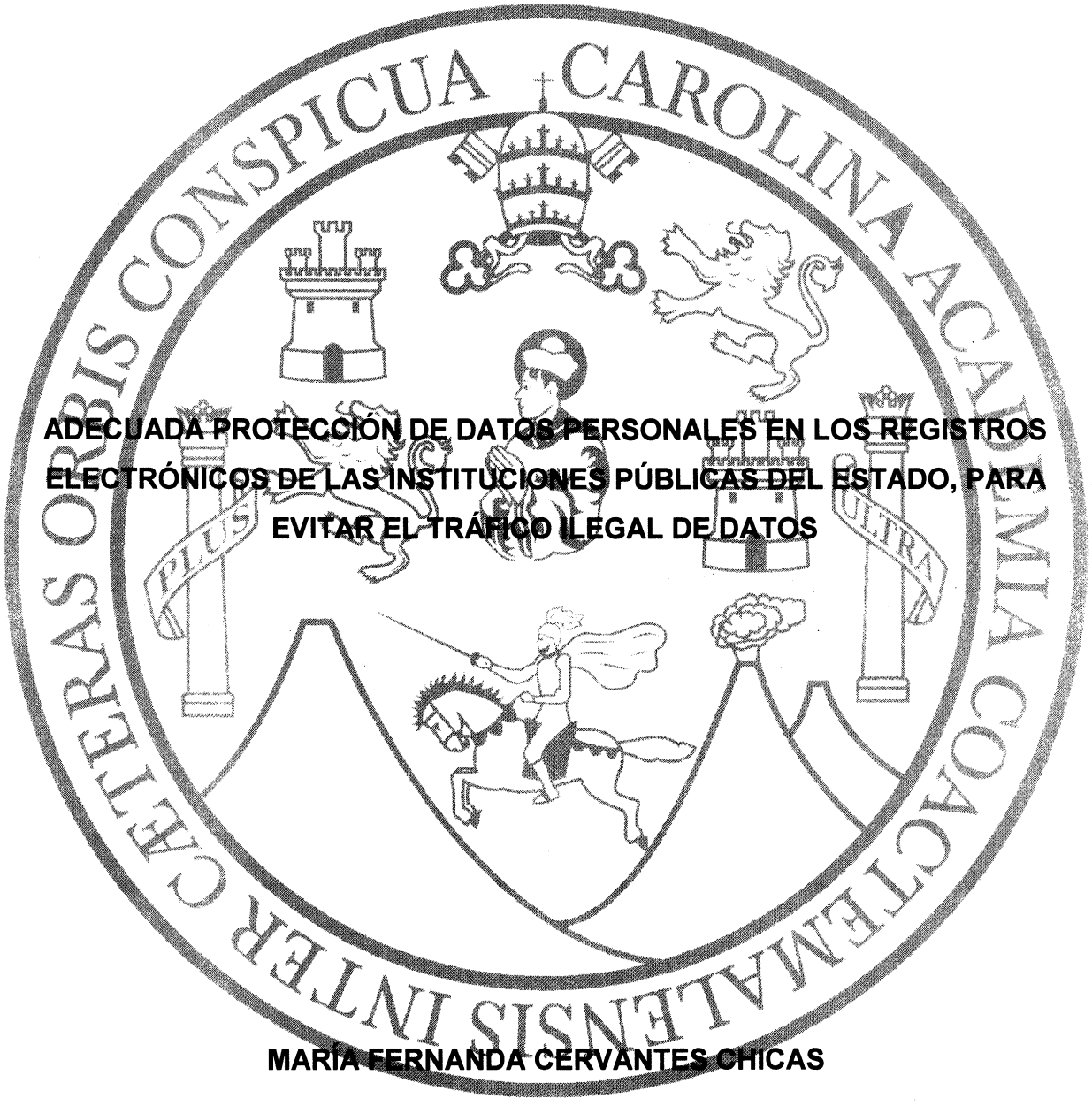
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES



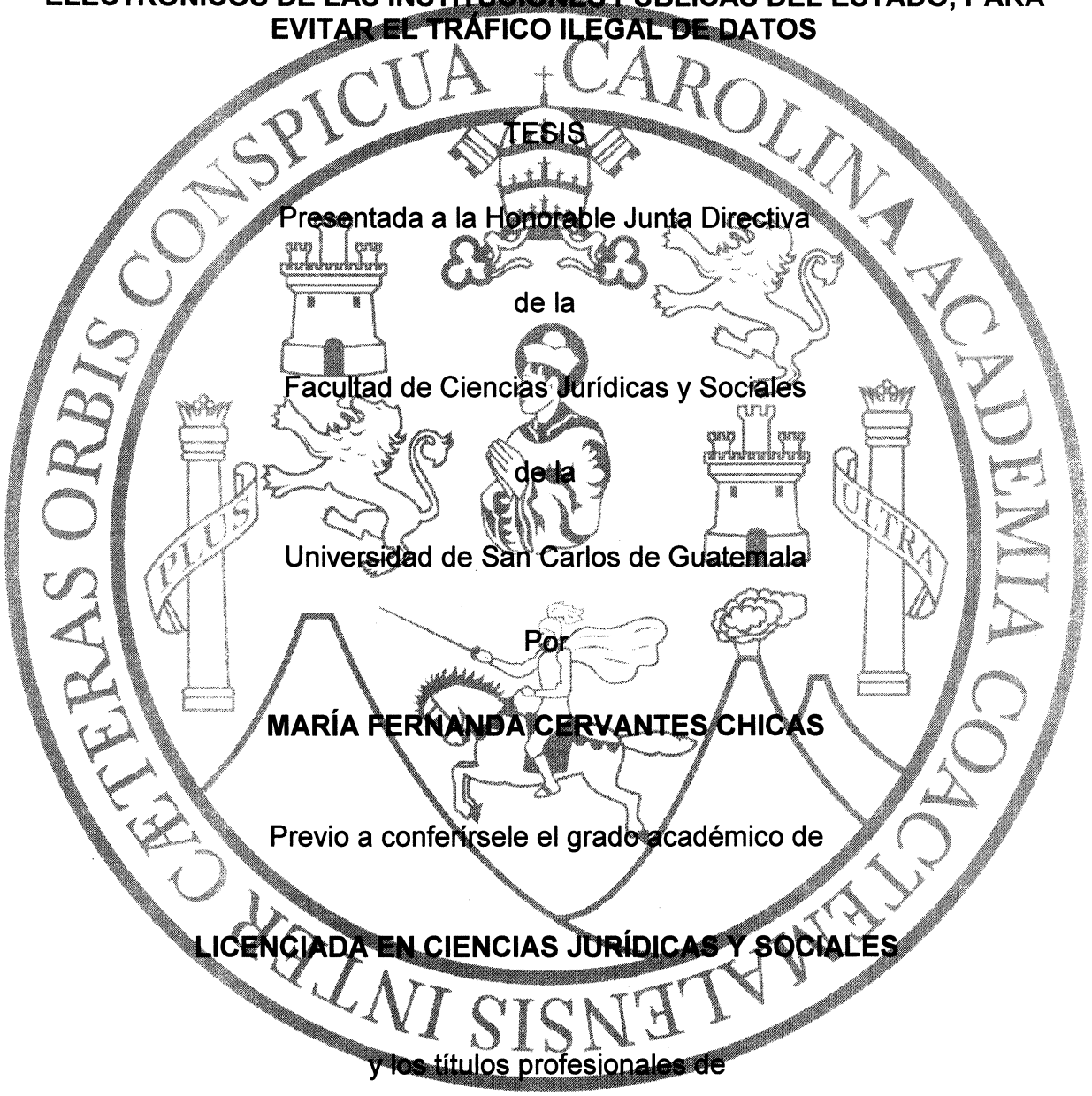
ADECUADA PROTECCIÓN DE DATOS PERSONALES EN LOS REGISTROS ELECTRÓNICOS DE LAS INSTITUCIONES PÚBLICAS DEL ESTADO, PARA EVITAR EL TRÁFICO ILEGAL DE DATOS

MARÍA FERNANDA CERVANTES CHICAS

GUATEMALA, NOVIEMBRE 2019

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

ADECUADA PROTECCIÓN DE DATOS PERSONALES EN LOS REGISTROS ELECTRONICOS DE LAS INSTITUCIONES PÚBLICAS DEL ESTADO, PARA EVITAR EL TRÁFICO ILEGAL DE DATOS



TESIS

Presentada a la Honorable Junta Directiva

de la

Facultad de Ciencias Jurídicas y Sociales

de la

Universidad de San Carlos de Guatemala

Por

MARÍA FERNANDA CERVANTES CHICAS

Previo a conferírsele el grado académico de

LICENCIADA EN CIENCIAS JURÍDICAS Y SOCIALES

y los títulos profesionales de

ABOGADA Y NOTARIA

Guatemala, noviembre 2019

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:	Licda. Astrid Jeannette Lemus Rodríguez
VOCAL II:	Lic. Henry Manual Arriaga Contreras
VOCAL III:	Lic. Juan José Bolaños Mejía
VOCAL IV:	Br. Denis Ernesto Velásquez González
VOCAL V:	Br. Abidán Carías Palencia
SECRETARIO:	Lic. Fernando Antonio Chacón Urízar

TRIBUNAL QUE PRACTICÓ EL
EXAMEN TÉCNICO PROFESIONAL

Primera Fase:

Presidente:	Lic. Jorge Eduardo Avilés Salazar
Vocal:	Lic. José Miguel Cermeño Castillo
Secretario:	Lic. Marvin Omar Castillo García

Segunda Fase:

Presidente:	Licda. Olga Aracely López Hernández
Vocal:	Lic. Luis Fernando Hernández Recinos
Secretario:	Lic. Mynor Rafael Prado Jacinto

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

USAC
TRICENTENARIA
Universidad de San Carlos de Guatemala

Facultad de Ciencias Jurídicas y Sociales
Universidad de San Carlos de Guatemala
SECRETARIA
Guatemala, C. A.

Facultad de Ciencias Jurídicas y Sociales, Unidad de Asesoría de Tesis. Ciudad de Guatemala, 16 de agosto de 2018.

Atentamente pase al (a) Profesional, **OTTO RENE ARENAS HERNÁNDEZ**, para que proceda a asesorar el trabajo de tesis del (a) estudiante **MARÍA FERNANDA CERVANTES CHICAS**, con carné **201312999**, intitulado **ADECUADA PROTECCIÓN DE DATOS PERSONALES EN LOS REGISTROS ELECTRÓNICOS DE LAS INSTITUCIONES PÚBLICAS DEL ESTADO, PARA EVITAR EL TRÁFICO ILEGAL DE DATOS.**

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.

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FAC. DE C.C. J.J. Y S.S.
UNIDAD DE ASESORIA DE TESIS
GUATEMALA, C. A.

LIC. ROBERTO FREDY ORELLANA MARTÍNEZ
Jefe(a) de la Unidad de Asesoría de Tesis

Fecha de recepción 05 / 09 / 2019. f)

Asesor(a)
(Firma y Sello)

LIC. OTTO RENE ARENAS HERNÁNDEZ
ABOGADO Y NOTARIO

Lic. Otto Rene Arenas Hernández
Abogado y Notario
Colegiado 3805

Guatemala, 5 de septiembre de 2019

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

Señor Jefe de la Unidad de Asesoría de Tesis:

De manera atenta me dirijo a usted, a efecto de hacer de su conocimiento que de conformidad con el nombramiento emitido por esta jefatura de fecha dieciséis de agosto de dos mil dieciocho, he procedido a revisar el trabajo de tesis de la bachiller **MARÍA FERNANDA CERVANTES CHICAS**, con número de carnet 20131299, intitulado: "**ADECUADA PROTECCIÓN DE DATOS PERSONALES EN LOS REGISTROS ELECTRÓNICOS DE LAS INSTITUCIONES PÚBLICAS DEL ESTADO, PARA EVITAR EL TRÁFICO ILEGAL DE DATOS**". Acorde a ello, procedí de acuerdo al requerimiento indicado, concluyendo lo siguiente:

a) Con respecto al contenido científico y técnico del trabajo de investigación de tesis, la bachiller realizo un análisis de aspectos actuales de doctrinas y legislación acorde con respecto al contexto del tema de la protección de datos personales en registros electrónicos, empleando un lenguaje apropiado en la redacción, desarrollándose cada una de las fases correspondientes de la investigación.

b) La metodología utilizada en la investigación que permitió la comprobación de la hipótesis, fueron la dialéctica, que permitió la investigación a base de la continua evolución de la tecnología relacionada con el Derecho; la analítica para poder distinguir los elementos que integran la informática jurídica, señalando la importancia de la seguridad informática y la protección de los datos personales; el inductivo por medio de la lógica para establecer las premisas generales de la investigación. La técnica bibliográfica para el desarrollo de la investigación permitió la recolección adecuada de información actual y suficiente.

c) La redacción del trabajo de investigación de tesis es clara, concisa, explicativa y de acuerdo a las reglas gramaticales, habiendo utilizado la bachiller un lenguaje técnico y comprensible para el lector, asimismo, se hizo uso de las reglas ortográficas de la Real Academia Española.

d) El informe final de tesis es una contribución científica para la sociedad y la legislación guatemalteca, en donde la bachiller señala la vulneración por la falta de protección

jurídica de los datos personales, siendo un tema importante que no ha sido suficientemente investigado. En todo caso puede servir como material de consulta para futuras investigaciones.

e) En la conclusión discursiva, la bachiller expone sus puntos de vista sobre la problemática sobre la seguridad informática en cuanto a los datos personales, determinando la importancia de la adecuada protección de los datos personales en los registros públicos como el Registro Nacional de las Personas de Guatemala, por medio de una adecuación legislativa para procurar la protección de los derechos fundamentes inherentes que amparan los datos personales.

f) La bibliografía utilizada fue acorde al tema de investigación, en virtud que se consultaron exposiciones temáticas de autores nacionales como extranjeros, cuyas teorías fueron de utilidad para sustentar y fortalecer el contenido de la investigación.

g) Se realizaron algunas sugerencias y recomendaciones en el contenido capitular, necesarias para una mejor comprensión del tema, las cuales fueron atendidas por la bachiller, respetando al mismo tiempo sus opiniones.

De acuerdo con lo expuesto, es menester declarar expresamente que no soy pariente dentro de los grados de ley de la bachiller MARÍA FERNANDA CERVANTES CHICAS.

Por las razones mencionadas, hago de su conocimiento que el trabajo de investigación de tesis cumple con todos los requisitos estipulados en el Artículo 31 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público; por lo que emito **DICTAMEN FAVORABLE**, para que pueda continuar con trámite correspondiente.

Atentamente,

Lic. Otto Rene Arenas Hernández
Abogado y Notario
Asesor de Tesis
Colegiado 3805

LIC. OTTO RENE ARENAS HERNÁNDEZ
ABOGADO Y NOTARIO

Universidad de San Carlos de Guatemala
Unidad de Asesoría de Tesis
Lic. Roberto Fredy Orellana Martínez
JEFE
Facultad de Ciencias Jurídicas y Sociales

DECANATO DE LA FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES. Guatemala, 19 de septiembre de 2019.

Con vista en los dictámenes que anteceden, se autoriza la impresión del trabajo de tesis de la estudiante MARÍA FERNANDA CERVANTES CHICAS, titulado ADECUADA PROTECCIÓN DE DATOS PERSONALES EN LOS REGISTROS ELECTRÓNICOS DE LAS INSTITUCIONES PÚBLICAS DEL ESTADO, PARA EVITAR EL TRÁFICO ILEGAL DE DATOS. 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/JP.

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: Quien me ha concedido la vida, inteligencia y sabiduría para poder desarrollarme, me fortalece día a día y por estar siempre conmigo.

A MIS PADRES: Fernando Arturo Cervantes Chacón y Marcia Yanira Chicas Castro, gracias por ser mi apoyo y brindarme educación, sin ustedes no podría estar aquí, toda meta que he logrado cumplir es también gracias a ustedes.

A MI HERMANO: Fernando Antonio Cervantes Chicas, no soy la mejor hermana del mundo, pero deseo que todos tus metas y anhelos se cumplan y seas un hombre de éxito.

A MI FAMILIA: Especialmente a mis tías Mercedes Cervantes Chacón y Patricia Cervantes Chacón gracias por su cariño y soporte; y a Mario Gordillo Galindo, Patricia Gordillo Cervantes, Mario Estuardo Gordillo Cervantes, Griselda Chicas Castro, Maribel Castro, quienes me han brindado su apoyo y son personas a quienes aprecio con todo mi corazón

A: Mynor Alfredo Ortíz Álvarez, gracias por formar parte de mi vida, por tu apoyo, por estar a mi lado y los momentos compartidos a lo largo de nuestra preparación profesional.

A: María Magdalena Escalante, gracias por cuidarme y defenderme desde pequeña.

A MIS AMIGOS: Gracias por todos los momentos compartidos, el apoyo y cariño demostrado, especialmente a Leticia del Rosario Ruiz Marroquín, gracias por tu amistad a través de los años.

ESPECIALMENTE A: Licda. Eloísa Mazariegos Herrera, Lic. Ricardo Alvarado Sandoval, Lic. Ricardo Ruiz, gracias por sus enseñanzas, apoyo y consejos.

A: La tricentenaria y gloriosa Universidad de San Carlos de Guatemala, alma mater, que me acogió para poder cumplir mis metas profesionales.

A: La tricentenaria Facultad de Ciencias Jurídicas y Sociales, por enseñarme grandes lecciones y conocimientos para formar mi vida profesional con los valores de servicio a la sociedad.

A: La Jornada Matutina, especialmente al Lic. Rafael Godínez, Lic. Gino Alessandro Ponce Vargas y Licda. Vera Analis Valvert Gamboa, por sus conocimientos brindados en la formación de mi carrera profesional.

PRESENTACIÓN

La preservación y adecuada protección de datos personales, por ser estos considerados internacionalmente como derechos humanos inherentes, deben considerarse como prioridad estatal en el control del acceso, manejo y utilización estos. Esto principalmente por el uso acelerado de la tecnología, que ha producido el involucramiento del derecho en la informática, surgiendo así, la informática jurídica como una herramienta al derecho en la sistematización de datos en instituciones estatales, tales como registros electrónicos.

En relación a lo expuesto anteriormente, la presente investigación, se enfoca en la determinación de las vulnerabilidades existentes en la legislación guatemalteca, y las consecuencias jurídicas y morales, derivado de los daños y perjuicios a sistemas informáticos de registros electrónicos como el Registro Nacional de las Personas de Guatemala, o bien, a las personas titulares del derecho, y por otra parte, los ataques cibernéticos a los cuales se encuentran expuestos los sistemas por la inadecuada protección de estos, en el término de los años 2015 al 2018.

HIPÓTESIS

En el Registro Nacional de las Personas de Guatemala, no existe una normativa jurídica adecuada ni estándar sobre el manejo de almacenamiento y preservación de los datos personales contenidos en la base de datos del sistema informático, así como su adecuada protección.

Al mismo tiempo, la ausencia de determinación de las consecuencias jurídicas por el inadecuado manejo, sustracción, perdida y tráfico ilegal de datos personales, produce vulnerabilidad jurídica en la seguridad informática de los sistemas informáticos, la cual debe ser garantizada por el Estado de Guatemala en los registros públicos, según sus deberes y fines constitucionales.

COMPROBACIÓN DE HIPÓTESIS

Al concluir esta investigación, se determinó que en efecto, el inadecuado manejo y protección de datos personales contenidos en el sistema informático de registros públicos del Estado, como el Registro Nacional de las Personas de Guatemala, se deriva de la ausencia normativa en la cual se contemple sobre la protección de estos, la determinación de responsabilidad jurídica a consecuencia de conductas antijurídicas, y coercitividad normativa ante los ataques al sistema informático, sustracción o pérdida, con o sin acceso autorizado al sistema, y así como el tráfico ilegal de datos personales. Derivado de lo anterior, se considera como comprobada la hipótesis.

Para la comprobación de la hipótesis, la metodología utilizada para su demostración fue por medio de la dialéctica, pues se han tomado en cuenta en la presente investigación la continua evolución tecnológica y el Derecho como parte de esta; la analítica, distinguiéndose cada uno de los elementos que conforman el derecho informático para arribar a la seguridad informática y protección de datos personales; y el método inductivo, partiendo de conceptos específicos para finalmente arribar en premisas generales por medio de la lógica.

Este estudio es de tipo cualitativo, lo que permite la interpretación y análisis de elementos que conforman el derecho informático, para determinar el adecuado manejo de datos. asimismo, se encuentra enfocada en las áreas del Derecho Informático, Derecho administrativo y del Derecho Penal.

ÍNDICE

Pág.

CAPÍTULO III

CAPÍTULO IV

CAPITULO V

INTRODUCCIÓN

La ausencia de normativa con respecto a la protección de datos en el sistema jurídico de Guatemala, desde el enfoque del manejo, uso y acceso de estos, representa la vulnerabilidad a la que se encuentran expuestos los sistemas informáticos de instituciones estatales, así como la trasgresión de derechos humanos fundamentales, partiendo de la autodeterminación informativa con el que cuenta toda persona. Los ataques o amenazas a los sistemas informáticos son aspectos que importan a la seguridad informática, y al mismo tiempo al Derecho, a consecuencia de las conductas antijurídicas que se traducen en afectaciones a la sociedad y los sistemas de los registros electrónicos de instituciones públicas del Estado, como el Registro Nacional de las Personas de la República de Guatemala, que maneja la mayor base de datos personales.

Los objetivos se encuentran orientados en la determinación de la existencia de vulnerabilidad en la seguridad informática en los registros que resguardan datos personales, por el no establecimiento de normas de carácter jurídico destinadas al debido manejo y protección de datos personales, así como, coadyuvar en la demostración de la desprotección jurídica en la seguridad informática con la que cuentan los registros y dar a conocer las falencias legales con sus posibles soluciones, los cuales fueron comprobados en la presente investigación.

En cuanto a la hipótesis, se demuestra si en el Registro Nacional de las Personas de Guatemala, no existe normativa jurídica sobre el manejo de almacenamiento y preservación de los datos personales en los sistemas informáticos, misma que se encuentra comprobada.

Esta investigación comprende de cinco capítulos, los cuales son: capítulo I, que abarca la relación del derecho con la informática, antecedentes y clasificación; capítulo II, en que se desarrolla la seguridad informática, definición, objetivos, técnicas, estrategias y políticas, tanto a nivel internacional como nacional; en el capítulo III, se aborda el derecho informático en el derecho internacional; en el capítulo IV, se enfoca en Registro Nacional de las Personas de Guatemala, desde la perspectiva del manejo de datos personales, registro electrónico, el manejo de seguridad informática y los antecedentes de los mismos; y por último, en el capítulo V, que expone el análisis de la protección jurídica de los datos personales contenidos en los registros electrónicos de las instituciones públicas del Estado, contemplando la vulnerabilidad jurídica de los datos personales, el tráfico ilegal de datos personales, su adecuado manejo y la responsabilidad jurídica del inadecuado uso y manejo.

Los métodos y técnicas empleados para este estudio, fue principalmente el científico, por medio de la recolección de la información a través de las fuentes primarias y secundarias, de consultas bibliográficas y solicitud de información a instituciones estatales, a través del método analítico, para la transformación de la información

CAPÍTULO I

1. El derecho y su relación con la informática

A través de la historia, el desarrollo tecnológico ha sido impulsado siempre por el hombre, especialmente en las últimas décadas teniendo un crecimiento acelerado, derivado de su naturaleza y necesidad descubrir nuevas formas del saber y la comunicación del ser humano, de ello se originan nuevas formas de comunicación por medio del uso de máquinas fabricadas para su agilización, por lo que "la informática surge de la misma inquietud racional del hombre, el cual ante la continua y creciente necesidad de información para una adecuada toma de decisiones, es impulsado a formular nuevos postulados y diseñar nuevas técnicas"[1]. De estas técnicas y herramientas, surge una era digital, el acceso y contacto del hombre con esta, surge lo expuesto por Barrios Osorio como la "sociedad de la información"[2], que conlleva beneficios al desarrollo integral de la sociedad, y se traduce en una necesidad y en un derecho humano reconocido por la comunidad internacional.

El Derecho es entendido como una ciencia, en la cual uno de sus enfoques es la sociedad, la regulación de su conducta, y su desarrollo en cuento a los derechos y

[1] Téllez Valdés, Julio. **Derecho Informático**. Pág. 5
[2] Barrios Osorio, Omar. **Introducción de las nuevas tecnologías**. Pág. 21

obligaciones que se van generando. Por otro lado, la informática, es la ciencia que se encarga del tratamiento automatizado y lógico de la información por medio de las tecnologías de la información y la comunicación, cuya aplicación se encuentra estrechamente relacionada con la mayoría de las actividades del ser humano moderno, por tal razón, se señala que el origen de la palabra informática se deriva de la unión de las palabras información y automática.

Asimismo, el Derecho se involucra en la solución de conflictos que se den en el ámbito de la informática, permitiendo que se provea de seguridad jurídica a las actuaciones que se realicen, coadyuvando en la creación de normas y establecimiento de reglas. Por otro lado, se debe destacar que el Derecho también se ve beneficiado con la informática por su aportación en el procesamiento de datos e información jurídica, proveyéndole un respaldo por medio de la tecnología de la información.

1.1. Antecedentes

La informática y su interrelación con el derecho surgió a partir del siglo XX, no data una fecha exacta de ello, pero Téllez señala que existen ciertos hechos históricos que marcaron un precedente en cuanto al derecho informático, con la obra de Norbert Wiener, Cibernética y sociedad, del año de 1950, en la cual desarrolla un capítulo denominado el Derecho y las comunicaciones. Norbert Wiener expuso que es a través

de las comunicaciones como se da la relación influyente de la cibernética en el ámbito jurídico, y es por los múltiples aportes sobre la cibernética que Norbert Wiener es considerado como el padre de esta disciplina.

Otro importante aporte fue el de Lee Loevinger, con su artículo "*The next step forward* publicado en la revista *Minnesota Law Review* en 1949""[3], por medio del cual, dio a conocer la jurimetría como un conjunto de estudios enfocados en el análisis y tratamiento tecnológico de la información jurídica, así como la implementación de esta disciplina como una herramienta práctica para mejorar los procesos judiciales y superar los problemas que enfrenta la jurisprudencia estática.

Por otro lado, Téllez señala que "a finales de la década de 1960 y luego cerca de diez años de aplicaciones comerciales de las computadoras, empezaron a surgir las primeras inquietudes respecto a eventuales repercusiones negativas motivadas por el fenómeno informático, las cuales requerían un tratamiento especial"[4], por lo que se podría aducir que tales eventos son el inició de la regulación del fenómeno de la informática, surgiendo el derecho a la informática, derecho informático, la cibernética y jurimetía, conceptos que

[3] Acosta Ramírez, René, Verdecia Díaz, Yadirka, y Amoroso Fernández, Yarina. Jurimetría: **Una opción para la sociedad**. http://www.egov.ufsc.br/portal/sites/default/files/1755-6338-1-pb.pdf (Consulta: 3 de diciembre de 2018)
[4] Téllez. **Op. Cit.** Pág. 12

pueden llegar a confundirse y que algunos tratadistas lo consideran como ramas autónomas.

1.2. Derecho informático

El Derecho informático es un área de las ciencias jurídicas relativamente joven, ya que, como se mencionó anteriormente comenzó a desarrollarse a mediados del siglo XX, y cuyos estudios y regulaciones han sido una herramienta para el ser humano moderno en el uso de las tecnologías de la información y la comunicación.

1.2.1. Definición

El Derecho informático se encarga de regular la informática en las diferentes áreas en las que es aplicada, y tal y como lo señala Lucerito, el derecho informático constituye un conjunto de conocimientos, principios, doctrinas, que tienen en su marco estricto de estudio a la *iuscibernética*, y como marco amplio la cibernética, por lo tanto "se obtiene que también constituye una ciencia, que estudia la regulación normativa de la informática su aplicación en todos los campos"[5].

[5] Flores Salgado, Lucerito Ludmina. **Derecho informático**. Pág. 83

Sin embargo, debemos determinar si el derecho informático es un área del derecho autónoma o no autónoma, para ello Héctor Peñaranda citado por Lucerito, hace mención de los supuestos a tomar en cuenta para determinar su autonomía, que son: "Legislación especificada (campo normativo); estudio particularizado de la materia (campo docente); investigaciones, doctrinas que traten la materia (campo científico); e instituciones propias que no se encuentran en otras áreas del derecho (campo institucional)"[6].

Por lo tanto, al realizar un análisis de los supuestos expuestos por Héctor Peñaranda, en Guatemala no se puede considerar al derecho informático como un área jurídica de carácter autónomo, ya que a pesar de que el surgimiento de esta sea consecuencia de los cambios sociales existentes en la materia de la informática y la cibernética, aún no se encuentra completamente desarrollada en los aspectos necesarios para considerarse como independiente y autónoma.

1.3. Derecho de la informática

El surgimiento de esta área se data a partir de la década de 1960, cuando empiezan a producirse las interrogantes de estudiosos y la sociedad, sobre las consecuencias negativas que podían llegar acaecerse por la aplicación de la informática, y es por esta

[6] **Ibid**, Pág. 85

razón que se originó el derecho a la informática como una respuesta social a dichas inquietudes.

El Derecho de la informática es el área que se encuentra dentro del derecho informático, y se encarga de regular todo fenómeno informático que se produce en la sociedad, siendo su objeto de estudio exclusivamente la informática y los problemas que se producen en este ámbito. Por lo que se puede concluir con la siguiente definición dada por Téllez, que concibe esta área como el "conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la informática"[7].

1.4. Informática Jurídica

El nacimiento de la informática jurídica de cómo la conocemos hoy en día se remonta en año de 1959, con los ideales de John Horty, director de la *Health Law Center* de la Universidad de Pittsburgh, que consideraba que era necesario la búsqueda de automatizar el acceso a la información legal, y derivado de ello, fue creado un sistema de "ordenamientos legales de Pensilvania en cintas magnéticas"[8] que posteriormente fue presentado en 1960, ante la Asociación de la Barra Americana (*American Bar Association, ABA),* como un sistema de búsqueda de información legal automatizado.

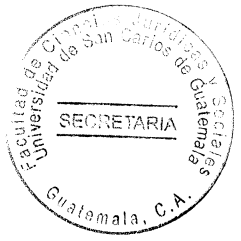
[7] Téllez. **Op. Cit**. Pág. 82
[8] **Ibid**. Pág. 9

La informática jurídica es considerada como una fuente del derecho informático, ya que su ámbito de estudio y regulación, ayuda al desarrollo y aplicación del Derecho en el ámbito tecnológico e informático. Además, se ha convertido en el enlace entre las Tecnologías de la Información y la comunicación, y del Derecho, involucrando a los operadores jurídicos con los avances tecnológicos.

1.4.1. Definición

La informática jurídica como parte del derecho informático se define según Téllez como una "técnica interdisciplinaria que tiene por objeto el estudio e investigación de los conocimientos de la informática general, aplicables a la recuperación de información jurídica, así como la elaboración y aprovechamiento de los instrumentos de análisis y tratamiento de información jurídica necesarios para lograr dicha recuperación"[9]. Por tal motivo, la informática jurídica es considerada un auxiliar del Derecho, en cuanto al tratamiento de información jurídica realizada por medios o aparatos electrónicos físicos.

[9] **Ibid**. Pág. 10



1.4.2. Clasificación

En el desarrollo inicial de la informática jurídica, esta empezó con un enfoque de informática documentaría con carácter jurídico; posteriormente, surgió la idea de desarrollar sistemas para gestionar datos jurídicos con el propósito de facilitar el trabajo de jueces, operadores de justicia, legislativos y funcionarios; por último, se concluye con la observación de procedimientos fidedignos y la efectiva funcionalidad reflejada en la mejora de resultados con la aplicación de la computadora en el ámbito jurídico.

Según lo expuesto, conforme al estudio y desarrollo de la informática jurídica, se advierte que esta se clasifica de la siguiente manera:

A) **Informática jurídica documental o documentaria**. Es conocida por ser la más antigua, y cuya función es la aplicación de técnicas de la informática para realizar procesos automatizados de almacenamiento-recuperación de información jurídica previamente almacenada y la creación de bancos de datos documentales jurídicos para hacer búsquedas de datos de forma eficaz y con mayor rapidez.

B) **Informática jurídica de control, gestión, u ofimática**. A diferencia de la anterior, que se encarga de la conservación de datos, la de control o gestión realiza cosas con los datos, así como la organización y control de información jurídica de

documentos, expedientes o libros. Esta tiene sus orígenes con el surgimiento de la creación y uso de procesadores para búsqueda sistematizada de palabras y de la automatización realizada en los registros públicos. Su ámbito de aplicación se encuentra según Téllez en lo administrativo, judicial, jurídico, registral y en despachos jurídicos, por ejemplo, el Sistema de Gestión de Tribunales que se utiliza en los juzgados de ramo penal en el Organismo Judicial de Guatemala, que ha permitido la agilización de asuntos contenidos en expedientes de juzgados.

C) **Informática jurídica de ayuda a la decisión o metadocumental y metadecisional**. Esta es la informática jurídica conformada por bases de datos constituida con conocimientos jurídicos, cuyo propósito es la solución y auxilio sistemático de problemas jurídicos por medio de la tecnología y las máquinas. En esta "no se facilitan documentos ya almacenados, tales como leyes, sentencias judiciales y pareceres, sino que producen documentos nuevos, diferentes de la base de conocimiento introducida en la máquina"[10], es decir, se perfecciona un conocimiento preorganizado con el que se pretende la creación y uso de inteligencia artificial.

[10] Taddei Elmi, Giancarlo. **Informática y Derecho**. Pág. 152.

1.5. Derecho a la Información

La comunicación ha sido necesidad esencial para el ser humano, misma que le ha servido en la creación de vínculos sociales, de igual manera surge la búsqueda de las personas por estar informadas, que se remota en la antigua Grecia, en la cual no existía libertad de información, ya que esta se encontraba restringida por los tiranos para evitar la criticas de aristas y literatos, reflejándose en una coacción informativa durante la época de Platón, que se caracterizó por el destierro a poetas y artistas, así como la selección de música, por ser considerados una perversión para la juventud.

Posteriormente, con Aristóteles, existió un "modelo comunicacional emergente, que fue el primer modelo experiencial, humanista de opinión"[11]. Por tales razones se ha señalado que el origen de la palabra informar se deriva del vocablo latín *informatio* cuyo significado según el diccionario de la lengua española de la Real Academia Española es dar forma, describir.

El derecho a la información se desarrolló como una libertad a partir de la formación de los Estados modernos, como se ve marcado históricamente a partir de julio de 1789 con la Revolución francesa la cual sentó los las bases para alcanzar las libertades de pensamiento y expresión, las cuales posteriormente, fueron plasmadas tanto en las

[11] Flores Salgado. **Op. Cit**. Pág. 13

legislaciones internas de los Estados, como en legislación internacional, particularmente en: la Declaración de Derechos del Hombre y del ciudadano (26 de agosto de 1789), en la que se reconoce en los artículos 10 y 12 la libertad de expresión; la Asamblea General de la Organización de las Naciones Unidas (1946), se expresó que la libertad de información es uno de los derechos fundamentales del hombre y sin obstáculos; la Declaración Universal de los Derechos del Hombre (10 de diciembre de 1948), en la cual se plasmó el derecho a la libertad de opinión y expresión; la Convención Americana de los Derechos Humanos (1969), en esta se reconoce en su artículo 13, el Derecho a la libertad de pensamiento y de expresiones.

De modo que, este derecho se caracteriza por ser un derecho individual y social, desde la perspectiva de la facultad doble que se desprende del derecho a la información, por un lado el **derecho a dar información,** que se encuentra vinculado con la libertad de opinión y expresión; y por el otro, el **derecho de recibir información**, relacionado con la publicidad de actos de gobierno y particulares qué debe proporcionar el Estado, asimismo, se asocia con el derecho de obtener información de interés público derivado de una gestión ante la Administración Pública, cuyo derecho en la legislación guatemalteca se ve materializado en la Ley de Acceso a la Información Pública, Decreto Número 57-2008 del Congreso de la República de Guatemala.

1.5.1. Los datos

El concepto dato proviene del vocablo latín *datum,* cuyo significado es **lo que se da**, en el ámbito del derecho a la información se trata a los datos como expresiones mínimas de información, que al encontrarse separadas no poseen sentido, sin embargo, en conjunto producen información de la cotidianidad del ser humano.

1.5.2. Tipos de datos

Para establecer una clasificación de tipos de datos, se debe verificar cual será el fin de su uso, de tal manera que se puede concluir en la siguiente división:

A) Según su almacenamiento digital e informático de datos procesados en archivos electrónicos o en bases de datos, estos pueden ser: a) Datos alfanuméricos, b) Datos numéricos, c) Datos lógicos. Esta clase de datos son mayormente utilizados en el ámbito de la informática.

B) Según su relación con la información de las personas:

a) **Datos personales**. Son el tipo de datos que interesa una mayor protección jurídica, pues contienen unidades de información, sensible o no, acerca de las

personas, cuyo uso en redes tecnológicas es frecuente, pues la mayoría de sitios y *software* solicitan el acceso a información personal, además de su uso y almacenamiento en registros automatizados. En la legislación guatemalteca se encuentra definido el concepto de datos personales en el Artículo 9 de la Ley de acceso a la información pública Decreto Número 57-2008 del Congreso de la República, como "cualquier información concerniente a personas naturales identificadas o identificables", siendo esta la única norma ordinaria que abarca los datos personales, no obstante, su protección normativa es insuficiente.

De igual forma, los datos personales se encuentran sub clasificados de la siguiente manera:

i. **Datos personales públicos**. Se refiere a los "descriptores que se encuentran en registros"[12], es decir, toda aquella información que las personas proporcionan para revestir de publicidad datos personales que le dan reconocimiento ante la sociedad.

ii. **Datos personales privados**. Estos son expuestos por el jurista Barrios Osorio como hechos o descriptores regulados y tasados. Estos a su vez pueden ser, **sensibles** cuando se refieren a características personales sobre aspectos físicos o morales acerca de su actuar privado, o **no sensibles** concernientes a características íntimas que tratan sobre la personalidad, creencias e ideologías con una protección más profunda.

[12] Barrios Osorio. **Op Cit.** Pág. 84

1.5.3. Almacenamiento de datos

La automatización de datos trajo consigo la necesidad de resguardar la información obtenida, especialmente la de datos personales, que antes de la era de digitalización de la información, esta era resguardada en libros. Es trabajo de la informática el ingresar la información procesada que ha sido obtenida de datos, para la creación de archivos informáticos en una base de datos, con el fin de ordenarlos y facilitar su posterior acceso.

Un antecedente importante en el mundo jurídico con respecto al almacenamiento sistematizado de datos personales e información jurídica, fue el que se realizó en registros públicos estatales, tales como, registros de la propiedad y registros civiles. Particularmente en Guatemala, la digitalización de información jurídica en el Registro General de la Propiedad se dio a partir de 1996, con la implementación de un sistema operativo electrónico, producto de proyectos de modernización.

En cuanto al almacenamiento de datos personales, en el Registro Nacional de las Personas de Guatemala, se dio a partir de su creación y con la recopilación de información almacenada en Municipalidades del país desde el año 2005, según la Ley del Registro Nacional de las Personas, Decreto Número 90-2005 del Congreso de la República el cual, en el Artículo 2 establece el uso de un sistema automatizado para el procesamiento de datos.

Por consiguiente, se puede afirmar que el almacenamiento de información y datos personales en una base de datos debe ser protegida adecuadamente, para evitar que los datos sean utilizados para fines delictivos, ya sea con intereses personales, o bien, lucrativos.

1.6. Cibernética

El origen etimológico de la palabra cibernética proviene de la voz griega *kybernetes* que se refiere a **piloto de una nave**, y está a su vez se deriva del vocablo *kybenes,* cuya locución hace referencia al **arte de gobernar** o **arte de guiar o dirigir ciertos fenómenos**, y es de estas locuciones fue que Norbert Wiener se basó para el desarrollo de sus estudios matemáticos concluyendo en la cibernética como una ciencia que "se utiliza para describir mecanismos mecánicos o electrónicos que desarrollan procesos"[13].

Como se expuso anteriormente, Norbert Wiener es considerado el padre de la cibernética, ya que desde 1940 inició sus trabajos de investigación, en primer lugar matemáticos orientados a la estadísticas para realizar pronósticos sobre las posiciones de los aviones atacantes del enemigo, durante la Segunda Guerra Mundial, posteriormente, redefinió la cibernética como "el estudio analítico del isomorfismo de la estructura de las comunicaciones en los mecanismos, en los organismos y en las

[13] Alvarado Lemus, José Rolando; Morales Pérez, Ronald Eduardo. **CIBER CRIMEN.** Pág. VIII.

sociedades"[14], de esta forma surgen de la cibernética las siguientes disciplinas: teoría de los sistemas, teoría de la comunicación y teoría de la información.

La cibernética, es reconocida como una ciencia producto de las teorías, campo de estudio y métodos científicos desarrollados para demostrar los fenómenos que se producen en la naturaleza o en la sociedad, así como el comportamiento humano, por medio de la matemática y la computadora. Por tal motivo se le considera como una ciencia con enfoque del control y de la comunicación.

Derivado de lo anterior, se puede definir a la cibernética, en el esquema de la tecnología, como la ciencia que se encuentra conformada por estructuras mecánicas de comunicación y control que se producen entre el hombre y las máquinas.

[14] Ríos Estavillo, Juan José. **Derecho e informática en México: informática jurídica y derecho de la informática**. Pág. 37

CAPITULO II

2. Seguridad informática

La seguridad ha sido siempre para el ser humano una necesidad imprescindible para alcanzar una protección mayor a la libertad y garantizar la estabilidad, cuyo mayor auge se ha dado a partir del surgimiento de los Estados modernos, al incluirse este concepto como un principio o garantía de carácter constitucional. Por tal razón, es el Estado quien debe realizar las acciones dirigidas a garantizar la seguridad como parte de estrategias de seguridad nacional.

La seguridad informática es también llamada seguridad de la información, esta es de reciente data, así pues, se establece que su origen se dio en el Reino Unido, a partir del trabajo en conjunto elaborado con el Departamento de Industrias y Comercio y el sector privado creando la norma BS7799, la cual posteriormente fue complementada y actualizada en el año 2000 con la norma ISO 17999, esta trataba los temas en materia de privacidad, seguridad de información y criptología. Dos años después, se dispuso actualizar nuevamente esta norma, la cual dio origen a la ISO 27001, con el propósito de abordar la organización y control de toda base de datos.

La aceleración del desarrollo tecnológico trajo consigo el origen del internet, el cual en las últimas décadas se convirtió en un modelo de gestión operativa de servicios públicos y comunicación entre los gobiernos y la ciudadanía. A partir de ello surgen lo denominado gobiernos abiertos o gobiernos electrónicos, los cuales para su efectivo funcionamiento cuentan con activos informáticos, que son: equipo de cómputo, telecomunicaciones, programas, sistemas, datos e información.

La seguridad informática fue desarrollada a consecuencia de búsqueda a la protección contra ataques a redes de comunicación, intensificándose con el auge del internet, por lo que surge el Foro de Gobernanza de Internet integrado por los sectores privado, gubernamental y sociedad civil. Se convirtió en una forma de cooperación internacional con el propósito de intercambio de información y buenas prácticas, que dio prioridad a la seguridad para evitar amenizas de ciber delitos, ciberterrorismo, y garantizar la seguridad de los recursos informáticos y la privacidad.

2.1. Definición

La seguridad informática, también llamada ciberseguridad o seguridad de la tecnología, es definido por algunos autores como un "proceso de prevenir y detectar el uso no autorizado de un sistema informático. Implica el proceso de proteger contra intrusos el uso de nuestros recursos informáticos con intensiones maliciosas o con intención de

obtener ganancias, o incluso la posibilidad de acceder a ellos por accidente."[15] De tal cuenta, que la proliferación de virus y malware o códigos malignos a través de redes de telecomunicación, dio paso a la creación de sistemas de seguridad.

Asimismo desde un punto de vista de la informática, Gómez define a la seguridad informática "como cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos pueden 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."[16] Por lo cual se establece que la importancia de la seguridad informática es evitar el robo o sustracción de datos, especialmente los personales.

Por consiguiente, se puede definir a la seguridad informática, como un proceso informático con el propósito de impedir operaciones no autorizadas en un sistema informático que puedan provocar vulnerabilidad o daños a recursos informáticos, y asimismo garantizar la integridad, disponibilidad y accesibilidad de información.

---

[15] Universidad Internacional de Valencia. **¿Qué es la seguridad informática y cómo puede ayudarme?**https://www.universidadviu.com/la-seguridad-informatica-puede-ayudarme/ (Consultado el 10 de diciembre de 2018).
[16] Gómez Vieites, Álvaro. **Enciclopedia de la Seguridad Informática**. Pág. 38

2.2. Objetivos

Para un efectivo tratamiento de la seguridad informática, debe existir claridad de los objetivos y fines que se deben de llevar a cabo para evitar la vulnerabilidad de sistemas informáticos, y al mismo tiempo, prevenir el comprometer la seguridad de lo contenido en el ciberespacio. Por ende, derivado a la necesidad de detectar y evadir las amenazas informáticas, se estableció una clasificación de los objetivos a tratar de la forma siguiente: objetivos primarios y objetivos secundarios.

Los objetivos primarios, pretenden que se mantenga en resguardo de los riesgos que representen vulnerabilidad en el sistema informático a los activos informáticos, que incluyen equipo de cómputo, telecomunicaciones, sistemas, programas, datos e información. Esto conlleva a la elaboración de estrategias, técnicas o políticas para gestionar y detectar los posibles problemas y amenazas a la seguridad al sistema informático.

Por el otro lado, los objetivos secundarios garantizan la protección de los documentos, registros y archivos informáticos, cuyo fin, desde el punto de vista de la preservación del material documentario, es mantener la confiabilidad del resguardo de información. Por el manejo de información, este se convierte en un objetivo primordial, en cuanto a la protección de datos en los registros electrónicos de instituciones Estatales, debido al flujo

y manejo de información que se obtiene y almacena, especialmente los datos personales.

La finalidad de los objetivos de la seguridad informática es el cumplimiento a la limitación de las pérdidas que puedan suscitar en un sistema en caso de incidentes de vulneración o amenazas al sistema informático. Asimismo, para garantizar que estos objetivos se lleven a cabo es indispensable tomar cuenta que es necesario la participación de diferentes sectores, los cuales se establecen desde los siguientes planos:

a) **Plano humano**, que se encuentra conformado por empleados, que deben participar en el desempeño del resguardo de datos e información y el adecuado tratamiento del sistema.

b) **Plano técnico**, al cual le interesa desde lo físico de los equipos informáticos, el *hardware*, y lógico comprendido por la informática en sí y los sistemas informáticos, el *software*.

c) **Plano organizativo**, comprende la creación, definición e implementación de políticas y estrategias, para un adecuado tratamiento de la seguridad informática en datos e información.

d) **Plano legislativo**, en este plano es indispensable la participación de órganos legislativos de un Estado debidamente organizado, el cual debe velar por la

protección contra la vulnerabilidad informática y que puedan traer consigo la comisión de conductas antijurídicas catalogadas según el cibercrimen, y, asimismo, evitar las amenazas contra sistemas informáticos que contengan datos e información personal, especialmente en los registros electrónicos. Ejemplo de esto, ha sido la regulación de la protección a los datos que la Unión Europea ha realizado por medio de su parlamento.

2.3. Técnicas de seguridad informática

El tema de seguridad ha sido abarcado desde el surgimiento de las tecnologías de la información y comunicación, así como del internet, este fue abarcado desde principios del siglo XX por técnicos y experto. Sin embargo, su interés de protección únicamente se limitó a los activos o recursos físicos e instalaciones informáticas, que se enfocaban únicamente a evitar daños físicos y sabotajes, como consecuencia a conflictos sociales y laborales que se daban en dicha época.

Toda actividad que se desarrolla en la actualidad depende, en su mayoría, de la tecnología e internet, los datos y la información que son registrados en sistemas informáticos, y estos a su vez en el ciberespacio, lo que nos lleva a concluir que todo impacto o problema que surja derivado de la seguridad informática tendrá consecuencias a una escala mundial.

En general, las técnicas según Morgan, R. son " un procedimiento o conjunto de procedimientos materiales, de medios, mecanismos, máquinas, dispositivos e instrumentos materiales, más las destrezas humanas idóneas, para aplicar aquellos procedimientos utilizando los instrumentos necesarios para ejecutar o hacer algo en la práctica"[17]. Por lo cual, de lo anterior puede establecerse que la creación de técnicas es indispensable para la adecuada aplicación de procesos de seguridad informática, asimismo, para la integración de disciplinas para el trabajo conjunto en temas de seguridad.

Las técnicas se convierten en herramientas fundamentales para fortalecer y mantener la seguridad informática, así como, combatir las vulnerabilidades informáticas a los que estén expuestos los sistemas. Es de gran importancia que toda institución que posea o maneje datos, especialmente datos personales, por medio de sistemas informáticos, realice estudios previos para formular y adecuar técnicas de manejo de estos. Para la formulación de técnicas, es necesario la delimitación de las etapas en las que debe desarrollarse las políticas o estrategias que debe desarrollar las instituciones para mantener una óptima seguridad en los sistemas.

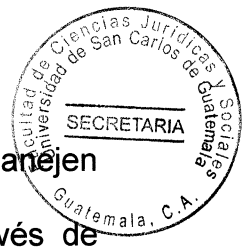
[17] Morgan Sanabria, Rolando. **Planeación del proceso de investigación científica**. Pág. 15

2.4. Estrategias de seguridad informática

Las estrategias comprenden todas aquellas directrices que se trazan para dirigir un asunto, y que por su naturaleza tienen un fin específico. Las estrategias son herramientas que deben ser formuladas por cada institución, tomándose en cuenta las necesidades que se deben abarcar. En cuanto al tema de seguridad informática, es importante que cada institución evalúe las formas de ejecutar los planes y políticas que han sido creadas para combatir la vulnerabilidad de los sistemas.

Asimismo, para la creación de estrategias se deben fijar los objetivos que complementen la realización de políticas públicas enfocadas a la seguridad informática a niveles escalonados, en primer lugar, a todo el gobierno electrónico que se ejerce; y en segundo lugar, a cada institución estatal que cuenta con registros electrónicos. Toda estrategia está orientada, en su formulación, al cumplimiento de propósitos por medio de herramientas que hagan efectiva las metas, objetivos, planes, proyectos y políticas.

En Guatemala no existen estrategias claras para el cumplimiento de la seguridad informática, solo se llevan a cabo planes de trabajo, relevando a un segundo plano los marcos estratégicos, asimismo, basándose en estándares internacionales, como lo son las normas establecidas por la Organización Internacional de Normalización (ISO). Por lo tanto, debe existir un manual de formulación de estrategias de seguridad informática



general que pueda aplicarse en las instituciones Estatales y de Gobierno que manejen datos e información electrónica y plataformas informáticas manejadas a través de internet, por el que se maneje gobierno abierto o electrónico, o bien el manejo interno de datos e información informática.

2.5. Políticas de seguridad informática

Existen diversas concepciones sobre lo que se considera como una política, según sea el contexto, temporalidad, ideología, enfoques de interés y criterios. La adecuación y formulación de las políticas son realizadas a base de la existencia de un fenómeno o asunto de interés según su contexto, temporalidad, o bien, los diferentes pensamientos que puedan darse con respecto a la realidad del fenómeno o asunto.

Así pues, según las necesidades que se requieran, ya sea del ámbito privado o público y tomando en cuenta los elementos para la formulación de políticas, se establece que estas se califican en **administrativas internas o institucionales**, cuando su ámbito de aplicación se encuentra limitada a la estructura interna de una institución para la solución de problemas internos, creadas en armonía con un marco jurídico nacional e internacional. Por otro lado, encontramos las **políticas públicas**, cuya creación se enfoca en la realización del interés o fin común con la intervención del Estado

fundamentada en la Constitución Política de la República, con respecto al cumplimiento del Estado en cuanto a la seguridad, educación, salud, la libertad.

Para la formulación de políticas públicas, es necesaria la identificación de los problemas públicos, los cuales poseen la característica de ser dinámicos, y cuya evolución depende de los cambios en el conocimiento, tecnología y la cultura. Al reconocer como inaceptable un problema, es admitida una intervención estatal y posteriormente se traslada el asunto para la conformación de la agenda nacional.

Según Mariñez, F. Y Garza, V. las políticas públicas son un "conjunto (secuencia, sistema, ciclo) de acciones, estructuradas en modo intencional y causal, que se orientan a realizar objetivos considerados de valor para la sociedad o a resolver problemas cuya solución es considerada de interés o beneficio público"[18]. Es decir, que estas son una forma de como los Estados plantean soluciones a problemas u oportunidades de interés nacional que puedan darse en los procesos social y político de gobierno, por lo que se constituyen como instrumentos de planificación y gestión del Estado.

En el contexto guatemalteco, se establece que las políticas públicas son cursos de acciones estratégicas establecidas por el Estado y el gobierno, este último se encarga

[18] Secretaría de Planificación y Programación de la Presidencia. **Guía para la formulación de Políticas Públicas.** Pág. 16

de su ejecución, los cuales poseen las características de participación y legitimación, marco jurídico y político, tanto nacional como internacional, orientadas a satisfacer las necesidades y bienestar de los habitantes, sobre la base de herramientas y estrategias de gestión pública y planificación nacional, los cuales, facilitan procesos de agenda nacional con coordinación, transparencia, monitoreo, evaluación y rendición de cuentas acerca de lo realizado.

Por otro lado, en cuanto a las políticas de seguridad informática, la aplicabilidad de esta clase de políticas está sujeta al tipo de necesidad o problema que se debe cubrir. Si la necesidad o problema de seguridad informática se ciñe al ámbito de una o determinadas instituciones, corresponde la formación e implementación de políticas administrativas internas; en cambio, si fuese sobre cuestiones de interés público o fin común, así como asuntos que impliquen la seguridad informática a nivel nacional, corresponde la creación e implementación de políticas públicas. En consecuencia, la forma para establecer estrategias de seguridad informática, que se encarguen de la protección de sistemas en registros electrónicos, es la prevención y ejecución a nivel nacional en el gobierno electrónico que se ejerce en el ciberespacio, incluyendo registros electrónicos de instituciones estatales, tal como, el registro electrónico del registro civil de las personas del Registro Nacional de las Personas de Guatemala.

En Guatemala, la entidad encargada de la planificación del Estado que asiste técnicamente las instituciones públicas que conforman el Estado, en cuanto a procesos

de políticas públicas, planificación, y programación es la Secretaría de Planificación y Programación de la Presidencia, que tiene a su cargo la Subsecretaría de Políticas Públicas que se encarga de la asesoría en cada una de las etapas del ciclo de políticas públicas, que son la formulación, implementación, monitoreo y evaluación, basados en la realidad nacional. Esta es la institución que posibilita la ejecución de agenda nacional, por medio de la programación de planes y programas.

Consecuentemente, todos los problemas de seguridad informática nacional deberían de canalizarse a normas a nivel nacional para su adecuado tratamiento estandarizado y controlado, por medio de la elaboración de políticas públicas con el asesoramiento de esta institución con enfoque técnico.

2.5.1. Políticas públicas de seguridad informática manejadas en Guatemala

En Guatemala no existe legislación orientada a la seguridad de la información personal ni protección a los datos personales, y esta ausencia provoca que cada institución del Estado establezca sus propias políticas y estrategias.

Así pues, en el Ministerio de Gobernación existe el Viceministerio de Tecnología, mismo que tiene a su cargo un equipo de respuesta a incidentes cibernéticas, el cual, en

armonía con lo expuesto anteriormente, solamente posee funciones a nivel institucional encargado de la seguridad a nivel interno del Ministerio de Gobernación y sus dependencias, coadyuvando en la detección de amenazas y vulnerabilidades en los sistemas. Por estas razones, esta institución a pesar de sus funciones, no realizan análisis de sistemas de seguridad informática de los registros públicos a nivel nacional.

Este Ministerio, en materia de seguridad informática únicamente se rige por la **Política Nacional de Datos Abiertos**, misma que es desarrollada y ejecutada por medio de la estrategia nacional de seguridad cibernética, cuyos fines son la apertura, inclusión y transparencia, ya que se considera que es indispensable para la lucha contra la corrupción y de inclusión y participación ciudadana. De modo que, el enfoque de seguridad cibernética se encuentra hacia la apertura a la ciudadanía, más no existen estrategias definidas sobre ataques cibernéticos a los sistemas, sustracción o perdida de datos e información tanto institucional como personal a cargo de instituciones Estatales.

Por otro lado, en cuanto al Registro Nacional de las Personas, al ser una institución que maneja información y datos personales de los guatemaltecos por medio de sistemas informáticos, cuenta con la Subdirección de Servicios Críticos, entidad supeditada a la Dirección de Informática y Estadística, cuyas funciones se enfocan en la planificación, organización, ejerciendo dirección y control de las actividades que se relacionan con la seguridad informática, según lo establece el Artículo 47 del Acuerdo de Directorio Número 80-2016. Derivado de lo anterior, se establece que las políticas institucionales

administrativas que han sido creadas para el Registro Nacional de las Personas en asuntos de seguridad informática son las siguientes:

a) Política de visitantes en línea (2011)

b) Política de uso de correo electrónico (2011)

c) Política de uso de Internet (2011)

d) Política de estaciones de trabajo (2011)

e) Política de seguridad de la información (2016)

f) Política de creación, administración y configuración de carpetas compartidas (2016)

CAPITULO III

3. Derecho informático en el derecho internacional

En el ámbito internacional, el Derecho informático es definido como un derecho global que se encuentra en constante evolución y progreso, y al mismo tiempo, es considerado como una disciplina jurídica autónoma e independiente, según doctrinarios que señalan que su área de estudio y regulación no se ciñe a una rama específica, como administrativa o penal. El acceso a los medios de las tecnologías de la información y comunicación se ha convertido en un derecho humano de nueva generación, reconocido por organismos internacionales, así como las Naciones Unidas. Esta evolución creciente ha generado una revolución tecno-informática, cuyo fin es la interconexión de los distintos ámbitos sociales.

Siendo el Derecho informático una disciplina relativamente joven, cuyo objeto de estudio es la informática e información, coadyuva en la creación de instituciones jurídicas nuevas enfocadas en las telecomunicaciones e información. Las sociedades de la información y las comunidades virtuales, permiten la capacidad de producir e intercambiar bienes y servicios, que traen como consecuencia el acceso a toda clase de información. Las comunidades virtuales han permitido la creación de espacios globales de interconexión,

que involucra naciones, el espacio más concurrido es el ciberespacio, cuya fluidez no se encuentra limitada por regulaciones.

Esta disciplina jurídica, como se ha mencionado anteriormente, se desarrolló a partir de mediados del siglo XX, al paso de la evolución de medios tecnológicos informáticos, como la computadora e internet, empezando con Norbert Wiener cuyos estudios estaban relacionados con las comunicaciones, informática y el Derecho. El acceso a la información es traducido como formas actuales de poder, de tal cuenta que la sistematización de datos e información son activos que interesan al Derecho informático, y que cada nación se mantiene en la búsqueda de mantener un mejor control, especialmente en el manejo datos personales.

La preocupación por el mayor resguardo, preservación y regulación de manejo de datos personales a través del Derecho Informático, empezó a brotar en los países donde el desarrollo evolutivo tecnológico fue acelerado, como en Estados Unidos de América, y países europeos como Inglaterra, Alemania, Italia, entre otros; trascendiendo a sociedades de naciones, como la Unión Europea y las Naciones Unidas, esto quiere decir, que las fronteras y límites físicos entre los Estado no existe en el medio tecnológico, en el cual, el flujo de información y datos no es limitativo.

No existe un país específico al que pueda atribuírsele el surgimiento del Derecho informático como una disciplina jurídica autónoma, ya que la característica global de la informática ha permitido la contribución a nivel internacional de doctrinarios e instituciones jurídicas que permiten la evolución de la aplicación de la informática. En el caso latinoamericano, el Derecho Informático es enfocado en las formas de gestión electrónica de gobierno ejercido en los Estados, y la seguridad de los sistemas, sin embargo, en cuanto a la protección de datos personales se ha procurado normativizar su protección, como en México y Chile, que clasifican los datos personales y restringen la inadecuada utilización.

En conclusión, el Derecho informático es de carácter internacional, cuyo desarrollo y fluidez no se encuentran restringidos por fronteras físicas, solamente existe una jurisdicción limitada que ejercen las naciones en el ciberespacio.

3.1. Cibercrimen en el Derecho internacional

Las comunidades virtuales, han permitido que se realice la producción e intercambio de bienes y servicios para poseer acceso a toda clase de información, de esta forma se generan las interconexiones de ámbitos. La intercomunicación del mundo a través de las redes de la comunicación y tecnologías de la información, apareja tanto ventajas como desventajas. Entre las desventajas encontramos los riesgos a consecuencia de ataques

maliciosos con intención de dañar y perjudicar los sistemas informáticos. Estos ataques toman distintas formas como el "acceso ilegal, la difusión de programas perjudiciales y ataques por denegación de servicio"[19], que se consideran como conductas antijurídicas.

El fenómeno de atacar redes de comunicación y tecnologías de la información surgió en el siglo XX, junto con la creación de tecnología y medios de telecomunicaciones, los cuales, en un principio fue una inquietud de estudiantes universitarios de atacar los sistemas que no tenía fines maliciosos ni dañar equipos informáticos.

Consecuentemente, se evidencio la vulnerabilidad que pueden experimentar los sistemas. Sin embargo, no se le dio la importancia debida a la seguridad informática de los sistemas, con la que se pretendía garantizar los medios informáticos. Y con el paso del tiempo, los desafíos de encontrar vulnerabilidades en los sistemas con fines recreativos, se convirtió en una actividad maliciosa por parte de algunos grupos para dañar sistemas, creándose virus y programas maliciosos que no solo dañan los sistemas, sino sustraen datos, información informática e información personal. Así mismo, estos virus y malware, se infiltran en los sistemas de tal forma que no puedan ser detectados para propagarse y causar daño al sistema informático, por esta razón son considerados dañinos y se procura la protección total de los sistemas.

[19] Téllez. **Op. Cit**. Pág. 187

Por otro lado, estas conductas maliciosas no se limitan a los ataques de sistemas, sino también, a el dolo o negligencia, falta de responsabilidad, mal uso, ignorancia o mala capacitación laboral que pueda provocar la pérdida, destrucción, alteración o tráfico de datos e información, tanto informáticos como personales sensibles o no sensibles, a consecuencia de la actividad que realicen el personal o empleados de la institución que se encuentre en riesgo o vulnerada. El sujeto activo de la comisión de estas conductas antijurídicas o ilícitas, son personas o grupos de personas mal intencionales que realizan actividades criminales y que utilizan estos ataques o amenazan con utilizarlos como medios de presión o extorsión, a las que se les denomina cibercriminales.

Todo ataque a los sistemas representa una amenaza a la construcción de las sociedades de la información, la seguridad, libertad y justicia de estas. Por tales razones, surge los denominados ciberdelitos o cibercrimen. Términos jurídicos, cuya denominación implica la definición de conductas en una norma jurídico penal, siendo esta la tipificación de los delitos informáticos o electrónicos para la calificación de una conducta como antijurídica. En algunos países ya se encuentran regulados los delitos informáticos como conductas típicas, antijurídicas y culpables cuyo instrumento o fin son las computadoras; por otro lado, en otros países se utiliza el termino de delitos informáticos, pero estos no se encuentran regulados, por lo que se determinan como actitudes ilícitas.

3.1.1. Características de los delitos informáticos

Según Téllez, existen ciertas características que define a los delitos informáticos, los cuales son:

a) La conducta criminal es realizada por un número limitado que poseen conocimientos técnicos en informática, por lo que son conocidas como conductas de cuello blanco o *White collar crimes*.

b) Se consideran como acciones ocupacionales, ya que el sujeto activo las realiza en su ámbito laboral.

c) Pueden ser realizadas a consecuencia del aprovechamiento de una ocasión.

d) La realización de estas conductas ilícitas puede llegar a provocar pérdidas económicas o materiales, a beneficio de estos sujetos.

e) Son de carácter de técnicos, por lo tanto, su comprobación es dificultosa.

f) Representan facilidades en cuanto a su comisión, ya que, no necesariamente dependen de un espacio físico ni de un tiempo específico, asimismo, por estos motivos, para los menores de edad representa una facilidad en su acceso.

g) Actualmente tienden a su proliferación, debido a la evolución de la tecnología.

Derivado de las anteriores características, el perfil del sujeto activo de la comisión de los ilícitos, no son como los delincuentes comunes, ya que deben poseer habilidades específicas del manejo de tecnología y sistemas informáticos. Además, se ha reportado según estudios, que "el 90% de los delitos realizados mediante la computadora los cometían empleados de la empresa afectada"[20], es decir, que existe vulnerabilidad en las empresas, en cuanto al manejo informático de sus empleados.

3.1.2. Formas de ataques a los sistemas informáticos

Existen diferentes formas de ataques cibernéticos maliciosos contra los sistemas informáticos, los cuales han sido establecidos de acuerdo a la frecuencia de daños producidos a los sistemas. Tal y como lo establece la comunicación de seguridad de las redes y de la información, y la decisión marco del consejo relativa a los ataques de los que son objeto los sistemas de información, propuestas por la Comisión de las Comunidades Europeas, clasifican los tipos de ataques informáticos de la siguiente manera:

A) **Acceso no autorizado a sistemas de información.** En esta clasificación comprende en tener acceso de forma no autorizada a un ordenador o red de ordenadores que corresponde al concepto de piratería informática. Asimismo,

[20] **Ibid.** pág. 189

puede implicar el mero uso de informaciones internas a través de ataques directos e interceptación de contraseñas, con la intensión dolosa de copiar, modificar o destruir datos.

B) **Perturbación de los sistemas de información.** El concepto perturbación engloba distintas formas de ataques, como la denegación de servicio (DdS), el cual tiene por objeto la sobre carga de servidores o a los proveedores de servicios de Internet; otro tipo de ataque es la perturbación de servidores que hacen funcionar el sistema de los nombres de dominio, los cuales son perjudiciales para las páginas web.

C) **Ejecución de programas informáticos perjudiciales que modifican o que destruyen datos.** El tipo de estos programas informáticos mal intencionados más conocido y utilizado es el virus. Otros de estos programas son los llamados bombas lógicas, que permanecen inactivos hasta que se cumple la fecha determinada que los permite desencadenar la destrucción o modificación de datos que maneje el sistema; los caballos de Troya, que parece inofensivo, sin embargo, sus ataques son altamente perjudiciales; o los llamados gusanos, que no infectan otros programas, pero se crean replicas en cadena para infectar a todo el sistema.

D) **Interceptación de las comunicaciones.** Es realizada con fines malintencionados, que perjudican la confidencialidad e integridad de los usuarios de redes de telecomunicación.

E) **Declaraciones falsas.** Este tipo de ataque comprende la usurpación de la identidad de una persona para su uso en internet, para utilizarla con fines malintencionados y fraudulentos.

Las conductas derivadas de las formas de ataques a los sistemas expuestos anteriormente, son realizados de forma malintencionada y con fines perjudiciales a los sistemas informáticos. Esto demuestra que, del plano informático, surge la afectación de derechos trascendiendo al plano jurídico.

3.1.3. Regulación a nivel internacional

La preocupación de los Estados por la regulación de las conductas informáticas ilícitas, se deriva de la característica global de la informática y de los delitos informáticos, así como el interés de cubrir los vacíos y ausencia normativa para el tratamiento del cibercrimen. Las contribuciones internacionales en materia de cibercrimen contribuye en el desarrollo nacional en investigaciones técnicas e informáticas a través del derecho penal.

Por lo que, la propuesta de uniformidad de legislaciones en materia de delitos informáticos, fomenta la cooperación internacional en cuanto a el control y prevención de delitos informáticos. El mayor ejemplo de cooperación internacional, ha sido Europa, que se ha preocupado por la suscripción de convenios y promulgación de legislación parlamentaria a nivel europeo para el control de los delitos informáticos a consecuencia de la búsqueda por la seguridad informática y control de las comunicaciones y tecnología, para garantizar la confidencialidad e integridad. Por otro lado, en países del continente americano la preocupación de garantizar la seguridad informática e interés de combatir los delitos informáticos, es consecuencia del desarrollo informático que posea cada país.

En el derecho comparado, la regulación de los delitos informáticos ha sido de acuerdo a la época, y actualmente, la preocupación de regular las conductas ilícitas se ha incrementado por parte de los Estados, de acuerdo a la vulnerabilidad y crecimiento de las tecnologías, y al mismo tiempo la integridad de las personas. Algunas naciones que han regulado los delitos informáticos son las siguientes:

a) **Alemania.** Destaca por la promulgación de la Ley contra la Criminalidad Económica, en el año 1986, la cual regulo en forma general los delitos de: espionaje de datos, fraude informático, alteración de datos y sabotaje informático.

b) **Austria**. En el año de 1987, se promulgaron reformas al Código Penal, que contempla la sanción a los sujetos que causen perjuicio patrimonial, a causa del dolo premeditado, de un tercero.

c) **Gran Bretaña**. A consecuencia de ataques informáticos por medio del hacking, en el año de 1991, se creó la normativa Ley de abusos informáticos, la *computer misuse act*, que prohíbe la alteración de datos informáticos, así como la modificación de datos y la propagación de virus informáticos.

d) **Holanda**. En esta nación se crea la ley de delitos informáticos el uno de marzo de 1993, la cual tipifica y penaliza el hacking y el preacking, ataques utilizados para evitar los pagos totales o parciales de los servicios de telecomunicaciones; la ingeniería social, conocido como una forma de entrega de información, que normalmente no sería entregada; y la distribución de virus a los sistemas informáticos.

e) **Francia**. A partir de enero de 1988, se implementa la ley sobre fraude informático, que regula las sanciones por la intromisión fraudulenta que suprima o modifique los datos.

f) **España**. Con la promulgación del nuevo Código Penal se dispuso las sanciones a quienes destruyan, alteren, inutilicen o dañe los datos, programas o documentos electrónicos que se encuentran en redes, soportes o sistemas informáticos. Asimismo, se reguló acerca de las estafas electrónicas que, a pesar de no detallarse las penas a aplicar, se tipifica la conducta antijurídica del infractor

g) **Chile**. El siete de junio de 1993, se sancionó la ley contra los delitos informáticos, siendo Chile el primer país latinoamericano en promulgar una ley en esta materia. Esta ley se enfoca en la tipificación de las conductas antijurídicas de destrucción o inutilización de datos contenidos en la computadora, destrucción o inutilización maliciosa de un sistema de tratamiento de información o de sus partes componentes, y la alteración, daño o destrucción de los datos contenidos en un sistema de tratamiento de información.

h) **Estados Unidos**. La preocupación por la seguridad informática, ha provocado las innovaciones aportadas al derecho informático, en cuanto a los delitos informáticos, a partir de 1986 se crea la Acta de fraude y abuso computacional, la cual fue posteriormente modificada en 1994 por él Acta Federal de abuso computacional, centrada en la transmisión de los virus y su postura en contra de estos, dando al mismo tiempo, un acercamiento a los problemas que producen los virus informáticos y no limitándose únicamente a estos, se enfoca en una nueva era de los ataque informáticos como estafas electrónicas y defraudaciones relacionadas con dispositivos de sistemas informáticos.

i) **México**. En este país se encuentra regulados en el Código Penal Federal, los delitos que puedan ser cometidos a consecuencia de conductas ilícitas a través de las tecnologías de la información y comunicación, tales como la revelación de secretos, el acceso ilícito a sistemas y equipos de informática.

Por lo otro lado, en **Guatemala**, el Código Penal, Decreto Número 17-73, sufrió una reforma por medio del Decreto Número 33-96 del Congreso de la República, en el cual, el capítulo séptimo del título octavo que corresponden al libro segundo, es modificado y se incluye en este apartado a los delitos informáticos, tipificados a partir del Artículo 274 "A" al Artículo 274 "G", siendo estos: a) Destrucción de registros informáticos; b) alteración de programas; c) Reproducción de instrucciones o programas de computación; d) Registros prohibidos; e) manipulación de información; f) uso de información; g) programas destructivos.

Por otra parte, en la ley de acceso a la información pública, decreto número 57-2008 del Congreso de la República, se contemplan delitos especiales, concernientes a la responsabilidad ante hechos o actos antijurídicos que afectan específicamente a los datos personales e información en los archivos, los cuales son: a) comercialización de datos personales; y b) alteración o destrucción de información en archivos.

Sin embargo, el catálogo de delitos informáticos contemplados, tanto en la legislación penal general como en leyes penales especiales guatemaltecas, puede considerarse insuficiente frente al avance de protección de la seguridad e intimidad, puesto que es necesario sancionar las conductas antijurídicas que perjudiquen la ciberseguridad de instituciones estatales y a los habitantes guatemaltecos que se encuentran expuestos a vulnerabilidades y amenazas sobre la seguridad informática y datos personales almacenados en archivos electrónicos.

3.2. Convenios y tratados internacionales

La interconectividad de naciones por medio de las tecnologías de la información y la creciente evolución de la tecnología e internet, ha provocado que surjan las comunidades virtuales, y al mismo tiempo, la preocupación de los Estados para la protección de los activos informáticos, el ciberespacio, seguridad y protección de datos. En consecuencia, comunidades de naciones se han unido con el propósito de tratar y desarrollar estos temas, de esta forma han surgido instrumentos internacionales como:

I) **Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal**.

Este convenio fue aprobado, emitido y signado por los Estados miembro del Consejo de Europa el 28 de enero de 1981 en Estrasburgo, el cual es conocido también como el Convenio de Estrasburgo. Este convenio fue realizado con el fin de garantizar el respeto al derecho a la vida privada, como un derecho y libertad fundamental, enfocado en la protección de datos en cuanto al tratamiento automatizado de los datos de carácter personal. La aplicación de este convenio se encuentra en la protección de ficheros y tratamiento automatizado de datos de carácter personal, tanto del sector público como del privado. Este convenio regula los principios sobre los compromisos de las partes, la calidad de los datos, las categorías particulares de los datos y la seguridad de los datos

contra la destrucción, perdida, así como el acceso, modificación y difusión no autorizado de datos.

Por otro lado, este convenio trata el flujo trasfronterizo de los datos personales y su trato internacional, y por la falta de su cumplimiento, fue plasmado el compromiso que deben adoptar los Estados signantes de establecer sanciones contra las infracciones cometidas. Este convenio es considerado el más importante en cuanto a la protección de datos personales, y no solamente ha sido ratificado por países europeos, sino también, por países como Ecuador, Costa Rica, Venezuela, Estados Unidos y Japón.

l) **Convenio sobre la Ciberdelincuencia**.

El convenio sobre la ciberdelincuencia es también conocido como el Convenio de Budapest, creado el 23 de noviembre de 2001 por el Consejo de Europa. La preocupación por el riesgo de la comisión de delitos por medio de redes informáticas e información electrónica, llevo a la cooperación de los Estados junto con el sector privado para la lucha contra el cibercrimen, por lo que la implementación del presente convenio ha sido para cubrir la necesidad de prevenir los actos que pongan en peligro la confidencialidad, integridad, disponibilidad de los sistemas, redes y datos, y el abuso de los sistemas, redes y datos.

La importancia de creación de este convenio fue debido a la necesidad de unificar normativa acerca de los delitos informáticos, y al mismo tiempo, definir tanto conductas antijurídicas como las medidas que debe adoptar cada Estado para prevenir y contrarrestar el cibercrimen. Este convenio, en su división temática abarca sobre la terminología en lo referente a la ciberdelincuencia; las medidas que deberán adoptarse a nivel nacional, en cuanto a los delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos; la cooperación internacional, estableciendo los principios de las bases de esta, la extradición y la asistencia mutua entre las naciones; y por ultimo las clausulas finales.

Según las clausulas finales del convenio, este se encuentra abierto para la adhesión de nuevos Estados que quieran adoptarlo y comprometerse al tratamiento e investigación de los delitos informáticos. Además de los países que pertenecen a la comunidad europea, este convenio ha sido firmado por países no europeos, tales como: Estados Unidos de América, Japón, Canadá, Sudáfrica, Israel, Senegal, Sri Lanka, Panamá, República Dominicana, Perú y Colombia.

II) **Directiva 2002/58/CE del Parlamento Europeo y del Consejo de la Unión Europea**.

Esta normativa es relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, emitido el siete de diciembre de 2002 por el Parlamento Europeo. Esta directiva trata sobre la privacidad y las comunicaciones electrónicas enfocada en la protección de las libertades y los derechos fundamentales. Su aplicación se suscribe a la protección de las libertades y derechos fundamentales para garantizar la privacidad y las comunicaciones electrónicas.

Esta Directiva emitida por el Parlamento Europeo se enfoca en los ámbitos de seguridad en cuanto a los proveedores de servicios de comunicación, datos de tráfico, y la presentación y restricción de la identificación de la línea de origen y de la línea conectada. Sin embargo, se estableció que dichas disposiciones son únicamente para la protección de la intimidad en la esfera privada de los habitantes de la Comunidad Europea, no se dedica a la seguridad y defensa estatal.

3.3. Seguridad informática y políticas de control informático

El tratamiento de la seguridad informática en cada uno de los países depende mayormente del desarrollo tecnológico con el que cuente a nivel mundial, puesto que, a mayor creación tecnológica, surgen más formas de poner a prueba o atacar las tecnologías de la información y comunicación, así como las formas en que pueden resolverse los problemas derivados de amenazas informáticas, como:

a) El hacking, son intrusos que "entran en los sistemas informáticos para demostrar y poner a prueba su inteligencia y sus conocimientos de los entresijos en Internet, pero no pretenden provocar daños en estos sistemas"[21]. Asimismo, se debe tomar en cuenta que su actividad les da la posibilidad de ingresar a los archivos confidenciales de sistemas informáticos institucionales;

b) Los crackers, por el contrario de los hackers, estos realizan actividades con el propósito de "atacar un sistema informático para obtener beneficios de forma ilegal, o simplemente, para provocar un daño a la organización propietaria del sistema"[22], estas personas se encuentran motivadas por intereses económicos, políticos, social o religioso;

[21] Gómez Vieites. **Op. Cit**. Pág. 195
[22] **Ibid.** Pág. 196

c) Los phreakers, son los que realizan actividades intrusivas en redes telefónicas para obtener beneficios gratuitos como llamadas;

d) Spammers, estos provocan el colapso de sistemas, servidores y correos electrónicos, por medio del envío masivo de mensajes y publicidad vía internet, catalogados como no deseados, pudiendo contener códigos dañinos como virus o medios de estafa por internet;

e) Los piratas informáticos, estos son individuos que se encargan de infringir las normas de propiedad intelectual, realizando actividades de reproducción ilegal de programas y contenidos digitales; o

f) Las amenazas internas de empleados o ex empleados de la institución, tanto privada como pública, en cuanto a la seguridad informática se debe tomar en cuenta el desempeño de los empleados en áreas informáticas y el acceso a estas, ya que pueden provocar incidentes o vulnerabilidad en el sistema, voluntaria o involuntariamente, y dañar el sistema informático, así como de los datos confidenciales. Siendo aún más dañino. la actividad realizada por ex empleados desleales que deseen causar daño a su ex empleador, que pueden usar las llamadas bombas lógicas, que extraen, suprimen y dañan los sistemas informáticos de las instituciones.

A consecuencia de dichas amenazas, algunos países catalogan las infracciones anteriores como delitos informáticos, y aquellos países que no cuentan con legislación

sobre los delitos informáticos, utilizan políticas de acción para el control de la seguridad informática a nivel nacional. Algunos países como Estados Unidos, Reino Unido, España, Alemania, Corea del Sur, China, Japón, han designado instituciones para el monitoreo, prevención y detección de los delitos informáticos bajo políticas de seguridad informática, y de esta manera fortalecer los sistemas informáticos institucionales.

El uso de políticas de seguridad informática a nivel internacional, tanto en la esfera privada como en la pública, son mayormente estandarizadas con normas de la *International Organization for Standardization (*Organización Internacional de Normalización), conocidas como normas ISO, y que se encuentra presente en más de 164 países como una institución independiente y no gubernamental. Esta organización fue fundada en 1926, sin embargo, en la segunda guerra mundial fueron suspendidas sus labores, y posteriormente se refundo el 23 de febrero 1947 con la coordinación de 25 países para establecer las bases de estandarización industrial internacionalmente.

Esta organización cuenta con más de 22,000 estándares redactados, y la seguridad es uno de los temas más abordados. En cuanto, a la protección de los sistemas, los riesgos y la seguridad se encuentra traducido en la norma 27001, como en un sistema de gestión de la seguridad de la información, centrado en asegurar la integridad y confidencialidad de la información. Sin embargo, la seguridad informática no solo depende de políticas y estándares, sino se debe tomar en cuenta el monitoreo y control de esta, para el efectivo cumplimiento de las normas establecidas en cada país.

La norma ISO 27001 contiene dominios que tienen la función de establecer ciclos de seguridad, aunque estos no están completamente relacionados con el ámbito jurídico. Los dominios de la ISO 27001 son: a) la política de seguridad de la información, b) organización de la seguridad de la información, b) gestión de activos, c) seguridad de recursos humanos, d) seguridad física y del entorno, e) gestión de comunicaciones y operaciones, f) control de acceso, g) adquisición, desarrollo, y mantenimiento de sistemas de información, h) cumplimiento.

En esta norma para gestión la seguridad de la información, desde la perspectiva jurídica, se tienen como prioritarios la protección de datos personales, contratación de bienes informáticos y telemáticos, derecho laboral y prestación de servicios, regulación de aspectos tecnológicos, comercio electrónico, propiedad intelectual y los incidentes informáticos; los cuales deben alinearse a las políticas de seguridad la cual a la inexistencia de ley o vacíos legislativos, sea esta la que siga como "guía a la organización en el cumplimiento de sus obligaciones, deberes o cargas"[23], y como lo afirma el mismo Velasco la adopción de prácticas o normas foráneas, que implican el cumplimiento extensivo de lo no preceptuado de la ley nacional, no perjudica a las organizaciones o instituciones públicas o privadas, es más, la Constitución Política de la República de Guatemala en el Artículo 44, establece la permisión de incorporación de derechos y garantías inherentes a la persona humana, por lo que la seguridad y protección de datos personales se convierte en una prioridad derivada del derecho de la intimidad.

---

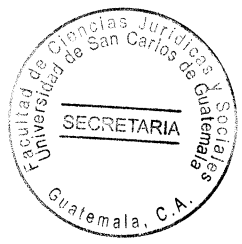
[23] Velasco Melo, Arean Hernando. **El derecho informático y la gestión de la seguridad de la información, una perspectiva con base en la norma ISO 27 001**. Pág. 343

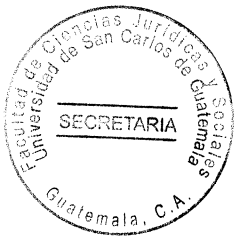
3.4. Regulación y manejo de datos personales

La importancia de la protección jurídica de los datos personales, se deriva de la del derecho de la intimidad, concepto que se relaciona con los términos intimidad, *privacy, riservatzz* y *vie privee,* que pretende una cobertura jurídica ante la informatización de los datos personales, para evitar y vedar la intromisión a determinados ámbitos de la vida personal que se mantienen en resguardo del titular. Asimismo, se incluye la prohibición de recolección e utilización de información personal, actuando de esta forma en el ámbito jurídico la protección de datos personales ante el derecho de uso y el derecho de acceso limitado, que proporciona un control sobre los propios datos personales.

Por consiguiente, la prioridad de la protección de datos personales, así como su adecuado manejo, por medio de normas jurídicas, no se ha dado igualitariamente en todos los países, limitándose conforme a la evolución tecnológica. En cuanto a regulación internacional podemos encontrar el Convenio de Estrasburgo, anteriormente mencionado, que trata sobre la protección de las personas con respecto al tratamiento automatizado de datos. Por otro lado, algunos países se han preocupado por la inclusión en su legislación del resguardo de los datos personales, así como la privacidad y la intimidad inherentes a la persona como un derecho humano.

Entre los países que sitúan en su normativa a nivel constitucional la protección y manejo de datos se encuentran: Portugal; España, con la constitución promulgada el 29 de diciembre de 1978; Austria; Holanda; Suiza; Alemania. Asimismo, otras naciones se interesaron por ampliar la protección jurídica de datos, por medio de normativa específica como: la ley de la privacidad del 31 de diciembre de 1974, promulgada en Estados Unidos; la ley de derechos humanos promulgada el 29 de diciembre de 1977 en Canadá, que trata los derechos de intimidad y protección de datos personales desde la perspectiva del *privacy*; ley de datos emitida en Suecia, el 11 de mayo de 1973, primera regulación en esta materia a nivel nacional y que crea un organismo supervisor denominado *Data Inspektion Borrad,* abreviado DIB; en la República Federal de Alemania fue promulgada el 27 de enero de 1977, la ley federal de protección de datos, creándose un comisario federal de datos para el debido control de estos; la ley relativa a la informática, archivos y libertadas creada en Francia el seis de enero de 1978, se crea un órgano especial con funciones de control, siendo este la Comisión Nacional de Informática y Libertades, con función de informar y resguardar; y la Ley Orgánica de Regulación del Tratamiento Autorizado de los Datos de Carácter Personal, conocida como LORTAD, creada en España y que incluye los derechos humanos inherentes de la persona como el derecho al honor, a la intimidad personal y familiar, así como el pleno ejercicio de sus derechos fundamentales.


Facultad de Ciencias Jurídicas y Sociales
Universidad de San Carlos de Guatemala
SECRETARIA
Guatemala, C.A.



CAPITULO IV

4. Registro Nacional de las Personas de Guatemala

Históricamente ha surgido la necesidad de poseer un registro para darle una publicidad a ciertos actos considerados relevantes por la sociedad. En consecuencia, los Estados modernos revistieron con normas constitucionales, basadas en el principio de legalidad, el fundamento de las instituciones registrales, los cuales otorgan primordialmente una seguridad jurídica preventiva. La Importancia de un registro civil que se encargue del orden registral sobre la persona natural es indispensable, puesto que son este tipo de instituciones las que le otorgan a la persona una publicidad a su derecho de identidad.

El Registro Nacional de las Personas, surge como un proceso indispensable de actualización sistemática de inscripciones y registros de los asuntos concernientes a la identidad de la persona natural, tales como los nacimientos, matrimonios, divorcios y defunciones, así como cualesquiera actos relativos a la capacidad civil y al estado civil de las personas naturales. La legislación del registro civil que se encontraba en el Código Civil, Decreto Ley 106 del Jefe de Estado, necesitaba una reforma moderna de acuerdo a las tendencias actuales de implementación de las tecnologías, para revestir de seguridad jurídica al registro civil de personas naturales, favoreciendo al mismo tiempo, a los inicios de una modernización del sistema electoral guatemalteco.

El Registro Nacional de las Personas es una institución de cuyas funciones principales se encuentran vinculadas con los asientos registrales de identificación de personas naturales, por lo cual, se hace necesario el uso de la tecnología para su adecuado manejo y resguardo, siendo fundamental la seguridad.

4.1. Antecedentes

El primer antecedente de los registros personales, son los registros parroquiales que la iglesia católica poseía, los cuales, inscribían y registraban bautismos y matrimonios religiosos, y que posteriormente, según el Código Civil, Decreto Ley 106 del Jefe de Estado, en su Artículo 389 regulaba que "los registros parroquiales, prueban el estado civil de las personas."[24] Por lo tanto, estos eran el único registro que otorgaba seguridad sobre la protección a la identidad de las personas. Uno de los registros parroquiales más antiguos en Guatemala, es la Catedral Metropolitana, cuyos registros datan desde finales del siglo XIV, asimismo el Arzobispado, cuenta con un archivo histórico asentados en libros que recopila datos de miles de guatemaltecos.

En la actualidad, los registros parroquiales aún siguen funcionando en cada parroquia, manejando en tales registros los libros de bautismos, confirmaciones, matrimonios,

[24] Figueroa Perdomo, Claudia Lavinia; Ramírez Gaitán, Daniel Ubaldo. **Derecho Registral I.** Pág. 18

defunciones y estado de almas. Llevándose a cabo una custodia de datos personales de sus feligreses católicos.

Posteriormente, fue el Doctor Mariano Gálvez quien intentó implementar formalmente la institución de un Registro Civil en Guatemala, como la encargada del registro de las personas, sin embargo, por su propuesta de la inclusión de la figura del matrimonio civil, y por consiguiente del divorcio, a consecuencia de la implementación de reformas a la legislación civil en el año de 1837. Dichas reformas fueron fuertemente criticadas y categorizadas como inconcebibles, ya que se consideraba que afectaba a la institución de la familia, así como las tradiciones y costumbres ancestrales conservadoras, produciéndose choques ideológicos e inconformidades con estas leyes.

De tal modo fue como se produjo el rechazo de la idea de un Registro Civil, continuándose con los registros parroquiales de la Iglesia Católica, hasta la promulgación del primer Código Civil de Guatemala, Decreto Número 175 del Presidente de la República de Guatemala, que estableció el Registro Civil en Guatemala como una dependencia Estatal a cargo del gobierno y del secretario municipal en los municipios, por lo que se establece que se manejaba el registro con un sistema mixto, y cuya función principal es la de hacer constar sobre el estado civil de las personas.

Más tarde, el registro civil sufre algunas modificaciones realizadas a través del Código Civil de 1933, en el cual, se destacó la importancia de la publicidad del registro estableciéndose obligatoriamente los siguientes libros: nacimientos; reconocimiento de hijos; matrimonios; capitulaciones matrimoniales; separación; divorcios; nulidad e insubsistencia del matrimonio y reconciliación; tutelas; protutelas; guardas; ciudadanía; extranjeros; y defunciones.

El Registro Nacional de las Personas fue creado mediante el Decreto Número 90-2005 del Congreso de la República, el cual sustituyó al Registro Civil del año de 1963 en el Código Civil, Decretó Ley 106 del Jefe de Estado. El fundamento de creación del Registro Nacional de las Personas fue el Acuerdo de Paz sobre Reformas Constitucionales y Régimen Electoral firmado el 7 de diciembre de 1996 en Estocolmo, en el cual se plasmó la propuesta para la promoción de reformas en materia electoral, en particular, la institución de un documento único de identidad, cuyo propósito sería sustituir la cédula de vecindad, otorgando una mejor seguridad a la identificación de actos en la vida civil y electoral de las personas guatemaltecas, así como las que residan en el país.

Es decir, que después de ocho años de la firma del Acuerdo de Paz sobre Reformas Constitucionales y Régimen Electoral, en el año 2005 se crea al Registro Nacional de las Personas, como una institución autónoma, reconociéndole personalidad jurídica, técnica e independiente y con patrimonio propio, a diferencia del Registro Civil anteriormente vigente, que se encontraba a cargo de las municipalidades del país, y que se manejaban

bajo los propios criterios de cada municipalidad. Asimismo, cada municipalidad era la encargada de nombrar a registradores civiles, quienes eran revestidos de fe pública.

El Registro Nacional de las Personas, es una institución autónoma con personalidad jurídica, patrimonio propio y con capacidad de adquirir derechos y contraer obligaciones, y entre sus atribuciones principales se encarga de organizar y mantener el registro único de identificación de todas las personas naturales, llevando a cabo los asientos registrales desde su nacimiento hasta su muerte, según lo establece los Artículos 1 y 2 de la Ley del Registro Nacional de las Personas, Decreto número 90-2005 del Congreso de la República. Es decir, que este registro es el más importante para los guatemaltecos, en cuanto a la información que resguarda y maneja, ya que cuenta con la mayor base de datos sobre información personal de los guatemaltecos que acuden a esta para obtener seguridad y certeza jurídica de su identidad en armonía con los principios generales registrales.

4.2. Registro electrónico

El Registro Nacional de las Personas cuenta con el Registro Central de las Personas, cuya dependencia tiene a su cargo los Registros Civiles de las Personas, con presencia a nivel nacional, que se encargan de inscribir los hechos y actos con respecto al estado civil, capacidad, y demás datos de identificación de las personas naturales. La actividad

registral que realizan es de manera modernizada para agilizar y proveer de seguridad jurídica a las personas naturales.

Al trasladar las funciones registrales del Registro Civil a cargo de las Municipales al Registro Nacional de las Personas, la transferencia de información de los hechos y actos sujetos a inscripción sobre las personas naturales fue un largo proceso tortuoso de recopilación y restauración de libros, en la cual, se registraba de forma manual por medio del sistema de folio personal. Este traslado implico la actualización informática para la tecnificación de una institución, cuyo manejo información personal de los guatemaltecos es de vital importancia para garantizar seguridad jurídica de su resguardo.

Derivado de lo anterior, según el Artículo 12 del Reglamento de Inscripciones del Registro Nacional de las Personas, Acuerdo de Directorio Número 104-2015, los libros que se llevan en los Registros Civiles de las Personas son de forma electrónica cumpliendo los principios y características registrales de uniformidad, inalterabilidad, seguridad, certeza jurídica y publicidad, garantizando la perdurabilidad de datos e información que se capta y almacena. Asimismo, todos los documentos registrales se encuentran almacenados en archivos digitales por los Registros Civiles, para un mejor control y eficaz localización de información con ayuda de la informática jurídica de control o gestión, así como garantizar de mejor manera la conservación y custodia de los documentos e información.

Así pues, las gestiones automatizadas que realiza el Registro Civil de las Personas del Registro Nacional de las Personas de Guatemala, con ayuda de la informática jurídica, lo convierte en un registro electrónico sistemático. Este se encuentra auxiliado por la Dirección de Informática y Estadística, una dependencia enfocada en las actividades de almacenamiento y procesamiento de datos que gestione, canalice y almacene el Registro Central de las Personas. La ventaja de modernización de los Registros Civiles de las Personas fue la agilidad y efectividad en la gestión de solicitudes de los guatemaltecos. Sin embargo, los registros electrónicos conllevan aumentar la protección y la seguridad para evitar vulnerabilidad en los sistemas, y al mismo tiempo, capacitación normalización para evitar la sustracción de datos personales o su pérdida.

Actualmente el Registro Nacional de las Personas únicamente cuenta con políticas administrativas internas y normativa internacional estandarizada, como las normas ISO, para cubrir las necesidades de protección y seguridad informática.

4.3. Manejo de seguridad informática

El Registro Nacional de las Personas en su estructura orgánica cuenta con dependencias administrativas internas con funciones de monitoreo del área informática de la institución, entre estas dependencias encontramos la Dirección de Informática y Estadística, cuyo enfoque de actividades es el reguardo de la información; y por el otro lado, se encuentra

el Departamento de Seguridad Informática, que según el Artículo 50 del Reglamento de Organización y Funciones del Registro Nacional de las Personas, Acuerdo de Directorio Número 80-2016, esta dependencia es la encargada de la seguridad informática, por medio de actividades de monitoreo de los sistemas, garantizando la confidencialidad de la información contenida en los archivos digitales y el sistema.

La seguridad informática de los sistemas informáticos representa una prioridad para el resguardo de la información, por lo que el Registro Nacional de las Personas, en conjunto a sus dependencias técnicas a falta de la regulación de protección de la información ha implementado normas estandarizadas, a través de la política de seguridad de la información del año 2016, esta política permite la implementación de la norma UNE - ISO / IEC 27001:2014, sobre el Sistema de Gestión de la Seguridad de la Información, una norma de estandarización de la Organización Internacional de Normalización. Este sistema consiste en garantizar la confidencialidad, integridad y disponibilidad de la seguridad de la información, de esta forma se controlan y administran los riesgos y vulnerabilidades. Estas características de protección de datos son importantes, ya que son el mayor activo que posee el Registro Nacional de las Personas de Guatemala.

Los sistemas de gestión de riesgos y seguridad desarrollada por la ISO 27001, es una norma internacional que permite mejorar el manejo de sistemas de la institución registral, estableciendo estándares de evaluación y control de riesgos para la disminución o eliminación de los posibles daños. Es decir, que este sistema promueve protección solida

a los datos e información de los ataques a software o sabotajes del sistema informático. Se debe destacar que dicha norma está dirigida a trabajadores, contratistas, proveedores o personal de instituciones que se relacionan con el Registro Nacional de las Personas para garantizar la seguridad de la información.

Sin embargo, a pesar de la implementación de normas a través de políticas administrativas, su estructura y normatividad se limita únicamente a establecer estrategias específicas y determinadas a una institución, mas no posee el enfoque de la estructura de una norma jurídica, compuesta por el supuesto jurídico y la disposición normativa[25], esto quiere decir que no existe una consecuencia jurídica, que regule el incumpliendo a las estrategias fijadas sobre seguridad informática. Consecuentemente, la transgresión a las medidas de seguridad y al mismo tiempo se produzca la perdida, sustracción o alteración de información y datos personales, no existen en Guatemala normas que responsabilicen al autor de los actos o hechos jurídicos.

4.4. Manejo de datos personales

En la estructura orgánica del Registro Nacional de las Personas de la República de Guatemala, según lo establecido en el artículo 8 de la Ley del Registro Nacional de las

[25] García Máynez, Eduardo. **Lógica del concepto jurídico**. Pág. 172

Personas, Decreto Número 90-2005 del Congreso de la República, existen oficinas ejecutoras a las cuales les corresponden funciones específicas para el adecuado funcionamiento del registro. En cuanto al manejo de datos personales encontramos las siguientes dependencias: a) Registro Central de las Personas, que organiza y realiza mantenimiento del archivo central, asimismo administra la base de datos de la información personal de los guatemaltecos; b) Departamento de Base de Datos, esta se encarga técnicamente por el correcto funcionamiento de la base de datos, implementando políticas y normas para el resguardo de la información; c) Departamento de Análisis y Estadísticas, esta dependencia provee información a otras dependencias que tengan que ver con la información procurando mantener la confidencialidad e integridad de los datos personales almacenados en la base de datos del registro. Esto indica que el Registro Nacional de las Personas ha sido de gran utilidad para el manejo y control de datos personales de los guatemaltecos.

Por otro lado, la confidencialidad e integridad de la información, como lo señalado anteriormente, son principios que el registro pretende mantener para garantizar la protección de datos personales y base de datos. Consecuentemente, el registro ha implementado estrategias que establecen medidas a sus empleados y funcionarios, tales como, la definición de horarios de acceso a los sistemas, restricción de logueo en equipos específicos y la firma de cláusula de confidencialidad en los contratos de trabajo de cada empleado. Sin embargo, esto no ha sido suficiente para restringir y proteger la información que maneja el registro, ya que existen casos de ex empleados del registro

que han sido investigados y ligados a un proceso penal por la facilitación de información para la configuración de conductas ilícitas.

El manejo de datos personales implica el resguardo por medio de la informática jurídica y la seguridad informática, pero es necesario de proveer de normas jurídicas que establezca la consecuencia jurídica a conductas antijurídicas que impliquen el daño a los activos informáticos, así como a la base de datos de los datos personales que maneja el registro.

4.4.1. Regulación y control de los datos personales

El almacenamiento y archivo de datos personales a través se ha incrementado con la evolución de la tecnología y la informática que ha coadyuvado la sistematización y automatización que garantizan la disponibilidad de la información. Las tecnologías y la informática no son ajenas, ni se encuentran alejadas al ámbito jurídico, puesto que son de gran trascendencia para la sociedad de la información, y es el Derecho como disciplina que se encarga de promover la gestión de la protección de la información, tomando en cuenta que actualmente la información se ha convertido en una forma de poder.

Tal y como lo establece Téllez, "la información es un bien en sí, inmaterial pero constitutivo de un producto autónomo que por su contenido económico requiere una tutela jurídica en razón de los diferentes derechos y obligaciones que genera"[26], esto quiere decir, que se debe promover una regulación de los datos desde la perspectiva al Derecho a la protección de datos e intimidad de la persona, y al mismo tiempo, el acceso a datos personales o habeas data. Sin embargo, en Guatemala no existe regulación nacional sobre la protección y control del manejo de datos personales, para evitar las conductas antijurídicas, y mucho menos, se ha adoptado el compromiso internacional, adoptando convenios e instrumentos internacionales, para acoger medidas de protección informática para proveerle al Estado y a todas las instituciones que lo componen, especialmente los registros que manejan información personal.

[26] Téllez, **Op. Cit**. Pág. 69

CAPITULO V

5. Protección jurídica de los datos personales contenidos en los Registros electrónicos de las instituciones públicas del Estado de Guatemala

La protección jurídica de los datos personales se encuentra vinculado a los derechos humanos, reconocidos como fundamentales e inherentes a la persona humana. En primer lugar, se encuentra el derecho a la intimidad, cuyo funcionamiento se dirige a la protección ante cualquier invasión o violación a la vida personal y familiar, y al mismo tiempo la prevención de riesgos ante cualquier daño moral que pueda afectar a la persona.

Del derecho a la interinidad se derivan otros derechos jurídico morales, tales como, el **derecho a la imagen personal**, enfocado en la apariencia física y rasgos que permiten identificar a una persona, y como estos medios de identificación son plasmados en medios de reproducción; el **derecho de la personalidad**, que radica en la facultad de la persona de impedir la reproducción de la apariencia física o rasgos del titular sin su consentimiento; el **derecho al honor**, ligado al concepto de intimidad personal y familiar, que se enfoca en el respeto y estimación de una persona posee de sí misma y ante la sociedad; y por último, el **derecho a la identidad**, no es más que un derecho humano inalienable con el que cuentan todas las personas desde su nacimiento, de poseer un

nombre y apellido, en la legislación guatemalteca se encuentra dicho derecho en el Artículo 14 de la Ley de Protección Integral de la Niñez y Adolescencia, Decreto Número 27-2003 del Congreso de la República, que garantiza su protección estatal, así como de la prestación de una debida asistencia.

Ahora bien, de la trasgresión de los derechos humanos fundamentales anteriormente señalados, surgen los daños morales, que se encuentran divididos en dos facetas, por una parte, la positiva como una facultad personalísima de distribuir, imprimir, difundir, o publicar la propia imagen del titular y, por otra parte, la negativa, que busca impedir la obtención, reproducción o distribución de terceros sin autorización o consentimiento del titular de la imagen. Consecuentemente, el concepto de autodeterminación informativa surge a partir de la combinación de estas dos facetas, para evitar los daños morales. La autodeterminación informativa, no es más que el derecho fundamental de las personas de poseer el control sobre sus propios datos.

La importancia de proteger jurídicamente los datos personales, se deriva del deber estatal plasmado en los Artículos 1 y 2 de la Constitución Política de la República de Guatemala, ya que es el Estado de Guatemala, quien debe proteger a la persona y su familia, así como garantizarle la seguridad, por lo que cualquier dato personal, sea este íntimo o no, es parte del derecho a la protección de la persona. Los datos personales que se encuentran en registros electrónicos de instituciones estatales, deben estar

jurídicamente protegidos ante las amenazas o riesgos cibernéticos a los cuales pueda encontrarse expuestos.

Actualmente, Guatemala no cuenta con mecanismos de protección e implementación de seguridad cibernética a nivel nacional en cada una de las instituciones, por el contrario, se opera por medio de políticas de seguridad a nivel institucional de carácter técnico, que no significa que estás sean negativas, sino que se vuelven ineficaces al momento de encontrarse un ataque o la comisión de un acto o hecho ilícito en contra de los sistemas informáticos que albergan los datos personales de la base de datos, configurándose la trasgresión de derechos a la sociedad.

5.1. Vulnerabilidad jurídica de los datos personales

La vulnerabilidad jurídica implica la debilidad en la legislación guatemalteca, al no contemplarse los medios de protección ante amenazas o riesgos de los sistemas informáticos que contienen datos personales, ante la comisión de conductas ilícitas que afectan a los activos informáticos. No obstante, la vulnerabilidad jurídica implica al mismo tiempo la falta de seguridad y certeza jurídica ante el manejo de situaciones que impliquen conductas antijurídicas que afecten los datos personales, así como los daños morales que puedan producirse.

Legislativamente, en Guatemala únicamente se tratan y regulan los datos personales en el capítulo sexto, que se refiere al habeas data, de la Ley de Acceso a la Información pública, Decretó Número 57-2008 del Congreso de la República, siendo esta la única norma de nivel ordinario que regula los datos personales. Sin embargo, es limitativa ya que únicamente se refiere a la prohibición de comercialización de los datos sensibles o datos personales sensibles, no trata de la regulación del derecho de la intimidad, siendo esta la garantía de protección ante cualquier invasión de la vida personal o familiar.

El concepto de *habeas data* es tan complejo, que no se trata únicamente de regular la prohibición de comercialización de datos, el acceso de los datos personales y su tratamiento, sino que debe contemplar el proceso jurisdiccional que ampare la autodeterminación informativa, así como el derecho del titular de solicitar información sobre su persona, eliminar los datos o solicitar su corrección, si esta no fuere correcta o fuere necesario su actualización. Sin embargo, la vulnerabilidad jurídica de los datos personales no se limita únicamente a la adecuada regulación del *habeas data*, sino de la seguridad jurídica de la que se debe proveer a los sistemas informáticos para evitar las amenazas informáticas.

Toda amenaza o riesgo informático a los sistemas implica vulnerabilidad, que se convierte en jurídica cuando no se cuenta con los procedimientos jurídicos para perseguir o prevenir las amenazas o riesgos que involucran los datos personales. El contar con normativa que respalde la persecución de conductas antijurídicas vinculadas con el

cibercrimen y grupos que se centran en el rompimiento de la seguridad jurídica e informática fortalece a la seguridad de un Estado. La ausencia de normativa, o bien, ratificación de convenios internacionales en materia de cibercrimen, delitos informáticos y protección de datos, convierte a Guatemala en punto de riesgo informático.

No es suficiente la cobertura de las vulnerabilidades con políticas de seguridad informática, puesto que, es necesario la uniformidad de procedimientos de actuación ante amenazas, sin embargo, esto significa la actualización y formación tecnológica e informática, así como de las conductas antijurídicas que se produzcan a consecuencia de las amenazas producida a los sistemas informáticos, a los juristas, jueces y empleados y funcionarios públicos. Toda vulnerabilidad jurídica, se traduce como falta de agenda legislativa prioritaria y desinterés de protección de datos personales que se encuentran en la base de datos de registros electrónicos de las instituciones públicas de Estado, especialmente en instituciones como el Registro Nacional de las Personas de Guatemala.

5.2. Tráfico ilegal de datos personales

El concepto tráfico posee una doble connotación, por un lado la positiva, que se refiere a la negociación o "actividad lucrativa con la venta, cambio o compra de cosas o con

trueque y préstamo de dinero"[27], o bien, el transporte de cosas. Así como en el caso de la informática, se utiliza el término tráfico para la referencia del flujo adecuado de datos en los sistemas informáticos. Y por el otro lado, la connotación negativa, que se vincula con la realización de negocios no lícitos, así como el contrabando u otro comercio de carácter ilegal, que no se encuentra bajo las normas de determinado territorio.

El tráfico ilegal, desde la connotación negativa es concebido como una conducta antijurídica, por ser un acto o hecho realizado sin la autorización legal que se requiere, y que al mismo tiempo produce daños morales o patrimoniales al titular o al Estado. En la legislación guatemalteca, únicamente se acoge este término en la Ley contra la Narcoatividad, Decretó Número 48-92 del Congreso de la República de Guatemala, específicamente para referirse a cualquier acto de producción, fabricación, extracción, preparación oferta, distribución, depósito, almacenamiento, transporte, venta, suministro, posesión, adquisición o tenencia de cualquier droga, estupefaciente o sustancia psicotrópica.

En el derecho informático, es fundamental la protección de datos personales contra cualquier acto ilegal que se traduzca en afectaciones o daños a la sociedad, o bien directamente al Estado, es decir, la protección contra el cibercrimen y los delitos informáticos, al producirse la sustracción, extracción, alteración, tránsito, obtención no

[27] Ossorio, Manuel. **Diccionario de ciencias jurídicas, políticas y sociales.** Pág. 961

autorizada, adquisición por medios no autorizados, distribución o venta de datos personales, como consecuencia de ataque de los sistemas informáticos, base de datos o acceso ilícito a los sistemas informáticos de las instituciones, tanto privadas como públicas, que almacenan datos personales, con fines lucrativos o interés personal, siendo formas de realización de conductas antijurídicas de tráfico de datos personales.

No obstante, el tráfico ilegal de datos personales debe ser catalogado como una medida estatal de protección legislativa en contra de los abusos y ataques de sistemas para el uso y mal manejo de datos personales, ya que implica la vulnerabilidad de derechos humanos fundamentales que tienen que ver íntimamente con la persona. Para la determinación de la comisión de esta conducta contraria a lo jurídico, se debe tomar en cuenta que puede ser realizada por cualquier persona con conocimiento, o no, de informática, y en casos especiales por los mismos empleados o funcionarios públicos que desempeñen sus labores en la institución que maneje registros electrónicos de datos personales.

Consecuentemente, no solamente se debe configurar la seguridad informática, sino se debe garantizar esta, por medio de la determinación de responsabilidad del mal uso o manejo de datos personales.

5.3. Adecuado manejo de los datos personales, por parte de los empleados y funcionarios públicos

Los avances tecnológicos y la implementación de la informática jurídica de gestión, así como la informática jurídica documentaría, para la información personal que se resguarda, siendo estos medios auxiliares que facilitan el manejo, almacenamiento y ubicación en las bases de datos en los sistemas informáticos, siendo determinantes en la agilización de los recursos estatales. El adecuado manejo de datos personales se rige por un riguroso y estricto apego a la ley, disposiciones reglamentarias y manuales emitidos por la institución.

Toda institución en la cual se manejen y almacenen datos personales, especialmente en los registros públicos, el cuidado de la información es fundamental. Sin embargo, la ausencia de normas y políticas públicas, destinadas para la protección de datos personales, trae como consecuencia que gran parte de las bases de datos que se encuentran en poder de instituciones públicas estatales sean explotadas de manera ilegal. En el sentido que, toda información personal confiada a una institución, debe garantizar y amparar su protección ante cualquier uso ilegítimo en observancia de la tutela constitucional de la seguridad jurídica, la autodeterminación informativa y el derecho a la intimidad.

El uso inadecuado de los datos personales, tal y como lo señala Velasco Melo esto "a partir del abuso, ignorancia o desconocimiento de los derechos que tienen los individuos sobre la información confiada"[28] en una institución a la cual se confía el manejo, resguardo y uso de datos personales, y está a su vez cuenta con empleados y funcionarios que en el desarrollo de sus funciones en la institución, manejan datos personales de una base de datos que conlleva más que perjuicios morales. Muchos de los empleados o funcionarios que según él puesto en el que se encuentran, realizan conductas como las mencionadas anteriormente, esto con la disposición para obtener favores personales o bien, para un interés propio y lucrativo, lo cual no puede eximirse por ser justificativo de abuso de poder o autoridad, ignorancia o desconocimiento, puesto que representa una responsabilidad personal, y al mismo tiempo, solidaria con el Estado, por todo perjuicio provocado a los titulares de la información personal.

Un adecuado manejo de datos personales implica no solamente velar por la protección de los sistemas informáticos, sino exigir la responsabilidad por parte de empleados y funcionarios públicos, que utilizan la información personal de manera ilegítima y no autorizada, y contrario a los fines de la institución que resguarda los datos. En Guatemala, existen casos en los cuales se ha responsabilizado por la vía penal a ex trabajadores del Registro Nacional de las Personas, como por ejemplo en el caso de falsificación de documentos del año 2014, como consecuencia de aprovecharse lucrativamente de su puesto laboral para facilitar el documento personal de identificación

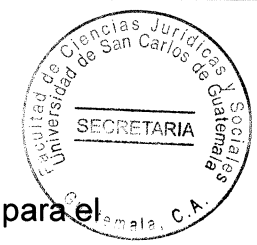
[28] Velasco Melo. **Op. Cit.** Pág. 346

a personas que no realizaron el trámite legal respectivo. Sin embargo, existen otros casos no reportados de acceso a sistemas informáticos para la sustracción y tráfico de datos personales.

5.3.1. Responsabilidad jurídica por el uso y manejo inadecuado de datos personales

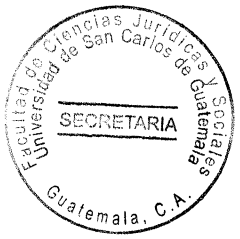
El actuar de los empleados y funcionarios públicos se encuentra estrictamente establecido en la ley, por tal motivo se encuentran constreñidos solamente a ella, puesto que su actuar puede ocasionar daños y perjuicios a terceros y al Estado. En lo que a datos personales implica, la responsabilidad de su manejo y utilización es aún más importante ante cualquier siniestro informático y actos antijurídicos que provoquen daños o perjuicios a esta. Según la Constitución Política de la República de Guatemala, en el Artículo 155 se establece las clases de responsabilidad existentes para funcionarios o trabajadores del estado que, en el ejercicio de su cargo, causen perjuicio a los particulares a consecuencia de la infracción a las leyes, y que convierte en solidario responsablemente a la institución donde este ejercida su cargo, o bien, al Estado.

Las clases de responsabilidad jurídica a las cuales debe responder el funcionario o trabajador del Estado, que haya realizado la conducta antijurídica son, por un lado, la responsabilidad administrativa, como consecuencia de la realización de una infracción a



normas establecidas o infracción a políticas, además de toda labor mal realizada para el Estado, implica un perjuicio en su funcionamiento; y por otro lado, la responsabilidad penal o criminal, la cual además de los delitos cometidos en afectación de la administración pública del Estado, se realizan conductas perjudiciales y que según el derecho internacional se catalogan como delitos informáticos.

El Estado de Guatemala en observancia del cumplimiento de sus funciones y en armonía por los principios de responsabilidad, legalidad, seguridad, protección a la persona y la justicia tutelados por la Constitución Política de la República, debe velar por la no alteración, sustracción y tráfico ilegal de datos personales e información personal que puedan realizados por empleados públicos o funcionarios.

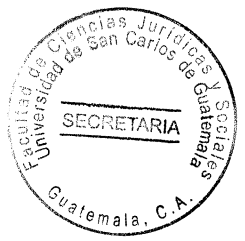

Facultad de Ciencias Jurídicas y Sociales
Universidad de San Carlos de Guatemala
SECRETARIA
Guatemala, C.A.

CONCLUSIÓN DISCURSIVA

En Guatemala, el uso de la informática jurídica, en especial la informática jurídica de gestión e informática jurídica documentaría, se ha convertido en una herramienta esencial para la sistematización y modernización de los registros públicos del Estado. Uno de los registros públicos más sistematizado, es el Registro Nacional de las Personas de Guatemala, el cual cuenta con la mayor base de datos sobre información personal y maneja un registro electrónico de los datos personales de los habitantes, que se refieren a actos y hechos que modifiquen el estado civil y la capacidad civil de las personas que en el registro se inscriban.

En esta investigación, se determina la importancia de la adecuada protección de los datos personales que debe llevarse a cabo en los registros públicos del Estado, como el Registro Nacional de las Personas de Guatemala. Debe alcanzar, en primer lugar, la seguridad de los sistemas ante los ataques cibernéticos; en segundo lugar, evitar el inadecuado uso y manejo de los datos personales; y, en tercer lugar, la determinación de la responsabilidad, tanto de terceros como de empleados y funcionarios públicos, a consecuencia de las conductas antijurídicas que causen perjuicio al titular del derecho.

La seguridad informática necesita la adecuación jurídica normativa para proteger y sancionar, derivado de los derechos humanos inherentes de los que se encuentran amparados los datos personales, tutelados constitucionalmente.


Facultad de Ciencias Jurídicas y Sociales
Universidad de San Carlos de Guatemala
SECRETARIA
Guatemala, C.A.

BIBLIOGRAFÍA

ACOSTA RAMÍREZ, René, Verdecia Díaz, Yadirka, y Amoroso Fernández, Yarina. **Jurimetría: Una opción para la sociedad**. La Habana, Cuba: Ed. Ediciones Futuro. Serie Científica de la Universidad de las Ciencias Informáticas. Vol. 9, 2016. http://www.egov.ufsc.br/portal/sites/default/files/1755-6338-1-pb.pdf (Consulta: 3 de diciembre de 2018)

ALVARADO LEMUS, José Rolando, Morales Pérez, Ronald Eduardo. **Ciber crimen.** Guatemala: Ius Ediciones, 2013.

BARRIOS OSORIO, Omar Ricardo**. Introducción de las nuevas tecnologías en el derecho**. Ciudad de Guatemala, Guatemala: Instituto de la Defensa Pública Penal, 2010.

FLORES SALGADO, Lucerito Ludmina**. Derecho informático**. México D.F., México: Ed. Grupo Editorial Patria. 2014.

FIGUEROA PERDOMO, Claudia Lavinia; Ramírez Gaitán, Daniel Ubaldo. **Derecho registral I**. Guatemala: Zona Gráfica, 2010.

MORGAN SANABRIA, Rolando. **Planeación del proceso de investigación científica para la elaboración de tesis de grado**. Guatemala: Impresos Ramírez, 2008.

GARCÍA MÁYNEZ, Eduardo. **Lógica del concepto jurídico**. México D.F., México: Fondo de Cultura Económica

GÓMEZ VIEITES, Álvaro. **Enciclopedia de la seguridad informática.** México, D.F., México: Alfaomega Grupo Editor S.A. de C.V. Ra.Ma., 2da. Ed., 2014.

OSSORIO, Manuel. **Diccionario de ciencias jurídicas, políticas y sociales**, Buenos Aires, Argentina: Ed. Heliasta S.RL., 1981.

PODER JUDICIAL DE LA FEDERACIÓN, Consejo de la Judicatura Federal. **Diccionario de derecho procesal constitucional y convencional.** México, D.F., México: instituto de investigaciones jurídicas, Universidad Autónoma de México. T. I, 2014.

RAMÍREZ, William, Juan Pablo Pons, Nadezhda Vásquez. **Libre acceso a la información, protección de datos y hábeas data.** Guatemala: Fundación Myrna Mack, 2003

REBOLLO DELGADO, Lucrecia, y SERRANO PEREZ, Mª Mercedes. **Introducción a la protección de datos**. 2ª ed., Madrid, España: Ed. Dynkinson, S.L., 2008.

RÍOS ESTAVILLO, Juan José. **Derecho e informática en México: Informática jurídica y derecho de la informática.** México D.F., México: Universidad Autónoma de México, Instituto de Investigaciones Jurídicas, 1997.

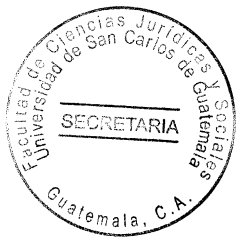
SECRETARÍA DE PLANIFICACIÓN Y PROGRAMACIÓN DE LA PRESIDENCIA. **Guía para la formulación de políticas públicas.** Guatemala: Segeplán, 2015.

TADDEI ELMI, Giancarlo. **Informática y derecho.** s.f. http://www.ittig.cnr.it/EditoriaServizi/AttivitaEditoriale/InformaticaEDiritto/IeD2004_1-2-Taddei.pdf (Consulta: 2 de diciembre de 2018)

TÉLLEZ VALDÉS, Julio. **Derecho informático**. Instituto de Investigaciones Jurídicas, Universidad Nacional Autónoma de México. 4ª ed., México, D.F., México: Ed. McGRAW-HILL/Interamericana Editores, S.A. de C.V., 2009.

UNIVERSIDAD INTERNACIONAL DE VALENCIA. **¿Qué es la seguridad informática y cómo puede ayudarme?** 21 de marzo de 2018. https://www.universidadviu.com/la-seguridad-informatica-puede-ayudarme/ (Consultado el 10 de diciembre de 2018).

VELASCO MELO, Arean Hernando. **El Derecho informático y la gestión de la seguridad de la información, una perspectiva con base en la norma ISO 27001.** Barranquilla, Colombia: Revista de Derecho, Fundación Universidad del Norte, enero-junio 2008.



Legislación:

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

Código Penal. Decreto Número 17-73, Congreso de la República de Guatemala, 1973.

Ley contra la Narcoactividad. Decreto Número 48-92, Congreso de la República de Guatemala, 1992.

Ley de Protección Integral de la Niñez y Adolescencia. Decreto Número 27-2003, Congreso de la República de Guatemala, 2003.

Ley del Registro Nacional de las Personas. Decreto Número 90-2005, Congreso de la República de Guatemala, 2005.

Ley de Acceso a la Información Pública. Decreto Número 57-2008, Congreso de la República de Guatemala, 2008.

Reglamento de Inscripciones del Registro Civil de las Personas. Acuerdo de Directorio Número 104-2015, Directorio del Registro Nacional de las Personas, 2015.

Reglamento de Organización y Funciones del Registro Nacional de las Personas. Acuerdo de Directorio Número 80-2016, Directorio del Registro Nacional de las Personas, 2016.

Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. Consejo de Europa. Estrasburgo, 1981.

Convenio sobre la Ciberdelincuencia. Consejo de Europa. Budapest, 2001.

Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas). Parlamento Europeo y del Consejo de la Unión Europea, 2002.