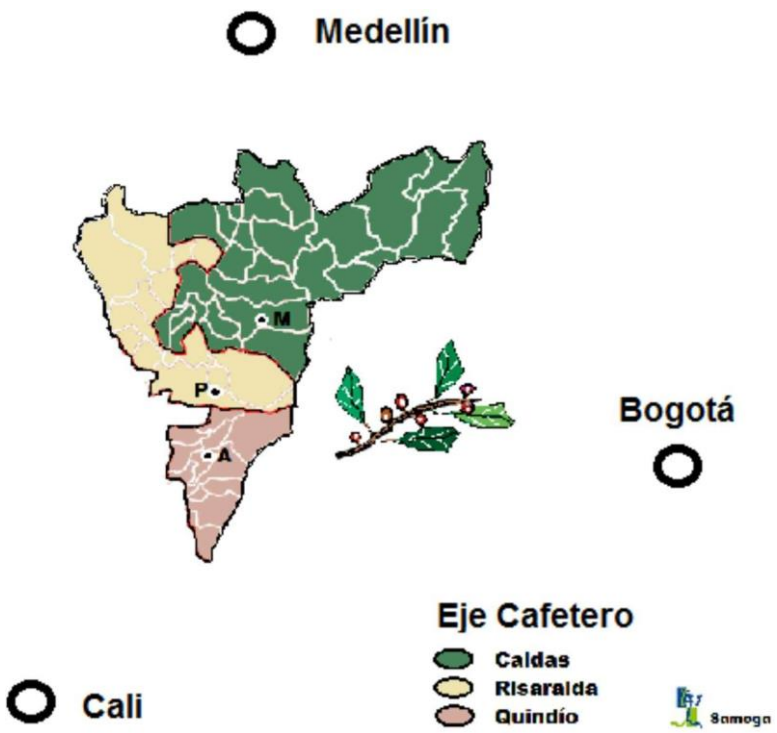
Dentro de estas organizaciones, lamentablemente se encuentran también universidades públicas y privadas del país, y en ellas aparecen las universidades públicas del Eje Cafetero colombiano, medio geográfico, laboral y cultural en el cual la autora de esta monografía se ha desenvuelto siempre. (Ver figura 1).

De Wikipedia[1], "se extrae que el SUE agrupa las 32 principales universidades públicas colombianas y entre ellas aparecen la Universidad Nacional de Colombia sede Manizales (una de las nueve sedes de la Universidad Nacional de Colombia), la Universidad de Caldas, la Universidad Tecnológica de Pereira UTP, la Universidad del Quindío y la Universidad Nacional Abierta y a Distancia UNAD sede Dosquebradas – Risaralda (una de las 53 sedes de la UNAD), ubicadas geográficamente dentro de lo que nacionalmente se conoce como el Eje cafetero colombiano por lo que ha significado históricamente para los tres departamentos que lo conforman (Caldas, Risaralda, Quindío) el cultivo, producción, exportación y venta de café de excelente calidad, con desarrollo de toda una cultura alrededor de este".

La presente monografía se ejecuta en el marco normativo de la UNAD que define una monografía de grado como una "opción de grado que le permite al estudiante el desarrollo de una investigación con base en la revisión de masas documentales" [2]. Con base en esto, se ha establecido igualmente que una monografía así concebida, según UNAD, "es una investigación de carácter bibliográfico a la cual se le pueden adicionar citas testimoniales, en caso de que el tema lo requiera, a partir de una indagación crítica del estado del arte" [3].

[1] Wikipedia. Sistema Universitario Estatal (SUE). [on-line]. 2018.
[2] UNAD. Acuerdo 0029. (13 de 12 de 2013). Por el cual se expide el Reglamento Estudiantil de la Universidad Nacional Abierta y a Distancia (UNAD) y se dictan otras disposiciones. Bogotá, D.C. 2013. p. 48.
[3] UNAD. Alternativas para Grado – ECACEN, Alternativas para Trabajo de Grado. [en línea]. 2013.

Figura 1 ***Mapa del Eje Cafetero Colombiano. Recuperado de EJE CAFETERO (*****M: Manizales, P: Pereira, A: Armenia*****).***



Fuente: CONSTRUCCIÓN SOCIAL E HISTÓRICA DEL TERRITORIO. Gonzalo Duque Escobar. 2018. http://godues.webs.com

Así, se puede concluir que el tipo de investigación que se aplica a esta monografía es el de "INVESTIGACIÓN DOCUMENTAL (Villamizar)",[4] pues la idea central es la de analizar la experiencia organizacional de las universidades públicas del eje cafetero colombiano en cuanto a seguridad informática, fabricar conclusiones, efectuar comparaciones y finalmente contribuir una visión personal que permita la generación de nuevo conocimiento.

El diseño de esta se basa, entonces, en la revisión de masas documentales sobre bibliografía relacionada y documentos institucionales, así como la adición de citas testimoniales recogidas de entrevistas personales con funcionarios públicos de las entidades en estudio.

[4] VILLAMIZAR, Iván. GUIA TRABAJO DE GRADO MODALIDAD MONOGRAFIA MAESTRIA EN ADMINISTRACIÓN DE LAS ORGANIZACIONES. Bogotá, 2017.

Se adiciona arriba un listado de siglas de instituciones y programas que aparecen mencionados en el documento, así como un glosario de términos que incluye la definición de las principales variables analizadas.

2. PLANTEAMIENTO DEL PROBLEMA.

2.1. DEFINICIÓN DEL PROBLEMA

Según Mejía:

> "las universidades públicas en Colombia son instituciones que tienen por finalidad generar y transmitir conocimiento y aplicarlo a la solución de problemas y a la satisfacción de necesidades de su entorno social, cultural, económico y ambiental, por la vía de la formación de profesionales, especialistas y expertos, pero también de la investigación de fenómenos de todo tipo, de la creación artística y cultural y de la interacción con otras instituciones, especialmente públicas, como ministerios, gobernaciones, alcaldías, corporaciones regionales, etc. Por lo mismo, son organizaciones que manejan su propia complejidad ante la necesidad de estar permanentemente adaptándose al cambio y dentro de él a los avances tecnológicos y culturales vertiginosos que se dan en la sociedad"[5].

Tal complejidad involucra lo relacionado con la necesidad que tiene toda organización, y entre ellas las universidades, de manejar las TIC's, los SGSI y las BDs, así como las redes de Internet e Intranet, pero, a su vez, de garantizar al máximo la seguridad de la información que posee.

En efecto, bien lo dice Ramírez,

> "con el avance tecnológico que ha sufrido nuestra sociedad, los términos de seguridad y responsabilidad en informática adquirieron gran importancia cuando se hablaba sobre protección de datos e información para empresas o dependencias públicas.
>
> Debido al desarrollo de las redes de computadores y de los sistemas de información interconectados entre sí, en las empresas se ha concentrado el término de seguridad aplicado a los grandes sistemas centralizados y, por este motivo, muchas organizaciones no conocen la información que se guarda en cada computador ni los riesgos presentes que se derivan de posibles ataques informáticos, fallas físicas, ni cómo la propia organización o el personal puede utilizar esa información de dichos computadores.
>
> Vivimos sumergidos en una sociedad que interactúa diariamente con las tecnologías de la información como parte de sus tareas diarias, desde el uso de un computador portátil, los cajeros automáticos, el pago de servicios y transferencias desde nuestros dispositivos móviles, hasta la actualización del estado en nuestra red social favorita.

[5] MEJÍA, Fernando. Universidad Nacional de Colombia – Sede Manizales. Manizales, Colombia. Charla con profesor. (R. E. Giraldo, entrevistador). 2018.

> En este contexto, surge una nueva preocupación por mantener la seguridad de nuestra información, desde un nivel personal hasta un nivel organizacional. Dependerá del uso que se le dé a esta información que beneficie o perjudique en las decisiones de una compañía.
>
> La preocupación o conciencia del peligro del mal uso de la información por agentes externos es, por decirlo de alguna manera, la mitad de la seguridad requerida. Resta aprender sobre la seguridad, los riesgos, las políticas y las prevenciones que deberemos tener al hacer uso o al manejar información" [6].

Por esto, y por el carácter de ente público de cada universidad pública en la cual interactúa un sinnúmero de personas entre estudiantes, profesores, empleados, egresados, visitantes, etc., ella se vuelve un organismo en donde no es fácil garantizar la total seguridad de sus sistemas y herramientas de la información.

Eso lo saben aquellos que, con diversos fines, frecuentemente malévolos, realizan ataques informáticos que pueden llegar a causar inmensos daños a los bienes, al patrimonio intelectual y a la credibilidad e imagen de la universidad, o sea, comprometer la confidencialidad, autenticidad e integridad de sus sistemas informáticos (CIA, por sus siglas en inglés). Según estadísticas reportadas en la lista Common Vulnerabilities and Exposures CVE, "en el año 2017 se reportaron más de 14.600 vulnerabilidades informáticas, y dicho año cerró con un récord histórico al alcanzar un aumento del 120 % en el número de casos" [7].

Es necesario conocer cuáles medidas implementar para salvaguardar los activos de la entidad ante amenazas que pueden surgir del exterior o incluso del interior de la institución, reducir los riesgos de ataques y evitar los sobre costos (generalmente muy grandes) que pueden generar los daños que se causen por esa vía.

Al respecto, una investigación realizada por CISCO[8] (2018) "y que implicó a más de 3600 personas en 26 países, planteó que el miedo a las violaciones se basa en el costo financiero de los ataques, que ya no es un número hipotético. Las infracciones causan un daño económico real a las organizaciones, daños que pueden tardar meses o años en resolverse". [Según los encuestados del estudio, un porcentaje

---

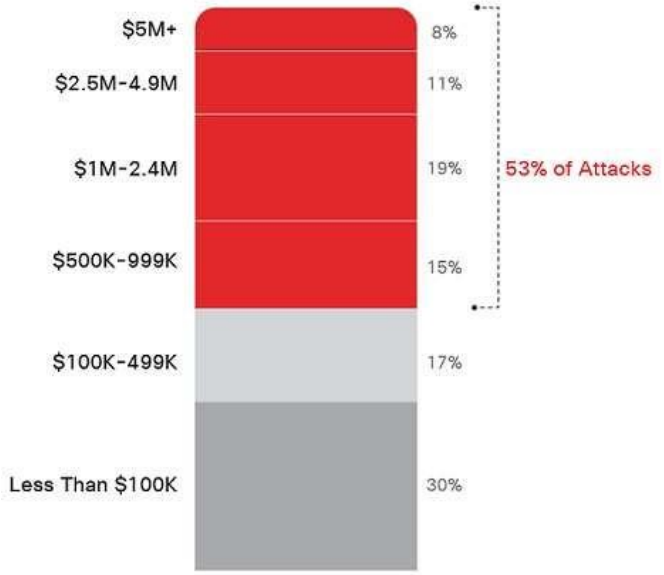
[6] RAMÍREZ MUNIVE, Yair, et al. Tecnologías de Información y Comunicación en las Organizaciones. En: Publicaciones Empresariales UNAM. 2016. 45p.

[7] Página web. En 2017 se reportaron más de 14.600 vulnerabilidades informáticas. En: El Tiempo. 15, enero, 2018. TECNÓSFERA.

[8] CISCO. Reporte Anual de Ciberseguridad. [en línea]. 2018.

alto de los ataques generaron daños en sus economías que superaron el medio millón de dólares] (Figura 2)".

***Figura 2** Cantidad de ataques que resultan en daños de USD 500,000 o más. CISCO – 2018.*



Fuente: CISCO. https://www.cisco.com/c/dam/assets/prod/sec/acr/2018/large/figure-40-attack-damages.png

Aunque las medidas son variadas y todas pueden ser eficientes, no siempre se implementan las mejores –generalmente por dificultades presupuestales o por inadecuadas gestiones en esa dirección, entre otras cosas- o sea, las que pueden garantizar de verdad un Sistema de Gestión de Seguridad Informática (de aquí en adelante SGSI).

Fueron importantes noticias de prensa las experiencias negativas que se vivieron hace unos dos años en universidades públicas e instituciones afines (U. de Caldas, ICFES) relacionadas con ataques informáticos a ellas que obligaron a tomar medidas radicales de emergencia por afectaciones a los procesos de pruebas y admisiones. Precisamente, el año informativo -2017-

> "en la página web del Instituto Colombiano para la Evaluación de la Educación (ICFES) abrió con una circular concreta, que dio cuenta de una situación grave: ESTÁN FALSIFICANDO LOS CERTIFICADOS QUE EXPIDE LA ENTIDAD SOBRE LOS GANADORES DE LA DISTINCIÓN ANDRÉS BELLO. Y La Patria, [(periódico de Manizales y Caldas)] alertó en publicaciones, el 13 y el 17 de diciembre de 2016, sobre inconsistencias en los admitidos en la Universidad de Caldas con la Andrés Bello para

el primer semestre de Medicina del presente año. Se incluyeron testimonios que dieron cuenta de una supuesta venta de cupos" [9].

De otra parte, algunas fuentes primarias consultadas por el autor (funcionario Oficina TIC)[10], dejaron entrever de manera muy preliminar que alguna o algunas universidades públicas en el eje cafetero no cuentan con un SGSI, lo que las hace muy vulnerables a situaciones graves como las utilizadas arriba a manera de ejemplo.

De todo lo anterior se desprende la pregunta problema que se busca solucionar en este trabajo: ¿qué tan vulnerable se encuentra la información en las universidades públicas del Eje Cafetero colombiano y qué medidas han tomado estas para su protección?

2.2. JUSTIFICACIÓN

En Colombia y en el mundo se han incrementado de manera importante y preocupante los ataques informáticos a organizaciones, con diversos fines, e incluso la pérdida de una ética en el actuar de muchas personas, incluyendo a quienes se consideran el futuro de las naciones como son los jóvenes, el afán por el éxito sin esfuerzo, acompañado del conocimiento que han desarrollado en informática, ha conducido a intentar fraudes en las universidades relacionados en particular con admisiones fraudulentas, plagios sobre el patrimonio intelectual de la misma universidad, robo de información, etc. Lo anterior se ilustra a manera de ejemplo con lo que incluye el periódico El Comercio de Ecuador el 13 de agosto de 2018 cuando titula en su página de tecnologías:

"Ataques informáticos aumentan un 60% en Latinoamérica en 2018, y añade: Latinoamérica registró 746 000 ciberataques entre mediados de 2017 y lo que va del 2018, lo que supone un incremento del 60% con respecto al periodo anterior y equivale a una media de 9 ataques por segundo, según un estudio divulgado este lunes 13 de agosto de 2018 en Panamá por la compañía rusa Kaspersky Lab., Venezuela, Bolivia y Brasil son los países que más ataques sufrieron en los últimos meses, la mayoría de los cuales estaban orientados al robo de dinero, de acuerdo al informe presentado este lunes por la empresa rusa durante un congreso en Panamá sobre ciberseguridad"[11].

[9] Página web. Están falsificando la Andrés Bello: Icfes. En: La Patria. 11, enero, 2017. Educación.
[10] Funcionario OTIC. Universidad Nacional de Colombia – Sede Manizales. Manizales, Colombia. Conversación informal con funcionario de la OTIC. (R. E. Giraldo, Entrevistador). 2018.
[11] Página web. Ataques informáticos aumentan un 60% en Latinoamérica en 2018. En: El Comercio. Ecuador. 13, agosto, 2018. Tecnología.

La universidad pública en general, sin embargo, tiene la inevitable necesidad de facilitar el acceso de personas –estudiantes, profesores, otros- a aulas informáticas, así como a bibliotecas, documentos de distinto tipo, oficinas administrativo-académicas, cubículos de profesores, páginas web institucionales, etc., por su misma naturaleza de ente educativo que se debe a los jóvenes y a la satisfacción de sus necesidades de aprendizaje (en cada Universidad se tienen reglamentos para el uso de libros de las bibliotecas, los estudiantes son dotados de un carnet para identificarse ante ella misma y el exterior, a cada estudiante le es asignado un correo institucional, el acceso a las salas de computadores es restringido y sólo puede darse mientras un profesor abra dicha sala y permita el acceso de sus alumnos a ella, hay un servicio de personal de vigilancia que está atento a la entrada y salida de personas a sitios de la universidad, lo cual puede hacerse sólo en horarios establecidos, el acceso a un cubículo de un profesor se tendrá, claro, cuando él esté presente, las oficinas administrativas tienen siempre un funcionario que recibe al visitante y se pone a sus órdenes para lo que requiera allí, se tiene servicio de wifi y cada integrante de la comunidad recibe la contraseña para usar la red, entre otras cosas), pero esto la hace muy vulnerable frente al riesgo de ataques informáticos. Y en un caso adicional, hay un riesgo de daños a las instalaciones físicas de la universidad por siniestros (referentes a amenazas naturales) de distinto tipo: terremotos, inundaciones, incendios, etc., que pueden afectar gravemente los equipos informáticos y la información que contienen.

A todo lo anterior hay que añadir que no siempre se tiene en estas instituciones todos los documentos importantes de la institución dentro de una copia de seguridad, y no todos se tienen “en la nube”; no siempre se desarrollan programas y actividades de capacitación del personal interno de la universidad en el manejo de la información; no existe en el país el personal experto idóneo en cantidad suficiente para atender las necesidades que en el campo de la gestión de la seguridad informática tienen tantas organizaciones nacionales, entre ellas las universidades públicas y, aunque la legislación en Colombia asociada a la seguridad informática es considerada buena, igualmente no se cuenta siempre con quien la pueda aplicar o hacer cumplir.

En vista de que no es muy reconocida la manera como nuestras universidades públicas del denominado Eje Cafetero en Colombia están enfrentando este asunto, amerita desarrollarse con criterio académico una monografía que dé claridades sobre ello y, de paso, sirva en algo a las autoridades académicas de esas universidades para la toma de decisiones al respecto en la mejor dirección posible, salvaguardando sus más caros intereses, y entre ellos su patrimonio físico e intelectual.

3. OBJETIVOS, ALCANCE Y RESULTADOS ESPERADOS.

3.1. OBJETIVO GENERAL

Conocer y analizar la experiencia organizacional de la gestión de la información que se desarrolla en las universidades públicas del Eje Cafetero colombiano.

3.2. OBJETIVOS ESPECÍFICOS

- Conocer de la gestión de la información que se lleva en las cinco universidades públicas del Eje Cafetero: Universidad Nacional de Colombia sede Manizales, Universidad de Caldas, Universidad Tecnológica de Pereira, Universidad del Quindío y Universidad Nacional Abierta y a Distancia UNAD sede Dosquebradas.
- Indagar el uso y aplicación de normas, estándares y metodologías asociadas a los sistemas de gestión de la información en las mencionadas universidades.
- Reforzar ante funcionarios de estas universidades la trascendencia que tiene el contar con un SGSI.

3.3. ALCANCE

Por tratarse de una monografía, el proyecto llega hasta conocer el estado de cosas de los SGSI que pudieran tenerse en cinco universidades públicas del eje cafetero en Colombia, con la aplicación de normas que existen para ello como la ISO 27001 y con el uso de metodologías modernas probadas en otros casos, como la metodología MAGERIT. Así, se tendría una semblanza de la realidad que se vive en estas entidades ante las vulnerabilidades y riesgos que enfrentan por ataques informáticos, tan en boga.

3.4. RESULTADOS ESPERADOS

Al terminar el proyecto se tendrá un documento monográfico conceptualizado y detallado, que establece diagnósticos y análisis de la situación de los SGSI en cinco universidades públicas del eje cafetero colombiano, hace claridad sobre la aplicación de normas internacionales y nacionales al respecto por parte de estas universidades y lleva a sus directivas a tomar conciencia plena de la trascendencia que adquiere hoy en día la implementación de un SGSI en su universidad, so pena

de incurrir en pérdidas graves de la información o en daños a la misma por ataques informáticos, causados por inescrupulosos o por hackers que tienen un interés particular, por ejemplo, en la alteración de notas y otros.

4. MARCO TEÓRICO.

4.1. LA SOCIEDAD DE LA INFORMACIÓN

A nivel mundial, la expresión Tecnologías de la información y las telecomunicaciones TIC se ha tomado buena parte de las actividades que se ejecutan en todos los campos de acción en pro del desarrollo de la sociedad e, incluso, en Colombia se creó el Ministerio de las TIC, como se le identifica en sigla.

Tal avance en el conocimiento especializado en esta área ha generado lo que se ha conocido como la sociedad de la información en cuanto a la facilidad que ha traído para transferir y utilizar esta en ámbitos de la productividad, la economía, el emprendimiento, la cultura, la recreación, etc. lo que conduce a vislumbrar mejores perspectivas hacía el futuro de la sociedad. Incluso, dentro de ello, las redes sociales han contribuido a democratizar el mundo.

Y todo se debe a los gigantescos avances científico – tecnológicos tenidos en por lo menos los últimos cuarenta años en tres áreas: la informática, la electrónica y las telecomunicaciones, cuyo análisis detallado daría para un libro.

Así, se ha constituido en el planeta una nueva sociedad y cultura que, sin embargo, ha traído de la mano problemas que están resultando graves para el devenir de las personas, como lo plantea claramente el profesor Ricardo Pérez Zúñiga (U. de Guadalajara, México) cuando escribe que:

> "la sociedad de la información ha ocasionado una dependencia tecnológica en las personas, las cuales han transformado su naturaleza y ha provocado una fuerte subordinación, así como un cambio de hábitos en la vida diaria del ser humano. Esto ha derivado en la aparición de una nueva cultura informática que no respeta fronteras y conduce a un mundo diferente e informado con la incorporación de las TIC y su principal insumo: la información, integrada a la vida cotidiana y generadora de poder"[12].

Consuelo Belloch, de la Universidad de Valencia, refuerza lo anterior cuando dice en sus escritos que "el gran desarrollo tecnológico que se ha producido recientemente ha propiciado lo que algunos autores denominan la nueva 'revolución'

[12] PÉREZ ZÚÑIGA, Ricardo, et al. La sociedad del conocimiento y la sociedad de la información como la piedra angular en la innovación tecnológica educativa. En: Revista iberoamericana para la investigación y el desarrollo educativo. (enero – junio, 2018). Vol. 8, Núm. 16.

social, con el desarrollo de la sociedad de la información. Y añade, los valores que dinamicen la sociedad serán los mismos que orienten el uso de las tecnologías"[13] .

José Luis Sampedro en Técnica y Globalización (2002) "realiza una reflexión en profundidad sobre la globalización y la tecnología incidiendo en esta idea sobre la importancia de orientar su utilización para lograr una sociedad más humana, justa e igualitaria" [14].

Se entiende aquí por información:

> "todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración […]. La seguridad de la información, según ISO 27001, consiste en la preservación de su [CIA], así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:
>
> - **Confidencialidad:** la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
> - **Integridad:** mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
> - **Disponibilidad:** acceso y utilización de la información y los sistemas de tratamiento de esta por parte de los individuos, entidades o procesos autorizados cuando lo requieran"[15].

4.2. DEFINICIONES DE SEGURIDAD INFORMÁTICA

La abundancia de información que ha generado la sociedad planteada en el numeral anterior, que crece exponencialmente y que debe medirse hoy por lo menos en hexabytes, ha traído consigo la necesidad de almacenarlos adecuadamente para su uso en sistemas informáticos, pero, simultáneamente, la conveniencia de proteger esos datos en su confidencialidad, en su integridad y en su disponibilidad contra inescrupulosos que están esperando para sacarles provechos indebidos.

---

[13] BELLOCH, Consuelo. Las Tecnologías de la Información y Comunicación en el aprendizaje. [on-line]. 2012.
[14] SAMPEDRO, José. Técnica y Globalización. Boletín Económico del ICE, N° 2750. [en línea]. 2002. [2018]. Citado por: BELLOCH
[15] ISO27000.es. Sistema de Gestión de la Seguridad de la Información. [en línea]. 2012.

Dicha protección puede ser lógica, a través de un programa de cómputo diseñado para ello, pero además contempla la identificación y/o autentificación de usuarios, contraseñas de acceso, privilegios, entre otros. O también puede ser física, en los equipos o dentro y/o alrededor del Centro de Cómputo (Oficina de las Tecnologías de la Información y las Comunicaciones, o como cada uno llame a este tipo de dependencias).

Sin embargo, no es posible garantizar totalmente la protección de la información ante amenazas múltiples, que además cada día se renuevan y son más creativas (por parte de los delincuentes).

Así, aparecen, por ejemplo, los virus, de amplia gama, muy dañinos, que pueden dañar o controlar la información privada y en muchas oportunidades lo han logrado, desafortunadamente, y que han obligado a producir –para contrarrestarlos- técnicas y herramientas denominadas de seguridad informática, como los programas antivirus, los firewalls, los antispyware, y tantos otros.

Se puede deducir fácilmente ahora, a partir de lo enunciado atrás, una definición de seguridad informática como la disciplina en esta área que tiene como fin garantizar la protección de toda la información digital que una entidad o persona natural tenga almacenada en computadores, utilizando herramientas diseñadas para ello.

Sin embargo, tal como nos lo señalan J. Pérez y M. Merino en una publicación suya:

> "lo esencial sigue siendo la capacitación de los usuarios. Una persona que conoce cómo protegerse de las amenazas sabrá utilizar sus recursos de la mejor manera posible para evitar ataques o accidentes.
>
> En otras palabras, puede decirse que la seguridad informática busca garantizar que los recursos de un sistema de información sean utilizados tal como una organización o un usuario lo ha decidido, sin intromisiones"[16].

4.3. AMENAZA, VULNERABILIDAD Y RIESGOS INFORMÁTICOS

En el caso que nos ocupa (la seguridad informática) se constituye en una amenaza para dicha seguridad todo aquello que, de darse desde el interior o desde el exterior

[16] PÉREZ PORTO, Julián y MERINO, María. Definición de seguridad informática. [en línea]. 2008.

de las organizaciones, pueda causar daños a la información, o pérdida de ella, o alterar los procesos.

Ahora bien, el nivel de perjuicios que puede ocasionar cierta amenaza depende del grado de vulnerabilidad (el nivel de exposición a las amenazas) de la tecnología empleada o de los procesos que se llevan, de tal forma que, finalmente, la ligazón entre amenaza y vulnerabilidad constituye el riesgo para la información.

Planteando el asunto de una manera simple, por ejemplo, una fuerte amenaza ante una baja vulnerabilidad confluye en un bajo riesgo, y una baja amenaza ante una alta vulnerabilidad puede terminar en un riesgo alto.

Al respecto, del consultor en seguridad C. H. Tarazona se toma lo siguiente de uno de sus escritos para ilustrar el tema de los tipos de amenazas:

> "Básicamente, podemos agrupar las amenazas a la información en cuatro grandes categorías:
>
> Factores Humanos (accidentales, errores); Fallas en los sistemas de procesamiento de información; Desastres naturales y; Actos maliciosos o malintencionados; algunas de estas amenazas son:

- Virus informáticos o código malicioso
- Uso no autorizado de Sistemas Informáticos
- Robo de Información
- Fraudes basados en el uso de computadores
- Suplantación de identidad
- Denegación de Servicios (DoS)
- Ataques de Fuerza Bruta
- Alteración de la Información
- Divulgación de Información
- Desastres Naturales
- Sabotaje, vandalismo
- Espionaje"[17].

4.4. ATAQUES INFORMÁTICOS

[17] TARAZONA T. Cesar. Amenazas informáticas y seguridad de la información. En: CSI/FBI Computer Crime and Security Survey, 138. (2007). Vol. 28 Núm. 84.

Dentro del tema de la seguridad informática se ha vuelto muy familiar, por razones obvias, el asunto de los ciberataques o ataques informáticos, pues ellos conforman en la actualidad una parte muy importante de las amenazas contra la información y los datos de las organizaciones.

Lo anterior significa que buena parte de las medidas de seguridad que se deben adoptar en ellas necesitan orientarse hacia la detección, control y rechazo de tales ataques, que permanentemente se están multiplicando y sofisticando.

En efecto, los ciberataques son hoy numerosos y de distintos tipos, de los cuales algunos de los más importantes son: los virus (que contaminan los archivos informáticos), los malware (softwares maliciosos), los troyanos (abren puertas traseras a otros programas dañinos), los spyware (programas espías), los gusanos (infectan los equipos, hacen copias de ellos y las difunden en las redes), los phishing (técnicas de suplantación de identidad para robar datos), los DDoS (realiza muchas peticiones a un servidor hasta lograr que se bloquee).

A manera de ilustración de lo dicho, Optical Networks nos dice:

> "en el 2018 hubo diferentes tipos de ciberataques a nivel mundial que afectaron a numerosas empresas de distintos países. Otros ejemplos los podemos ver a través de Digital Attack Map que es una página web donde se muestran los ataques que han tenido lugar en un día en concreto del año […]. Un tipo de ramsomware afectó a millones de equipos en todo el mundo, entre otros, a los equipos de la sede de Telefónica en Madrid, al Sistema de salud británico o el Ministerio del Interior ruso […]. Dado el creciente volumen de ciberataques al que los gobiernos municipales y estatales se están enfrentando en los últimos años, es muy probable que, en 2018, estos ataques aumenten, aprovechando la mayor inversión realizada por la Administración en servicios online y cloud, dejando de lado la seguridad. Estos asaltos tendrán un efecto dominó, exponiendo a los ciudadanos a más casos de fraude, robo o exposición de datos […]. El incremento de la efectividad de los ataques DDoS combinado con la conexión a Internet de nuevos dispositivos (IoT) va a provocar un potencial aumento de este tipo de ciberataques.
>
> El [IoT] puede contribuir a este tipo de ataques en la medida en que estos dispositivos sean contagiados. Basta con infiltrarse en uno de ellos, aparentemente sin interés, como puede ser un Smarth TV, para que se propague al resto de nuestros dispositivos e involucrarlos en un ataque DDoS […]. El aumento de datos migrados a la nube, y la gestión de esta por parte de proveedores de gran importancia, hacen que el objetivo sea altamente deseable. Los proveedores de servicios en la nube se convierten en un objetivo"[18].

[18] NETWORKS, O. Tipos de ataques informáticos y previsiones para el 2018. [en línea]. 2018.

4.5. POLÍTICAS DE SEGURIDAD INFORMÁTICA EN LAS ORGANIZACIONES

Son muchas las organizaciones -desde las más grandes a las más pequeñas- que, aún en los tiempos que se viven, no han tomado entera conciencia de lo que significa exponer su información y sus datos a amenazas antrópicas, pero también naturales, de manera muy vulnerable, generando altos riesgos de pérdidas materiales y definitivas de la información digital, como también, por ende, de pérdidas económicas cuantiosas que ponen en grave peligro la supervivencia de la organización.

Sin embargo, para esas entidades y empresas privadas y públicas nunca será tarde para empezar a manejar políticas de seguridad que las protejan, por ejemplo, de ciberataques.

Existen muchos modelos que pueden seguirse para adoptar dichas políticas de seguridad informática, y estos se encuentran en la literatura disponible en redes, bibliotecas y empresas.

En uno de ellos, ofrecido por la empresa española RCG – Comunicaciones[19], experta en el tema de la seguridad informática de las empresas, se plantean siete (7) políticas de seguridad, a saber:

- Realización de una prueba de seguridad, que analice la situación de la empresa en cuanto a vulnerabilidades y otras.
- Ejecución de un análisis de riesgos, que permita saber cuál es el nivel de seguridad de la red empresarial, si bajo, medio o alto.
- Revisión de contraseñas, para hacerlo regularmente y cambiarlas, cuando sea necesario, por contraseñas complejas.
- Establecer protocolos de seguridad, por ejemplo, haciendo copias de seguridad de la documentación que se usa en la red y otras.
- Formar e informar a los empleados de la empresa en el tema de la SI.
- Crear un equipo de seguridad y una estructura, con buena organización y personal que vele por el cumplimiento de los protocolos y las medidas adoptadas.
- Protección antivirus de equipos y computadores en general, revisándolos constantemente y utilizando las últimas versiones de antivirus, cortafuegos y otros programas que eviten la entrada de códigos maliciosos.

[19] RCG Comunicaciones. 7 políticas de seguridad de red que debes conocer. [en línea]. 2018.

4.6. NORMAS INTERNACIONALES Y LEYES DE SEGURIDAD INFORMÁTICA

Fue prácticamente a principios de este siglo que se empezó a desarrollar el tema de producir normas y leyes que ampararan la información y los datos digitales de las organizaciones, con la expedición del código penal, la Ley 599 de 2000, que ya incorpora algunos delitos informáticos. A partir de allí, se siguieron expidiendo Normas, Decretos y Leyes entre las cuales se destacan la Norma Técnica Colombiana ISO 27001 de 2005, actualizada y ratificada en el 2013, que se constituye en la base para la seguridad de la gestión de los sistemas informáticos (luego, la Norma 27002 complementó la 27001); también, la Ley 1273 de 2009 que modifica el Código Penal e introduce como bien tutelado la protección de la información y los datos; hasta la Ley 1581 de 2012 y reglamentada con el decreto 1377 de 2013, dictando disposiciones sobre la protección de datos personales.

La expedición de estas normas y leyes ha resultado fundamental para los procesos de gestión de la seguridad informática en todo tipo de organización, entre ellas las entidades públicas, como las universidades.

El Servicio Geológico Colombiano SGC permite complementar este documento con un listado de normas y leyes nacionales e internacionales que aplican a la seguridad informática:

- "Ley Estatutaria 1581 de 2012 y Reglamentada Parcialmente por el Decreto Nacional 1377 de 2013: Por la cual se dictan disposiciones generales para la protección de datos personales.
- Decreto 2693 de 2012: Lineamientos generales de la Estrategia de Gobierno de la República de Colombia que lidera el Ministerio de las Tecnologías de Información y las Comunicaciones, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones.
- Decreto 2578 de 2012: Por medio del cual se reglamenta el Sistema Nacional de Archivos. Incluye "El deber de entregar inventario de los documentos de archivo a cargo del servidor público, se circunscribe tanto a los documentos físicos en archivos tradicionales, como a los documentos electrónicos que se encuentren en equipos de cómputo, sistemas de información, medios portátiles" entre otras disposiciones.
- Decreto 2609 de 2012: Por medio del cual se reglamenta el Título V de la Ley General de Archivo del año 2000. Incluye aspectos que se deben considerar para la adecuada gestión de los documentos electrónicos.
- Ley 1437 de 2011: Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
- Ley 1273 de 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien tutelado denominado "de la protección de la información y los datos" y

se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

- Ley 1341 de 2009: Por medio de la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y comunicaciones - TIC, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.
- Ley 1150 de 2007: Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos.
- BS 7799-3 de 2006: Proporciona una guía para soportar los requisitos establecidos por ISO/IEC 27001:2005 con respecto a todos los aspectos que debe cubrir el ciclo de análisis y gestión del riesgo en la construcción de un sistema de gestión de la seguridad de la información (SGSI).
- NTC 27001 de 2006: Sistema de Gestión de Seguridad de la Información (SGSI). En 2005, con más de 1700 empresas certificadas en BS7799-2, ISO publicó este esquema como estándar ISO 27001, al tiempo que se revisó y actualizó ISO 17799 y esta última norma se denomina ISO 27002 de 2005 el 1 de julio de 2007, manteniendo el contenido, así como el año de publicación formal de revisión.
- ISO 27002 de 2005: Esta norma proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar e implantar o mantener sistemas de gestión de la seguridad de la información.
- ISO/IEC 27001 de 2005: Es la evolución certificable del código de buenas prácticas ISO 17799. Define cómo organizar la seguridad de la información en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande.
- Ley 962 de 2005: Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos.
- Modelo Estándar de Control Interno MECI 1000 de 2005: Proporciona una estructura para el control de la estrategia, la gestión y la evaluación en las entidades, con el fin de orientarlas hacia el cumplimiento de los objetivos institucionales y la contribución de estos a los fines esenciales del Estado Colombiano.
- NTCGP1000 de 2004: Esta Norma establece los requisitos para la implementación de un sistema de gestión de la calidad aplicable a la rama ejecutiva del poder público y otras entidades prestadoras de servicio.
- ISO/IEC TR 18044 de 2004: Ofrece asesoramiento y orientación sobre la seguridad de la información de gestión de incidencias para los administradores de seguridad de la información y de los administradores de sistemas de información.
- Ley 599 de 2000: Por la cual se expide el Código Penal. Se crea el bien jurídico de los derechos de autor e incorpora algunas conductas relacionadas indirectamente con los delitos informáticos como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas, y manifiesta que el acceso abusivo a un sistema informático protegido con medida de seguridad o contra la voluntad de quien tiene derecho a excluirlo, incurre en multa"[20].

[20] MINTIC. Manual de Normas y Políticas de Seguridad Informática. [en línea]. (26 de 09 de 2014).

Sin embargo, vale la pena anotar que, si bien no se mencionan en el listado anterior, existen otras normas y modelos internacionales que se utilizan para la gestión de la seguridad de la información, entre los cuales se quiso aquí, para mejor ilustrar el asunto, destacar uno de ellos, conocido como el ISM3 (Information Security Management Maturity Model, su nombre en inglés) el cual se presenta como alternativo y crítico frente a lo que se ofrece en la ISO/IEC 27001.

Como dice Pallas sobre este modelo:

> "es un modelo de gestión de madurez de la seguridad de la información alineado con los principios de gestión de calidad de la ISO 9001 y aplicados a los sistemas de gestión de seguridad de la información (SGSI).
>
> En él se establecen diferentes niveles de seguridad, donde partiendo desde un nivel inicial en el que se identifica el posicionamiento de la empresa, ésta puede plantearse como meta alcanzar determinado nivel que considere conveniente para sus necesidades de seguridad y adecuado para su disponibilidad de recursos.
>
> Es un modelo basado en procesos con foco en las necesidades de seguridad del negocio, de forma de establecer la seguridad requerida en forma top down basado en las funciones de negocio. Para ello sigue un criterio de efectividad de las medidas de seguridad tomadas y su impacto en el mismo, estableciendo la necesidad de métricas y apoyándose en el paradigma: "lo que no se puede medir no se puede gestionar."
>
> Sus creadores y seguidores tienen una visión crítica de la norma ISO/IEC 27.001 porque la conciben como una norma basada en controles (y no en procesos) y no lo suficientemente alineada con las necesidades del negocio. No obstante, declaran la compatibilidad de ISM3 con la norma referida para la implementación y mejora de un SGSI, aplicando el modelo propuesto por ISM3 y dando cumplimiento a los requerimientos de la norma ISO/IEC 27001"[21].

4.7. LA SEGURIDAD DE LA INFORMACIÓN Y SUS SISTEMAS DE GESTIÓN SGSI

4.7.1. Definición

[21] PALLAS MEGA, Gustavo. Metodología de Implantación de un SGSI en un grupo empresarial jerárquico. Montevideo, Uruguay. 2009. Tesis de Maestría en Ingeniería en Computación. Universidad de la República. Instituto de Computación – Facultad de Ingeniería.

Por tratarse del tema central de esta monografía -la implementación de un SGSI en universidades públicas- se hace necesario hacer claridad sobre lo que se entiende normalmente por un sistema de ese tipo. Se apoya la autora para ello en una Guía de aplicación de la norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes desarrollada por L. Gómez F. y A. Andrés A., de la cual extraemos lo sustancial para el caso.

> "Un Sistema de Gestión de Seguridad Informática (SGSI), según la Norma UNE-ISO/IEC 27001, hace parte en una empresa de su sistema de gestión en general, [y tiene como propósito fundamental] crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información.
>
> De acuerdo con dicha norma, un SGSI [debe incluir] las políticas, la planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos de la empresa o entidad. En resumen, su documentación de soporte y sus tareas.
>
> La norma ISO 27001 [tiene una estructura y unos requisitos iguales a los de otras normas que aplican a los] sistemas de gestión (UNE-EN ISO 9001 y UNE-EN ISO 14001) [lo que indica que estas deben aplicarse en forma integral]"[22].

Si no se cuenta con una buena administración de la seguridad informática en las organizaciones, ya se sabe que el riesgo de daños y pérdidas asociados a la información y los datos se incrementa; por lo tanto, dentro de la estructura interna de la entidad, la Gerencia, según SGSIBlog[23] debe trazar políticas que respalden la seguridad informática en ella, la aplicación de la Norma ISO 27001 y el establecimiento de un Sistema de Gestión que debe abarcar toda la entidad con criterios de colaboración entre dependencias, sus jefes y su personal.

La gestión de la seguridad informática se debe realizar a través de un proceso continuo, complejo y dado a conocer a todos los miembros de la entidad, y a tal proceso se le conoce como su SGSI, que tiene como fundamento para su implementación la Norma NTC ISO 27001:2013.

Sólo así se puede tener un cierto (no total) nivel de protección de la información y los datos, porque con un SGSI se logran minimizar los riesgos, conocer los que se mantienen y estar alerta frente a ellos.

---

[22] ÁLVAREZ, Andrés y GÓMEZ FERNÁNDEZ, Ana. Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes. España. AENOR. 2009. 201p.

[23] SGSIBlog especializado en Sistemas de Gestión de Seguridad de la Información. ¿Qué objetivo persigue la seguridad de la información? 2017.

4.7.2. El Ciclo de mejora continua PDCA en el establecimiento de un SGSI

"También conocido como ciclo Deming, este ciclo se ha vuelto tradicional en su uso en los S.G.C. y ha demostrado ser muy eficaz a la hora de buscar garantizar una mejora continua en cualquier empresa o entidad.

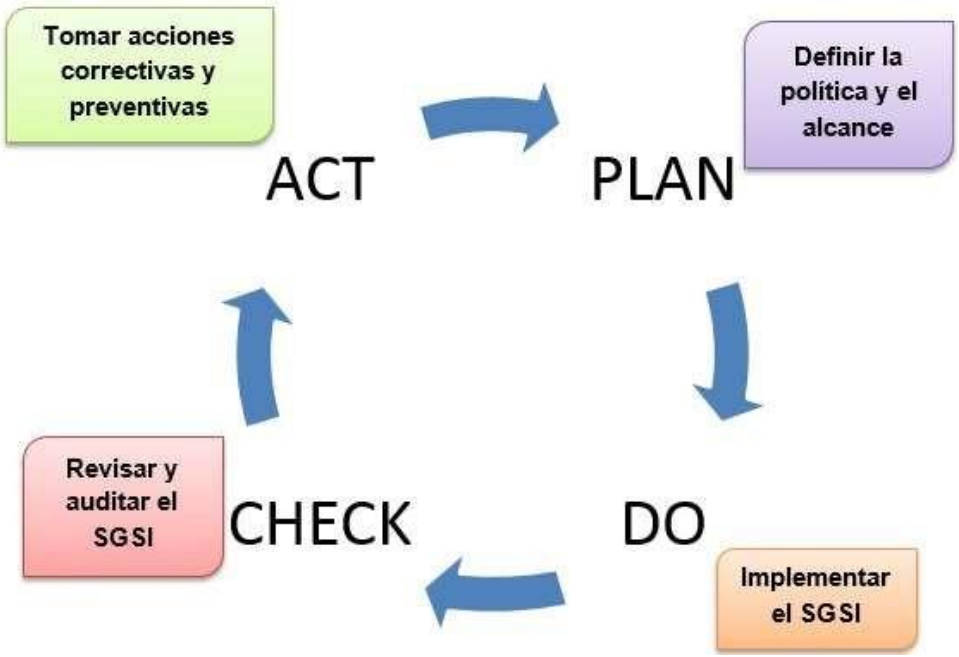
Este ciclo, cuya sigla significa Planificar – Hacer – Verificar – Actuar (Plan – Do – Check – Act, su significado en inglés), está conformado, como su nombre lo indica, por una sucesión de fases y acciones que permiten evaluar de forma cuantitativa el avance en la mejora de la empresa o entidad (ver Figura 3 Ciclo PDCA):

- Plan (planificar): En esta fase se planifica y diseña el SGSI, siguiendo un proceso de sistematización de las políticas de gestión que tenga la empresa o entidad.
- Do (hacer): Esta segunda fase corresponde ya a la implementación y puesta en funcionamiento del SGSI, a partir de los recursos con que se cuenta y que son necesarios para dicha implementación, y asignando responsabilidades en la ejecución de cada tarea.
- Check (verificar): La tercera fase equivale al monitoreo, evaluación y seguimiento del SGSI implementado. Es decir, que se verifica (audita) por esta vía que los objetivos se han estado alcanzando, las políticas y los procesos establecidos se han estado cumpliendo y las fallas se han estado identificando.
- Act (actuar): Corresponde a la última fase, en la cual se está garantizando que el SGSI no sólo funciona adecuadamente, sino que está en permanente mejora. En ella se emprenden, entonces, acciones de prevención y de corrección de fallas.

La aplicación del ciclo PDCA en una empresa o entidad conlleva el mensaje de que no es necesario pretender la implementación de un SGSI perfecto desde los inicios. La idea es que se diseñe e implemente un SGSI ajustado lo mejor posible a las realidades de la empresa, que incluya las mínimas medidas de seguridad que son indispensables en la protección de la información y que cumpla con la norma 27001, sin necesidad de consumir excesivos esfuerzos y recursos"[24].

[24] ÁLVAREZ y GÓMEZ. Op. cit., p. 14-15

Figura 3 CICLO PDCA



Fuente: Construcción propia a partir Guía de aplicación de la norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes.

4.7.3. Etapas de implementación de un SGSI

Se ilustran en la Figura 4, apoyados en la experiencia internacional, las etapas que se requieren para la implementación de un SGSI en una empresa o entidad.

Figura 4 Etapas de implementación de un SGSI

Fuente: Construcción propia a partir de documento Implementación de Sistema de Gestión de Seguridad de la Información (SGSI). Disponible en: https://portal.igp.gob.pe/sites/default/files/SGSI/presentacion_sgsi_otidg.pdf

4.8. METODOLOGÍAS Y HERRAMIENTAS PARA EL ANÁLISIS Y GESTIÓN DE RIESGOS

La gestión del riesgo de daño o pérdida de la información digital (riesgo informático) se rige por la Norma ISO 31000 de 2009, la cual establece los principios que se deben tener para garantizar una adecuada gestión del riesgo y la importancia de hacer un manejo de dicha gestión en todos sus aspectos organizacionales, entre otros.

De la aplicación de esta norma en toda organización pública o privada se desprende la necesidad de realizar un análisis de riesgos, vinculada al SGSI de la entidad. Al respecto, Novoa y Rodríguez plantean la necesidad de realizar:

> "unos importantes escaneos de vulnerabilidades mediante el uso de una serie de modelos y procesos para, así, proponer una forma más segura de cuidar la información y los recursos de TI. Algunos de los objetivos de las metodologías de análisis de riesgos corresponden a: planificación de la reducción de riesgos, prevención de

accidentes, visualización y detección de las debilidades existentes en los sistemas y ayuda en la toma de las mejores decisiones en materia de seguridad de la información.

En la seguridad de la información existen diversas metodologías de análisis de riesgos dentro de las que sobresalen: Octave, Magerit, Mehari, NIST SP 800:30 y Coras, Cramm y Ebios"[25].

4.9. POTENCIALES DIFICULTADES PARA LA IMPLEMENTACIÓN DE SGSI EN LAS UNIVERSIDADES PÚBLICAS EN COLOMBIA Y EN EL EJE CAFETERO

En los numerales anteriores de este capítulo se ha evidenciado la necesidad imperiosa que mantienen las organizaciones, y entre ellas las universidades públicas, de la adopción de una Política de gestión de la información y, consecuentemente, la implantación de un SGSI. El propósito de ello es básicamente el de garantizar y asegurar la CIA de los datos que posee y maneja la Universidad.

El estándar que se tiene establecido nacional e internacionalmente para esto es la aplicación y uso de la Norma ISO 27001, expedida en el año 2005 y actualizada en el 2013, con la cual se logra un eficiente SGSI, bajo el principio de que la información, los datos que existen en la Universidad, son activos claves en su funcionamiento transparente.

En efecto, se está aquí de acuerdo con lo expresado por ISOTools Excellence, cuando dice que los beneficios que aporta un SGSI en las universidades (públicas y privadas) son:

- "Análisis de los posibles riesgos, que permite la identificación de vulnerabilidades, impactos en la actividad universitaria y amenazas.
- Garantía y seguridad de la disponibilidad y continuidad del negocio.
- Disminución de los [costos] producidos por los incidentes en la institución.
- Aumento de la confianza del personal y del alumnado.
- Incremento del reconocimiento y prestigio de la universidad.
- Gestión de la seguridad en constante mejora.
- Intención de cumplir con la legislación actual para la salvaguarda de datos, servicios de la sociedad, propiedad intelectual, y comercio electrónico relacionados con la seguridad de la información"[26].

[25] ALEMÁN NOVOA, Helena y RODRÍGUEZ BARRERA, Claudia. Metodologías para el análisis de riesgos en los SGSI. En: Revista Especializada en Ingeniería - UNAD. Volumen 9. 2015.
[26] SGSIBlog especializado en Sistemas de Gestión de Seguridad de la Información. ¿Cómo influye ISO 27001 en las universidades? [en línea]. 2014.

Sin embargo, existen varias razones por las cuales se vislumbra una deficiente gestión de la seguridad de la información (incluyendo, como consecuencia, escasa existencia de SGSI) en las universidades públicas en Colombia -y entre ellas las del Eje Cafetero- pero la razón fundamental apunta al crónico déficit presupuestal que se mantiene con motivo de la expedición y vigencia de la conocida Ley 30 de 1992 (y que ha sido bandera en las protestas adelantadas por estas universidades en octubre de 2018 y otras en fechas más recientes, amén de otras similares en el pasado). De ella se desprenden inevitablemente otras razones, como:

- Falta de equipos y herramientas para la implementación de un SGSI
- Falta de personal especializado en seguridad informática (nóminas congeladas desde la década de los noventa)
- Falta de adecuaciones en el espacio universitario para atender necesidades en este sentido del SGSI
- Algunos pocos casos que pudieran darse de negligencia administrativa al interior de las instituciones.

Este panorama amerita estudios como el que aquí se está presentando, lo que reafirma su justificación.

5. REFERENTES PARA ESTE ESTUDIO EN OTROS PAÍSES Y EN COLOMBIA.

En la pesquisa realizada se encuentran documentos que relacionan algunas experiencias tenidas por universidades públicas y privadas en Colombia y en Cuba, de las cuales se extractan aquí los aspectos más destacables en cuanto a lo que en ellas se ha planteado sobre su gestión en seguridad informática. Son ellas, la Universidad de Holguín (estatal, Cuba), la Universidad del Atlántico (pública, Colombia), la Universidad de Los Llanos (pública, Colombia) y la Universidad Libre (privada, Colombia).

5.1. UNIVERSIDAD DE HOLGUÍN, CUBA

Investigadores de la institución realizaron en la Universidad de Ciencias Médicas de Holguín (Cuba)[27] una investigación que llevó a la Universidad a contar, parafraseando a los autores, con una herramienta informática de apoyo para la gestión de reportes de incidentes, para la protección de los medios informáticos y para la formación de sus funcionarios en seguridad informática.

5.2. UNIVERSIDAD DEL ATLÁNTICO, COLOMBIA

Esta Universidad pública del caribe colombiano (sede en Barranquilla) es una de las primeras en el país en adelantar acciones concretas para implementar un SGSI, en su búsqueda de proteger y garantizar la eficacia y veracidad de la información, el tratamiento de datos personales y el buen uso de los recursos públicos.

En ese proceso, definió el alcance y los límites de su SGSI, promulgó su política (2014) que incluyó en su Sistema Integrado de Gestión SIG, y elaboró su manual de Seguridad y Política de Informática, el cual fue socializado ante la comunidad universitaria. Para ello, acogió los requisitos de la Norma ISO/IEC 27001.

Al respecto, plantea en sus documentos los siguientes beneficios que aporta el implementar un SGSI:

- “Análisis de riesgos, identificando amenazas, vulnerabilidades e impactos en la actividad educativa, administrativa y comercial.
- Mejoramiento continuo en la gestión de la seguridad.

[27] DÍAZ RICARDO, Yanet; PÉREZ-DEL CERRO, Yunetsi y PROENZA PUPO, Dayami. Op. cit., p.

- Garantizar la continuidad, seguridad y disponibilidad de la información en nuestra institución educativa.
- Reducción de los costos vinculados a los incidentes.
- Incremento de los niveles de confianza de la comunidad universitaria, clientes y proveedores.
- Aumento del valor comercial y mejora de la imagen institucional.
- Cumplimiento con la legislación vigente de protección de datos de carácter personal, comercio electrónico, propiedad intelectual y en general, relacionada con la seguridad de la información"[28].

5.3. UNIVERSIDAD DE LOS LLANOS, COLOMBIA

La Universidad de los Llanos (pública, con sede en Villavicencio) divulga en 2013 un documento borrador de su Manual del SGSI en el cual: "expone los lineamientos sobre el uso y aprovechamiento de las tecnologías de la información y las comunicaciones de la Universidad por parte de sus administradores, usuarios y terceros, integra estos esfuerzos y da una visión global a la Universidad en materia de seguridad de la información, entre otros propósitos" [29].

5.4. UNIVERSIDAD LIBRE, COLOMBIA

La Universidad Libre[30]: "(privada, sede principal en Bogotá) empieza en el 2009 a implementar un Modelo de Seguridad de la Información con el fin de establecer una cultura de la seguridad informática en la Universidad, a la vez que, a desarrollar un protocolo para el aseguramiento de los activos de información de esa institución, que garantice los tres puntos fundamentales dentro de la seguridad de la información: integridad, disponibilidad y confidencialidad. Para ello, establece un Comité de seguridad con funcionarios de la institución".

5.5. METODOLOGÍA DE IMPLANTACIÓN DE UN SGSI EN UN GRUPO EMPRESARIAL JERÁRQUICO. TESIS DE MAESTRÍA, URUGUAY

Pallas M.:

[28] UNIVERSIDAD DEL ATLÁNTICO. Alcance del SGSI Universidad del Atlántico. [en línea]. 2016.
[29] UNIVERSIDAD DE LOS LLANOS. Manual del Sistema de Gestión de Seguridad de la Información (SGSI). [en línea]. 2013.
[30] UNIVERSIDAD LIBRE. Nuestro Sistema de Gestión de Seguridad de la Información (SGSI). [en línea]. 2009.

> "elabora una tesis de maestría para: dar lineamientos metodológicos, de aplicación sistemática para el diseño, implantación, mantenimiento, gestión, monitoreo y evolución de un SGSI según la norma ISO 27.001, para una empresa perteneciente a un grupo empresarial, la cual además está subordinada con respecto a una empresa principal del grupo. Además, se ilustra con un Caso de Estudio, los principales aspectos de aplicación de esta"[31].

Un aspecto interesante del estudio es que se realiza para una empresa subordinada o que hace parte de un grupo empresarial jerárquico, donde otra empresa se denomina principal.

La metodología que se propone en esta tesis de Pallas M.:

> "tiene un amplio campo de aplicación, donde exista una relación de dependencia o integración vertical entre empresas. También puede aportar aspectos metodológicos, en lo referente a la jerarquización de los lineamientos de seguridad, para una entidad gubernamental en su rol de regular o generar lineamientos y/o (meta) políticas en seguridad de la información para empresas y organismos estatales"[32].

5.6. CIBERSEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN DE LAS UNIVERSIDADES

Como lo dice Carlos E. Anchundia-Betancourt: De este interesante artículo de revista (Anchundia) se quiere resaltar el texto de uno de sus párrafos en donde se detalla muy bien la familia de normas ISO 27.000. En efecto, el autor plantea que:

> "con el uso de las normas internacionales para los Sistemas de Gestión de Seguridad de la Información (SGSI), las organizaciones pueden desarrollar e implementar un marco para gestionar la seguridad de sus activos de información y preparar la evaluación independiente de su SGSI en materia de seguridad de la información, y, además, pueden ser usadas por las organizaciones para prepararse ante una evaluación independiente de su SGSI aplicada a la protección de la información (ISO, 2016). En esta familia de normas, además de la 27.000 que presenta una descripción general y terminología, la 27.001 y 27.006 que especifican requisitos, la 27.002, 27.003, 27.004 y 27.005 que describen directrices generales, y las 27.010, 27.011 que describen directrices especificas generales, entre muchas otras, se destaca la norma 27.0032 (ISO, 2012), que aborda la seguridad del Ciberespacio o cuestiones de Ciberseguridad que se concentran en tender puentes entre los diferentes vacíos del

[31] PALLAS, op. cit, p. 2
[32] Ibíd., p. 3

Ciberespacio; en particular, proporciona una guía técnica para abordar riesgos de Ciberseguridad comunes”[33].

[33] ANCHUNDIA, Carlos. Ciberseguridad en los sistemas de información de las universidades, Revista Científica - Dominio de las Ciencias, ISSN: 2477-8818, Vol. 3, agos. 2017, p. 200-217.

6. PORQUÉ SE JUSTIFICA IMPLEMENTAR UN SGSI EN LAS UNIVERSIDADES.

Para poder conocer más a fondo sobre la conveniencia de la implementación de un SGSI en las universidades es necesario, primero, saber la importancia que este tiene, la cual se enfoca en la trascendencia que ha adquirido todo lo relacionado con las TIC's en el mundo de hoy. Ya muchas de las actividades diarias en cualquier empresa se encuentran ligadas al manejo de equipos de cómputo, de las redes y del uso de telecomunicaciones. Gestionar los servicios de las TIC's se ha vuelto una necesidad para poder realizar las actividades de forma más rápida y práctica y las Universidades tanto públicas como privadas no pueden ser ajenas a esta situación. Si lo que buscan las empresas y entre ellas las universidades públicas del Eje Cafetero es ser cada vez más eficientes, deben ir a la vanguardia del mundo moderno. Es allí donde el implementar un SGSI a partir de la Norma ISO 27001 les va a ayudar a dar el valor que la información se merece como un activo sumamente importante que, si se pone en peligro, puede llevar a tener pérdidas incalculables para las universidades. Esto generará un trabajo más eficiente con la información dentro de las mismas, y garantizar un éxito total. En resumen, todas las universidades tanto públicas como privadas deben garantizar con la implementación de un SGSI que la información sea confiable, íntegra y que se encuentre disponible en el momento en que se necesite.

Los beneficios que trae la implementación de un SGSI dentro de las universidades serían, entre otros:

- A partir del análisis de riesgos se pueden identificar las vulnerabilidades y verificar los impactos que se presentan por las actividades realizadas por toda la comunidad universitaria, que puede generar diferentes amenazas y poner en peligro la información como activo primordial.
- A partir de la correcta implementación del SGSI es posible garantizar en su totalidad que la información se encuentre disponible en cualquier momento, que se encuentre segura y que por lo tanto la Universidad puede realizar sus actividades sin tropiezos y tanto con seguridad como con garantía de la disponibilidad y continuidad del negocio.
- Al tener implementado el SGSI se disminuyen en su mayoría las posibilidades de incidentes, lo que se puede traducir en la disminución de costos producidos por ataques informáticos que pueden llevar a pérdidas de información y por lo tanto a pérdida de dinero, entre otros.
- También, ayuda a mejorar la percepción que tiene toda la comunidad universitaria frente a, por ejemplo, la navegación (internet e intranet), ya que de esta manera se asegura la información personal y se evitan problemas a profesores, alumnos y comunidad en general.

En otras palabras, a partir de la implementación del SGSI se puede garantizar la constante mejora de la SI dentro de la universidad.

Adicionalmente, es necesario destacar que la implementación del SGSI debe tener una mejora continua, cada cierto tiempo es necesario hacer una revisión y, posterior a ello, se deben tomar correctivos que ayuden a mejorar aquellas cosas en las que se encontraron falencias, con el fin de poder tener cada vez un SGSI más eficiente. Así, la información se encuentra a salvo de personas inescrupulosas que quieren obtener beneficios con ataques informáticos. Para poder garantizar un SGSI eficiente es necesario estar revisando cosas como la política de seguridad y sus objetivos, los resultados obtenidos de las auditorías realizadas, entre otros, pero además se debe garantizar que todo lo anterior ayude a lograr el alcance que se había planteado a partir de todas las actividades de la universidad a la que se le está aplicando el SGSI.

Por último, es bueno reiterar por qué es importante implementar un SGSI con el fin de mejorar la seguridad de la información dentro de las universidades y es ahí donde debemos tener en cuenta que con este se puede ahorrar tanto tiempo como dinero; lo que pareciera estar pasando realmente en nuestro tiempo es que muchos directivos de las empresas consideran que no es tan prioritario invertir dinero en el tema de la seguridad informática porque existen otros temas más urgentes, pero se equivocarían en esa apreciación porque la información es uno de los activos más importantes que tiene cualquier empresa; quizás lo que sucede es que no hay dentro de las empresas una persona idónea para liderar este asunto y ayudar a los directivos a tomar decisiones acertadas que procuren que la información esté siempre resguarda, protegida (por ejemplo, que no tenga cambios que la puedan afectar, que se encuentre siempre disponible, o sea, que no se tengan problemas cuando esta se deba consultar, por ejemplo, por un ataque de DoS, entre otros).

Es de vital importancia para cualquier empresa o entidad garantizar que la información siempre va a estar disponible y completa, a fin de ayudar a que todos los usuarios de ella se sientan de una u otra manera mucho más seguros a la hora de, por ejemplo, usar la red Wifi de una universidad.

Una opción para lo anterior es hacer una combinación de empleados con expertos externos. Es bueno implantar el estándar internamente, pero un experto externo puede realizar una guía paso a paso de todo el proceso completo. Esta es una buena opción si se quieren obtener los conocimientos necesarios para implantar un SGSI y tener la seguridad de que no se hace nada mal en el desarrollo del proceso.

Realmente, existe un eslabón muy débil en esta cadena y debe ser reforzado: el usuario, ya que muchos de ellos nunca toman ni la más mínima precaución para resguardar la información y por ello la ponen en riesgo todo el tiempo. Una de las medidas que se debe tomar en cuenta al implementar una política de seguridad debe ser la de capacitar a todos los usuarios para que aprendan a manejar mejor todos los canales de comunicación que pueden perjudicar la información. Este es sólo un ejemplo de lo importante que puede ser el manejar bien la seguridad de la información dentro de las universidades, ya que se podría pensar que la información que se tiene en ellas puede no ser tan relevante y que quizás los atacantes buscan peces más grandes, pero eso no es del todo cierto, hay algunos que hasta pueden llevar a cabo ataques por el solo hecho de divertirse un poco, lo que puede poner en grave peligro información confidencial. Mientras más preparadas se encuentren las universidades para evitar ataques de tipo informático, mejor guardada estará su información y por lo tanto menos peligro podrá correr esta.

Concretando esta última idea, una buena forma de implementar un SGSI dentro de una universidad puede ser contratando a algún especialista en el tema de la seguridad informática que maneje la norma correspondiente, la ISO 27001. Él cuenta con todos los conocimientos para ello. De nada sirve intentar hacer algo si aquellos que lo hacen no tienen conocimientos en el tema y por tal motivo se la pasan cometiendo errores que pueden generar pérdidas de tiempo y dinero, además de otras pérdidas.

7. LAS UNIVERSIDADES Y EL ÁNALISIS DE LA LEY COLOMBIANA 1273 DE 2009.

Hasta el momento seguimos legislados por la Ley 1273[34] del 2009, la cual es denominada “De la protección de la información y los datos”. Realmente, es difícil pensar que durante estos 10 años que han pasado no se han hecho modificaciones a esta ley; los delitos informáticos han ido en aumento y, adicionalmente, se han creado otros que no existían en esa época. Es necesario pensar como profesionales de seguridad informática lo importante que es que la ley esté actualizada frente a los delitos que se pueden ir presentando, ya que esta es una herramienta que puede ayudar a resolver casos delictivos complejos en donde los autores pudieran salirse con la suya si no se tienen suficientes elementos para poder judicializar a los delincuentes que los cometen. Revisando bibliografía referente a la Ley 1273 del 2009, se encontró un documento - monografía que habla del ANÁLISIS DE LA LEY 1273 DE 2009 Y LA EVOLUCIÓN DE LA LEY CON RELACIÓN A LOS DELITOS INFORMÁTICOS EN COLOMBIA, en donde Sánchez, su autora, concluye lo siguiente:

> “se realizó un análisis de las sentencias de ley SP1245-2015 y 34564 emitidas sobre la Ley 1273 de 2009, dentro del marco de apoyo para continuar con el análisis de la evolución de la misma frente al constante crecimiento de los delitos informáticos en Colombia. Este análisis permitió determinar que en realidad en Colombia hacen falta muchas herramientas o bienes jurídicos, que puedan adaptarse a la constante evolución de la cibercriminalidad, sus técnicas y nuevos métodos”[35].

Después de leer esta monografía y revisar todo lo que allí se plantea se pudo concluir que realmente la normatividad vigente sobre los delitos informáticos en nuestro país no se encuentra actualizada y que por tal motivo es factible que muchos delincuentes informáticos no reciban el castigo que se merecen porque los jueces finalmente no van a tener las suficientes herramientas para poder judicializarlos y de esa manera dar penas ejemplares que pudieran poner a pensar a otros que tengan la intención de cometer esos mismos delitos. Adicionalmente, la ley no es muy clara y puede prestarse para confusiones, porque las personas que las manejan son personas que dominan el tema jurídico, pero no son profesionales en seguridad informática, y les harían falta mejores herramientas para evaluar los delitos y decidir las penas que se pueden imponer por cometerlos.

Al plantear un análisis de la Ley 1273 de 2009 enfocado a las universidades del país para saber cuáles de los delitos informáticos mencionados en ella están ligados a

---

[34] MINTIC. Ley 1273 de 2009. (05 de 01 de 2009). Bogotá, D.C. 2009. p. 4.

[35] SANCHÉZ CASTILLO, Zulay. Análisis de la Ley 1273 de 2009 y la evolución de la ley con relación a los delitos informáticos en Colombia. Chiquinquirá. 2017.

las universidades públicas del Eje Cafetero se sabría cómo pueden afectarlas, aún más si estas no están blindadas frente a los delincuentes informáticos y sus ganas de obtener beneficios de los vacíos que las universidades pueden tener en el tema de la seguridad informática.

A continuación, se van a mencionar los artículos de esta ley y se va a dar una breve explicación de cada uno frente a lo que podría suceder dentro de las universidades si hipotéticamente se presentaran ataques informáticos relacionados con dichos delitos. Una reflexión que se puede hacer en este tema es que las universidades que no tienen aún implementado un SGSI se encuentran mucho más vulnerables que aquellas que sí lo tienen frente a los delitos informáticos, y esto se debe a que la información se encuentra más expuesta y por lo tanto es mucho más fácil de manipular, secuestrar, entre otros.

Es de reconocer que nuestro país ha emprendido acciones para subsanar los problemas que se derivan de los ataques informáticos por parte de delincuentes que no tienen ningún tipo de escrúpulos, a partir de la toma de decisiones penales que buscan judicializar a los involucrados en algún tipo de delito informático, pero, evidentemente, aún falta.

Un antecedente interesante de mencionar al respecto es el de la promulgación de leyes en diferentes países del mundo (anteriores a la colombiana) para poder tener herramientas que ayudaran a aminorar los ataques informáticos, las cuales propiciaron el que durante el año 2001 se realizase en la ciudad de Budapest el Primer Convenio Mundial sobre Ciberdelincuencia, pero que entró en vigencia en julio de 2004.

Para el tema y a nuestro parecer, el capítulo I de la ley 1273 es el más importante, porque es el que habla de la integridad, disponibilidad y confidencialidad de la información. Este capítulo tiene varios artículos que vale la pena evaluar y analizar a continuación en cuanto a su relación con las universidades, sean estas públicas o privadas:

- “Artículo 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo[...]”[36].

[36] MINTIC. Ley 1273. Op. cit., p. 1

Las universidades se pueden ver altamente afectadas si un delincuente decide realizarles un ataque de este tipo, ya que podría afectar gravemente toda la información de estas, con grandes pérdidas; por ejemplo, interceptar información vital de las universidades (correos electrónicos cruzados entre altos cargos -Rector, Vicerrector-, notas de los estudiantes, promedios, etc.); esta información posteriormente podría ser utilizada por el delincuente y manipulada para modificar las disposiciones que se han tomado inicialmente. En este sentido, se puede atacar la confidencialidad de la información y podría verse afectada también la integridad de los datos.

- "Artículo 269B. OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones[...]"[37].

En este sentido, es factible que un delincuente realice un ataque de DoS, lo que puede acarrear el mal funcionamiento de los servicios, ya que los usuarios no pueden acceder a ellos de forma normal; un ejemplo puede ser que la comunidad universitaria en general no pueda acceder al correo electrónico. Esto puede generarle contratiempos a dicha comunidad. Pero ese es solo un ejemplo, ya que se podrían presentar otras situaciones que de igual forma afecten el funcionamiento de las universidades y que puedan generar pérdidas.

- "Artículo 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte[...]"[38].

Este delito se puede dar en las universidades porque algún inescrupuloso puede intentar obtener información de tipo confidencial, por ejemplo, de las bases de datos que manejan información, como notas de alguna materia específica, con el fin de posteriormente vender a estudiantes que hayan perdido dicha materia la idea de que se pueden cambiar las notas en el sistema. De esa manera, ellos habrán pasado la materia y el delincuente habrá obtenido dinero por ello. Esto puede ser crítico para la universidad porque se estará modificando información sumamente importante. Aquí se ve afectada la confidencialidad de la información, pero además podría afectarse la integridad.

[37] MINTIC, Ley 1273. Op. cit., p. 1

[38] Ibít., p.1

- “Artículo 269D. DAÑO INFORMÁTICO. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos[...]”[39].

En este caso, un buen ejemplo podría ser el del interés de un inescrupuloso en alterar el presupuesto de una Universidad a fin de favorecer un rubro frente a otros o de efectuar un fraude. Es, evidentemente, un delito que perjudica la integridad de la información y hace que se pierda su confidencialidad porque alguien pudo acceder a ella.

- “Artículo 269E. USO DE SOFTWARE MALICIOSO. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos[...]”[40].

Los usuarios de los correos electrónicos institucionales de las universidades pueden ser objeto de correos maliciosos infectados con algún tipo de malware que pueden estar buscando infectar los dispositivos de los usuarios y de esa forma obtener información confidencial de la posible víctima. Este tipo de delito puede no ser crítico, pero puede afectar el correcto funcionamiento del correo electrónico institucional.

- “Artículo 269F. VIOLACIÓN DE DATOS PERSONALES. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes[...]”[41].

En las universidades, esto podría afectar la propiedad intelectual de algunos miembros de la comunidad universitaria que realizan trabajos de tipo académico y/o investigativo, por ejemplo, escribiendo libros, artículos, entre otros y que pueden ser modificados, o robados con el fin de lucrarse de alguna manera de dicha información obtenida de forma ilícita. En este delito se podría ver afectada la integridad de la información porque esta puede ser modificada para lucrar al delincuente informático.

[39] MINTIC, Ley 1273. Op. cit., p. 1
[40] Ibít., p. 1
[41] Ibít., p. 1

- “Artículo 269G. SUPLANTACIÓN DE SITIOS WEB PARA CAPTURA DE DATOS PERSONALES. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes [...][42].

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave. La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito” **[43]**.

Se considera aquí, por el momento, que este tipo de delito no se debe estar presentando en las universidades porque los encargados del área de sistemas deben tener algunas políticas de seguridad que ayuden a aminorarlo. Por tal motivo, se llega a la conclusión de que este delito tiene una muy baja posibilidad de que se presente y por lo tanto no se va a tener en cuenta dentro del estudio.

Hasta aquí, los delitos detallados en el capítulo I de la ley que la autora considera más importantes de relacionar con las universidades.

NOTA: Todos los delitos mencionados anteriormente manejan una pena de prisión; claro está que cada caso es particular y dicha pena está estipulada a partir del delito cometido.

Sin embargo, existen otros delitos detallados esta vez en el capítulo II de la misma ley que vale la pena analizar. Son ellos:

- “Artículo 269I. HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos[...]”[44].

[42] MINTIC, Ley 1273. Op. cit., p. 2
[43] Ibít., p. 2
[44] Ibít., p. 2

En este caso, podemos encontrar que varias de estas conductas se pueden presentar en las universidades del país, un ejemplo de ello es un ataque por medio de malware, como se había mencionado anteriormente. Otro ejemplo es la manipulación de información, lo que hace que esta pierda su integridad; en este caso se puede mencionar lo que sucedió con la Universidad de Caldas y el ICFES, donde se modificaron datos para que algunos estudiantes pudieran acceder a la Facultad de Medicina de dicha Universidad.

- “Artículo 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave [...]. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa” [45].

Se detalla aquí con el propósito de analizar si tal vez este delito ya fue definido y establecida su sanción en el Artículo 269E. USO DE SOFTWARE MALICIOSO del capítulo I. De ser así, amerita mayor análisis de la mano de los juristas.

NOTA: Para consultar en su totalidad la Ley 1273 de 2009 remítase al Anexo A de este documento.

[45] MINTIC, Ley 1273. Op. cit., p. 2

8. ESTADO DEL ARTE DE LA SEGURIDAD INFORMÁTICA EN LAS UNIVERSIDADES PÚBLICAS DEL EJE CAFETERO.

8.1. INFORMACIÓN GENERAL SOBRE LAS CINCO UNIVERSIDADES

Las universidades públicas del Eje Cafetero fueron fundadas en distintos momentos históricos y desde entonces han estado brindando servicios académicos de transcendencia para el desarrollo de la región a partir de la formación de jóvenes en distintos saberes y disciplinas, de actividades investigativas generadoras de conocimiento nuevo y de prestación de servicios al medio en procura de soluciones a problemas locales y regionales. En este capítulo de la monografía se quiere dar un vistazo resumido a partes de lo anterior, con el fin de contextualizar histórica, académica y organizativamente esas universidades e irse acercando a lo relacionado con el asunto tema, es decir, con la manera como se organiza y se enfrenta en ellas (a partir de una dependencia encargada) la seguridad informática de un bien tan preciado como es la información. Se presentan enseguida las cinco universidades, una a una.

8.1.1. Universidad Nacional de Colombia.[46]

Se considera como el padre de esta universidad al intelectual, humanista y político colombiano José María Samper Agudelo, quien impulsó su creación en 1984. En 1867 se expidió la ley que finalmente la fundó, inicialmente en Bogotá.

- Otras sedes de la Universidad Nacional de Colombia

Además de la sede central en Bogotá, cuya reseña se tiene en los párrafos anteriores, desde 1936 la Universidad Nacional de Colombia emprendió la tarea de crear otras sedes en el territorio nacional, lo cual ha logrado de manera importante con ocho (8) de ellas, así:

- Sede Medellín: En 1936.
- Sede Palmira: En 1946.
- Sede Manizales: En 1948.
- Sede Amazonía: En 1994.
- Sede Orinoquía: En 1996.
- Sede Caribe: En 1997.

[46] Universidad Nacional de Colombia. Historia. [en línea]. 2018.

- Sede Tumaco: En 1997.
- Sede de La Paz: En 2017.

 La Universidad Nacional de Colombia – Sede Manizales[47]

Fue creada, como ya se dijo, en el año 1948 en la ciudad de Manizales bajo la rectoría en Bogotá de Gerardo Molina, inicialmente como Facultad de Ingeniería.

El primer programa de pregrado abierto fue el de Ingeniería Electromecánica que, un año después, cambió su currículo por el de Ingeniería Civil.

Entre los años 1965 y 1970 se crearon otros programas, también de pregrado, como los de Administración de Empresas, Arquitectura, y nuevas ingenierías, Química, Industrial y Eléctrica.

Más adelante, en 1988, la sede Manizales de la Universidad Nacional de Colombia adquirió la categoría de Vicerrectoría, con dos facultades, Administración e Ingeniería y Arquitectura y Ciencias (que evolucionaron ya en este siglo a tres).

En la década de los 90 esta sede tuvo un gran impulso con la creación de nuevos programas de pregrado y posgrado, como las carreras de Ingeniería Electrónica y Administración de Sistemas Informáticos, varios programas de especialización en áreas de la Ingeniería Civil e Ingeniería Química, varias Maestrías y otros programas en el área de Administración. Igualmente, fue creado el capítulo Manizales del Instituto de Estudios Ambientales IDEA, único -hasta ahora- Instituto intersedes de la Universidad Nacional de Colombia (en cuatro (4) de sus sedes).

Y a principios del nuevo siglo, se crean nuevas carreras como Ingeniería Física, Matemáticas y Gestión Cultural y Comunicativa, mientras se consolidaban programas de posgrado a nivel de especialización, Maestría y Doctorado en distintas ramas del saber, apoyada en su fortalecimiento profesoral con la incorporación de profesores con nivel de formación doctoral, la mayor infraestructura de laboratorios especializados y el surgimiento de nuevos grupos de investigación cada vez mejor categorizados por Colciencias (Departamento Administrativo de Ciencia, Tecnología e Innovación) en Colombia. Esta sede posee tres (3) campus que son:

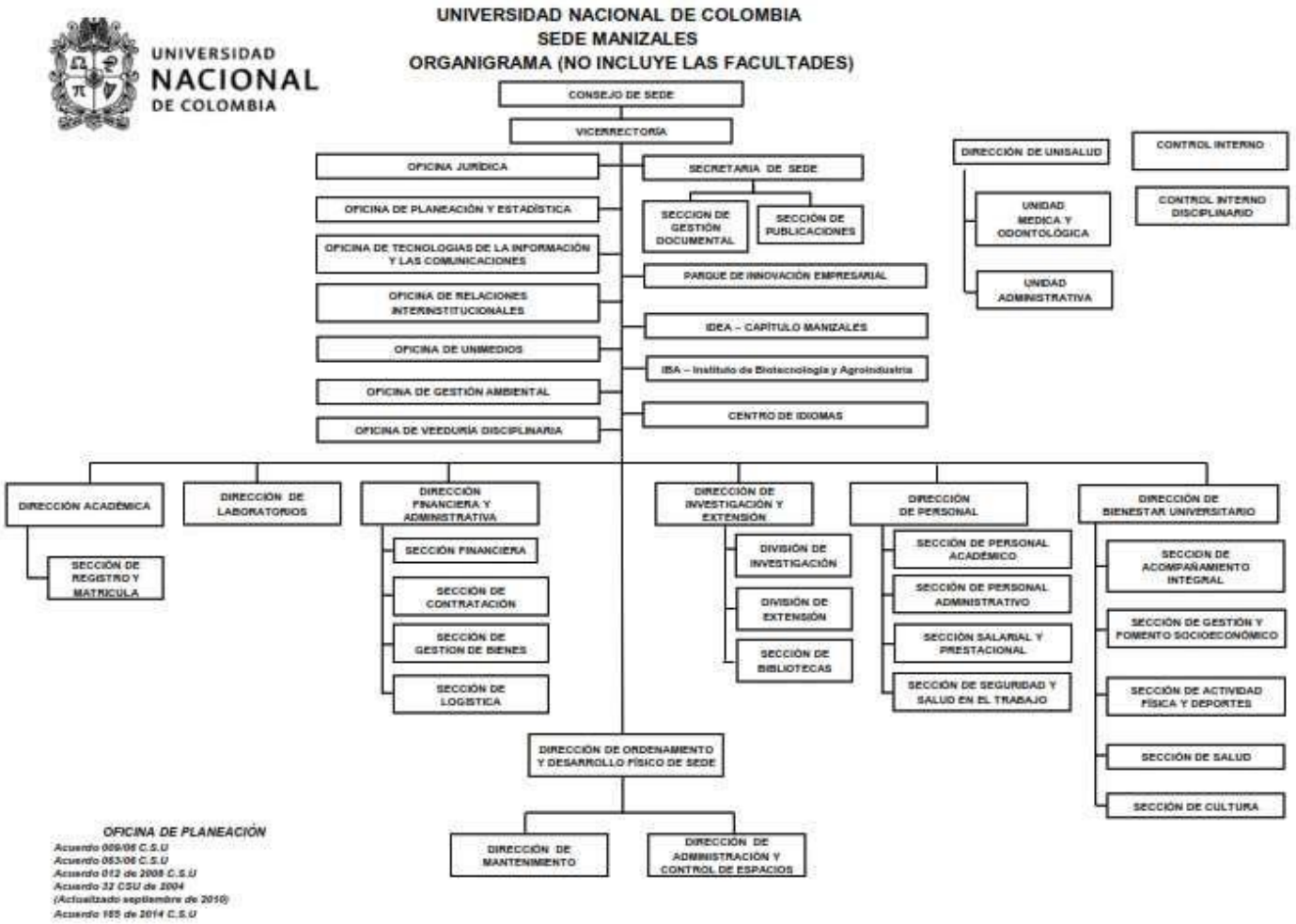
[47] Universidad Nacional de Colombia – Sede Manizales. RESEÑA HISTORICA. [en línea]. 2017.

- Campus Palogrande, carrera 27 No. 64 – 60
- Campus El Cable, antigua sede del cable aéreo Manizales – Mariquita, Avenida Santander y Avenida Lindsay, esquina (Calle 65 No. 23 – 29).
- Campus La Nubia, contiguo al Aeropuerto La Nubia de Manizales.

 Estructura organizacional de la UNAL sede Manizales.

Se presenta en la Figura 5 la estructura organizacional de la Universidad Nacional de Colombia en su sede de Manizales, desde la Vicerrectoría (recordemos que la Universidad tiene un solo rector (a) –actualmente la Dra. Dolly Montoya-, y en la sede Manizales la máxima autoridad académico – administrativa es el Consejo de Sede como cuerpo colegiado y el Vicerrector), pues en este organigrama es en donde aparece la Oficina de Tecnologías de la Información y las Comunicaciones, dependencia en la cual se desarrollarían las actividades que están relacionadas con la seguridad informática y en la cual se busca la información detallada sobre ello.

Figura 5 Estructura organizacional Universidad Nacional de Colombia – Sede Manizales.



Fuente: Página web Universidad Nacional de Colombia. Disponible en: http://www.manizales.unal.edu.co/menu/institucional/organigrama/. 2019

8.1.2. Universidad de Caldas.[48]

Fue creada en Manizales como Universidad Popular inicialmente, en 1943.

A mediados de los años cincuenta del siglo XX aparecen los programas de pregrado de Agronomía, Veterinaria, Derecho, Medicina, Escuela de Bellas Artes y Filosofía y Letras.

En el año 1966 el departamento de Caldas se escinde en tres: (Caldas, Risaralda y Quindío) y esto da pie para que la Universidad de Caldas, hasta entonces del orden departamental, pasara a ser del orden Nacional (1967).

En la década de los setenta se crean la Facultad de Enfermería y la de Geología y Minas.

En 1989 se crea el programa de Educación Física y Recreación y en 1990 el Programa de Diseño Visual.

Más adelante, en 1994, se crean los programas de Ingeniería de Alimentos y Tecnología de Sistemas Informáticos.

Finalmente, en 1995 se aprueban cambios académico-administrativos en la universidad que dan origen a que los diferentes programas académicos se agrupen en seis grandes Facultades, a saber: Ciencias para la salud, Ingeniería, Ciencias agropecuarias, Ciencias exactas y naturales, Artes y humanidades y Ciencias jurídicas y sociales.

La Universidad de Caldas posee varios Campus y espacios Institucionales en Manizales, a saber:

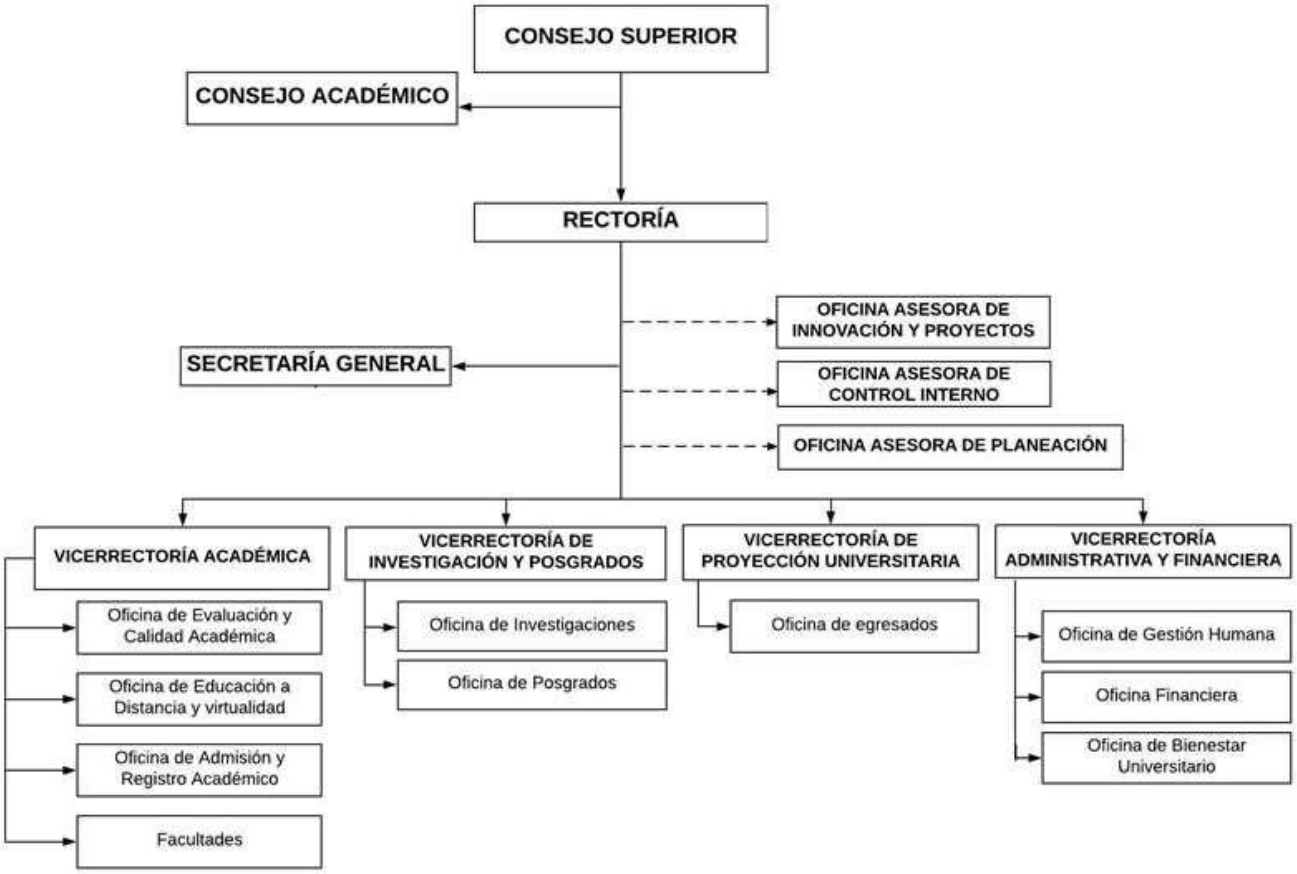
- Sede Principal, ubicación: Calle 65 No 26-10
- Sede Bellas Artes, ubicación: Carrera 21 No 13-02 Av. 12 de octubre
- Sede Palogrande, ubicación: Carrera 23 No 58-65
- Sede Sancancio, ubicación: Carrera 35 No 62-160
- Sede Versalles, ubicación: Carrera 25 No 48-57

[48] Universidad de Caldas. Historia de la Universidad. [en línea]. 2019.

☐ Estructura organizacional de la Universidad de Caldas

Encabezada por los Consejos Superior y Académico y por el Rector. La dependencia que se encargaría de los asuntos de la seguridad informática sería la Oficina de Planeación y Sistemas, hacía la cual se dirigen las pesquisas sobre ello. Enseguida, la Figura 6 con dicha estructura:

Figura 6 Estructura organizacional Universidad de Caldas.



Fuente: Página web Universidad de Caldas. Disponible en: http://www.ucaldas.edu.co/portal/estructura-organica-organigrama/. 2019.

8.1.3. Universidad Nacional Abierta y a Distancia – UNAD[49].

La Universidad Nacional Abierta y a Distancia (UNAD) nació en 1981 con el nombre de Unidad Universitaria del Sur de Bogotá, UNISUR durante la

[49] Universidad Nacional Abierta y a Distancia. UNAD. Reseña histórica. [en línea]. [2019].

presidencia de Belisario Betancur, considerada como un establecimiento público del orden nacional adscrito al Ministerio de Educación Nacional, y luego se transforma, en 1997, en la Universidad Nacional Abierta y a Distancia UNAD.

En el 2005 la UNAD fue reconocida legalmente como Universidad y en el 2006 como establecimiento público de carácter nacional adscrito al Ministerio de Educación Nacional.

Luego, en el 2009 y 2012 la Universidad recibe sus certificados de calidad en la norma en Gestión Pública NTCGP 1000 y en la Norma Técnica en Calidad NTC ISO 9001.

En 2012 la UNAD recibe Alta Acreditación por parte del Ministerio de Educación Nacional para cinco programas: Comunicación Social, Licenciatura en Etnoeducación, Zootecnia, Ingeniería de Sistemas y Administración de Empresas.

En la Figura 7 se muestran las múltiples seccionales de la UNAD en Colombia y en USA (Florida), que cubren distintas zonas del territorio nacional, entre ellas la zona Occidente (nodo zonal CEAD) donde se encuentra ubicada la sede Dosquebradas (asiento de la especialización en Seguridad Informática cursada por la autora de esta monografía):

Figura 7 **Mapa sedes Universidad Nacional Abierta y a Distancia - UNAD**

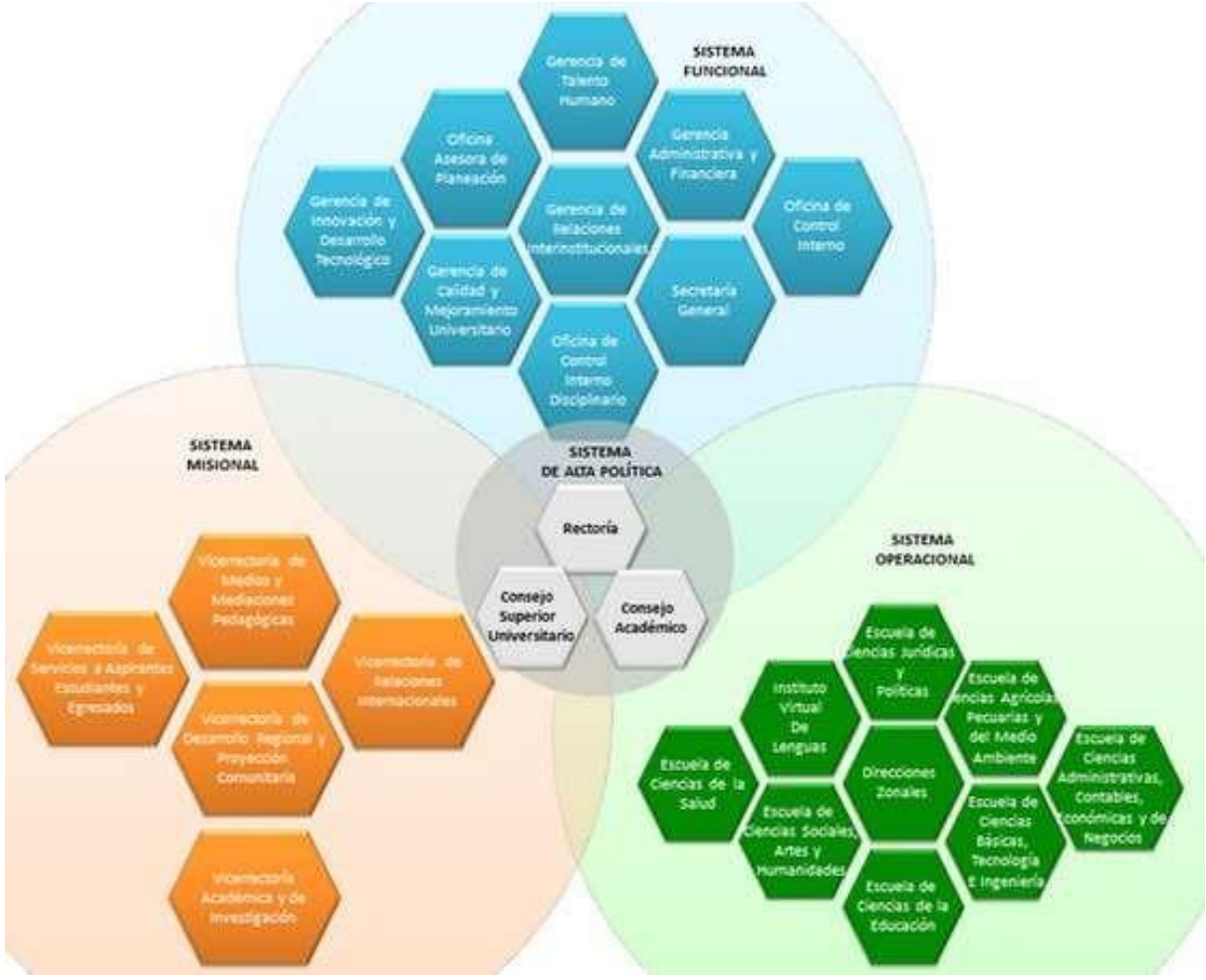
Fuente: Página web UNAD. Disponible en: https://directorio.unad.edu.co/images/mapa/Mapa_centros_UNAD_2017.pdf.

☐ Estructura organizacional de la UNAD.

Aquí también (ver Figura 8) la máxima autoridad académico – administrativa la constituye el Consejo Superior y el Consejo Académico, junto al Rector.

Luego, se tienen varias vicerrectorías y varias escuelas. La Oficina Asesora de Planeación sería la dependencia encargada de los asuntos de la seguridad de la información, y hacia ella se dirigen las consultas al respecto:

Figura 8 Estructura organizacional UNAD.



Fuente: Página web UNAD. Disponible en: https://informacion.unad.edu.co/transparencia-y-acceso-a-la-informacion/acerca-de-la-unad/estructura-organizacional. 2019

8.1.4. Universidad Tecnológica de Pereira – U.T.P.[50].

- Fue creada en 1958 con carácter nacional, adscrita al Ministerio de Educación Nacional.
- Empieza actividades académicas con la Facultad de Ingeniería Eléctrica y en 1962 se crean las Facultades de Ingeniería Mecánica e Industrial.
- En 1965 se funda el Instituto Pedagógico Musical de Bellas Artes como dependencia de extensión cultural de la Universidad y en 1966 las Escuelas Auxiliares de Ingeniería: Eléctrica, Mecánica e Industrial, que se transforman más adelante en la Facultad de Tecnologías, con los programas de Tecnología Eléctrica, Mecánica e Industrial.
- En 1967 se crea la Facultad de Ciencias de la Educación.
- En 1977 es creada la Facultad de Medicina.
- En 1981 se transforma el Instituto Pedagógico Musical de Bellas Artes en la Facultad de Bellas Artes y Humanidades.
- En 1984, como resultado de la aplicación del Decreto Ley 80 de 1980, se aprueba una nueva estructura orgánica para la Universidad que da origen a la Facultad de Ciencias Básicas y a la Facultad de Tecnologías. Esta última denominada anteriormente Instituto Politécnico Universitario.
- En 1983 se crea el Programa de Maestría en Sistemas Automáticos de Producción y en 1984 la Escuela de Postgrados en la Facultad de Ingeniería Industrial con los programas de Maestría en Administración Económica y Financiera e Investigación de Operaciones y Estadísticas.
- En 1988 se crea el pregrado en Filosofía adscrito a la Facultad de Bellas Artes y Humanidades.
- En 1989 se crea el programa de Ciencias del Deporte y la Recreación adscrito a la Facultad de Medicina.
- En 1991 se crea en la Facultad de Ciencias Básicas el programa de Ingeniería en Sistemas y Computación y la Facultad de Ciencias Ambientales con el pregrado en Administración del Medio Ambiente.
- En 1993 en la Facultad de Ingeniería Industrial se crea el Programa de Especialización en Administración del Desarrollo Humano.
- En 1994 se crean en la facultad de Ingeniería Eléctrica los programas de Maestría en Ingeniería Eléctrica y la Especialización en Electrónica de Potencia.
- En 1995 la Facultad de Ciencias de la Educación abre el Programa de Especialización en Historia Contemporánea de Colombia y Desarrollos Regionales, y la Facultad de Medicina el programa de Especialización Gerencia en Sistemas de Salud.

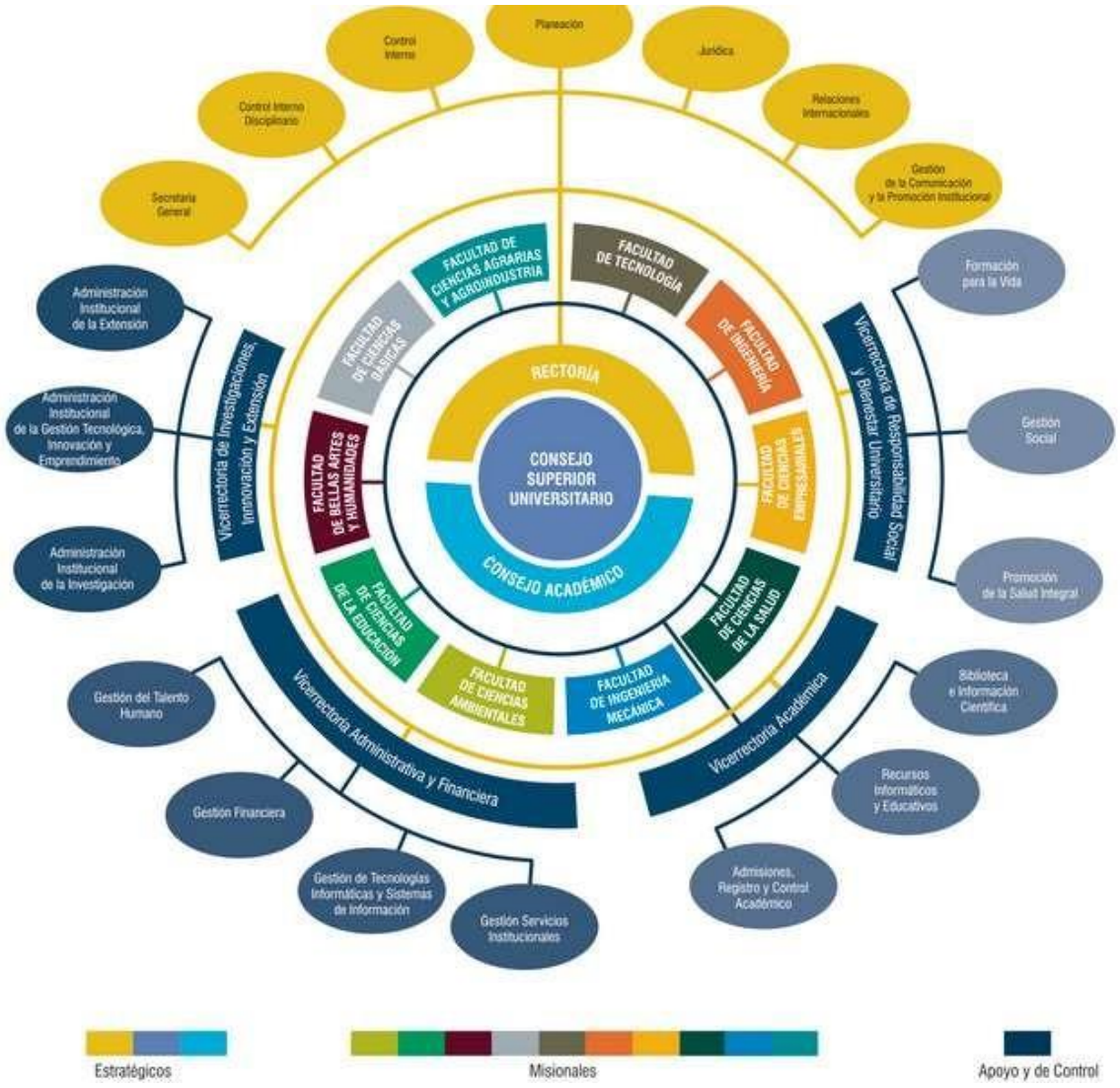
Ya en este siglo, crea nuevos programas de posgrado en áreas como Gerencia de Tecnología, Especialización en Salud Ocupacional, Especialización en Redes y Servicios Telemáticos, Especialización en Literatura y Especialización en Citricultura. Igualmente, crea el Programa de Maestría en Comunicación Educativa.

[50] Universidad Tecnológica de Pereira. 40 años. [en línea]. [2013].

☐ Estructura organizacional de la UTP

Al igual que las anteriores (ver Figura 9) la máxima autoridad académico – administrativa la constituye el Consejo Superior y el Consejo Académico, junto al Rector. Luego, se tienen varias vicerrectorías, una de ellas, la Vicerrectoría Administrativa y Financiera, de la cual depende la Oficina de Gestión de Tecnologías Informáticas y Sistemas de Información, donde se encontraría la información que se busca respecto del manejo de la seguridad informática en esa universidad:

Figura 9 Estructura organizacional UTP.



Fuente: Página web UTP. Disponible en: https://www.utp.edu.co/institucional/organigrama-utp.html. 2019.

8.1.5. Universidad del Quindío[51].

La Universidad del Quindío fue creada en1960, y transformada en una institución de carácter departamental en 1982.

[51] Universidad del Quindío. Historia Universidad del Quindío. [en línea]. 2018.

En 1962 comienza actividades académicas con los programas de Agronomía y Topografía.

Actualmente, la conforman siete (7) facultades, así: Ciencias económicas y administrativas, Ciencias agroindustriales, Ciencias humanas, Ciencias de la salud, Ciencias básicas y tecnologías, Educación, e Ingenierías, con 23 programas en total.

Cuenta además con el Instituto Interdisciplinario de las Ciencias, el Laboratorio de Optoelectrónica, el Instituto de Bellas Artes, el Laboratorio de Investigaciones Biomédicas, la Planta Piloto de Alimentos, la Granja Agroindustrial Bengala, el Laboratorio de Lenguas, el Laboratorio de Aguas, el Laboratorio de Análisis Químico de Suelos, el Laboratorio de Pos cosecha, y otros.

Su campus universitario en la ciudad de Armenia - Quindío se encuentra en la Carrera 15 Calle 12 Norte y posee Centros de tutoría en las ciudades de Buga, Buenaventura, Candelaria, Cali, Manizales, Pereira, Cartago y Quimbaya.

- Estructura organizacional de la Universidad del Quindío

Su estructura es similar a la de la UTP, como se observa en la Figura 10, y en la Vicerrectoría Administrativa se tiene el Área de Sistemas y Nuevas Tecnologías, hacia donde se encaminan las pesquisas correspondientes al tema de la seguridad informática:

Figura 10 Estructura organizacional U. Quindío.

Fuente: Página web Universidad del Quindío. Disponible en: https://portal.uniquindio.edu.co/publicaciones/organigrama_universidad_del_quindio_pub. 2019.

9. INFORMACIÓN ESTADÍSTICA DE LAS UNIVERSIDADES PÚBLICAS DEL EJE CAFETERO.

Lo siguiente condensa la información estadística recogida de las páginas web de las universidades o de documentos sobre el asunto producidos por ellas o de manos de funcionarios consultados vía correo electrónico.

Tabla 1 Estadística de las Universidades públicas del Eje Cafetero. Construcción propia.

Información estadística de las Universidades públicas del Eje Cafetero								
Universidad	Año información	No. de estudiantes matriculados		Total (estudiantes pregrado y posgrado)	No. Profesores		Total profesores	No. de administrativos de planta, provisional, temporal y libre nombramiento y remoción
		Pregrado	Posgrado		De planta	Otro tipo de vinculación		
Nacional - sede Manizales	2018-I	4771	812	5583	279	No especificado	279	202
De Caldas	2019-I	13469	988	14457	395	546	941	419
Tecnológica de Pereira	2019-I	15578	1724	17302	295	1091	1386	402
Del Quindío	2019-I	16808	339	17147	268	593	861	No se tiene información
UNAD - Dosquebradas	2018 – II	70996	2599	73595	80	2519	2599	312

Fuente: El autor. Datos obtenidos de las diferentes páginas web y correos electrónicos de las universidades públicas del Eje Cafetero.

NOTA: Los datos que se presentan de la UNAD son de la totalidad de la Universidad.

10. MARCO METODOLÓGICO

10.1. JUSTIFICACIÓN DE UN CUESTIONARIO

Uno de los propósitos fundamentales de esta monografía es el de conocer qué tanto se ha adelantado en las universidades públicas del eje cafetero en cuanto a la aplicación de normas y estándares nacionales e internacionales al proceso interno de garantizar la protección de su bien más preciado, la información, frente a potenciales ataques informáticos que, incluso, alguna o algunas pudieran haber sufrido ya. Lo anterior podría verse en ellas completado de manera satisfactoria con el diseño y puesta en marcha de un SGSI.

Y como lo anterior debe ser indagado directamente en estas universidades y particularmente en las dependencias que se ocupan de las tecnologías de la información y las comunicaciones, se considera procedente y útil diseñar una herramienta que facilite el asunto.

Se presenta en el Anexo B de este documento la herramienta que se considera en este caso más aplicable, un cuestionario con preguntas asociadas al tema, porque ella da la oportunidad de orientar la pesquisa a través de una entrevista personalizada, que se gestionará ante las instancias pertinentes, lo cual hará más cálida y mejor ambientada la recopilación de la información. Incluso, el desarrollo de la entrevista permitirá ir acomodando las preguntas del cuestionario según como se vaya desarrollando la charla. Es probable que, en algún caso, no sea posible la entrevista directa por motivos ajenos a la voluntad de ambas partes, y entonces en ese caso deberá recurrirse al envío del cuestionario vía correo electrónico con algún mensaje diplomático en el sentido de que se requiere la atención a la solicitud de solución del cuestionario “en el menor tiempo posible”, para no afectar el cronograma de trabajo.

11. RESULTADOS Y ANÁLISIS

11.1. RESULTADOS DE LA APLICACIÓN DEL CUESTIONARIO

Una vez se recibieron todos los cuestionarios (5) diligenciados -lo que ocurrió durante el segundo semestre de 2019- (ver Anexo C), con espacios de tiempo entre uno y otro -lo que normalmente sucede- se procedió a tabular los resultados obtenidos con ellos. También, como era de esperarse, el diligenciamiento del cuestionario no es completamente uniforme, algunas preguntas en algunos casos no aparecen respondidas y entonces la respuesta debe deducirse del comentario que la acompaña, lo cual no ofreció ninguna dificultad. Se destaca el espíritu colaborativo de los funcionarios de las universidades que diligenciaron el cuestionario.

A continuación, se presenta la tabla No. 2 con estos resultados.

Tabla 2 Respuestas a cuestionario diligenciado por funcionario de las universidades públicas del Eje Cafetero

Pregunta cuestionario	Respuesta por Universidad				
	UNAL - MANIZALES	DE CALDAS	UTP	DEL QUINDÍO	UNAD - DOSQUEBRADAS
1. ¿Su Universidad, dentro del área de las Tecnologías de la Información y las Comunicaciones, cuenta con una dependencia que maneje la seguridad informática?	No	No	Sí	Sí	Sí
Observación	N/A	Se tiene el servicio con outsourcing.	N/A	N/A	N/A
2. ¿Su Universidad ha tenido incidentes informáticos que hayan afectado de alguna manera su funcionamiento?	No	Sí	Sí	No	Sí

Si su respuesta es sí, explique cuáles y de qué forma	N/A	Es reserva de la Universidad.	N/A	N/A	Virus ransomware, el cual sólo afectó pocos funcionarios ya que se implementaron políticas de seguridad inmediata

3. ¿De acuerdo con lo anterior, ¿cómo ha manejado o maneja su Universidad los incidentes informáticos que se presentaron o pudieran presentarse en el futuro?	N/A	Trazabilidad, reportes, custodia de equipos si es necesario.	Se cuenta con una mesa de ayuda y se aplican procedimiento de incidentes informáticos.	La Universidad por medio del Área de TI viene adelantando un proyecto de consultoría, incluyendo una herramienta para la gestión de la seguridad informática.	Boletines informáticos, implementado políticas de seguridad, actualizaciones, usando Firewall físico y lógico.
4. ¿Su Universidad tiene políticas de seguridad informática respecto de los activos de información que la universidad posee? Si las conoce, ¿podría incluirlas aquí?	No	No	Sí	Sí	Sí
Observación	N/A	En construcción.	Se cuenta con el Manual General de directrices del Sistema de Gestión de Seguridad de la Información.	Políticas de seguridad informática, políticas de gobierno de TI, políticas de seguridad de infraestructura, están en revisión por parte del Comité de gobierno digital para posibles correcciones y después oficializarlas con la comunidad universitaria.	Copias de seguridad físicas y en la nube de CISCO.
5. ¿Su Universidad tiene un inventario de activos de la información?	Sí	Sí	Sí	Sí	No

¿Si su respuesta es no, conoce la razón por lo cual ocurre esto?	N/A	N/A	N/A	N/A	El activo más custodiado se encuentra inventariado y custodiado por personal experto, la información de los funcionarios son los responsables cada uno de tener un inventario de su información.

6. ¿Su Universidad ha realizado en algún momento un análisis de riesgos frente a amenazas (naturales o antrópicas) que tenga en cuenta qué tan vulnerables son los bienes y las personas ante la eventual ocurrencia de estas?	Sí	Sí	Sí	Sí	Sí
Observación	No aparece respuesta	Muy vulnerable.	No aparece respuesta.	No aparece respuesta.	No aparece respuesta.
7. ¿Su Universidad tiene implementadas acciones preventivas y correctivas frente a los riesgos que pueda tener la información como activo? Si las conoce, ¿podría relacionarlas aquí?	No	Sí	Sí	No aparece respuesta.	Sí
Observación	N/A	No aparece información.	No aparece respuesta.	Se definió la matriz de riesgos y se encuentra en proceso de implantación, con sus respectivos controles.	Firewall, Puertos monitoreados, doble autenticación, seguridad física y lógica, sistemas actualizados.
8. ¿Su Universidad realiza copias de seguridad de la información de forma periódica?	Sí	Sí	Sí	Sí	Sí
9. ¿El sistema operativo de cada uno de los computadores de la Universidad está licenciado y es actualizado con regularidad?	Sí	Sí	Sí	Sí	Sí
10. ¿Su Universidad tiene implementados controles físicos y/o lógicos para salvaguardar la	Sí	Sí	Sí	Sí	No aparece respuesta (la respuesta se deduce que es sí).

información?					
¿Cuál (es)? (ambos controles o solo uno)	Ambos.	Ambos.	No aparece respuesta.	Ambos.	Copias de seguridad físicas, en la nube de CISCO, Movistar Moratos.
11. ¿Para ingresar al área donde se encuentran los servidores se maneja algún tipo de restricciones?	Sí	Sí	Sí	Sí	No aparece respuesta (la respuesta se deduce que es sí).
¿Cuál (es)?	Control de acceso, seguridad.	Llave.	Control de acceso físico.	Control de acceso con tarjeta, y sistemas de	Sólo personal autorizado y sólo las llaves las tiene el

				video y registro de actividades dentro del Data center.	responsable de Data center.
12. ¿Todos los computadores de su Universidad cuentan con antivirus y estos son actualizados con regularidad?	Sí	Sí	Sí	Sí	Sí
13. ¿Su universidad tiene implementado un sistema de gestión en seguridad informática (SGSI)?	Sí	No	No aparece respuesta.	Sí	Sí
Observación	No aparece respuesta	N/A	Actualmente se está implementando.	En proceso de implementación.	N/A
14. ¿Los funcionarios que trabajan en el área de sistemas (TIC' s) conocen y manejan las Normas ISO 27001 y 27002?	Sí	Sí	Sí	Sí	Sí
Observación	N/A	N/A	N/A	3 de los funcionarios están certificados.	N/A
Si su respuesta es no, ¿podría darnos aquí las razones que Ud. considera por las cuales esto sucede?	N/A	N/A	N/A	N/A	N/A

Fuente: El autor. Datos obtenidos de las respuestas de los cuestionarios diligenciados por los funcionarios de las universidades públicas del Eje Cafetero.

a. ANÁLISIS DE RESULTADOS DE LA APLICACIÓN DEL CUESTIONARIO

- Con respecto a la pregunta No. 1 que se les hizo a los funcionarios de las universidades sobre si contaban con una dependencia que maneja la seguridad informática, 3 de 5 contestaron positivamente, lo que indicaría que el 60% de dichas universidades tienen dicha dependencia.

Nota: Esta situación incluye la particularidad de que una de las universidades tiene

el servicio contratado externamente por outsourcing.

- En la pregunta No. 2 se les preguntó a los diferentes funcionarios de las universidades si estas han tenido incidentes informáticos que hayan afectado su

funcionamiento. El 60%, o sea 3 de 5, mostró que sí. Este porcentaje viene siendo bastante alto, y da luces de lo vulnerable de la información de dichas universidades frente a delincuentes informáticos que pudieran tener algún tipo de interés a partir de un ataque a dichos sistemas.

Nota: Como complemento a la anterior pregunta se les solicitó que, por favor, explicaran cuáles incidentes había tenido y de qué forma. Es de anotar que sólo dos (2) de esas universidades dieron algún tipo de respuesta, una de ellas habló sobre la confidencialidad de dicha información y por lo tanto no se pudo obtener información sobre el tipo de ataque del que fue víctima, y la otra contó que fue atacada con ransomware (esta información fue más concreta), pero que no afectó a muchos usuarios por la implementación de políticas de seguridad que ayudaron a minimizar de forma efectiva dicho ataque. Es de anotar que si esto no se hubiera implementado el ataque podría haber afectado bastante a dicha universidad, comprometiendo la información de toda la comunidad universitaria.

- En cuanto a la pregunta No. 3, de las 5 universidades el 80%, o sea 4 de ellas, habló sobre la manera como ha manejado o maneja la universidad los incidentes informáticos que se han presentado o que se pueden presentar. Cada una de ellas dijo algo diferente, por lo que se puede concluir que todas abordan el tema de la seguridad informática desde un punto de vista distinto (las medidas que toman o tomarían se pueden consultar en el cuestionario respondido. Ver Anexo C).

- En la siguiente pregunta (No. 4) se indaga a los funcionarios sobre las políticas de seguridad informática; con esta pregunta se quería saber si las universidades tenían implementadas dichas políticas. Se encontró en la pesquisa que contestaron positivamente 3 de 5 universidades, el 60% de los encuestados. Hay que resaltar que una de las universidades que contestó que no tienen políticas de seguridad informática dijo que en el momento se están construyendo. Esto nos podría indicar que por lo menos el 80% de las universidades le da toda la importancia a la necesidad de contar con las políticas de seguridad informática.

- En cuanto a la pregunta No. 5, el 80% de las universidades, o sea 4 de 5 universidades, contestó que sí tiene inventariados los activos de la información de su universidad. Es de anotar que, aunque una de ellas contestó que no se tiene dicho inventario, pareciera ser que maneja otros tipos de mecanismos encaminados a conocer los activos informáticos que tiene la universidad.

- En relación con la pregunta No. 6 que habla sobre si alguna vez se ha hecho un análisis de riesgos frente a las amenazas con el fin de saber la vulnerabilidad de los bienes y las personas ante alguna ocurrencia de esto, el 100% contestó que sí han realizado dicho análisis de riesgos. Es de resaltar que sólo una de ellas contestó que son muy vulnerables.

- En cuanto a la pregunta No. 7, 3 de los 5 funcionarios, o sea el 60%, contestaron que dichas universidades tienen implementadas acciones preventivas y correctivas frente a los riesgos que la información pueda tener. Aunque uno de ellos no contestó ni positiva ni negativamente, con la respuesta que da en cuanto a que se definió una matriz de riesgos y que además se encuentra en proceso de implantación, con sus respectivos controles, se puede deducir que efectivamente sí existen acciones de tipo preventivo y correctivo frente a los riesgos. Hay que resaltar que sólo 2 de ellas hablaron de dichas acciones.

- Frente a la pregunta No. 8, todos los funcionarios contestaron de forma positiva a la realización de copias de seguridad de la información de forma periódica, lo que representa el 100% de las universidades; algo muy positivo que ayuda a minimizar los riesgos que se pueden tener en cuanto a integridad de la información.

- En cuanto a la pregunta No. 9, sobre el SO y si estos se encuentran licenciados y son actualizados con regularidad, nuevamente -como en la pregunta anterior- la totalidad de las universidades contestó afirmativamente, o sea el 100% de ellas. Esto ayuda de igual forma a minimizar los riesgos que se pudieran tener por ataques informáticos.

- En relación con la pregunta No. 10 que habla sobre si las universidades tienen implementados controles físicos y/o lógicos para salvaguardar la información, 4 de las 5 universidades (80%) contestaron afirmativamente a esta pregunta, pero hay que resaltar que la No. 5, aunque no contestó ni sí ni no, dio a entender con la respuesta a si se tiene implementado uno o ambos, que sí tiene dichos controles porque, además, amplía la respuesta (esto se puede consultar en el cuestionario. Ver anexo C); las demás también dieron una respuesta a esta pregunta que es un complemento de la anterior (esta información también se puede consultar en las respuestas al cuestionario. Ver Anexo C). Adicionalmente, lo anterior también ayuda a tener una visión más amplia frente a lo que hacen las universidades por salvaguardar su información y se puede ver que cada una de ellas toma medidas para mitigar los riesgos a los que están expuestas.

- En lo referente a la pregunta No. 11 que habla de si para ingresar al lugar donde se encuentran los servidores las universidades tienen algún tipo de restricciones, 4 de 5 contestaron que sí, el 80%, pero hay que dejar claro que, aunque la universidad número 5 no contestó ni afirmativa ni negativamente, es posible deducir de lo que complementa la pregunta que sí existen medidas (estas se pueden consultar en el cuestionario respondido por ellos. Ver anexo C), lo que podría cambiar el porcentaje de esta pregunta al 100%. Es de resaltar que ésta es una de las medidas más importantes para salvaguardar la información porque el lugar donde se encuentran los servidores debe estar aislado de las personas en general, a esa zona sólo pueden ingresar personas con permisos especiales.

- En cuanto a la pregunta No. 12, la respuesta de los funcionarios de las universidades fue unánime y fue afirmativa en su totalidad, el 100%. Esto es muy importante también porque todos los computadores deben tener antivirus, pero no sólo eso, sino que además deben estar actualizados para que funcionen de forma correcta.

- En lo que concierne a la pregunta No. 13, que habla sobre si las universidades tienen implementado un SGSI, 3 de ellas, el 60%, contestaron de forma afirmativa, y una cuarta no contestó ni afirmativa ni negativamente, pero contestó que se está implementando actualmente (esto hace pensar que la respuesta no es negativa porque, aunque no está implementado, se están tomando medidas y es factible que pronto se tenga un SGSI en dicha universidad; también, hay que resaltar que una de las universidades que contestó de forma positiva dice que en el momento de la respuesta del cuestionario se encontraban en proceso de implementación; esto es muy interesante, ya que podría llevar a que en poco tiempo el 80% de las universidades públicas del Eje Cafetero tenga implementado un SGSI, que les ayudará a minimizar las vulnerabilidades que puedan tener frente a uno de sus activos más importantes como lo es la información.

- Por último, en cuanto a la respuesta de la pregunta No. 14 se tiene que todas las universidades, el 100%, tienen funcionarios que conocen y manejan las normas ISO 27001 y 27002, y una de ellas complementa su respuesta diciendo cuántos de sus funcionarios se encuentran certificados.

b. POLÍTICAS DE SEGURIDAD INFORMÁTICA EN UNIVERSIDADES PÚBLICAS DEL EJE CAFETERO

i. Introducción

Como se pudo evidenciar en las respuestas al cuestionario, no se ha implementado de manera completa aún un SGSI en ellas, aunque es de anotar que varias de ellas se encuentran en dicho proceso. Se aclara que, evidentemente, todas las universidades han tomado medidas para mitigar los riesgos que puedan tener frente a los inescrupulosos y a los ataques que estos les puedan generar para apoderarse o dañar la información, lo cual ha sido objeto de estudio durante la realización de esta monografía. En otras palabras, todas las universidades han tenido contacto con la seguridad informática pues han dejado en claro que de esta manera están procurando evitar tener un sistema informático vulnerable. Para ilustrar lo dicho y lo hecho por las universidades en este aspecto, a continuación, se presenta un resumen de lo adelantado en una fase crucial de los SGSI, las políticas de seguridad informática, y para ello se desglosará de cada universidad de manera resumida la información que al respecto se pudo recopilar.

ii. Universidad Nacional de Colombia UNAL

La Universidad Nacional de Colombia promulga en el año 2016 el Acuerdo 228 por el cual se adopta la Política de Seguridad Informática y de la Información dentro de ella, lo que le ayudará a proteger dicha información. En el mismo Acuerdo, se contempla incluir dicha política de seguridad en el Sistema Integrado de Gestión Académica, Administrativa y Ambiental – SIGA y en el Sistema de Control Interno.

Como preámbulo de lo anterior, la UNAL generó en 2015 (Dirección Nacional de Tecnologías de la información y las telecomunicaciones – Vicerrectoría General) un documento (denominado Política de seguridad informática y de la información, que aparece en el portal Web de la universidad) en el que plasmaron las políticas de seguridad informática que debían ser implementadas dentro de la universidad.

Del documento, que es extenso, se transcriben aquí apartes de la política en sí, para destacar en detalle su importancia:

> “Aplicabilidad:
>
> Esta política es de aplicación a todas las dependencias que componen la comunidad académica e institucional, a sus recursos, a la totalidad de los procesos internos o externos vinculados a la universidad a través de contratos, convenios o acuerdos con terceros y a todo el personal de la Universidad Nacional de Colombia, cualquiera sea

su vinculación, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe dentro del alcance definido para la seguridad informática y de la información y en general a todos los usuarios de la información o aquellos que sean beneficiados con el uso de la infraestructura, servicios, sistemas misionales de la Universidad.

- Responsabilidad:

a) La Dirección Nacional de Tecnologías de la Información y las Comunicaciones (DNTIC) con la participación de las Oficinas de Tecnologías de la información y de las Comunicaciones (OTICs), diseña y elabora la propuesta de políticas de seguridad informática y de la información que son presentadas al Comité Nacional de Informática y Comunicaciones (CNTIC), quien propone y presenta esta propuesta al Consejo Superior Universitario (CSU), para que recomiende aprobar el texto de la política de seguridad de la información, las funciones generales en materia de seguridad de la información y la estructuración, seguimiento y mejora de la seguridad informática y de la información de la Universidad.
b) Es responsabilidad del CNTIC definir las estrategias de capacitación en materia de seguridad de la información al interior de la Universidad.
c) El grupo responsable de seguridad informática se configura de la siguiente manera: Gobierno de seguridad y operaciones de seguridad. El Gobierno de seguridad es responsabilidad de DNTIC y tiene como función principal velar por el gobierno corporativo de la seguridad, emitir disposiciones relativas a la materia y practicar evaluaciones, control, seguimiento y auditorías de seguridad que evidencien el nivel de maduración de la seguridad en la institución. La operación y gestión de la seguridad es responsabilidad de cada una de las OTIC y deberá cumplir funciones relativas a la seguridad de los sistemas de información misionales, su infraestructura, servicios y activos de información asociados. El nivel de supervisión que pueda realizar cada grupo responsable de seguridad está relacionado con el talento humano que lo conforma y en todo caso deberá ser aprobado por el CSU.
d) La Dirección Nacional de Personal Académico y Administrativo de la Vicerrectoría General, cumplirá la función de notificar a las sedes, para que éstas a través de la Secretaría de Sede notifiquen a todo el personal que se vincula contractualmente con la Universidad, de las obligaciones respecto del cumplimiento de la política de seguridad informática y de la información y de todas las directrices, estándares, procesos, procedimientos, prácticas y guías que surjan de la seguridad de la información; adscrita al Sistema de Control Interno y al Sistema de Gestión de Calidad Institucional. De igual forma, será responsable de la notificación de la presente política y de los cambios que en ella se produzcan a todo el personal, por medio de los canales establecidos a través de la suscripción de los compromisos de confidencialidad y de tareas de capacitación continua en materia de seguridad según lineamientos dictados por CNTIC.
e) El director de la Dirección Jurídica Nacional verificará el cumplimiento de la presente política en la gestión de convenios, acuerdos u otra documentación de la institución con empleados y con terceros. Asimismo, asesorará en materia legal a la entidad en lo que se refiere a la seguridad de la información.
f) La Gerencia Nacional Financiera y Administrativa, a través de sus divisiones de gestión de la contratación, verificará el cumplimiento de la presente política en la

gestión de todos los contratos firmados entre la institución y terceros en lo que se refiere a la seguridad de la información.

g) Los usuarios de la información, infraestructura tecnológica, servicios utilizados para su procesamiento y sistemas misionales son responsables de conocer y cumplir la política de seguridad de la información vigente.

h) La DNTIC es responsable de practicar auditorías periódicas sobre los sistemas y actividades vinculadas con la gestión de activos de información y tecnología de información. Es su responsabilidad informar sobre el cumplimiento de las especificaciones y medidas de seguridad de la información establecidas por esta política y por las normas, procedimientos y prácticas que de ella surjan.

- Reglas:

a) Establecer, implementar, hacer seguimiento, auditar y promover la mejora continua de la política de seguridad de la información en toda la comunidad universitaria.

b) Desarrollar y mantener actualizado un inventario de activos de información y recursos tecnológicos y brindar esta información a DNTIC para mantener actualizado el repositorio de arquitectura de seguridad informática que compone el marco de arquitectura empresarial.

c) Establecer indicadores que determinen y aseguren el eficiente cumplimiento de las funciones y actividades misionales en las que se demuestre cómo se ha logrado minimizar los riesgos asociados de pérdida, robo, daño, uso intencionado y no intencionado de información.

d) Definir estándares y lineamientos técnicos para la gestión de seguridad informática y de la información de TIC's en los niveles nacionales, sedes y facultades.

e) Evaluar y hacer seguimiento a la gestión de seguridad informática y de la información de TIC's a nivel nacional, de sedes y facultades.

f) Orientar, proponer y contratar los sistemas de seguridad y contingencia y de buen uso de recursos informáticos y de comunicaciones, para mejorar el nivel de seguridad y confiabilidad de los sistemas de información de la universidad.

g) Implementar los mecanismos necesarios para garantizar la integridad, confiabilidad, oportunidad, disponibilidad y la seguridad en los sistemas informáticos y de comunicaciones de la universidad.

h) Establecer y responder por el manejo y mantenimiento adecuado de los datos, en cuanto a consulta, ingreso, modificación, eliminación o divulgación de los datos de los sistemas de información misionales y demás activos de información y verificar mediante auditorías internas su cumplimiento.

i) Verificar que los usuarios finales (sean funcionarios o contratistas), se hacen responsables de la información contenida en sus equipos.

j) Instaurar y verificar qué procesos y servicios que requieran el uso de activos informáticos a nivel institucional cuentan con los componentes de seguridad informática y de la información: i) medidas técnicas; ii) recursos humanos y desarrollo de capacidades; iii) legal y regulatorio; y iv) educación y conciencia institucional y pública.

k) Emitir disposiciones en materia de seguridad (directrices técnicas, específicas, normativas y procedimentales, estándares y lineamientos técnicos, instructivos u otras) de acuerdo con la normatividad vigente, que sujeten a los usuarios a mantener

una alta responsabilidad respecto de la seguridad informática y de la información, derivada de la manipulación o uso de diferentes activos de información, infraestructura y servicios tecnológicos informáticos a disposición de la misión institucional.

l) Incorporar como parte del Sistema de Gestión de Calidad y del Control Interno la regulación y puesta en operación de la política de seguridad informática y de la información y verificar que toda la comunidad universitaria es responsable y mantiene habilitados y en correcto funcionamiento controles de protección contra pérdida, daño, uso intencionado y no intencionado y modificación de información o de su procesamiento para la prestación de las obligaciones y responsabilidades de los usuarios de los servicios de tecnologías informáticas de Universidad.

m) Establecer como requisito para la toma de decisiones en seguridad informática y de la información los resultados de la gestión del riesgo, con miras a obtener un impacto positivo a nivel institucional.

n) Validar la operacionalización de la seguridad informática y de la información en el ejercicio de funciones o roles, a bien de acatar las políticas y disposiciones aquí contenidas.

o) Incluir todas las disposiciones legales y reglamentarias en el ejercicio y demostración de la seguridad informática y de la información a todo nivel, aplicables a la institución en cumplimiento de la misión institucional.

p) Coordinar e integrar la seguridad informática y de la información a los diferentes sistemas de gestión de la Universidad sin que ello implique duplicidad o realización de esfuerzos aislados. Ej. Integración al Sistema de Control interno, al Sistema de Gestión de Calidad, al Sistema de Gestión Ambiental; entre otros.

q) Fortalecer el marco de cooperación científica y tecnológica realizado por la Universidad, facilitando mecanismos y recursos necesarios que garanticen el cumplimiento de la presente disposición de seguridad informática y de la información.

r) Implementar, revisar y actualizar las políticas de seguridad informática y de la información a través de los mecanismos establecidos en el Sistema de Gestión de Calidad.

s) Diseñar, programar y realizar los programas de auditoría de la seguridad informática y de la información, los cuales estarán a cargo de los entes que ejercen el control interno y DNTIC.

t) El Rector, los Vicerrectores, directores, gerentes, jefes de área o dependencia deben asegurar que todos los procedimientos de seguridad de la información dentro de su área de responsabilidad se realizan correctamente para lograr el cumplimiento de las políticas y estándares de seguridad de la información de UNAL"[52].

Como se deduce fácilmente, se trata también de un documento muy completo que puede ser consultado en sus detalles por los interesados lectores de esta monografía en el Anexo D. Numeral 1.

iii. Universidad de Caldas

[52] Política de Seguridad Informática y de la Información. Universidad Nacional de Colombia. [on-line]. 2015.

En cuanto a las políticas de seguridad informática de la Universidad de Caldas, en el año 2013 se realizó en la ciudad de Manizales el Segundo encuentro colombiano de gestión universitaria, en donde la Oficina de Sistemas de dicha universidad realizó una presentación que trata sobre la seguridad informática en las instituciones de educación superior, y para ello la universidad dio a conocer cuáles eran las políticas de seguridad que manejaba para ese entonces. En virtud de que no se conoce un documento más actualizado de dichas políticas, a continuación, se hace una transcripción de apartes de lo presentado en esa ocasión:

"CLASIFICACIÓN Y SEGMENTACIÓN DE LAS REDES INSTITUCIONALES

- Definir una política de apertura y cierre de servicios haciendo uso de las redes institucionales.
- Clasificar las redes institucionales por servicios y poblaciones de usuarios.
- Definir los servicios y capacidades que se brindarán para cada segmento.
- Segmentar los grupos de usuarios y las conexiones, infraestructura de redes.
- Aplicar los servicios y capacidades en cada segmento y monitorear el funcionamiento y la manifestación de los usuarios.

INCORPORAR TECNOLOGÍA DE SEGURIDAD EFICIENTE Y ACTUALIZABLE AUTOMÁTICAMENTE

- Adquirir y configurar un equipo de seguridad perimetral (UTM).
- Aplicar en cada segmento de red los servicios y capacidades predefinidos y acoplarlos al equipo de seguridad perimetral.
- Revisar constantemente los reportes arrojados por el equipo UTM y ajustar las condiciones del perímetro y de los segmentos.
- Incorporar software para el monitoreo de la red, permitiendo revisar cada segmento o equipo activo de la red institucional.

SOFTWARE ANTIVIRUS Y ACTUALIZACIÓN MODIFICADA

- Implementar el uso del software antivirus en todas las estaciones de trabajo y para todos los usuarios.
- La actualización del software antivirus se debe realizar desde un servidor dedicado y aplicarlo a las estaciones de trabajo en periodos de tiempo distribuido.
- Los parches de actualización del sistema operativo y del software ofimático también se deben surtir por medio del servidor de actualizaciones y aplicarlo de manera distribuida en el tiempo.
- Los usuarios son invitados, no administradores de los equipos.

SERVIDORES EN NUEVA INFRAESTRUCTURA

- Consolidar servidores con misiones específicas: servidor de bases de datos, servidor de aplicaciones o servidor de sistemas de información, servidor de copias de seguridad, servidor de respaldo, servidor de actualizaciones, servidor de pruebas de los sistemas y servidor de desarrollo.
- Virtualizar el uso de los servidores para ofrecer optimización de esta tecnología y ofrecer niveles rápidos de recuperación ante fallas.
- El data center se debe conformar y desarrollar con servidores por cuchillas, servidores NAS y servidores SAN, con el fin de optimizar recursos tecnológicos y crecer ordenadamente.

CERTIFICAR EL ACCESO Y USO DE LOS SERVIDORES

- Asegurar la identidad de un equipo remoto suscribiendo el certificado de seguridad con empresa altamente reconocida.
- Permitir el acceso de los usuarios sólo hasta los servidores de aplicaciones y permitir los cambios transaccionales en las bases de datos sólo entre servidores.
- Configurar claves seguras de los usuarios con complejidad y solicitar el cambio periódicamente.
- Capacitar y concientizar a los usuarios en el manejo y cuidado de las claves, en la importancia de realizar cambios periódicos y la construcción de la complejidad de esta.

INTEGRACIÓN SISTEMAS DE INFORMACIÓN

- Selección de un motor de bases de datos robusto y acorde con el crecimiento institucional.
- Selección e incorporación de sistemas de información ampliamente reconocidos.
- Alcanzar la interoperabilidad de los sistemas de información a nivel de procesos, contenidos y transporte.
- Los sistemas deben generar trazabilidad y que permitan la auditoría.
- Las casas de software son aliados tecnológicos para las instituciones debido al desarrollo de los sistemas de información".[53]

Como se deduce fácilmente, se trata también de un documento muy completo que puede ser consultado en sus detalles por los interesados lectores de esta monografía en el Anexo D. Numeral 2.

[53] SEGURIDAD INFORMATICA EN LAS INSTITUCIONES DE EDUCACION SUPERIOR. Universidad de Caldas – Oficina de Sistemas. [en línea]. 2013.

iv. Universidad Tecnológica de Pereira UTP

En el año 2017, esta universidad produjo un importante, extenso y detallado documento que denominó SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN. MANUAL GENERAL DE DIRECTRICES, con el objetivo de "establecer las directrices de Seguridad de la Información en la Universidad Tecnológica de Pereira, con el fin de generar conciencia y buenas prácticas de la seguridad de la información al interior de la entidad, a través de su cumplimiento e interiorización".

Así, el documento mencionado establece las directrices de seguridad de la información sobre:

- "DISPOSITIVOS MÓVILES: En cuanto a su configuración y uso.
- CORREO ELECTRÓNICO INSTITUCIONAL: En cuanto a disposiciones generales sobre el correo electrónico, usos, restricciones, suspensiones, eliminaciones y casos especiales.
- CONTROL DE ACCESO: En cuanto a usuarios, sus claves y generalidades del caso.
- ACCESO A REDES Y A SERVICIOS EN RED: En cuanto a prevenir y controlar el acceso, la comunicación con entidades externas, sistemas de monitoreo, características del cableado, registro de eventos, configuración de calidad del servicio, etc.
- USO DE CONTROLES CRIPTOGRÁFICOS: En cuanto a accesos cifrados, uso de técnicas de criptografía, almacenamientos cifrados, etc.
- PANTALLAS, ESCRITORIOS LIMPIOS Y EQUIPOS DESATENDIDOS: En cuanto a ubicación de escritorios y pantallas, mantenimiento de escritorios limpios de información, medidas de protección al terminar la jornada, bloqueo de sesión de usuario cuando no se esté, uso de carpetas con controles de seguridad, equipos de reproducción controlados, salas y tableros limpios, etc.
- PROTECCIÓN CONTRA SOFTWARE MALICIOSO: En cuanto a la instalación, configuración y modificación de software de los equipos de cómputo, la instalación, configuración y modificación de software de servidores, el manejo del software contra código malicioso, el análisis de archivos adjuntos en correos, etc.
- RESPALDO DE LA INFORMACIÓN: En cuanto a las copias de respaldo para sistemas de información y servidores, las copias de respaldo para el personal que labora prestan servicio y terceros, etc.
- TRANSFERENCIA DE INFORMACIÓN: En cuanto a la existencia de documentos de aceptación de las políticas de seguridad entre las partes, la firma de cláusulas de confidencialidad, la definición de mecanismos y protocolos a usar, el empleo de controles criptográficos, acciones ante incumplimiento de acuerdos, etc.
- DESARROLLO SEGURO DE SOFTWARE: En cuanto al cumplimiento de normas de desarrollo, normas alineadas con las normas ISO, implementación de planes de capacitación y de sistemas de auditorías, acuerdos de licencias, propiedad de código y derechos de propiedad intelectual, entre otros.

- RELACIONES CON TERCEROS Y EL PERSONAL QUE PRESTA SERVICIOS: En cuanto al conocimiento, aceptación y cumplimiento de las políticas de seguridad de la información por parte de ellos, compromisos en el cuidado de la información, acceso limitado a información, la gestión de la prestación del servicio con un interventor o supervisor, la devolución de información o activos de información que estuvieron bajo su responsabilidad, el uso no autorizado de información, el uso de equipos que no cumplan con controles de seguridad, el tratamiento del riesgo dentro de acuerdos, entre otros.
- PROTECCIÓN DE DATOS PERSONALES: En cuanto a canales habilitados para peticiones, consultas y reclamos, derechos de los titulares de los datos personales tratados por la Universidad Tecnológica de Pereira, derechos de niños y adolescentes, la legitimación para el ejercicio del derecho del titular, el tratamiento y finalidad al cual serán sometidos los datos personales, las condiciones para el tratamiento de los datos personales, las autorizaciones y los medios para el tratamiento de la información, la revocatoria de la autorización o supresión de los datos, la transferencia y transmisión de datos personales e información personal por parte de la Universidad, los deberes en el tratamiento de los datos personales, la implementación de un Aviso de Privacidad, y otros más.
- DATOS ABIERTOS: En cuanto a los requisitos internos para la publicación de datos abiertos y a su ruta de cargue"[54].

Como se deduce fácilmente se trata también de un documento muy completo que puede ser consultado en sus detalles por los interesados lectores de esta monografía en el Anexo D. Numeral 3.

v. Universidad del Quindío

La Universidad del Quindío en el año 2015 produjo un documento con el nombre Hoja de Ruta – Implementación de las Políticas de Seguridad de la Información; dicho documento aparece como aprobado en su versión 2.0. con fecha septiembre del 2017. Es de anotar que este documento figura como confidencial, pero al estar publicado en la página web se utiliza en este trabajo para ampliarlo.

A continuación, se hace un resumen de las políticas de seguridad informática y de otros temas que se abordan en el citado documento, con el fin de realizar luego un análisis de ello.

> "Implementación de las políticas de seguridad de información: Se debe definir como estrategia para la implementación del Modelo de seguridad de información en la Universidad del Quindío, el cumplir con una serie de fases que se sugieren en esta

[54] MANUAL GENERAL DE DIRECTRICES del SGSI. UTP. [en línea]. 2017.

hoja de ruta, las cuales tienen como objetivo que la universidad, desarrolle, apruebe, implemente, socialice e interiorice estas políticas, para un uso efectivo por parte de todos los funcionarios, contratistas y/o terceros de la universidad.

La Universidad del Quindío considera importante contar con políticas de seguridad informática, pues guiarán ellas las acciones sobre el manejo de la información institucional de sus funcionarios, contratistas o terceros sobre la información obtenida, y garantizarán el cumplimiento de requisitos legales que todas tienen.

Las fases planteadas en dicha Hoja de ruta son:

- Desarrollo de las políticas: En esta fase la Universidad del Quindío debe responsabilizar las áreas para la creación de políticas, estructurarlas, escribirlas, revisarlas y aprobarlas.
- Cumplimiento: Fase mediante la cual todas aquellas políticas escritas deben estar implementadas y relacionadas con los controles de seguridad de la información.
- Comunicación: Fase mediante la cual se dan a conocer las políticas a los funcionarios, docentes, contratistas y/o terceros de la Universidad del Quindío.
- Monitoreo: Fase según la cual las políticas deben ser monitoreadas para determinar la efectividad y cumplimiento de estas.
- Mantenimiento: Esta fase es la encargada de asegurar que la política se encuentre actualizada, íntegra y que contenga los ajustes necesarios y obtenidos de las retroalimentaciones.
- Retiro: Fase mediante la cual se hace eliminación de una política de seguridad en cuanto esta ha cumplido su finalidad o la política ya no es necesaria en la Universidad del Quindío.

- Implementación de controles de seguridad de la información: La intención es hacer las recomendaciones de políticas de seguridad de la información para el Modelo de Seguridad y Privacidad de la información para la Universidad del Quindío. A continuación, se agruparán las políticas con el objetivo de hacer una implementación transversal de Seguridad de la Información en esta entidad.

ORGANIZACIÓN: Esta política tiene como finalidad establecer el Comité directivo de la seguridad de la información.
GESTIÓN DE ACTIVOS: Este grupo de políticas hacen referencia a todas aquellas directrices mediante las cuales se indican a los funcionarios y contratistas los límites y procedimientos frente a la identificación, uso, administración y responsabilidad ante los activos de información.
CONTROL DE ACCESO: Este grupo de políticas se refieren a todas aquellas directrices mediante las cuales la Universidad determina los mecanismos de protección, los límites y procedimientos frente a la administración y responsabilidad, relacionados con los accesos a la información, sin importar si estos accesos sean electrónicos o físicos.

NO REPUDIO: La política de seguridad y privacidad comprende la capacidad de no repudio con el fin de que los usuarios eviten realizar alguna acción impropia. La política deberá incluir mínimo los aspectos de trazabilidad, retención, auditoría, intercambio electrónico de información, privacidad y confidencialidad.
INTEGRIDAD: Se refiere esta política al manejo íntegro e integral de la información tanto interna como externa, conocida o administrada por funcionarios y demás. Debe ser complementaria al Código de Ética y Buen Gobierno emitido por Resolución de Rectoría.
DISPONIBILIDAD DEL SERVICIO E INFORMACIÓN: La Universidad deberá contar con un plan de continuidad del negocio con el fin de asegurar, recuperar o restablecer la disponibilidad de los procesos que soportan el SGSI y procesos misionales de la Universidad, ante el evento de un incidente de seguridad de la información.
REGISTRO Y AUDITORÍA: Esta política vela por el mantenimiento de las evidencias de las actividades y acciones que afectan los activos de información y deberá incluir la responsabilidad de la Oficina de Control Interno de llevar a cabo auditorías periódicas a los sistemas y actividades relacionadas con la gestión de activos de información, así como la responsabilidad de dicha Oficina de informar los resultados de las auditorías.
GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN: La Universidad deberá documentar una política general de gestión de eventos, incidentes y vulnerabilidades de seguridad de la información. Debe ir dirigido a todos los usuarios que tienen un acceso autorizado a cualquier sistema de información.
CAPACITACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN: Esta política se centra en la formación del personal en temas relacionados con la seguridad de la información, cuya finalidad es disminuir las vulnerabilidades y amenazas relacionadas con el recurso humano.
IDENTIFICAR LOS RIESGOS: La universidad debe realizar la identificación de amenazas potenciales y vulnerabilidades para cada activo y los niveles de confidencialidad, integridad y disponibilidad de los activos (…) así como enumerar las opciones para el tratamiento/reducción del riesgo (selección de controles). (Es posible utilizar el conjunto de controles de la norma NTC/ISO 27002, NIST SP-800-53).
PLAN DE TRATAMIENTO DEL RIESGO: En esta etapa se deben aprobar los objetivos de control y controles a implementar con el fin de tratar los riesgos identificados.
El plan de tratamiento del riesgo debe contener el método aplicable para cada riesgo: aceptar, reducir, transferir o eliminar el listado de controles actualmente implementados, los controles adicionales propuestos y el espacio de tiempo en el cual los controles propuestos serán implementados.
GENERAR EL DDA – DECLARACIÓN DE APLICABILIDAD: La declaración de aplicabilidad es un documento orientado a dar cumplimiento al estándar NTC:ISO/IEC 27001:2013, y optar por una futura certificación.

- LINEAMIENTOS DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN: Se sugiere verificar el cumplimiento de los siguientes lineamientos:

  USO DE CONTRASEÑAS Y USUARIOS: Debe definir las condiciones, normas y procedimientos necesarios para fijar los requisitos que se deben cumplir por cualquier funcionario, contratistas o estudiante de la universidad para obtener acceso a los sistemas de información, hardware y software propiedad de la Universidad del Quindío.

USO DEL SERVICIO DE CORREO ELECTRÓNICO: Debe generar conciencia a los funcionarios, contratistas o estudiantes de la universidad de los riesgos asociados con el uso de correo electrónico y presenta las normas y protocolos a seguir para el buen uso de este servicio.

USO DEL SERVICIO DE INTERNET/INTRANET: Concientizar a los funcionarios, contratistas o estudiantes de la universidad de las buenas prácticas a seguir sobre las normas de uso del servicio de internet/intranet, así como el conocimiento de los riesgos asociados por el uso indebido de los mismos.

USO DE SERVICIO DE MENSAJERÍA INSTANTÁNEA: Concientizar a los funcionarios, contratistas o estudiantes de la universidad de las buenas prácticas a seguir sobre las normas y el uso del servicio de mensajería instantánea, así como el conocimiento de los riesgos asociados por el uso indebido de estos.

USO DE DISPOSITIVOS DE ALMACENAMIENTO EXTERNO: Describir el uso permitido de los dispositivos de almacenamiento externo en la universidad y las restricciones en su empleo al interior de la institución.

USO DE DISPOSITIVOS DE CAPTURA DE IMÁGENES Y/O GRABACIÓN DE VIDEO: Definir el acceso y el uso de cámaras fotográficas, cámaras de video y demás dispositivos que permitan el registro de imágenes, fotografías y/o video.

USO DE ESCRITORIOS Y PANTALLAS DESPEJADAS: Definir los mecanismos necesarios que se deben aplicar en la universidad con el fin de proteger la información física residente en los escritorios y puestos de trabajo y la información digital almacenada en los computadores e infraestructura técnica a disposición de todos los funcionarios, contratistas o estudiantes para el normal desarrollo de las actividades.

USO DE DISPOSITIVOS MÓVILES (TABLETS, CELULARES): Define los mecanismos necesarios que se deben aplicar en la universidad, con el fin de proteger la confidencialidad de la información mediante el uso de los dispositivos móviles personales o de la universidad. Se deben definir en qué áreas o para qué macroprocesos se restringe o no el uso de los dispositivos personales móviles y cuáles son las medidas de seguridad para el transporte de estos fuera de las instalaciones en el caso de los dispositivos móviles de la universidad.

CONEXIONES REMOTAS / TELETRABAJO: Definir los requisitos y los casos en los cuales se concede acceso remoto a las plataformas tecnológicas de la universidad y las medidas de seguridad que se establecen para garantizar la integridad, confidencialidad y disponibilidad de la información que es accedida por este medio o teletrabajo.

PLAN DE ACCIÓN GENERAL GOBIERNO DE TECNOLOGÍA. Iniciativas para realizar en el marco del cumplimiento componente seguridad

MODIFICAR LA VISIÓN DE TI, PASANDO DE ADMINISTRADORES DE DISPOSITIVOS A ADMINISTRADORES DE SERVICIOS DE TI: Adoptar un Framework de arquitectura empresarial que permita alinear los procesos, datos, aplicaciones e infraestructura con los objetivos estratégicos de la Universidad del Quindío. Evaluar, seleccionar e implementar un estándar, regulación y/o mejores prácticas para gobierno de TI. Definir y ejecutar un plan de capacitación especializada y/o certificaciones relacionado con el estándar seleccionado. Definir y ejecutar un plan de socialización y adaptación al cambio para toda la Universidad del Quindío. Evaluar, seleccionar e implementar una herramienta de gestión de servicios de TI que facilite la

implementación del estándar seleccionado. Generar y/o actualizar los procedimientos de TI acorde al estándar seleccionado.
IMPLEMENTAR ACCIONES TRANSVERSALES DE SEGURIDAD DE LA INFORMACIÓN: Establecer formalmente un sistema de gestión de la seguridad de la información, ya sea en desarrollo propio o con el acompañamiento especializado. Implementar los planes de transición de los protocolos IPv4 a IPv6. Diseñar y ejecutar planes de pruebas a la implementación de la transición IPv4 a IPv6. Implementar buenas prácticas de ciberseguridad. Establecer una estrategia para la implementación del tratamiento de riesgos de seguridad de la información. Implementar la política de protección de datos personales para dar cumplimiento a la legislación vigente relacionada con protección de datos personales. Implementar el principio de responsabilidad demostrada (Accountability). Planificar e implementar el Modelo de Seguridad y privacidad de la información – MSPI.
IMPLEMENTAR AL PLAN ESTRATÉGICO DE TI (PETI): Definir las estrategias en cuanto a TI, sistemas de información, servicios tecnológicos y del uso y aprobación de los anteriores. Garantizar el valor estratégico de la capacidad y la inversión en tecnología. Definir la estrategia organizacional y las necesidades del negocio de TI. Definir la planeación estratégica de gestión de TI. Definir el portafolio de planes, servicios y proyectos de TI. Definir las políticas de TI en cuanto a seguridad, información, acceso y uso, etc. Reforzar el plan de continuidad de TI"[55] .

Como se deduce con facilidad, se trata igualmente de un documento muy completo que puede ser consultado en sus detalles por los interesados lectores de esta monografía en el Anexo D. Numeral 4.

vi. Universidad Nacional Abierta y a Distancia UNAD

La UNAD estableció en 2013 sus políticas de seguridad de la información (Res. 4793) y luego, en 2014 (Res. 7966) conformó su Sistema Integrado de Gestión, que incluyó el componente de Gestión de la Seguridad de la Información (SGSI) y el componente de Gestión de Servicios de Infraestructura Tecnológica. En 2015, expidió la Res. 4256 en la cual definió las políticas del Marco de Referencia del SGSI. Esta derogó entonces la Res. 4793 de 2013 y otras anteriores.
A continuación, se hace un resumen de las políticas de que trata esta última Resolución:

"POLÍTICA PARA DISPOSITIVOS MÓVILES: Tiene que ver con limitaciones y condicionamientos en el uso de dispositivos móviles al interior de las instalaciones de la UNAD, con el cifrado de datos de sus medios de almacenamiento, con controles en el retiro de ellos de las instalaciones de la UNAD, con controles a la conexión de dispositivos personales de este tipo a la red institucional, con restricciones al ingreso

[55] Hoja de Ruta - IMPLEMENTACIÓN DE LAS POLITICAS DE SEGURIDAD DE INFORMACIÓN. Universidad del Quindío. [en línea]. 2015.

de celulares y otros dispositivos a los centros de datos y centros de cableado, con el hecho de que este tipo de controles se aplican también a visitantes y personal de apoyo, entre otros asuntos.

POLÍTICA DE CONTROL DE ACCESO LÓGICO: Tiene que ver a su vez con permisos para el acceso a los recursos tecnológicos de la UNAD por parte de personal nuevo, con las responsabilidades que al respecto asume la GIDT, con autorizaciones para el uso de cuentas de usuario, entre otros.

POLÍTICA SOBRE EL USO DE CONTROLES CRIPTOGRÁFICOS: Se refiere aquí la Resolución en cuestión al establecimiento de sistemas y técnicas criptográficas para protección de la información, al apoyo que debe dar la GIDT a todo el personal en el uso de herramientas tecnológicas para protección de información que debe ser cifrada, a la definición del procedimiento de gestión de claves, al establecimiento del proceso para desactivar, bloquear o eliminar accesos que no estén autorizados o estén vencidos por finalización de contratos, entre otros.

POLÍTICA DE TRANSFERENCIA E INTERCAMBIO DE INFORMACIÓN: Tiene que ver este aspecto con el uso de protocolos para transferencias de información entre unidades, usuarios y otros, con el cifrado de mensajes enviados por medios electrónicos, con la verificación de firmas de acuerdos de confidencialidad con proveedores y contratistas, con controles en el envío de información a través de impresoras y otros medios, con el cumplimiento de protocolos de manejo de la información verbal, con el control en el diligenciamiento de formularios electrónicos o de datos de la UNAD, con la definición de roles por parte de la GIDT para la administración, operación y gestión de la información, con los permisos para acceder a la Red de Área de Almacenamiento SAN, con la información clasificada como sensible o vulnerable y el uso de algoritmos de cifrado, con las responsabilidades asignadas para la clasificación, foliación y rotulación de documentos, entre otros asuntos.

POLÍTICAS DE DESARROLLO SEGURO: Se refiere aquí la citada resolución a temas como el manejo de solicitudes de desarrollos nuevos o modificaciones a lo instalado, a la realización de estos desarrollos, al manejo de los recursos asignados al grupo de desarrollo, al uso del instructivo de pruebas de software de la GIDT, entre otros.

POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIOS: Tiene que ver esta política con el manejo, control y mantenimiento de los escritorios de trabajo de todo el personal, con la presencia de documentos en ellos, con las responsabilidades adquiridas por todos en cuanto a velar por la protección de la información institucional, entre otros.

POLÍTICA DE GESTIÓN DE CAMBIOS: Se trata aquí de detallar asuntos de la política que tienen que ver con los recursos que son cobijados por el procedimiento de Gestión de Cambios y Despliegue del Servicio, con las posibles modificaciones a las condiciones actuales de funcionamiento de dichos recursos, con el cumplimiento de procedimientos y protocolos por parte de servicios tecnológicos que se encuentren tercerizados, entre otras cosas.

POLÍTICA DE VERSIONES: Tiene que ver esta política con la responsabilidad de la GIDT de gestionar la implementación, prueba y despliegue de versiones y de versiones de emergencia, así como de realizar la entrega de nuevas funcionalidades, cambios o servicios nuevos y de definir planes de pruebas, de implementar los repositorios, medios y herramientas seguras para realizar la gestión y el control de las versiones, con la aplicación de controles o actualización de versiones, entre otros.

BACKUPS O COPIAS DE SEGURIDAD: Se refiere la Resolución en este caso a la asignación de responsabilidades en la gestión de las copias de respaldo y la

administración de los equipos de respaldo masivo de datos, a la ejecución de tareas y a la definición de mecanismos adecuados de respaldo a los archivos, aplicaciones, BDs y configuración de los sistemas operativos de los servidores calificados como críticos para la UNAD, con el establecimiento de una periodicidad definida en el establecimiento de copias de respaldo, con la revisión periódica del estado de las copias, con la ubicación en centros de datos de los equipos para el respaldo de información UNAD, entre otros asuntos.
POLÍTICA DE GESTIÓN, ADMINISTRACION Y CONSERVACIÓN DOCUMENTAL:
Esta política está relacionada aquí con la obligación que tiene la UNAD de crear, organizar, preservar y controlar los archivos, garantizar espacios e instalaciones necesarias para su conservación teniendo en cuenta especificaciones técnicas establecidas por el Archivo General de la Nación, el pleno control que ejercerá la UNAD sobre su documentación (no susceptible de enajenación), con las responsabilidades sobre documentos y archivos que tienen funcionarios al desvincularse de la UNAD, con la obligación de la Secretaría General de velar por la integridad, autenticidad, veracidad y fidelidad de la información de los documentos de archivo, con el cumplimiento de los funcionarios de archivo de los principios de la ética profesional y las leyes, con la incorporación de tecnologías de avanzada en el manejo de archivos por parte de la UNAD, previos estudios técnicos, con la obligación que tiene la universidad de elaborar y adoptar tablas de retención y valoración documentales, elaborar inventarios de documentos y garantizar el derecho que tienen las personas a consultar sus documentos de archivos públicos, con el trámite para la salida temporal de documentos de archivo, con el Plan Institucional de Archivos, el Programa de Gestión Documental Físico y/o Electrónico, el Sistema Integrado de Conservación y demás instrumentos informacionales o de control, con la preservación y conservación a largo plazo de los archivos tanto físicos como electrónicos en cualquier soporte material, entre otros.
APLICABILIDAD: Tiene que ver con que el contenido del documento de la Resolución aplica a todos los procesos y procedimientos que conforman el Sistema Integrado de Gestión de la universidad, así como a todas las actuaciones administrativas que desarrollen las distintas unidades, y con las sanciones a quienes violen lo dispuesto en ella.

Como puede deducirse de este resumen, se trata de un documento institucional de la UNAD que detalla sus políticas de seguridad de la información de manera muy completa, ordenada y juiciosa y que aporta sustancialmente al proceso de implementación del SGSI de la universidad.

Más adelante, en 2016 la UNAD da un nuevo paso en esta dirección expidiendo la Resolución 8547, por la cual se reglamenta el uso de los Servicios de Tecnología de la Universidad.

Siguiendo el mismo ejercicio empleado aquí con la Resolución 4256 de 2015, se procede a presentar un resumen de esta con lo que se considera lo esencial de ella.

RESPONSABLES: Establece la responsabilidad general del asunto en la GIDT.

TIPOLOGÍAS DE SERVICIOS Y EQUIPOS DE TRABAJO: Tiene que ver con la agrupación por tipologías de los servicios de tecnología, de la siguiente manera: Plataforma Tecnológica Integrada (PTI), Soporte Técnico, Telecomunicaciones, Dotación Tecnológica, Seguridad Informática, Desarrollo de Aplicaciones, Administración de Servidores, Estrategia, Comunicación Digital, Administración de BDs, Espejos Zonales y Locales GIDT.

RESPONSABILIDADES DE LOS USUARIOS: Como su título lo indica, tiene que ver con las responsabilidades que asumen las personas que hagan uso de la infraestructura tecnológica de la universidad.

PROHIBICIONES EN EL USO DE LA INFRAESTRUCTURA TECNOLÓGICA: Con este título se hace una relación detallada y numerada de las actividades que le son prohibidas a las personas que usan la infraestructura tecnológica de la universidad.

MODALIDADES PARA LA RENOVACIÓN DE HARDWARE: Tales modalidades son: arrendamiento o leasing operativos, y adquisición.

SOLICITUDES ADICIONALES DE EQUIPOS: Donde se indica que únicamente los líderes de unidades de la universidad podrán elevar solicitudes adicionales de equipos de cómputo.

CENTROS DE DATOS: Tiene que ver con la ubicación de los elementos tecnológicos de la plataforma tecnológica integrada – PTI en Centros de Datos que cumplan con estándares internacionales.

ACOMPAÑAMIENTO TÉCNICO: Tiene que ver con la asesoría que dará la GIDT para el diseño, construcción y actualización de Centros de Datos, Centros de Cableado y otros.

EQUIPOS DE DETECCIÓN Y EXTINCIÓN DE INCENDIOS: Se relaciona con los elementos de este tipo que debe tener todo Centro de Datos y Centro de Cableado.

EQUIPOS DE MONITOREO AMBIENTAL: Tiene que ver con la instrucción de que todo Centro de Datos y Centro de Cableado deberá contar con los elementos necesario de monitoreo ambiental.

ALIMENTACIÓN Y DISTRIBUCIÓN DE ENERGÍA: En cuanto a que estos equipos deberán satisfacer las necesidades de soporte eléctrico para mantener en funcionamiento los equipos del Centro de Cómputo y los conectados a la red regulada.

DISTRIBUCIÓN DE HARDWARE SUMINISTRADO MEDIANTE LEASING: Indica que esta distribución la hará la GIDT.

ASIGNACIÓN DE EQUIPOS DE CÓMPUTO ADQUIRIDOS POR LEASING: Lo cual indica que se hará a funcionarios, contratistas y docentes de acuerdo con las necesidades del servicio.

ASIGNACIÓN DE IMPRESORAS: A cada unidad, una impresora monocromática. Si alguna requiere una impresora a color, la solicitará a la GIDT.

DEVOLUCIÓN DE HARDWARE DE MODALIDAD DE LEASING: Tiene que ver con el proceso que debe seguir la GIDT para realizar dicha devolución.

GARANTÍAS Y MANTENIMIENTO DE EQUIPOS DE LEASING: Indica que tales garantías y mantenimientos respetan las condiciones del contrato de leasing.

MANTENIMIENTO DE HARDWARE PROPIEDAD DE LA UNIVERSIDAD: Tiene que ver con la responsabilidad que lleva la GIDT para realizar el mantenimiento de equipos de cómputo y hardware propiedad de la UNAD.

OBSOLESCENCIA DE EQUIPOS: Establecida en un periodo no mayor a cinco años. Su baja la dará la Oficina de Adquisiciones e Inventarios.

RENOVACIÓN DE SOFTWARE: De lo cual se encargará la GIDT, de acuerdo con la función que cumpla.

RENOVACIÓN DE HARDWARE: Al igual que con el software, indica que de esto se encargará la GIDT, de acuerdo con las proyecciones anuales de crecimiento de cada área y del presupuesto.
EQUIPOS EXTERNOS: Dice que la UNAD no se responsabiliza del soporte técnico de los equipos personales, no pertenecientes a la UNAD. Todo equipo externo debe ser registrado al ingreso y salida de la universidad.
ALMACENAMIENTO DE INFORMACIÓN EN LOS DISPOSITIVOS DE PROPIEDAD DE LA UNIVERSIDAD: Tiene que ver con que la GIDT no se responsabiliza por la pérdida de información de índole personal en los dispositivos de la UNAD.
CARPETA COMPARTIDA INDIVIDUAL: Se relaciona con las responsabilidades de la GIDT y de cada unidad o Centro en el almacenamiento de carpetas compartidas.
ALMACENAMIENTO DE ARCHIVOS TEMPORALES, EJECUTABLES, AUDIOS Y VIDEOS NO INSTITUCIONALES: Trata de la prohibición de dicho almacenamiento en carpetas compartidas grupales e individuales.
COPIAS DE SEGURIDAD: Define la responsabilidad de funcionarios y contratistas en la realización de copias de seguridad de la información institucional a su cargo.
CARPETAS DE ESCÁNER: Determina a su vez la responsabilidad de cada funcionario o contratista de extraer información digitalizada de la carpeta de escáner asignada a la unidad.
MESA DE AYUDA: Tiene que ver con la existencia de la mesa de ayuda para la atención de solicitudes de soporte técnico, a cargo de la GIDT, con las funciones del Screener de dicha mesa, entre otros asuntos.
GESTIÓN DE PROBLEMAS: Establece el procedimiento a seguir cuando se presenta un incidente grave, repetitivo o desconocido.
GESTIÓN DE USUARIOS: Indica que esta gestión debe hacerse a través de la Mesa de Ayuda.
CREDENCIALES Y CUENTAS DE CORREO DE USUARIO: Tiene que ver con la relación entre la GIDT y la GTHUM para el manejo de la información sobre novedades en el personal administrativo, docente y contratista en cuanto a la creación o actualización del estado de cuenta de intranet y correo institucional.
INFORMACIÓN SOBRE ESTUDIANTES NUEVOS: Tiene que ver con la información que el Sistema de Registro y Control Académico – RCA entregará a la GIDT sobre estudiantes nuevos, matriculados y novedades de estos para la creación o actualización de sus cuentas de correo electrónico y licencias para descarga y uso de software Microsoft.
SUSPENSIÓN DE LAS CUENTAS DE CORREO ELECTRÓNICO Y CREDENCIALES DE ACCESO: Como se indica en el título, tiene que ver con la suspensión de cuentas de correo electrónico y credenciales de acceso a personas que se retiran.
BUZÓN DE ALMACENAMIENTO DE CORREO ELECTRÓNICO: Indica que el almacenamiento máximo del correo es definido por el proveedor del servicio y está sujeto a cambios por este.
RESPONSABILIDADES DE LOS USUARIOS CON LAS CREDENCIALES DE ACCESO Y USO DE CORREO ELECTRÓNICO INSTITUCIONAL: Incluye una relación detallada de las responsabilidades de los usuarios en los temas indicados.
RESPALDO DE LA INFORMACIÓN CUENTAS VIP: Tiene que ver las copias de respaldo de la información de correo electrónico de directivos o funcionarios que tengan a cargo información reservada o controlada de la institución y se retiren.
ENVÍO MASIVO DE INFORMACIÓN INTERNA: Se relaciona con el envío por parte de los jefes de unidades de una solicitud para tal fin usando el correo institucional.

SOPORTE BRINDADO POR LA GIDT: Donde se indica que este soporte se brindará únicamente a lo que se encuentre alojado en servidores administrados por la UNAD. MESA TÉCNICA DE LA GIDT E INTEGRANTES: Tiene que ver con la creación de esta mesa para analizar, conceptuar y dar lineamientos sobre los proyectos, servicios y/o solicitudes de ámbito técnico y tecnológico que impliquen la actuación de la GIDT. Esta mesa estará integrada por los líderes de cada uno de los equipos de trabajo de la GIDT"[56] .

Como se deduce fácilmente se trata también de un documento muy completo que puede ser consultado en sus detalles por los interesados lectores de esta monografía en el Anexo D. Numeral 5.

c. ANÁLISIS DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA DE LAS UNIVERSIDADES PÚBLICAS DEL EJE CAFETERO

Después de haber realizado una lectura de todos los documentos que han servido de instrumento para conocer sobre las políticas de seguridad implementadas dentro de las universidades públicas del Eje Cafetero, se ha llegado a la conclusión de que cada entidad tiene definidas sus políticas de forma algo diferente y que, aunque todo hace parte de un SGSI, por lo menos una de ellas hasta el momento sólo cuenta con este instrumento para resguardar su información. A continuación, se hace un análisis de las políticas implementadas por cada una de las universidades.

Al revisar el documento de la Universidad Nacional de Colombia que se encuentra publicado en la página web de la DNTIC se puede observar que, efectivamente, la universidad tiene un documento que habla de políticas de seguridad informática, pero, para la autora de esta monografía, ellos no son muy claros en las políticas que mencionan (esto pudiera deberse a que tal vez exista un documento interno que no es divulgado a toda la comunidad y al cual sólo pueda acceder la comunidad universitaria como tal, por temas de confidencialidad que son totalmente entendibles. Sin embargo, la hipotética existencia de ese documento estaría por comprobarse). Cuando se habla de que la política de seguridad informática no es muy clara lo que se quiere dar a entender es que la universidad debería ser más concreta, más explícita, más detallada, en sus políticas de seguridad informática; por ejemplo, detallando los asuntos y procesos sobre el manejo del correo electrónico, el control de acceso de los usuarios (uso de claves, etc.), acceso a redes y a los servicios en red, entre otros. Esto se hace necesario porque dentro de la universidad existen personas que se mueven en un mundo multidisciplinar y que,

[56] Políticas Marco de Referencia del Sistema de Gestión de Seguridad de la Información (SGSI). [en línea]. 2015.

por obvias razones, en muchos de esos casos no manejan a cabalidad el tema de la seguridad informática. Por tal motivo, las políticas de seguridad informática de la universidad deberían estar encaminadas a que todo el mundo pudiera comprender totalmente lo que la universidad tiene planteado al respecto, con el fin de evitar problemas de comprensión que pueden afectar gravemente la información. No se debe olvidar que el usuario viene siendo uno de los eslabones más débiles cuando de seguridad informática se trata, por lo que se hace necesario, primero, elaborar unas políticas de seguridad informática entendibles para cualquier persona que haga parte de la universidad y, segundo, estarlos capacitando constantemente para que conozcan los peligros que pueden afectar la información que ellos manejan.

En lo que tiene que ver con el análisis a las políticas de seguridad informática de la Universidad de Caldas, se puede resaltar que esta universidad en un documento del año 2013 presenta unas políticas de seguridad informática, pero está enfocada a todo el tema de seguridad de su área de sistemas, mas no involucra a la comunidad académica en general. No se habla del uso del correo electrónico institucional, de las claves que utilizan los usuarios, entre otros. (es de anotar que, durante el contacto con el ingeniero encargado del área de sistemas, se pudo conocer que actualmente están actualizando dichas políticas y es factible que todo esto se encuentre incluido en un nuevo documento que se publicaría más adelante).

En cuanto al análisis que se le pudo realizar a la información contenida en el documento de la Universidad Tecnológica de Pereira UTP, se puede colegir que las políticas de seguridad informática implementadas por dicha universidad son muy claras y ayudan a la comunidad universitaria en general. Claro está que también se puede decir que falta hablar de otras políticas de seguridad informática que pueden no aparecer en este documento por temas de confidencialidad, porque hay que resaltar que las entidades llegan a ser muy celosas con su información. Se trata, pues, de un documento muy completo y explícito sobre lo que deben ser las políticas de seguridad de la información de una universidad pública.

Por su parte, al realizar una lectura de la Hoja de ruta que habla sobre la implementación de las políticas de seguridad de la información de la Universidad del Quindío, se puede deducir que dicho documento define muy bien la información que al respecto se tiene; sin embargo, dentro de lo que se define como políticas -y quizás porque ha pasado un tiempo desde que este se publicó- hace falta incluir algunas otras políticas que apunten a salvaguardar mejor la información.

En cuanto a lo que trata de la UNAD, fue posible concluir que no sólo ha apuntado a lo que tiene que ver con políticas de seguridad, sino que también se ha adentrado en aspectos más a fondo relacionados con un SGSI. Por esto, aquí se destaca que

dicha universidad tiene muy clara la importancia de salvaguardar su información no sólo a partir de unas políticas de seguridad, sino que esto debe hacerse a partir de un SGSI bien estructurado e implementado.

Finalmente, como complemento de este análisis se detalla si estas universidades usan o aplican alguna norma, estándar o metodología asociada a los sistemas de gestión de la información.

La Universidad del Quindío, en su documento Hoja de Ruta. IMPLEMENTACIÓN DE LAS POLITICAS DE SEGURIDAD DE INFORMACIÓN[57] y en el cual define sus políticas de seguridad informática, adopta como normas para la elaboración de dicho documento varias de las normas de la familia ISO/IEC 27000 (que, como se sabe, son los estándares de seguridad más usados en el mundo). Se destaca entonces aquí el uso de las normas ISO 27001:2013 y 27002 como las más relevantes en este documento.

Adicionalmente, y con el fin de identificar los riesgos, en el mismo documento se encuentra que es posible utilizar el conjunto de controles de la norma NTC/ISO 27002 y NIST SP800-53.

Y más adelante, en el capítulo del PLAN DE ACCIÓN GENERAL GOBIERNO DE TECNOLOGÍA del mismo documento tiene como una de sus propuestas “evaluar, seleccionar e implementar un estándar, regulación y/o mejores prácticas para gobierno de TI como: ITIL, ISO-20000, CobiT, SOX, ISO27001, PCI”[58] .

En cuanto a la Universidad de Caldas, no se tiene información de cuáles son los estándares de seguridad, metodologías, entre otros, que se utilizan, ya que, como se dijo anteriormente, la universidad tiene subcontratado sus servicios de seguridad informática y, por tal motivo, es la empresa encargada de esa información la que tiene conocimiento al respecto. Las entrevistas que se tuvieron se hicieron con el Ingeniero Jefe del área de sistemas y no se pudo tener acceso a dicha información, ni se encontraron documentos en internet, posiblemente por temas de confidencialidad que se resalta es tan importante para los expertos en el tema de seguridad informática.

[57] Hoja de Ruta - IMPLEMENTACIÓN DE LAS POLITICAS DE SEGURIDAD DE INFORMACIÓN. Op. cit., p. 4.
[58] Ibít., p. 12

De igual manera, de la UTP no se logró tener información de cuáles son los estándares de seguridad, metodologías, entre otros, que se utilizan. Los contactos que se tuvieron telefónicamente y por medio de correos electrónicos no permitieron lograr el cometido de acceder a este tipo de información, ni se encontraron documentos en internet. Aquí se cree también que esto se debe muy posiblemente a asuntos relacionados con la confidencialidad de la información que muchas organizaciones manejan en el tema de la seguridad informática.

La UNAD crea una política de seguridad de la información de la cual se habla en la Resolución 4256[59], que está basada en la norma ISO 27001:2013. Lo que busca con ello es asegurar el establecimiento, la implementación, la operación, el seguimiento, la revisión, el mantenimiento y mejora del SGSI. Dentro de lo encontrado en dicha Resolución no se evidenció información de otras normas o de metodologías que tenga que ver con los SGSI.

La Universidad Nacional de Colombia[60], en aras de cumplir con las disposiciones legales y normativas en el tema de la seguridad informática, contempla en el documento Política de Seguridad Informática y de la Información que adopta las disposiciones que se manejan en la norma internacional ISO 27001.

[59] Políticas Marco de Referencia del Sistema de Gestión de Seguridad de la Información (SGSI). Op. cit., p. 2

[60] Política de Seguridad Informática y de la Información. Universidad Nacional de Colombia. Op cit., p. 2.

15. PROPUESTA CON MECANISMOS PARA REFORZAR LA IMPORTANCIA DE UN SGSI EN LAS UNIVERSIDADES PÚBLICAS DEL EJE CAFETERO

Después de analizar la situación actual de si existe o no un SGSI en cada una de las cinco universidades públicas del Eje Cafetero y de las políticas de seguridad informática que estas tendrían o no implementadas, se identificaron de alguna manera las falencias que en este sentido podrían tener dichas universidades. Por ello, se vio la necesidad de realizar una propuesta que describa los mecanismos para reforzar, ante los funcionarios de estas, la trascendencia que tiene el contar con un SGSI. Esta propuesta metodológica podría ser:

Entregar una copia de la monografía a cada funcionario de las oficinas de las TIC que diligenció el cuestionario, en copia papel debidamente encuadernada y en copia digital (CD adjunto), tal y como se les anunciara durante el trámite del diligenciamiento del cuestionario.

Preparar una charla corta o conferencia apoyada en diapositivas sobre la trascendencia e importancia de los SGSI en las universidades públicas, y concertar con los citados funcionarios una fecha y hora para hacer esta charla, la cual se basaría en los siguientes asuntos:

- Necesidad creciente de asegurar la información institucional
- Evolución de los ataques informáticos
- Amenaza, vulnerabilidad y riesgos informáticos
- Medidas estructurales frente a los riesgos informáticos: políticas de seguridad informática, adopción de un SGSI, implementación
- Importancia de la auditoría de sistemas
- Necesidad de la revisión de las normas de cara a su actualización
- Dinámica de los SGSI frente a los adelantos tecnológicos y frente a nuevos tipos de ataques informáticos (por ejemplo, ataques a información en la nube)

16. CONCLUSIONES

Se consideran logrados los objetivos de la monografía en cuanto a que se tiene con ella un panorama bastante claro del estado de cosas de los sistemas de gestión de la información que se lleva en las cinco universidades públicas del Eje Cafetero: Universidad Nacional de Colombia sede Manizales, Universidad de Caldas, Universidad Tecnológica de Pereira, Universidad del Quindío y Universidad Nacional Abierta y a Distancia UNAD sede Dosquebradas, en las cuales se pudo indagar el conocimiento y uso que en ellas se tiene de normas -especialmente la 27001- y metodologías para la definición de sus políticas de seguridad informática y otras acciones en dirección a poner en marcha -y lograrlo en algunos casos- un SGSI.

El uso de una herramienta como un cuestionario para indagar tales cosas, con la cual se ganó la confianza de los funcionarios que lo contestaron -a pesar de que pudieron mostrarse algo más recelosos y reservados, pero no lo fueron a nuestro parecer- contribuyó sustancialmente al logro de los resultados destacados arriba. Esto pudiera interpretarse como una forma de manifestar gran interés en el tema, de demostrar que se estaba efectivamente trabajando de manera ardua en él y que su importancia y trascendencia se encontraba al orden del día en cada una de sus universidades. Se considera que, al calor de charlas y de cuestionarios y de enterarlos de la ejecución de esta monografía se hizo por parte de la autora un reforzamiento en ellos de la importancia del asunto ante las vulnerabilidades y riesgos que enfrentan por ataques informáticos, cada vez mayores.

Como asunto particular, pero de mucha importancia, sorprende que el 40% de las universidades que aquí se están estudiando no cuenten con funcionarios que sean expertos en el tema de la seguridad informática, porque esta es una de más manifestaciones más contundentes de la vulnerabilidad de la entidad frente a ataques informáticos, a pesar de la disposición de ánimo y el conocimiento que al respecto pudiera tener el funcionario actualmente encargado.

Del análisis discriminado por universidad en el capítulo 11, el autor encuentra de manera satisfactoria que los adelantos en la implementación de un SGSI logrados por las Universidades UNAD y UTP se muestran hasta ahora mayores que los alcanzados por las otras tres universidades, pero mantiene la esperanza de que ellas estén en el proceso para igualar y hasta superar los de las mencionadas, para lo cual mantendrá sus ojos puestos en ello, en su condición de especialista en el área que está cercana -geográfica y profesionalmente- a dos de ellas, la UNAL y la UDECALDAS.

La autora considera que hubiera sido posible conseguir información más particularizada en cada universidad sobre detalles de los estándares y metodologías usados, pero también concluye que esto tal vez no se tuvo por razones obvias, como los criterios de confidencialidad con que deben manejar hacia afuera de la entidad dicha información.

Finalmente, se tiene un documento monográfico bien concebido y suficientemente detallado, que establece diagnósticos y análisis de la situación de los SGSI en cinco universidades públicas del eje cafetero colombiano, da claridades sobre la aplicación de normas internacionales y nacionales al respecto, y que aspira a llevar a las directivas que menos han avanzado en el asunto a ampliar sus niveles de conciencia sobre la inmensa importancia que tiene hoy en día la implementación de un SGSI en su universidad, so pena de incurrir en pérdidas graves de la información o en daños a la misma por ataques informáticos, causados por inescrupulosos o por hackers que tienen un interés particular en alterar y dañar el bien preciado de la información institucional.

17. RECOMENDACIONES

Como complemento de las conclusiones de este trabajo y apoyados en ellas, se hacen las siguientes recomendaciones:

Si alguna universidad de las estudiadas aquí no posee aún un SGSI, convendría trazarse como una meta de su desarrollo institucional el contar con este sistema en un plazo no mayor a dos (2) años.

Para poder garantizar lo anterior, se haría necesario reforzar las OTIC de esas universidades tanto en su estructura orgánica como en la vinculación de personal especializado en el tema de la seguridad informática y de los SGSI.

En algunos casos concretos conocidos por la autora de la monografía, se deja entrever cierta laxitud y hasta baja de guardias en el seguimiento y evaluación de los procesos que llevan, así como en la aplicación de las políticas de seguridad informática que tienen, lo que justifica el recomendar acciones de auditoria periódicas de dichos procesos (por ejemplo, cada año).

Se debería buscar, desde un esfuerzo interinstitucional de las universidades públicas y otras, hacerle ver a MINTIC la necesidad de gestionar un proyecto de ley modificatorio de la Ley 1273 de 2009, dada la desactualización que esta presenta en cuanto a la identificación de ataques y delitos informáticos, debido a la evolución que estos han ido teniendo de manera acelerada en los últimos años, con las particularidades que se tienen para las universidades públicas.

Finalmente, todas las universidades públicas que tengan implementado un SGSI deben revisar permanentemente las actualizaciones que se van teniendo en el mundo de las normas y estándares para adoptarlas y con ellas actualizar tales SGSI. Por ejemplo, lo que se está viviendo con la ISO-IEC 27001 y toda esa familia de normas, sin descartar la conveniencia que pudiera tener el país a través del ICONTEC de adoptar otra familia de normas que estuvieran utilizándose con éxito en otros países.

18. BIBLIOGRAFÍA

ANCHUNDIA, Carlos. Ciberseguridad en los sistemas de información de las universidades, Revista Científica - Dominio de las Ciencias. Vol. 3, agos. 2017, pp. 200-217. Disponible en: <http://dx.doi.org/10.23857/dom.cien.pocaip.2017.3.mono1.ago.200-217> ISSN: 2477-8818

ALEMÁN, Helena y RODRÍGUEZ, Claudia. Metodologías para el análisis de riesgos en los SGSI. En: Revista Especializada en Ingeniería - UNAD. 2015. Volumen 9. Disponible en: <http://hemeroteca.unad.edu.co/index.php/publicaciones-e investigacion/article/view/1435/1874> ISSN 1900-6608

ÁLVAREZ, Andrés y GÓMEZ FERNÁNDEZ, Ana. Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes. España. AENOR. 2009. 201p. ISBN: 9788481436020.

BELLOCH, Consuelo. Las Tecnologías de la Información y Comunicación en el aprendizaje. [en línea]. 2012. [2018]. Disponible en <http://www.uv.es/bellochc/pedagogia/EVA1.pdf>

BETECH. Si recibes un email con uno de estos asuntos, bórralo directamente. [en línea]. 2019. [2019]. Disponible en: <https://as.com/meristation/2019/09/24/betech/1569350875_189985.html>

CISCO. Reporte Anual de Ciberseguridad. [en línea]. 2018. [2018]. Disponible en: <https://www.cisco.com/c/dam/global/es_mx/solutions/pdf/reporte-anual-cisco-2018-espan.pdf>

COLOMBIA. MINTIC. Ley 1273 de 2009. (05 de 01 de 2009). "Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado – denominado “de la protección de la información y de los datos”. Y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Bogotá, D.C. 2009. p. 4. Disponible en: https://mintic.gov.co/portal/604/articles-3705_documento.pdf

COLOMBIA. UNAD. Acuerdo 0029. (13 de 12 de 2013). Por el cual se expide el Reglamento Estudiantil de la Universidad Nacional Abierta y a Distancia (UNAD) y se dictan otras disposiciones. Bogotá, D.C. 2013. p. 48. Disponible en: https://sgeneral.unad.edu.co/images/documentos/consejoSuperior/acuerdos/2013/COSU_ACUE_029_20131229.pdf

COLOMBIA. UNAD. Resolución No. 004793. (22 de agosto de 2014). Por la cual se crea la Política de Seguridad de la Información para la Universidad Nacional Abierta y a Distancia – UNAD. Bogotá, D.C. 2014. p. 18. Disponible en: https://sgeneral.unad.edu.co/images/documentos/RESO_NORMOGRAMAS/RESO_4793_20130822.pdf

COLOMBIA. UNAD. Resolución No. 006858. (22 de agosto de 2014). Por la cual se conforma el Sistema Integrado de Gestión – SIG de la Universidad Nacional Abierta y a Distancia – UNAD, se establece la Política Integrada de Gestión, y se derogan las resoluciones 2271 de 2008, 2627 de 2008, 2055 de 2007 y 02861 de 2010. Bogotá, D.C. 2014. p. 3. Disponible en: https://sig.unad.edu.co/documentos/sig/resoluciones_sig/Resolucion_7966_2014_SIG_modificatoria.pdf

COLOMBIA. UNAD. Resolución No. 007966. (16 de octubre de 2014). Por la cual se modifica la Resolución No. 6858 del 22 de agosto de 2014, por medio de la cual se conforma el Sistema Integrado de Gestión – SIG de la Universidad Nacional Abierta y a Distancia – UNAD, se establece la Política Integrada de Gestión, y se derogan las resoluciones 2271 de 2008, 2627 de 2008, 2055 de 2007 y 02861 de 2010. Bogotá, D.C. 2014. p. 3. Disponible en: https://sig.unad.edu.co/documentos/sig/resoluciones_sig/Resolucion_7966_2014_SIG_modificatoria.pdf

COLOMBIA. UNAD. Resolución No. 8547. (08 de septiembre de 2016). Por la cual se reglamenta el uso de los Servicios de Tecnología de la Universidad Nacional Abierta y a Distancia – UNAD. Bogotá, D.C. 2016. p. 15. Disponible en: https://sgeneral.unad.edu.co/images/documentos/RESO_NORMOGRAMAS/RESO_8547_20160908.pdf

COLOMBIA. UNAL. Acuerdo 228. (Acta 07 del 26 de julio de 2016). Por el cual se expide la Política de Seguridad Informática y de la Información de la Universidad Nacional de Colombia. Bogotá, D.C. 2016. p. 2. Disponible en: http://www.legal.unal.edu.co/rlunal/home/doc.jsp?d_i=87116

COLOMBIA. UTP. Resolución No. 6123. (05 de 12 de 2017). Por medio del cual se adopta el manual general de directrices del Sistema de Gestión de Seguridad de la Información de la Universidad Tecnológica de Pereira. Pereira. 2017. p. 60. Disponible en: <https://www.utp.edu.co/cms-utp/data/bin/UTP/web/uploads/media/secretaria/documentos/RR%206123%20DE%202017-SEGURIDAD%20DE%20LA%20INFORMACION.pdf>

Correos electrónicos cruzados con funcionarios de las Universidades (Nacional, de Caldas, del Quindío y UNAD).

DÍAZ, Yanet; PÉREZ-DEL CERRO, Yunetsi y PROENZA, Dayami. Sistema para la Gestión de la Información de Seguridad Informática en la Universidad de Ciencias Médicas de Holguín. En: Revista Ciencias Holguín. (abril - junio, 2014). Vol. XX, Núm. 2. Disponible en: <http://www.redalyc.org/articulo.oa?id=181531232002> E-ISSN: 1027-2127

EL COMERCIO (Tecnología). Ataques informáticos aumentan un 60% en Latinoamérica en 2018. Ecuador. 13, agosto, 2018. [en línea]. Disponible en: <https://www.elcomercio.com/tendencias/seguridadinformatica-ciberataques-latinoamerica-kaspersky-informe.html>

EL ESPECTADOR (Judicial). Fiscalía imputará cuatro delitos a director de oficina de interceptaciones ilegales. Bogotá. 06, 05, 2014. Disponible en: <https://www.elespectador.com/noticias/judicial/fiscalia-imputara-cuatro-delitos-director-de-oficina-de-articulo-490789>

EL TIEMPO (TECNÓSFERA). En 2017 se reportaron más de 14.600 vulnerabilidades informáticas 15, enero, 2018. Disponible en: <https://www.eltiempo.com/tecnosfera/novedades-tecnologia/numero-de-vulnerabilidades-informaticas-registradas-en-2017-171214>

ESAN. Sistema de Gestión de Seguridad Informática: ¿por qué es útil y cómo se aplica? Lima. [en línea]. 2018. [2018]. Disponible en: <https://www.esan.edu.pe/apuntes-empresariales/2018/08/sistema-de-gestion-de-seguridad-informatica-por-que-es-util-y-como-se-aplica/>

FISCALIA GENERAL DE LA NACIÓN. Condenado hacker ecuatoriano por acceso a los correos del exvicepresidente Francisco Santos. Bogotá. 13, 08,2015.

Disponible en: <https://www.fiscalia.gov.co/colombia/noticias/condenado-hacker-ecuatoriano-por-acceso-a-los-correos-del-exvicepresidente-francisco-santos/>

FERNÁNDEZ BARCELL, Manuel. Estudio de una Estrategia para la implantación de los sistemas de gestión de la seguridad de la información. Andalucía (Cádiz), 2010. Trabajo de Doctorado (Plan 7440 Ingeniería en Automática y Electrónica Industrial, Ingeniería Informática y Sistemas Eléctricos). Universidad de Cádiz. Departamento de Lenguajes y Sistemas Informáticos. Disponible en: http://www.mfbarcell.es/conferencias/Metodolog%C3%ADas%20de%20seguridad_2.pdf

Funcionario OTIC. Universidad Nacional de Colombia – Sede Manizales. Manizales, Colombia. Conversación informal con funcionario de la OTIC. (R. E. Giraldo, Entrevistador). 2018.

Gobierno de España – Ministerio de Hacienda y Administraciones Públicas. MAGERIT - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I – Método. España. Versión 3.0, 2012. 127p.

Gobierno de España – Ministerio de Hacienda y Administraciones Públicas. MAGERIT – Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II - Catálogo de Elementos. España. Versión 3.0, 2012. 75p.

Gobierno de España – Ministerio de Hacienda y Administraciones Públicas. MAGERIT – Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro III - Guía de Técnicas. España. Versión 3.0, 2012. 42p.

GÓMEZ FERNÁNDEZ Luis y FERNÁNDEZ RIVERO, Pedro. Cómo implantar un SGSI según UNE-ISO/IEC 27001. España, AENOR - Asociación Española de Normalización y Certificación, 2015. pp 156. ISBN de libro impreso: 9788481439007 Disponible en: http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=3&docID=11087537&tm=1456691767083

GÓMEZ VIEITES, Álvaro. Auditoría de seguridad informática. Capítulo 1. Vulnerabilidad de los sistemas informáticos. Bogotá, Ediciones de la U, 2013. 140p. ISBN 978-958-762-085-6.
GÓMEZ, VIETES, Álvaro. Gestión de incidentes de seguridad informática. [en línea]. ES: RA-MA Editorial. Madrid, 2014, RA-MA. 124p. libro impreso: 9788492650774

Disponible en: <http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?docID=11046422> ISBN de libro electrónico: 9788499643311.

GÓMEZ VIEITES, Álvaro. Seguridad Informática básico. Bogotá. ECOE Ediciones. 2011. 142p. ISBN 978-958-648-721-4.

ISOTOOLS. Blog Calidad y Excelencia. Cómo implementar un Sistema de Gestión de Seguridad de la Información. [en línea]. 2015. [2019]. Disponible en: <https://www.isotools.org/2015/08/13/como-implementar-un-sistema-de-gestion-de-seguridad-de-la-informacion/>

ISOTOOLS. Blog Calidad y Excelencia. ¿Cómo llevar a cabo la mejora continua del SGSI? [en línea]. 2019. [2019]. Disponible en: <https://www.isotools.org/2019/01/24/como-llevar-a-cabo-la-mejora-continua-del-sgsi/>

ISOTOOLS. Blog Corporativo. ¿Por qué implementar un SGSI? [en línea]. 2015. [2019]. Disponible en: <https://www.isotools.pe/por-que-implementar-sgsi/>

ISOTOOLS. Blog Calidad y Excelencia. ISO 27001: Seguridad informática y seguridad de la información, Colombia. [en línea]. 2018. [2018]. Disponible en: <https://www.isotools.org/2015/01/05/iso-27001-seguridad-informatica-seguridad-informacion/>

ISO 27000.es. El portal de ISO 27001 en español. [en línea]. 2018. [2018]. Disponible en: <http://www.iso27000.es/iso27000.html>

ISO27000.es. Sistema de Gestión de la Seguridad de la Información. [en línea]. 2012. [2018]. Disponible en: <http://www.iso27000.es/download/doc_sgsi_all.pdf>

IT Governance. 9 razones para implementar un Sistema de Gestión de Seguridad de la Información (SGSI), Reino Unido. [en línea]. 2018. [2018]. Disponible en: <https://www.itgovernance.eu/blog/es/9-razones-para-implementar-un-sistema-de-gestion-de-seguridad-de-la-informacion-sgsi>

LA PATRIA (Educación). Están falsificando la Andrés Bello: Icfes. [en línea]. 11, enero, 2017. Disponible en: <http://www.lapatria.com/educacion/estan-falsificando-la-andres-bello-icfes-341591>

LISOT. ¿Qué es un Sistema de Gestión de la Seguridad de la Información (SGSI)? [en línea]. 2018. [2019]. Disponible en: <https://www.lisot.com/que-es-un-sistema-de-gestion-de-la-seguridad-de-la-informacion-sgsi/>

MANJÓN CABEZA, José. Elaboración de un Plan de Implementación de la ISO/IEC 27001:2013. España, 2014. Trabajo de grado (Máster Interuniversitario en Seguridad de las TIC). Universitat Oberta de Catalunya. Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/43102/6/manjonikoTFM0615memoria.pdf

MEJÍA, Fernando. Universidad Nacional de Colombia – Sede Manizales. Manizales, Colombia. Charla con profesor. (R. E. Giraldo, Entrevistador). 2018.

MINTIC. Manual de Normas y Políticas de Seguridad Informática. [en línea]. (26 de 09 de 2014). [2018]. Disponible en: https://www2.sgc.gov.co/ControlYRendicion/TransparenciasYAccesoAlaInformacion/CircularesManuales/MO-TEC-001-I.pdf

MOLANO ESPINEL, Rafael. Estrategia para implementar un Sistema de Gestión de la Seguridad de la Informaciónbasada en la Norma Iso 27001 en el Área de TI para la Empresa Market Mix. Bogotá, 2017. Trabajo de grado (Especialista en Auditoria de Sistemas). Universidad Católica de Colombia. Facultad de Ingeniería. Disponible en: https://repository.ucatolica.edu.co/bitstream/10983/15240/1/Esp%20Auditoria%20de%20sistemas.pdf

NETWORKS, O. Tipos de ataques informáticos y previsiones para el 2018. [en línea]. 2018. [2018]. Disponible en: <https://www.optical.pe/tipos-de-ataques-informaticos-y-previsiones-para-el-2018/>

PALLAS MEGA, Gustavo. Metodología de Implantación de un SGSI en un grupo empresarial jerárquico. Montevideo, Uruguay. 2009. Tesis de Maestría en Ingeniería en Computación. Universidad de la República. Instituto de Computación – Facultad

de Ingeniería. Disponible en: https://www.fing.edu.uy/inco/pedeciba/bibliote/cpap/tesis-pallas.pdf

PÉREZ PORTO, Julián y MERINO, María. Definición de seguridad informática. [en línea]. 2008. [2018]. Disponible en: <https://definicion.de/seguridad-informatica/>

PÉREZ, Ricardo, et al. La sociedad del conocimiento y la sociedad de la información como la piedra angular en la innovación tecnológica educativa. En: Revista iberoamericana para la investigación y el desarrollo educativo. (enero – junio, 2018). Vol. 8, Núm. 16. Disponible en: <http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2007-74672018000100847> ISSN 2007-7467.

RAMÍREZ MUNIVE, Yair, et al. Tecnologías de Información y Comunicación en las Organizaciones. México,D. F., 2016. Publicaciones Empresariales UNAM. 45p. ISBN impreso: 978-607-02-7341-4 e ISBNe electrónico: 978-607-02.

RCG COMUNICACIONES. 7 políticas de seguridad de red que debes conocer. [en línea]. 2018. [2018]. Disponible en: <http://rcg-comunicaciones.com/7-politicas-de-seguridad/>

SAFESOCIETY. IMPORTANCIA DE IMPLEMENTAR UN SGSI EN NUESTRA ORGANIZACIÓN. [en línea]. 2018. [2018]. Disponible en: <https://www.safesociety.co/importancia-de-implementar-un-sgsi-en-nuestra-organizacion/>

SAMPEDRO, José. Técnica y Globalización. Boletín Económico del ICE, N° 2750. [en línea]. 2002. [2018]. Disponible en: <https://dialnet.unirioja.es/servlet/articulo?codigo=291209>

SANCHÉZ, Zulay. Análisis de la Ley 1273 de 2009 y la evolución de la ley con relación a los delitos informáticos en Colombia [en línea]. Chiquinquirá. 2017. Trabajo de grado (Especialista en seguridad informática). Universidad Nacional Abierta y a Distancia – UNAD. Escuela de Ciencias Básicas e Ingeniería. Disponible en: <https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/11943/1/1053323761.pdf>

SEGURIDAD INFORMATICA EN LAS INSTITUCIONES DE EDUCACION SUPERIOR. UNIVERSIDAD DE CALDAS – Oficina de Sistemas. [en línea]. 2013. [2019]. Disponible en: <https://docplayer.es/2402261-Seguridad-informatica-en-las-instituciones-de-educacion-superior.html>

SGSIBlog especializado en Sistemas de Gestión de Seguridad de la Información. ¿Cómo influye ISO 27001 en las universidades? [en línea]. 2014. [2018]. Disponible en: <https://www.pmg-ssi.com/2014/04/como-influye-iso-27001-en-las-universidades/>

SGSIBlog especializado en Sistemas de Gestión de Seguridad de la Información. ¿Qué es SGSI? [en línea]. 2015. [2018]. Disponible en: <https://www.pmg-ssi.com/2015/07/que-es-sgsi/>

SGSIBlog especializado en Sistemas de Gestión de Seguridad de la Información. ¿Qué objetivo persigue la seguridad de la información? [en línea]. 2017. [2018]. Disponible en: <https://www.pmg-ssi.com/2017/08/que-objetivo-persigue-la-seguridad-de-la-informacion/>

TARAZONA T. Cesar. Amenazas informáticas y seguridad de la información. En: CSI/FBI Computer Crime and Security Survey, 138. (2007). Vol. 28 Núm. 84. Disponible en: https://revistas.uexternado.edu.co/index.php/derpen/article/download/965/915/

UNIVERSIDAD DEL ATLÁNTICO. Alcance del SGSI Universidad del Atlántico. [en línea]. 2016. [2018]. Disponible en: <https://www.uniatlantico.edu.co/uatlantico/node/5604>

UNIVERSIDAD DE CALDAS. Campus y Espacios Institucionales. [en línea]. [en línea]. [2019]. Disponible en: <http://www.ucaldas.edu.co/portal/sedes-y-espacios-institucionales/>

UNIVERSIDAD DE CALDAS. Historia de la Universidad. [en línea]. 2019. [2019]. Disponible en: <http://www.ucaldas.edu.co/portal/historia-de-la-universidad/>

UNAD. Mapa de Sedes UNAD. [en línea]. 2017. [2019]. Disponible en: <https://directorio.unad.edu.co/images/mapa/Mapa_centros_UNAD_2017.pdf>

UNAD. Políticas Marco de Referencia del Sistema de Gestión de Seguridad de la Información (SGSI). [en línea]. 2015. [2019]. Disponible en: <https://gidt.unad.edu.co/images/Documentos/20150303%20-%20Resolucin%204256%20-%20Polticas%20Marco%20de%20Referencia%20del%20SGSI.pdf>

UNAD. Reseña histórica. [2019]. Disponible en: <https://informacion.unad.edu.co/transparencia-y-acceso-a-la-informacion/acerca-de-la-unad/resena-historica>

UNAL. Historia. [en línea]. 2018. [2019]. Disponible en: <http://lineadetiempoun.unal.edu.co/detail/#!/page/hitos-historicos/mainmenu-app/introduccion>

UNAL. Política de Seguridad Informática y de la Información. [en línea]. 2015. [2019]. Disponible en: <http://dntic.unal.edu.co/images/seguridad/PolticadeSeguridadInformaticaydelaInformacion.pdf>

UNAL. UN en un vistazo. [en línea]. [2019]. Disponible en: <http://estadisticas.unal.edu.co/index.php?id=2>

UNAL – Sede Manizales. RESEÑA HISTORICA. [en línea]. 2017. [2019]. Disponible en: <http://www.manizales.unal.edu.co/menu/institucional/resena-historica/>

UNIVERSIDAD DE LOS LLANOS. Manual del Sistema de Gestión de Seguridad de la Información (SGSI). [En línea]. 2013. [2018]. Disponible en: <http://pruebapagina.unillanos.edu.co/docus/MN-GRT-XX%20MANUAL%20DEL%20SISTEMA%20DE%20GESTION%20DE%20SEGURIDAD%20DE%20LA%20INFORMACION%20CORREGIDO.pdf>

UNIVERSIDAD DEL QUINDÍO. Historia Universidad del Quindío. [en línea]. 2018. [2019]. Disponible en: <https://www.uniquindio.edu.co/publicaciones/historia_universidad_del_quindio_pub>

UNIVERSIDAD DEL QUINDÍO. RESEÑA HISTÓRICA DE LA UNIVERSIDAD DEL QUINDÍO. [en línea]. 2018 [2019]. Disponible en: <https://www.uniquindio.edu.co/publicaciones/historia_universidad_del_quindio_pub>

UNIVERSIDAD DEL QUINDÍO. Hoja de Ruta - IMPLEMENTACIÓN DE LAS POLITICAS DE SEGURIDAD DE INFORMACIÓN. [en línea]. 2015. [2019]. Disponible: <http://www.uniquindio.edu.co/descargar.php?idFile=23227>

UNIVERSIDAD LIBRE. Nuestro Sistema de Gestión de Seguridad de la Información (SGSI). [en línea]. 2009. [2018]. Disponible en: <http://www.unilibre.edu.co/bogota/ul/noticias/noticias-universitarias/153-nuestro-sistema-de-gestion-de-seguridad-de-la-informacion-sgsi>

UTP. 40 años. [en línea]. 2013. [2019]. Disponible en: <https://www.utp.edu.co/institucional/40-anos.html>

UTP. Estadísticas e Indicadores Estratégicos. [en línea]. [2019]. Disponible en: <https://www.utp.edu.co/estadisticas-e-indicadores/>

UTP. Reseña histórica UTP. [en línea]. 2010 [2019]. Disponible en: <https://www.utp.edu.co/institucional/resena-historica>

UTP. MANUAL GENERAL DE DIRECTRICES del SGSI. [en línea]. 2017. [2019]. Disponible en: <https://www.utp.edu.co/cms-utp/data/bin/UTP/web/uploads/media/calidad/documentos/1313-MGD-01-Manual-General-de-Directrices-del-SGSI-V2.pdf>

VALENCIA DUQUE Francisco Javier y OROZCO ALZATE Mauricio. Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. En: RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao. (Junio, 2017). disponible en: https://www.researchgate.net/publication/317904811_Metodologia_para_la_implementacion_de_un_Sistema_de_Gestion_de_Seguridad_de_la_Informacion_basado_en_la_familia_de_normas_ISOIEC_27000

WIKIPEDIA. Sistema Universitario Estatal (SUE). [en línea]. 2018. [2018]. Disponible en: <https://es.wikipedia.org/wiki/Sistema_Universitario_Estatal>

VILLAMIZAR, Iván. GUIA TRABAJO DE GRADO MODALIDAD MONOGRAFIA MAESTRIA EN ADMINISTRACIÒN DE LAS ORGANIZACIONES. Bogotá, 2017. Disponible en: https://es.slideshare.net/IVANVILLAMIZAR/unad-monografa-estructura

19. ANEXOS

ANEXO A.

“LEGISLACIÓN COLOMBIANA SOBRE DELITOS INFORMÁTICOS

LEY 1273 DEL 05 DE ENERO DE 2009

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

El CONGRESO DE COLOMBIA DECRETA:

Artículo 1. Adicionase el Código Penal con un Título VII BIS denominado "De la Protección de la información y de los datos", del siguiente tenor:

CAPITULO I
De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos

- Artículo 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.
- Artículo 269B. OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarent-a y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.
- Artículo 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.
- Artículo 269D. DAÑO INFORMÁTICO. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos,

incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

- Artículo 269E. USO DE SOFTWARE MALICIOSO. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.
- Artículo 269F. VIOLACIÓN DE DATOS PERSONALES. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.
- Artículo 269G. SUPLANTACIÓN DE SITIOS WEB PARA CAPTUDATOS PERSONALES. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave. la pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

- Artículo 269H. CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

  - Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
  - Por servidor público en ejercicio de sus funciones
  - Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
  - Revelando o dando a conocer el contenido de la información en perjuicio de otro.
  - Obteniendo provecho para sí o para un tercero.
  - Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
  - Utilizando como instrumento a un tercero de buena fe.

- Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

CAPITULO II

De los atentados informáticos y otras infracciones

- Artículo 2691. HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.
- Artículo 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes.

La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.

Artículo 2. Adiciónese al artículo 58 del Código Penal con un numeral 17, así:

Articulo 58 CIRCUNSTANCIAS DE MAYOR PUNIBILIDAD. Son circunstancias de mayor punibilidad, siempre que no hayan sido previstas de otra manera:
(...)
17. Cuando para la realización de las conductas punibles se utilicen medios informáticos, electrónicos o telemáticos.

Artículo 3. Adiciónese al artículo 37 del Código de Procedimiento Penal con un numeral 6, así:

Artículo 37. DE LOS JUECES MUNICIPALES. los jueces penales municipales conocen:
(...)

6. De los delitos contenidos en el título VII Bis.

Artículo 4. La presente ley rige a partir de su promulgación y deroga todas las disposiciones que le sean contrarias, en especial el texto del artículo 195 del Código Penal"[61].

[61] MINTIC. Ley 1273 de 2009. (05 de 01 de 2009). Bogotá, D.C. 2009. p. 4.

ANEXO B.

Cuestionario

Dirigido a: FUNCIONARIO FULANO DE TAL, DEPENDENCIA TAL (relacionada con la planeación y las tecnologías de la información y las telecomunicaciones TIC), UNIVERSIDAD TAL

.

Asunto: Solicitud de información

Apreciado funcionario (o, apreciado Ingeniero o Administrador de sistemas Informáticos):

Me llamo Ruby Esperanza Buitrago Giraldo, estudiante de último semestre de la especialización en Seguridad Informática que ofrece la Universidad Nacional Abierta y a Distancia UNAD y me encuentro desarrollando mi último curso, el trabajo de grado, en la modalidad de monografía, que se denomina SISTEMAS DE GESTIÓN EN SEGURIDAD INFORMÁTICA SGSI EN UNIVERSIDADES PÚBLICAS DEL EJE CAFETERO - COLOMBIA. Para la ejecución de este trabajo, requiero abusar de su amabilidad pidiéndole que, por favor, me conteste el siguiente cuestionario, lo cual me suministraría información valiosa para tener finalmente una buena monografía, que pienso compartir con Ud. una vez sea aprobada para divulgación.

Si lo desea, yo pudiera reunirme con Ud. en su oficina el día y la hora que concertemos por este medio o telefónicamente.

Quedo atenta a su respuesta, que -perdone- requeriría lo más pronto que le sea posible, por razones de cumplimiento de un cronograma en el semestre académico, lo cual seguro Ud. comprenderá.

Cordial saludo,

RUBY ESPERANZA BUITRAGO G.
Estudiante

Vo. Bo. Yenny Stella Núñez Álvarez

Directora del trabajo de grado UNAD

Cuestionario:

1. ¿Su Universidad, dentro del área de las Tecnologías de la Información y las Comunicaciones, cuenta con una dependencia que maneje la seguridad informática?

Sí____ No _____

Si su respuesta es NO, le pregunto:

2. ¿Su Universidad ha tenido incidentes informáticos que hayan afectado de alguna manera su funcionamiento?

Sí____ No _____

Si su respuesta es sí, explique cuáles y de qué forma:

_____

3. ¿De acuerdo con lo anterior, ¿cómo ha manejado o maneja su Universidad los incidentes informáticos que se presentaron o pudieran presentarse en el futuro?

_____

4. ¿Su Universidad tiene políticas de seguridad informática respecto de los activos de información que la universidad posee? Si las conoce, ¿podría incluirlas aquí?

Sí____ No _____

_____

5. ¿Su Universidad tiene un inventario de activos de la información?

Sí____ No _____

¿Si su respuesta es no, conoce la razón por lo cual ocurre esto?

---

6. ¿Su Universidad ha realizado en algún momento un análisis de riesgos frente a amenazas (naturales o antrópicas) que tenga en cuenta qué tan vulnerables son los bienes y las personas ante la eventual ocurrencia de estas?

Sí____ No _____

7. ¿Su Universidad tiene implementadas acciones preventivas y correctivas frente a los riesgos que pueda tener la información como activo? Si las conoce, ¿podría relacionarlas aquí?

Sí____ No _____

---

8. ¿Su Universidad realiza copias de seguridad de la información de forma periódica?

Sí____ No _____

9. ¿El sistema operativo (S.O.) de cada uno de los computadores de la Universidad está licenciado y es actualizado con regularidad?

Sí____ No _____

10. ¿Su Universidad tiene implementados controles físicos y/o lógicos para salvaguardar la información?

Sí ____ No _____ ¿Cuál (es)? (ambos controles o solo uno)

11. ¿Para ingresar al área donde se encuentran los servidores se maneja algún tipo de restricciones?

Sí ____ No _____ ¿Cuál (es)?

12. ¿Todos los computadores de su Universidad cuentan con antivirus y estos son actualizados con regularidad?

Sí____ No _____

13. ¿Su universidad tiene implementado un sistema de gestión en seguridad informática (SGSI)?

Sí____ No _____

14. ¿Los funcionarios que trabajan en el área de sistemas (TIC's) conocen y manejan las Normas ISO 27001 y 27002?

Sí____ No _____

Si su respuesta es no, ¿podría darnos aquí las razones que Ud. considera por las cuales esto sucede?

_____

ANEXO C.

Cuestionarios diligenciados universidades

UNIVERSIDAD NACIONAL DE COLOMBIA – SEDE MANIZALES

Nombre funcionario: Carlos Alberto Marín Gómez

Cargo: jefe

Oficina: De Tecnologías de Información y Comunicaciones OTIC

Cuestionario

1. ¿Su Universidad, dentro del área de las Tecnologías de la Información y las Comunicaciones, cuenta con una dependencia que maneje la seguridad informática?

Sí ___ No _X___

Si su respuesta es NO, le pregunto:

2. ¿Su Universidad ha tenido incidentes informáticos que hayan afectado de alguna manera su funcionamiento?

Sí ___ No _X___

Si su respuesta es sí, explique cuáles y de qué forma:

_____

3. ¿De acuerdo con lo anterior, ¿cómo ha manejado o maneja su Universidad los incidentes informáticos que se presentaron o pudieran presentarse en el futuro?

_____

4. ¿Su Universidad tiene políticas de seguridad informática respecto de los activos de información que la universidad posee? Si las conoce, ¿podría incluirlas aquí?

Sí ___ No _X___

_____

5. ¿Su Universidad tiene un inventario de activos de la información?

Sí _X__ No ____

¿Si su respuesta es no, conoce la razón por lo cual ocurre esto?

---

6. ¿Su Universidad ha realizado en algún momento un análisis de riesgos frente a amenazas (naturales o antrópicas) que tenga en cuenta qué tan vulnerables son los bienes y las personas ante la eventual ocurrencia de estas?

Sí _X__ No ____

7. ¿Su Universidad tiene implementadas acciones preventivas y correctivas frente a los riesgos que pueda tener la información como activo? Si las conoce, ¿podría relacionarlas aquí?

Sí ___ No _X___

---

8. ¿Su Universidad realiza copias de seguridad de la información de forma periódica?

Sí _X__ No ____

9. ¿El sistema operativo de cada uno de los computadores de la Universidad está licenciado y es actualizado con regularidad?

Sí _X__ No ____

10. ¿Su Universidad tiene implementados controles físicos y/o lógicos para salvaguardar la información?

Sí _X__ No ____ ¿Cuál (es)? (ambos controles o solo uno) Ambos

11. ¿Para ingresar al área donde se encuentran los servidores se maneja algún tipo de restricciones?

Sí _X_ No ____ ¿Cuál (es)? Control de acceso, seguridad.

12. ¿Todos los computadores de su Universidad cuentan con antivirus y estos son actualizados con regularidad?

Sí _X__ No ____

13. ¿Su universidad tiene implementado un sistema de gestión en seguridad informática (SGSI)?

Sí _X__ No ____

14. ¿Los funcionarios que trabajan en el área de sistemas (TIC's) conocen y manejan las Normas ISO 27001 y 27002?

Sí _X__ No ____

Si su respuesta es no, ¿podría darnos aquí las razones que Ud. considera por las cuales esto sucede?

UNIVERSIDAD DE CALDAS

Nombre funcionario: Carlos Alberto Gutiérrez Rodas

Cargo: Jefe de Sistemas

Oficina: De Sistemas

Cuestionario

1. ¿Su Universidad, dentro del área de las Tecnologías de la Información y las Comunicaciones, cuenta con una dependencia que maneje la seguridad informática?

Sí ___ No _x_

Si su respuesta es NO, le pregunto: se tiene el servicio con outsourcing

2. ¿Su Universidad ha tenido incidentes informáticos que hayan afectado de alguna manera su funcionamiento?

Sí _x_ No ____

Si su respuesta es sí, explique cuáles y de qué forma:

__es reserva de la Universidad_____

3. ¿De acuerdo con lo anterior, ¿cómo ha manejado o maneja su Universidad los incidentes informáticos que se presentaron o pudieran presentarse en el futuro?

____trazabilidad, reportes, custodia de equipos si es necesario___

4. ¿Su Universidad tiene políticas de seguridad informática respecto de los activos de información que la universidad posee? Si las conoce, ¿podría incluirlas aquí?

Sí ___ No _x_

_____en construcción_____

5. ¿Su Universidad tiene un inventario de activos de la información?

Sí _x_ No ____

¿Si su respuesta es no, conoce la razón por lo cual ocurre esto?

---

6. ¿Su Universidad ha realizado en algún momento un análisis de riesgos frente a amenazas (naturales o antrópicas) que tenga en cuenta qué tan vulnerables son los bienes y las personas ante la eventual ocurrencia de estas?

Sí _x_ No ____ muy vulnerable

7. ¿Su Universidad tiene implementadas acciones preventivas y correctivas frente a los riesgos que pueda tener la información como activo? Si las conoce, ¿podría relacionarlas aquí?

Sí _x_ No ____ enviar correo solicitando los riesgos

---

8. ¿Su Universidad realiza copias de seguridad de la información de forma periódica?

Sí _x_ No ____

9. ¿El sistema operativo de cada uno de los computadores de la Universidad está licenciado y es actualizado con regularidad?

Sí _x_ No ____

10. ¿Su Universidad tiene implementados controles físicos y/o lógicos para salvaguardar la información?

Sí _x_ No ____ ¿Cuál (es)? (ambos controles o solo uno) ambos

11. ¿Para ingresar al área donde se encuentran los servidores se maneja algún tipo de restricciones?

Sí _x_ No ____ ¿Cuál (es)? llave

12. ¿Todos los computadores de su Universidad cuentan con antivirus y estos son actualizados con regularidad?

Sí _x_ No ____

13. ¿Su universidad tiene implementado un sistema de gestión en seguridad informática (SGSI)?

Sí ___ No _x__

14. ¿Los funcionarios que trabajan en el área de sistemas (TIC's) conocen y manejan las Normas ISO 27001 y 27002?

Sí _x_ No ____

Si su respuesta es no, ¿podría darnos aquí las razones que Ud. considera por las cuales esto sucede?

UNIVERSIDAD DEL QUINDÍO

Nombre Completo: Luis Horacio Buitrago Gallego

Cargo: director

Oficina: Centro de Sistemas y Nuevas Tecnologías

Cuestionario

1. ¿Su Universidad, dentro del área de las Tecnologías de la Información y las Comunicaciones, cuenta con una dependencia que maneje la seguridad informática?

Sí __X_ No ____

Si su respuesta es NO, le pregunto:

2. ¿Su Universidad ha tenido incidentes informáticos que hayan afectado de alguna manera su funcionamiento?

Sí ___ No __X__

Si su respuesta es sí, explique cuáles y de qué forma:

_____

3. ¿De acuerdo con lo anterior, ¿cómo ha manejado o maneja su Universidad los incidentes informáticos que se presentaron o pudieran presentarse en el futuro?

__La Universidad por medio del Área de TI viene adelantando un proyecto de consultoría, incluyendo una herramienta para la gestión de la seguridad informática.

4. ¿Su Universidad tiene políticas de seguridad informática respecto de los activos de información que la universidad posee? Si las conoce, ¿podría incluirlas aquí?

Sí __X_ No ____

Políticas de seguridad informática, políticas de gobierno de TI, políticas de se guridad de infraestructura.

5. ¿Su Universidad tiene un inventario de activos de la información?

Sí __X_ No ____

¿Si su respuesta es no, conoce la razón por lo cual ocurre esto?

_____

6. ¿Su Universidad ha realizado en algún momento un análisis de riesgos frente a amenazas (naturales o antrópicas) que tenga en cuenta qué tan vulnerables son los bienes y las personas ante la eventual ocurrencia de estas?

Sí __X_ No ____

7. ¿Su Universidad tiene implementadas acciones preventivas y correctivas frente a los riesgos que pueda tener la información como activo? Si las conoce, ¿podría relacionarlas aquí?

Sí ___ No ____

Se definio la matriz de riesgos y se encuntra en proceso de implnatación, con sus respectivos controles.

8. ¿Su Universidad realiza copias de seguridad de la información de forma periódica?

Sí __X_ No ____

9. ¿El sistema operativo de cada uno de los computadores de la Universidad está licenciado y es actualizado con regularidad?

Sí __X_ No ____

10. ¿Su Universidad tiene implementados controles físicos y/o lógicos para salvaguardar la información?

Sí __X_ No ____ ¿Cuál (es)? (ambos controles o solo uno) Ambos.

11. ¿Para ingresar al área donde se encuentran los servidores se maneja algún tipo de restricciones?

Sí __X_ No ____ ¿Cuál (es)? Control de acceso con tarjeta, y sistemas de video y registro de actividades dentro del Data center.

12. ¿Todos los computadores de su Universidad cuentan con antivirus y estos son actualizados con regularidad?

Sí __X_ No ____

13. ¿Su universidad tiene implementado un sistema de gestión en seguridad informática (SGSI)?

Sí __X_ No ____ En proceso de implantación.

14. ¿Los funcionarios que trabajan en el área de sistemas (TIC's) conocen y manejan las Normas ISO 27001 y 27002?

Sí __X_ No ____ 3 de los funcionarios estan certificados.

Si su respuesta es no, ¿podría darnos aquí las razones que Ud. considera por las cuales esto sucede?

UNIVERSIDAD TECNOLÓGICA DE PEREIRA – UTP

Nombre funcionario: No hay un funcionario único responsable.

Responsables: Comité Técnico Interdisciplinario SGSI UTP, conformado por profesionales de diferentes áreas de la universidad: Secretaría General, Recursos Informáticos y Educativos, Gestión de Tecnologías Informáticas y Sistemas de Información, Planeación, Control Interno y Sistema Integral de Gestión.

Oficina: Sistema Integral de Gestión

Cuestionario

1. ¿Su Universidad, dentro del área de las Tecnologías de la Información y las Comunicaciones, cuenta con una dependencia que maneje la seguridad informática?

Sí X No ____

Si su respuesta es NO, le pregunto:

2. ¿Su Universidad ha tenido incidentes informáticos que hayan afectado de alguna manera su funcionamiento?

Sí X No ____

Si su respuesta es sí, explique cuáles y de qué forma: N/A

3. ¿De acuerdo con lo anterior, ¿cómo ha manejado o maneja su Universidad los incidentes informáticos que se presentaron o pudieran presentarse en el futuro?

Se cuenta con una mesa de ayuda y se aplica procedimiento de incidentes informáticos.

4. ¿Su Universidad tiene políticas de seguridad informática respecto de los activos de información que la universidad posee? Si las conoce, ¿podría incluirlas aquí?

Sí X No ____

Se cuenta con el Manual General de directrices del Sistema de Gestión de Seguridad de la Información

5. ¿Su Universidad tiene un inventario de activos de la información?

Sí X No ____

¿Si su respuesta es no, conoce la razón por lo cual ocurre esto?

_____

6. ¿Su Universidad ha realizado en algún momento un análisis de riesgos frente a amenazas (naturales o antrópicas) que tenga en cuenta qué tan vulnerables son los bienes y las personas ante la eventual ocurrencia de estas?

Sí X No ____

7. ¿Su Universidad tiene implementadas acciones preventivas y correctivas frente a los riesgos que pueda tener la información como activo? Si las conoce, ¿podría relacionarlas aquí?

Sí X No ____

_____

8. ¿Su Universidad realiza copias de seguridad de la información de forma periódica?

Sí X No ____

9. ¿El sistema operativo de cada uno de los computadores de la Universidad está licenciado y es actualizado con regularidad?

Sí X No ____

10. ¿Su Universidad tiene implementados controles físicos y/o lógicos para salvaguardar la información?

Sí X No ____ ¿Cuál (es)? (ambos controles o solo uno)

11. ¿Para ingresar al área donde se encuentran los servidores se maneja algún tipo de restricciones?

Sí X No ____ ¿Cuál (es)?

Control de acceso físico

12. ¿Todos los computadores de su Universidad cuentan con antivirus y estos son actualizados con regularidad?

Sí X No ____

13. ¿Su universidad tiene implementado un sistema de gestión en seguridad informática (SGSI)?

Sí ___ No ____ Actualmente se está implementando

14. ¿Los funcionarios que trabajan en el área de sistemas (TIC's) conocen y manejan las Normas ISO 27001 y 27002?

Sí X No ____

Si su respuesta es no, ¿podría darnos aquí las razones que Ud. considera por las cuales esto sucede?

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

Nombre funcionario: Leonardo Montilla Malaver

Cargo: Líder Zona Occidente GIDT

Oficina: Gerencia de Innovación y Desarrollo Tecnológico

Cuestionario

1. ¿Su Universidad, dentro del área de las Tecnologías de la Información y las Comunicaciones, cuenta con una dependencia que maneje la seguridad informática?

Sí _X_ No ____

Si su respuesta es NO, le pregunto:

2. ¿Su Universidad ha tenido incidentes informáticos que hayan afectado de alguna manera su funcionamiento?

Sí _X_ No ____

Si su respuesta es sí, explique cuáles y de qué forma:

Virus ransomware, el cual solo afecto pocos funcionarios ya que se implementó políticas de seguridad inmediata

3. ¿De acuerdo con lo anterior, ¿cómo ha manejado o maneja su Universidad los incidentes informáticos que se presentaron o pudieran presentarse en el futuro?

Boletines informáticos, implementado políticas de seguridad, actualizaciones, usando Firewall físico y lógico

4. ¿Su Universidad tiene políticas de seguridad informática respecto de los activos de información que la universidad posee? Si las conoce, ¿podría incluirlas aquí?

Sí _X_ No ____

Copias de seguridad físicas y en la nube de CISCO

5. ¿Su Universidad tiene un inventario de activos de la información?

Sí ___ No _X__

¿Si su respuesta es no, conoce la razón por lo cual ocurre esto?

El activo más custodiado se encuentra investario y custodiado por personal experto, la información de los funcionarios son los responsables cada uno de tener un inventario de su informaicon

6. ¿Su Universidad ha realizado en algún momento un análisis de riesgos frente a amenazas (naturales o antrópicas) que tenga en cuenta qué tan vulnerables son los bienes y las personas ante la eventual ocurrencia de estas?

Sí _X__ No ____

7. ¿Su Universidad tiene implementadas acciones preventivas y correctivas frente a los riesgos que pueda tener la información como activo? Si las conoce, ¿podría relacionarlas aquí?

Sí _X_ No ____

Firewall, Puertos monitoreados, doble autenticación, seguridad física y lógica, sistemas actualizados

8. ¿Su Universidad realiza copias de seguridad de la información de forma periódica?

Sí _X_ No ____

9. ¿El sistema operativo de cada uno de los computadores de la Universidad está licenciado y es actualizado con regularidad?

Sí _X_ No ____

10. ¿Su Universidad tiene implementados controles físicos y/o lógicos para salvaguardar la información?

Sí ___ No ____ ¿Cuál (es)? (ambos controles o solo uno)

Copias de seguridad físicas, en la nube de CISCO, Movistar Moratos

11. ¿Para ingresar al área donde se encuentran los servidores se maneja algún tipo de restricciones?

Sí _X_ No ____ ¿Cuál (es)? Solo personal autorizado y solo las llaves las tiene el responsable de Datacenter

12. ¿Todos los computadores de su Universidad cuentan con antivirus y estos son actualizados con regularidad?

Sí _X_ No ____

13. ¿Su universidad tiene implementado un sistema de gestión en seguridad informática (SGSI)?

Sí _X_ No ____

14. ¿Los funcionarios que trabajan en el área de sistemas (TIC's) conocen y manejan las Normas ISO 27001 y 27002?

Sí _X_ No ____

Si su respuesta es no, ¿podría darnos aquí las razones que Ud. considera por las cuales esto sucede?

ANEXO D.

Documentación, políticas de seguridad informática Universidades Públicas del Eje Cafetero. Enlaces en la web.

1. Universidad Nacional de Colombia UNAL:

- Acuerdo 228 de 2016. Por el cual se expide la Política de Seguridad Informática y de la Información de la Universidad Nacional de Colombia. Disponible en: http://www.legal.unal.edu.co/rlunal/home/doc.jsp?d_i=87116
- Política de seguridad informática y de la información. Disponible en: http://dntic.unal.edu.co/images/seguridad/PolticadeSeguridadInformaticaydelaInformacion.pdf

2. Universidad de Caldas:

- Presentación en pdf para el Segundo encuentro colombiano de gestión universitaria. Disponible en: https://docplayer.es/2402261-Seguridad-informatica-en-las-instituciones-de-educacion-superior.html

3. Universidad Tecnológica de Pereira UTP:

- SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN. MANUAL GENERAL DE DIRECTRICES. Disponible en: https://www.utp.edu.co/cms-utp/data/bin/UTP/web/uploads/media/calidad/documentos/1313-MGD-01-Manual-General-de-Directrices-del-SGSI-V2.pdf
- COLOMBIA. UTP. Resolución No. 6123 2017. Por medio del cual se adopta el manual general de directrices del Sistema de Gestión de Seguridad de la Información de la Universidad Tecnológica de Pereira. Disponible en: https://www.utp.edu.co/cms-utp/data/bin/UTP/web/uploads/media/secretaria/documentos/RR%206123%20DE%202017-SEGURIDAD%20DE%20LA%20INFORMACION.pdf

4. Universidad del Quindío:

- Hoja de Ruta – Implementación de las Políticas de Seguridad de la Información (versión 2.0.). Disponible en: http://www.uniquindio.edu.co/descargar.php?idFile=23227

5. Universidad Nacional Abierta y a Distancia UNAD:

- Acuerdo 0029 de 2013. Por el cual se expide el Reglamento Estudiantil de la Universidad Nacional Abierta y a Distancia (UNAD) y se dictan otras disposiciones. Disponible en:

https://sgeneral.unad.edu.co/images/documentos/consejoSuperior/acuerdos/2013/COSU_ACUE_029_20131229.pdf

- Resolución No. 8547 de 2016. Por la cual se reglamenta el uso de los Servicios de Tecnología de la Universidad Nacional Abierta y a Distancia – UNAD. Disponible en: https://sgeneral.unad.edu.co/images/documentos/RESO_NORMOGRAMAS/RESO_8547_20160908.pdf
- Resolución No. 006858 de 2014. Por la cual se conforma el Sistema Integrado de Gestión – SIG de la Universidad Nacional Abierta y a Distancia – UNAD, se establece la Política Integrada de Gestión, y se derogan las resoluciones 2271 de 2008, 2627 de 2008, 2055 de 2007 y 02861 de 2010. Disponible en: https://sig.unad.edu.co/documentos/sig/resoluciones_sig/Resolucion_7966_2014_SIG_modificatoria.pdf
- Resolución No. 007966 de 2014. Por la cual se modifica la Resolución No. 6858 del 22 de agosto de 2014, por medio de la cual se conforma el Sistema Integrado de Gestión – SIG de la Universidad Nacional Abierta y a Distancia – UNAD, se establece la Política Integrada de Gestión, y se derogan las resoluciones 2271 de 2008, 2627 de 2008, 2055 de 2007 y 02861 de 2010. Disponible en: https://sig.unad.edu.co/documentos/sig/resoluciones_sig/Resolucion_7966_2014_SIG_modificatoria.pdf
- Políticas Marco de Referencia del Sistema de Gestión de Seguridad de la Información (SGSI). Disponible en: https://gidt.unad.edu.co/images/Documentos/20150303%20-%20Resolucin%204256%20-%20Polticas%20Marco%20de%20Referencia%20del%20SGSI.pdf
- Resolución No. 004793 de 2014. Por la cual se crea la Política de Seguridad de la Información para la Universidad Nacional Abierta y a Distancia – UNAD. Disponible en: https://sgeneral.unad.edu.co/images/documentos/RESO_NORMOGRAMAS/RESO_4793_20130822.pdf