Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

PROPUESTA DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

Rodely Alberto Navarro Pérez
Asesorado por la Inga. Mayra Grisela Corado García

Guatemala, noviembre de 2019

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERIA

PROPUESTA DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

RODELY ALBERTO NAVARRO PÉREZ
ASESORADO POR LA INGA. MAYRA GRISELA CORADO GARCIA

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN CIENCIAS Y SISTEMAS

GUATEMALA, NOVIEMBRE DE 2019

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANA	Inga. Aurelia Anabela Cordova Estrada
VOCAL I	Ing. José Francisco Gómez Rivera
VOCAL II	Ing. Mario Renato Escobedo Martínez
VOCAL III	Ing. José Milton de León Bran
VOCAL IV	Br. Luis Diego Aguilar Ralón
VOCAL V	Br. Cristian Daniel Estrada Santizo
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Murphy Olympo Paiz Recinos
EXAMINADOR	Ing. Pedro Pablo Hernández Ramírez
EXAMINADOR	Ing. Oscar Alejandro Paz Campos
EXAMINADOR	Ing. Ludwing Federico Altán Sac
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

PROPUESTA DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería en Ciencias y Sistemas, con fecha 24 de enero de 2019.

Rodely Alberto Navarro Pérez

Guatemala 30 de septiembre de 2019

Ingeniero
Carlos Alfredo Azurdia Morales
Coordinador del Área de Trabajos de Graduación
Escuela de Ciencias y Sistemas
Facultad de Ingeniería
Universidad de San Carlos de Guatemala

Estimado Ingeniero Azurdia:

Le informo que he asesorado y revisado el trabajo de graduación realizado por el estudiante **Rodely Alberto Navarro Pérez** con carné **1999-11445** y CUI **2556 44914 1201**, titulado **PROPUESTA DE POLITICA DE SEGURIDAD DE LA INFORMACION DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA**, habiendo cumplido con el objetivo establecido, doy mi aprobación y solicito autorizar el trámite correspondiente.

Atentamente,

Inga. Mayra Grisela Corado García
Asesora
Colegiado No. 4271

Mayra Grisela Corado García
Ingeniera en Ciencias y Sistemas
Colegiado No. 4271

Universidad San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

Guatemala, 7 de octubre de 2019

Ingeniero
Carlos Gustavo Alonzo
Director de la Escuela de Ingeniería
En Ciencias y Sistemas

Respetable Ingeniero Alonzo:

Por este medio hago de su conocimiento que he revisado el trabajo de graduación del estudiante **RODELY ALBERTO NAVARRO PÉREZ** con carné **199911445 y CUI 2556 44914 1201** titulado **"PROPUESTA DE POLITICA DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA"** y a mi criterio el mismo cumple con los objetivos propuestos para su desarrollo, según el protocolo aprobado.

Al agradecer su atención a la presente, aprovecho la oportunidad para suscribirme,

Atentamente,

Ing. Carlos Alfredo Azurdia
Coordinador de Privados
y Revisión de Trabajos de Graduación

ESCUELA DE INGENIERÍA EN CIENCIAS Y SISTEMAS

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÌA
ESCUELA DE INGENIERÍA EN
CIENCIAS Y SISTEMAS
TEL: 24188000 Ext. 1534

El Director de la Escuela de Ingeniería en Ciencias y Sistemas de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer el dictamen del asesor con el visto bueno del revisor y del Licenciado en Letras, del trabajo de graduación, ***"PROPUESTA DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA"*** *realizado por el estudiante, RODELY ALBERTO NAVARRO PÉREZ, aprueba el presente trabajo y solicita la autorización del mismo.*

"ID Y ENSEÑAD A TODOS"

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION DE INGENIERIA EN CIENCIAS Y SISTEMAS

MSc. Ing. Carlos Gustavo Alonzo
Director
Escuela de Ingeniería en Ciencias y Sistemas

Guatemala, 07 de noviembre de 2019

Universidad de San Carlos
De Guatemala

Facultad de Ingeniería
Decanato

Ref. DTG.519.2019

La Decana de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería en Ciencias y Sistemas, al trabajo de graduación titulado: **PROPUESTA DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA,** presentado por el estudiante universitario: **Rodely Alberto Navarro Pérez,** y después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, se autoriza la impresión del mismo.

IMPRÍMASE.

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANO
FACULTAD DE INGENIERÍA

Inga. Aurelia Anabela Cordova Estrada
Decana

Guatemala, noviembre de 2019

/cc

ACTO QUE DEDICO A:

Dios	Por todo su amor, protección y sabiduría dotada.
Mis padres	German Navarro e Idalia Marilú Pérez, por brindarme su amor, su apoyo incondicional y sus consejos.
Mis hermanos	Hannia, Madelina, Kenia y Rudy Navarro Pérez, por todo su apoyo y fortaleza que me brindaron para seguir adelante.
Mis abuelitos	Benjamín Navarro (q.d.e.p), Celsa Monzón (q.d.e.p), Enrique Pérez (q.d.e.p) y Arcadia Gonzales, por sus consejos, regaños, experiencias y sobre todo por darme cariño.
Mis tíos y primos	Por sus palabras de ánimo y cariño.

AGRADECIMIENTOS A:

Universidad de San Carlos de Guatemala	Mi apreciada Tricentenaria Universidad, por haberme brindado la oportunidad de formarme como profesional.
Facultad de Ingeniería	Por abrirme sus puertas y brindarme los conocimientos y las habilidades necesarias para formarme como profesional.
Los ingenieros	Mayra Corado y Rene Ornéliz, por su apoyo, su conocimiento y sus consejos durante el desarrollo de mi trabajo de graduación.
Mis tíos y primos	Carlos Pérez, Floridalma Cruz y a mis primos Anahí, Carlos, Bencelia, Idalia y Merary Pérez Cruz, por haber abierto las puertas de su hogar y tomarme como un miembro de su familia. Tía Candelaria Pérez (q.d.e.p)**,** Por su cariño y cuidados brindados.
Mis amigos y compañeros	Por sus experiencias, su apoyo, su conocimiento y su cariño brindado.

ÍNDICE GENERAL

GLOSARIO

Centro de datos	Espacio dedicado a albergar recursos tecnológicos para almacenar y procesar información.
Ciberseguridad	Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados.
Consejo Superior Universitario	Es el máximo órgano de dirección de la Universidad de San Carlos de Guatemala; en su calidad de cuerpo colegiado y con base en los artículos 82 y 83 de la Constitución Política de la República de Guatemala le corresponde el gobierno universitario.
Copia de seguridad	Se refiere a la copia y al archivo de datos de la computadora de modo que se puede utilizar para restaurar la información original después de una eventual pérdida de datos.
***Firewalls* (cortafuegos)**	Es un sistema diseñado para prevenir el acceso no autorizado hacia o desde una red privada. Se puede implementar en forma de hardware, de

	software o en una combinación de ambos. Los cortafuegos impiden que los usuarios no autorizados accedan a redes privadas conectadas a Internet, especialmente a intranets.
Firma electrónica	Conjunto de datos en forma electrónica asociados a un mensaje de datos o documento electrónico, utilizados para acreditar la identidad del emisor con relación al mensaje, que indican que es el autor legítimo de este, por lo que asume como propia la información contenida en este; produce los mismos efectos jurídicos que la firma autógrafa.
ISO 27001	Es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.
Red troncal	Es una red utilizada para interconectar otras redes, es decir, un medio que permite la comunicación de varias (LAN) o segmentos. Suelen ser de alta capacidad y permiten un mayor rendimiento de las conexiones (LAN).
Router	También conocido como enrutador, es un dispositivo de red que se encarga de llevar por la mejor ruta, el tráfico de la red; direcciones IP.

Servidor	Es un computador que forma parte de una red informática y provee determinados servicios por medio de una aplicación al resto de los computadores de la misma, llamados a su vez estaciones o clientes.
Switch	También conocido como conmutador, es un dispositivo de interconexión utilizado para conectar equipos en red formando lo que se conoce como una red de área local (LAN).
VPN (v*irtual private network*)	Es una tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando internet, es un túnel seguro entre su dispositivo y la internet.

RESUMEN

El presente trabajo consiste en desarrollar una propuesta de políticas de seguridad de la información de la Universidad de San Carlos de Guatemala para dar protección a sus activos de información, que de acuerdo con la norma ISO 27001 es considerado como los bienes más valiosos dentro de una organización.

Con base en la experiencia, el conocimiento y el apoyo en materia de tecnología que ha brindado el Departamento de Procesamiento de Datos de la Dirección General Financiera a la Universidad fue posible establecer vulnerabilidades y amenazas de seguridad que han ocurrido.

Para la implementación de las políticas de seguridad de la información es necesario crear el Comité de Seguridad quien será el encargado de elevarlo al Consejo Superior Universitario para su aprobación. También, será el encargado de revisar y actualizar las políticas en tiempos que sean determinados por el comité.

Con la implementación de las políticas se establece una mejor seguridad de la información; se protege de esta manera la integridad, confidencialidad y disponibilidad de la información.

OBJETIVOS

General

Proponer políticas de seguridad de las tecnologías de la información y comunicación (TIC) de la Universidad de San Carlos de Guatemala.

Específicos

1. Proponer reglas específicas que protejan y preserven la integridad, disponibilidad y confiabilidad de la información de la Universidad de San Carlos de Guatemala ante amenazas internas o externas.

2. Definir normas para un correcto análisis de riesgo de seguridad de la información de la Universidad de San Carlos de Guatemala.

INTRODUCCIÓN

En la actualidad, las tecnologías de la información y comunicación constituyen herramientas vitales dentro de una organización para el buen funcionamiento de las distintas tareas que sus colaboradores realizan. Por tanto, es necesario que el personal que tiene relación adquiera competencias mínimas en el uso de la información en general y en especial en el campo de las políticas a las cuales ha de enfrentar.

El presente trabajo tiene el fin de establecer una propuesta de políticas de seguridad de la información para la Universidad de San Carlos de Guatemala, para proteger los activos y garantizar la confidencialidad, integridad y disponibilidad de la información.

En la Universidad de San Carlos de Guatemala se hace uso de las tecnologías de la información y comunicación, principalmente a través del Departamento de Procesamiento de Datos que depende de la Dirección General Financiera. Los principales servicios que este departamento provee a las distintas unidades ejecutoras y demás dependencias son: la administración de la red troncal, servicio de internet, correos electrónicos, sistemas integrados de información financiera (SIIF), servicio de control académico de algunos centros regionales y escuelas no facultativas, alojamiento de servidores de algunas unidades y alojamiento web. Cabe mencionar que dentro del *Manual de organización del Departamento de Procesamiento de Datos de la Dirección General Financiera*, del año 2016, se encuentran los siguientes incisos que serán considerados como fuente de antecedentes:

- Velar por la seguridad e integridad del flujo de información durante cada etapa del procesamiento de datos dentro de cada uno de los sistemas que integran la información financiera.

- Establecer normas, políticas y estrategias en el uso de la tecnología de la información y comunicación para automatizar, facilitar y hacer más eficiente las actividades académicas; con el desarrollo de aplicaciones informáticas para tales fines, según sea requerido dentro de la Universidad de San Carlos de Guatemala.

- Supervisar, autorizar, facilitar el crecimiento y mantenimiento de la red troncal de datos para los usuarios de la Universidad de San Carlos de Guatemala.

- Normar y definir requerimientos mínimos para toda aplicación que se interconecte con las desarrolladas por este departamento, así como para todo equipo de cómputo o de gestión que se integre a la red troncal de datos.

Por lo anterior, este departamento deberá generar las normas para la creación de política de seguridad de la información.

1. ANTECEDENTES

La Universidad de San Carlos de Guatemala no cuenta con una política de seguridad de la información, debido a ello, la seguridad de la información únicamente se ha encomendado al personal técnico; actualmente, no se ha tomado conciencia que se debe involucrar a todo el personal.

En la universidad uno de los mayores riesgos en la seguridad de la información lo constituye el compartir usuario. Han existido casos en los cuales han denunciado cobros ilegales para los cuales ha sido difícil determinar a los responsables por el uso de un solo usuario quien registra las operaciones en los sistemas. Muchos jefes y altos funcionarios comparten su usuario principalmente a subalternos para revisión de información, hacer estadísticas o enviar información a través de su correo electrónico. Aunque existen circulares que el departamento de Procesamientos de Datos de la Dirección General Financiera ha emitido donde, claramente, informa que cada usuario es responsable del uso y que no debe ser compartido.

La instalación de software sin aprobación en la universidad es muy frecuente por parte del personal, lo cual ocasiona una alta vulnerabilidad de introducir código malicioso en el equipo de cómputo con una alta probabilidad de propagarse por toda la red de datos.

También, han existido debilidades en algunas unidades en el manejo de los datos en las notas de cursos, los cuales se han dado por falta de control y delimitación de las funciones y operaciones en el personal asignado.

Existe carencia en el control de acceso físico a varios centros de datos, también, en su mantenimiento.

Hay unidades que han contratado servicios externos para el desarrollo y la implementación de software los cuales no han sido realizados bajo estándares de desarrollo, muchos de los cuales se han alojado fuera de los servidores de la universidad en sitios con seguridad muy baja. No entregan el código fuente, lo cual constituye un riesgo en el mantenimiento y en la escalabilidad del software. Se han encontrado situaciones en las cuales la información no está disponible, debido a que el proveedor del desarrollo del software también es el del alojamiento y dado a la dependencia que la universidad tiene, al existir un desacuerdo simplemente bloquean el acceso. Además, al estar en servidores fuera de la universidad la información se encuentra disponible a terceros con intenciones desconocidas.

La falta de una política de copia de seguridad en varias unidades hace que se exponga la información a una pérdida ante un desastre o ataque.

El Departamento de Procesamiento de Datos de la Dirección General Financiera ha apoyado estableciendo normas dentro de las cuales figuran el uso de correo electrónico, compra de equipo, etc., pero no existe un documento integrado con normas de uso general de la tecnología dentro de la universidad.

El Departamento de Procesamiento de Datos fue fundado el 27 de octubre de 1964. El 16 de agosto de 1979 paso a depender jerárquicamente de la Dirección General Financiera por Acuerdo de Rectoría No. 725-79.

En 1997 por medio de fibra óptica se inició la interconexión de distintas unidades académicas y administrativas. En el 2000 se integra el Centro

Universitario de Occidente (Cunoc) a la red central financiera de la universidad. En el 2007 se pone en marcha el módulo de Gestión Automatizada de Ingresos (SIIF). En el 2008 se inicia la habilitación de la Red de Servicios Integrados dentro del campus central y el Centro Universitario Metropolitano (CUM). En el 2009 fue implementada la red inalámbrica RIUSAC. En el 2012 se pone en marcha el módulo de Gestión Automatizada de Sueldos y el de Ejecución Presupuestal Web (SIIF). En el 2014 se pone en marcha el módulo de Gestión Automatizada de Compras (SIIF). Así como la asignación en línea de la prueba de orientación vocacional para el campus central y los centros regionales. En el 2017 se pone en marcha el sistema de Control Académico Web en el Centro Universitario del Sur (Cunsur).

El Departamento de Procesamiento de Datos de la Dirección General Financiera, es quien más ha apoyado y asesorado a la universidad en cuestión de tecnología tal como lo indica su visión: “ser el ente que proporcione las directrices, infraestructura, asesoría y desarrollo en sistemas de información, telecomunicaciones, tecnología en general para la Universidad de San Carlos de Guatemala”[1].

A través del Departamento de Procesamiento de Datos de la Dirección General financiera se podrá realizar una propuesta de una política de seguridad de la información.

[1] Universidad de San Carlos de Guatemala.*Manual de organización del Departamento de Procesamiento de Datos de la Dirección General Financiera*. p. 9.

2. ¿QUÉ ES LA INFORMACIÓN?

Es un grupo de datos ya supervisados y ordenados, que sirven para construir un mensaje basado en un cierto fenómeno o ente. La información permite resolver problemas y tomar decisiones, ya que su aprovechamiento racional es la base del conocimiento. La información puede existir en muchas formas: impresa o escrita en un papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, mostrada en películas o hablada en una conversación. Cualquiera que sea la forma que tome la información, o medio por el cual sea almacenada o compartida, siempre debiera estar apropiadamente protegida.

La información es una serie de datos que es preciso obtener para conocer acciones y funciones que permitirán tomar decisiones y que trascienden en su planificación y el control de sus actividades. La información puede darse de varias formas que van desde la comunicación cara a cara, comunicación inalámbrica y virtual; extendiéndose a otras formas que la lleva a ser compleja debido a su codificación, interpretación y manejo. “La información es un conjunto de datos transformados de forma que contribuye a reducir la incertidumbre del futuro y, por tanto, ayuda la toma de decisiones. La información representa los datos transformados de forma significativa para personas que la reciben, es decir, tiene un valor real o percibido para sus decisiones y para sus acciones. Así pues, la información son datos que han sido interpretados y comprendidos por el receptor del mensaje”[2].

[2] LAPIEDRA, Rafael; DEVECE, Carlos; GUIRAL, Joaquín. *Introducción a la gestión de sistemas de información en la empresa*. p. 6.

Por otra parte, sobre el concepto de información se hace un cuestionamiento que adquiere significado en tanto que se plantea: ¿cuál es la escala en que la información puede seleccionarse?

"La información puede seleccionarse en primera instancia, como concepto con direccionalidad a lo que aún no se ha procesado dentro de la organización. Además, se separa de lo que ya ha sido trabajado o lo que se trabaja permanentemente. Por lo tanto, la información se trata de hechos que actualiza el uso de procedimientos y que se concretan con el pasar del tiempo"[3].

2.1. Clasificación de la información

Según la clasificación de la información, esta obedece a los siguientes cuatro criterios de acceso:

2.1.1. Información confidencial

La confidencialidad de la información es aquella que se constituye como reservada, que no se puede expresar de forma verbal y que, por su naturaleza, las personas tienen un deber intrínseco de no pronunciarse sobre ella. Por lo tanto, es privilegiada y, se comprende que es aquella que contiene un contenido profesional y que solo puede ser usada dentro del oficio o profesión y ser intercambiada por las personas inmersas y comprometidas según sus funciones y sus cargos.

Según Sosa en su artículo de clasificación de la información menciona la confidencialidad como un "tipo de información crítica y que solamente podrá ser

[3] RÍOS, Jaime. *Conceptos de información: dimensiones bibliotecológicas, sociológicas y cognoscitivas*. http://www.scielo.org.mx/pdf/ib/v28n62/0187-358X-ib-28-62-00143.pdf>. Consulta: 11 de noviembre de 2018.

conocida al interior de la entidad ya que su conocimiento externo podrá ocasionar efectos negativos sobre la entidad"[4].

Por otra parte, se entenderá la confidencialidad de la información, como "algo íntimo que la máxima autoridad o aquel que ha sido seleccionado de apreciar y autorizar el manejo de su valor, deba mantener dicha información con reserva y confidencialidad"[5].

2.1.2. Información restringida

Es aquella que se encuentra temporalmente fuera del acceso público, debido a que su difusión puede poner en riesgo la vida, seguridad y salud de las personas; así como la estabilidad, gobernabilidad y democracia de la entidad. De acuerdo a su naturaleza se recomienda, tener una base criptográfica porque el riesgo de su divulgación pudiera afectar a la institución en sus distintas acciones que esta realiza. Entonces, si cada entidad administrativa de la institución tiene información pertinente y exclusiva en su poder es obligación resguardarla como un tesoro invaluable.

"Por consiguiente, la información restringida solo deberá tener acceso un grupo específico de usuarios que requieran del conocimiento, porque de ellos dependerá el cumplimiento estricto de sus mandatos"[6].

---

[4] SOSA, Diego. *Clasificación de la información*. https://www.academia.edu/39201006/Clasificaci%C3%B3n_de_la_Informaci%C3%B3n. Consulta: 30 de octubre de 2018.

[5] Hites S.A. *Manual de manejo de información*. www.cmfchile.cl/institucional/inc/despliega_manual_manejo_info.php?nombre_archivo=MMI_20100830_120157_96947020.pdf. Consulta: 15 de enero de 2019.

[6] SOSA, Diego. *Clasificación de la información*. https://www.academia.edu/39201006/Clasificaci%C3%B3n_de_la_Informaci%C3%B3n. Consulta: 30 de octubre de 2018.

2.1.3. Información de uso interno

La departamentalización administrativa permite disponer de este tipo de información, que constituye un valor manejado al interior y de conocimiento del personal.

Según Rodrigo Zúñiga, que fue encargado de seguridad de la información de la Subsecretaria de Desarrollo Regional y Administrativa de Chile, determinó el uso de la información como un "bien disponible para todos los empleados, además, de terceros específicamente seleccionados" [7]. También, es objeto de ser proporcionada al público siempre y cuando se sujete a la normativa interna, con el aval de la gerencia o las jefaturas correspondientes. El riesgo de conceder esta información sin previa autorización puede ocasionar daños al interior de la institución de bajo impacto. No obstante, sus implicaciones tienen grados de riesgo mínimos.

2.1.4. Información pública

De acuerdo a la clasificación de la información según los niveles y criterios categorizados; la de orden público, por su soporte y forma de expresión en que obra en poder de los administradores y las dependencias públicas vinculadas, es toda aquella que se genera para su divulgación abierta a todos los interesados en obtenerla, manejarla, interpretarla, compartirla y utilizarla para fines académicos, culturales, de referencia o soporte de análisis.

Una de las características esenciales en el uso de esta información es asegurar su integridad y disponibilidad. Ejemplos de este tipo de información lo

[7] ZÚÑIGA, Rodrigo. *Política de seguridad sobre clasificación y manejo de la información*. http://www.chileindica.cl/instructivos/ Politica-Seguridad-Clasificacion-y-Manejo-de-Informacion-v4.pdf. Consulta: 12 de diciembre de 2018.

constituyen: resultados de investigaciones, campañas informativas, información de carácter bibliográfico, propuestas de ordenamiento, información que por ley reviste carácter público.

2.2. Objetivos específicos de seguridad de la información

Los objetivos de la seguridad de la información son:

- Garantizar el uso correcto y el manejo adecuado de la información a través del fiel cumplimiento de las políticas sugeridas por la comisión de seguridad y aprobadas por los órganos competentes. En esta tarea están involucrados los funcionarios universitarios, mandos medios, ejecutores de acciones administrativas, docentes, trabajadores administrativos, de servicios y estudiantes.

- Establecer la tecnología para el control eficiente y efectivo de la información.

- Aplicar las políticas que fortalezcan la seguridad de la información.

- Proteger y resguardar los activos físicos y electrónicos.

- Aplicar normas de ejecución y apreciación en el tratamiento de los riesgos que aseguren la confidencialidad, la integridad, la disponibilidad, sus rutas de seguimiento y la autenticidad de la información.

- Generar adaptabilidad evolutiva acorde a las necesidades e intereses institucionales, en relación con los planteamientos de eficacia y eficiencia en el manejo de la información.

- Proteger y resguardar los activos de información que la institución considere valioso: activos de información, datos oficiales, datos de personal, documentos impresos, resoluciones, acuerdos, actas, circulares, normas y procedimientos, dictámenes, cédulas de nombramientos y otros.

2.3. Seguridad de la información

J. M. Royer define la seguridad informática como la "protección contra todos los daños sufridos o causados por las herramientas del contexto y originados por el acto voluntario y de mala fe de un individuo"[8]. Entonces, para detener las amenazas se necesita poner un alto y multiplicar las barreras para que cuando se intente violar el espacio virtual, el ataque será bloqueado por otra barrera; sin embargo, ninguna protección es infalible. Para elegir un nivel de seguridad apto implica consecuencias ligadas con restricciones para los usuarios, la carga financiera por la adquisición de programas de protección, tiempo para implementar estas soluciones y mejoras en las instalaciones.

Según la Real Academia Española de la Lengua, el término seguridad esta acuñado a la cualidad de lo seguro, y lo seguro es algo que está libre de peligro fuera de daño alguno o exento de riesgo. Entonces, la seguridad de la información para efectos del presente estudio lo constituye el conjunto de controles, métodos, técnicas y herramientas que adopta la organización para proteger la información de cualquier amenaza; con el propósito de preservar confidencialidad, validez, confiabilidad y otras categorías que son inherentes en el buen manejo de la información.

[8] PALACIOS, Andres. *Diseño de un modelo de políticas de seguridad informática para la superintendencia de industria y comercio de Bogotá*. p. 21.

Por otro lado, Jeimy Cano en su análisis referente a la literatura de la seguridad de la información tipifica, en dos conceptos la esencia del término como “disciplina en el arte y la ciencia de la protección, enfocado en: los riesgos, las amenazas, el análisis de los escenarios, buenas prácticas y los esquemas normativos, que exigen niveles de aseguramiento de procesos y tecnologías para elevar el nivel de confianza en la creación, uso, almacenamiento, transmisión, recuperación y disposición final de la información. De conformidad con la secuencia del tratamiento de la temática es necesario abordar con precisión y claridad categorías que adopte la institución para el desarrollo de la información en el uso de metodologías ágiles, como la generación del conocimiento su protección y divulgación a los sistemas de información, establecimiento de sistemas o modelos de gestión de seguridad de la información institucional”[9].

2.4. Protección de la información

Las organizaciones poseen información que se traduce en activos que deben estar auditados por el personal inherente al puesto según la estructura organizacional. Estos deberán saber procedimientos y acciones que estarán fijadas en los nombramientos que formalizan los contratos. Estos controles deben de normalizarse y adecuarse a las necesidades de la organización a sus requerimientos y particularidades internas.

Robbins afirma que los gerentes pueden implementar controles, ya sea antes de comenzar una actividad, mientras está se encuentra en marcha o después que la misma ha terminado. Entonces, se puede decir que esta

[9] CANO, Jeimy. *La gerencia de la seguridad de la información: evolución y retos emergentes*. https://www.isaca.org/Journal/archives/2011/Volume-5/Pages/JOnline-La-Gerencia-de-la-Segurid ad-de-la-Informacion-Evolucion-y-Retos-Emergentes.aspx. Consulta: 9 de diciembre de 2018.

tipología de controles tiene como fin tratar de prevenir los problemas antes de que se realice la actividad en los diversos órdenes que se produzca, se maneje o prepare la información. Cuando se da en esta circunstancia el control de la información se pueden corregir estos inconvenientes antes que pongan en riesgo o se incurra en amenazas para asegurar el correcto funcionamiento institucional.

Una de las acciones más conocida es supervisar al subordinado mediante una vigilancia simultánea que le permita al empleado sentirse acompañado y que las actividades que realiza cuentan con respaldo necesario. Actualmente, los diseños de software ya cuentan con controles concurrentes en donde se le da al usuario una respuesta inmediata, que está incorporada a los programas y sus niveles de calidad son eficaces y eficientes. Además, los controles correctivos se basan en la retroalimentación, con el inconveniente de que cuando se han cometido estos infortunios y se recibe la información de su ejecución el daño ya está hecho.

2.5. Organización institucional para la protección de la información

Adquiere significancia este concepto dentro del contexto universitario por cuanto existen lineamientos sugeridos por los estándares internacionales para desarrollar un marco de gestión para la seguridad, normas ISO 27001 e ISO/IEC 27002; es de consideración la concepción central de esta norma. No cabe duda de que la implantación de un sistema de gestión de seguridad de la información es una decisión estratégica que debe involucrar a toda la universidad; implica a sus unidades ejecutoras que realicen diversas actividades para cumplir con el mandato constitucional. Las anteriores deben estar apoyadas y dirigidas desde Rectoría y con respaldo del Consejo Superior Universitario como máximo órgano de dirección.

La ISO/IEC 27001, en términos generales, no propone requisitos absolutos para la gestión de riesgos de seguridad de la información, pero sí sugiere procedimientos y la manera más eficaz de minimizarlos; se asegura que son identificados, evaluados y gestionados. Materializada la propuesta, considerando las medidas, adoptando los controles y procedimientos más eficaces de seguridad, el impacto que se espera tener dentro de la organización será con el firme propósito de darle protección.

2.6. Implementación del sistema de gestión de la seguridad de la información (SGSI) basado en la Norma ISO 27001

Para que el sistema de gestión de seguridad de la información funcione adecuadamente, es necesario que la institución establezca una adecuada gestión de riesgos la cual permita con certeza saber cuáles son las principales vulnerabilidades de sus activos de información y cuáles son las amenazas que evidencian la fragilidad de exponer las vulnerabilidades. A razón que la institución tenga fehacientemente esta identificación de riesgos podrá establecer las medidas preventivas y correctivas de viabilidad que garanticen mayores niveles de seguridad en su información.

La creciente preocupación de las entidades gubernamentales, no gubernamentales, autónomas o semiautónomas y empresas privadas gira en torno a cómo enfrentar los riesgos e inseguridades procedentes de diversas instancias. Instituciones de educación, como las de talla superior, que en su dinámica estructural manejan activos de información como uno de sus valores más importantes, se encuentran ligados o asociados a riesgos y amenazas que explotan una amplia tipología de vulnerabilidades.

La seguridad de estos activos de información gira en función de la apropiada y consecuente gestión de una serie de acciones: la capacidad de estructurar un plan de contingencia frente a los incidentes, la capacidad de análisis de riesgos, el grado en el que las autoridades se involucren en sus mandos superiores medios y de ejecución, la predisposición y voluntad para invertir en seguridad y el grado de implementación de controles serán factores importantes para realizar esta tarea.

Las consideraciones respecto a la seguridad de la información, según ISO 27001, están dirigidas en la preservación de su confidencialidad, integridad y disponibilidad, que es inclusivo de los sistemas que se constituyen para su tratamiento dentro de una institución. En términos generales, sobre estos conceptos se cimienta la base sobre la que se rige todo el andamiaje 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 la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran. Para garantizar que la seguridad de la información es gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI.

Con base en los aspectos claves de su diseño e implantación, la norma ISO 27001 establece las siguientes fases para elaborar un SGSI:

- Análisis y evaluación de riesgos
- Implementación de controles
- Definición de un plan de tratamiento de los riesgos o esquema de mejora.
- Alcance de la gestión
- Contexto de organización
- Partes interesadas
- Fijación y medición de objetivos
- Proceso documental
- Auditorías internas y externas

2.7. Riesgo de la información

Metodológicamente, lo que la línea de análisis señala como base para el control de riesgos es la identificación de activos de información. Resultado de esto es reconocer todos los recursos que involucra la gestión, traduciendo datos electrónicos de hardware, software, documentos escritos, documentos con características especiales, como fotográficos, fonográficos, proteger la propiedad intelectual y la información importante de las organizaciones y del recurso humano. Con este trabajo efectuado con relación a estos activos de información se puede hacer concretamente la identificación de riesgo.

2.8. Amenazas de la información

Según Camilo Gutiérrez, una amenaza se puede definir entonces como “un evento que puede afectar los activos de información y están relacionadas

con el recurso humano, eventos naturales o fallas técnicas"[10]. Algunos ejemplos pueden ser ataques informáticos externos, errores u omisiones del personal de la institución, infecciones con *malware*, terremotos, tormentas eléctricas o sobrecargas en el fluido eléctrico.

2.8.1. Tipos de amenazas

Para César Tarazonas "básicamente se pueden agrupar las amenazas de la información en cuatro 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"[11]

[10] GUTIÉRREZ, Camilo*. ¿Qué es y porque hacer un análisis de Riesgos?* https://www.welivesecurity.com/la-es/2012/08/16/en-que-consiste-analisis-riesgos/. Consulta: 17 de enero de 2019.
[11] TARAZONAS, César. *Amenazas informáticas y seguridad de la información*. p 138.

Por otro lado, se hace una descripción de algunas de las principales amenazas en la red:

- Programas espías (spyware): es común que en el uso de navegadores existan código malicioso cuyo principal objetivo es recoger información sobre las actividades de un usuario en un computador (tendencias de navegación), para permitir el despliegue sin autorización en ventanas emergentes de propaganda de mercadeo, o para robar información personal (p.ej. números de tarjetas de crédito).

- Troyanos, virus y gusanos: son programas de código malicioso, también conocido en el ambiente técnico como softwares maliciosos por la agrupación común en función de programas que han sido desarrollados para entrar en ordenadores sin permiso de su propietario y producir efectos no deseados. Estos efectos se producen algunas veces sin que se dé cuenta en el acto. Los profesionales de la computación suelen definir una variedad de software o programas de códigos hostiles e intrusivos. Sin embargo, la expresión 'virus informático' es más utilizada en el lenguaje coloquial y con regularidad en los medios de comunicación para referirse a todos los tipos de malware.

- Phishing: es la utilización de mensajes, correo electrónico o falsos sitios web que suplantan perfectamente a los sitios originales. Es una de las formas muy comunes, unido con la ingeniería social, con la razón esencial en forma fraudulenta de obtener datos confidenciales de un usuario, especialmente financieros; se aprovecha la creciente dependencia que éste tiene en los servicios electrónico-tecnológicos, aunados con desconocimiento de la forma en que operan y la oferta de servicios con mínimas medidas de seguridad.

- Spam: recibo de mensajes no solicitados, principalmente por correo electrónico, cuyo propósito es difundir grandes cantidades de mensajes comerciales o propagandísticos. Se han presentado casos en los que los envíos se hacen a sistemas de telefonía celular – mensajes de texto, o a sistemas de faxes. Según Prensa Libre "la primera conferencia de la 5 Cumbre Latinoamericana de Analistas de Seguridad de Kaspersky Lab, que se celebra en Santiago de Chile, estuvo a cargo del especialista en seguridad informática Dmitry Bestuzhev, quien dio a conocer que Brasil, México, Colombia, Perú, Chile, Guatemala, República Dominica, Costa Rica, Argentina, Paraguay y Venezuela son los países que más riesgo tienen en cuanto a ataque informáticos"12. Y el argumento continúa señalando que Guatemala ocupa el puesto 111 en el conteo mundial particularizando que en Latinoamérica en los primeros ocho meses del 2015 se había registrado un total de trecientos noventa y ocho mil seiscientos once (398,611) incidentes que atentan contra la seguridad de la población de este sector. Esto significa que ocurren 20.1 vulnerabilidades por segundo, destaca.

- Botnets (redes de robots): se constituyen por equipos de cómputo infectadas y controladas remotamente, que se comportan como 'zombis', quedando incorporadas a redes distribuidas de computadores llamados robot, los cuales envían de forma masiva mensajes de correo spam o código malicioso, con el objetivo de atacar otros sistemas. Portatilic/EP indica que el malware se ha incrementado en un 51 % entre noviembre de 2016 y octubre de 2017 y que de acuerdo al informe anual de Ciberseguridad de 2018 de Cisco, el crecimiento de Botnes de dispositivos del internet de las cosas (loT, por sus siglas en inglés)

[12] DÁVILA, Cristian. *Así está Guatemala en cuanto a seguridad informática.* Prensa Libre.27 de agosto de 2015. https://www.prensalibre.com/vida/tecnologia/asi-esta-guatemala-en-cuanto-a-seguridad-informa tica/. Consulta: 1 de marzo de 2019.

siendo evidente el crecimiento el uso de técnicas de cifrado por parte de los cibercriminales que se evidencia el paso de un 19 % a un 70 % incremento del *malware* que evita su detección ocultando la actividad de mando y control.

- Trashing: término que tiene que ver con los desechos, y aunque parezca insólito los cibercriminales intentan apropiarse del control de equipos y de información. Este es un delito informático poco conocido al ser relativamente reciente su incorporación a este ámbito, pero no por ello menos relevante. La Agencia Española de Protección de Datos (AEPD) establece que se trata de una técnica que consiste en obtener información privada a partir de la recuperación de archivos, documentos, directorios e, incluso, contraseñas que el usuario ha enviado a la papelera de reciclaje de su equipo. “Si la información se recolecta de ‘las papeleras’ como papeles o discos duros se habla de trashing físico”, explican desde el organismo regulador.

Para Camilo Gutiérrez en su análisis de la vulnerabilidad, define que “una característica esencial de un activo de información es aquel que representa un riesgo para la seguridad de la información”[13]. Si se concreta una amenaza y hay una vulnerabilidad que pueda ser aprovechada, hay una exposición a que se presente algún tipo de pérdida para la institución. Por ejemplo, el hecho de tener contraseñas débiles en los sistemas y que la red de datos no esté correctamente protegida puede ser aprovechado para los ataques informáticos externos. En esa dimensión, para que la institución pueda tomar decisiones sobre cómo actuar ante los diferentes riesgos es necesario hacer una valoración para determinar cuáles son los más críticos. Esta valoración, con

[13] GUTIÉRREZ, Camilo*. ¿Qué es y porque hacer un análisis de riesgos?* https://www.welivesecurity.com/la-es/2012/08/16/en-que-consiste-analisis-riesgos/. Consulta: 17 de enero de 2019.

regularidad se ejecuta en términos de la posibilidad de ocurrencia del riesgo y del impacto que tenga la materialización del riesgo. La valoración del impacto se mide identificando las variables en sus diferentes mediciones categóricas o numéricas: la pérdida económica, si es posible cuantificar la cantidad de dinero que se pierde, la reputación de la empresa dependiendo si el riesgo pueda afectar la imagen de la empresa en el mercado o de acuerdo al nivel de afectación por la pérdida o daño de la información.

La identificación precisa de estas categorías y la valoración matricial de los principales riesgos están propensos afectar los activos de información de la institución, conjuntamente con la identificación de amenazas, debe llevar a la identificación de controles ya sea para mitigar la posibilidad de ocurrencia de la amenaza o para mitigar su impacto. Las medidas de control que puede asumir una empresa están relacionadas con el tipo de amenaza y el nivel de exposición que represente para la información corporativa.

El sistema de gestión de seguridad de la información debe garantizarle a la institución la tranquilidad de tener identificados sus riesgos y los controles que le van a permitir actuar ante una eventual materialización o simplemente evitar que se presenten. Esta gestión debe mantener el equilibrio entre el costo que tiene una actividad de control, la importancia del activo de información para los procesos de la empresa y el nivel de criticidad del riesgo.

3. GENERALIDADES DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Según Álvaro Gómez, en su Enciclopedia de la Seguridad Informática, cita los procedimientos de seguridad como “componentes para tareas y operaciones que generan una serie de registros y evidencias para facilitar el seguimiento, control y supervisión de la seguridad de la información”[14]. Por consiguiente, los procedimientos de seguridad permiten implementar políticas que constituyen una herramienta para hacer frente a futuros problemas, fallo de sistemas, imprevistos o posibles ataques de informática. En este sentido, las políticas definen qué se debe proteger en el sistema, mientras que los procedimientos describen cómo se debe conseguir dicha protección.

Entonces, una política de seguridad es una declaración de intenciones de alto nivel, que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requieran.

Por otra parte, la organización deberá tener identificado al personal para garantizar el adecuado nivel de cumplimiento de las normas y procedimientos de seguridad.

[14] GÓMEZ, Álvaro*. Enciclopedia de la seguridad informática.* p. 72.

3.1. Clasificación de las políticas

Dentro de las políticas de la información existe una tipología o clasificación que determina la jerarquía en la que se posicionan las antes mencionadas. A continuación, se plantea el orden según su importancia:

3.1.1. Políticas generales de alto nivel

Las políticas de alto nivel se clasifican en:

3.1.1.1. Política de seguridad

El objetivo de una política de seguridad consiste en proporcionar orientación y apoyo en la dirección de la seguridad informática. La dirección establecerá políticas correspondientes con los objetivos de la entidad, las cuales deberán comunicarse a todos los usuarios de manera accesible y comprensible. Comenzar con la definición de las políticas de seguridad a partir de los riesgos estimados debe asegurar que las medidas y procedimientos proporcionen un adecuado nivel de protección para todos los bienes informáticos.

Por otra parte, una política de seguridad es la que "establece límites que permiten la gobernanza y dan la normativa necesaria para seguridad basada en resultados"[15]. Derivado de lo anterior, toda organización debe disponer de un sistema de seguridad como marco institucional, instrumental y funcional para enfrentar riesgos y amenazas que le impidan cumplir con sus fines.

[15] CONSEJO NACIONAL DE SEGURIDAD. *Política Nacional de Seguridad. Referencias institucionales, marco normativo*. p. 6.

3.1.2. Políticas de alto nivel por temas específicos

Se clasifican en:

3.1.2.1. Políticas de seguridad de la información

Para crear una política es necesario planear y no caer en la improvisación. Entonces, planear es una acción de categoría intelectual que se apoyará en la prevención, que se inclina en la voluntad con un análisis definido en lo más conveniente, que opta por una variedad de posibilidades. Constituyen también principios generales de acción que adopta la organización para formular, interpretar o sustituir las normas concretas. Entonces, una política se constituye en una norma de acción legitimada y ejecutada por un responsable o una comisión de trabajo. Además "la determinación de políticas es una herramienta importante para coordinar y controlar las actividades de planeación ya que las políticas fijan los limites dentro de los cuales deben funcionar determinadas actividades o unidades de operación"[16]

3.1.2.2. Políticas de SGSI

"El sistema de gestión de la seguridad de la información (SGSI) es un modelo que busca brindar que se establezca, implemente, opere, de seguimiento, revise, mantenga y mejore un sistema de información. El SGSI está diseño para aplicarlo con base en las necesidades y los objetivos de una organización; se espera por ejemplo que una situación simple requiera de una solución de SGSI simple"[17].

[16] GÓMEZ, Guillermo. *Planificación y organización de empresas*. p. 265.

[17] ICONTEC. *Norma técnica colombiana*. http://intranet. bogotaturismo.gov.co/ sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf. Consulta: 3 de enero de 2019.

Por otra parte, la Oficina de Seguridad para las Redes Informáticas recomienda en su metodología para la gestión de la seguridad informática que durante la implementación del SGSI se comience por identificar los riesgos mediante la aplicación de controles, seleccionando acciones correctas por parte de personal definido y las medidas administrativas porque estas garantizarán la implantación de controles efectivos para lograr la seguridad en correspondencia con los objetivos de la institución, de manera que se mantenga el riesgo por debajo del nivel asumido por la propia entidad.

Entonces, se puede decir que mientras exista entrenamiento, programas de capacitación y las responsabilidades estén definidas, se podrá garantizar que el personal al que se le asignen tareas exigidas en torno al SGSI podrá responder ante la toma de decisiones. La institución debe asegurar que el personal debe tener conciencia de la importancia de las actividades de seguridad informática que le corresponde realizar y cómo ellas contribuyen al logro de los objetivos del SGSI que a continuación se hará mención:

- Concienciar al personal de la importancia que el SGSI tiene para la institución.

- Garantizar la divulgación, el conocimiento y la comprensión de las políticas de seguridad que se implementen.

- Capacitar a los usuarios en las medidas y los procedimientos que se implantarán.

- Lograr que el personal esté consciente de los roles a cumplir dentro del SGSI.

Finalmente, se implementarán los procedimientos y controles que se requieran para detectar y dar respuesta oportuna a los incidentes de seguridad que se presenten; incluye su reporte a las instancias pertinentes.

3.1.2.3. Políticas sobre control de acceso

El control de quién accede a la información es el primer paso para protegerla. Es de mucha importancia delegar quién tiene pase para acceder a la información, cómo, cuándo y con qué finalidad. Al momento de gestionar el control de acceso a la base de datos se debe considerar que la información, los servicios y las aplicaciones no tienen por qué centralizarse en una sola instalación, sino que pueden estar dispersos en equipos y redes propias o de terceros. Se debe considerar hoy por hoy que cada vez es más utilizado el dispositivo móvil en los centros de trabajo. Por lo anterior, se incluirán una serie de controles, que según Benítez, ayudan al cumplimiento de las políticas de seguridad de control de acceso, por ejemplo:

- Las empresas destinarán un área que servirá como centro de ubicación para los sistemas de telecomunicaciones y servidores.
- Todos los sistemas de comunicaciones estarán debidamente protegidos con la infraestructura apropiada de manera que el usuario no tenga acceso físico directo. Se entiende por sistema de comunicaciones: el equipo activo y los medios de comunicación.
- El acceso de terceras personas debe ser identificado plenamente, controlado y vigilado durante el acceso portando una identificación que les será asignado por el área de seguridad de acceso al edificio y a las oficinas de la institución.
- Las visitas internas o externas podrán acceder a las áreas restringidas siempre y cuando se encuentren acompañadas cuando menos por un responsable del área de tecnología o con permiso del departamento encargado de autorización.
- Las visitas a las instalaciones físicas de los centros de telecomunicaciones se harán en el horario establecido.

- El personal autorizado para mover, cambiar o extraer equipo de cómputo es el poseedor del mismo o el superior responsable, a través de formatos de autorización de entrada/salida, los cuales notificarán a las personas delegadas del área administrativa de las empresas y al personal de seguridad del edificio[18].

Por otro lado, la Universidad Distrital Francisco José de Caldas plantea dentro de sus políticas seguridad que "se debe tener acceso controlado y restringido a los cuartos de servidores principales y a los cuartos de comunicación si existen. La oficina de control de datos será la que mantendrá las normas, controles y registros a dichas áreas"[19]. El acceso a los recursos de tecnologías de información institucional debe estar restringidos según los perfiles de usuarios definidos por el Departamento de Procesamiento de Datos.

3.1.2.4. Políticas sobre criptografía

Guillermo Gómez describe la criptografía como una "ciencia que se encarga de estudiar las distintas técnicas empleadas para cifrar la información y hacerla irreconocible a todos aquellos usuarios no autorizados"[20]. Mediante la criptografía es posible garantizar la confidencialidad, la integridad y la autenticidad de los mensajes y documentos guardados en un sistema o red informático.

Un sistema criptográfico moderno se basa en un algoritmo cifrado que transformará el texto conocido como texto claro. Mediante el proceso inverso se podrá recuperar el texto original. Esto dependerá de una clave que será la que determine el resultado esperado. De manera que, aunque los algoritmos sean

[18] BENÍTEZ, María. *Gestión integral*. p. 5.
[19] Universidad Distrital Francisco José de Caldas. *Políticas para la seguridad de la información*. https://portalws. udistrital.edu.co/CIT/paginas/polSeguridad.php Versión: 0.0.0.11. Consulta: 21 de enero de 2019.
[20] GÓMEZ, Guillermo. *Planificación y organización de empresas*. p. 361.

públicos y conocidos por todos, si no se dispone de las claves, resultará imposible realizar el proceso de descifrado.

Por otra parte, la Universidad Oberta de Catalunya en su texto aprobado por el comité de dirección ejecutiva hace mención que una política criptográfica es aplicable a todos los sistemas de información de apoyo a procedimientos, actividades académicas y de gestión electrónica; también, a las relaciones por medios electrónicos con terceros que no forman parte de la comunidad universitaria. Aunado a lo anterior las normativas de desarrollo de esta política deben indicar la aplicación de criptografía en cada caso y escenario concretos: Firma electrónica, autenticación electrónica, cifrado y una prueba electrónica.

3.1.2.5. Políticas de gestión de incidentes

La oficina de seguridad para las redes informáticas hace énfasis en su metodología para la gestión de la seguridad informática diciendo que estas políticas describen las medidas, procedimientos de detección, neutralización y recuperación ante cualquier evento, que pueda paralizar total o parcialmente las actividades informáticas. Se puede definir un incidente de seguridad a cualquier evento que se produzca de forma accidental o intencional, que afecte o ponga en peligro las tecnologías de la información o los procesos que con ellas se realicen, incluyendo entre otros:

- Acceso o intento de acceso no autorizado a un sistema de datos.
- Uso no autorizado de un sistema para el procesamiento o almacenamiento de información.
- Suplantación de identidad.

- Cambios a las características del equipamiento, las aplicaciones o datos del sistema sin el conocimiento o consentimiento del responsable de dicho sistema.

3.2. Pasos para la creación de políticas

- Analizar la función del negocio u organización y los procesos inmersos en este.

- Estudiar el departamento o unidad de informática que administre o maneje los procesos fundamentales de la organización.

- Investigar y analizar los incidentes de seguridad ocurridos en la organización.

- Seleccionar ISO 27001 y 27002 como modelo de referencia de mejores prácticas internacionales en seguridad de la información.

- Identificar los activos de información.

- Las políticas a decretar deben redactarse especificando su alcance.

"Dentro de las recomendaciones que se deben considerar para la creación de una política es pensar en la convivencia clara y específica porque de ellas dependerá que se pueda lograr la fragmentación por departamento o unidad de trabajo. Solo así, se podrá jerarquizar la aplicabilidad general y aplicabilidad para grupos o tareas"[21].

[21] DOMÍNGUEZ, Jorge. *Seguridad informática personal y corporativa*. p. 108.

4. PROPUESTA DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

4.1. Política general de la seguridad de la información

La Universidad de San Carlos de Guatemala, como única universidad estatal, le corresponde con exclusividad dirigir, organizar y desarrollar la educación superior del Estado y la educación profesional universitaria estatal, así como la difusión de la cultura en todas sus manifestaciones.

Como tal, establece que la información es vital para el desarrollo de las actividades de la educación superior. Por lo que garantiza su protección ineludible frente a las amenazas y vulnerabilidades, comprometiéndose a minimizar los riesgos y generar mecanismos para la difusión, estudio y actualización de la presente política.

Consiente de la importancia que la seguridad de la información tiene para el desarrollo y buen funcionamiento de sus procesos internos que están encaminados a mejorar, entendiéndose esta como la preservación de la confidencialidad, la integridad y la disponibilidad de la misma, así como de los sistemas que la soportan, incrementando los niveles de confianza de sus acciones primigenias constituidas en: investigación, docencia, extensión y en sus acciones administrativas motivo por el cual: el Consejo Superior Universitario, la Rectoría, sus dependencias, facultades, escuelas no facultativas, centros regionales, centros de investigación y otras están comprometidos a proteger los activos de la información de la institución. Y para

tal fin el Consejo Superior Universitario debe establecer un ente de tecnología con potestad para normar y velar el que hacer en dicho ámbito.

La presente Política de Seguridad de la Información Universitaria será aplicada por todos los empleados y funcionarios públicos, estudiantes, docentes, investigadores y proveedores.

4.2. Comité de seguridad de la información

Se crea el Comité se Seguridad, el cual estará conformado por:

- Rector de la Universidad o delegado.
- Director General Financiero o delegado.
- Jefe de la Oficina de Seguridad de la Información (quien funge como secretario).
- Representante del área de tecnología de la Facultad de Ingeniería (delegado del Decano, se sugiere sea el Director de Escuela de Ciencias y Sistemas).
- Director General de Administración o delegado.
- Director General de Docencia o delegado.

4.2.1. Funciones del comité

- Someter al Consejo Superior Universitario la aprobación de las políticas de seguridad de la información.

- Revisar y actualizar las políticas de seguridad de la información periódicamente en un tiempo no mayor a un año.

- Someter al Consejo Superior Universitario las actualizaciones y modificaciones de las políticas de seguridad de la información.

4.3. Oficina de Seguridad de la Información

Se crea la Oficina de Seguridad de la Información, encargada de realizar las funciones siguientes:

- Crear las políticas y elevarlas al comité para su revisión.

- Ejecutar las políticas dictadas por el Consejo Superior Universitario.

- Supervisar que los empleados y funcionarios públicos, estudiantes, docentes, investigadores y proveedores, cumplan con las políticas de seguridad de la información.

- Afianzar la seguridad y privacidad de la información de la universidad.

- Informar al Comité sobre incidentes de seguridad ocurridos.

- Coordinar y gestionar el equipo de respuesta ante incidentes de seguridad de la información.
- Aprobar y revisar los métodos de encriptación y de autenticación.

4.3.1. Conformación de la oficina

Personal básico de la Oficina de Seguridad de la Información:

- Oficial de seguridad (jefe de la oficina).
- Ingeniero de infraestructura TI.
- Administrador de seguridad de red (ingeniero en sistemas o electrónico, experto en seguridad perimetral).
- Secretaria.

4.4. Política de seguridad de la información

Las presentes constituyen un conjunto de políticas iniciales, las más importantes o base para realizar la creación, revisión y aprobación por parte del Comité de Seguridad de la Información.

4.4.1. Recurso humano

Todo el personal y los estudiantes de la Universidad son responsables de la seguridad de la información.

- El usuario tiene restringida la instalación de software en su computador a excepción de casos extraordinarios con previa autorización de la unidad de informática correspondiente.

- La detección de programas sospechosos o maliciosos, virus, intentos de intromisión que los usuarios detecten deben ser reportados de inmediato a su unidad Informática.

- Las intromisiones, escaneos a las redes o cualquier equipo tecnológico por parte del personal universitario, los estudiantes y los proveedores que carezcan de autorización serán reportadas y analizadas por las autoridades de la unidad. Para ser tratados de acuerdo a la legislación universitaria vigente.

- Los usuarios no deben proporcionar información de la universidad a persona o entidad externa sin la debida autorización.

- El departamento responsable del control, el manejo y la distribución del fluido eléctrico debe estar informado de los cortes sectoriales por parte de los proveedores del servicio a fin de prever contingencias en los sistemas de información. Debe informar con anticipación a las autoridades responsables en cada unidad ejecutora de la universidad.

- El jefe del departamento o la autoridad de la unidad ejecutora al momento cuando un usuario termine su contratación o exista un cambio de funciones debe gestionar ante el departamento de informática correspondiente la inhabilitación del acceso a los sistemas.

- Los usuarios no deben utilizar el equipo de cómputo, sistemas u otro equipo tecnológico para actividades personales. Únicamente deben usarse para desarrollar las actividades de la universidad.

- Los empleados y funcionarios públicos no deben distribuir, copiar, destruir archivos o documentos físicos sin la debida autorización.

- El empleado o funcionario público que utilice los sistemas de información debe velar por la integridad, disponibilidad, confiabilidad y confidencialidad de la información que utilice.

- Los funcionarios y empleados con equipo de la universidad bajo su cargo, si estos sufren daños o pérdida deben ser reportados inmediatamente al jefe de su departamento.

- El usuario no debe desinstalar por ningún motivo la herramienta contra software malicioso proporcionado por el departamento o unidad de informática.

- Las contraseñas que el usuario utilice deben ser por lo menos de ocho caracteres y utilizar como mínimo una letra mayúscula.

- La Unidad de Sueldos y Nombramientos de la División de Recursos Humanos, debe incluir dentro de la documentación del nombramiento o contrato del empleado, un acuerdo de confidencialidad de la información de la universidad. El formato del acuerdo de confidencialidad debe estar aprobado por la Oficina de Seguridad de la Información.

4.4.2. Adquisición, desarrollo y mantenimiento de los sistemas informáticos

Los sistemas informáticos que sean desarrollados por el personal de la universidad o por terceros deben establecerse buenas prácticas y lineamientos de control que aseguren la seguridad de la información.

- El Departamento de Procesamiento de Datos, los controles académicos u otra unidad de la universidad que construya software debe realizarlo con una metodología de desarrollo aprobada por la Oficina de Seguridad de la Información.

- Las solicitudes de modificación al software deberán ser requeridas por la entidad que le compete, la cual previo a la modificación debe ser avalada por el jefe de la unidad de procesamiento de datos, control académico o por la unidad que le corresponda realizar la modificación.

- Las contraseñas del ambiente de producción no deben ser compartidos a los desarrolladores de software.

- Los sistemas de software que se encuentren en funcionamiento únicamente podrán ser modificados por personal autorizado de acuerdo a las normas y procedimientos establecidos por la Oficina de Seguridad de la Información.

- Las unidades o departamentos que desarrollen software deben tener separado su ambiente de desarrollo y pruebas del ambiente de producción.

- Todo software desarrollado por personal de la universidad o por terceros deben realizarse pruebas de funcionamiento, técnicos y de seguridad.

- La configuración del ambiente de pruebas debe ser equivalente al ambiente de producción.

- El software que sea desarrollado o modificado por personal de la universidad, los derechos de propiedad intelectual son exclusivamente de la universidad.

- El software que sea desarrollado o modificado por terceras personas dentro de las cláusulas de contratación debe especificarse, que no puede compartir o revelar información técnica del desarrollo, así como su confidencialidad e indicar que los derechos de propiedad intelectual son exclusivamente de la universidad. Así mismo, debe entregar el código fuente, así como la documentación respectiva.

4.4.3. Hardware

Las unidades ejecutoras deben acoger los lineamientos siguientes en la compra y mantenimiento de equipo de cómputo o de telecomunicaciones.

- La unidad o departamento que compre equipo debe ser de marca reconocida y contar con asistencia nivel nacional e internacional.

- El equipo tecnológico que se compre para el procesamiento de información de la universidad, debe ser tecnología de punta que garantice el fiel cumplimiento de factores como: velocidad de transferencia, procesamiento y capacidad de almacenamiento.

4.4.4. Seguridad física y ambiental

Los departamentos o unidades de informática deben velar porque únicamente personal autorizado ingrese a las instalaciones físicas de los centros de datos. Asegurar controles en la administración y mantenimiento del equipo de telecomunicaciones.

- La jefatura del Departamento de Procesamiento de Datos de la Dirección General Financiera es la única quien puede autorizar el acceso a la red troncal de la universidad. Si la autorización es para personas ajenas al Departamento de Procesamiento de Datos esta debe ser por escrito y durante el acceso estar acompañado por personal del área de redes.

- El acceso a las redes propias de las facultades, las escuelas no facultativas o los centros regionales debe ser autorizado por el jefe o encargado de la unidad de informática correspondiente.

- Solo el personal autorizado podrá ingresar al centro de datos para lo cual debe llevarse bitácora del acceso.

- No es permitido ingresar alimentos y bebidas al centro de datos.

- Todo gabinete de red debe contar con un sistema de energía de respaldo o UPS.

- Los mantenimientos que se realicen a los gabinetes de red deben ser previamente calendarizados y realizados de acuerdo al cronograma y comunicado a la comunidad universitaria que pueda verse afectado.

- Todo mantenimiento a los gabinetes de red que no fuese realizado por personal del área de informática de la universidad, el área encargada de realizar debe pedir acompañamiento o supervisión al área o departamento de informática.

- Los centros de datos deben contar con sistema de alerta de humedad, inundaciones, temperatura, sistemas contra incendios, sistema de vigilancia. Los cuales deben estar siempre monitoreados.

- Cuando un empleado o funcionario deje de laborar para la universidad todas las credenciales de acceso a las instalaciones deben ser desactivados.

4.4.5. Control de acceso

Los departamentos o unidades de informática de la universidad encargadas de administrar las redes deben velar que únicamente los accesos autorizados puedan hacer uso de los recursos de red.

- El acceso remoto a la red debe ser a través de VPN la cual será otorgada y monitoreada por el departamento o unidad informática encargada de la administración.

- Los puertos y servicios de red que no sean necesarios deben ser deshabilitados.

- La configuración de los servidores, *routers, switchs, firewalls* deben estar bien documentadas. La documentación debe estar custodiada por el jefe del departamento o unidad informática.

- Los analizadores de red únicamente pueden ser usados por los administradores de red o por personal de informática previamente autorizados por la autoridad competente.

- Las redes de la universidad deben ser monitoreadas, guardando y analizando las actividades registradas para reducción y previsión de riesgos en la seguridad de la información.

- Cuando una red comprometa la seguridad de la información en la red principal de datos debe ser desconectada. El Departamento de Procesamiento de Datos de la Dirección General Financiera informará de lo actuado a la unidad o departamento de informática correspondiente y a la Oficina de Seguridad de la Información.

4.4.6. Código malicioso

Es importante definir métodos de control de software malicioso para garantizar la disponibilidad, confidencialidad e integridad de la información de la universidad. Corresponde al Comité de Seguridad definir la herramienta de software que se implemente en la institución.

- El departamento o unidad de informática es quien proporciona el software antivirus, *antimalware, antispam, antispyware* y otras.

- El departamento o unidad de informática debe velar porque las licencias se encuentren actualizadas.

- Todo equipo de cómputo de la universidad debe tener instalado antivirus.

- El departamento o unidad de informática debe velar porque la configuración de la herramienta proporcionada no sea modificada por el usuario.

- Los casos de código malicioso detectados o reportados por el usuario deben ser documentados por la Oficina de Seguridad de la Información.

4.4.7. Correo electrónico

Restringir el uso del servicio de correo que provee la universidad para asegurar el resguardo de la información de la universidad en las actividades que requieran su uso.

- La información de uso interno o público que sea requerida a través de correo electrónico deberá ser atendido únicamente a través del correo institucional.

- El departamento o unidad de informática encargada de administrar el servidor de correo es quien crea las cuentas a los usuarios que estén previamente autorizados.

- Las cuentas de correo son individuales e inalienables.

- El correo institucional debe usarse únicamente para el desarrollo de las actividades laborales. No se permite el uso del correo para asuntos personales.

- Los correos de dudosa procedencia deben ser reportados al departamento o unidad informática.

- Las listas de correo electrónico únicamente deben usarse para tratar temas de difusión, comunidad, organización e investigación.

4.4.8. Criptografía

Los Departamentos o unidades de informática cuidan la información de la universidad considerada como confidencial y restringida mediante métodos de cifrado.

- Todas las claves o contraseñas de acceso a los sistemas informáticos de la universidad deben estar encriptadas en la base de datos.

- En el desarrollo de software se deben establecer lineamientos de cifrado de la información y las aplicaciones a utilizar, aprobadas por la Oficina de Seguridad de la Información.

- La información clasificada como confidencial y restringida debe cifrarse para su almacenamiento y transmisión.

- La Oficina de Seguridad de la Información debe establecer estándares en el uso de controles criptográficos.

- Los controles criptográficos establecidos por la Oficina de Seguridad de la Información, el personal de desarrollo de la universidad o externo debe cerciorarse que se cumplan en el desarrollo del software.

CONCLUSIONES

1. El Departamento de Procesamiento de Datos ha desempeñado un rol importante en el proceso de tecnificación de los procesos de la universidad.

2. Lo más valioso dentro de una organización son sus activos de información, por ende, estos deben ser resguardados y protegidos de la mejor manera.

3. Para la seguridad de la información su enfoque u objetivo principal consiste en garantizar la confidencialidad, integridad y disponibilidad de la información.

4. Al implementar las políticas de seguridad de la información en la universidad se reducen las amenazas internas y externas y se protege la integridad, confidencialidad y disponibilidad de la información.

RECOMENDACIONES

1. Que la universidad imparta cursos de informática básica a sus colaboradores a fin de crear una cultura informática dentro de la institución.

2. Crear un plan de concientización y formación en el recurso humano de la universidad, para la seguridad de la información.

3. Para garantizar la seguridad de la información, la universidad tendrá que invertir en tecnología para los centros de datos como: biométricos, sistema de video-vigilancia monitorizada y activada por movimiento, sistema de detección de agua y humedad, sistema contra incendios, sistema de refrigeración con capacidad de detección de contaminantes del exterior, el sistema eléctrico debe contar con respaldo de energía, sistemas de copias de respaldo, sistema de autenticación de red, sistema de eventos de ataques, dispositivos de protección en cada *rack, firewall* físicos, filtro de *spam*, filtro de contenido, sistema de monitoreo de servicios, personal capacitado en *ethical hacking y penetration test*.

4. Que el jefe de la Oficina de Seguridad de la Información posea título de ingeniero en ciencias y sistemas o carrera a fin y que tenga conocimientos en desarrollo de políticas, procesos, estándares, procedimientos y controles, basado en ISO/IEC 27001 y COBIT.

BIBLIOGRAFÍA

1. BENÍTEZ, María. *Gestión integral*. Las Palmas de Gran Canaria, España: Revista. No. 1., 2013. 18 p.

2. CANO, Jeimy. *La gerencia de la seguridad de la información: evolución y retos emergentes*. [en línea]. <https://www.isaca.org/Journal/archives/2011/Volume-5 /Pages/JOnline-La-Gerencia-de-la-Seguridad-de-la-Informacion-Evolucion-y-Retos-Emergentes.aspx>. [Consulta: 9 de diciembre de 2018].

3. Consejo Nacional de Seguridad. *Política nacional de seguridad*. Guatemala: Consejo Nacional de Seguridad, 2017. 58 p.

4. DÁVILA, Cristian. *Así está Guatemala en cuanto a seguridad informática.* Prensa Libre.27 de agosto de 2015. [en línea]. <https://www.prensalibre.com/vida/tecnologia/asi-esta-guatemala-en-cuanto-a-seguridad-informatica/>. [Consulta: 1 de marzo de 2019].

5. DOMÍNGUEZ, Jorge. *Seguridad informática personal y corporativa*. Venezuela: IEASS Editores, 2015. 158 p.

6. GÓMEZ, Álvaro. *Enciclopedia de la seguridad informática*. 2a ed. México: Alfaomega Grupo Editor S. A., 2014. 830 p.

7. GÓMEZ, Guillermo. *Planificación y organización de empresas*. 8a ed. México: McGraw-Hill, 1994. 61 p.

8. GUTIÉRREZ, Camilo*. ¿Qué es y porque hacer un análisis de riesgos?* [en línea]. <https://www.welivesecurity.com/la-es/2012/08/16/en-que-consis te-analisis-riesgos/>. [Consulta: 17 de enero de 2019].

9. Hites S.A. *Manual de manejo de información*. [en línea]. <www.cmfchile.cl/institucional/inc/despliega_manual_manejo_info. php?nombre_archivo=MMI_20100830_120157_96947020.pdf>. [Consulta: 15 de enero de 2019].

10. ICONTEC. *Norma técnica colombiana*. [en línea]. <http://intranet. bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/ Norma.%20NTC-ISO-IEC%2027001.pdf>. [Consulta: 3 de enero de 2019].

11. LAPIEDRA, Rafael; DEVECE, Carlos; GUIRAL, Joaquín. *Introducción a la gestión de sistemas de información en la empresa*. España: Castellón de la Plana, 2011. 553 p.

12. Ministerio de Cultura y Juventud. *Políticas de clasificación de la información*. [en línea]. <http://www.mcj.go.cr/ministerio/organi zacion/administrativo/informatica/politicasti/DI-PO-04-2014%20Po litica%20de%20Clasificacion%20de%20la%20Informacion.pdf>. [Consulta: 12 de enero de 2019].

13. Oficina de Seguridad para las Redes Informáticas. *Metodologías para la gestión de la seguridad informática*. [en línea]. <https://www.google.com.gt/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwiIsuuh4fhAhXCwFkKHUUfCEcQFjAAegQICRAC&url=https%3A%2F%2Finstituciones.sld.cu%2Fdnspminsap%2Ffiles%2F2013%2F08%2FMetodologia-PSI-NUEVAProyecto.pdf&usg=AOvVaw2jg3bQAhbsjUDMdkHaY5uP>. [Consulta: 12 de febrero de 2019].

14. PALACIOS, Andres. *Diseño de un modelo de políticas de seguridad informática para la superintendencia de industria y comercio de Bogotá*. Colombia: Universidad Libre de Colombia, 2015. 87 p.

15. Portaltic. *El malware oculto en tráfico cifrado y las botnets IoT incrementan su actividad en 2017*. [en línea]. <https://www.europapress.es/portaltic/ciberseguridad/noticia-malware-oculto-trafico-cifrado-botnets-iot-incrementan-actividad-2017-2018032218 2059.html>. [Consulta: 5 de marzo de 2019].

16. RÍOS, Jaime. *Conceptos de información: dimensiones bibliotecológicas, sociológicas y cognoscitivas*. [en línea]. <http://www.scielo.org.mx/pdf/ib/v28n62/0187-358X-ib-28-62-00143.pdf>. [Consulta: 11 de noviembre de 2018].

17. SOSA, Diego. *Clasificación de la información*. [en línea]. <https://www.academia.edu/39201006/Clasificaci%C3%B3n_de_la_Informaci%C3%B3n>. [Consulta: 30 de octubre de 2018].

18. Universidad Distrital Francisco José de Caldas. *Políticas para la seguridad de la información*. [en línea]. <https://portalws.udistrital.edu.co/CIT/paginas/polSeguridad.php Versión: 0.0.0.11>. [Consulta: 21 de enero de 2019].

19. Universidad Oberta de Catalunya. *Política de seguridad criptografía de la Universidad Oberta de Catalunya*. Barcelona, España: Universidad de Oberta, 2015. 17 p.

20. Universidad de San Carlos de Guatemala. *Actualización manual de normas y procedimientos*. [en línea]. <http://dpd.usac.edu.gt/wp-content/uploads/2017/07/Manual-de-Normas-y-Procedimientos-DPD.pdf>. [Consulta: 20 de octubre de 2018].

21. ZÚÑIGA, Rodrigo. *Política de seguridad sobre clasificación y manejo de la información*. [en línea]. <http://www.chileindica.cl/instructivos/Politica-Seguridad-Clasificacion-y-Manejo-de-Informacion-v4.pdf>. [Consulta: 12 de diciembre de 2018].