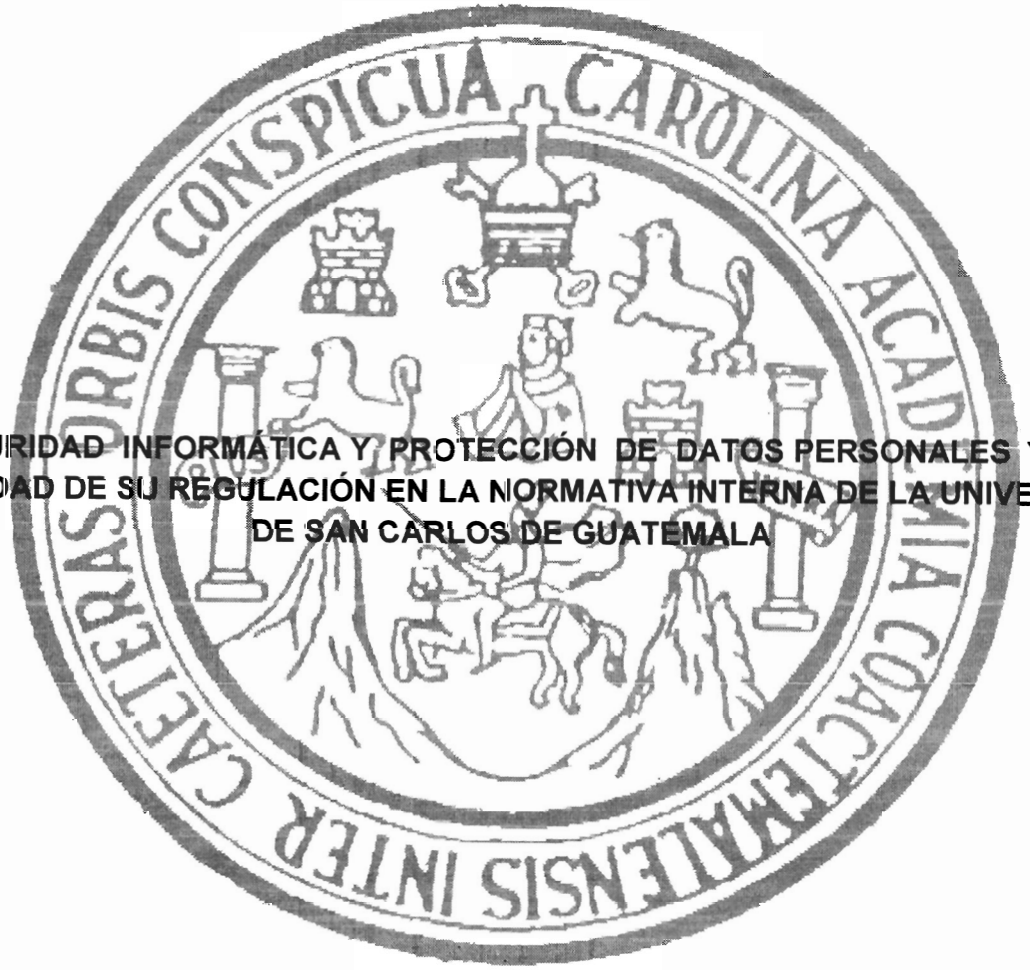
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES



SEGURIDAD INFORMÁTICA Y PROTECCIÓN DE DATOS PERSONALES Y LA NECESIDAD DE SU REGULACIÓN EN LA NORMATIVA INTERNA DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

NINETH YARIBEL JEREZ MOLINA

GUATEMALA, JUNIO DE 2017

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

SEGURIDAD INFORMÁTICA Y PROTECCIÓN DE DATOS PERSONALES Y LA NECESIDAD DE SU REGULACIÓN EN LA NORMATIVA INTERNA DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

TESIS

Presentada a la Honorable Junta Directiva
de la

Facultad de Ciencias Jurídicas y Sociales
de la

Universidad de San Carlos de Guatemala

Por

NINETH YARIBEL JEREZ MOLINA

Previo a conferírsele el grado académico de

LICENCIADA EN CIENCIAS JURÍDICA Y SOCIALES

Y los títulos profesionales de

ABOGADA Y NOTARIA

Guatemala, junio 2017

HONORABLE JUNTA DIRECTIVA

DE LA

FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

DE LA

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

DECANO:	Lic. Gustavo Bonilla
VOCAL I:	Lic. Luis Rodolfo Polanco Gil
VOCAL II:	Licda. Rosario Gil Pérez
VOCAL III:	Lic. Juan José Bolaños Mejía
VOCAL IV:	Br. Jhonathan Josué Mayorga Urrutia
VOCAL V:	Br. Freddy Noé Orellana Orellana
SECRETARIO:	Lic. Fernando Antonio Chacón Urizar

TRIBUNAL QUE PRACTICÓ
EL EXAMEN TÉCNICO PROFESIONAL

Primera Fase:

Presidente:	Lic. Ervin Enrique Dionisio Navarro
Vocal:	Licda. Ileana Noemí Villatoro Fernández
secretaria:	Licda. Roxana Elizabeth Alarcón Monzón

Segunda Fase:

Presidenta:	Licda. Adela Lorena Pineda Herrera
Vocal:	Licda. Ninfa Nidia Cruz Oliva
Secretaria:	Licda. Ileana Noemí Villatoro Fernández

RAZÓN: "Únicamente el autor es responsable de las doctrinas sustentadas y contenido de la tesis". (Artículo 43 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público).

USAC
TRICENTENARIA
Universidad de San Carlos de Guatemala

Facultad de Ciencias Jurídicas y Sociales, Unidad de Asesoría de Tesis. Ciudad de Guatemala, 13 de mayo de 2015.

Atentamente pase al (a) Profesional, **MIRNA ELIZABETH CABALLEROS SALGUERO DE CABRERA**, para que proceda a asesorar el trabajo de tesis del (a) estudiante **NINETH YARIBEL JEREZ MOLINA**, con carné **201014079**, intitulado **LA INFORMÁTICA Y LA NECESIDAD DE SU REGULACIÓN DENTRO DE LA NORMATIVA INTERNA DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA.**

Hago de su conocimiento que está facultado (a) para recomendar al (a) estudiante, la modificación del bosquejo preliminar de temas, las fuentes de consulta originalmente contempladas; así como, el título de tesis propuesto.

El dictamen correspondiente se debe emitir en un plazo no mayor de 90 días continuos a partir de concluida la investigación, en este debe hacer constar su opinión respecto del contenido científico y técnico de la tesis, la metodología y técnicas de investigación utilizadas, la redacción, los cuadros estadísticos si fueren necesarios, la contribución científica de la misma, la conclusión discursiva, y la bibliografía utilizada, si aprueba o desaprueba el trabajo de investigación. Expresamente declarará que no es pariente del (a) estudiante dentro de los grados de ley y otras consideraciones que estime pertinentes.

Adjunto encontrará el plan de tesis respectivo.

FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
SECRETARIA
GUATEMALA, C. A.

DR. BONERGE AMILCAR MEJIA ORELLANA
Jefe(a) de la Unidad de Asesoría de Tesis

Fecha de recepción 20 / 01 / 2017. f)

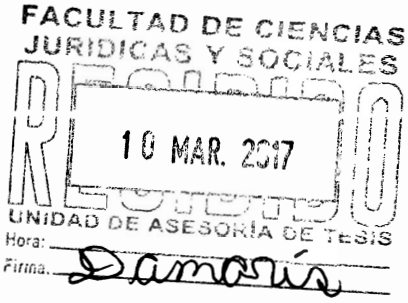
Asesor(a)
(Firma y Sello)

LICDA. MIRNA ELIZABETH CABALLEROS SALGUERO
ABOGADA Y NOTARIA

Licda. Mirna Elizabeth Caballeros Salguero de Cabrera
Abogada y Notaria

Guatemala, 06 de marzo de 2017

Lic.
Roberto Freddy Orellana Martínez
Jefe de la Unidad de Asesoría de Tesis
Facultad de Ciencias Jurídicas y Sociales
Universidad de San Carlos de Guatemala
Su Despacho.



Respetable Lic. Orellana:

De acuerdo al nombramiento de fecha 13 de mayo de 2015, que me fue notificado con fecha 20 de enero de 2017, he procedido a asesorar el trabajo de tesis intitulado: **"LA INFORMÁTICA Y LA NECESIDAD DE SU REGULACIÓN DENTRO DE LA NORMATIVA INTERNA DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA"** de la bachiller **NINETH YARIBEL JEREZ MOLINA,** motivo por el cual *emito el siguiente dictamen:*

a) Respecto al contenido científico y técnico del trabajo de tesis, puede verificarse que se emplearon los métodos analítico, analógico e inductivo y técnicas bibliográficas, documentales, los cuales se ven reflejados a lo largo de la investigación en cuanto al desarrollo de cada tema de forma exhaustiva e interrelacionada. La elaboración de la misma fue realizada con base en un escogido y satisfactorio repertorio bibliográfico para el desarrollo de cada capítulo, incluyéndose bibliografía electrónica y respetándose los derechos de autor.

b) En cuanto a su redacción, a lo largo de la investigación puede apreciarse el uso correcto del lenguaje técnico y jurídico, lo cual permite que el contenido sea comprensible para el lector. Asimismo, los capítulos han sido desarrollados sistemáticamente, fundamentándose cada tema en el anterior, a fin de que el lector pueda llevar una secuencia tanto de los aspectos teóricos como de los fácticos y que en cada capítulo pueda ir comprobando una parte de la hipótesis, llegando a comprobarse su totalidad en los últimos capítulos.

De esa manera, la investigación comienza exponiendo la informática y la tecnología y la relación de éstas con el Derecho; posteriormente se analiza la seguridad informática y los datos personales; luego de ello se expone la comparación de la normativa universitaria de universidades de otros países, todo esto explicándose a la vez con

términos técnicos y de forma accesible para el lector. Por último, se interrelacionan todos los temas anteriores en el análisis de la normativa interna de la Universidad de San Carlos de Guatemala concluyendo en la exposición de un Reglamento que propone posibles soluciones para para las deficiencias en relación al tema expuesto, siendo ello el aporte científico del trabajo de tesis.

c) El tema central de la investigación, la seguridad informática y la protección de los datos personales, fue desarrollado sustanciosa, novedosa y satisfactoriamente, habiéndose explicado el tema en su totalidad, citando casos concretos y actuales. Asimismo, se realizó un esbozo completo de la normativa internacional y nacional, lo cual permite conocer y entender la realidad jurídica de esta temática.

d) La conclusión discursiva permite percibir un panorama completo del desarrollo de la investigación y la solución propuesta.

e) He asesorado, revisado y corregido cada una de las partes de la presente investigación, verificando que las correcciones señaladas hayan sido realizadas.

f) Con base en el desarrollo y conclusión de la investigación y de acuerdo a las facultades que como asesora de tesis me confiere el Artículo 26 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público a través del nombramiento realizado, he sugerido a la estudiante modificar el tema propuesto, quedando este de la siguiente manera: **"SEGURIDAD INFORMÁTICA Y PROTECCIÓN DE DATOS PERSONALES Y LA NECESIDAD DE SU REGULACIÓN EN LA NORMATIVA INTERNA DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA".**

g) Declaro que no soy pariente de la estudiante dentro de los grados de ley.

Por lo anterior, y habiendo cumplido con los requisitos establecidos en el Artículo 31 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público, procedo a emitir **DICTAMEN FAVORABLE** a la bachiller **NINETH YARIBEL JEREZ MOLINA**, para que prosiga con los trámites necesarios para su graduación.

Atentamente,

Licda. Mirna Elizabeth Caballeros Salguero de Cabrera
Colegiada No. 5,168

LICDA. MIRNA ELIZABETH
CABALLEROS SALGUERO
ABOGADA Y NOTARIA

DECANATO DE LA FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES. Guatemala, 20 de abril de 2017.

Con vista en los dictámenes que anteceden, se autoriza la impresión del trabajo de tesis de la estudiante NINETH YARIBEL JEREZ MOLINA, titulado SEGURIDAD INFORMÁTICA Y PROTECCIÓN DE DATOS PERSONALES Y LA NECESIDAD DE SU REGULACIÓN EN LA NORMATIVA INTERNA DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA. Artículos: 31, 33 y 34 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público.

RFOM/srrs.

FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
SECRETARIO
GUATEMALA, C. A.

FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANO
GUATEMALA, C. A.

DEDICATORIA

A DIOS: Por darme la sabiduría, inteligencia y fuerza necesaria para alcanzar cada meta propuesta y especialmente este logro.

A MIS PADRES: Rubery y Leticia Jeréz, por su amor y apoyo incondicional, por cada consejo y el esfuerzo conjunto que han hecho durante todo el trayecto de mis estudios el cual me ha impulsado y permitido alcanzar este logro y por enseñarme a no rendirme durante todo este trayecto.

A MIS HERMANOS: Jonathan, Arlene y David Jeréz por ser una parte de inspiración en mi vida y por el apoyo moral incondicional que me han brindado.

A MI ESPOSO: Pedro Jonathán Velásquez Caballeros, por ser parte importante y de inspiración en mi vida, por el ejemplo de esfuerzo que me has dado el cual ha sido parte del impulso para seguir adelante durante todo este trayecto y por tu amistad, amor y apoyo sinceros e incondicionales.

A MIS AMIGOS: Aquellos a quienes aprecio y quiero mucho y que han estado a mi lado por mucho tiempo, Norma Gramajo, Lisbeth Corzántes, Kevin Blanco y Claudia Gramajo, porque sus consejos y apoyo fueron de gran importancia para poder alcanzar este triunfo y por brindarme su amistad sincera. También a mis amigos de la Universidad que permitieron que este proceso de estudios fuera mejor, especialmente a Wendy Cajbón y Sara Conde.

A MIS FAMILIARES: Mis abuelos y tíos, por su apoyo durante todo este trayecto y en especial a Sofía y Antonio Jeréz y Elsa Contreras por siempre estar pendientes de mí y por cada uno de sus consejos. También a la familia Caballeros Salguero por haberme acogido dentro de su núcleo familiar y brindarme de su apoyo.

A: La Facultad de Ciencias Jurídicas y Sociales y cada uno de mis catedráticos, por ser el centro forjador de mis conocimientos e impulsarme siempre en la búsqueda de la excelencia.

A: La gloriosa y tricentenaria Universidad de San Carlos de Guatemala, Alma Mater, por abrirme sus puertas y permitirme obtener este grado académico y títulos profesionales y de donde me siento muy orgullosa de ser egresada.

PRESENTACIÓN

El presente estudio es de importancia tomando en cuenta que los avances tecnológicos son cada vez mayores y son de reciente inclusión dentro de la sociedad y sobre todo en el ámbito educativo, por lo que se hacen vulnerables cada vez más los datos de las personas y quedan en riesgo todos aquellos sistemas y medios informáticos.

Esta investigación es de tipo cualitativa y pertenece a la informática jurídica y al derecho informático. La investigación se desarrolló de enero a noviembre del año 2016 y de enero a febrero del año 2017 en el municipio de Guatemala, departamento de Guatemala. El objeto de la investigación es la necesidad implementar un reglamento dentro de la Universidad de San Carlos de Guatemala que permita proteger los datos personales y asimismo se dé énfasis a la seguridad informática.

El sujeto de la investigación está constituido por el derecho informático, la informática jurídica y la normativa interna universitaria, tanto de universidades extranjeras como aquellas que se encuentran en Guatemala, específicamente la Universidad de San Carlos.

Se considera que el presente estudio contiene aporte científico, pues el mismo puede ser consultado por estudiantes y profesionales del derecho, así como por personas particulares, por la importancia de su contenido tanto en el ámbito de la informática jurídica como en el derecho informático en tanto que se persigue la implementación de una normativa interna en la Universidad de San Carlos de Guatemala que regule la protección de los datos personales así como la fomentación de la seguridad informática.

HIPÓTESIS

La hipótesis planteada en el plan de investigación es la siguiente: A medida que la sociedad se va desarrollando conjuntamente se van generando nuevos medios informáticos, por lo que la falta de un reglamento que regule tanto los procedimientos como el uso y manejo de los medios y sistemas informáticos, genera la falta de seguridad y certeza de los actos académicos, administrativos y registrales que los alumnos, docentes y personal administrativo, como usuarios, realizan a través de los medios informáticos y por lo tanto, la base de datos se encuentra un riesgo a medida que se deja desprotegida.

Es necesario que los equipos de computación sean adecuados, así como que existan lineamientos que especifiquen el modo de empleo y manejo de cada uno de los medios informáticos porque de esa forma existirá un orden adecuado para que el manejo de la base de datos sea exacto y sin ningún riesgo de inseguridad para todo aquel usuario servidor.

Se considera indispensable la regulación de la informática dentro de la normativa interior universitaria, en el sentido de implementar un proyecto de creación de reglamento en el cual se estipulen tanto los lineamientos que deben seguir cada uno de los encargados del manejo de la base de datos como también el uso del equipo adecuado. Normativa dentro de la cual debe asegurarse la calidad de los medios y sistemas informátios, brindando seguridad y certeza a cada procedimiento, protegiendo la informacion y datos personales del usario servidor, mediante la supervision constante del equipo que almacene la base de datos, así como la actualizacion de programas que permitan el uso adecuado de los sistemas informáticos.

COMPROBACIÓN DE HIPÓTESIS

La hipótesis fue comprobada por la necesidad de seguridad informática y protección de los datos personales y la necesidad de su regulación en la normativa interna de la Universidad de San Carlos de Guatemala.

Lo anterior fue confirmado por la urgente importancia y necesidad de resguardar la información personal de todos los usuarios, estudiantes, docentes y personal administrativo, contando con una base de datos segura, eficiente y eficaz de acuerdo a las necesidades de la Universidad de San Carlos de Guatemala.

Dentro de la metodología utilizada para la comprobación de la hipótesis se encuentra el método científico, analítico, sintético, inductivo, deductivo y dialéctico. En cuanto a las técnicas de investigación utilizadas son las bibliográficas.

ÍNDICE

Pág.

CAPÍTULO III

CAPÍTULO IV

CAPÍTULO V

Pág.

INTRODUCCIÓN

El tema objeto de investigación se justifica porque la falta de regulación de los medios y sistemas informáticos es trascendental ya que sin los lineamientos necesarios se abre camino a la mala utilización de los mismos y dejará en estado vulnerable la base de datos debido a que la implementación y el uso de la tecnología permite que la transportación y la accesibilidad de la información sean mayores.

Los sectores vulnerables a todos los riegos provenientes de la falta de regulación de la informática en la Universidad de San Carlos de Guatemala son los estudiantes, personal docente y personal administrativo, así también los mismos serían beneficiados al momento de la resolución de dicha problemática, brindándoles seguridad en la protección de sus datos personales.

El objetivo general propuesto es: actualizar al sector universitario en el ámbito de la informática para generar la seguridad de la base de datos de los estudiantes, personal docente y personal administrativo. Este fue alcanzado por la importancia de actualizar la informática en la Universidad de San Carlos de Guatemala

La hipótesis planteada es: a medida que la sociedad se va desarrollando conjuntamente se van generando nuevos medios informáticos, por lo que la falta de un reglamento que regule tanto los procedimientos como el uso y manejo de los medios y sistemas informáticos genera la falta de seguridad y certeza de los actos académicos, administrativos y registrales que los alumnos, docentes y personal administrativo, como usuarios, realizan a través de los medios informáticos y por lo tanto, la base de datos se encuentra un riesgo a medida que se deja desprotegida.

La hipótesis fue comprobada por la necesidad de seguridad informática y protección de los datos personales y la necesidad de su regulación en la normativa interna de la Universidad de San Carlos de Guatemala.

La investigación se estructuró en los capítulos siguientes: en el primer capítulo, Informática y tecnología; en el segundo capítulo, seguridad informática y datos personales; en el tercer capítulo, mecanismos normativos para la fomentación de la seguridad informática y protección de los datos personales en la universidades a nivel internacional; en el cuarto capítulo, seguridad informática y protección de datos personales en la normativa interna de la Universidad de San Carlos de Guatemala; en el quinto capítulo, Proyecto de Reglamento de seguridad informática y protección de datos personales de la Universidad de San Carlos de Guatemala.

Dentro de la metodología utilizada se encuentra el método científico, analítico, sintético, inductivo, deductivo y dialéctico. En cuanto a las técnicas de investigación utilizadas son: Entrevistas y bibliográficas.

Se concluye el presente trabajo con la proposición al Consejo Superior Universitario de la Universidad de San Carlos de Guatemala, como ente superior de la universidad, que por los medios necesarios se inicien las diligencias correspondientes para la implementación del reglamento correspondiente a la protección de los datos personales y la fomentación de la seguridad informática a nivel universitario.

CAPÍTULO I

1. Informática y tecnología

A medida que el hombre ha evolucionado la sociedad a su vez cambia, lo que permite el desarrollo y avances en cada aspecto social. El mundo contemporáneo gira sobre la circulación y el intercambio de informaciones, lo que ha dado lugar a nuevos inventos. Tales inventos han generado la necesidad de creación de una ciencia nueva que estudie y regule dichos aspectos, los cuales han permitido a las personas que el ciclo de comunicación no se vea limitado por factores como el tiempo, la distancia o costos.

En la actualidad se ha implementado el uso de la informática tanto en el ámbito laboral, en el ámbito social, así como en el ámbito estudiantil. El término informático también es conocido comúnmente como computación, y esto debido a que el uso de la computadora es la forma más común de acceder a la informática.

Para comprender este tema se hace necesario definir algunos términos que tienen relación con la informática y para tal efecto se definen los siguientes.

1.1. Informática

"El término informática se origina del idioma francés *Informatique,* (atribuida su creación al ingeniero francés Philippe Dreyfus) término formado por dos elementos que son *information y automatique* (información automática). Pronto adaptaciones locales del

término aparecieron en italiano, español, rumano, portugués y holandés, entre otras lenguas, refiriéndose a la aplicación de las computadoras para almacenar y procesar la información."[1]

De conformidad con el Diccionario de la Real Academia Española se contemplan diferentes definiciones para el término informática siendo el siguiente el que corresponde al presente trabajo: "Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de computadoras."

"La informática es una teoría de la información que la aborda desde un punto de vista racional y automático, a fin de transformar la información en símbolos y, mediante una serie de mecanismos electrónicos para aplicarla a la mayor cantidad posible de actividades."[2]

En virtud de las anteriores definiciones la informática puede considerase como la teoría que envuelve un conjunto de conocimientos y técnicas que permiten la automatización de la información a través de actividades realizadas por medio de un computador.

[1]Carvajal Pimentel, Milena. http://milenacarvajalpimentel.blogspot.com/2013/05/origen-de-la-palabra informatica-html. (Consultado: 2 de junio de 2016)

[2] Solano B., Orlando. **Manual de informática jurídica.** Pág. 31.

1.1.1. Medios informáticos

Los medios informáticos son el resultado de los avances en la ciencia y la tecnología, los cuales han permitido desarrollar numerosos recursos que representan las nuevas tecnologías de información y comunicación. Estos medios permiten integrar el sonido, códigos verbales y la utilización de imágenes fijas o en movimiento; dentro de esta clasificación encontramos al computador u ordenador como principal representación de dicha clasificación.

A finales del siglo XX se introdujo la computadora a las diferentes áreas de desenvolvimiento social, tales como los centros educativos y de trabajo, entre algunas de las razones que justifican su incorporación son: la posibilidad de que el individuo entre en contacto con personas de otras culturas y países, la democratización de la información y la preparación de los estudiantes y trabajadores ante los avances técnicos que le permitan desarrollarse para el futuro.

Es oportuno indicar que entre los medios informáticos se pueden encontrar recursos a nivel de hardware (parte física del computador, parte tangible) y software (conjunto de programas que permiten realizar operaciones en un sistema de información, es la parte intangible del computador) que permiten integrar el texto, el sonido, la imagen, la animación, el video y la interactividad; esto también es conocido como multimedia.

Considerando lo anterior, los medios informáticos son aquellos que han resultado de los avances que ha tenido la ciencia y que permiten desarrollar las diferentes formas de

comunicación y de utilización de información los cuales se han incorporado y representado a través de un equipo informático.

1.1.2. Sistemas informáticos

Para poder definir lo que es un sistema informático es preciso definir inicialmente lo que es un sistema. Según el Diccionario de la Real Academia Española un sistema es "el Conjunto estructurado de unidades relacionadas entre sí que se definen por oposición".

Partiendo de lo que es un sistema se puede explicar que un sistema informático es, un sistema de información cuya base fundamental es el empleo de equipos de cómputo y además el uso de un conjunto de funciones que se interrelacionan entre sí, o sea que el sistema informático incluye tanto los elementos de hardware como del software y entre todos se da vida a el sistema que puede ser utilizado de diversas formas por los usuarios.

"Un sistema informático (SI) es un sistema que permite almacenar y procesar información; es el conjunto de partes interrelacionadas: hardware, software y personal informático. El hardware incluye computadoras o cualquier tipo de dispositivo electrónico, que consisten en procesadores, memoria, sistemas de almacenamiento externo, etc. El software incluye al sistema operativo, firmware y aplicaciones, siendo especialmente importante los sistemas de gestión de bases de datos. Por último, el

soporte humano incluye al personal técnico que crean y mantienen el sistema (analistas, programadores, operarios, etc.) y a los usuarios que lo utilizan."[3]

Entre los elementos que se pueden encontrar en un sistema informático están las personas, las computadoras, equipos de apoyo, equipos de procesamiento de información, programas de cómputo, sistemas operativos, manuales técnicos, bases de datos, discos duros, impresoras, entre otros.

1.2. Tecnología

"La tecnología es una palabra de origen griego, τεχνολογία, formada por *téchnē* (τέχνη, *arte, técnica u oficio*, que puede ser traducido como *destreza*) y *logía* (λογία, el estudio de algo)."[4]

Se define a la tecnología como el conjunto de conocimientos técnicos, instrumentos, recursos técnicos y procedimientos, ordenados científicamente, los cuales son empleados en un determinado campo o sector para permitir diseñar, crear bienes o servicios que faciliten la adaptación al medio ambiente y satisfacer tanto las necesidades esenciales como los deseos de la humanidad.

---

[3] https://es.wikipedia.org/wiki/Sistema_inform%C3%A1tico. (Consultado: 4 de junio de 2016)
[4] https://es.wikipedia.org/wiki/Tecnolog%C3%ADa. (Consultado: 4 de junio de 2016)

1.2.1. Recursos tecnológicos

Un recurso es aquel medio por el cual se satisface una necesidad o bien se consigue aquello que se procura. La tecnología por su parte, como anteriormente se ha definido, se refiere a las técnicas y teorías que hacen posible el aprovechamiento práctico de un conocimiento científico.

Por lo tanto, los recursos tecnológicos se pueden definir como aquellos medios que se valen de la tecnología para poder alcanzar determinado fin o cumplir con un propósito.

En la actualidad los recursos tecnológicos son una parte imprescindible de las esferas de la sociedad como empresas, centros educativos o de los hogares. Esto se debe a que la tecnología se ha convertido en un aliado clave para realizar todo tipo de tareas.

De las distintas formas de aplicación que en la actualidad tienen los recursos tecnológicos destaca el uso que se le dan dentro del ámbito educativo. De ahí que existan Centros de la Tecnología de la Información y la Comunicación. Asimismo son varias las ventajas que esos recursos tecnológicos ofrecen también dentro del ámbito de la docencia.

La única desventaja que podría atribuírsele a los recursos tecnológicos al aplicarlos y utilizarlos, en este caso, a niveles universitarios es que en ocasiones presentan fallos y errores.

En el ámbito laboral se puede tomar en cuenta que se ha implementado el uso de computadoras modernas, acceso a internet, redes informáticas internas, teléfonos inteligentes y equipos multifunción que les permitirán estar en condiciones de competir con éxito en el mercado, más allá de las características propias de sus productos o servicios.

1.3. Derecho e informática

Como se hizo mención al inicio del presente trabajo, no se puede dejar por un lado la relación existente entre la informática y el derecho, ya que el fenómeno de la informática así como el desarrollo de programas, la manera de procesar la información y todo aquel perfeccionamiento que se tenga de las tecnologías debe ser tutelado por el Estado y esto es a través del derecho ya que por un lado contempla la protección a través de la propiedad industrial e intelectual, así como de algunos delitos informáticos regulados en la ley penal guatemalteca, sin dejar de lado la normativa reglamentaria.

1.3.1. Ciencia del derecho

Desde el principio la humanidad ha perseguido ambiciosamente el conocimiento y ha intentado definirlo a través de conceptos claros y bien diferenciables entre sí. Los estudiosos de la antigua Grecia decidieron establecer un concepto que permitiera contener los conocimientos, a lo que llamaron ciencia. Para definir y entender correctamente al derecho como ciencia, es necesario definir por separado cada término.

"La ciencia (del latín scientĭa 'conocimiento') es un conjunto ordenado de conocimientos estructurados sistemáticamente."[5]

"La palabra derecho proviene del término latino *directum*, que significa lo que está conforme a la regla. El derecho se inspira en postulados de justicia y constituye el orden normativo e institucional que regula la conducta humana en sociedad. La base del derecho son las relaciones sociales, las cuales determinan su contenido y carácter. Dicho de otra forma, el derecho es un conjunto de normas que permiten resolver los conflictos en el seno de una sociedad."[6]

En virtud de las anteriores definiciones se define a la ciencia del derecho como el conjunto ordenado de conocimientos del orden normativo, los cuales tienen por objeto regular las relaciones y conducta humana en sociedad, así como resolver los conflictos que surjan en consecuencia de dichas relaciones y conductas.

1.3.2. Relación entre el derecho y la informática

La ciencia jurídica tradicional se ha anclado al pasado, lo que la convierte en una disciplina estática tanto en su funcionalidad como en su estructura y resultados. En la época contemporánea en que se han marcado grandes cambios y transformaciones, necesariamente se debe adecuar el derecho a las nuevas condiciones de la sociedad y la tecnología.

---

[5] https://es.wikipedia.org/wiki/Ciencia. (Consultado: 6 de junio de 2016)
[6] http://definicion.de/derecho/. (Consultado: 6 de junio de 2016)

El auge de la informática, el incremento de la tecnología y la llegada del computador ha tenido distintos puntos de vista en la cual es o no aceptada dentro del ámbito del derecho, lo cual ha generado posiciones extremistas en las que se establece que éstas solo generarán un avasallamiento de la libertad, o por el contrario está la postura que la ve como un medio más avanzado para que el ciudadano disfrute de mayor libertad y bienestar.

Las relaciones que hoy existen entre el derecho y la informática han producido una importante transformación en el orden jurídico tradicional, por lo que se ha obligado a los juristas actuales a elaborar normas y principios que respondan a las necesidades existentes.

Es por ello que la relación entre ambas ciencias comienza desde el momento en que se utilizan alguna o algunas de las ventajas que proporcionan las aplicaciones de la informática en el procesamiento de la información que produce el derecho. En este sentido se estaría hablando de la informática jurídica, aplicar conocimientos de la informática al derecho. Sin embargo, con el auge y desarrollo de la informática surgen bienes jurídicos que no existían en la sociedad, además de una nueva forma de comunicación y un nuevo espacio de interactividad de las personas conocido como el ciberespacio, por lo que se hace necesario estudiar los efectos que tienen esos fenómenos, así como su regulación para una correcta convivencia social. En este caso se estaría hablando del derecho informático.

El auge de las comunicaciones entre ordenadores, cuyo máximo exponente es la macrored mundial internet, ha creado un nuevo espacio virtual poblado por millones de datos, en el que se puede navegar infinitamente en busca de información. Se trata, en una contracción de cibernética y espacio, del ciberespacio. Por lo que es necesario ahondar en lo que es el tema del derecho informático y la informática jurídica.

1.3.3 Derecho informático

Debido a que la sociedad se encuentra en constante evolución y el derecho es la ciencia encargada de regular la conducta dentro de ella, se hace necesaria la investigación, estudio y regulación de los principios e instituciones que permitan adecuar las acciones que se deriven de esos cambios que son consecuencia de la implementación de la informática.

El uso de las herramientas informáticas en el ámbito del derecho es similar a la aplicación de la informática a otras ciencias y disciplinas, pero en particular en el campo del derecho. Lo que se busca es encontrar una herramienta que permita incrementar la capacidad de análisis y de procesamiento de la información jurídica, así como el perfeccionamiento de la actividad legislativa y judicial. Es decir, que se busca facilitar los procesos de tratamiento de la información jurídica.

"El derecho informático tiene pues como objeto de estudio la informática en tanto que esta busque clarificar las relaciones entre las personas, las obligaciones que se pacten

entre ellas, las relaciones de tipo contractual que funden, etc. Es decir, que tengan como objeto de estudio lo jurídico pero tratado electrónicamente."[7]

Para tener un concepto más completo de lo que es el Derecho Informático es necesario conocer algunas de las definiciones que se le dan a ésta:

"El derecho de la Informática es el conjunto de normas jurídicas que regulan la creación, desarrollo, uso, aplicación de la informática o los problemas que se deriven de la misma en las que existen algún bien que es o deba ser tutelado jurídicamente por las propias normas."[8]

De una forma general, el profesor Julio Téllez, citado por Barrios Osorio, define al derecho de la informática como el "conjunto de leyes, normas, y principios aplicables a los hechos y actos derivados de la informática."[9]

En relación a las definiciones anteriores se infiere que el derecho informático es aquél conjunto de normas, principios, instituciones y doctrinas que se encarga del estudio y regulación de los hechos, actos y bienes jurídicos que surgen de la aplicación de la informática, así mismo estudia y regula la responsabilidad de las personas derivada del uso de la tecnología.

---

[7] Solano, **Op. Cit.** Pág. 188.

[8] https://es.wikipedia.org/wiki/Derecho_inform%C3%A1tico. (Consultado: 12 de junio de 2016)

[9] Barrios Osorio, Omar Ricardo. **Derecho e informática nociones generales.** Pág. 111.

Ahondando más en lo que es la materia del derecho informático, es oportuno resaltar alguno de los temas o contenido del que se encarga éste los cuales, según Rodolfo Herrera Bravo, citado por Barrios Osorio, enumera indicándolos como una propuesta meramente pedagógica:

1. "El valor probatorio de los soportes modernos de información, provocado por la dificultad en la aceptación y apreciación de los elementos de prueba derivados de estos soportes entre los órganos jurisdiccionales.
2. La protección de datos personales, ante el manejo inapropiado de informaciones nominativas que atenta contra derechos fundamentales de las personas.
3. Los delitos informáticos, es decir, la comisión de verdaderos actos ilícitos en los que se tenga a los computadores como instrumentos o fines.
4. El flujo de datos transfronterizos, con el favorecimiento o restricción en la circulación de datos a través de las fronteras nacionales.
5. La protección de los programas computacionales, como respuesta a los problemas provocados por la piratería de software que atenta contra la propiedad intelectual.
6. Los contratos informáticos, en función de esta categoría contractual *sui generis* con evidentes repercusiones fundamentalmente económicas.
7. La regulación de los bienes informacionales, en función del innegable carácter económico de la información como producto informático.
8. La ergonomía informática, como aquellos problemas laborales suscitados por la informatización de actividades."[10]

[10] Barrios Osorio, Omar Ricardo. **Derecho e informática. Aspectos fundamentales.** Pág. 111 y112.

Aunque muy acertada y correcta la enumeración anterior hecha por Rodolfo Herrera Bravo, no cubre ni describe en su totalidad el derecho informático ya que el avance de la tecnología incrementa cada vez más e incorpora más temas o problemas a solucionar, no obstante, los anteriormente descritos son los comunes actualmente.

1.3.4. Informática jurídica

El desarrollo de los sistemas de información ha permitido satisfacer necesidades así como liberarse de rutinas pesadas o tediosas, principalmente en los aspectos de información, base de datos y la informatización.

Con la aplicación de la informática en el campo del derecho en los aspectos anteriores se puede y podrían realizar algunas tareas como registro de expedientes, seguimiento de la prueba, agenda de audiencias, estadísticas, archivo de jurisprudencias, todo esto desde el aspecto de la informatización y aplicada desde el aspecto de la base de datos en materia jurídica se logran y lograrían inmensos beneficios como encontrar fácilmente leyes, reglamentos, fallos jurisprudenciales, doctrina, entre otros.

Con lo anteriormente señalado se determina la importancia de estimular las relaciones del derecho con la ciencia y la tecnología y no sólo permitir que éste dé pasos vacilantes detrás de los fenómenos que surjan de los avances científicos y tecnológicos.

"Durante el desarrollo de la informática se realizaron estudios para utilizar sus aplicaciones en todas las ciencias; cuando se utilizan los sistemas informáticos en el campo del derecho, surge lo que conocemos como la informática jurídica."[11]

"Se define a la informática jurídica como la técnica que tiene por finalidad almacenar, ordenar, procesar y entregar según criterio lógico y científico, todos los datos jurídicos necesarios para documentar o proponer la solución al problema de que se trate, mediante el estudio del tratamiento automatizado de las fuentes de conocimiento jurídico y de los medios instrumentales con que se gestiona el derecho. Es una ciencia que estudia la utilización de aparatos o elementos físicos electrónicos, como la computadora, en el derecho; es decir, la ayuda que este uso presta al desarrollo y aplicación del derecho. En otras palabras, es ver el aspecto instrumental dado a raíz de la informática en el derecho."[12]

Por lo que se entiende por informática jurídica el uso de los distintos conceptos, categorías, métodos, herramientas, recursos, procedimientos y técnicas propios de la informática aplicados en el ámbito, materia, contenido o fines del derecho.

[11] Barrios, **Op. Cit.** Pág. 95.
[12] http://estudianteigv.galeon.com/. (Consultado: 13 de junio de 2016.)

CAPÍTULO II

2. Seguridad informática y datos personales

Varias de las actividades que se realizan cotidianamente dependen, ya sea en menor o mayor medida, de los sistemas y redes informáticas. El enorme crecimiento de la internet, así como los servicios telemáticos (comercio electrónico, correo electrónico, videoconferencias, administración electrónica, etc.) han favorecido a extender aún más el uso de la informática y de las redes de ordenadores, llegando al punto que en la actualidad se han convertido en un elemento cotidiano abarcando el ámbito profesional, educativo y laboral.

Por otra parte, los servicios esenciales como lo es la propia administración pública están soportados por sistemas y redes informáticas, en el punto que se ha reducido el uso de papeles y procesos manuales debido a la creciente complejidad de las relaciones con el entorno y la elevada carga de trabajo que propician el soporte automatizado e informatizado de muchos de sus procesos.

Atendiendo a todo lo anterior y debido a que en la actualidad las actividades diarias tanto de la administración pública como el de muchas instituciones de ámbito laboral, educativo y otros organismos, así como las de cada persona en su vida cotidiana, se observa que es necesario el correcto funcionamiento de los sistemas y redes informáticas que las soportan y especialmente atender lo relacionado a la seguridad de los mismos.

Con base a lo antes expuesto y también de la proliferación de virus y códigos malignos y su rápida distribución a través de redes como lo es la internet y como los muchos ataques he incidentes de seguridad que se producen día con día, debe concedérsele importancia a todos los aspectos relacionados con la seguridad informática y la protección de los datos personales.

2.1. Seguridad informática

"Se puede definir a la seguridad informática como cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema."[13]

Así también se encuentra otra definición propuesta por el INFOSEC Glossary 2000: "Seguridad informática son las medidas y controles que aseguran la confidencialidad, integridad y disponibilidad de los activos de los sistemas de información, incluyendo el hardware, software, firmware y aquella información que procesan, almacenan y comunican".

[13] Gómez Vieites, Álvaro. **Enciclopedia de la seguridad informática.** Pág. 4.

En virtud de las anteriores definiciones se define la seguridad informática como un conjunto de mecanismos enfocados en la protección de datos e información contenidos en un sistema informático.

2.1.1. Consecuencias de la falta de seguridad

En la actualidad el desarrollo de varias de las actividades de instituciones y organizaciones dependen de los datos e información que se encuentran registrados en sus sistemas informáticos para poder facilitar el procesamiento, almacenamiento y distribución de los mismos.

Por lo anterior, es indispensable valorar y proteger dicha información, así es como de vital importancia conocer cuál es el impacto de los incidentes de seguridad en materia informática.

Sin embargo, si se descuida el tema de la seguridad informática dentro de una institución, cualquiera que sea su denominación, puede causar consecuencias e importantes perjuicios, entre los cuales se puede mencionar: inversión en reparaciones de equipo y redes, pérdidas por indisponibilidad de servicios informáticos, filtración de datos personales, robo de información confidencial, retrasos en procesos de producción, entre otros, sin dejar de lado aquellos que pueden llegar a ser un delito.

2.1.2. Gestión de seguridad de la información

Para poder gestionar la seguridad de la información es necesario contemplar una serie de procedimientos y tareas los cuales permitan garantizar los niveles de seguridad exigibles en una organización, tomando en cuenta que los riesgos no se pueden eliminar por completo, pero sí se pueden gestionar.

Para efecto de lo descrito en el párrafo anterior se define el Sistema de Gestión de la Seguridad de la Información (SGSI) como "aquella parte del sistema general de gestión que comprende la política, la estructura organizativa, los procedimientos, los procesos y los recursos necesarios implantar la gestión de la seguridad de la información en una organización."[14]

Con base a la definición anterior es necesario establecer lo que son las políticas de gestión para la seguridad de la información, por lo cual se entiende como el conjunto de procedimientos, buenas prácticas y normas reguladoras que determinan la manera en que todos los recursos son gestionados, distribuidos y protegidos dentro de una organización.

Por lo antes manifestado se hace necesario, durante todo el proceso, contemplar una guía que tome en cuenta varios aspectos entre los cuales, en opinión propia, se destacan los siguientes:

---

[14] **Ibíd.** Pág. 18.

- Aspectos tecnológicos: configuración y actualización de soluciones hardware y software, criptografía, estandarización de productos.
- Aspectos de organización: procedimientos, normas y políticas, planes de contingencia, relaciones con terceros (clientes, proveedores, etc.).
- Factor humano: control y supervisión, formación, sensibilización, obligaciones, responsabilidad del personal, personal (Directores, programadores, administradores, usuarios, etc.)
- Marco legal: adaptación y cumplimiento de la legislación vigente

Además de los aspectos anteriores es de suma importancia conseguir el soporte adecuado brindado por parte de la dirección de la organización o institución, la cual debe proporcionar recursos técnicos y humanos necesarios para definir y establecer las políticas y procedimientos de seguridad.

Existen varias etapas en la gestión de la seguridad de la información en una organización o institución entre las cuales se pueden encontrar:

1. **Implantación de medidas básicas de seguridad por sentido común**.

Puede decirse que en una primera etapa la institución u organización se preocupa por implementar medidas de seguridad aplicadas por sentido común, aplicando únicamente medidas de seguridad mínimas siendo éstas insuficientes para garantizar una adecuada gestión de los riesgos.

2. Adaptación a los requisitos del marco legal.

En esta etapa se toma conciencia de la importancia y la necesidad de cumplir con las exigencias de la legislación vigente, como ejemplo cabe mencionar la protección de los datos personales, delitos informáticos protección de la propiedad intelectual, entre otros.

3. Gestión integral de la seguridad de la información.

Como una tercera etapa, la organización o institución se preocupa de gestionar con un planteamiento global la seguridad de la información, en la cual ya se establecen una serie de políticas de seguridad y se implementan procedimientos y planes de seguridad, así como el análisis y gestión de riesgos y se establece un plan de contingencia como respuesta a riesgos o incidentes.

4. Certificación de la gestión de la seguridad de la información.

Como última etapa se pretende llevar a cabo una certificación de la gestión de la seguridad de la información y con ello obtener el reconocimiento de las prácticas instituidas y acreditarlas frente a terceros (administración pública, clientes, y otras instituciones)."[15]

[15] **Ibíd.** Pág. 47.

En la mayoría de los países todavía no existe una legislación específica que obligue a las organizaciones públicas y privadas a implementar medidas para gestionar la seguridad de sus sistemas informáticos, por lo que es de suma importancia empezar a tomar en cuenta cada uno de los aspectos anteriores e implementar una gestión de seguridad.

2.1.3. Importancia del factor humano en la seguridad

Como anteriormente se menciona, la implementación de medidas de seguridad informática exige contemplar ciertos aspectos tanto técnicos como organizativos y legales, es entendido que en diversas ocasiones no se presta atención suficiente al factor humano, el cual es muy importante.

Dentro de la seguridad informática podría decirse que las personas representan el "eslabón más débil", ya que a diferencia de un ordenador, las personas pueden no seguir instrucciones tal y como fueron establecidas. Además de que pueden realizar acciones que provoquen un agujero de seguridad en la red de una organización o institución como la revelación de información a terceros o bien instalar un software malicioso (por ejemplo, un spyware).

Es fundamental contemplar el papel que desempeñan las personas y su relación con los sistemas y redes informáticas en la institución u organización, por lo que resulta en definitiva y como principio básico a tener en cuenta, desde el punto de la seguridad informática, que todas las soluciones tecnológicas (antivirus, cortafuegos, sistemas de

detección de intrusiones, etc...) implementadas pueden resultar inútiles ante el desconocimiento o desinterés del personal o empleados desleales, que con mala intención provoquen algún daño.

Los principales expertos en materia de seguridad informática han alertado en estos últimos años sobre considerar el factor humano como uno de los más importantes y determinantes al momento de implementar un buen sistema de seguridad informática. Así en palabras de Kevin Mitnick, uno de los *hackers* más famosos de la historia, "usted puede tener la mejor tecnología, *firewalls*, sistemas de detección de ataques, dispositivos biométricos... Lo único que se necesita es una llamada a un empleado desprevenido y acceden al sistema sin más. Tienen todo en sus manos".[16]

Todo lo antes expuesto hace evidente que es importante atender el elemento humano en el tema de la seguridad informática, en la cual se deben establecer funciones y responsabilidades específicas de empleados y directivos, así también implementar el control, supervisión y capacitación de los usuarios y contratar personal profesional capacitado en materia informática para la implantación de sistemas de seguridad informática.

[16] **Ibíd.** Pág. 78.

2.1.4. Vulnerabilidad de los sistemas informáticos

Existen diversas causas que generan vulnerabilidad en los sistemas informáticos, las cuales se deben tomar en cuenta para evitar incidentes o causar riesgos en el sistema de seguridad informático. Entre las más comunes se encuentran:

a. Debilidad en el diseño de los protocolos utilizados en las redes.

Algunos de los protocolos utilizados para ofrecer distintos servicios como Internet fueron diseñados sin contemplar la seguridad o sin prever cómo reaccionar frente a situaciones anómalas, considerando que éstas únicamente iban a ser utilizadas en redes fiables y con usuarios de confianza.

b. Errores de programación.

Una causa de vulnerabilidad de los sistemas informáticos es que se encuentran fallos en su diseño y/o en la codificación de los programas. Así otra causa frecuente de vulnerabilidad en aplicaciones informáticas puede darse por un comportamiento incorrecto frente a entradas que no son válidas y pueden provocar situaciones indeseadas como por ejemplo un desbordamiento de una zona de memoria (buffer).

c. Políticas de seguridad deficientes o inexistentes.

Muchas de las organizaciones e instituciones no han definido o implementado en forma eficaz y adecuada, en base a sus necesidades, políticas y procedimientos de seguridad para la protección de la información, por lo que se podrían dar distintas circunstancias en las que se vería vulnerable el sistema informático. Por ejemplo: procedimientos inadecuados para la gestión de soportes informáticos, contraseñas poco robustas, falta de control de los tratamientos realizados por terceros (mantenimiento de equipos por empresas de informática), instalación de programas poco fiables, entre otros.

d. Desconocimiento y falta de sensibilización de los usuarios y de los responsables de informática.

Como principio básico desde el punto de la seguridad informática que hay que tener en cuenta es que todas las prevenciones o soluciones tecnológicas que se implementen en una organización o institución pueden resultar inútiles si hay desconocimiento, falta de información, desinterés o ánimo de causar algún daño de alguna de las personas que se encuentran dentro de ésta.

e. Disponibilidad de herramientas que facilitan los ataques.

Los ataques que se realizan por personas sin conocimientos informáticos o con conocimientos mínimos se han incrementado en los últimos años debido a que en

Internet se pueden encontrar todo tipo de programas gratuitos y fáciles de utilizar que han permitido llevar a cabo ataques contra redes y sistemas informáticos."[17]

2.1.5. Protección jurídica del software

Como resultado de la creciente demanda de los programas de computación, así como de su vulnerabilidad y alto costo económico el software adquiere, para la ciencia del derecho, un valor independiente al del hardware. Estos programas de ordenador son bienes abstractos que requieren de igual protección o tutela jurídica que las invenciones o las obras literarias o artísticas, protegidas respectivamente por las patentes o propiedad industrial y por el derecho de autor.

"El conjunto de instrucciones que conforma cada programa, dirigidas a conseguir un resultado determinado a través de su ejecución por el ordenador, son fruto del ingenio humano, y aunque requiera de un soporte físico no se confunde con él, sino que es susceptible de operar simultáneamente en un número indefinido de ordenadores o estar almacenado en un número de copias igualmente indefinido. Precisamente por ello, surge la necesidad de otorgar una protección eficaz tanto a los programas como a sus creadores."[18]

---

[17] **Ibíd.** Pág. 174.

[18] https://rua.ua.es/dspace/bitstream/10045/13057/7/TEMA%206%20RJB%20%20La%20protecci%C3%B3n%20jur%C3%ADdica%20del%20software.pdf (Consultado: 12 de agosto de 2016).

Tradicionalmente no ha existido una mayor polémica en lo que se refiere a la protección de los derechos intelectuales de los creadores de componentes del hardware y esto se debe a que éstas se producen dentro de los llamados inventos patentables. Por lo tanto, si el titular del derecho de propiedad intelectual cumple con los requisitos formales para patentar que lo que se establece en cada legislación, la protección se encontrará dada por las leyes de patentes vigentes en cada uno de los distintos países.

En cambio, la situación en lo que respecta a la protección jurídica de los derechos intelectuales de los creadores de programación (todos aquellos programas que se encuentran dentro de la parte intangible del computador o también llamado software) es menos clara. En el derecho comparado, se han postulado tres sistemas distintos para brindar tal protección, siendo estos las patentes de invención, derechos de autor y un sistema propio o sui generis.

Los programas de ordenador, como creaciones intelectuales del ser humano, actualmente se encuentran establecidos en la categoría de derechos de autor, por lo tanto, se regulan y protegen en Guatemala por la Ley de Derechos de Autor y Derechos Conexos -LDADC- (Decreto Número 33-98 del Congreso de la República) en la cual se establece la definición legal del concepto programa de ordenador en el artículo cuarto como "La obra constituida por un conjunto de instrucciones expresadas mediante palabras, códigos, planes o en cualquier otra forma, que al ser incorporadas a un soporte legible por máquina, es capaz de hacer que un ordenador ejecute determinada tarea u obtenga determinado resultado."

Así también es regulada en especial, por convenios internacionales en la materia, siendo un ejemplo de ello el Tratado sobre Derechos de Autor de la Organización Mundial de Propiedad Intelectual adoptado el 20 de diciembre de 1996 el cual establece que: "Artículo 4. Programas de Ordenador. Los programas de ordenador están protegidos como obras literarias en el marco de lo dispuesto en el Artículo 2 del Convenio de Berna del Convenio de Berna. Dicha protección se aplica a los programas de ordenador, cualquiera que sea su modo o forma de expresión."

En virtud de lo establecido en el tratado indicado y considerando las características y particularidades que incorporan los programas de ordenador, se hace necesario tener consideraciones especiales en lo referente a la protección de los programas de ordenador (software), por lo que la Ley de Derechos de Autor y Derechos Conexos ha seguido dicha corriente como se puede encontrar en el Título II Derecho de Autor, Capítulo IV Disposiciones Especiales para ciertas categorías de obras, sección segunda programas de ordenador y bases de datos como se encuentra regulado actualmente; la norma específica establece: "Artículo 30. Los programas de ordenador se protegen en los mismos términos que las obras literarias. Dicha protección se extiende tanto a los programas operativos como a los programas aplicativos, ya sea en forma de código fuente o código objeto y cualquiera que sea su forma o modo de expresión. La documentación técnica y los manuales de uso de un programa gozan de la misma protección prevista para los programas de ordenador."

2.2. Datos personales

"Para comprender lo que es un dato personal es necesario aclarar la diferencia entre dato e información, ya que no son sinónimos. Para entender cada término es necesario conocer la raíz etimológica. Así, dato viene del latín *datum* que significa lo que se da, se aplica a los hechos sin forma y sin orden. Por su parte, información viene del latín *informatio,* lo que equivale a lo que tiene forma y se refiere a los datos que poseen forma, estructura, orden y organización."[19]

El dato en sí, únicamente representa un hecho o un significado, pero carece de algún valor. Cuando una computadora procesa el dato o los datos y una persona le asigna un valor es cuando ese o esos datos se convierten en información.

Los datos personales comprenden aquella información que corresponden a cada persona para individualizarla y dan alguna idea o representación de ésta. Dentro de estos datos podemos encontrar nombre, domicilio, edad, número de documento de identificación, teléfono, dirección de residencia o dirección laboral, número de tarjeta de crédito, número de cuenta bancaria, número de licencia de conducir, fotografías, impresiones dactilares, filiación, estado civil, fecha y lugar de nacimiento, sexo, raza, religión entre otros.

[19] Barrios, **Op. Cit.** Pág. 337.

La Ley de Acceso a la Información Pública –LAIP- (Decreto Número 57-2008 del Congreso de la República) define los datos personales en el artículo noveno como "Los relativos a cualquier información concerniente a personas naturales identificadas o identificables."

En base a lo anterior, los datos personales son aquellos que proporcionan una idea o representación de hechos o circunstancias que tienen relación con una persona, los cuales a su vez pueden ser públicos o privados, como a continuación se detalla.

2.2.1. Datos personales públicos

"La información de las personas que se clasifican como datos personales públicos son todos los descriptores que figuran dentro de los registros de carácter público, que no excluyen poder estar en registros privados, que tienen la característica esencial de estar al alcance de todas o la mayoría de personas que deseen consultarlos."[20]

Un ejemplo de estos es aquellos que se encuentran en el Registro Nacional de las Personas -RENAP-, entidad encargada de organizar y mantener el registro único de identificación de las personas físicas, así como inscribir los hechos y actos relativos a su estado civil, capacidad civil y demás datos de identificación desde su nacimiento hasta la muerte, emitir el Documento Personal de Identificación, entre otras que son asignadas por la ley específica de la materia.

[20] Barrios Osorio, Omar Ricardo. **Introducción de las nuevas tecnologías en el Derecho.** Pág. 84.

Otros ejemplos son los datos de las personas contenidos en otros registros como el Registro General de la Propiedad, el Registro Mercantil, el Sistema de Contrataciones y Adquisiciones de Guatemala, e inclusive otros de origen privado como las guías telefónicas y comerciales, el directorio de profesionales, esto siempre y cuando se limiten a publicar los datos de naturaleza pública y no aquellos que puedan afectar la intimidad y privacidad de las personas.

2.2.2. Datos personales privados

Existen otra clase de hechos o descriptores de las personas que se denominan datos privados y se definen según el Manual de Protección de Datos como los "datos personales que tienen reguladas y tasadas las situaciones o circunstancias en que la persona se ve obligada a proporcionarlos, o ponerlos en conocimiento de terceros, siendo la conciencia social favorable a impedir su difusión y respetar la voluntad de secreto sobre ellos de su titular." Estos datos se subclasifican en datos personales no sensibles y datos personales sensibles.

Los datos personales privados no sensibles son los que se refieren a un sujeto específico y son relativos a su dominio interno o íntimo, pero sin llegar a ser información puramente sensible. Son aquellos que identifican su personalidad, creencias e ideologías, pensamientos, sentimientos y salud, entre otras cosas. finalmente son aquellos relacionados al orden privado de los individuos que los hacen merecedores de una protección más específica y profundizada que los demás tipos de datos generales,

esto debido a que se revelan exclusivamente de forma particular e individual, y rara vez son objeto de tratamiento público.

En el extremo de la privacidad e intimidad de una persona encontramos los datos personales sensibles los cuales se definen en la Ley de Acceso a la Información Pública en el artículo noveno como "Aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o actividad, tales como los hábitos personales, de origen racial, el origen étnico, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos, preferencia o vida sexual, situación moral y familiar u otras cuestiones íntimas de similar naturaleza."

2.2.3 Protección de los datos personales

La protección de datos personales se ubica dentro del campo de estudio del derecho informático. Se trata de la garantía o la facultad de control de la propia información frente a su tratamiento automatizado o no, es decir, no sólo a aquella información albergada en sistemas computacionales, sino en cualquier soporte que permita su utilización, ya sea almacenamiento, organización y acceso.

"Existen varias clases de datos, pero son los datos personales los que se revisten de una protección jurídica especial derivada del desarrollo de los derechos sobre aspectos inherentes a la persona, como lo son su identidad y su intimidad, y que con el surgimiento de las tecnologías de la información y comunicaciones están cobrando

importancia y relevancia para el Derecho, por la facilidad de poder afectar a cualquier sujeto en estos derechos."[21]

El derecho fundamental de la protección de datos personales se encuentra en constante cambio y desarrollo debido al auge de las bases de datos y su informatización, por lo tanto, se ha generado el incremento del uso de las TIC. Este derecho fundamental protector de los datos personales es aquel que reconoce la facultad de una persona para ejercer control sobre sus datos personales y la facultad de controlar y disponer sobre los mismos.

Se define en doctrina además como el derecho a la intimidad entendido como "la autorrealización del individuo. Es el derecho que toda persona tiene a que permanezcan desconocidos determinados ámbitos de su vida, así como a controlar el conocimiento que terceros tienen de él."[22]

El tema referente a la protección de los datos personales y la privacidad de los mismos ha sido una cuestión que ha generado bastante polémica, esto debido a que existen varias posturas al respecto en las que se manejan una postura de estricta regulación estatal o bien una postura más permisiva sin intervención por parte de los Estados.

En el caso de Guatemala se ha creado la ley de Libre Acceso a la Información Pública, la cual estable en el Título Primero, Capítulo Sexto lo siguiente: "Artículo 31.

[21] **Ibíd,** Pág. 83.
[22] **Ibíd,** Pág. 86.

Consentimiento expreso. Los sujetos obligados no podrán difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información desarrollados en el ejercicio de sus funciones, salvo que hubiere mediado el consentimiento expreso por escrito de los individuos a que hiciere referencia la información. El Estado vigilará que en caso de que se otorgue el consentimiento expreso, no se incurra en ningún momento en vicio de la voluntad en perjuicio del gobernado, explicándole claramente las consecuencias de sus actos. Queda expresamente prohibida la comercialización por cualquier medio de datos sensibles o datos personales sensibles".

En virtud de lo anterior el Estado y en especial los empleados y funcionarios públicos deben mantener los mecanismos técnicos y legales para la protección de los datos de las personas que se encuentran en las bases de datos administradas o manejadas por los mismos, así como el derecho de acceso a éstos conocidos como habeas data.

La Ley de libre Acceso a la Información Pública en el artículo noveno establece: "Habeas data: Es la garantía que tiene toda persona de ejercer el derecho para conocer lo que de ella conste en archivos, fichas, registros o cualquier otra forma de registros públicos, y la finalidad a que se dedica esta información, así como a su protección, corrección, rectificación o actualización. Los datos impersonales no identificables, como aquellos de carácter demográfico recolectados para mantener estadísticas, no se sujetan al régimen de hábeas data o protección de datos personales de la presente ley."

El mismo cuerpo normativo en el artículo 30 establece que, "en cuanto a las personas que administran las bases de datos denominados como sujetos obligados, como responsables de la data de las personas deberán cumplir con:

1. Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos que sean presentados por los titulares de los mismos o sus representantes legales, así como capacitar a los servidores públicos y dar a conocer información sobre sus políticas en relación con la protección de tales datos;

2. Administrar datos personales sólo cuando éstos sean adecuados, pertinentes y no excesivos, en relación con los propósitos para los cuales se hayan obtenido;

3. Poner a disposición de la persona individual, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento;

4. Procurar que los datos personales sean exactos y actualizados;

5. Adoptar las medidas necesarias que garanticen la seguridad, y en su caso confidencia o reserva de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado."

En la actualidad se celebra internacionalmente el movimiento sobre la protección de datos personales como un recordatorio de la importancia del derecho a la privacidad que gozan todos los seres humanos, teniendo como antecedente la aprobación del Convenio 108 del Consejo de Europa, el cual estableció la garantía del respeto a la información que por la propia naturaleza de cada persona.

En consecuencia de lo anterior se puede establecer que el Estado es responsable de proteger los derechos vulnerados por particulares. Resaltando la importancia del respeto a las garantías de la libertad de expresión o emisión del pensamiento, atendiendo a que estos derechos personales pertenecen con exclusividad a sus titulares. Una cultura responsable y de respeto al estado de derecho, privilegia a una sociedad y sus relaciones humanas. Mientras tanto, corresponde al Estado y por ende a las instituciones estatales, la protección de estos derechos.

2.2.4 Riesgos tecnológicos para la protección de datos personales

Existe una cantidad elevada de riesgos por falta de protección de los datos de las personas, que van desde el desconocimiento de las garantías y derechos, hasta una deficiente administración de las bases de datos; pero el riesgo es cada vez mayor con el uso de las tecnologías de la información y comunicaciones (TIC), especialmente para la accesibilidad a materiales de almacenamiento y captación de datos.

Los empleadores tanto estatales como privados, realizan recopilación de datos de las personas por medio de formularios de solicitud de empleos, administración de la planilla

laboral, declaraciones de seguros, plan de prestaciones, nombres de beneficiarios y condiciones de los mismos, historiales clínicos o expediente médico, controles laborales mediante el uso de tecnología, así como de la administración de cuentas de correo electrónico y navegadores, desplegado de mensajes de texto, grabación de llamadas telefónicas, entre otras. Ese control o recopilación de información personal se ha incrementado al sector de educación siendo el nivel de educación superior o universitario el más involucrado en la captación de datos personales, tanto de los estudiantes como del personal administrativo y docente de la institución.

A través de las actuales tecnologías también se pueden vulnerar los derechos de los usuarios mediante otros procedimientos informáticos como los virus, el spyware o el malware, incluso se están dando estos tipos de afectaciones en los teléfonos móviles o celulares de las personas; el desconocimiento técnico sobre cómo prevenir o contrarrestar estas situaciones, así también la falta de una regulación legal al respecto, permiten que se sigan afectando los derechos de los usuarios informáticos.

CAPÍTULO III

3. Mecanismos normativos para la fomentación de la seguridad informática y protección de los datos personales en las universidades a nivel internacional.

En vista a lo expuesto en los capítulos anteriores se hace notoria la necesidad de la protección de los datos personales desde el punto de vista y en el ámbito universitario. Es por ello que en la actualidad hay universidades que han iniciado proyectos referentes a la informática y con especial enfoque en la seguridad informática y en la protección de los datos personales.

Para entender el enfoque específico que se necesita para brindar una buena y eficiente seguridad en el sistema informático y protección a los datos personales en la Universidad de San Carlos de Guatemala se hace importante conocer de otras universidades que han implementado distintos sistemas normativos y así mismo analizarlos para comprender los puntos más importantes a abarcar.

3.1. Universidades latinoamericanas

Es preciso conocer y así también analizar a las universidades de Latinoamérica que han implementado mecanismos normativos para la fomentación de la seguridad informática y la protección de los datos personales de todos los usuarios dentro de la universidad.

3.1.1. Colombia

Colombia es uno de los países latinoamericanos que ha implementado la seguridad informática en cuanto a la protección de los datos personales. Varias de sus universidades poseen normativas internas las cuales están actualizadas dentro del campo de la informática y la seguridad de los datos personales.

La Universidad Nacional de Colombia ha implementado una política de tratamiento de protección de datos personales de los titulares de dicha Universidad Nacional.

Lo que se pretende con esta política es establecer los derechos que le asisten al titular de la información, así como los deberes tanto de éstos como los de la Universidad. Entre otros aspectos básicos necesarios para proteger los datos personales es indispensable determinar cuál será el tratamiento al que serán sometidos asimismo de la finalidad de dicho tratamiento.

Es importante resaltar uno de los puntos, a mi parecer, más importantes de dicho documento para analizar y asimismo ampliar el conocimiento en relación al tema.

"XIII. TRATAMIENTO AL CUAL SERÁN SOMETIDOS LOS DATOS Y FINALIDAD DEL MISMO

El tratamiento para los datos personales indispensables de estudiantes, docentes, trabajadores y/o contratistas, egresados estará enmarcado en el orden legal y en virtud de la condición de la Universidad como institución de educación superior, y serán todos

los necesarios para el cumplimiento de la misión institucional de docencia, investigación y extensión. Para el caso de datos personales sensibles, se podrá hacer uso y tratamiento de ellos cuando:

a) El Titular haya dado su autorización explícita a dicho Tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización;
b) El Tratamiento sea necesario para salvaguardar el interés vital del Titular y este se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización;
c) El Tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin la autorización del Titular;
d) El Tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial;
e) El Tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares.

El tratamiento de datos personales de niños, niñas y adolescentes está prohibido, excepto cuando se trate de datos de naturaleza pública, y cuando dicho tratamiento cumpla con los siguientes parámetros y/o requisitos:

a) Que respondan y respeten el interés superior de los niños, niñas y adolescentes.

b) Que se asegure el respeto de sus derechos fundamentales.

Cumplidos los anteriores requisitos, el representante legal de los niños, niñas o adolescentes otorgará la autorización, previo ejercicio del menor de su derecho a ser escuchado, opinión que será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto. La Universidad velará por el uso adecuado del tratamiento de los datos personales de los niños, niñas o adolescentes."[23]

En atención a lo estipulado se puede analizar que, de alguna manera la Universidad Nacional de Colombia está proporcionando seguridad informática en tanto que implementa medios y controles que aseguran la confidencialidad, integridad y disponibilidad de los activos de los sistemas de información y como resultado protege íntegramente los datos personales de los estudiantes, docentes y trabajadores.

En materia de protección de los datos personales en las diversas Casas de Estudios Superiores de Latinoamérica Colombia es de los más destacados al ser uno de los primeros países en implementarla, siendo la Universidad Nacional la que específicamente lo hace en materia de protección de datos personales, en tanto que otras solamente han llegado a regular el uso adecuado de salas de informática (o conocidas también como salones de computación), lo cual es un gran avance.

[23] http://www.unal.edu.co/contenido/habeas/POLITICA%20DE%20 TRATAMIENTO%20DE% 20DATOS. (Consultado: 22 de octubre de 2016).

En las universidades de otros países de Latinoamérica aún no se ha implementado una normativa que regule específicamente lo relacionado a la protección de los datos personales de los estudiantes, docentes, personal y demás trabajadores que dependan específicamente de la universidad. Por lo que Colombia es el país que ha sobresalido en el ámbito de la regulación de la informática y como es de admirar, la Universidad Nacional es la que sobresale en la seguridad informática.

3.2. Universidades europeas

Así como en Latinoamérica, es preciso también hacer un análisis de universidades en países de Europa que hayan implementado alguna normativa interna en la que se protejan los datos personales de los usuarios universitarios y en la que se impulse la búsqueda de la seguridad informática.

3.2.1. España

Uno de los países europeos que es prescindible comparar es España, ya que éste está relacionado histórica, social, cultural y jurídicamente con nuestro país por lo que de él podemos extraer información acerca del tema relacionado y así avanzar en Guatemala en cuanto lo referente a la materia informática.

España ha tenido un gran avance en lo relacionado a la materia de informática, desde lo más esencial que es su Carta Magna y así desglosándose en su normativa ordinaria como lo es su Código Penal, llegando hasta el punto de legislar de una forma más

específica como lo es en una universidad, asegurando un correcto uso de la informática y tutelar en este caso el bien jurídico de la información y datos personales protegiendo a su vez al titular.

Varias de las universidades españolas han incursionado en el mundo de la informática por lo que a su vez les ha sido necesario proteger a todos aquellos usuarios de la misma. Algunas específicamente han creado normativa interna al respecto de esa materia, otras han creado políticas de seguridad y por último hay otras que han reglamentado únicamente sobre el uso de los servicios y recursos informáticos, lo que de igual forma es un gran avance en materia de seguridad jurídica.

A continuación, se presenta un análisis de algunas de las universidades españolas que han implementado dicha normativa en materia informática.

a. Universidad de Catilla- La Mancha

Esta Universidad española ha implementado un Código de Conducta de Protección de los Datos Personales con el objeto, como hace mención en el preámbulo de dicho Código, de conocer que se ha generalizado el uso de los medios electrónicos, informáticos y telemáticos, lo cual es un evidente beneficio para los ciudadanos pero que cabe reconocer que también se incrementa el riesgo de vulnerabilidad de los datos almacenados, por lo que se debe adoptar medidas de seguridad que generen confianza en las personas usuarios de las aplicaciones.

Para tal efecto se encuentra en sus primeros artículos las disposiciones generales de dicho Código el objeto fundamental:

"Artículo1. Objeto. Este código de conducta tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimi dad personal y familiar.

Artículo 2. Ámbito de aplicación. El presente código de conducta será de aplicación a los datos de carácter personal que figuren registrados en soportes físicos de la Universidad de Castilla-La Mancha, que los hagan susceptibles de tratamiento y a toda modalidad de uso posterior de estos datos. La relación actualizada de ficheros y tratamientos de datos de carácter personal sometidos a este código de conducta se puede obtener en las direcciones de Internet www.uclm.es/psi y www.agpd.es."[24]

Es así como se muestra un extracto de como la Universidad de castilla-La Mancha ha implementado la protección de los datos personales por medio del código de conducta antes mencionado, en el que resaltando el objeto principal dentro de los primeros artículos podemos analizar el objeto general del documento y así mismo tomar un ejemplo del mismo.

[24] file:///C:/Users/nj152/Downloads/Codigo_de_conducta_de_proteccion_de_datos_personales_en_la_UCLM.pdf (Consultado: 20 de noviembre de 2016).

b. Universidad de Zaragoza

En el año 2002 esta universidad aprobó la normativa propia en materia de protección de datos de carácter personal en la cual se pretende reestructurar el fichero de datos personales de la universidad y adaptar el tratamiento de dichos datos a las exigencias de seguridad informática.

Asimismo, como se establece en sus consideraciones, esta normativa es propia y regula con carácter general el tratamiento de los datos personales en la institución universitaria sin perjuicio de la organización y diseño interno de las funciones y responsabilidades del personal, así como de la normativa vigente dentro de la institución.

Dentro de los artículos que contienen aspectos importantes a resaltar se encuentran:

"**Artículo 2.** Calidad de los datos. Los datos recabados deben ser adecuados, pertinentes y no excesivos en relación con la finalidad para la cual hayan sido recabados. Los datos recabados en la Universidad deberán servir a fines directamente relacionados con sus competencias y funciones.

Artículo 5. Usos y finalidades del tratamiento. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos fueron recogidos. No se considerará incompatible el tratamiento posterior de los datos para fines históricos, estadísticos o científicos. Tal y como se establece en el

artículo 3 anterior, el interesado deberá ser informado de la finalidad determinada, explícita y legítima del tratamiento."[25]

Analizando los artículos anteriores es notorio que lo que se pretende principalmente es proteger al individuo en el inminente riesgo de violación a sus datos personales y a toda aquella información que pueda ser mal utilizada, por lo que específicamente se señala que tipo de datos se deben solicitar y que los mismos sean los necesarios y de acorde a los fines relacionados a funciones y competencias dentro de la universidad.

c. Universidad de Almería

Universidad española que también ha puesto su interés en hacer uso de las denominadas TIC, lo que a su vez genera la necesidad de ser administradas diligentemente tomando las medidas adecuadas para su protección y así no afectar la integridad o confidencialidad de la información tratada o de los servicios prestados. Por lo que la esta universidad ha creado una política de seguridad de la información aprobada por el Consejo de Gobierno en el año 2012.

De acuerdo a esta Política de Seguridad de la Información, los sistemas TIC deben estar protegidos contra las amenazas que rápidamente evolucionan, por lo que para defenderse de las mismas se requiere de una estrategia que se adapte tanto a las

[25] https://protecciondatos.unizar.es/sites/protecciondatos.unizar.es/ files/users/lopd/Resolucion20020606modificada%20con%202015.pdf (Consultado: 2 de diciembre de 2016).

condiciones del entorno como a los cambios que se puedan dar en este y así garantizar seguridad en la información.

Entre los puntos desarrollados por este documento se encuentran aspectos importantes en lo referente a la seguridad informática, desarrollada en los capítulos anteriores, como lo es el establecer una determinada política de seguridad desarrollada por medio de una normativa de seguridad en la que se afronten aspectos específicos la cual debe de estar a disposición de todos aquellos que necesiten conocerla, en especial de aquellos que utilicen, operen o administren los sistemas de información y comunicaciones; instaurar una organización para la seguridad en la que se pretende establecer los roles, funciones y responsabilidades de cada área encargada del manejo de la información; establecer una gestión de riesgos que realice un análisis evaluando las amenazas a las que se está expuesto.

En general el documento abarca los aspectos y elementos más importantes de la seguridad informática por lo que genera una correcta protección de los datos personales.

d. Universidad Politécnica de Valencia

Esta universidad ha creado el Reglamento de uso de los servicios y recursos informáticos en el cual en el capítulo primero establece las disposiciones generales estableciendo principalmente el objetico de dicho reglamento.

"Artículo 1. Objetivo y ámbito de aplicación. La Universidad Politécnica de Valencia (UPV) ofrece a la comunidad universitaria el acceso a la red de la Universidad Politécnica de Valencia (UPVnet) para el mejor desarrollo de su actividad docente, de investigación o de gestión académica. El acceso a esta red permite que los diferentes usuarios utilicen una serie de servicios como correo electrónico, transferencia de archivos, acceso a ordenadores remotos, instalación de servidores web, creación de páginas personales en webs, entre otros. Dichos servicios pueden ser utilizados por alumnos, personal docente e investigador (PDI) y personal de administración y servicios (PAS), en las condiciones previstas en cada caso.

El objetivo de este reglamento es garantizar, pese a la gran demanda de estos servicios, la calidad de los mismos y un uso de acuerdo con los fines últimos de la Universidad: la investigación, la docencia y los servicios académicos.

La presente normativa es de aplicación a todos los usuarios de la red UPVnet. Cualquier equipo que se conecte a la red UPVnet, aunque no sea propiedad de la Universidad, quedará sujeto a las normas y condiciones contenidas en este Reglamento.

El presente Reglamento será de aplicación sin perjuicio de las disposiciones aplicables en la materia."[26]

---

[26] https://www.upv.es/entidades/ASIC/normativa/normativa_servicios_ c.pdf (Consultado: 5 de enero de 2017).

Aunque este Reglamento no es específicamente regulador de una protección integral de los datos personales, conforme el extracto anterior se puede determinar que éste va encaminado a dicha protección, ya que como lo establece en su artículo primero, pretende garantizar la calidad de los servicios y recursos informáticos, lo que es a su vez un elemento esencial de la seguridad informática.

Asimismo, en los demás artículos del mismo reglamento se encuentran elementos importantes para proteger los datos personales como lo es la determinación de quien será usuario de dichos servicios y recursos informáticos, lo que de igual manera genera una obligación y responsabilidad para los mismos ya que se encuentran identificados. También en el reglamento mencionado, a fin de tener un correcto funcionamiento, goza de un detallado procedimiento a seguir para mantener un orden y control de cada equipo conectado lo que permite identificar en cualquier circunstancia de donde proviene un ataque o intento de ataque al sistema informático.

Para finalizar el análisis de dicho reglamento es preciso hacer mención de unos artículos que son de suma importancia dentro del tema de estudio que es la seguridad informática y la protección de los datos personales.

"Artículo 3.

...3.3 Compromiso de confidencialidad con relación a los servicios UPVnet

Todo el personal de la Universidad Politécnica de Valencia que por su trabajo tenga acceso al contenido almacenado en los recursos que dan soporte a los servicios debe cumplir con la obligación de secreto y confidencialidad.

La confidencialidad de contenidos y contraseñas a las que se refiere este apartado no excluye la posibilidad de que, en estricto cumplimiento de los pertinentes requerimientos judiciales o, en su caso, autoridad legalmente autorizada, deban revelarse los contenidos, así como la identidad de los autores.

Artículo 4. Responsabilidades del usuario. El usuario es responsable exclusivo del uso que realice de los servicios y recursos ofrecidos por UPVnet, debiendo en todo caso hacerse responsable de la custodia de su clave de acceso.

El usuario debe notificar inmediatamente a la Universidad Politécnica de Valencia cualquier uso no autorizado de su contraseña o cuenta o de cualquier otro fallo de seguridad. Asimismo, el usuario debe asegurarse de que su cuenta queda cerrada al final de cada sesión."[27]

Analizando el inciso 3.3 del artículo tercero y el artículo cuarto se encuentra que el personal que maneje o tenga acceso a los recursos o servicios informáticos está obligado al secreto y confidencialidad de los datos encontrados ahí, por lo que para su cumplimiento se establece una serie de responsabilidades específicas.

Fue preciso un análisis más profundo de este reglamento a efecto de que lo que regula no es específicamente una protección a los datos personales, pero en cuanto a su contenido se observa que se desarrollan ciertos elementos importantes para la

[27] **Ibíd.**

seguridad informática que, aunque desarrollados de forma general, forman un escalón para alcanzar una normativa más específica si más adelante la Universidad toma cada elemento y lo desarrolla más detalladamente.

Como se ha visto en este inciso España es un país en el que la seguridad informática y la protección de datos personales es de mucha importancia al punto que la mayoría de universidades lo ha implementado dentro de su normativa interna, lo que permite tomar ejemplo de ello para ir avanzando en ese ámbito también.

3.3 Universidades de Guatemala

Anteriormente se hizo análisis de las universidades latinoamericanas y europeas que más se asemejan al sistema de Guatemala, por lo que ahora es conveniente un análisis para verificar si en las universidades que son parte del sistema educativo superior guatemalteco se encuentra alguna normativa que tenga relación al tema de la seguridad informática y a la protección de los datos personales, por lo que se podría analizar su normativa interna y tomar ejemplos.

Para esto mismo es preciso señalar que en Guatemala existe una cantidad significativa de universidades privadas, entre las cuales se encuentran:

- Universidad Mariano Gálvez
- Universidad Rafael Landívar
- Universidad Mesoamericana

- Universidad Panamericana
- Universidad Rural
- Universidad Internaciones
- Universidad Galileo
- Universidad San Pablo
- Universidad del Istmo
- Universidad del Valle
- Universidad Francisco Marroquín
- Universidad Da Vinci
- Universidad de Occidente
- Universidad Regional

Es interesante ver como es que, en el sistema de educación superior en Guatemala, a pesar de que existen varias universidades privadas, al tema de la informática no se le toma en cuenta desde el punto de vista jurídico, en tanto que ninguna de las universidades mencionadas cuenta con alguna normativa interna que proteja los datos personales y que fomente la seguridad informática, por lo que se hace de suma importancia iniciar a incursionar dentro de ese ámbito.

CAPÍTULO IV

4. Seguridad informática y protección de datos personales en la normativa interna de la Universidad de San Carlos de Guatemala

En los capítulos anteriores se ha introducido al tema de la informática especificando y ahondando en el tema de la seguridad informática y la protección de los datos personales, aplicándolo posteriormente a las universidades en países que más se asemejen al sistema guatemalteco, ello con el fin de conocer si en la Universidad de San Carlos de Guatemala se ha aplicado o es necesario aplicar lo referente al tema mencionado.

Por lo anterior y para llegar a realizar un buen análisis es imprescindible conocer más a fondo acerca de la Universidad de San Carlos, desde un poco de historia hasta ahondar en lo que es de nuestro interés en esta investigación, la normativa interna y qué es lo que ésta comprende.

4.1. Historia de la Universidad de San Carlos

La Universidad de San Carlos de Guatemala fue fundada por Real Cédula de Carlos II, de fecha 31 de enero de 1676. La Constitución de Guatemala emitida en el año de 1945, consagró como principio fundamental la autonomía universitaria, y el Congreso de la República complementó las disposiciones de la Carta Magna con la emisión de una Ley

Orgánica de la Universidad, y una Ley de Colegiación obligatoria para todos los graduados que ejerzan su profesión en Guatemala.

"Desde septiembre del año 1945, la Universidad de San Carlos de Guatemala funciona como entidad autónoma con autoridades elegidas por un cuerpo electoral, conforme el precepto legal establecido en su Ley Orgánica; y se ha venido normando por los siguientes principios que, entre otros, son el producto de la Reforma Universitaria en 1944: Libertad de elegir autoridades universitarias y personal docente, o de ser electo para dichos cuerpos sin injerencia alguna del Estado; Asignación de fondos que se manejan por el Consejo Superior Universitario con entera autonomía; Libertad administrativa y ejecutiva para que la Universidad trabaje de acuerdo con las disposiciones del Consejo Superior Universitario; Dotación de un patrimonio consistente en bienes registrados a nombre de la Universidad; Elección del personal docente por méritos, en examen de oposición; Participación estudiantil en las elecciones de autoridades universitarias y Participación de los profesionales catedráticos y no catedráticos en las elecciones de autoridades."[28]

4.2. Legislación Universitaria

Para conocer más a fondo acerca del tema en mención es necesario conocer de la legislación interna de la Universidad de San Carlos de Guatemala, iniciando desde lo más esencial de la legislación nacional, la Constitución Política de la República:

[28] http://redusacunoc.tripod.com/HISTORIA_USAC.html (Consultado: 20 de enero de 2017).

"Artículo 82. Autonomía de la Universidad de San Carlos de Guatemala. Es una institución autónoma con personalidad jurídica. En su carácter de 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. Promoverá por todos los medios a su alcance la investigación en todas las esferas del saber humano y cooperará al estudio y solución de los problemas nacionales. Se rige por su Ley Orgánica y por los estatutos y reglamentos que ella emita, debiendo observarse en la conformación de los órganos de dirección, el principio de representación de sus catedráticos titulares, sus graduados y sus estudiantes."

En la Constitución Política de la República se establece que la Universidad de San Carlos en tanto que es una Institución autónoma se rige por su Ley Orgánica y por los Estatutos y Reglamentos que ésta emita.

Por lo que tomando en cuenta lo anterior se desarrolla parte de la normativa general y superior de la Universidad que en su mayoría se encuentra contenida en:

- **Estatuto de la Universidad de San Carlos de Guatemala (nacional y autónoma).** El Estatuto consta de 133 artículos. Principalmente lo que regula es la Universidad y su autonomía como se establece en el **Artículo 1**: "La Universidad de San Carlos de Guatemala, continuadora de la Universidad Carolina fundada por Real Cédula del 31 de enero de 1676, es una institución de alta cultura, Nacional y Autónoma con personalidad jurídica y patrimonio propio. Se rige por su Ley Orgánica,

Estatutos, Reglamentos y demás disposiciones que ella emita. Tiene su sede central ordinaria en la ciudad de Guatemala." Además de ello se encarga de regular lo referente a las Unidades Académicas; fines de la Universidad; gobierno de la universidad; de las Facultades; de las elecciones universitarias; Organización de la enseñanza; de la disciplina en la universidad; Distinciones y honores; Bibliotecas; del Personal Administrativo; Revista de la Universidad; Patrimonio cultural y natural y de la estructura económica de la Universidad.

- **Decreto Número 325. Ley Orgánica de la Universidad de San Carlos de Guatemala.** Promulgada en el año 1947 y lo que ésta primordialmente establece es la autonomía universitaria como está regulada en el Artículo primero: "La Universidad de San Carlos de Guatemala es una institución autónoma, con personalidad jurídica, regida por esta Ley y sus estatutos, cuya sede central ordinaria es la ciudad de Guatemala." Además de ello regula entre sus normas: la integración de la Universidad; de su Régimen; Régimen económico y disposiciones generales.

Dentro de los reglamentos que conforman el resto de la normativa interna de la Universidad se encuentra:

- Reglamento Interior del Consejo Superior Universitario
- Reglamento de la Carrera Universitaria del Personal Académico
- Reglamento del Personal Académico Fuera de Carrera
- Reglamento de la Junta Universitaria de Personal Académico

- Reglamento de formación y desarrollo de personal académico
- Reglamento de Evaluación y Promoción del Personal Académico de la Universidad de San Carlos de Guatemala
- Reglamento de Concursos de Oposición del Profesor Universitario
- Reglamento de los Concursos de Oposición para Profesores Auxiliares de la Universidad de San Carlos de Guatemala
- Reglamento del Programa Sabático del Personal Académico
- Reglamento para la Contratación del Profesor Visitante
- Reglamento de Relaciones Laborales entre la Universidad de San Carlos de Guatemala y su Personal
- Reglamento de la Tasa Estudiantil
- Reglamento General de los Centros Regionales Universitarios de la Universidad de San Carlos de Guatemala
- Reglamento General del Centro Universitario de Occidente
- Reglamento de Apelaciones
- Reglamento del Consejo Editorial de la Universidad de San Carlos de Guatemala
- Reglamento General de Evaluación y Promoción del Estudiante de la Universidad de San Carlos de Guatemala
- Reglamento para Autorización de Carreras en las Unidades Académicas de la Universidad de San Carlos de Guatemala
- Reglamento para la Administración de las Áreas de Parqueo de la Universidad de San Carlos de Guatemala
- Reglamento para la Actividad Comercial en las Instalaciones de la Universidad de San Carlos de Guatemala

- Reglamento para el Desarrollo de Actividades Públicas en la Universidad de San Carlos de Guatemala
- Normas y Procedimientos para la Concesión de Licencias, Otorgamiento de Ayudas Becarias y Pago de Prestaciones Especiales al Personal de la Universidad de San Carlos de Guatemala
- Reglamento de la Junta Administradora del Plan de Prestaciones de la Universidad de San Carlos de Guatemala
- Reglamento Interno de Funcionamiento y Organización de la Junta Universitaria de Personal
- Reglamento de Administración Estudiantil de la Universidad de San Carlos de Guatemala
- Reglamento de Elecciones de la Universidad de San Carlos de Guatemala
- Reglamento para el Registro y Control de Bienes Muebles y otros Activos Fijos de la Universidad de San Carlos de Guatemala
- Reglamento del Sistema de Estudios de Postgrado.

Como se observa en lo anteriormente expuesto, dentro de la normativa general interna de la Universidad de San Carlos no existe todavía un reglamento que regule lo referente a la seguridad informática y la protección de los datos personales por lo que se hace necesario conocer quién es el ente encargado de emitir los reglamentos internos de la Universidad y verificar si es factible la implementación de un reglamento en relación a este tema.

4.2.1. Régimen de la Universidad de San Carlos de Guatemala

Para poder entender y conocer más del régimen de la universidad hay que tener conocimiento de las normas que regulan al respecto, en tanto que sepamos de donde emana la normativa interna y quienes son los competentes para emitirla. Por lo tanto, es indispensable conocer de las normas que establecen dicho régimen.

Ley Orgánica de la Universidad de San Carlos: **"Artículo 12.** La Universidad de San Carlos de Guatemala, tendrá para su gobierno e integración, los siguientes organismos: un Consejo Superior Universitario, un Cuerpo Electoral Universitario y un Rector."

El órgano superior de la Universidad de San Carlos es el Consejo Superior Universitario, así como se establece primordialmente en la Constitución Política de la República de Guatemala en el artículo 83: **"Gobierno de la Universidad de San Carlos de Guatemala.** El gobierno de la Universidad de San Carlos de Guatemala corresponde al Consejo Superior Universitario, integrado por el Rector, quien lo preside; los decanos de las facultades; un representante del colegio profesional, egresado de la Universidad de San Carlos de Guatemala, que corresponda a cada facultad; un catedrático titular y un estudiante por cada facultad."

En virtud de lo anterior es necesario analizar si el Consejo Superior Universitario de la Universidad de San Carlos tiene alguna competencia o interviene en la emisión de la normativa interna, por lo que se analizarán las atribuciones de este órgano según la normativa interna.

Ley Orgánica de la Universidad de San Carlos de Guatemala, TÍTULO IV, Atribuciones y deberes del Consejo Superior Universitario: **"Artículo 24.** El Consejo Superior Universitario, además de Cuerpo Consultivo del Rector tiene las siguientes atribuciones y deberes: ... b) Elaborar los estatutos y aprobar los reglamentos que le sometan las juntas directivas de las Facultades y los Jefes de los Institutos, siempre que se ajusten al espíritu de esta Ley; ..."

Estatuto de la Universidad de San Carlos de Guatemala, CAPÍTULO II, Del Consejo Superior Universitario: **"ARTÍCULO 11. (Modificado por el punto Noveno, del Acta 27-2005 del Consejo Superior Universitario, de fecha 26/10/2005)** El Consejo Superior Universitario tiene las siguientes atribuciones: ... b) Reformar total o parcialmente los Estatutos de la Universidad; emitir, reformar o derogar Reglamentos Generales que sometan a consideración. El Estatuto de la Universidad de San Carlos de Guatemala tendrá jerarquía normativa superior a los reglamentos. A ningún reglamento se le denominará Estatuto o Estatutos. Los Normativos Específicos de las facultades, escuelas no facultativas o centros universitarios, serán emitidos por las Juntas Directivas o Consejos Directivos de cada unidad; los normativos específicos de organización de unidades administrativas que dependan de la Rectoría, serán emitidos, reformados o derogados por el Rector; y los instructivos serán emitidos por los decanos o directores, respectivamente. De cada normativo emitido se informará al Consejo Superior Universitario..."

En atención a los anteriores artículos es preciso analizar que el Consejo Superior Universitario sí tiene injerencia dentro de la creación y modificación de la normativa

interna universitaria. Por lo que sí sería posible la implementación de un nuevo reglamento en materia de seguridad informática y protección de los datos personales.

4.3. Riesgos o consecuencias de una mala seguridad informática en la Universidad

Existen distintos riesgos los cuales van a variar dependiendo de la naturaleza de la institución u organización, pero aun así las vulneraciones en cuestión de seguridad informática no se conocen por todos los usuarios y por lo tanto no saben cómo protegerse de dicha vulnerabilidad.

Entre los riesgos más comunes que pueden darse por falta de seguridad informática se encuentran:

- Tener información dispersa. Lo que genera esta dispersión de información es que impide un control centralizado de la información, por lo que se convierte en una amenaza en tanto que esté asociada a otros problemas como la inconsistencia de la misma dentro de la institución.
- Pérdidas de información. Ésta puede darse por efecto de algún virus.
- Robo de información.
- Adulteración de información.
- Revelación de información confidencial.
- Sabotaje.
- Fallas en los sistemas y medios informáticos.

Ahora enfocando estos riesgos desde el ámbito universitario, aquellos que podrían suceder son:

- Los sistemas dejan de funcionar. No solamente en el ámbito universitario se puede dar este caso, pero puede afectar dentro de éste ya que las páginas educativas o de asignación u otras utilizadas por catedráticos y personal administrativo se saturen o dejen de funcionar adecuada o totalmente, lo que perjudica grandemente a todos los usuarios.

- Desaparición de información almacenada o manipulación de la misma. En el caso de catedráticos se pueden filtrar exámenes, calificaciones de los alumnos, folletos o manuales pedagógicos; en el caso de los estudiantes sería el tema de las asignaciones de cursos, envío de tareas o trabajos en línea, inscripciones, etc.; en el caso de los trabajadores y personal administrativo se debe tomar en cuenta el tipo de información que ellos manejan acerca de temas ligados a la Universidad además de su información privada, pagos mensuales, generación de contratos, publicación de contratos, manejo de cuentas asociadas con el fisco. Estas anteriores no son únicamente las existentes, pero en su mayoría son las más comunes.

- Violación de la privacidad a cuentas personales. En el entendido que cada estudiante, docente y trabajador de la universidad posee cuentas de tipo personal como lo son comúnmente los correos electrónicos.

Estos son algunos de los riesgos que se corren cuando no se tiene una buena y eficiente seguridad informática y una protección de datos, sin embargo, hay que tomar en cuenta que no son los únicos y que éstos en su mayoría pueden tomarse como delitos.

4.4. Cómo evitar la vulnerabilidad o los riegos

Al momento en que existe un riesgo o el sistema es vulnerable es necesario buscar los mecanismos de defensa para combatir los mismos, sin embargo, es de mayor utilidad y efectividad tener estos medios antes de que alguno de ellos ocurra como mecanismo de prevención, por lo que es de preferencia, y como en los capítulos anteriores se ha tratado, definir una política de seguridad de red lo cual significa elaborar una serie de procedimientos y planes que protejan los recursos de la red contra pérdidas y daños.

Para elaborar una política eficiente para cada institución se necesita de un enfoque que hará posible la elaboración de dicha política, la cual, entre otras, propondrá examinar lo siguiente:

- "¿Qué recursos se está tratando de proteger?
- ¿De quiénes se necesita proteger los recursos?
- ¿Qué tan posibles son las amenazas?
- ¿Qué tan importante es el recurso?

- ¿Qué medidas se pueden implementar para proteger los bienes de forma económica y oportuna?
- Examinar periódicamente la política de seguridad de red para ver si han cambiado los objetivos y las circunstancias de la red.
- Participación de las personas adecuadas y especializadas en el diseño de la política de seguridad.
- Un aspecto importante de la política de seguridad es establecer las diferentes funciones del personal, así como hacer de su conocimiento las responsabilidades de cada persona para poder darle mantenimiento a los servicios y recursos informáticos.
- Tener conocimiento de que los niveles de seguridad pueden ser variados dentro de las normas a establecerse, en este caso se puede ejemplificar con que cada usuario de la red debe ser responsable de sus accesos o contraseñas; pero, por otra parte, los administradores de la red y/o encargados del sistema son responsables de inspeccionar y garantizar la seguridad de la red.
- Los riesgos se deben clasificar por el nivel de importancia y gravedad de la perdida, tratando de evitar terminar en una situación en que sea más el gasto de asegurar que el propio valor de lo que se esté protegiendo. Por lo que para lograr lo anterior es necesario realizar un análisis del riesgo en el cual se deben determinar dos factores importantes: 1. Estimación del riesgo en el momento de perder el recurso y 2. Estimación de la importancia del recurso tales como el hardware, software, datos, personas/usuarios, documentación y suministros."[29]

[29] González Agudelo, Daniel Felipe., El riesgo y la falta de políticas de seguridad informática una amenaza en las empresas certificadas base con URL http://repository.unimilitar.edu.co/bitstream /10654/12251/1/ENSAYO%20FINAL.pdf. (Consultado: 5 de febrero de 2017).

Además del contenido del enfoque anterior se debe tener en cuenta que, aunque existan políticas las cuales ayudan a anticipar todo tipo de amenazas, éstas no pueden asegurar que para cada tipo de proceso haya personas que los manejen de forma responsable y consciente por lo que es de suma importancia garantizar la seguridad general de la red.

Es por ello, y tomando en cuenta lo anterior, que surgen las políticas de seguridad como una herramienta que permite concientizar a los usuarios y personas encargadas de la red sobre la importancia que se le debe dar al uso responsable de los medios y recursos informáticos, así como hacer de su conocimiento la sensibilidad de la información y sobre los métodos existentes que permiten asegurar el buen uso de dichos recursos informáticos, manteniéndolos así libres de peligros, daños y riesgos.

Para finalizar el tema de la creación de políticas de seguridad es de suma importancia que estas sean basadas en 3 principios fundamentales, los cuales se deben cumplir para garantizar la seguridad en todo sistema informático, los cuales son:

- **"Confidencialidad.** esta se refiere a que debe existir privacidad de los elementos de información almacenados y procesados en un sistema informático.

- **Integridad.** Este principio hace referencia a la validez y consistencia de los elementos de información almacenados y procesados en un sistema informático, por lo que se debe asegurar que los procesos de actualización estén bien sincronizados y no se dupliquen, de forma que todos los elementos del sistema manipulen adecuadamente los mimos datos.

- **Disponibilidad.** En base a este principio se debe mantener la continuidad de acceso a los elementos de información almacenados y procesados en un sistema informático. Por lo tanto, se debe reforzar la permanencia del sistema en condiciones de actividad adecuadas para que los usuarios puedan acceder a los datos con la frecuencia y dedicación que requieran."[30]

[30] **Ibíd.**

CAPÍTULO V

5. Proyecto de Reglamento de seguridad informática y protección de datos personales de la Universidad de San Carlos de Guatemala

Una vez que se ha tratado en los capítulos anteriores el tema de la informática y los datos personales, se hace necesario conocer también la aplicación de éstos al sistema universitario y la comparación de las distintas universidades que han implementado un sistema para proteger los datos y brindar seguridad informática; por ende, se hizo necesario indagar sobre la comunidad universitaria de Guatemala y en especial la Universidad de San Carlos de Guatemala, en lo que se llegó al punto de observar que es preciso implementar dentro de la normativa interna universitaria un reglamento que permita proteger los datos personales y que brinde seguridad informática dentro de la misma.

A continuación, se presenta un proyecto de reglamento que idealmente se recomienda aplicar dentro de la Universidad.

TÍTULO I

Disposiciones Generales

Artículo 1. Objeto.

El objeto del presente Reglamento es garantizar y proteger lo concerniente al tratamiento de los datos personales y observar dentro de la Universidad de San Carlos de Guatemala la seguridad informática.

Artículo 2. Ámbito de aplicación.

Este reglamento será de aplicación a los datos de carácter personal que se encuentren registrados en soportes físicos de la Universidad de San Carlos, que sean susceptibles de tratamiento y a toda modalidad de uso posterior de estos datos.

Artículo 3. Definiciones.

Para los efectos del presente reglamento se entenderá por:

a) Afectado o interesado: persona física titular de los datos que sean objeto de tratamiento.
b) Datos de carácter personal: información numérica, gráfica, fotográfica, o de cualquier otro tipo concerniente a personas físicas identificables.
c) Destinatario o cesionario: persona física o jurídica, pública o privada al que se le revelen datos.

d) Cancelación: procedimiento en virtud del cual el responsable cesa el uso de los datos. La cancelación implicará el bloqueo de los datos impidiendo su tratamiento, exceptuando los casos en que sea solicitado órganos de justicia competentes.

e) Comunicación de datos: tratamiento de datos que supone su revelación a una persona distinta al interesado.

f) Consentimiento del interesado: manifestación de voluntad libre, expresa y específica mediante la que el interesado consienta el tratamiento de datos personales que le conciernan.

g) Dato separado: aquél que no permite la identificación del interesado o afectado.

h) Tratamiento de datos: cualquier operación o procedimiento técnico, automatizado o no, que permita recoger, conservar, grabar, consultar, utilizar, modificar, cancelar, bloquear o suprimir datos.

i) Encargado del tratamiento: persona física o jurídica encargada de tratar los datos de carácter personal por cuenta de la universidad de San Carlos de Guatemala como consecuencia de una relación jurídica delimitando su actuación únicamente para la prestación de un servicio.

j) Archivo: conjunto organizado de datos personales que permita el acceso a dichos datos con arreglo a criterios determinados, cualquiera que sea su forma o modalidad de creación, almacenamiento, acceso y organización.

k) Responsable interno del archivo o del tratamiento: persona de la Universidad de San Carlos de Guatemala, que por delegación de autoridad competente realiza las tareas encargadas al responsable del archivo.

l) Persona identificable: persona cuya identidad pueda determinarse directa o indirectamente mediante cualquier tipo de información referida a su identidad.

m) Tercero: persona física o jurídica, pública o privada, distinta del afectado o interesado, de la Universidad de San Carlos de Guatemala, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa de la Universidad de San Carlos de Guatemala o del encargado del tratamiento.

n) Usuario: sujeto o proceso autorizado para acceder a datos o recursos.

o) Autenticación: procedimiento de comprobación de la identidad de un usuario o en el acceso a un recurso.

p) Contraseña: información confidencial, frecuentemente constituida por una cadena de caracteres que puede ser usada en la autenticación de un usuario.

q) Control de acceso: mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.

r) Documento: todo escrito, gráfico, imagen, sonido o cualquier otra clase de información que pueda ser tratada en un sistema de información como una unidad separada.

s) Archivos temporales: archivos de trabajo creados por usuarios o procesos que son necesarios para determinada ocasión o como paso intermedio durante la realización de un tratamiento.

t) Responsable de seguridad: persona o personas a las que el responsable interno del archivo asigna formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

u) Sistema de información: conjunto de archivos, programas, tratamientos, equipos y soportes empleados para el almacenamiento y tratamiento de datos personales.

v) Soporte: objeto físico que almacena o contiene datos o documentos; objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos.

w) Transmisión de documentos: cualquier traslado, envío, entrega o comunicación de la información contenida en documentos.

x) Universidad: Universidad de San Carlos de Guatemala.

TÍTULO II

Principios de protección de los datos personales

Artículo 4. Finalidad de los datos.

Los datos de carácter personal únicamente se podrán recoger para su tratamiento y para someterlos a dicho tratamiento cuando sean pertinentes y no excesivos en relación con el ámbito y finalidades determinadas y legítimas para las que se hayan obtenido.

Los datos personales que sean objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, científicos o estadísticos.

Artículo 5. Exactitud de los datos.

Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado. Son exactos los datos cuando han sido recogidos directamente del afectado.

Artículo 6. Verificación de datos en solicitudes formuladas a otras administraciones o dependencias.

Si se formularen solicitudes a través de medios electrónicos en las que e interesado declare datos que obren en otras dependencias o administraciones, la Universidad podrá efectuar, en el ejercicio de sus competencias, las verificaciones necesarias para comprobar la autenticidad de los datos.

Artículo 7. Cancelación de los datos.

Los datos de carácter personal únicamente serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados. Sin embargo, los datos podrán conservarse durante el tiempo en que pueda exigirse algún tipo de responsabilidad derivada de una relación u obligación jurídica.

Los datos personales serán tratados de forma que permitan el ejercicio del derecho de acceso, en tanto no proceda su cancelación.

Artículo 8. Información durante la recolección de datos.

A los interesados a los que se les solicite datos deberán ser informados previamente y de forma expresa y precisa:

- De la existencia de un archivo de datos personales y la finalidad del mismo, así como de los destinatarios de la información.
- De la posibilidad de ejercer derechos de acceso, rectificación cancelación y oposición.

Dicha información solamente es necesaria brindarla cuando los datos vayan a formar parte de un archivo de la Universidad y se informará siempre de la finalidad de los mismos cuando éstos sean recogidos a través de un formulario.

Cuando los datos personales no hayan sido recabados del interesado, éste deberá ser informado de forma expresa por la Universidad dentro del plazo de un mes, salvo que hubiera sido informado con anterioridad, del contenido del tratamiento; de la procedencia de los datos; del derecho de acceso, rectificación, cancelación y oposición y de la identidad del responsable del tratamiento.

Artículo 9. Consentimiento del afectado.
El tratamiento de datos personales requerirá el consentimiento expreso del afectado, salvo disposición en contrario de la ley.

No es preciso el consentimiento del afectado cuando los datos personales se recojan para el ejercicio de las funciones propias de la Universidad dentro del ámbito de su competencia y cuando se refiera a las partes de un contrato o relación laboral o administrativa y sean necesarios para su cumplimiento.

El consentimiento podrá ser revocado cuando exista causa justificada para ello. En los casos que no sea necesario el consentimiento del afectado, éste puede oponerse al tratamiento de los datos personales cuando existan motivos fundados y legítimos relativos a una situación personal concreta, por lo que en ese caso la Universidad excluirá del tratamiento los datos relativos al afectado.

Artículo 10. Deber de secreto.

Toda persona que intervenga en el tratamiento de datos personales, en cualquiera de sus fases, está obligado al secreto profesional respecto de los mismos. Dicha obligación subsistirá aun después de finalizar sus relaciones con la Universidad.

Artículo 11. Comunicación de datos.

Los datos de carácter personal objeto de tratamiento únicamente pueden ser comunicados a un tercero para el cumplimiento de fines directamente relacionados a funciones legítimas del cedente y del cesionario con el consentimiento previo del interesado.

Artículo 12. Comunicación de datos personales de estudiantes y trabajadores.

La comunicación de los datos de carácter personal a terceros solamente se producirá cuando una ley obligue a la Universidad a esa comunicación o el interesado de su consentimiento.

Artículo 13. Comunicación de datos con fines de investigación.

La comunicación de los datos personales o su uso interno con fines de investigación únicamente se producirá si está autorizada por una ley o se ha utilizado un procedimiento de análisis.

Artículo 14. Acceso a los datos por cuenta de terceros para la prestación de servicios a la Universidad.

No se considera comunicación de datos el acceso que un tercero tenga a los datos personales cuando dicho acceso sea necesario para la prestación de un servicio a la Universidad.

La realización de tratamiento de datos por cuenta de terceros deberá estar regulada mediante un contrato escrito que deberá contener expresamente que el encargado del tratamiento de los datos únicamente los tratará conforme a las instrucciones de la Universidad y que no los aplicará o utilizará con fines distintos a los que figuren en dicho contrato, ni los comunicará o conservará. El encargado del tratamiento de datos de la Universidad será también responsable en caso de incumplimiento a las estipulaciones establecidas, por lo que en el mismo contrato se establecerán, además, las medidas de seguridad que el encargado del tratamiento está obligado a implementar.

Una vez cumplida la relación contractual, los datos de carácter personal deberán ser destruidos o devueltos a la Universidad, al igual que cualquier soporte o documento en el que conste algún dato de carácter personal. No se procederá a la destrucción de los datos si existiere alguna previsión legal que exija su conservación, en cuyo caso deberá hacerse la devolución de los mismos a la Universidad.

Artículo 15. Derecho de acceso.

El interesado tendrá derecho de solicitar y obtener información se sus datos de carácter personal sometidos a tratamiento, así como el origen de los datos y las comunicaciones realizadas o por realizarse.

La universidad resolverá sobre la solicitud de acceso en el plazo máximo de quince días a contar a partir de la recepción de la solicitud. En el caso de que la Universidad no disponga datos de carácter personal del interesado, se le hará saber dentro del mismo plazo.

Podrá denegarse el acceso en los supuestos en los que así lo prevea una ley.

Artículo 16. Derecho de rectificación y cancelación.

La Universidad deberá hacer efectivo el derecho de rectificación o cancelación de los datos del interesado dentro del plazo de diez días. En el caso de que la Universidad no cuente con dichos datos lo deberá comunicar al interesado dentro del mismo plazo.

La cancelación de los datos dará lugar al bloqueo de los mismos, conservándolos únicamente para ponerlos a disposición de órganos jurisdiccionales competentes en virtud de posibles responsabilidades nacidas del tratamiento de dichos datos, dicha conservación subsistirá hasta la prescripción de las posibles responsabilidades. Cumplido dicho plazo deberá procederse a la supresión.

Pueden negarse la cancelación y la rectificación de los datos en tanto que una ley así lo disponga. Si los datos hubiesen sido comunicados previamente, la Universidad deberá comunicar de su cancelación o rectificación.

Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o a las relaciones contractuales entre la Universidad y el interesado.

TÍTULO III

Gestión de los archivos con datos de carácter personal

Capítulo I

Disposiciones generales

Artículo 17. Procedimiento de creación, modificación o supresión de archivos.
La creación, modificación o supresión de archivos de la universidad corresponde a la autoridad de cada unidad, departamento o dependencia en la que se deberá tomar en cuenta las disposiciones siguientes:

- Identificar el archivo, indicando su denominación, así como la descripción de su finalidad y usos previstos.
- Indicar el origen de los datos, el colectivo de personas sobre los que se pretende obtener los datos, el procedimiento utilizado para su recogida y su procedencia.
- Indicar la estructura básica del archivo mediante la descripción detallada de los datos identificativos, así como las categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización.

- Indicar las comunicaciones de datos que se tengan previstas con los destinatarios o categorías de destinatarios.
- Indicar las medidas de seguridad que se tomarán para la protección de los datos contenidos en dicho archivo.
- En las disposiciones de supresión se deberá indicar el destino que se le dará a los datos o en su caso las previsiones que se adoptarán en su destrucción.
- Cada archivo tendrá un responsable interno nombrado por la autoridad superior de cada dependencia, unidad o departamento.

Artículo 18. Niveles de seguridad.

Con el objeto de aumentar las garantías en el tratamiento de los datos de carácter personal, la Universidad implementará medidas de seguridad en los niveles medio y alto.

Dichos niveles se establecerán según la naturaleza de la información tratada y en relación a la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información.

Artículo 19. Aplicación de los niveles de seguridad.

Todos los archivos que contengan datos de carácter personal deberán adoptar las medidas de seguridad calificadas como medias.

Los archivos que contengan datos sobre ideologías, afiliación sindical o salud, deberán, además de reunir las medidas de seguridad de nivel medio, las calificadas de nivel alto. Cuando en un sistema de información existan archivos o tratamientos de datos que en función de su finalidad o naturaleza de los datos que contengan requieran de la aplicación de un nivel de medidas de seguridad diferente al sistema principal, podrán dividirse de este último, siendo de aplicación en cada caso el nivel de medidas de seguridad correspondientes.

Artículo 20. Responsable de seguridad

Todos los archivos de la Universidad deberán tener uno o varios responsables de seguridad encargados de controlar y coordinar las medidas de seguridad definidas para cada archivo.

Cada encargado responsable deberá ser apto y poseer grado académico que demuestre su conocimiento en materia de protección de datos personales y seguridad informática.

Artículo 21. Documento de seguridad.

La Universidad debe implementar la normativa de seguridad mediante un documento de cumplimiento obligatorio para el personal con acceso a los datos de carácter personal y a los sistemas de información.

Como mínimo éste documento debe contener:

- Especificación detallada de los recursos protegidos.

- Medidas y procedimientos de actuación encaminados a garantizar el nivel de seguridad exigido en este reglamento.
- Obligaciones y funciones del personal.
- Estructura de los archivos con datos de carácter personal y descripción de los sistemas de información que los tratan.
- Procedimientos de realización de copias de respaldo y de recuperación de los datos.
- Controles periódicos que se deban realizar para verificar el cumplimiento de los dispuesto en el propio documento de seguridad.
- Medidas a adoptar para el transporte de soportes y documentos.
- Medidas a adoptar para la destrucción o reutilización de los documentos y soportes.

El documento de seguridad debe mantenerse actualizado en todo momento y será revisado siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en el contenido de la información incluida en los archivos como consecuencia de los controles periódicos realizados. Se entenderá como un cambio relevante aquel que pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.

El contenido del documento de seguridad debe adecuarse en todo momento a las disposiciones vigentes en materia de seguridad de los datos personales.

Capítulo II

Medidas de seguridad de nivel medio

Artículo 22. Identificación y autenticación.

El responsable interno del archivo deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.

Se debe establecer un mecanismo que permita la identificación de forma inequívoca y personalizada de todo usuario que intente acceder al sistema de información y la verificación de que está autorizado.

Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento que garantice su confidencialidad e integridad. Las contraseñas deberán cambiarse con periodicidad la cual será determinada en el documento de seguridad, que en ningún caso será superior a un año y deberán ser almacenadas de forma ininteligible.

Artículo 23. Control de acceso.

Los usuarios deben tener acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.

El responsable interno del archivo se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios y los accesos autorizados para cada uno de ellos.

Se deben establecer mecanismos para evitar que un usuario pueda acceder a datos o recursos con derechos distintos de los autorizados.

Exclusivamente el personal autorizado establecido en el documento de seguridad podrá conceder, anular o alterar el acceso autorizado sobre los datos y recursos conforme a los criterios establecidos por el responsable interno del archivo en el documento de seguridad.

Artículo 24. Control de acceso físico.

Únicamente el personal autorizado en el documento de seguridad podrá tener acceso a los locales donde se hallen instalados los equipos físicos que den soporte a los sistemas de información.

Los elementos, archivadores u otros en los que consten documentos con carácter personal deberán encontrarse en áreas en donde el acceso esté protegido. Asimismo, los sistemas y recursos informáticos en donde se encuentren datos personales deberán estar asegurados con todas aquellas protecciones informáticas actualizadas y con equipos especializados y adecuados para brindar tal seguridad.

Artículo 25. Copias de respaldo y recuperación.

Se deben establecer procedimientos de actuación para la realización de copias de respaldo. Asimismo, se establecerán procedimientos para la recuperación de los datos que puedan garantizar en todo momento su reconstrucción al estado en que se encontraban al tiempo de la pérdida o destrucción.

El responsable del archivo se encargará de verificar cada seis meses el correcto funcionamiento y aplicación de los procedimientos de aplicación para la realización de copias de respaldo y de recuperación de datos.

Se deberá conservar una copia de respaldo y de los procedimientos de recuperación de los datos en un lugar diferente de aquél en que se encuentren los equipos informáticos que los tratan.

Artículo 26. Acceso a datos a través de redes de comunicaciones.

La transmisión de datos personales a través de redes públicas o inalámbricas de comunicaciones electrónicas se debe realizar cifrando dichos datos o utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulable por terceros.

Artículo 27. Auditoría.

Los sistemas de información y los lugares en donde se lleve a cabo el tratamiento y almacenamiento de datos se someterán a una auditoría externa anual que verifique el cumplimiento del presente reglamento y de los procedimientos vigentes en materia de seguridad informática y protección de datos personales.

Se deberá emitir un informe de la auditoría sobre la adecuación de las medidas y controles al presente reglamento e identificar sus deficiencias y proponer medidas correctoras o complementarias necesarias. Se deben incluir además datos, hechos y observaciones en que se base el dictamen alcanzado y las recomendaciones

propuestas. Estos informes se deberán remitir al responsable de seguridad competente, quien lo analizará y elevará las conclusiones al responsable interno del archivo o tratamiento de datos de la Universidad.

Capítulo III

Medidas de seguridad de nivel alto

Artículo 28. Gestión y distribución de soportes.

La identificación de los soportes deberá realizarse por un sistema comprensible y con significado que permita a los usuarios con acceso autorizado a los citados soportes y documentos, identificar su contenido y asimismo dificulten la identificación para el resto de personas.

La distribución de los soportes que contengan datos personales se realizará cifrando dichos datos o utilizando otro mecanismo que garantice que dicha información no se inteligible ni manipulada durante su transporte.

Artículo 29. Registro de accesos.

De cada acceso se guardarán como mínimo, la identificación del usuario, fecha y hora en que se realizó, el fichero accedido, tipo de acceso y si dicho acceso fue aceptado o denegado.

Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente. El responsable de seguridad se encargará de

revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y problemas detectados.

Artículo 30. Acceso a la documentación.

El acceso a la documentación se limitará exclusivamente al personal autorizado.

Se deberán establecer mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios.

TÍTULO IV

Disposiciones finales

Artículo 31.

El presente reglamento será de aplicación general a la Universidad de San Carlos de Guatemala, a sus dependencias, unidades, departamentos, direcciones y centros universitarios departamentales.


SECRETARIA
GUATEMALA, C. A.

CONCLUSIÓN DISCURSIVA

Se considera que una de las herramientas más importantes producida en el siglo XX ha sido el computador, y por lo tanto este ha provocado cambios enormes en la sociedad. En la actualidad, el entorno está prácticamente rodeado por las nuevas tecnologías y a medida que transcurre el tiempo avanzan sin límites y en ocasiones son utilizadas de forma incorrecta, provocando así daños de grandes dimensiones. Aunque se ha ampliado la posibilidad de interconectarse a través de redes, ésta a su vez, lógicamente ha traído consigo la aparición de nuevas amenazas para los sistemas de información por lo que es de suma importancia iniciar una búsqueda de los medios que permitirían combatir tales riesgos y fortalecer así mismo la seguridad de los medios y sistemas informáticos que se estén utilizando. Con la constante evolución de las computadoras es fundamental saber qué recursos se necesitan para obtener seguridad en los sistemas de información.

En el desarrollo del presente trabajo también se ha llegado a la conclusión que, en Guatemala dentro del ámbito de la educación superior, no se ha implementado el uso de políticas internas para la protección de los datos de carácter personal, así como tampoco se ha preocupado por brindar seguridad informática a cada uno de los usuarios.

Al observar y conocer todos los riesgos que se corren sin una protección a los datos personales y sin una adecuada seguridad informática, específicamente aplicándolo al área de la educación superior, además de conocer que en Guatemala ninguna

universidad lo ha implementado, como Universidad del Estado de Guatemala, la Universidad de San Carlos debe implementar dentro de su normativa interna un reglamento que contenga las políticas necesarias y adecuadas para poder brindar seguridad informática dentro de la institución y sus dependencias, así como proteger los datos personales, tanto de los estudiantes como de docentes, personal administrativo y demás trabajadores. Por lo tanto, se hace un llamado al Consejo Superior Universitario, como ente superior de la Universidad de San Carlos de Guatemala y en atención a sus atribuciones especificadas en la ley, para que se inicie el trámite correspondiente para la implementación de la normativa interna en relación a la seguridad informática y la protección de los datos personales dentro de la misma universidad.

ANEXOS

ANEXO I

Glosario de términos informáticos

Buffer: Espacio de memoria que se utiliza como regulador y sistema de almacenamiento intermedio entre dispositivos de un sistema informático.

Ciberespacio: nuevo espacio virtual, poblado por millones de datos, en el que se puede «navegar» infinitamente en busca de información. Se trata, en una contracción de cibernética y espacio.

Corta fuegos: Es un ordenador o un programa que conecta una red a Internet, pero impide el acceso no autorizado desde Internet. Es un mecanismo que permite que las comunicaciones entre una red local e Internet se realicen conforme a las políticas de seguridad de quien los instala. Estos sistemas suelen incorporar elementos que garantizan la privacidad, auntentificación, etc., con lo que se impide el acceso no autorizado desde Internet.

Criptografía: Ciencia que estudia la manera de cifrar y descifrar los mensajes para que resulte imposible conocer su contenido a los que no dispongan de unas claves determinadas.

Firewalls: ver cortafuegos.

Hacker: Usuario de ordenadores especializado en penetrar en las bases de datos de sistemas informáticos estatales con el Fin de obtener información secreta. En la actualidad, el término se identifica con el de delincuente informático, e incluye a los

cibernautas que realizan operaciones delictivas a través de las redes de ordenadores existentes.

Malware: Programa maligno. Son todos aquellos programas diseñados para causar daños al hardware, software, redes. Es un término común que se utiliza al referirse a cualquier programa malicioso.

Ordenador: Dispositivo electrónico compuesto básicamente de procesador, memoria y dispositivos de entrada/salida. Poseen parte física (hardware) y parte lógica (software), que se combinan entre sí para ser capaces de interpretar y ejecutar instrucciones para las que fueron programadas.

Protocolo: Se denomina protocolo a un conjunto de normas y/o procedimientos para la transmisión de datos que ha de ser observado por los dos extremos de un proceso comunicacional (emisor y receptor). Estos protocolos «gobiernan» formatos, modos de acceso, secuencias temporales, etc. Un protocolo es el lenguaje (conjunto de reglas formales) que permite comunicar nodos (computadoras) entre sí.

Red: Una red de computadoras es una interconexión de computadoras para compartir información, recursos y servicios. Esta interconexión puede ser a través de un enlace físico (alambrado) o inalámbrico.

Spyware: Los programas espía o spyware son aplicaciones que recopilan información sobre una persona u organización sin su conocimiento.

TIC: Las tecnologías de la comunicación (TIC), se encargan del estudio, desarrollo, implementación, almacenamiento y distribución de la información mediante la utilización de hardware y software como medio de sistema informático.

Virus: Es un programa informático que se ejecuta en el ordenador sin previo aviso y que puede corromper el resto de los programas, ficheros de datos e, incluso el mismo sistema operativo.

BIBLIOGRAFÍA

BARRIOS OSORIO, Omar Ricardo. **Derecho e informática. Aspectos fundamentales.** Guatemala: Ed. Mayté, 2006.

BARRIOS OSORIO, Omar Ricardo. **Introducción de las nuevas tecnologías en el Derecho.** Guatemala: 1ª Ed., 2010. (s.e).

DAVARA RODRÍGUEZ, Miguel Ángel. **Manual de protección de datos.** Ed. Aranzadi, 2ª Ed, 2008. (s.l.i).

file:///C:/Users/nj152/Downloads/Codigo_de_conducta_de_proteccion_de_datos_personales_en_la_UCLM.pdf. (Consultado: 20 de noviembre de 2016).

GÓMEZ VIEITES, Álvaro. **Enciclopedia de la seguridad informática.** Madrid, España: Ed. RA-MA, 2011.

http://definicion.de/derecho/. (Consultado: 6 de junio de 2016).

http://dle.rae.es/?w=diccionario. (Consultado: consultado 2 de junio de 2016).

http://estudianteigv.galeon.com/. (Consultado: 13 de junio de 2016).

http://redusacunoc.tripod.com/HISTORIA_USAC.html. (Consultado: 20 de enero de 2017).

http://www.unal.edu.co/contenido/habeas/POLITICA%20DE%20TRATAMIENTO%20DE% 20DATOS. (Consultado: 22 de octubre de 2016).

https://es.wikipedia.org/wiki/Ciencia. (Consultado: 6 de junio de 2016).

https://es.wikipedia.org/wiki/Derecho_inform%C3%A1tico. (Consultado: 12 de junio de 2016).

https://es.wikipedia.org/wiki/Sistema_inform%C3%A1tico. (Consultado: 4 de junio de 2016).

https://es.wikipedia.org/wiki/Tecnolog%C3%ADa. (Consultado: 4 de junio de 2016).

https://protecciondatos.unizar.es/sites/protecciondatos.unizar.es/files/users/lopd/Resolucion20020606modificada%20con%202015.pdf. (Consultado: 2 de diciembre de 2016).

http://repository.unimilitar.edu.co/bitstream/10654/12251/1/ENSAYO%20FINAL.pdf. GONZÁLEZ AGUDELO, Daniel Felipe. **El riesgo y la falta de políticas de seguridad informática una amenaza en las empresas certificadas base**. (Consultado: 2 de febrero de 2017).

https://rua.ua.es/dspace/bitstream/10045/13057/7/TEMA%206%20RJB%20%20La%20protecci% C3%B3n%20jur%C3%ADdica%20del%20software.pdf. (Consultado: 12 de agosto de 2016).

https://www.upv.es/entidades/ASIC/normativa/normativa_servicios_ c.pdf. (Consultado: 5 de enero de 2017).

SOLANO BÁRCENAS, Orlando. **Manual de informática jurídica.** Santa Fe de Bogotá D.C. Colombia: Ed. Jurídica Gustavo Ibáñez, 1997.

Legislación

Constitución Política de la República de Guatemala. Asamblea Nacional Constituyente, 1986.

Ley de Acceso a la Información Pública. Decreto 57-2008, 2008.

Ley de Derechos de Autor y Derechos Conexos. Decreto No. 33-98, 1998. Modificado por el Decreto 56-2000, 2000.

Tratado sobre Derechos de Autor de la Organización Mundial de la Propiedad Intelectual, adoptado el 20 de diciembre de 1996.

Ley Orgánica de la Universidad de San Carlos de Guatemala. Decreto No. 325, 1947.

Estatuto de la Universidad de San Carlos de Guatemala. 2001.