UNIVERSIDAD DEL AZUAY

FACULTAD DE CIENCIAS DE LA ADMINISTRACIÓN

ESCUELA DE INGENIERÍA DE SISTEMAS Y TELEMÁTICA

ENTORNO LEGAL SOBRE SEGURIDAD INFORMÁTICA DEL SECTOR FINANCIERO COOPERATIVO ECUATORIANO.

TRABAJO DE GRADUACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO DE SISTEMAS Y TELEMÁTICA

AUTOR: MARCOS VINICIO CALLE ARÉVALO

DIRECTOR: ING. ESTEBAN CRESPO MARTÍNEZ

CUENCA, ECUADOR

2017

Dedicatoria

El presente trabajo de graduación dedico a mis padres, Blanca y Marco, quienes me han ayudado y brindado todos los recursos necesarios para el cumplimiento de esta meta académica.

También dedico esta tesis a mis hermanos, Cristian y Michelle, y a mi abuelita Libia, que siempre han estado apoyándome y dándome ánimos para culminar la etapa Universitaria.

A María Belén por el apoyo que me ha brindado durante varios años de la carrera.

Agradecimientos

Agradezco a mi director de tesis, el Ing. Esteban Crespo por acompañarme en el desarrollo de este trabajo de graduación. Por su apoyo, enseñanzas y paciencia durante la guía en la realización del trabajo. Así mismo, agradezco a los miembros del tribunal conformado por el Ing. Francisco Salgado y el Ing. Diego Astudillo quienes me apoyaron con sus consejos y experiencia.

Así también, agradezco a los profesionales entrevistados por su apertura y por compartir sus conocimientos y experiencias en torno al tema del trabajo de graduación.

Índice

Índice de imágenes

Índice de tablas

Resumen

El riesgo en el tratamiento y custodia de información, debido al auge tecnológico, indudablemente es cada vez mayor. Este trabajo aborda el estudio de las normativas sobre seguridad de la información, considerando el contexto internacional hasta llegar a un nivel local, enfocándose específicamente en las regulaciones del sector financiero cooperativista del Ecuador. Se fundamenta en conceptos de Seguridad Informática y Seguridad de la Información, la Ley Orgánica de Protección de Datos, la Ley de Propiedad Intelectual, las Leyes relacionadas a servicios de información y las disposiciones del Sector Financiero ecuatoriano, emitidas por la Superintendencia de Economía Popular y Solidaria (SEPS).

Abstract

Risk in the treatment and custody of information due to the technological boom, is undoubtedly increasing. This work addresses the study of information security regulations, taking into account the international context up to a local level, and focusing specifically on the regulations of the cooperative financial sector of Ecuador. The study is based on IT security and information security concepts, the Organic Law on Data Protection, the Intellectual Property Law, regulations related to information services, and the provisions of the Ecuadorian financial sector issued by the Superintendency of Popular and Solidarity Economy (SEPS, as per its Spanish acronym).

UNIVERSIDAD DEL AZUAY
Dpto. Idiomas

Translated by,
Lic. Lourdes Crespo

Introducción

En la actualidad, el crecimiento exponencial de la tecnología ha ayudado a la automatización de los procesos y al almacenamiento de la información generada por las organizaciones. Sin embargo, conjuntamente han surgido técnicas para el robo de la información y esto se evidencia en gran medida en las instituciones financieras que manipulan información delicada y valiosa para las personas, como, por ejemplo, almacenar cantidades de dinero y de bienes. Existen órganos de control y leyes que sugieran buenas prácticas para la manipulación de dicha información. Sin embargo, en el ámbito nacional estas leyes están presentes, pero existe gran desconocimiento, que origina delitos que han quedado impunes, por ejemplo, el robo de números de tarjetas de crédito que han provocado fraudes económicos, entre otros.

Esta investigación se desarrollará con una indagación de conceptos fundamentales de Seguridad de la Información y Seguridad Informática, analizando el concepto de riesgo y de los estándares de la familia ISO/IEC 27000. Se realizará un análisis de las tendencias de ataques informáticos en el sector financiero a nivel internacional y local.

Así también, existirá una investigación sobre las leyes: (i) Ley Orgánica de protección de datos, (ii) Ley de la propiedad intelectual, (iii) leyes relacionadas con servicios de información y un estudio de las regulaciones o disposiciones que las mismas emiten.

Finalmente, se indagará sobre el sistema financiero ecuatoriano, específicamente del sector cooperativo, de sus órganos de control y normativas existentes en cuanto a la Seguridad de la Información. Una vez estudiado todo este marco legal, se procederá a realizar un extracto con las leyes aplicables al sector financiero cooperativo ecuatoriano.

Objetivos

Objetivo general:

Estudiar los aspectos legales que regularizan la seguridad de la información en el Ecuador, aplicados al sector financiero de la economía popular y solidaria.

Objetivos específicos:

- Evaluar los aspectos regulatorios sobre seguridad de la información a nivel local. Además, evaluar los aspectos internacionales usando como referencia

"Five Eyes", la Organización de Cooperación y Desarrollo Económico (OCDE), y la Asociación de Derecho Penal.

- Realizar un extracto de las leyes más relevantes que debería considerar una metodología para la gestión de riesgos en entidades de ahorro y crédito del Ecuador.

Justificación

La información generada, almacenada y manipulada por parte de las entidades del sector financiero cooperativo ecuatoriano es sensible y valiosa por lo que dichas organizaciones deben contar con mecanismos de protección de la misma. Estas entidades manipulan procesos sumamente delicados que deben ser respaldados y protegidos por leyes. A nivel local existen normativas que garantizan la seguridad informática, sin embargo, el desconocimiento casi total de las mismas genera delitos que en su gran mayoría no son sancionados.

A partir de este antecedente, se ve necesario realizar un estudio del entorno legal sobre Seguridad Informática del Sector Financiero Cooperativo Ecuatoriano que permita obtener un extracto de las normativas más importantes y relevantes que deberían ser aplicadas en dichas instituciones.

Alcance y Limitaciones

Este trabajo tiene como alcance el obtener un extracto con las leyes más importantes a ser consideradas para la gestión de riesgos en el sector financiero de la economía popular y solidaria del Ecuador. Mediante el estudio de las diferentes normativas tanto locales como internacionales existentes.

Capítulo I: Fundamentación teórica

1.1 Introducción

En este capítulo se profundizará los conceptos de seguridad de la información y seguridad informática con sus respectivas características. Se explicará el concepto de riesgo y sus tipos. Posteriormente, se realizará una indagación en la Ley de protección de datos, en la Ley de propiedad intelectual y en el Principio de no repudio. Se profundizará los estándares ISO de la seguridad de la información: ISO 27001, ISO 27002, ISO 27005 e ISO 31000. Finalmente, se indicarán las tendencias en ataques informáticos en el sector financiero a nivel internacional y local.

1.2 Seguridad de la información y seguridad informática

El avance de la tecnología ha permitido que las organizaciones involucren sus procesos con las tecnologías de la información facilitando la automatización de los mismos. La información que genera cada una de las organizaciones es muy valiosa, esto ha conllevado a la protección de dicha información ya que es vulnerable y puede ser hurtada.

La Seguridad de la Información agrupa un conjunto de medidas preventivas y reactivas que sirven para proteger la información de las organizaciones manteniendo la confidencialidad, disponibilidad e integridad de la misma. (Tola & Freire, 2015), involucrando al hardware, software y activos que almacenen información confidencial de la organización.

Está caracterizada por tres propiedades: (i) integridad, (ii) confidencialidad y (iii) disponibilidad.

(i) Integridad: se encarga de garantizar que los datos no sean alterados o destruidos de un modo no autorizado.

(ii) Confidencialidad: la información está disponible solamente para personas autorizadas, en determinados momentos y de manera acreditada.

(iii) Disponibilidad: se caracteriza por la capacidad que tiene la información de estar disponible para usuarios autorizados cuando estos la necesiten. (Aguilera, 2010)

Por otro lado, se define a la seguridad informática como la encargada de diseñar normas, procedimientos, métodos y técnicas que buscan establecer un sistema de información seguro y confiable. (Aguilera, 2010)

También se considera a la seguridad informática como un conjunto de recursos que garanticen la confidencialidad, integridad, consistencia y disponibilidad de los activos de una organización, los cuales, posean mecanismos de control de acceso y puedan ser auditados. (Ulloa, 2015)

Por ende, la seguridad informática y la seguridad de la información son las áreas encargadas de proteger y salvaguardar todo activo de una organización que genere información de la misma o que intervenga en sus procesos, es decir, hablamos del hardware y software que interviene en los procesos de la organización tanto para el almacenamiento como para la generación de la información.

1.3 Riesgo

El riesgo se puede definir como la medida del peligro que puede tener cualquier bien y se expresa a través de la ecuación:

Riesgo = Amenaza x Vulnerabilidad x Valor del bien

Donde:

- Amenaza se define como la causa potencial de un incidente no deseado.
- Vulnerabilidad es aquella acción negligente o de mala utilización que se realiza ante un bien.
- Valor de bien se precisa como los recursos necesarios para reemplazar o recuperar el bien a su estado anterior. (Nuñez, 2013)

Así también, se puede definir al riesgo como la estimación del grado de exposición de que una amenaza se haga realidad sobre uno los activos de una organización causando daños, es decir, es un impacto negativo para una organización ya que no permite cumplir los objetivos de una organización. (Matalobos Vega, 2009)

A pesar de esto, el riesgo está presente en cualquier situación por lo que es conveniente conocerlo y gestionarlo ya que si éste puede ser tratado correctamente generará una ventaja competitiva con otras organizaciones. Por esta razón el riesgo adopta un doble sentido:

(i) Tolerancia al riesgo: es la cantidad de riesgo que una organización pueda manejar.

(ii) Apetito de riesgo: es la cantidad de riesgo que una organización gestione con el fin de cumplir los objetivos establecidos. (Matalobos Vega, 2009)

Al gestionar correctamente el riesgo se puede conseguir varias ventajas, entre ellas las siguientes:

(iii) La organización es capaz de enfrentarse a situaciones con mayor seguridad.

(iv) Permite manejar información de mejor calidad que facilita la toma de decisiones.

(v) Facilita la detección temprana de las desviaciones brindando mayor tiempo para la toma de decisiones.

(vi) Brinda mayores ventajas competitivas debido a la comunicación con todos los grupos de interés. (Matalobos Vega, 2009)

1.4 Ley de protección de datos

Es "*Aquella parte de la legislación que protege el derecho fundamental de la libertad, en particular del derecho individual a la intimidad respecto del procesamiento manual o autónomo de datos*". El tratadista Antonio Pérez define señalando que "*Es el conjunto de bienes e intereses que pueden ser afectados por la elaboración de informaciones referente a las personas identificadas o identificables*". (García, 2011)

1.4.1 Datos Personales

Para José García, los datos personales hacen referencia a toda información que posee una persona, por ejemplo, su nombre, fecha de nacimiento, sexo, entre otras. Estos datos son los que permiten identificar al individuo como una persona única. Un dato personal debe ser correcto, completo, actualizado y relevantes según sea la actividad en la que vayan a ser utilizados (García, 2011)

Así también, en la legislación francesa, se considera a los datos personales como informaciones que de manera directa o indirecta identifiquen a una persona sin importar si su procesamiento haya sido hecho por una persona física moral. (García, 2011)

1.4.2 Protección de datos

Según García, es necesario que exista una protección de estos datos que garanticen la integridad de los mismos ante vulnerabilidades existentes en la actualidad. Existen

tratados internacionales que garantizan la protección de los datos personales, algunos se citan a continuación:

(i) Convención Europea de Salvaguardia de los Derechos del Hombre y las Libertades Fundamentales
(ii) El Pacto de San José de Costa Rica que es la Convención Americana de Derechos Humanos de 1969.
(iii) La Declaración Americana de Derechos y Deberes del Hombre, aprobada en la IX Conferencia Interamericana en la ciudad de Bogotá Colombia, en 1948;
(iv) La Declaración Universal de Derechos Humanos, aprobados por la Organización de las Naciones Unidas.
(v) El Pacto Internacional de Derechos Civiles y Políticos, firmado en Nueva York el 19 de diciembre de 1966.
(vi) Tratado de la Unión Europea de 07 de febrero de 1992.
(vii) El Parlamento Europeo ha dictado varias Resoluciones en el año de 1989.
(viii) La Organización de Cooperación y Desarrollo Económico OCDE en la Recomendación del 23 de Noviembre de 1980. (García, 2011)

A nivel mundial la Declaración Universal de Derechos Humanos garantiza el derecho a la protección de datos en su Art. 12. En la Convención Europea de Salvaguardia de los Derechos del Hombre y las Libertades Fundamentales cita en el Art. 18.1 el derecho que tiene toda persona a su vida privada. En el ámbito regional El Pacto de San José de Costa Rica reconoce en el Art. 25 el derecho que posee toda persona a un recurso sencillo y práctico, que lo ampare contra actos que violen los derechos fundamentales reconocidos por la Constitución y la ley; y, entre ellos el de la vida privada. (García, 2011)

A nivel local, es oportuno citar el Art. 66 de la Constitución del Ecuador en donde: "…*Se reconoce y garantizará a las personas: 19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos de información requerirán la autorización del titular y el mandato de la ley*". (Const., 2008, art. 66)

De igual manera, en el Art. 92, existe el habeas data que dicta lo siguiente: "*toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Asimismo, tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos.*

Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley.

La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación. En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias. Si no se atendiera su solicitud, ésta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados". (Const., 2004, art.92)

1.5 Ley de propiedad intelectual

El ser humano desde sus inicios ha estado en constante creación de nuevos artefactos que le faciliten el desarrollo de su vida y esta creación tiene un propietario de la obra generada. El propietario tiene el derecho de conservar y de compartir su obra como lo desee. Durante el desarrollo de la historia de la humanidad se han presentado casos de robo de obra por lo que ha sido necesario establecer leyes que protejan dichos derechos.

En la actualidad, el uso de las tecnologías de la información ha creado un nuevo ámbito en donde es necesario la creación de una legislación que abarque esta nueva esfera digital, la podemos denominar "*ciberlegislación*" que es la encargada de velar por los derechos de obra de los autores en el área digital. (Delgado, 2014)

La propiedad intelectual desarrolla dos objetivos:

(i) Protección del autor de la obra dada

(ii) Asegurar la difusión de la obra para beneficio del interés público.

Existen acuerdos internacionales de la propiedad intelectual de los cuales se han aprovechado muchos países poco desarrollados por considerar que el Internet es una fuente de intercambio científico, de crecimiento económico y de expansión cultural. A pesar de esto, nuestro país ha sido considerado como "*hiperproteccionista*" ya que cuenta con estándares superiores a los descritos en normas internacionales. (Delgado, 2014)

En el Art. 292 de la ley de propiedad intelectual se describe que al violar los derechos de autor la responsabilidad recae en el que comete el acto y en el que tenga el control del sistema informático siempre que el mismo tenga conocimiento de la posible infracción. (Delgado, 2014)

1.6 Principio de no repudio

En este principio se establece que al firmar un documento se manifiesta la conformidad con el contenido del mismo y que el autor que consta en el certificado, debidamente aceptado por el ente certificador, expresa su voluntad en dicho documento electrónico y acepta los efectos que del mismo se deriven, estando obligado a responder por lo que se establezca en el mismo ya que el documento es verídico. (Restrepo Figueroa, 2015)

1.7 ISO

La organización internacional de estándares conocida por sus siglas como ISO es una organización independiente, no gubernamental que cuenta con 162 miembros nacionales de normalización cuya sede está en Ginebra, Suiza. Se originó el 23 de febrero de 1947 en Londres bajo la reunión de 25 países. Esta organización se encarga de reunir a expertos con el fin de compartir sus conocimientos y desarrollar estrategias para apoyar la innovación y crear soluciones a los retos globales. (ISO International Standar Organization, 2016)

Existen normas para diferentes campos aplicativos van desde la tecnología, seguridad alimentaria, agricultura y salud. Estas normas son utilizadas para garantizar la calidad, seguridad y eficiencia de productos, servicios o sistemas facilitando el comercio internacional. En la actualidad existen 162 países como miembros y 3368 organismos técnicos que ayudan a elaborar los estándares. (ISO International Standar Organization, 2016)

1.7.1 ISO 27001

La norma ISO 27001 se encarga de proporcionar un modelo que establece, implementa, utiliza, monitorea, revisa, mantiene y mejora un Sistema de Gestión de Seguridad de la Información denotado por las siglas SGSI. (Tola & Otros, 2015)

Se enfoca en la gestión de riesgos y en la mejora continua de los procesos. Es a través de esta norma que se detalla los requisitos necesarios para la implementación del SGSI. (Ulloa, 2015)

Esta norma permite la certificación a nivel mundial que garantiza la seguridad de la información, está basada en el "*ciclo de Deming*", el cual sigue el proceso de: Planear, Hacer, Revisar y Actuar cuyas siglas en inglés forman el acrónimo PDCA. (Plan, Do, Check, Act). (Albarrán Trujillo & Otros, 2014)

La metodología que utiliza la norma ISO 27001 es la siguiente:

(i) Fase Plan: en esta fase se establece los objetivos, procesos, procedimientos para la administración de los riesgos con el fin de establecer el plan para la seguridad de la información que van de la mano de las políticas y objetivos de la organización.

(ii) Fase Hacer: en esta fase se pone en marcha el plan descrito en la fase anterior, es decir, se opera e implementa la política, controles, procesos y procedimientos.

(iii) Fase Revisar: en esta fase se monitoriza y revisa el SGSI evaluando objetivos, experiencias e informando los resultados a la administración de la organización.

(iv) Fase Actuar: consiste en ejecutar las acciones preventivas y correctivas basadas en las auditorías internas que permitan la mejora continua del SGSI. (Corletti Estrada, 2006)

1.7.2 ISO 27002

La norma ISO 27002 es la norma de buenas prácticas encargada de describir los objetivos de control y controles que se recomiendan seguir en cuanto a la seguridad de la información. Esta norma no es certificable (Ulloa, 2015)

Está formada por 39 objetivos de control y 133 controles agrupados en 11 dominios. Esta norma no se encuentra traducida en España. Para Colombia y Perú se encuentra traducida desde el 2006 y 2007 respectivamente. La descarga de la misma para el Perú

es gratuita. En la página oficial de las ISO se puede descargar la norma original en inglés y la traducción en francés. (ISO27000.es, 2012).

En Ecuador se adopta este estándar como NTE ISO/IEC 270002:2009 Tecnologías de la Información - Técnicas de Seguridad – Código de Práctica para los controles de Seguridad de la Información regida bajo la norma INEN. Dicha norma se encuentra traducida idéntica a la Norma Internacional ISO/IEC 27002:2013 con dos correcciones técnicas: 1:2014 y 2:2015, respectivamente. En el texto de la misma se han cambiado las palabras: "esta norma internacional" por "esta norma nacional". Así también, han sido necesarios los documentos:

(i) ISO/IEC 27000, Information technology-Security techniques-Information security management systems – Overwiev and vocabulary
(ii) NTE INEN-ISO/IEC 27000:2012, Tecnologías de la información – Técnincas de seguridad – Sistema de gestión de seguridad de la información – Descripción general y vocabulario. (INEN, 2015)

Los 11 dominios de la norma son:

(i) Política de seguridad
(ii) Aspectos Organizativos de la Seguridad Informática
(iii) Gestión de Activos
(iv) Seguridad ligada a los recursos humanos
(v) Seguridad física y del entorno
(vi) Gestión de comunicaciones y operaciones
(vii) Control de acceso
(viii) Adquisición, desarrollo y mantenimiento de sistemas de información
(ix) Gestión de incidentes en la seguridad de la información
(x) Gestión de la continuidad del negocio
(xi) Cumplimiento (Romo Villafuerte & Otros, 2012)

1.7.3 ISO 27005

Esta norma se encarga de suministrar las guías necesarias para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales de la norma ISO 27001 diseñada para colaborar en la aplicación satisfactoria de la seguridad de la información basada en la gestión de riesgos. La descripción de los conceptos, modelos, procesos y

términos que describe la ISO 27001 y la ISO 27002 facilitan el entendimiento de la ISO 27005:2008. (Ulloa, 2015)

La norma ISO 27005 puede ser aplicada en todos los ámbitos como en empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro cuya finalidad es la gestión de riesgos de la organización. Se puede adquirir su publicación original en inglés en la ISO. (ISO International Standar Organization, 2016)

1.7.4 ISO 31000

La ISO 31000 está encargada de proporcionar los principios y directrices genéricas para gestionar el riesgo. Fue publicada en noviembre de 2009. El ámbito de aplicación de la norma es amplio puede ir desde las empresas públicas, privadas o sociales, asociaciones, grupos o individuos. (ISACA, 2011)

Esta norma está estructurada en tres elementos:

(i) Principios para la gestión de riesgos
(ii) Estructura de soporte o Marco de Trabajo
(iii) El proceso de gestión de riesgos. (ISO Tools Excellence , 2016)

La ISO 31000 establece algunos principios que debe cumplir una organización, estos son:

(iv) La gestión del riesgo crea y protege al valor
(v) Es una parte integral de todos los procesos de organización
(vi) La gestión de riesgos es parte de la toma de decisiones.
(vii) Aborda explícitamente la incertidumbre
(viii) La gestión del riesgo es sistemática, estructurada y oportuna.
(ix) Se basa en la mejor información disponible
(x) La gestión de riesgo es la medida
(xi) La gestión de riesgo tiene los factores humanos y culturales en cuenta
(xii) La gestión de riesgo sea transparente e inclusivo
(xiii) La gestión de riesgos es dinámico, interactivo y de respuesta al cambio
(xiv) La gestión de riesgos facilita la mejora continua de la organización. (ISO International Standar Organization, 2009)

1.8 Ataques a la seguridad informática

1.8.1 Tendencias de ataques informáticos en el sector financiero a nivel Internacional

Según el informe de tendencias de *Kaspersky Lab* del 2015, son las familias de troyanos *Faketoken* y *Marcher* las principales amenazas financieras a celulares. *Faketoken* manipula al usuario a instalar una aplicación en su teléfono inteligente interceptando el código de confirmación (mTAN) y así toma el control de la base de datos bancaria del usuario. Por otra parte, *Marcher* roban los datos de pago de dispositivos con sistema operativo *Android*. Para robar los datos de la tarjeta de crédito, utilizan una falsa ventana de la aplicación "*Google Play*" que se activa cuando el usuario ingresa a la misma. También descarga una aplicación de banca móvil de un banco europeo.

Según Yuri Namestnikov: "*Este año los ciberdelincuentes han centrado su tiempo y recursos en el desarrollo de programas financieros maliciosos para dispositivos móviles. Esto no es sorprendente, ya que millones de personas ahora utilizan sus smartphones para pagar.*" (NAmestnikov, 2016)

Por lo que se comprende que la tendencia de este año ha sido encontrar formas de atacar a los dispositivos móviles en los cuales se realicen operaciones financieras. (Juste, Las amenazas de banca móvil, entre los ataques informáticos más extendidos, 2016)

Sin embargo, las amenazas tradicionales siguen presentes utilizando ordenadores cuyo fin es obtener la información financiera del usuario. La familia de troyanos *Zeus* que es la más utilizada para este fin, ha disminuido su presencia debido al crecimiento de *Dyre*, *Dyzap*, *Dyreza*. El último de estos es el encargado de generar el 40% de víctimas bancarias robando datos y accediendo al sistema online. (Juste, Las amenazas de banca móvil, entre los ataques informáticos más extendidos, 2016)

Según Intel, la nueva forma de ataque para robar información en los procesos de pago es buscar los nombres de usuario y contraseñas atacando a los consumidores, debido a que son los más vulnerables durante el sistema de pago utilizando ataques de pishing en las plataformas de pago de los celulares. (Juste, Ciberdelincuencia: ¿Cuáles serán las principales amenazas en 2016?, 2015)

En el ranking de países que generen ataques informáticos a nivel mundial se encuentra Estados Unidos, le siguen China, Francia y Holanda. A nivel regional Colombia es el

que ocupa el primer lugar, seguido por Perú, México y Chile. Latinoamérica tiene el 14.34% de ataques al sector financiero. (Gordón, 2016)

En Ecuador los ataques financieros se calculan alrededor de 6.600.000 por día, siendo el 75,29% del total de ataques con una tendencia de aumento al futuro. El ciberdelincuente estudia los perfiles en redes sociales, redes de seguridad y modos de acceso. (Freire, 2015)

1.8.2 Tendencias de ataques informáticos en el sector financiero a nivel local

Digiware considera a Ecuador como el primer país que genera ataques SQL Injection en la región. Estos ataques se caracterizan por infiltrar código intruso a través de una vulnerabilidad informática detectada en una aplicación que permita consultar a una base de datos. (Gordón, 2016)

Ecuador es considerado el cuarto país con mayor presencia de ataques con un 11.22%. (Freire, 2015)

1.9 Conclusión

Se ha demostrado que el desarrollo de la tecnología ha permitido la automatización de procesos y el almacenamiento digital de la información. Así también, ha facilitado la comunicación y la realización de procesos por parte de entidades o individuos. Por esta razón, se confirma la creación de leyes encargadas de proteger dicha información y de implementar una seguridad que ampare la integridad, confidencialidad y disponibilidad de la misma. Las áreas encargadas de dicha función son tanto la seguridad de la información como la seguridad informática que se encargan de proteger todo activo que le pertenezca a una organización o entidad que genere información o forme parte de sus procesos.

Se ha comprendido que toda información puede presentar cualquier tipo de situación que la afecte o cause daños, esto se conoce como riesgo y es de vital importancia contar con un plan que lo mitigue y permita corregirlo.

Con el fin de proteger a los datos de vulnerabilidades actuales y de garantizar la integridad de los mismos se ha establecido la Ley de protección de datos. Por otra parte, la información que genera un individuo o una entidad es propiedad de su autor y debe gozar de sus derechos o beneficiarse de la misma. Con este precedente, se estable la Ley de propiedad intelectual que se encarga de proteger al autor de la obra y de asegurar la

difusión de la obra para beneficio del interés público. Existen organismos internacionales creados específicamente para este fin.

La Organización Internacional de Estándares, conocida como ISO, ha implementado una serie de normas destinadas a la seguridad de la información, entre ellas: ISO 27001, ISO 27002, ISO 27005, ISO 31000.

Finalmente, se ha evidenciado que los principales ataques al sector financiero a nivel internacional son a través de virus troyanos que se implantan en teléfonos inteligentes a través de una aplicación que instala el usuario y roban códigos bancarios. Los ataques se han centrado y especializado en dispositivos móviles debido a su popularidad en los últimos años. Estados Unidos es el primer país en generar ataques informáticos, seguido por China, Francia y Holanda.

A nivel regional Colombia se posiciona en el primer lugar, seguido por Perú, México y Chile. Latinoamérica cuenta con un 14.34 % de ataques dirigidos al ámbito financiero. Es importante recalcar que nuestro país se encuentra como el primer país generador de ataques SQL Injection con la finalidad de robar información de una base de datos atacando su vulnerabilidad y cuenta con un 11.22% de ataques.

Capitulo II: Ley Orgánica de protección de datos

2.1 Introducción

En este capítulo se analizará la Ley Orgánica de protección de datos y el ámbito de acción de la misma. Se detallará el contexto de la Ley a nivel internacional y local. Así también, se profundizará en los conceptos de datos personales y datos institucionales. Finalmente, se realizará un estudio de las disposiciones y regulaciones que emite la presente Ley.

2.2 Aspectos generales

Las personas generan, consumen y poseen información diariamente, esta información no posee las medidas de seguridad y privacidad necesarias ya que cualquier persona puede acceder a la misma sin restricción alguna. El auge de las redes sociales y de la interacción de las personas con los medios digitales, ha facilitado el acceso a la información generada por las mismas. Debido a esto, es necesario que exista un control sobre el acceso, transformación, modificación o utilización de estos datos. Esta situación ha desencadenado regulaciones con el fin de equilibrar la protección de los datos y el uso de los mismos.

A nivel de Latinoamérica, específicamente en: Brasil, Colombia, Paraguay, Perú, Argentina, Ecuador, Panamá y Honduras, la regulación de la protección de datos se realiza a través del Habeas Data como derecho constitucional. Así también, en países como Argentina, Uruguay, México, Perú, Costa Rica y Colombia se han establecido leyes de protección de datos fundados en la Directiva de la UE de 1995. (Díaz, Jackson, & Motz, 2015)

En otro contexto, existe una mayor regulación en la protección de Datos en Europa, por ejemplo, España cuenta con la Ley Orgánica de Protección de Datos de Carácter Personal aprobada el 14 de diciembre de 1999 basada en el artículo 18 de la constitución española de 1978. El objetivo de esta ley es: "*garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar*" (DE ESPAÑA, 2013)

A nivel local, se puede señalar el hábeas data en el Art. 66, numeral 19 de la Constitución del Ecuador, que dicta lo siguiente: *"Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de*

la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Asimismo tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos.

Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley.

La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación. En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias. Si no se atendiera su solicitud, ésta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados". (Const., 2008, art 66)

Según el "Anuario del Derecho de las Tecnologías de la Información y las Comunicaciones" de España, la protección de datos personales se define como: "*el amparo debido a los ciudadanos contra la posible utilización por terceros, en forma no autorizada, de sus datos personales susceptibles de tratamiento automatizado, para de esta forma, confeccionar una información que, identificable con él, afecte a su entorno personal, social o profesional, en los límites de su intimidad.*" (Davara, 2004)

2.3 Datos personales

Al hablar de datos personales, se hace referencia a cualquier tipo de información que permita la identificación directa o indirecta de una persona, es decir, un nombre, una foto, la cédula de identidad, entre otros aspectos que tipifican a un individuo. (Díaz & Otros, 2015)

Así también, datos de carácter personal son aquellos que se consideran como cualquier información referente a personas físicas reconocidas. (DE ESPAÑA, 2013)

Para realizar la protección de estos datos rigen los siguientes principios:

(i) Previo consentimiento informado: los datos no podrán ser recabados, procesados, publicados o comunicados sin contar con el consentimiento del propietario. El consentimiento puede tener los siguientes estados:

a. Libre: podrá brindarse o no.
b. Previo: obtenido antes de solicitar los datos.
c. Expreso: no tácito o implícito.
d. Documentado: verificable
e. Informado: se notificará la finalidad de la recolección de los datos y dónde se realizará el control.

(ii) Legalidad: se debe seguir la normativa de las bases de datos personales e incluso inscribirse en un registro en algunos países.

(iii) Veracidad: estos datos deben ser auténticos, adecuados, imparciales y no excesivos según sea el propósito con el cual fueron obtenidos.

(iv) Finalidad: los datos serán utilizados únicamente para el propósito con el cual fueron recolectados, cumplido el mismo deberán ser eliminados.

(v) Seguridad: seguir las medidas mínimas de seguridad de los datos personales.

(vi) Reserva: estos datos deberán ser utilizados para el único propósito con el que fueron recolectados y aplicar la confidencialidad a las personas que accedan a los mismos.

(vii) Responsabilidad: estarán a cargo de la persona física o jurídica que acceda a la base de datos. Así como, el tratamiento o procesamiento que se realicen con los mismos. (Díaz, Jackson, & Motz, 2015)

2.4 Datos Institucionales

Al mencionar datos institucionales, se ha referencia a la información generada por una empresa o una entidad, como, por ejemplo, estados financieros, balances, entre otros. Esta información es sensible ya que almacena datos de suma importancia para las empresas, que no debe ser revelada a cualquiera.

La información que genera una empresa es su mayor activo intangible, ya que, mediante ésta, se adquiere ventaja competitiva, además permite conocer el estado de la empresa, los clientes o socios que posee, resoluciones tomadas, planes estratégicos, medidas de seguridad, nómina de empleados y otros, que al ser vulnerada o robada genera grandes pérdidas. Así también, cuando una persona le otorga sus datos a la empresa estos deben ser tratados de la manera adecuada garantizando el buen uso por parte de la empresa. En este ámbito entra la Ley de la protección de datos personales, ya que debe velar por los datos otorgados.

Por otro lado, existen convenios en los que diferentes entidades realizan cruces de información, es decir, una entidad puede transferir los datos a otra con el fin de validar la información. Para esto, en nuestro país, se ha creado la Dirección Nacional de Registro de Datos Públicos que a través de la Ley del Sistema Nacional de Registro de Datos Públicos, publicada en el Suplemento número 162 de 31 de marzo de 2010 del Registro Oficial, se encarga de regular el sistema de registro de datos públicos y su acceso, en entidades públicas o privadas, con el fin de garantizar la seguridad, organización, sistematización e interoperabilidad de los datos. (Carvallo, Protección de datos y habeas data en la legislación ecuatoriana: presente y futuro, 2014). Sustentándose en lo que describe en su Capítulo II: "*las instituciones del sector público y privado y las personas naturales que actualmente o en el futuro administren bases o registros de datos públicos son responsable de la integridad, protección y control de los registros y bases de datos a su cargo*".

Con estos antecedentes, en Ecuador la Constitución establece la Función de Transparencia y Control Social, encargada de promover e impulsar el control de las entidades y organismos del sector público, y de las personas naturales o jurídicas del sector privado que presten servicios o desarrollen actividades de interés público. (Carvallo, 2014)

En otro contexto en España, la Agencia de protección de datos establece una serie de medidas y parámetros que las empresas o entidades deben cumplir para garantizar la protección de datos. (DE ESPAÑA, 2013)

2.5 Regulaciones y disposiciones sobre la protección de datos

La protección de datos descansa sobre los siguientes principios:

(i) Consentimiento del titular de los datos: la persona titular de los datos es la única capaz de decidir cuándo, cómo, dónde y quién trata los mismos.

(ii) Calidad de datos: los datos necesitan ser pertinentes, adecuados y no excesivos según sea la finalidad con la cual se receptaron.

(iii) Información en la recolección de los datos: la persona que realizará el tratamiento de los datos deberá informar a su titular antes de realizar las operaciones sobre los mismos e indicará la finalidad y los destinatarios. Así también, será capaz de responder las interrogantes generadas por el titular.

(iv) Cesión o comunicación de datos: la cesión de los datos deberá tener el consentimiento del titular y garantizará que su uso será sólo para la finalidad expresada.

(v) Principio de no discriminación: la recolección de datos no permitirá discriminación sobre raza, color, vida sexual, religión, afiliación política o cualquier creencia. (DE ESPAÑA, 2013)

A su vez, existen derechos que comprenden la protección de datos. Por parte el titular de los datos tiene el derecho a la autodeterminación informativa que le brinda el conocimiento de todo lo relacionado con el tratamiento de sus datos.

Desde la parte del responsable de realizar las operaciones con los datos surgen tres derechos:

(i) Derecho de acceso: se caracteriza por la potestad que tiene el titular de los datos en dirigir al responsable del tratamiento información relacionada con la misma.

(ii) Derecho de rectificación: el titular de los datos cuenta con la facultad de exigir al responsable del tratamiento la calidad de los datos.

(iii) Derecho de cancelación: el titular de los datos tiene la potestad de retirar sus datos del tratamiento ya sea porque están incorrectos o porque no tiene la disposición de hacerlo. (Núñez , 2007)

A nivel regional la situación tiene varios contrastes, ya que en algunos países existen legislaciones establecidas y organismos de control pero en otros la protección de datos se ampara en algunos artículos de su constitución. En la mayoría de casos, se desconoce la existencia de las leyes y muchas violaciones quedan sin castigo.

Se presenta una vista general de algunos países de Latinoamérica y la legislación vigente en los mismos en cuanto a la Protección de Datos. Por ejemplo, Argentina cuenta con la ley de Protección de datos personales desde el año 2000. Es uno de los primeros países de Latinoamérica en contar con un órgano de control para la protección de datos personales. Este órgano es la Dirección Nacional de Protección de Datos Personales (PDP). Se presentan a continuación las leyes que interfieren en dicha protección:

(i) Ley 25.326, del 2 de noviembre, de Protección de Datos

(ii) Decreto 1558/2001. Reglamentación de la Ley de Protección de Datos

(iii) Ley 26.343, de 8 de enero de 2008 (modificación de la Ley 25.326)

(iv) Ciudad Autónoma de Buenos Aires. Ley 1845 de Protección de Datos Personales. (PDP Protección de Datos Personales, 2016)

Bolivia no posee una ley específica para la protección de datos, sin embargo, en su constitución existen varios artículos que amparan la protección de los mismos. Estos son: artículo 21.2, artículo 130 y artículo 131. También existen leyes que avalan este principio, estas son:

(i) Código Penal, en sus artículos 363 Bis y 363 ter. Delitos informáticos

(ii) Ley N. 28168, de 18 de mayo de 2005. Acceso a la Información del Poder Ejecutivo (Artículo 19: Petición de Hábeas Data)

(iii) Ley Nº 018, de 16 de junio de 2010, del Órgano Electoral Plurinacional. Artículos 72 (obligaciones); 74 (Registro y actualización de datos); 76 (Padrón Electoral); 77 (Lista de habilitados e inhabilitados), y 79 (acceso a información del Padrón Electoral).

(iv) Ley Nº 164, de 8 de agosto de 2011, General de Telecomunicaciones, Tecnologías de la Información y Comunicación. Artículos 54 (derechos de los usuarios); 56 (inviolabilidad y secreto de las comunicaciones); 59 (obligaciones de los operadores y proveedores); 84 (reglamentación); 89 (correo electrónico personal); 90 (correo electrónico laboral), y 91 (comunicaciones comerciales publicitarias por correo electrónico o medios electrónicos).

(v) Decreto Supremo Nº 1793, de 13 de noviembre de 2013. Reglamento de la Ley Nº 164. Artículos 3 (definiciones); 4 (principios), 40 (funciones de la Agencia de Registro); 54 (derechos del titular del certificado); 56 (Protección de datos personales), y 57 (comunicaciones comerciales publicitarias). (NovaGob La red social de administración pública, 2015)

En Chile existe la Ley 19628 a la protección de la privacidad de las personas que dicta lo siguiente: "*El tratamiento de los datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares se sujetará a las disposiciones de esta ley, con excepción del que se efectúe en ejercicio de las libertades de emitir opinión y de informar, el que se regulará por la ley a que se refiere el artículo 19, N° 12, de la Constitución Política. Toda persona puede efectuar el tratamiento de datos personales,*

siempre que lo haga de manera concordante con esta ley y para finalidades permitidas por el ordenamiento jurídico. En todo caso deberá respetar el pleno ejercicio de los derechos fundamentales de los titulares de los datos y de las facultades que esta ley les reconoce.". La Constitución de este país protege a los datos a través de su artículo 19, en el numeral 4. (NovaGob La red de administración pública, 2015)

En otro contexto, Colombia cuenta con una ley de protección de datos personales establecida desde el 2012 y su reglamento creado en el 2013. Este país cambió la figura del Hábeas Data por esta nueva ley. La finalidad de dicha ley es la siguiente: "*La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma."* (Ley Estatutaria 1581, 2012, art. 1) Así también, cuenta con el artículo 15 de su constitución que vela por la seguridad de los datos y con leyes específicas para el tratamiento de los datos, enumeradas a continuación:

(i) Decreto 886 del 134 de mayo de 2014. Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos.
(ii) Ley 1712 del 6 de marzo de 2014. Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones.
(iii) Ley 270/1996, sobre Administración de Justicia (Artículo 95).
(iv) Ley 527, del 18 de agosto de 1999, sobre Mensajes de Datos, Comercio Electrónico y Firma Digital (Arts. 2 y 32).
(v) Ley 57/1985, en materia de Acceso a la información (Arts. 12 y 20).
(vi) Decreto 2870/ 2007, sobre utilización de la red de telecomunicaciones del Estado.
(vii) Resolución 575/2002, sobre Telecomunicaciones.
(viii) Resolución MC 2578/ 2007. Garantiza inviolabilidad de comunicaciones (NovaGob La red de administración pública, 2015)

Una vez analizado el ámbito de algunos países, se procede a investigar sobre la legislación que rige en el Ecuador referente a la protección de los datos. El Ecuador

posee una legislación sectorial, detallada en varias leyes, que involucran la protección de datos, estas son:

(i) Ley No. 162, de 31 de marzo de 2010 del Sistema Nacional de Registro de Datos Públicos

(ii) Ley No. 13, de 18 de octubre de 2005, de Burós de Información Crediticia:

a. Artículo 5. "*La información de riesgos que obtengan y mantengan los burós tendrá· por exclusiva finalidad destinarla a la prestación del servicio de referencias crediticias y deberán mantenerla en el país.*

La información histórica crediticia requerida sobre personas naturales y jurídicas, no podrá exceder de 6 años, por tanto, a los burós de información crediticia les está· prohibido expresamente recabar y proporcionar información anterior a este límite. Sólo con el conocimiento pleno y la autorización previa del titular de la información crediticia, en cada operación, los burós de crédito podrán obtener y mantener en sus archivos la nueva información crediticia distinta de aquella proveniente de la Central de Riesgos. En este caso, los clientes de los burós pondrán en conocimiento de los titulares de la información crediticia, lo siguiente:

i. La existencia de las bases de datos que administran los burós, su finalidad y los potenciales destinatarios de la información;

ii. La identidad y dirección de los burós que recepten la información;

iii. Las posibles consecuencias del uso de la información; y,

iv. *Los derechos que les asisten. El buró de crédito que obtenga y archive esa información, con la simple solicitud del titular de la información y sin ningún otro trámite, obligatoriamente, deberá entregársela tantas y cuantas veces la requiera, de forma irrestricta y totalmente gratuita. La información crediticia ser· lícita, exacta y veraz, de forma tal que responda a la situación real de su titular en determinado momento. En cada reporte los burós deberán especificar la fecha a la que corresponde la información. Los titulares de información crediticia pueden proporcionar directamente a los burós su propia información, en*

cuyo caso los burós deberán informarles previamente lo señalado en las letras a), b), c) y d) de este artículo. La información proveniente de la Central de Riesgos, no requiere autorización." (Ley 13, 2005, art 5)

b. Artículo 6. "*Los burós solo podrán recolectar, acopiar, almacenar, actualizar, grabar, organizar, sistematizar, elaborar, seleccionar, confrontar, interconectar en sus bases de datos, información referente al riesgo crediticio. En consecuencia, no podrán manejar la siguiente información:*

i. Aquella que, por afectar el derecho a la intimidad personal o familiar, lesione las garantías previstas en los numerales 8, 11 y 21 del artículo 23 de la Constitución Política de la República, a través de la difusión de características físicas, morales o emocionales de una persona o cualquier otra información relacionada con circunstancias de su vida afectiva o familiar, hábitos personales y de consumo, ideologías, opiniones políticas, creencias o convicciones religiosas, estados de salud físico o psicológico, vida sexual o información genética; así como toda violación a las garantías previstas por las leyes, tratados y convenios internacionales; y,

ii. *La información que de conformidad con la Ley General de Instituciones del Sistema Financiero, se encuentre protegida por el sigilo bancario, así como la información del patrimonio personal y familiar, las cuales solo pueden ser entregadas por expresa orden judicial. El buró no podrá· recolectar, procesar o difundir la información prohibida expresamente en este artículo, aunque cuente con la autorización del titular de la información; en todo caso, 4 quien se considere afectado por la violación del presente artículo podrá· iniciar las acciones civiles y penales a que hubiere lugar.*" (Ley 13, 2005, art 6)

c. Artículo 7. "*Los burós sólo podrán prestar servicios de referencias crediticias a clientes debidamente identificados. Solo podrán ser clientes de los burós de información crediticia:*

i. *Las instituciones controladas por la Superintendencia de Bancos y Seguros;*

ii. *Las personas jurídicas, empresas, fundaciones y otras sociedades legalmente autorizadas y que otorguen crédito; y,*

iii. *Las personas naturales que se dediquen a actividades económicas, que cuenten con el Registro único de Contribuyentes actualizado y que otorguen crédito. Los burós no podrán comercializar a título universal sus bases de datos ni entregar toda la información crediticia contenida en las mismas, ni podrán dar a conocer esta información por medios de comunicación colectiva tales como radio, prensa, televisión u otros medios."* (Ley 13, 2005, art 7)

d. Artículo 8. "*Los clientes de los burós y cualquier otra persona que por diversas causas lleguen a tener acceso a reportes emitidos por los burós (incluyendo a funcionarios, empleados, agentes, entre otros), deberán obligatoriamente guardar confidencialidad sobre la información contenida en ellos, siendo prohibido utilizarla para fines distintos del análisis de riesgo crediticio. Quien empleare o divulgare indebidamente la información contenida en un reporte de crédito o alterare la información proporcionada por la fuente, estar· sujeto a las sanciones establecidas en el artículo 201 del Código Penal, sin perjuicio de las acciones y responsabilidades civiles a las que hubiere lugar."* (Ley 13, 2005, art 8)

e. Artículo 9. "*El titular de la información crediticia tendrá derecho a:*

i. *Conocer si en la base de datos de un buró existe información sobre sí mismo y acceder a ella sin restricción alguna; y,*

ii. *Exigir de la fuente de información crediticia, la rectificación de la información ilegal, inexacta o errónea y comunicarla al buró para que Éste, de ser el caso, la rectifique. Dentro del plazo de quince días desde la presentación de la solicitud, las fuentes de información crediticia obligatoriamente la resolverán, por escrito, admitiéndola o rechazándola motivadamente y poniendo en conocimiento de los burós autorizados para operar. Hasta tanto, sin perjuicio de continuar incluyéndola en los reportes de*

riesgos que emitan, los burós anunciaron que la información materia de la solicitud estará siendo revisada a pedido del titular. Si se concluye que la información materia de impugnación del titular es ilegal, inexacta o errónea, el buró, por cuenta de la fuente de información crediticia, inmediatamente enviar· comunicaciones certificatorias a todos quienes hubieren recibido reportes conteniéndola." (Ley 13, 2005, art 9)

f. Artículo 10. "*Los burós y las fuentes de información crediticia serán legalmente responsables por los dos ocasionados al titular como consecuencia de la transmisión de información 5 ilegal, inexacta o errónea y, por tanto, no estarán exonerados alegando ausencia de dolo o de culpa. La responsabilidad de las fuentes es entregar información a los burós de manera exacta y legal; la responsabilidad de los burós es reportarla sin alteración o modificación alguna. Sin perjuicio de lo anterior, en los procesos promovidos contra los burós, Éstos podrán pedir que se cite también con la demanda a la o las fuentes de las que hubieren obtenido la información crediticia materia del proceso, siguiendo el procedimiento establecido en el artículo 94 del Código de Procedimiento Civil. También responderán por los dos causados al titular de la información crediticia, quienes utilicen dolosa o culposamente informaciones o reportes provenientes de los burós. El afectado podrá· demandar indemnización, cuando la información errónea no ha sido rectificada por los burós."* (Ley 13, 2005, art 10)

(iii) Ley No. 67, de 17 de abril de 2002, de Comercio Electrónico, Firmas y Mensajes de Datos

a. Artículo 9. "*Protección de datos.- Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros. La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República y esta ley, los cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente. No será preciso el*

consentimiento para recopilar datos personales de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de la administración pública, en el ámbito de su competencia, y cuando se refieran a personas vinculadas por una relación de negocios, laboral, administrativa o contractual y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato. El consentimiento a que se refiere este artículo podrá ser revocado a criterio del titular de los datos; la revocatoria no tendrá en ningún caso efecto retroactivo." (Ley 67, 2002, art 9)

(iv) Ley Orgánica de Transparencia y Acceso a la Información Pública, de 18 de mayo de 2004.

Así también, la Asociación Ecuatoriana de Derecho Informático y Telecomunicaciones, conocida por sus siglas AEDIT, desarrolla un proyecto para la Protección de Datos que se encarga de realizar una propuesta para la creación de una ley que regule el acceso y confidencialidad de los datos. (AEDIT Asociación Ecuatoriana de Derecho Informático y Telecomunicaciones, 2003)

Se presenta a continuación los artículos de la Constitución del Ecuador que hacen referencia a la protección de datos:

(v) Artículo 11. Número 9: "*Determina que el más alto deber del Estado consiste en respetar y hacer respetar los derechos garantizados en la Constitución, lo cual implica la obligación estatal de adecuar formal y materialmente, las leyes y normas de inferior jerarquía a la Constitución y los instrumentos internacionales, e implementar las normas que sean necesarias para garantizar la dignidad del ser humano."* (Const., 2008, art. 11)

(vi) Artículo 66. Número 19: "*"El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley*"." Número 20: "El derecho a la intimidad personal y familiar."" Número 21: ""*El derecho a la inviolabilidad y al secreto de la correspondencia física y virtual; ésta no podrá ser retenida, abierta ni examinada, excepto en los casos previstos en*

la ley, previa intervención judicial y con la obligación de guardar el secreto de los asuntos ajenos al hecho que motive su examen. Este derecho protege cualquier otro tipo o forma de comunicación"."(Const., 2008, art66)

(vii) Artículo 92. ""*Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Asimismo tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos.*

(viii) Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley.

(ix) *La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación. En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias. Si no se atendiera su solicitud, ésta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados*"." (Const., 2008 , art 92)

2.6 Conclusión

El crecimiento de la tecnología, en especial de los medios sociales, ha generado la implementación de nuevas medidas para salvaguardar la información que es creada, usada y almacenada por las personas. Se considera dos tipos de datos: los datos personales que se encargan de identificar de manera directa o indirecta a una persona y los datos institucionales que son aquellos producidos por entidades o empresas, como por ejemplo: estados financieros, balances, planes estratégicos, entre otros. Esta información es sumamente valiosa siendo considerada como el activo principal de las entidades.

Es así que países como Brasil, Colombia, Paraguay, Perú, Argentina, Ecuador, Panamá y Honduras han implementado el derecho constitucional conocido como Habeas Data que se encarga de proteger los datos que los individuos generen. En nuestro país el

numeral 19 del Art. 66, numeral 9 del Art. 11 y Art. 92 de la Constitución patrocinan la protección de los datos. Así también, la Ley No. 62 del Sistema Nacional de Registro de Datos públicos y la Ley No. 13 de Burós de Información Crediticia se han implementado con el fin de salvaguardar los datos.

El Ecuador se encuentra en una etapa de inicio en cuanto a la protección de datos en comparación a otros contextos como el de España, que tiene la Ley Orgánica de Protección de Datos de Carácter Personal establecida en 1999 con antecedentes positivos en cuanto a su control y regulación.

Capítulo III: Ley de propiedad intelectual

3.1 Introducción

En este capítulo se describirá el concepto y ámbito de acción de la Ley de propiedad intelectual. Se explicará la propiedad intelectual personal e institucional. También, se detallará y citará cuáles son las regulaciones y disposiciones de la misma Ley.

3.2 Aspectos generales

Se entiende como propiedad intelectual a las creaciones de la mente: invenciones, obras literarias y artísticas, así como símbolos, nombres e imágenes utilizados en el comercio. (OMPI, 2015)

La propiedad intelectual puede definirse como todas las invenciones de la mente, por ejemplo, obras literarias, artísticas, invenciones científicas e industriales con sus símbolos, nombres e imágenes que reconocen a su autor como titular de la creación o invento y beneficiario del mismo. (IEPI , 2016)

A su vez, la propiedad intelectual se divide en dos categorías:

(i) Propiedad industrial: incluye las patentes de invención, registros de marca, los diseños industriales y las indicaciones geográficas.

(ii) Derecho de autor: incluye las obras literarias, novelas, poemas, obras de teatro, películas, música, dibujos, pinturas, fotografías, esculturas y diseños arquitectónicos.

   a. Derechos conexos: derechos de los artistas intérpretes y ejecutantes, de los productores de fonogramas y de los organismos de radiodifusión. (OMPI, 2015)

España define como Propiedad Intelectual: *"al conjunto de derechos que corresponden a los autores y a otros titulares (artistas, productores, organismos de radiodifusión) respecto de las obras y prestaciones fruto de su creación"* y el ente regulador es el Ministerio de Educación, Cultura y Deporte del Gobierno de España. (Ayllón Gutiérrez, 2014)

En el Ecuador la Ley de Propiedad Intelectual en su Art. 1 describe el ámbito que comprende la Propiedad Intelectual:

(i) "*Los derechos de autor y derechos conexos.*

(ii) La propiedad industrial, que abarca, entre otros elementos, los siguientes:

i. Las invenciones;

ii. Los dibujos y modelos industriales;

iii. Los esquemas de trazado (topografías) de circuitos integrados;

iv. La información no divulgada y los secretos comerciales e industriales;

v. Las marcas de fábrica, de comercio, de servicios y los lemas comerciales;

vi. Las apariencias distintivas de los negocios y establecimientos de comercio;

vii. Los nombres comerciales;

viii. Las indicaciones geográficas; e,

ix. Cualquier otra creación intelectual que se destine a un uso agrícola, industrial o comercial.

(iii) Las obtenciones vegetales."

3.3 Propiedad intelectual personal

Se hace referencia a propiedad intelectual personal a las creaciones o invenciones personales que se encuentran amparadas en la Ley de la Propiedad Intelectual. A partir de esto, se reconoce los derechos de autor como: "una disciplina que protege las obras de la capacidad humana, su relación con el autor y con la sociedad". Por lo tanto, este derecho es el encargado de velar por las facultades que goza el autor en relación con su obra y de todos los beneficios que genere la misma. (Solorzano, 203)

Se considera como persona física a la que realiza la creación intelectual y quien tiene la titularidad de los derechos de su obra. El derecho de autor le reconoce dos facultades:

(i) De carácter personal: conforma el derecho moral, es decir, la tutela de la personalidad del autor en relación con su obra destinada a garantizar intereses intelectuales.

(ii) De carácter patrimonial: conforma el derecho patrimonial, es decir, la explotación de la obra que posibilitan al autor la obtención de un beneficio económico. (Solorzano, 203)

En la Ley de Protección de Datos del Ecuador, la protección del derecho de autor abarca "*todas las obras de ingenio, en el ámbito literario o artístico cualquiera que sea su*

género, forma de expresión, mérito o finalidad". Si un individuo desea obtener los derechos de autor y derechos conexos de su obra, es necesario que registre su obra en la Unidad de Registro del Instituto Ecuatoriano de la Propiedad Intelectual (IEPI), con el fin de obtener los beneficios que genere la misma (Solorzano, 203). A través de la Ley de la Propiedad Intelectual y del registro en el IEPI podrá acceder a sus derechos y beneficios por su obra, no habrá distinción alguna por el género o ámbito en el que se desarrolle o se cree.

3.4 Propiedad intelectual institucional

Así como las creaciones personales poseen sus derechos de autor y derechos conexos, las instituciones que realicen alguna invención también poseen los mismos derechos sin distinción alguna de su ámbito de desarrollo. De igual forma, cada institución deberá registrar su obra en el IEPI con el fin de proteger la misma y de gozar de los beneficios que le genere.

La Ley de la Propiedad Intelectual, en su Libro II, detalla cada uno de los derechos y de las obligaciones de las Instituciones que generen algún tipo de invención. Así mismo, explica que la protección a la propiedad intelectual se "*encargará de garantizar la tutela del patrimonio biológico y genético del país; en tal virtud, la concesión de patentes de invención o de procedimientos que versen sobre elementos de dicho patrimonio debe fundamentarse en que éstos hayan sido adquiridos legalmente*"

Así también, en este mismo libro se realiza una serie de explicaciones y detalle de requisitos necesarios para que las instituciones o entidades registren sus creaciones, es decir, con la creación de patentes, marcas, dibujos, certificados, etc.

La OMPI define a una patente como un derecho exclusivo concedido por una invención que determina una nueva manera de hacer algo o propone una nueva solución a un problema, la protección que se concede es de un tiempo limitado de 20 años. Una creación que cuente con patente no pude ser fabricada, utilizada, distribuida o vendida sin el consentimiento del titular de la patente, siendo éste el único que puede decidir quién podría utilizar o no la misma. (OMPI, 2015)

Para obtener una patente es necesario presentar una solicitud con el título de la invención y una indicación de su ámbito técnico. Incluir antecedentes y descripción con un lenguaje claro y sencillo para que cualquier persona con un nivel medio de conocimientos pudiese entenderlo. Se recomienda incluir dibujos, planos, diagramas,

entre otros para aclarar los conceptos. Finalmente, se incluye las reivindicaciones, es decir, el alcance de protección de la patente. (OMPI, 2015)

Una marca es un signo distintivo del productor de un servicio o producto, es decir, a través de la marca se puede conocer que empresa o industria creo tal producto o servicio. El derecho de marca puede ser por tiempo ilimitado si se cancelan ciertas tasas. (OMPI, 2015)

Para realizar el registro y gestión de marcas se ha creado el Sistema internacional de registro de marcas conocido como Sistema de Madrid. El proceso a seguir consta de 3 etapas:

(i) Etapa 1.-Solicitud por conducto de la oficina de Protección Intelectual nacional o regional del solicitante: el solicitante previamente deberá haber registrado su marca en su oficina de Protección Intelectual de origen. Posteriormente, deberá presentar una solicitud internacional en su misma oficina regional, la cual certificará y enviará a la OMPI.

(ii) Etapa 2.-Examen de forma efectuado por la OMPI: La OMPI realiza un examen de forma a la solicitud y una vez aprobada, la marca es inscrita en el Registro Internacional y publicada en la Gaceta de la OMPI de Marcas Internacionales. A su vez, el solicitante recibe un certificado del registro internacional y las oficinas de Protección Intelectual son notificadas de este registro con el fin de proteger la marca.

(iii) Etapa 3.-Examen de fondo efectuado por las oficinas nacionales o regionales de la Protección Intelectual: en esta etapa las oficinas de Protección Intelectual de los territorios en los que se desea proteger la marca determinarán una decisión en un plazo de 12 a 18 meses. Una vez tomadas las decisiones por parte de las mismas la OMPI inscribirá dichas decisiones en el Registro Internacional.

Si una oficina niega la protección total o parcialmente, no afecta a las decisiones de las otras oficinas.

Este registro internacional tendrá una vigencia de 10 años, al terminar cada período se puede renovar directamente en la OMPI. (OMPI, 2015)

Ilustración 1 Funcionamiento del Sistema de Madrid Fuente: (OMPI, 2015)

Así también, se deberá realizar el pago de ciertas tasas, las mismas que deberán abonarse en francos suizos (CHF). A continuación se presenta la tabla de las tasas mencionadas:

	Francos suizos
1. Solicitudes internacionales regidas exclusivamente por el Arreglo. Deberán abonarse las siguientes tasas para un período de 10 años:	
1.1 Tasa básica (Artículo 8.2)a) del Arreglo) ver detalle al final del cuadro	
1.1.1 cuando no se presente ninguna reproducción de la marca en color	653
1.1.2 cuando se presente alguna reproducción de la marca en color	903
1.2 Tasa suplementaria por cada clase de productos y servicios que exceda la tercera (Artículo 8.2)b) del Arreglo)	100
1.3 Complemento de tasa por la designación de cada Estado contratante designado (Artículo 8.2)c) del Arreglo)	100
2. Solicitudes internacionales regidas exclusivamente por el Protocolo. Deberán abonarse las siguientes tasas para un período de 10 años:	
2.1 Tasa básica (Artículo 8.2)i) del Protocolo) ver detalle al final del cuadro	

2.1.1 cuando no se presente ninguna reproducción de la marca en color	653
2.1.2 cuando se presente alguna reproducción de la marca en color	903
2.2 Tasa suplementaria por cada clase de productos y servicios que exceda la tercera (Artículo 8.2)ii) del Protocolo), excepto si únicamente se designan Partes Contratantes respecto de las cuales se deban pagar tasas individuales (véase el punto 2.4, infra) (véase el Artículo 8.7)a)i) del Protocolo)	100
2.3 Complemento de tasa por la designación de cada Parte Contratante designada (Artículo 8.2)iii) del Protocolo), excepto si la Parte Contratante designada es una Parte Contratante respecto de la cual se deba pagar una tasa individual (véase el punto 2.4 infra) (véase el Artículo 8.7)a)ii) del Protocolo)	100
2.4 Tasa individual por la designación de cada Parte Contratante designada respecto de la cual se debe pagar una tasa individual (en lugar de un complemento de tasa) (véase el Artículo 8.7)a) del Protocolo) excepto cuando la Parte Contratante designada sea un Estado obligado (también) por el Arreglo y la Oficina de origen sea la Oficina de un Estado obligado (también) por el Arreglo (respecto de esa Parte Contratante, se deberá pagar un complemento de tasa): la cuantía de la tasa individual es determinada por cada Parte Contratante interesada	
3. Solicitudes internacionales regidas tanto por el Acuerdo como por el Protocolo. Se abonarán las siguientes tasas, correspondientes a un período de 10 años:	
3.1 Tasas básica ver detalle al final del cuadro	
3.1.1 cuando no se presente ninguna reproducción de la marca en color	653
3.1.2 cuando se presente alguna reproducción de la marca en color	903
3.2 Tasa suplementaria por cada clase de productos y servicios que	100

exceda la tercera	
3.3 Complemento de tasa por la designación de cada Parte Contratante designada respecto de la cual no se deba pagar una tasa individual (véase el punto 3.4, infra)	100
3.4 Tasa individual por la designación de cada Parte Contratante designada respecto de la cual se deba pagar una tasa individual (véase el Artículo 8.7)a) del Protocolo), excepto cuando la Parte Contratante designada sea un Estado obligado (también) por el Arreglo y la Oficina de origen sea la Oficina de un Estado obligado (también) por el Arreglo (respecto de esa Parte Contratante, se deberá pagar un complemento de tasa): la cuantía de la tasa individual la determinará cada Parte Contratante interesada	
4. Irregularidades respecto a la clasificación de los productos y servicios. Se abonarán las tasas siguientes (Regla 12.1)b)):	
4.1 Cuando los productos y servicios no estén agrupados en clases	77 más 4 por cada término que exceda 20
4.2 Cuando la clasificación de uno o más términos, tal como figura en la solicitud, sea incorrecta queda entendido que, cuando la cuantía total adeudada en virtud de este punto respecto a una solicitud internacional sea inferior a 150 francos suizos, no deberá pagarse tasa alguna	20 más 4 por cada término clasificado incorrectamente
5. Designación posterior al registro internacional. Se deberán pagar las siguientes tasas, correspondientes al período comprendido entre la fecha en que surta efecto la designación y el vencimiento del período de vigencia del registro internacional:	
5.1 Tasa básica	300
5.2 Complemento de tasa para cada Parte Contratante designada indicada en la misma petición y respecto de la cual no se deba pagar una tasa individual (véase el punto 5.3, infra)	100

5.3 Tasa individual por la designación de cada Parte Contratante designada respecto de la cual se deba pagar una tasa individual (en lugar de un complemento de tasa) (véase el Artículo 8.7)a) del Protocolo) excepto cuando la Parte Contratante designada sea un Estado obligado (también) por el Arreglo y la Oficina de la Parte Contratante del titular sea la Oficina de un Estado obligado (también) por el Arreglo (respecto de esa Parte Contratante se deberá pagar un complemento de tasa): la cuantía de la tasa individual es determinada cada Parte Contratante interesada	
6. Renovación Se abonarán las siguientes tasas, correspondientes a un período de 10 años:	
6.1 Tasa básica	653
6.2 Tasa suplementaria, excepto si la renovación se efectúa sólo para Partes Contratantes designadas respecto de las cuales se deban pagar tasas individuales (véase el punto 6.4, infra)	100
6.3 Complemento de tasa para cada Parte Contratante designada respecto de la cual no se deba pagar una tasa individual (véase el punto 6.4, infra)	100
6.4 Tasa individual por la designación de cada Parte Contratante designada respecto de la cual se deba pagar una tasa individual (en lugar de un complemento de tasa) (véase el Artículo 8.7)a) del Protocolo) excepto cuando la Parte Contratante designada sea un Estado obligado (también) por el Arreglo y la Oficina de la Parte Contratante del titular sea la Oficina de un Estado obligado (también) por el Arreglo (respecto de esa Parte Contratante se deberá pagar un complemento de tasa): la cuantía de la tasa es determinada cada Parte Contratante interesada	
6.5 Sobretasa por la utilización del plazo de gracia	50% de la cuantía de la tasa requerida en virtud del punto

	6.1
7. Otras inscripciones	
7.1 Transmisión total de un registro internacional	177
7.2 Transmisión parcial (para algunos de los productos y servicios o para algunas de las Partes Contratantes) de un registro internacional	177
7.3 Limitación solicitada por el titular con posterioridad al registro internacional, a condición de que, si la limitación afecta a más de una Parte Contratante, sea la misma para todas ellas	177
7.4 Cambio en el nombre y/o de la dirección del titular de uno o más registros internacionales, cuando se pida en una única petición la inscripción de la modificación	150
7.5 Inscripción de una licencia relativa a un registro internacional o modificación de la inscripción de una licencia	177
7.6 Petición de continuación de la tramitación en virtud de la Regla 5bis.1)	200
8. Información relativa a los registros internacionales	
8.1 Elaboración de un resumen analítico certificado extraído del Registro Internacional, consistente en un análisis de la situación de un registro internacional (extracto certificado detallado),	
hasta tres páginas	155
por cada página que exceda de la tercera	10
8.2 Elaboración de un extracto certificado del Registro Internacional consistente en una copia de todas las publicaciones y de todas las notificaciones de denegación que tengan relación con un registro internacional (extracto certificado sencillo),	
hasta tres páginas	77
por cada página que exceda de la tercera	2

8.3 atestación o una sola información por escrito,	
para un solo registro internacional	77
para cada uno de los registros internacionales adicionales, si se solicita la misma información en la misma petición	10
8.4 Reimpresión o fotocopia de la publicación de un registro internacional, por página	5
9. Servicios especiales. La Oficina Internacional estará autorizada a cobrar una tasa, cuya cuantía fijará ella misma, por las operaciones que deban efectuarse con carácter urgente, así como por servicios no previstos en la presente Tabla de tasas	

Para las solicitudes internacionales presentadas por solicitantes cuyo país de origen sea un País Menos Adelantado de conformidad con la lista establecida por las Naciones Unidas, la tasa básica se reduce al 10% del importe prescrito (en cifras redondeadas a la unidad más cercana). En dicho caso, la tasa básica ascenderá a 65 francos suizos (cuando no se presente ninguna reproducción de la marca en color) o a 90 francos suizos (cuando se presente alguna reproducción de la marca en color).

Tabla 1 Sistema de Madrid - Tabla de Tasas Fuente: (OMPI, 2015)

Un diseño industrial hace referencia a las características de forma, superficie, configuración, líneas o el color de un objeto. Puede alcanzar ámbitos variables desde: instrumentos médicos a joyas de lujo, electrodomésticos, vehículos, teléfonos, etc. Un diseño industrial debe ser nuevo y original no necesariamente funcional. Estos diseños se limitan al país que concede la protección. (OMPI, 2015)

Todos estos conceptos analizados son los que podrían tener acceso las industrias, empresas o entidades que buscan proteger sus creaciones.

3.5 Regulaciones y disposiciones sobre propiedad intelectual

A nivel mundial el organismo encargado de la protección de la Propiedad Intelectual es la Organización Mundial de la Protección Intelectual (OMPI). Fue creada en 1967 con sede en Ginebra (Suiza) y cuenta con 189 Estados miembros. La OMPI está conformada por los estados miembros, la administración y el personal y los observadores. (OMPI, 2015)

Algunos estados miembros son: Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Ecuador, El Salvador, España, Estados Unidos de América, Federación de Rusia, Guatemala, Honduras, Italia, Panamá, Perú, República Dominicana, Uruguay, Venezuela, entre otros. (OMPI, 2015)

La Organización de Naciones Unidas (ONU) reconoce como derecho fundamental el amparo de las creaciones intelectuales y declara como defensor al Estado. En el contexto internacional existen varios países que tienen una ley que proteja la Propiedad Intelectual como: Argentina, Chile y España.

Argentina cuenta con la Ley 11723 Régimen Legal de la Propiedad Intelectual establecida el 26 de Septiembre de 1933. (InfoLEG, 2016) En Chile está vigente la Ley 17336 sobre Propiedad Intelectual que se encarga de regular los derechos de autor y derechos conexos en este país cuyas normas reglamentarias se encuentran contenidas en:

(i) Decreto Supremo de Educación N. 277
(ii) Decreto N. 425 del Ministerio de Educación

Con la publicación de esta ley, el 2 de octubre de 1970, se decretó la creación del Departamento de Derechos Intelectuales que se encarga de la atención de consultas e informes por parte de los particulares y los servicios públicos en cuanto a los derechos de autor, derechos conexos y materias afines. (DDI, 2015)

Ecuador cuenta con la Ley de Propiedad Intelectual conocida por sus siglas LPI, que fue creada y publicada el 18 de mayo de 1998 en el Registro Oficial No. 320 y el ente estatal que garantiza una clara legislación para la propiedad intelectual es el Instituto Ecuatoriano de la Propiedad Intelectual, conocido como IEPI. Este organismo se encarga de la protección, divulgación y conducción del buen uso de la Propiedad Intelectual reconocidos en la Ley y en los tratados y convenios internacionales. Se encarga de promover una gestión de calidad, talento humano competitivo y servicios técnicos que cumplan con las necesidades de los usuarios. Dicho organismo se basa en las áreas de:

(i) Propiedad Industrial: se refiere a la protección de todas las invenciones, marcas, distintivos, lemas comerciales, descubrimientos relacionados con el mercado, industria y comercio realizadas por una persona natural o jurídica

(ii) Derecho de Autor: protege a los creadores de obras ya sean literarias o artísticas, por ejemplo, libros, textos de investigación, software, folletos, discursos, conferencias, composiciones musicales, coreografías, obras de teatro, obras audiovisuales, esculturas, dibujos, grabados, litografías, historietas, comics, planos, maquetas, mapas, fotografías, videojuegos, entre otros.

(iii) Obtenciones Vegetales: se protege a la persona que desarrolle una variedad vegetal incluyendo la biodiversidad y saberes ancestrales. (IEPI , 2016)

Así también, en la Constitución del Ecuador en el Capítulo Segundo de los Derechos del Buen Vivir, en su Sección Cuarta, el Artículo 22 reconoce a todas las personas en los términos del mismo cuerpo constitucional y demás Tratados Internacionales aplicables, derechos sobre las creaciones culturales y científicas.

En cuanto al avance tecnológico, la LPI en su Artículo 25 decreta: *"El titular del derecho de autor tiene el derecho de aplicar o exigir que se apliquen las protecciones técnicas que crea pertinentes, mediante la incorporación de medios o dispositivos, la codificación de señales u otros sistemas de protección tangibles o intangibles, a fin de impedir o prevenir la violación de sus derechos. Los actos de importación, fabricación, venta, arrendamiento, oferta de servicios, puesta en circulación o cualquier otra forma de facilitación de aparatos o medios destinados a descifrar o decodificar las señales codificadas o de cualquier otra manera burlar o quebrantar los medios de protección aplicados por el titular del derecho de autor, realizados sin su consentimiento, serán asimilados a una violación del derecho de autor para efectos de las acciones civiles así como para el ejercicio de las medidas cautelares que corresponda, sin perjuicio de las penas a que haya lugar por el delito."* En cuanto a las disposiciones especiales sobre ciertas obras el parágrafo primero abarca a las obras de los Programas de Ordenador desde el Art. 28 hasta el Art. 32 de la Ley Propiedad Intelectual, detallados a continuación:

(i) Artículo 28. "*Los programas de ordenador se consideran obras literarias y se protegen como tales. Dicha protección se otorga independientemente de que hayan sido incorporados en un ordenador y cualquiera sea la forma en que estén expresados, ya sea en forma legible por el hombre (código fuente) o en forma legible por máquina (código objeto), ya sean programas operativos y programas aplicativos, incluyendo diagramas de flujo, planos,*

manuales de uso, y en general, aquellos elementos que conformen la estructura, secuencia y organización del programa." (Ley de Propiedad Intelectual, 1998, art 28)

(ii) Artículo 29. "*Es titular de un programa de ordenador, el productor, esto es la persona natural o jurídica que toma la iniciativa y responsabilidad de la realización de la obra. Se considerará titular, salvo prueba en contrario, a la persona cuyo nombre conste en la obra o sus copias de la forma usual*

Dicho titular está además legitimado para ejercer en nombre propio los derechos morales sobre la obra, incluyendo la facultad para decidir sobre su divulgación.

El productor tendrá el derecho exclusivo de realizar, autorizar o prohibir la realización de modificaciones o versiones sucesivas del programa, y de programas derivados del mismo.

Las disposiciones del presente artículo podrán ser modificadas mediante acuerdo entre los autores y el productor." (Ley de Propiedad Intelectual, 1998, art 29)

(iii) Artículo 30. "*La adquisición de un ejemplar de un programa de ordenador que haya circulado lícitamente, autoriza a su propietario a realizar exclusivamente:*

a. Una copia de la versión del programa legible por máquina (código objeto) con fines de seguridad o resguardo;

b. Fijar el programa en la memoria interna del aparato, ya sea que dicha fijación desaparezca o no al apagarlo, con el único fin y en la medida necesaria para utilizar el programa; y,

c. Salvo prohibición expresa, adaptar el programa para su exclusivo uso personal, siempre que se limite al uso normal previsto en la licencia. El adquirente no podrá transferir a ningún título el soporte que contenga el programa así adaptado, ni podrá utilizarlo de ninguna otra forma sin autorización expresa, según las reglas generales.

d. *Se requerirá de autorización del titular de los derechos para cualquier otra utilización, inclusive la reproducción para fines de uso personal o el aprovechamiento del programa por varias personas, a través de redes u otros sistemas análogos, conocidos o por conocerse*." (Ley de Propiedad Intelectual, 1998, art 30)

(iv) Artículo 31. "*No se considerará que existe arrendamiento de un programa de ordenador cuando éste no sea el objeto esencial de dicho contrato. Se considerará que el programa es el objeto esencial cuando la funcionalidad del objeto materia del contrato, dependa directamente del programa de ordenador suministrado con dicho objeto; como cuando se arrienda un ordenador con programas de ordenador instalados previamente.*" (Ley de Propiedad Intelectual, 1998, art 31)

(v) Artículo 32. "*Las excepciones al derecho de autor establecidas en los artículos 30 y 31 son las únicas aplicables respecto a los programas de ordenador*." (Ley de Propiedad Intelectual, 1998, art 32)

Las normas contenidas en el presente Parágrafo se interpretarán de manera que su aplicación no perjudique la normal explotación de la obra o los intereses legítimos del titular de los derechos.

3.6 Conclusión

Se ha comprendido por Propiedad Intelectual a toda creación de la mente independientemente del área de aplicación ya que puede ser artística, literaria, científica e industrial y a su vez reconoce al autor como el titular y beneficiario de la misma. El Organismo Mundial de la Propiedad Intelectual es el encargado de establecer una protección a estas creaciones y se encuentra formado por 189 Estados Miembros, entre ellos el Ecuador. Así también, la Organización de Naciones Unidas (ONU) ampara a la Propiedad Intelectual. A nivel internacional países como: Argentina, Chile y España cuentan con una ley específica para velar por este derecho.

A su vez, el Ecuador también posee la Ley de Propiedad Intelectual establecida en 1998 y el Instituto Ecuatoriano de la Propiedad Intelectual (IEPI) que juntos interactúan estableciendo un Sistema de control y regulación en cuanto a las creaciones realizadas por los individuos. Este sistema se encuentra establecido y en una etapa de crecimiento ya que a nivel nacional existe gran difusión y uso del mismo. A nivel internacional se pueden establecer marcas y patentes avalados por el Organismo Mundial de Propiedad Intelectual que velan y cuidan los derechos y obligaciones de sus autores. Es por esto, que se verifica que la Propiedad Intelectual tanto a nivel local como internacional cuenta con un sistema estructurado y eficaz que garantiza la protección de derechos y aplicación de beneficios a los autores de creaciones sin importar el área en que se desarrollen.

Capítulo IV: Leyes relacionadas con servicios de información

4.1 Introducción

En el presente capítulo se detallarán las leyes que se encuentren relacionadas con los servicios de información tanto a nivel internacional como nacional. Así también, se revisará el contexto mundial en cuanto al espionaje cibernético analizando específicamente el caso "Five Eyes". Por otro lado, se revisará las competencias y funciones de la Organización de Cooperación y Desarrollo Económico y de la Asociación de Derecho Penal. Se dará mayor connotación al aspecto local y se detallará las regulaciones y disposiciones legales en cuanto a las leyes relacionadas con los servicios de información.

4.2 Aspectos generales

Las leyes que se encargan de salvaguardar el uso de sistemas de información, redes electrónicas, el uso de Internet para el desarrollo del comercio y la producción tanto en el sector público como privado son consideradas como leyes relacionadas con servicios de información. Así también, pueden ser consideradas aquellas leyes cuyo objetivo es regular el régimen jurídico de los servicios relacionados con Internet y la contratación electrónica. (LSSI, 2015)

A nivel internacional, específicamente en España, existe la Ley 34/2002 de Servicios de la Sociedad de la Información y del Comercio Electrónico. Esta ley controla los servicios de la Sociedad de la Información:

(i) Comercio electrónico
(ii) Contratación en línea
(iii) Información y publicidad
(iv) Servicios de intermediación (LSSI, 2015)

Esta ley considera que existe actividad económica cuando se reciba ingresos directos por las actividades de comercio electrónico que se realicen a través de una página web, así también por ingresos indirectos ya sean por publicidad o entre otros. Por otra parte, esta ley no se aplica a las actividades realizadas sin ánimo de lucro. (LSSI, 2015)

Así también, esta ley protege la práctica del *spam*, es decir, no permite el envío de correos electrónicos no deseados a destinatarios que desconocen el remitente con publicidad u otra información, dicha regulación abarca los mensajes de textos que se envíen a teléfonos móviles. Para realizar este control la ley obliga a etiquetar los mensajes con la palabra publicidad para que sean identificados de una manera fácil y sencilla. (Perez, 2008)

Otro ámbito que regula esta ley es la validez de los contratos electrónicos, de este modo los prestadores de servicios no tendrán que enviar documentos en papel para garantizar la validez del contrato celebrado vía electrónica. Por otro lado, contempla algunas disposiciones para garantizar una navegación segura de los niños por Internet con criterios de clasificación y etiquetado de contenidos. (Perez, 2008)

Para los usuarios de Internet esta ley ofrece los siguientes derechos:

(i) Derecho a obtener información sobre los prestadores de servicios, precios de productos o servicios con los respectivos impuestos y gastos de envío

(ii) Respeto a la publicidad, derecho a conocer la identidad del anunciante, no recibir mensajes promocionales no solicitados y a dejar de recibir los que hubiera autorizado.

(iii) Derecho a conocer los pasos necesarios para contratar por Internet, a acceder a las condiciones generales de la contratación antes de realizar el pedido y a obtener un acuse de recibo del vendedor.

(iv) Si se realiza una compra a través de internet, se beneficia de la protección por parte de la Ley de ordenación del comercio minorista para todas las ventas a distancia. (LSSI, 2015)

A nivel local, en Ecuador existe la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos cuyo objetivo es: "*regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas*" (Ley 67, 2002, art 1)

Esta ley se caracteriza por el reconocimiento internacional de certificados de firma electrónica, es decir, un certificado emitido en el extranjero tiene validez en el Ecuador una vez validados por el Consejo Nacional de Telecomunicaciones. Esto se encuentra amparado en los artículos 2, 8, 14, 15 y 51 de la mencionada ley. (Castellanos, 2014)

4.3 Realidad Mundial

Se considera analizar el contexto mundial en cuanto a la seguridad de la información, ya sea las organizaciones que garantizan la misma o las que atacan este principio. Se plantea el Caso Five Eyes como espionaje cibernético y OCDE como una organización que genera e impulsa el desarrollo de los países en el ámbito económico.

4.3.1 Espionaje cibernético: Caso Five Eyes

El caso "Five Eyes" conocido en español como "El Club de los cinco ojos" tuvo su inicio durante la II Guerra Mundial cuando Bletchley Park descifró los códigos alemanes y japoneses a través de la estrecha colaboración en materia de espionaje entre Estados Unidos y Reino Unido. En 1946 surgió la alianza UKUSA con acuerdos en secreto hasta el 2010 cuando ambos países los hicieron públicos. Así también, crearon el Cuartel General de Comunicaciones del Gobierno Británico y la Agencia de Seguridad Nacional con una cooperación extremadamente estrecha. Posteriormente se unieron Australia, Canadá y Nueva Zelanda a esta alianza. (Corera, 2013)

Esta alianza permite la intercepción, recolección, adquisición, análisis y descifrado de información de inteligencia que cada país genera y luego comparten entre sí pero sin espiarse mutuamente. Para interceptar y analizar la información utilizan el sistema *Tempora,* localizado en Reino Unido, y que por su ubicación geográfica facilita la extracción de datos ya que por esta región cruzan gran cantidad de cables submarinos que conectan a Norteamérica con Europa. Dicho sistema se encarga de filtrar mensajes de texto, correos electrónicos, llamadas, archivos u otra información y luego es reportada al gobierno de Estados Unidos. Este sistema era desconocido hasta que Edward Snowden colocó algunos archivos en dominio público, dando a conocer la existencia de grandes cantidades de datos de personas espiadas sin el conocimiento de estas o de sus gobiernos. (R3D Red en Defensa de los Derechos Digitales, 2016)

A través de la publicación de estos archivos se descubrió que el "Club de los cinco ojos" planificaba infiltrar una aplicación espía para teléfonos inteligentes, *hackeando* la tienda de aplicaciones de Google y Samsung. Se planeaba engañar al usuario enviando información de la supuesta tienda de aplicaciones cuando en realidad estarían extrayendo la información de sus teléfonos ya sea recopilación de datos de correo electrónico, archivos de texto, el historial de búsquedas en internet, el historial de llamadas, los vídeos y los archivos de fotos. (SPUTNIK , 2015)

4.3.2 Organización de Cooperación y Desarrollo Económico

Al hablar de la organización de cooperación y desarrollo económico se hace referencia a un grupo de 34 países miembros cuyo objetivo es promover políticas que favorezcan el bienestar económico y social de las personas a nivel mundial. A esta organización se le conoce con las siglas OCDE y fue fundada en 1961, se establece como un foro donde los gobiernos trabajan conjuntamente con el fin de compartir experiencias y buscar

soluciones a problemas comunes. Busca encontrar el camino para un cambio económico, social y ambiental a través de la medición de la productividad y flujos globales del comercio e inversión. (OCDE, 2016)

Sin embargo, a nivel de América Latina solo Chile y México son miembros de esta organización, en estado de adhesión se encuentran Colombia y Costa Rica, como socio clave se encuentra Brasil y como Programa País se encuentra Perú. Cabe destacar, que Ecuador no es miembro de este organismo. (OCDE, 2016)

La OCDE genera estadísticas económicas e información política a nivel mundial alrededor de 250 nuevas investigaciones, 40 actualizaciones de bases de datos, miles de cuadros estadísticos cada año. Así también, cuenta con una biblioteca digital con más de 10000 publicaciones disponibles para descarga y lectura en diferentes formatos. (OCDE, 2016)

Cuando un país es miembro de la OCDE posee las siguientes ventajas:

(i) Evaluación constante que impulsa su mejoramiento continuo
(ii) Utiliza los informes emitidos por la OCDE, que facilitan el desarrollo e implementación de políticas y soluciones de otros países.
(iii) Contar con un asesor que basa sus recomendaciones en evidencias comprobadas
(iv) Contar con una excelente carta de presentación debido a que los estándares que debe cumplir cada país son muy altos. (Salas, 2014)

4.3.3 Asociación de derecho penal

La Asociación de Derecho Penal fue fundada en 1924 en París, es considerada como una de las sociedades culturales más antiguas del mundo que reúne a especialistas de las ciencias penales. Se encarga de los problemas de derecho penal internacional y de la responsabilidad de los autores de crímenes internacionales, específicamente de:

(i) La política criminal y la codificación del Derecho Penal
(ii) El Derecho penal comparado
(iii) Los Derechos humanos en la administración de justicia penal
(iv) El Derecho penal internacional

Esta asociación se caracteriza por su dinamismo, la continuidad en el cumplimiento de sus objetivos y su capacidad de adaptación a las necesidades del mundo moderno. (AIDP, 2015)

4.4 Regulaciones y disposiciones sobre servicios de información

En la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de datos se entiende como firma electrónica a: "*los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que puedan ser utilizados para identificar al titular de la firma en relación con el mensaje de datos, e indicar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos*" (Ley 67, 2002, art 13)

La validez de la misma es protegida por los siguientes artículos:

(i) Artículo 14.- "*Efectos de la firma electrónica.- La firma electrónica tendrá igual validez y se le reconocerán los mismos efectos jurídicos que a una firma manuscrita en relación con los datos consignados en documentos escritos, y será admitida como prueba en juicio*." (Ley 67, 2002, art 14)

(ii) Artículo 15.- "*Requisitos de la firma electrónica.- Para su validez, la firma electrónica reunirá los siguientes requisitos, sin perjuicio de los que puedan establecerse por acuerdo entre las partes:*

a. Ser individual y estar vinculada exclusivamente a su titular;

b. Que permita verificar inequívocamente la autoría e identidad del signatario, mediante dispositivos técnicos de comprobación establecidos por esta Ley y sus reglamentos;

c. Que su método de creación y verificación sea confiable, seguro e inalterable para el propósito para el cual el mensaje fue generado o comunicado.

d. Que al momento de creación de la firma electrónica, los datos con los que se creare se hallen bajo control exclusivo del signatario; y,

e. *Que la firma sea controlada por la persona a quien pertenece.*" (Ley 67, 2002, art 15)

Así también, La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de datos se encarga de velar por los derechos de los usuarios o consumidores de servicios electrónicos a través de los siguientes artículos:

(i) Artículo 48.- "*Consentimiento para aceptar mensajes de datos.- Previamente a que el consumidor o usuario exprese su consentimiento para aceptar registros electrónicos o mensajes de datos, debe ser informado clara, precisa y satisfactoriamente, sobre los equipos y programas que requiere para acceder a dichos registros o mensajes. El usuario o consumidor, al otorgar o confirmar electrónicamente su consentimiento, debe demostrar razonablemente que puede acceder a la información objeto de su consentimiento. Si con posterioridad al consentimiento del consumidor o usuario existen cambios de cualquier tipo, incluidos cambios en equipos, programas o procedimientos, necesarios para mantener o acceder a registros o mensajes electrónicos, de forma que exista el riesgo de que el consumidor o usuario no sea capaz de acceder o retener un registro electrónico o mensaje de datos sobre los que hubiera otorgado su consentimiento, se le deberá proporcionar de forma clara, precisa y satisfactoria la información necesaria para realizar estos cambios, y se le informará sobre su derecho a retirar el consentimiento previamente otorgado sin la imposición de ninguna condición, costo alguno o consecuencias. En el caso de que estas modificaciones afecten los derechos del consumidor o usuario, se le deberán proporcionar los medios necesarios para evitarle perjuicios, hasta la terminación del contrato o acuerdo que motivó su consentimiento previo.*" (Ley 67, 2002, art 48)

(ii) Artículo 49.- "*Consentimiento para el uso de medios electrónicos.- De requerirse que la información relativa a un servicio electrónico, incluido el comercio electrónico, deba constar por escrito, el uso de medios electrónicos para proporcionar o permitir el acceso a esa información, será válido si:*

a. El consumidor ha consentido expresamente en tal uso y no ha objetado tal consentimiento; y,

b. El consumidor en forma previa a su consentimiento ha sido informado, a satisfacción, de forma clara y precisa, sobre:

i. *Su derecho u opción de recibir la información en papel o por medios no electrónicos;*

ii. *Su derecho a objetar su consentimiento en lo posterior y las consecuencias de cualquier tipo al hacerlo, incluidas la terminación contractual o el pago de cualquier tarifa por dicha acción;*

iii. *Los procedimientos a seguir por parte del consumidor para retirar su consentimiento y para actualizar la información proporcionada; y,*

iv. *Los procedimientos para que, posteriormente al consentimiento, el consumidor pueda obtener una copia impresa en papel de los registros electrónicos y el costo de esta copia, en caso de existir*." (Ley 67, 2002, art 49)

(iii) Artículo 50.- "*Información al consumidor.- En la prestación de servicios electrónicos en el Ecuador, el consumidor deberá estar suficientemente informado de sus derechos y obligaciones, de conformidad con lo previsto en la Ley Orgánica de Defensa del Consumidor y su Reglamento. Cuando se tratare de bienes o servicios a ser adquiridos, usados o empleados por medios electrónicos, el oferente deberá informar sobre todos los requisitos, condiciones y restricciones para que el consumidor pueda adquirir y hacer uso de los bienes o servicios promocionados. La publicidad, promoción e información de servicios electrónicos, por redes electrónicas de información, incluida la Internet, se realizará de conformidad con la ley, y su incumplimiento será sancionado de acuerdo al ordenamiento jurídico vigente en el Ecuador. En la publicidad y promoción por redes electrónicas de información, incluida la Internet, se asegurará que el consumidor pueda acceder a toda la información disponible sobre un bien o servicio sin restricciones, en las mismas condiciones y con las facilidades disponibles para la promoción del bien o servicio de que se trate. En el envío periódico de mensajes de datos con información de cualquier tipo, en forma individual o a través de listas de correo, directamente o mediante cadenas de mensajes, el emisor de los mismos deberá proporcionar medios expeditos para que el destinatario, en cualquier tiempo, pueda confirmar su suscripción o solicitar su exclusión de las listas, cadenas de mensajes o bases de datos, en las*

cuales se halle inscrito y que ocasionen el envío de los mensajes de datos referidos. La solicitud de exclusión es vinculante para el emisor desde el momento de la recepción de la misma. La persistencia en el envío de mensajes periódicos no deseados de cualquier tipo, se sancionará de acuerdo a lo dispuesto en la presente ley. El usuario de redes electrónicas, podrá optar o no por la recepción de mensajes de datos que, en forma periódica, sean enviados con la finalidad de informar sobre productos o servicios de cualquier tipo." (Ley 67, 2002, art 50)

4.5 Conclusión

Se ha comprendido que las leyes relacionadas con servicios de información son aquellas que se encargan de controlar y establecer un marco jurídico que proteja a los sistemas de información y el uso del Internet para el desarrollo del comercio y producción ya sea en el sector público o privado. Estas leyes velarán por el bienestar de los usuarios y el cumplimiento de sus derechos y deberes.

A nivel internacional se estableció la Ley 34/2002 de Servicios de la Sociedad de la Información y del Comercio Electrónico en España cuyo ámbito de acción está considerado el comercio electrónico, contratación en línea, información y publicidad y servicios de intermediación. El contexto de la aplicación y desarrollo de esta Ley está en una etapa de crecimiento y fortalecimiento ya que se encuentra fundamentada y existen evidencias de su aplicación en su país.

El Ecuador cuenta con la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos encargada de salvaguardar los mensajes de datos, firmas electrónicas, contratación electrónica y telemática, prestación de servicios informáticos, comercio electrónico y protección de usuarios. Sin embargo, existe desconocimiento de la misma y muy poca aplicación, apenas está en una etapa de inicio.

Al analizar el caso "Five Eyes" conocido como el "Club de los cinco ojos" se ha comprendido que los cinco países que lo conforman dedican su esfuerzo a extraer la información generada por el resto de países y analizarla sin espiarse entre sí. Al realizar estas acciones están vulnerando los derechos de protección de datos ya que los propietarios de la información desconocen que este club está usando su información. Desde que Edward Snowden dio a conocer la manera de actuar de este club se ha generado una serie de debates sobre si esto es un delito o no. Simplemente, se está robando la información de las personas para analizarla y luego emitir reportes solo para los países miembros.

En otro contexto, existe la Organización de Cooperación y Desarrollo Económico que en principio se muestra como una organización que busca mejorar la condición social y económica de los países miembros, sin embargo, el ingreso a esta organización está

condicionado a una serie de requerimientos muy complicados para países en desarrollo, como el caso de Ecuador. Esto se puede comprobar al constatar que de América Latina los únicos países miembros son: Chile y México.

Así también, a nivel internacional la Asociación de Derecho Penal que tiene una larga trayectoria ya que fue fundada en 1924 y es considerada como la sociedad cultural más antigua del mundo se considera como una organización que reúne a los mejores especialistas en derechos penales.

Capítulo V: Disposiciones en el sector financiero ecuatoriano

5.1 Introducción

En el presente capítulo se realizará una indagación sobre el Sistema Financiero Ecuatoriano y su estructura. Se ahondará sobre los órganos rectores del mismo sistema y la Ley General de Instituciones Financieras. Por otra parte, se conocerá el significado de Junta Bancaria y las resoluciones consideradas en cuanto a las tecnologías de la información. Se analizará la definición, funciones y disposiciones de la Superintendencia de Economía Popular y Solidaria y de la Superintendencia de Bancos y Seguros.

5.2 Aspectos generales

5.2.1 Sistema Financiero Ecuatoriano

Ley General de Instituciones Financieras

En el Ecuador, la Ley encargada de la regulación de la creación, organización, actividades, funcionamiento y extinción de las instituciones del sistema financiero privado, así como la organización y funciones de la Superintendencia de Bancos y Seguros, en la órbita de su competencia, entidad encargada de la supervisión y control del sistema financiero, en todo lo cual se tiene presente la protección de los intereses del público es la Ley General de Instituciones del Sistema Financiero. (Ley 55, 1994, art 1)

Por su parte las instituciones financieras públicas, compañías de seguros y de reaseguros se rigen por sus propias leyes para la creación, actividades, funcionamiento y organización. En lo relacionado a la aplicación de normas de solvencia y prudencia financiera y al control y vigilancia que realizará la Superintendencia dentro del marco legal que regula a estas instituciones en todo cuanto fuere aplicable según su naturaleza jurídica se someterán a esta ley. (Ley 55, 1994, art 1)

Se considera como instituciones financieras privadas a:

(i) Bancos
(ii) Sociedades financieras
(iii) Asociaciones Mutualistas de Ahorro y Crédito para la vivienda
(iv) Cooperativas de Ahorro y Crédito que realizan intermediación financiera con el público.

Órganos rectores del Sistema Financiero

El órgano central rector de los sistemas de presupuestos, de determinación y recaudación de recursos financieros, y de tesorería es el Ministerio de Finanzas. El

órgano encargado de los sistemas de contabilidad y control es la Contraloría General. (García & Otros, 2011)

Así cada órgano rector de cada uno de los sistemas establece unidades centrales de trabajo que se encargan de investigar, proyectar y preparar las normas secundarias de carácter general necesarias para el cumplimiento de las actividades que les competan a cada sistema. De igual forma se encargan de la verificación de los proyectos de reglamento, normas técnicas, manuales de procedimiento, instructivos y demás instrumentos para que concuerden con la ley evitando duplicaciones o inconsistencias. (García & Otros, 2011)

Por otra parte, están presentes las superintendencias que son organismos técnicos de vigilancia, auditoría, intervención y control de las actividades económicas, sociales y ambientales y de los servicios que prestan entidades públicas y privadas cuyo objetivo es sujetar a estas actividades y servicios al ordenamiento público y atiendan al interés general. (García & Otros, 2011)

Estructura del Sistema Financiero Ecuatoriano

El sistema financiero ecuatoriano es el eje central de la economía del país, a través de este se realizan las principales transacciones económicas nacionales e internacionales. A continuación, se detalla su estructura.

Banca

A la Banca se considera como una entidad de origen privado y público, autorizada y constituida legalmente para receptar dinero en moneda nacional o extranjera de manera continua o habitual de sus clientes. Así también, esta entidad concede créditos con el fin de generar desarrollo económico social y productivo del país. (Morán Carvajal, 2004)

La Banca en el Ecuador tuvo su auge en los años 70 con un gran crecimiento en activos fijos, personal y número de instituciones debido al descubrimiento del petróleo en este país, ya que el estado ofrecía a este sector condiciones como: líneas de crédito subsidiadas, controles administrativos para las tasas de interés y asignación de crédito. Sin embargo, a finales de esta década surgió un problema con el banco La Previsora, por la mala cartera por préstamos vinculados. Dicho problema fue resuelto por un crédito concedido por el Banco Central del Ecuador capitalizándolo por parte del Estado y en el año de 1988 fue privatizado nuevamente. (Domínguez & Otros, 2009)

En los 80 incrementa radicalmente la crisis de la deuda externa adquirida por el Ecuador, llegando a cifras exorbitantes y generando la incapacidad de pago por parte de los deudores privados y públicos. Como consecuencia, aumentaron las tasas de interés internacionales, suspendieron líneas de crédito externas, y el precio de los productos de exportación bajó considerablemente, entre ellos el del petróleo. Debido a esto, el sistema bancario presentó una iliquidez por los altos índices de cartera vencida, sobregiros en cuentas del exterior y alta dependencia de los créditos otorgados por el Banco Central. Así, se liquidaron los bancos: Banco de Descuento, FIMASA, FINANSA, FINANDES, BANCO INDUSTRIAL Y COMERCIAL Y FINIBER. (Domínguez & Otros, 2009)

En los 90 se reemplaza la Ley de Bancos por la Ley General de Instituciones Financieras intentando implantar la vigilancia sobre el cumplimiento de las normativas preventivas aplicadas a los agentes financieros. Se redujo el tipo de instituciones financieras de 7 a 4, se creó la Junta Bancaria, se instauró la publicación de información contable como balances e indicadores financieros, entre otros. A pesar de estas nuevas políticas esta década es considerada como una década de crisis debido al conocido feriado bancario en el cual todas las operaciones financieras quedaron suspendidas y el dinero paso a un estado de congelamiento generando así graves consecuencias al sistema financiero y produciendo el cierre de algunas instituciones financieras del país. (Domínguez & Otros, 2009)

Banca Privada

El economista Juan Pablo Jaramillo califica a la banca privada como la base de financiamiento para que el sector productivo y de consumo generen mayores y nuevos proyectos, creando empleos, liquidez y producción en el país. (Jaramillo Albuja, 2016)

Banca Pública

La banca pública fue creada con el propósito de erradicar la pobreza y fomentar la inversión y el ahorro en el Ecuador. El Banco del Estado, Banco Ecuatoriano de la Vivienda, Banco Nacional de Fomento, Corporación Financiera Nacional y el Instituto Ecuatoriano de Créditos Educativos pertenecen a este sector. (Aguirre Gudiño & Otros, 2011)

Cooperativismo

El cooperativismo tiene sus inicios a finales del siglo XVIII, es aquí en donde adquiere sus principios fundamentales para luego continuar con su difusión y consolidación. Los principios del cooperativismo son los siguientes:

(i) Adhesión abierta y voluntaria
(ii) Control democrático de los socios
(iii) Participación económica de los socios
(iv) Autonomía e independencia
(v) Educación, capacitación e información
(vi) Cooperación entre Cooperativas
(vii) Compromiso con la comunidad

Se puede definir como una cooperativa a una asociación voluntaria de personas y no de capitales, con plena personería jurídica, de duración indefinida y responsabilidad limitada. En esta asociación los individuos están organizados democráticamente con el fin de satisfacer sus necesidades y promover su mejoramiento económico y social. Todas las actividades de producción, distribución y consumo son realizadas por servicio y no por lucro. (García & Otros, 2011)

De igual forma, se define como coooperativa a "una sociedad de derecho privado, formada por personas naturales o jurídicas que sin perseguir finalidades de lucro, tienen por objeto planificar y realizar actividades o trabajos de beneficio social o colectivo a través de una empresa manejada en común y formado con la aportación económica, intelectual y moral de sus miembros" (Chiriboga Rosales, 2007)

En el Ecuador se establece la primera Ley de Cooperativas en el año de 1937 conjuntamente con las primeras seis cooperativas. Sin embargo, la ausencia de una identidad no les permitió afianzarse. En 1966 se emite la segunda Ley de Cooperativas pero la escasa capacitación a los integrantes de las cooperativas las convirtió en espacios para el ejercicio de poder de ciertos caudillos. Las ONG's de desarrollo social y comunitario tuvieron gran importancia para el cooperativismo ya que se conviertieron en canales de acceso a recursos internacionales. Las décadas del 70 y 80 no fueron las mejores para el cooperativismo. (García & Otros, 2011)

En la actualidad, el cooperativismo tiene un nuevo marco jurídico se cambia el concepto de la economía social de mercado para asumir el de economía social y solidaria. En este nuevo concepto prevalece el ser humano y deja de ser mercancía, se da privilegios al trabajo y al ser humano como sujeto y fin de su gestión, por sobre la apropiación individual, el lucro y la acumulación del capital. (Miño Grijalva, 2013)

Mutualismo

Se considera como mutualismo a la asociación libre, sin fines de lucro, por personas inspiradas en la solidaridad, con el fin de obtener ayuda mutua en riesgos eventuales mediante una contribución periódica. Los socios del mutualismo no aportan capital, ni cuota inicial, no distribuyen excedentes y solo los socios activos participan del gobierno de la misma, no tienen derecho al reintegro de aportes. (Aguirre Gudiño & Otros, 2011)

Servicios Financieros en la tecnología

El avance de la tecnología ha influenciado en el sistema financiero ya que ha introducido nuevas formas de interacción con el cliente como por ejemplo: transacciones virtuales, firma electrónica, uso de redes sociales para el intercambio de información, entre otros. (Aguirre & Otros, 2011)

Se ha implementado nuevos canales con el fin de proveer servicios financieros, entre ellos los enumerados a continuación:

(i) Cajeros Automáticos
(ii) Banca Virtual
(iii) Banca Celular
(iv) Banca Telefónica
(v) Ventanillas
(vi) Intranets y Extranets
(vii) Marketing
(viii) Portales web
(ix) Kioskos electrónicos
(x) Puntos de venta POS
(xi) Botones de pago (Aguirre & Otros, 2011)

5.3 Disposiciones sobre la Junta Bancaria

La Junta Bancaria se encarga de decretar las políticas y lineamientos de regulación para las instituciones financieras públicas y privadas, de seguros, reaseguros y seguridad social que son controladas por la Superintendencia de Bancos y Seguros . Se conforma

por cinco miembros: el presidente de la Superintendencia de Bancos y Seguros, dos representantes del presidente de la República, el Gerente del Banco Central y un miembro elegido por los demás miembros que conforman la Junta Bancaria. (Seguros, 2008)

Las resoluciones por parte de la Junta Bancaria que han afectado al libro I "Normas generales para la aplicación de la Ley General de Instituciones del Sistema Financiero" son las siguientes:

(i) JB-2014-3066 encargada de la gestión del riesgo operativo, establece una serie de disposiciones para la implementación de medidas de seguidad en los diferentes canales electrónicos con los cuales las instituciones financieras ofrecen sus servicios a sus clientes. Se encarga de reformar el capítulo V "De la gestión del riesgo operativo" con el fin de mejorar los controles de gestión de la tecnología de la información y comunicaciones. Así también, favorecer a la continuidad de las operaciones del negocio e implementar medidas de seguridad que mitiguen los fraudes relacionados a cajeros automáticos. (JB-2014-3066, 2014)

(ii) JB-2012-2148 pretende que las instituciones del sistema financiero cuenten con grandes medidas de seguridad en la tecnología de información y comunicaciones para garantizar la seguridad y confiabilidad de los elementos tecnológicos que se usen para ofrecer sus servicios o productos. De igual manera, reforma el título X "De la gestión y administración del riesgo" del capítulo V "De la gestión del riesgo operativo" (JB-2014-2148, 2012)

(iii) JB-2012-2090 establece que las instituciones financieras adquieran una "Póliza de fidelidad bancaria" que cubra el "delito informático y cibercrimen". Esta resolución modifica el título II "De la organización de las instituciones del sistema financiero privado" del capítulo I "Apertura y cierre de oficinas en el país y en el exterior, de las instituciones financieras privadas y públicas sometidas al control de la Superintendencia de Bancos y Seguros" (JB-2014-2090, 2012)

5.4 Disposiciones de la Superintendencia de Economía Popular y Solidaria

La Superintendencia de Economía Popular y Solidaria conocida por sus siglas como SEPS es una entidad técnica de supervisión y control de las organizaciones de la

economía popular y solidaria, con personalidad jurídica de derecho público y autonomía administrativa y financiera, que busca el desarrollo, estabilidad, solidez y correcto funcionamiento del sector económico popular y solidario. Fue establecida en la Asamble Nacional el 5 de junio de 2012 con Hugo Jácome como Superintendente de Economía Popular y Solidaria . (SEPS, 2015)

Las funcionalidades de este órgano de control son:

(i) Reconocer a las organizaciones de la economía popular y solidaria como motor del desarrollo del país, promover los principios de cooperación, democracia, reciprocidad y solidaridad de estas organizaciones

(ii) Velar por la estabilidad, solidez y correcto funcionamiento de las organizaciones, establecer mecanismos de rendición de cuentas de los directivos hacia los socios y miembros de las organizaciones de la economía popular y solidaria

(iii) Impulsar la participación activa de los socios y miembros en el control y toma de decisiones dentro de sus organizaciones, a diferencia de las actividades económicas privadas

(iv) Identificar nuevos desafíos para el diseño de políticas públicas que beneficien, fortalezcan y consoliden al sector económico popular y solidario

(v) Fortalecer la gestión de las organizaciones en beneficio de sus integrantes y la comunidad. (SEPS, 2015)

Al hablar de Economía Popular y Solidaria se hace referencia "a la forma de organización económica, donde sus integrantes, individual o colectivamente, organizan y desarrollan procesos de producción, intercambio, comercialización, financiamiento y consumo de bienes y servicios, para satisfacer necesidades y generar ingresos basadas en relaciones de solidaridad,cooperación y reciprocidad, privilegiando al trabajo y al ser humano como sujeto y fin de su actividad, orientada al buen vivir, en armonía con la naturaleza, por sobre la apropiación, el lucro y la acumulación de capital." (Ley 001, 2011, art 1)

Así también, la constitución ecuatoriana respalda a la Economía Popular y Solidaria como un sector de la economía nacional formada por la asociación de diversos sectores desde cooperativas hasta comunidades. Esto se evidencia a través del artículo 283: "*El sistema económico es social y solidario; reconoce al ser humano como sujeto y fin;*

propende a una relación dinámica y equilibrada entre sociedad, Estado y mercado, en armonía con la naturaleza; y tiene por objetivo garantizar la producción y reproducción de las condiciones materiales e inmateriales que posibiliten el buen vivir. El sistema económico se integrará por las formas de organización económica pública, privada, mixta, popular y solidaria, y las demás que la Constitución determine. La economía popular y solidaria se regulará de acuerdo con la ley e incluirá a los sectores cooperativistas, asociativos y comunitarios " (Const., 2008, art 283)

El reconocimiento del sector financiero popular y solidario se ampara en el artículo 309, que describe: "*El sistema financiero nacional se compone de los sectores público, privado, y del popular y solidario, que intermedian recursos del público*" (Const., 2008, art 309)

La organización del sector financiero popular y solidario está descrita en el articulo 311 de la constitución, el cual dice: "*El sector financiero popular y solidario se compondrá de cooperativas de ahorro y crédito, entidades asociativas o solidarias, cajas y bancos comunales, cajas de ahorro. Las iniciativas de servicios del sector financiero popular y solidario, y de las micro, pequeñas y medianas unidades productivas, recibirán un tratamiento diferenciado y preferencial del Estado, en la medida en que impulsen el desarrollo de la economía popular y solidaria.*" (Const., 2008, art 311)

La Ley Orgánica de la Economía Popular y Solidaria se encarga de:

(i) "*Reconocer, fomentar y fortalecer la Economía Popular y Solidaria y el Sector Financiero Popular y Solidario en su ejercicio y relación con los demás sectores de la economía y con el Estado*

(ii) *Potenciar las prácticas de la economía popular y solidaria que se desarrollan en las comunas, comunidades, pueblos y nacionalidades, y en sus unidades económicas productivas para alcanzar el Sumak Kawsay*

(iii) *Establecer un marco jurídico común para las personas naturales y jurídicas que integran la Economía Popular y Solidaria y del Sector Financiero Popular y Solidario*

(iv) *Instituir el régimen de derechos, obligaciones y beneficios de las personas y organizaciones sujetas a esta ley*

(v) *Establecer la institucionalidad pública que ejercerá la rectoría, regulación, control, fomento y acompañamiento*" (LOEPS,2011,art 3)

Se puede resumir cinco aspectos positivos de esta ley, detallados a continuación:

(i) El estado se convierte en promotor del cooperativismo amparado en: "*tratamiento diferenciado y preferencial del Estado, en la medida en que impulsen el desarrollo de la economía popular y solidaria*"

(ii) La ley mantiene los principios de cooperativismo en términos de identidad, autogestión, responsabilidad social y ambiental, solidaridad y rendición de cuentas ya que la elección universal de socios para consejos de administración y vigilancia será democrática.

(iii) Permite una interrelación amplia y profunda, con los sectores público, privado e intra sectorialmente.

(iv) El establecimiento del órganismo de control SEPS que se encarga de la supervisión del conjunto del sistema de economía popular y solidaria basado en los principios del cooperativismo con contenido social. (Miño Grijalva, 2013)

5.5 Regulaciones y disposiciones de la Superintendencia de Bancos y Seguros

La Superintendencia de Bancos es el organismo de control, regulación y supervisión del sistema financiero del país. Así también, se encarga de que las instituciones reguladas cumplan con las leyes y que los usuarios depositen su confianza en el sistema. (Romero, 2015)

Las funciones principales de la Superintendencia de Bancos se detallan a continuación:

(i) Salvaguardar el interés general en el ámbito financiero

(i) Velar que las instituciones que controla sean estables, sólidas y posean un correcto funcionamiento

(i) Verificar que las instituciones reguladas presenten y adopten medidas correctivas y de saneamiento

(i) Elaboración y publicación trimestral del boletín de información financiera. (Romero, 2015)

La Junta Bancaria en la resolución JB-2012-2148 enfatiza en la implementación de medidas de seguridad por parte del sistema financiero con el fin de mitigar el riesgo de fraude por el uso de la tecnología de información y comunicaciones. Es por esto que modifica:

En el artículo 39 del título II "De la organización de las instituciones del sistema financiero privado" del capítulo I "Apertura y cierre de oficinas en el país y en el exterior, de las instituciones financieras privadas y públicas sometidas al control de la Superintendencia de Bancos y Seguros" del libro I "Normas generales para la aplicación de la Ley General de Instituciones del Sistema Financiero":

(i) Artículo 39, numeral 2: "*Protección contra clonación de tarjetas.- Contar con dispositivos electrónicos y/o elementos físicos que impidan y detecten de manera efectiva la colocación de falsas lectoras de tarjetas, con el fin de evitar la clonación de tarjetas de débito o de crédito, además de los correspondientes mecanismos de monitoreo en línea de las alarmas que generen los dispositivos electrónicos en caso de suscitarse eventos inusuales*" (JB-2012-2148, 2012)

(ii) Artículo 39, numeral 6: "*Protección al software e información del cajero automático.- Disponer de un programa o sistema de protección contra intrusos (Antimalware) que permita proteger el software instalado en el cajero automático y que detecte oportunamente cualquier alteración en su código, configuración y/o funcionalidad. Así mismo, se deberá instalar mecanismos que sean capaces de identificar conexiones no autorizadas a través de los puertos USB, comunicaciones remotas, cambio de los discos duros y otros componentes que guarden o procesen información. En una situación de riesgo deben emitir alarmas a un centro de monitoreo o dejar inactivo al cajero automático hasta que se realice la inspección por parte del personal especializado de la institución*" (JB-2012-2148, 2012)

Así también, se decreta incluir y renumerar los siguientes artículos:

(i) Artículo 39, numeral 7: *" Procedimientos para el mantenimiento preventivo y correctivo en los cajeros automáticos.- Disponer de procedimientos auditables debidamente acordados y coordinados entre la institución y los proveedores internos o externos para la ejecución de las tareas de mantenimiento preventivo y correctivo del hardware y software, provisión de suministros y recarga de dinero en las gavetas. Las claves de acceso tipo "administrador" del sistema del cajero automático deben ser únicas y reemplazadas periódicamente"* (JB-2012-2148, 2012)

(ii) Artículo 39, numeral 8: "*Accesos físicos al interior de los cajeros automáticos.- Disponer de cerraduras de alta tecnología y seguridades que garanticen el acceso controlado al interior del cajero automático por parte del personal técnico o de mantenimiento que disponga de las respectivas llaves. Estas cerraduras deben operar con llaves únicas y no genéricas o maestras"* (JB-2012-2148, 2012)

(iii) Artículo 39, numeral 9: *"Reportes de nivel de seguridad de los cajeros- Comunicar oportunamente la información sobre los estándares de seguridad implementados en los cajeros automáticos, incidentes de seguridad (vandalismo y/o fraudes) identificados en sus cajeros automáticos y/o ambientes de software o hardware relacionados*" (JB-2012-2148, 2012)

En el artículo 2 del título X "De la gestión integral y control de riesgos" del capítulo V "De la gestión del riesgo operativo" del libro I "Normas generales para la aplicación de la Ley General de Instituciones del Sistema Financiero":

(i) Artículo 2, numeral 35: *"Calidad de la información.- Es el resultado de la aplicación de los mecanismos implantados que garantizan la efectividad, eficiencia y confiabilidad de la información y los recursos relacionados con ella;"* (JB-2012-2148, 2012)

(ii) Artículo 2, numeral 36: *"Efectividad.- Es la garantía de que la información es relevante y pertinente y que su entrega es oportuna, correcta y consistente;"* (JB-2012-2148, 2012)

(iii) Artículo 2, numeral 37: *"Confiabilidad.- Es la garantía de que la información es la apropiada para la administración de la entidad, ejecución de transacciones y para el cumplimiento de sus obligaciones;"* (JB-2012-2148, 2012)

(iv) Artículo 2, numeral 38*: "Banca electrónica.- Son los servicios suministrados por las instituciones del sistema financiero a los clientes a través de internet en el sitio que corresponda a uno o más dominios de la institución, indistintamente del dispositivo tecnológico a través del cual se acceda;"* (JB-2012-2148, 2012)

(v) Artículo 2, numeral 39: *"Banca móvil.- Son los servicios suministrados por las instituciones del sistema financiero a los clientes a través de equipos*

celulares mediante los protocolos propios de este tipo de dispositivos;" (JB-2012-2148, 2012)

(vi) Artículo 2, numeral 40: *"Tarjetas.- Para efectos del presente capítulo, se refiere a las tarjetas de débito, de cajero automático y tarjetas de crédito;"* (JB-2012-2148, 2012)

(vii) Artículo 2, numeral 41: *"Canales electrónicos.- Se refiere a todas las vías o formas a través de las cuales los clientes o usuarios pueden efectuar transacciones con las instituciones del sistema financiero, mediante el uso de elementos o dispositivos electrónicos o tecnológicos, utilizando o no tarjetas. Principalmente son canales electrónicos: los cajeros automáticos (ATM), dispositivos de puntos de venta (POS y PIN Pad), sistemas de audio respuesta (IVR), señal telefónica, celular e internet u otro similares;"* (JB-2012-2148, 2012)

(viii) Artículo 2, numeral 42:*"Tarjeta inteligente.- Tarjeta que posee circuitos integrados (chip) que permiten la ejecución de cierta lógica programada, contiene memoria y microprocesadores y es capaz de proveer seguridad, principalmente en cuanto a la confidencialidad de la información de la memoria; y,"* (JB-2012-2148, 2012)

Se incluye el numeral 4.3.8 con lo siguientes:

(ix) Artículo 2, numeral 4.3.8 "*Medidas de seguridad en canales electrónicos.- Con el objeto de garantizar que las transacciones realizadas a través de canales electrónicos cuenten con los controles, medidas y elementos de seguridad para evitar el cometimiento de eventos fraudulentos y garantizar la seguridad y calidad de la información de los usuarios así como los bienes de los clientes a cargo de las instituciones controladas, éstas deberán cumplir como mínimo con lo siguiente:*

a. *4.3.8.1 Las instituciones del sistema financiero deberán adoptar e implementar los estándares y buenas prácticas internacionales de seguridad vigentes a nivel mundial para el uso y manejo de canales electrónicos y consumos con tarjetas, los cuales deben ser permanentemente monitoreados para asegurar su cumplimiento;* (JB-2012-2148, 2012)

b. *4.3.8.2 Establecer procedimientos y mecanismos para monitorear de manera periódica la efectividad de los niveles de seguridad implementados en hardware, software, redes y comunicaciones, así como en cualquier otro elemento electrónico o tecnológico utilizado en los canales electrónicos, de tal manera que se garantice permanentemente la seguridad y calidad de la información;* (JB-2012-2148, 2012)

c. *4.3.8.3 El envío de información confidencial de sus clientes y la relacionada con tarjetas, debe ser realizado bajo condiciones de seguridad de la información, considerando que cuando dicha información se envíe mediante correo electrónico o utilizando algún otro medio vía Internet, ésta deberá estar sometida a técnicas de encriptación acordes con los estándares internacionales vigentes;"* (JB-2012-2148, 2012)

d. *4.3.8.4 La información que se transmita entre el canal electrónico y el sitio principal de procesamiento de la entidad, deberá estar en todo momento protegida mediante el uso de técnicas de encriptación y deberá evaluarse con regularidad la efectividad y vigencia del mecanismo de encriptación utilizado;* (JB-2012-2148, 2012)

e. *4.3.8.5 Las instituciones del sistema financiero deberán contar en todos sus canales electrónicos con software antimalware que esté permanentemente actualizado, el cual permita proteger el software instalado, detectar oportunamente cualquier intento o alteración en su código, configuración y/o funcionalidad, y emitir las alarmas correspondientes para el bloqueo del canal electrónico, su inactivación y revisión oportuna por parte de personal técnico autorizado de la institución;* (JB-2012-2148, 2012)

f. *4.3.8.6 Las instituciones del sistema financiero deberán utilizar hardware de propósito específico para la generación y validación de claves para ejecutar transacciones en los diferentes canales electrónicos y dicha información no deberá ser almacenada en ningún momento;* (JB-2012-2148, 2012)

g. *4.3.8.7 Establecer procedimientos para monitorear, controlar y emitir alarmas en línea que informen oportunamente sobre el estado de los*

canales electrónicos, con el fin de identificar eventos inusuales, fraudulentos o corregir las fallas; (JB-2012-2148, 2012)

h. *4.3.8.8 Ofrecer a los clientes los mecanismos necesarios para que personalicen las condiciones bajo las cuales desean realizar sus transacciones a través de los diferentes canales electrónicos y tarjetas, dentro de las condiciones o límites máximos que deberá establecer cada entidad. Entre las principales condiciones de personalización por cada tipo de canal electrónico, deberán estar: registro de las cuentas a las cuales desea realizar transferencias, registro de direcciones IP de computadores autorizados, el ó los números de telefonía móvil autorizados, montos máximos por transacción diaria, semanal y mensual, entre otros. Para el caso de consumos con tarjetas, se deberán personalizar los cupos máximos, principalmente para los siguientes servicios: consumos nacionales, consumos en el exterior, compras por internet, entre otros;* (JB-2012-2148, 2012)

i. *4.3.8.9 Incorporar en los procedimientos de administración de seguridad de la información la renovación de por lo menos una vez (1) al año de las claves de acceso a cajeros automáticos; dicha clave deberá ser diferente de aquella por la cual se accede a otros canales electrónicos;* (JB-2012-2148, 2012)

j. *4.3.8.10 Las instituciones deberán establecer procedimientos de control y mecanismos que permitan registrar el perfil de cada cliente sobre sus costumbres transaccionales en el uso de canales electrónicos y tarjetas y definir procedimientos para monitorear en línea y permitir o rechazar de manera oportuna la ejecución de transacciones que no correspondan a sus hábitos, lo cual deberá ser inmediatamente notificado al cliente mediante mensajería móvil, correo electrónico, u otro mecanismo;* (JB-2012-2148, 2012)

k. *4.3.8.11 Incorporar en los procedimientos de administración de la seguridad de la información, el bloqueo de los canales electrónicos o de las tarjetas cuando se presenten eventos inusuales que adviertan situaciones fraudulentas o después de un número máximo de tres (3) intentos de acceso fallido. Además, se deberán establecer procedimientos que permitan la notificación en línea al cliente a través*

de mensajería móvil, correo electrónico u otro mecanismo, así como su reactivación de manera segura; (JB-2012-2148, 2012)

l. *4.3.8.12 Asegurar que exista una adecuada segregación de funciones entre el personal que administra, opera, mantiene y en general accede a los dispositivos y sistemas usados en los diferentes canales electrónicos y tarjetas;* (JB-2012-2148, 2012)

m. *4.3.8.13 Las entidades deberán establecer procedimientos y controles para la administración, transporte, instalación y mantenimiento de los elementos y dispositivos que permiten el uso de los canales electrónicos y de tarjetas;* (JB-2012-2148, 2012)

n. *4.3.8.14 Las instituciones del sistema financiero deben mantener sincronizados todos los relojes de sus sistemas de información que estén involucrados con el uso de canales electrónicos;* (JB-2012-2148, 2012)

o. *4.3.8.15 Mantener como mínimo durante doce (12) meses el registro histórico de todas las operaciones que se realicen a través de los canales electrónicos, el cual deberá contener como mínimo: fecha, hora, monto, números de cuenta (origen y destino en caso de aplicarse), código de la institución del sistema financiero de origen y de destino, número de transacción, código del dispositivo: para operaciones por cajero automático: código del ATM, para transacciones por internet: la dirección IP, para transacciones a través de sistemas de audio respuesta - IVR y para operaciones de banca electrónica mediante dispositivos móviles: el número de teléfono con el que se hizo la conexión. En caso de presentarse reclamos, la información deberá conservarse hasta que se agoten las instancias legales. Si dicha información constituye respaldo contable se aplicará lo previsto en el tercer inciso del artículo 80 de la Ley General de Instituciones del Sistema Financiero;* (JB-2012-2148, 2012)

p. *4.3.8.16 Incorporar en los procedimientos de administración de la seguridad de la información, controles para impedir que funcionarios de la entidad que no estén debidamente autorizados tengan acceso a consultar información confidencial de los clientes en ambiente de producción. En el caso de información contenida en ambientes de*

desarrollo y pruebas, ésta deberá ser enmascarada o codificada. (JB-2012-2148, 2012)

q. *Todos estos procedimientos deberán estar debidamente documentados en los manuales respectivos. Además, la entidad deberá mantener y monitorear un log de auditoría sobre las consultas realizadas por los funcionarios a la información confidencial de los clientes, la cual debe contener como mínimo: identificación del funcionario, sistema utilizado, identificación del equipo (IP), fecha, hora, e información consultada. Esta información deberá conservarse por lo menos por doce (12) meses;* (JB-2012-2148, 2012)

r. *4.3.8.17 Las instituciones del sistema financiero deberán poner a disposición de sus clientes un acceso directo como parte de su centro de atención telefónica (call center) para el reporte de emergencias bancarias, el cual deberá funcionar las veinticuatro (24) horas al día, los siete (7) días de la semana;* (JB-2012-2148, 2012)

s. *4.3.8.18 Mantener por lo menos durante seis (6) meses la grabación de las llamadas telefónicas realizadas por los clientes a los centros de atención telefónica (call center), específicamente cuando se consulten saldos, consumos o cupos disponibles; se realicen reclamos; se reporten emergencias bancarias; o, cuando se actualice su información. De presentarse reclamos, esa información deberá conservarse hasta que se agoten las instancias legales;* (JB-2012-2148, 2012)

t. *4.3.8.19 Las entidades deberán implementar los controles necesarios para que la información de claves ingresadas por los clientes mediante los centros de atención telefónica (call center), estén sometidas a técnicas de encriptación acordes con los estándares internacionales vigentes;* (JB-2012-2148, 2012)

u. *4.3.8.20 Las instituciones del sistema financiero deberán ofrecer a los clientes el envío en línea a través de mensajería móvil, correo electrónico u otro mecanismo, la confirmación del acceso a la banca electrónica, así como de las transacciones realizadas mediante cualquiera de los canales electrónicos disponibles, o por medio de tarjetas;* (JB-2012-2148, 2012)

v. *4.3.8.21 Las tarjetas emitidas por las instituciones del sistema financiero que las ofrezcan deben ser tarjetas inteligentes, es decir, deben contar con microprocesador o chip; y, las entidades controladas deberán adoptar los estándares internacionales de seguridad y las mejores prácticas vigentes sobre su uso y manejo;* (JB-2012-2148, 2012)

w. *4.3.8.22 Mantener permanentemente informados y capacitar a los clientes sobre los riesgos derivados del uso de canales electrónicos y de tarjetas; y, sobre las medidas de seguridad que se deben tener en cuenta al momento de efectuar transacciones a través de éstos;* (JB-2012-2148, 2012)

x. *4.3.8.23 Informar y capacitar permanentemente a los clientes sobre los procedimientos para el bloqueo, inactivación, reactivación y cancelación de los productos y servicios ofrecidos por la entidad;* (JB-2012-2148, 2012)

y. *4.3.8.24 Es función de auditoría interna verificar oportunamente la efectividad de las medidas de seguridad que las instituciones del sistema financiero deben implementar en sus canales electrónicos; así también deberán informar sobre las medidas correctivas establecidas en los casos de reclamos de los usuarios financieros que involucren debilidades o violación de los niveles de seguridad;* (JB-2012-2148, 2012)

z. *4.3.8.25 Implementar técnicas de seguridad de la información en los procesos de desarrollo de las aplicaciones que soportan los canales electrónicos, con base en directrices de codificación segura a fin de que en estos procesos se contemple la prevención de vulnerabilidades"* (JB-2012-2148, 2012)

En cuanto a cajeros automáticos decreta lo siguiente:

(x) "4.3.9 Cajeros automáticos.- Con el objeto de garantizar la seguridad en las transacciones realizadas a través de los cajeros automáticos, las instituciones del sistema financiero deberán cumplir como mínimo con lo siguiente:

a. *4.3.9.1 Los dispositivos utilizados en los cajeros automáticos para la autenticación del cliente o usuario, deben encriptar la información*

ingresada a través de ellos; y, la información de las claves no debe ser almacenada en ningún momento; (JB-2012-2148, 2012)

b. *4.3.9.2 La institución controlada debe implementar mecanismos internos de autenticación del cajero automático que permitan asegurar que es un dispositivo autorizado por la institución del sistema financiero a la que pertenece;* (JB-2012-2148, 2012)

c. *4.3.9.3 Los cajeros automáticos deben ser capaces de procesar la información de tarjetas inteligentes o con chip;* (JB-2012-2148, 2012)

d. *4.3.9.4 Los cajeros automáticos deben estar instalados de acuerdo con las especificaciones del fabricante, así como con los estándares de seguridad definidos en las políticas de la institución del sistema financiero, incluyendo el cambio de las contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores;* (JB-2012-2148, 2012)

e. *4.3.9.5 Disponer de un programa o sistema de protección contra intrusos (Anti-malware) que permita proteger el software instalado en el cajero automático y que detecte oportunamente cualquier alteración en su código, configuración y/o funcionalidad. Así mismo, se deberán instalar mecanismos que sean capaces de identificar conexiones no autorizadas a través de los puertos USB, comunicaciones remotas, cambio de los discos duros y otros componentes que guarden o procesen información. En una situación de riesgo deben emitir alarmas a un centro de monitoreo o dejar inactivo al cajero automático hasta que se realice la inspección por parte del personal especializado de la institución;* (JB-2012-2148, 2012)

f. *4.3.9.6 Establecer y ejecutar procedimientos de auditoría de seguridad en sus cajeros automáticos por lo menos una vez al año, con el fin de identificar vulnerabilidades y mitigar los riesgos que podrían afectar a la seguridad de los servicios que se brindan a través de estos. Los procedimientos de auditoría deberán ser ejecutados por personal capacitado y con experiencia;* (JB-2012-2148, 2012)

g. *4.3.9.7 Para la ejecución de transacciones de clientes, se deberán implementar mecanismos de autenticación que contemplen por lo menos dos de tres factores: "algo que se sabe, algo que se tiene, o algo que se es"* (JB-2012-2148, 2012)

Referente a banca electrónica dispone lo siguiente:

Banca electrónica.- Con el objeto de garantizar la seguridad en las transacciones realizadas mediante la banca electrónica, las instituciones del sistema financiero que ofrezcan servicios por medio de este canal electrónico deberán cumplir como mínimo con lo siguiente:

(i) *4.3.11.1 Implementar los algoritmos y protocolos seguros, así como certificados digitales, que ofrezcan las máximas seguridades en vigor dentro de las páginas web de las entidades controladas, a fin de garantizar una comunicación segura, la cual debe incluir el uso de técnicas de encriptación de los datos transmitidos acordes con los estándares internacionales vigentes;* (JB-2012-2148, 2012)

(ii) *4.3.11.2 Realizar como mínimo una vez (1) al año una prueba de vulnerabilidad y penetración a los equipos, dispositivos y medios de comunicación utilizados en la ejecución de transacciones por banca electrónica; y, en caso de que se realicen cambios en la plataforma que podrían afectar a la seguridad de este canal, se deberá efectuar una prueba adicional. Las pruebas de vulnerabilidad y penetración deberán ser efectuadas por personal independiente a la entidad, de comprobada competencia y aplicando estándares vigentes y reconocidos a nivel internacional. Las instituciones deberán definir y ejecutar planes de acción sobre las vulnerabilidades detectadas;* (JB-2012-2148, 2012)

(iii) *4.3.11.3 Los informes de las pruebas de vulnerabilidad deberán estar a disposición de la Superintendencia de Bancos y Seguros, incluyendo un análisis comparativo del informe actual respecto del inmediatamente anterior;* (JB-2012-2148, 2012)

(iv) *4.3.11.4 Implementar mecanismos de control, autenticación mutua y monitoreo, que reduzcan la posibilidad de que los clientes accedan a páginas web falsas similares a las propias de las instituciones del sistema financiero;* (JB-2012-2148, 2012)

(v) *4.3.11.5 Implementar mecanismos de seguridad incluyendo dispositivos tales como IDS, IPS, firewalls, entre otros, que reduzcan la posibilidad de que la información de las transacciones de los clientes sea capturada por terceros no autorizados durante la sesión;* (JB-2012-2148, 2012)

(vi) *4.3.11.6 Establecer un tiempo máximo de inactividad, después del cual deberá ser cancelada la sesión y exigir un nuevo proceso de autenticación al cliente para realizar otras transacciones;* (JB-2012-2148, 2012)

(vii) *4.3.11.7 Se deberá informar al cliente al inicio de cada sesión, la fecha y hora del último ingreso al canal de banca electrónica;* (JB-2012-2148, 2012)

(viii) *4.3.11.8 La institución del sistema financiero deberá implementar mecanismos para impedir la copia de los diferentes componentes de su sitio web, verificar constantemente que no sean modificados sus enlaces (links), suplantados sus certificados digitales, ni modificada indebidamente la resolución de su sistema de nombres de dominio (DNS);* (JB-2012-2148, 2012)

(ix) *4.3.11.9 La institución del sistema financiero debe implementar mecanismos de autenticación al inicio de sesión de los clientes, en donde el nombre de usuario debe ser distinto al número de cédula de identidad y éste así como su clave de acceso deben combinar caracteres numéricos y alfanuméricos con una longitud mínima de seis (6) caracteres;* (JB-2012-2148, 2012)

(x) *4.3.11.10 Para la ejecución de transacciones de clientes, se deberán implementar mecanismos de autenticación que contemplen por lo menos dos de tres factores: "algo que se sabe, algo que se tiene, o algo que se es", considerando que uno de ellos debe: ser dinámico por cada vez que se efectúa una operación, ser una clave de una sola vez OTP (one time password), tener controles biométricos, entre otros;* (JB-2012-2148, 2012)

(xi) *4.3.11.11 En todo momento en donde se solicite el ingreso de una clave numérica, los sitios web de las entidades deben exigir el ingreso de éstas a través de teclados virtuales, las mismas que deberán estar enmascaradas;"* (JB-2012-2148, 2012)

Finalmente, para Banca móvil se sujetarán a los numerales 4.3.8 y 4.3.11.

Por otra parte, la resolución JB-2014-3066 con el fin de mejorar la gestión de la tecnología de información y comunicaciones, la continuidad del negocio y mitigar los fraudes relacionados a cajeros automáticos bajo referencia de la norma ISO/IEC 27000 reforma lo siguiente:

En el Artículo 2 del título X "De la gestión y administración de riesgo" del capítulo V "De la gestión del riesgo operativo" del libro I "Normas generales para la aplicación de la Ley General de Instituciones del Sistema Financiero":

(i) Artículo 2, numeral 18: *"Responsable de la información.- Es la persona encargada de cuidar la integridad, confidencialidad y disponibilidad de información; debe tener autoridad para especificar y exigir las medidas de seguridad necesarias para cumplir con sus responsabilidades"* (JB-2014-3066, 2014)

(ii) Artículo 2, numeral 29: "*Plan de continuidad.- Está orientado a asegurar la continuidad del negocio, la satisfacción del cliente y la productividad a pesar de eventos inesperados. Se ejecuta permanentemente como parte de la administración de riesgos. Un plan de continuidad debe contener procedimientos que se ajusten a la realidad del negocio de cada institución"* (JB-2014-3066, 2014)

(iii) Artículo 2, numeral 30: *"Administración de la continuidad.- Es un proceso permanente que garantiza la continuidad de las operaciones del negocio de las instituciones del sistema financiero, a través de la efectividad del mantenimiento del plan de continuidad;"* (JB-2014-3066, 2014)

Se incluyen los siguientes numerales:

(i) Artículo 2, numeral 42: *"Transacción.- Se refiere a las acciones realizadas por los clientes a través de canales electrónicos, tales como: consultas, transferencias, depósitos, retiros, pagos, cambios de clave, actualización de datos y otras relacionadas"* (JB-2014-3066, 2014)

(ii) Artículo 2, numeral 43: *"Incidente de tecnología de la información.- Evento asociado a posibles fallas en la tecnología de la información, fallas en los controles, o situaciones con probabilidad significativa de comprometer las operaciones del negocio"* (JB-2014-3066, 2014)

(iii) Artículo 2, numeral 44: *"Incidente de seguridad de la información.- Evento asociado a posibles fallas en la seguridad de la información, o una situación con probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información"* (JB-2014-3066, 2014)

En el Artículo 4 del título X "De la gestión y administración de riesgo" del capítulo V "De la gestión del riesgo operativo" del libro I "Normas generales para la aplicación de la Ley General de Instituciones del Sistema Financiero":

(i) Artículo 4, numeral: "*En función del tamaño y complejidad de las operaciones, las entidades deben conformar el comité de tecnología, que es el responsable de planificar, coordinar y supervisar las actividades de tecnología. El directorio asumirá las responsabilidades del comité de tecnología en las entidades que decidieran no conformarlo. La Superintendencia de Bancos y Seguros podrá disponer la conformación de este comité, si las condiciones de tamaño y complejidad de la entidad lo amerita.*

Dicho comité debe estará integrado como mínimo por: un delegado del directorio, quien lo presidirá, el representante legal de la institución y el funcionario responsable del área de tecnología" (JB-2014-3066, 2014)

a. Artículo 4, numeral 3.1.5: "*Políticas, procesos, procedimientos y metodologías de tecnología de la información definidos bajo estándares de general aceptación que garanticen la ejecución de los criterios de control interno de eficacia, eficiencia y cumplimiento, alineados a los objetivos y actividades de la institución, así como las consecuencias de la violación de éstas.*

Los procesos, procedimientos y metodologías de tecnología de la información deben ser revisados por el comité de tecnología y propuestos para la posterior aprobación del directorio o el organismo que haga sus veces" (JB-2014-3066, 2014)

b. Artículo 4, numeral 3.2.1: "*Procedimientos que establezcan las actividades y responsables de la operación y el uso de las instalaciones de procesamiento de información*" (JB-2014-3066, 2014)

c. Artículo 4, numeral 3.2.2: " *Procedimientos de gestión de incidentes de tecnología de la información, que considere al menos su registro, priorización, análisis, escalamiento y solución*" (JB-2014-3066, 2014)
d. Artículo 4, numeral 3.2.3: *" Inventario de la infraestructura tecnológica que considere por lo menos, su registro, responsables de uso y mantenimiento"* (JB-2014-3066, 2014)
e. Artículo 4, numeral 3.2.4: *"Procedimientos de respaldo de información periódicos, acorde a los requerimientos de continuidad del negocio que incluyan la frecuencia de verificación, las condiciones de preservación y eliminación y el transporte seguro hacia una ubicación remota, que no debe estar expuesto a los mismos riesgos del sitio principal"* (JB-2014-3066, 2014)

El Artículo 15 del título X "De la gestión y administración de riesgo" del capítulo V "De la gestión del riesgo operativo" del libro I "Normas generales para la aplicación de la Ley General de Instituciones del Sistema Financiero" es reestructurado a:

"*ARTÍCULO 15.- Las instituciones controladas deben administrar la continuidad del negocio, manteniendo procedimientos actualizados, a fi n de garantizar su capacidad para operar en forma continua y minimizar las pérdidas en caso de una interrupción del negocio."* (JB-2014-3066, 2014)

"Para el efecto, las instituciones del sistema financiero deben establecer un proceso de administración de la continuidad del negocio, tomando como referencia el estándar ISO 22301 o el que lo sustituya, y considerar al menos lo siguiente:" (JB-2014-3066, 2014)

(i) *"15.1 La definición de objetivos, políticas, estrategias, procedimientos, metodología, planes y presupuesto para la administración de la continuidad;*"(JB-2014-3066, 2014)
(ii) *"15.2 Un comité de continuidad del negocio que esté conformado como mínimo por los siguientes miembros: el funcionario responsable de la unidad de riesgos, quien lo preside, el funcionario responsable de la administración de la continuidad, quien hará las veces de secretario, el funcionario responsable del área de tecnología de la información, el*

funcionario responsable del área de talento humano, el auditor interno, solo con voz, y el máximo representante de cada una de las áreas involucradas en el proceso de administración de la continuidad. El comité de continuidad del negocio debe sesionar mínimo con la mitad más uno de sus integrantes, al menos una vez cada trimestre, y sus decisiones serán tomadas por mayoría absoluta de votos. El presidente del comité tendrá voto dirimente. El comité de continuidad del negocio debe dejar evidencia de las decisiones adoptadas, las cuales deben ser conocidas y aprobadas por el comité de administración integral de riesgos. El comité de continuidad del negocio debe tener al menos las siguientes responsabilidades:

a. *15.2.1. Monitorear la implementación del plan y asegurar el alineamiento de éste con la metodología; y, velar por una administración de la continuidad del negocio competente;*
b. *15.2.2. Proponer cambios, actualizaciones y mejoras al plan;*
c. *15.2.3. Revisar el presupuesto del plan y ponerlo en conocimiento del comité de administración integral de riesgos;*
d. *15.2.4. Dar seguimiento a las potenciales amenazas que pudieran derivar en una interrupción de la continuidad de las operaciones y coordinar las acciones preventivas; y,*
e. *15.2.5. Realizar un seguimiento a las medidas adoptadas en caso de presentarse una interrupción de la continuidad de las operaciones;* (JB-2014-3066, 2014)

(iii) *"15.3 Análisis de impacto que tendría una interrupción de los procesos que soportan los principales productos y servicios. Para ello, deben determinar el impacto en términos de magnitud de daños, el período de recuperación y tiempos máximos de interrupción que puedan ocasionar los siniestros."* (JB-2014-3066, 2014)

(iv) *"El análisis de impacto debe ser revisado periódicamente y actualizado cuando existan cambios en la organización o en su entorno, que puedan afectar sus resultados;*" (JB-2014-3066, 2014)

(v) *"15.4 Análisis que identifique los principales escenarios de riesgos, incluyendo las fallas en la tecnología de la información, tomando en cuenta el impacto y la probabilidad de que sucedan. Para ello, debe seguirse una*

metodología consistente con aquella utilizada para la evaluación de los demás riesgos"; (JB-2014-3066, 2014)

(vi) *"15.5 Evaluación y selección de estrategias de continuidad por proceso que permitan mantener la continuidad de los procesos que soportan los principales productos y servicios, dentro del tiempo objetivo de recuperación definido para cada proceso, mismas que deben tomar en cuenta, al menos lo siguiente: la seguridad del personal, habilidades y conocimientos asociados al proceso, instalaciones alternas de trabajo, infraestructura alterna de procesamiento e información que soporte el proceso, seguridad de la información y equipamiento necesario para el proceso;"* (JB-2014-3066, 2014)

(vii) *"15.6 Realización de pruebas del plan de continuidad del negocio que permitan comprobar su efectividad y realizar los ajustes necesarios, cuando existan cambios que afecten la aplicabilidad del plan o al menos una vez al año;"* (JB-2014-3066, 2014)

(viii) *"15.7 Procedimientos de difusión, comunicación, entrenamiento y concienciación del plan y su cumplimiento; e,*

(ix) *15.8 Incorporación del proceso de administración de la continuidad del negocio al proceso de administración integral de riesgos, que garantice la actualización y mejora continua del plan de continuidad del negocio*." (JB-2014-3066, 2014)

El Artículo 16 del título X "De la gestión y administración de riesgo" del capítulo V "De la gestión del riesgo operativo" del libro I "Normas generales para la aplicación de la Ley General de Instituciones del Sistema Financiero" es reestructurado a:

" ARTÍCULO 16.- El plan de continuidad del negocio debe contener al menos los procedimientos operativos, tecnológicos, de emergencias y comunicaciones para cada proceso crítico y para cada escenario cubierto, los cuales deben considerar, según corresponda, como mínimo lo siguiente:

(i) *16.1 Escenarios de riesgos y procesos críticos cubiertos y alertas de los escenarios y procesos críticos no cubiertos por el plan;*

(ii) *16.2 Roles y responsabilidades de las personas encargadas de ejecutar cada actividad;*

(iii) *16.3 Criterios de invocación y activación del plan;*

(iv) *16.4 Responsable de su actualización;*

(v) *16.5 Acciones y procedimientos a ejecutar antes, durante y después de ocurrido el incidente que ponga en peligro la operatividad de la institución, priorizando la seguridad del personal;*

(vi) *16.6 Tiempos máximos de interrupción y de recuperación de cada proceso;*

(vii) *16.7 Acciones y procedimientos a realizar para trasladar las actividades de la institución a ubicaciones transitorias alternativas o para el restablecimiento de los procesos críticos de manera urgente;*

(viii) *16.8 Información vital y cómo acceder a ella (incluye información de clientes, contratos, pólizas de seguro, manuales técnicos y de operación, entre otros);*

(ix) *16.9 Comunicaciones con el personal involucrado, sus familiares y contactos de emergencia, para lo cual debe contar con la información para contactarlos oportunamente (direcciones, teléfonos, correos electrónicos, entre otros);*

(x) *16.10 Interacción con los medios de comunicación;*

(xi) *16.11 Comunicación con los grupos de interés;*

(xii) *16.12 Establecimiento de un centro de comando (considerar al menos un sitio principal, y uno alterno); y,*

(xiii) *16.13 Ante eventos de desastre en el centro principal de procesamiento, los procedimientos de restauración en una ubicación remota de los servicios de tecnología de la información deben estar dentro de los parámetros establecidos en el plan, permitiendo una posterior recuperación de las condiciones previas a su ocurrencia. La ubicación remota no debe estar expuesta a los mismos riesgos del sitio principal."* (JB-2014-3066, 2014)

El Artículo 17 del título X "De la gestión y administración de riesgo" del capítulo V "De la gestión del riesgo operativo" del libro I "Normas generales para la aplicación de la Ley General de Instituciones del Sistema Financiero" es reestructurado a:

"ARTÍCULO 17.- Las responsabilidades del directorio, en cuanto a la administración del riesgo operativo, se regirán por lo dispuesto en la sección III "Responsabilidad en la administración de riesgos", del capítulo I "De la gestión integral y control de riesgos", de este título.

Adicionalmente, el directorio tendrá las siguientes responsabilidades en relación con la administración del riesgo operativo:

(i) *17.1 Crear una cultura organizacional con principios y valores de comportamiento ético que priorice la gestión eficaz del riesgo operativo;*

(ii) *17.2 Aprobar las políticas y estrategias relacionadas con la administración y gestión del riesgo operativo que permitan el cumplimiento de las disposiciones establecidas en este capítulo;*

(iii) *17.3 Podrá delegar la aprobación de los procesos, procedimientos y metodologías para la gestión de procesos, personas, tecnología de la información y servicios provistos por terceros a la instancia que considere pertinente, la misma que debe velar que los mismos estén alineados al cumplimiento de las políticas y estrategias de la administración del riesgo operativo aprobadas por el directorio; y,*

(iv) *17.4 Aprobar el proceso, metodología y plan para la administración de la continuidad del negocio."* (JB-2014-3066, 2014)

El Artículo 18 del título X "De la gestión y administración de riesgo" del capítulo V "De la gestión del riesgo operativo" del libro I "Normas generales para la aplicación de la Ley General de Instituciones del Sistema Financiero" es reestructurado a:

"ARTÍCULO 18.- Las funciones y responsabilidades del comité de administración integral de riesgos se regirán por lo dispuesto en la sección III "Responsabilidad en la administración de riesgos", del capítulo I "De la gestión integral y control de riesgos".

Adicionalmente, el comité de administración integral de riesgos tendrá las siguientes responsabilidades en relación con la administración del riesgo operativo:

(i) *18.1 Evaluar y proponer para la aprobación del directorio las políticas para la administración del riesgo operativo;*

(ii) *18.2 Evaluar y proponer mejoras al proceso de administración de riesgo operativo y asegurarse que sean implementados en toda la institución y que todos los niveles del personal entiendan sus responsabilidades con relación al riesgo operativo;*

(iii) *18.3 Definir los mecanismos para monitorear y evaluar los cambios significativos y la exposición a riesgos;*

(iv) *18.4 Evaluar y someter a aprobación del directorio el proceso, metodología y plan de continuidad del negocio a los que se refiere la sección IV, del este capítulo; asegurar su aplicabilidad; y, cumplimiento del mismo; y,*

(v) *18.5 Analizar y aprobar la designación de líderes encargados de llevar a cabo las actividades previstas en el plan de continuidad del negocio."* (JB-2014-3066, 2014)

En el Artículo 19 del título X "De la gestión y administración de riesgo" del capítulo V "De la gestión del riesgo operativo" del libro I "Normas generales para la aplicación de la Ley General de Instituciones del Sistema Financiero":

(i) Artículo 19, numeral 4: *"Liderar el desarrollo, la aplicabilidad y cumplimiento del proceso y plan de continuidad del negocio, al que se refiere la sección IV de este capítulo; así como proponer el nombre de los líderes de las áreas que deban cubrir el plan de continuidad del negocio, para lo cual debe designar de manera formal, un responsable del proceso de la administración de la continuidad, el cual debe tener a su cargo, entre otras, las siguientes funciones:"* (JB-2014-3066, 2014)

a. Artículo 19, numeral 4.1: " *Proponer las políticas, procedimientos y metodologías para la administración de la continuidad del negocio, incluyendo la asignación de roles y responsabilidades"* (JB-2014-3066, 2014)

b. Artículo 19, numeral.4.2: "*Proponer cambios, actualizaciones y mejorar al plan de continuidad"* (JB-2014-3066, 2014)

c. Artículo 19, numeral.4.3: *"Informar al comité de continuidad los aspectos relevantes de la administración de la continuidad del negocio para una oportuna toma de decisiones;"* (JB-2014-3066, 2014)

En el Artículo 20 del título X "De la gestión y administración de riesgo" del capítulo V "De la gestión del riesgo operativo" del libro I "Normas generales para la aplicación de la Ley General de Instituciones del Sistema Financiero":

(i) Artículo 20, numeral 6: *"Si las instituciones del sistema financiero desean contratar la ejecución de los procesos productivos y/o servicios críticos en el exterior, deben notificar a la Superintendencia de Bancos y Seguros,*

adjuntando la documentación de respaldo que asegure el cumplimiento de este artículo. Además, las instituciones deben exigir al proveedor del servicio en el exterior, se encuentre sujeto a una supervisión efectiva por parte de la autoridad supervisora del país en el cual se brindará dicho servicio; y, que los servicios objeto de contratación en el exterior sean sometidos anualmente a un examen de auditoría independiente, por una empresa auditora de prestigio" (JB-2014-3066, 2014)

El Artículo 21 del título X "De la gestión y administración de riesgo" del capítulo V "De la gestión del riesgo operativo" del libro I "Normas generales para la aplicación de la Ley General de Instituciones del Sistema Financiero" es reestructurado a:

"ARTÍCULO 21.- Con el objeto de gestionar la seguridad de la información para satisfacer las necesidades de la entidad y salvaguardar la información contra el uso, revelación y modificación no autorizados, así como daños y pérdidas, las instituciones controladas deben tener como referencia la serie de estándares ISO/IEC 27000 o la que la sustituya y deben al menos:

(i) *21.1 Determinar funciones y responsables de la implementación y administración de un sistema de gestión de seguridad de la información que cumpla con los criterios de confidencialidad, integridad y disponibilidad, acorde al tamaño y complejidad de los procesos administrados por el negocio; para lo cual las instituciones del sistema financiero podrán conformar un comité de seguridad de la información que se encargue de planificar, coordinar y supervisar el sistema de gestión de seguridad de la información.*

El comité debe estar conformado como mínimo por: el miembro del directorio delegado al comité integral de riesgos, quien lo presidirá, el representante legal de la institución y el funcionario responsable de la seguridad de la información.

El organismo de control puede requerir la creación del comité y de una unidad especializada para la gestión de los sistemas de seguridad de la información en las instituciones del sistema financiero que por su complejidad y volumen de negocio lo requieran, así como en aquellas que

no hubieren puesto en práctica de una manera adecuadas las disposiciones de este sección;" (JB-2014-3066, 2014)

(ii) *"21.2 Establecer las políticas, procesos, procedimientos y metodologías de seguridad de la información definidos bajo estándares de general aceptación que garanticen la ejecución de los criterios de control interno de eficacia, eficiencia y cumplimiento, alineados a los objetivos y actividades de la institución, así como las consecuencias de violación de éstas. Los procesos, procedimientos y metodologías de seguridad de la información deben ser revisados por el comité de seguridad de la información y en caso de no tener dicho comité, por el comité de administración integral de riesgos; y,*

(iii) *21.3Difundir las políticas de seguridad de la información y propiciar actividades de concienciación y entrenamiento en estos temas"* (JB-2014-3066, 2014)

El Artículo 22 del título X "De la gestión y administración de riesgo" del capítulo V "De la gestión del riesgo operativo" del libro I "Normas generales para la aplicación de la Ley General de Instituciones del Sistema Financiero" es reestructurado a:

"ARTÍCULO 22.- Las instituciones deben establecer, implementar, ejecutar, monitorear, mantener y documentar un sistema de gestión de seguridad de la información que considere al menos lo siguiente:

(i) *22.1 Disponer de un inventario de la información con la designación de sus propietarios, mismos que deben tener como mínimo las siguientes responsabilidades:*

a. *22.1.1. Clasificar la información en términos de su valor, requerimientos legales, sensibilidad y criticidad para la entidad, éste debe ser revisado periódicamente con la finalidad de mantenerlo actualizado;*
b. *22.1.2 Definir y revisar periódicamente las restricciones y clasificaciones de acceso tomando en cuenta las políticas de control de acceso aplicables;*
c. *22.1.3 Autorizar los cambios funcionales a las aplicaciones; y,*
d. *22.1.4 Monitorear el cumplimiento de los controles establecidos;"* (JB-2014-3066, 2014)

(ii) *"22.2 Identificar y documentar los requerimientos mínimos de seguridad para cada tipo de información, con base en una evaluación de los riesgos que enfrenta la institución, aplicando la metodología de gestión de riesgo operativo de la entidad; y, con los controles de seguridad de la información;"* (JB-2014-3066, 2014)

(iii) *"22.3 Establecer procedimientos de eliminación de la información crítica de la entidad, de manera segura y considerando los requerimientos legales y regulatorios; Mantener segregación de funciones y responsabilidades para mitigar los riesgos de modificación no autorizada o no intencionada o un mal uso de los activos de la organización;"* (JB-2014-3066, 2014)

(iv) *"22.5 Definir los procedimientos de gestión de cambios en los sistemas de información, hardware y software base, elementos de comunicaciones, entre otros, que consideren su registro, manejo de versiones, segregación de funciones y autorizaciones, e incluyan los cambios emergentes;"* (JB-2014-3066, 2014)

(v) *"22.6 Procedimientos de afectación directa a las bases de datos que permitan identificar los solicitantes, autorizadores, y motivo de la modificación a la información, así como el registro de pistas de auditoría que facilite la trazabilidad del cambio;"* (JB-2014-3066, 2014)

(vi) *"22.7 Determinar los sistemas de control y autenticación tales como: sistemas de detección de intrusos (IDS), sistemas de prevención intrusos (IPS), firewalls, firewall de aplicaciones web (WAF), entre otros, para evitar accesos no autorizados, inclusive de terceros y, ataques externos especialmente a la información crítica;"* (JB-2014-3066, 2014)

(vii) *"22.8 Gestionar la realización de las auditorías de seguridad de la infraestructura tecnológica con base en el perfil de riesgo de la institución, por lo menos una vez al año, con el fin de identificar vulnerabilidades y mitigar los riesgos que podrían afectar a la seguridad de los servicios que se brindan. Los procedimientos de auditoría deben ser ejecutados por personal independiente a la entidad, capacitado y con experiencia, aplicando estándares vigentes y reconocidos a nivel internacional; estas auditorías deben incluir al menos pruebas de vulnerabilidad y penetración a los equipos, dispositivos y medios de comunicación. Las instituciones deben*

definir y ejecutar planes de acción sobre las vulnerabilidades detectadas;" (JB-2014-3066, 2014)

(viii) *"22.9 Controles para detectar y evitar la instalación de software no autorizado o sin la respectiva licencia, así como instalar y actualizar periódicamente aplicaciones de detección y desinfección de virus informáticos y demás software malicioso;"* (JB-2014-3066, 2014)

(ix) *"22.10 Medidas para proteger la información contenida en: documentos, medios de almacenamiento u otros dispositivos externos e intercambio electrónico, contra: robo, utilización o divulgación no autorizada de información para fines contrarios a los intereses de la entidad, por parte de su personal o de terceros;"* (JB-2014-3066, 2014)

(x) *"22.11 Un procedimiento para el control de accesos a la información que considere la concesión; administración de derechos y perfiles para el registro, eliminación y modificación de la información, que garanticen una adecuada segregación de funciones y reduzcan el riesgo de error o fraude; así como la revocación de usuarios;"* (JB-2014-3066, 2014)

(xi) *"22.12 Establecer un procedimiento para el monitoreo periódico de accesos, operaciones privilegiadas, intentos de accesos no autorizados, para asegurar que los usuarios solo estén realizando actividades para las cuales han sido autorizados;"* (JB-2014-3066, 2014)

(xii) *"22.13 Implementar procedimientos que permitan contar con pistas de auditoría a nivel de aplicativos y bases de datos que registren los cambios realizados a la información crítica de la entidad. Los administradores no deben tener permiso para borrar o desactivar las pistas de sus propias actividades"* (JB-2014-3066, 2014)

(xiii) *"22.14 Aplicar técnicas de encriptación sobre la información crítica, confidencial o sensible;"* (JB-2014-3066, 2014)

(xiv) *"22.15 Considerar en la definición de requerimientos para nuevos sistemas o mantenimiento, aquellos relacionados con la seguridad de la información;"* (JB-2014-3066, 2014)

(xv) *"22.16 Establecer procedimientos de gestión de incidentes de seguridad de la información, en los que se considere al menos su registro, priorización, análisis, escalamiento y solución;"* (JB-2014-3066, 2014)

(xvi) *"22.17 Definir y mantener un sistema de registros históricos que permitan verificar el cumplimiento de las políticas, procesos, procedimientos y controles definidos para gestionar la seguridad de la información; y,"* (JB-2014-3066, 2014)

(xvii) *"22.18 Evaluar periódicamente el desempeño del sistema de gestión de la seguridad de la información, a fi n de tomar acciones orientadas a mejorarlo."* (JB-2014-3066, 2014)

En el Artículo 39 del título II "De la organización de las instituciones del sistema financiero privado" del capítulo I "Apertura y cierre de oficinas en el país y en el exterior, de las instituciones financieras privadas y públicas sometidas al control de la Superintendencia de Bancos y Seguros" del libro I "Normas generales para la aplicación de la Ley General de Instituciones del Sistema Financiero":

(i) Artículo 39, numeral 10: *"Cámaras de vigilancia.- Para su operación, cada cajero automático debe contar al menos con dos cámaras de vigilancia en las siguientes ubicaciones:*

a. 39.10.1 Una periférica con vista panorámica de arriba hacia abajo, que permita captar el entorno del equipo; y,

b. 30.10.2 Una cámara frontal que permita captar al usuario."

Si en alguna localización existen cajeros contiguos, las entidades pueden disminuir el número total de cámaras periféricas, con el sustento técnico respectivo. De ninguna manera se pueden disminuir el número de las cámaras frontales.

Las cámaras de vigilancia deben operar de forma ininterrumpida las veinticuatro (24) horas del día.

El funcionamiento de las cámaras debe ser evaluado permanentemente y mantener un registro actualizado de sus niveles de operación, a fin de garantizar la nitidez y fidelidad de las grabaciones realizadas;" (JB-2014-3066, 2014)

(ii) Artículo 39, numeral 11: "*Sistema de grabación de video.- Para su operación, cada cajero automático debe tener un grabador de videos*

exclusivo, mismo que debe registrar la grabación sin degradar la definición capturada por sus cámaras.

Las instituciones del sistema financiero deben mantener un archivo de grabaciones que cubra por lo menos noventa (90) días, mientras que de las transacciones que sean objeto de reclamo, se guardarán hasta que haya una resolución en firme del órgano competente" (JB-2014-3066, 2014)

En la resolución JB-2012.2090 se enfatiza que las entidades financieras deberán poseer una "Póliza de fidelidad bancaria" que garantice el amparo contra fraudes informáticos, por lo que se incluye el artículo 41 en el título II "De la organización de las instituciones del sistema financiero privado", del capítulo I "Apertura y cierre de oficinas en el país y en el exterior, de las instituciones financieras privadas y públicas sometidas al control de la Superintendencia de Bancos y Seguros" del libro I "Normas generales para la aplicación de la Ley General de Instituciones del Sistema Financiero":

"ARTÍCULO 41.- Las instituciones financieras contratarán anualmente con las compañías de seguro privado, coberturas que aseguren a la entidad contra fraudes generados a través de su tecnología de la información, sistemas telemáticos, electrónicos o similares, como mínimo ante los siguientes riesgos:

(i) *41.1 Alteraciones de bases de datos;*
(ii) *41.2 Accesos a los sistemas informáticos y de información de forma ilícita;*
(iii) *41.3 Falsedad informática;*
(iv) *41.4 Estafa informática;*
(v) *41.5 Daño informático; y,*
(vi) *41.6 Destrucción a la infraestructura a las instalaciones físicas necesarias para la transmisión, recepción o procesamiento de información."* (JB-2012-2090, 2012)

5.6 Conclusión

Se ha comprendido que el sistema financiero ecuatoriano está conformado por la Banca privada y pública, cooperativas y mutualistas. Así también, se entiende que el principal organismo de control es el Ministerio de Finanzas y la ley que regula al sistema financiero ecuatoriano es la Ley General de Instituciones del Sistema Financiero. A su vez, existen superintendencias encargadas de velar por las buenas prácticas de cada una de las entidades que pertenezcan al sector financiero ecuatoriano.

En los últimos años, la economía popular y solidaria ha sido implementada y desarrollada a nivel cooperativo con el fin de establecer entidades que cumplan con los siete principios de cooperativismo dando mayor valor al ser humano como sujeto de trabajo. Todo esto se encuentra fundamentado en la constitución ecuatoriana establecida en el 2008 en sus artículos 283, 309 y 311. A su vez, el órgano de control es la Superintendencia de Economía Popular y Solidaria que emite resoluciones en la Ley Orgánica Popular y Solidaria.

Al comparar el desarrollo de disposiciones por parte de la SEPS y de la Superintendencia de Bancos y Seguros, se determina que existe enfoque y desarrollo por parte de la Superintendencia de Bancos y Seguros en los temas de seguridad de la información e infraestructura tecnológica, ya que en la Ley Orgánica Popular y Solidaria no se mencionan estos aspectos, haciendo referencia únicamente a la entrega de información sobre la situación económica y de gestión de la organización. Por otra parte, la Superintendencia de Bancos y Seguros, en las resoluciones de la Junta Bancaria JB-2012-2148, JB-2014-3066 y JB-2012.2090, hace referencia a la implementación de medidas que disminuyan el riesgo por fraudes informáticos, a la continuidad del negocio y mitigar los fraudes relacionados a cajeros automáticos mediante la implementación de la norma ISO/IEC 27000 y a la contratación seguros que prevengan el fraude informático, respectivamente. Bajo este contexto, se considera que estas resoluciones deberían ser implementadas en la Ley Orgánica de Economía Popular y Solidaria.

Conclusiones

El gran crecimiento y desarrollo de la tecnología ha facilitado los procesos y el almacenamiento de la información generada por personas e instituciones, así mismo, han surgido técnicas para sustraer información y cometer delitos o fraudes electrónicos. Para contrarestrar esta situación se ha desarrollado la Seguridad de la Información que es la encargada de proteger toda información que le pertenezca a una organización o entidad o que forme parte de sus procesos.

Se considera que el desarrollo de la Seguridad de la Información en el país se encuentra encaminado pero aún le falta desarrollo para lograr un sistema eficaz y completo que salvaguarde la información que generan tanto las personas como las instituciones y que mitigue el riesgo. Es así que, al comparar al Ecuador con España se nota una gran brecha entre estos dos países. Mientras que, España cuenta con organismos de control, leyes en vigencia y un exahustivo control para la protección de datos, Ecuador está en una etapa de incio y de socialización de las leyes, ya que existe gran desconocimiento de las mismas. A nivel de Latinoamérica, la protección de datos se encuentra amparada en el Hábeas Data, descrito en sus constituciones.

En un nivel más específico, la Seguridad de la Información es un área poco desarrollada en las entidades del sector cooperativo ecuatoriano, a pesar de que las mismas producen, almacenan y gestionan información sensible. Sin embargo, la Superintendencia de Economía Popular y Solidaria, con el objetivo de que las cooperativas de Ahorro y Crédito posean un buen desarrollo, estabilidad, solidez y correcto funcionamiento, se encuentra desarrollando y aplicando medidas para que cada cooperativa implemente una serie de acciones para mitigar el riesgo en cuanto a la seguridad de la información.

Al realizar entrevistas a varios profesionales en el área de Seguridad de la Información y que son empleados de cooperativas de la región, se ha comprobado que el proceso de implementar medidas de control y prevención en cuanto a la Seguridad de la Información se encuentra dando sus primeros pasos y obteniendo grandes resultados. Así mismo, se ha constatado que se comenten delitos por las vulnerabilidades existentes en cuanto a la protección de la información. Estos delitos, en su mayoría, se han presentado por parte de los mismos empleados que han tenido acceso ya sea porque

robaron claves o porque las funciones y perfiles de usuario se encontraban mal distribuidos.

De igual forma, estos profesionales coinciden que las normativas internacionales aplicadas para la seguridad de la Información son la familia de la ISO/IEC 27000. Se evidencia la falta de una normativa local y de un organismo de control específico para la Seguridad de la Información. Así mismo, coinciden que las resoluciones JB-2014-3066 y JB-2012-2148 son las más aptas para las entidades en donde laboran.

Analizando una red local de Cooperativas de Ahorro y Crédito, se puede constatar que una de nueve cooperativas poseen una política de Seguridad de la Información y un manual de buenas prácticas referente al mismo tema. Esto se debe a que por parte de las autoridades no existe el apoyo necesario para la implemetación de normas que garanticen la Seguridad de la Información. Cabe mencionar que son cooperativas de segmento 3, 4 y 5 que no cuentan con los recursos suficientes, por lo que no aplican estas medidas.

El marco jurídico que rige a las cooperativas es la LOEPS (Ley Orgánica de Economía Popular y Solidaria) si bien la misma detalla el comportamiento de las cooperativas, los principios que esta debe cumplir y exige que se presente información constante de su gestión financiera, no existe un artículo formal que exprese como debe ser el comportamiento en cuanto a la Seguridad de la Información. Desde el 2015, la Superintendencia de Economía Popular y Solidaria desarrolla el proyecto Sistema de Gestión de Seguridad de la Información con el fin de asegurar la continuidad de las instituciones, sin embargo, este proyecto se encuentra en una primera etapa de socialización y concientización. Por otro lado, las resoluciones JB-2014-3066, JB-2012-2148 y JB-2012-2090 emitidas por la Junta Bancaria abordan de manera completa las medidas de seguridad para la tecnología de información y comunicaciones, sugiriendo una metodología basada en la norma ISO/IEC 27000 para la continuidad del negocio, y obligando a la contratación de pólizas de seguro que cubran el delito informático y cibercrimen. Bajo este contexto, se ha entendido que dichas resoluciones deben ser incluidas en la LOEPS con el fin de que facilite el conocimiento de la seguridad de la información en el sector cooperativo ecuatoriano.

Una vez descrito el estado del marco legal y analizado el mismo, se detallará un extracto de las leyes que se han considerado las más importantes y oportunas para la Seguridad de la Información en el sector financiero cooperativo ecuatoriano:

La protección de datos se encuentra amparada bajos los artículos 92 y 66 en su numeral 19 de la constitución ecuatoriana en los que se garantiza el derecho de protección de los datos que generen las personas como individuos o como representantes legales de entidades. De igual forma, se encargan de garantizar el derecho de conocer cuál será el tratamiento de la misma, distribución o difusión de los datos con autorización del propietario de la información. En cuanto al comportamiento con datos sensibles, que son el tipo de datos que maneja el sector financiero cooperativo ecuatoriano, el almacenamiento de los mismos debe ser autorizado por la ley o por el propietario y es de vital importancia contar con seguridades necesarias. Si esto no se cumpliera la persona propietaria de la información podría demandar por perjuicios ocasionados ante un juez o jueza.

Es importante destacar que la Economía Popular y Solidaria, que es la que manejan las cooperativas de Ahorro y Crédito, se encuentra amparada en los artículos 283, 309 y 311 de la constitución ecuatoriana, en los que se reconoce al ser humano como sujeto y fin, recalcan que debe existir una relación equilibrada y dinámica entre la sociedad, el Estado y el mercado garantizando el bienestar de la naturaleza. Así mismo, reconoce que las cooperativas de ahorro y crédito pertenecen a esta economía y garantiza un tratamiento diferenciado y preferencial por parte del Estado con el fin de impulsar su economía popular y solidaria.

En el mismo contexto, la Ley Orgánica de Economía Popular y Solidaria reconoce a las cooperativas de ahorro y crédito en su artículo 21 de la sección 3 como una sociedad de personas unidas voluntariamente con el fin de satisfacer sus necesidades económicas, sociales y culturales. Esta sociedad se constituye de manera democrática, con personalidad jurídica de derecho privado e interés social. Las actividades y relaciones establecidas por las cooperativas de ahorro y crédito serán reguladas por esta Ley y a los valores y principios universales del cooperativismo y a las prácticas de Buen Gobierno Corporativo.

Por otra parte, luego del análisis de las resoluciones JB-2012-2148, JB-2014-3066 y JB-2012-2090 se ha considerado que las mismas deberían formar parte del marco legal que garanticen la seguridad de la información en las cooperativas. A continuación se realiza un resumen de los aspectos más relevantes que consideran las mismas:

En la resolución JB-2012-2148 se describen políticas que impidan la clonación de tarjetas, medidas de protección al software e información del cajero automático, medidas de mantenimiento preventivo y correctivo en los cajeros automáticos, políticas de seguridad para el acceso al interior de cajeros automáticos como por ejemplo, cerraduras de alta tecnología que operen con llaves únicas. Así mismo, indica la obligatoriedad de realizar reportes oportunos sobre incidentes de vulnerabilidad en los cajeros automáticos ya sean de tipo software o hardware. (JB-2012-2148, 2012)

Por otra parte, en cuanto a la gestión integral y control de riesgos indica que la información debe ser de calidad, es decir, se deben implementar mecanismos que garanticen la efectividad, eficiencia y confiabilidad de la información y de los recursos que se relacionen con la misma. Así también, describe las medidas de seguridad que deben tomarse en canales electrónicos siendo la más importante la implementación de normas y estándares internacionales para el uso y manejo de canales electrónicos y consumos con tarjetas. Establece procedimientos de monitoreo, garantiza que la información enviada por los clientes debe ser encriptada en todo momento de la transacción. Obliga a que los canales electrónicos cuenten con un software antimalware que protega el software instalado, detecte oportunamente cualquier intento o alteración en el código, configuración o funcionalidad y que emita alarmas oportunas para el bloqueo del canal electrónico y revisión del personal técnico autorizado de la institución. La generación y validación de claves para ejecutar transacciones deberán utilizar un hardware específico y no debe existir el almacenamiento de esta información. (JB-2012-2148, 2012)

Así mismo, ordena implementar un proceso de bloqueo de los canales electrónicos o de las tarjetas cuando se presenten eventos inusuales que pudiesen ser fraudes o por un número de 3 intentos fallidos. Además, estos eventos deberán ser notificados al cliente a través de correo electrónico u otro mecanismo. (JB-2012-2148, 2012)

Una de las disposiciones que se considera de suma importancia es la adecuada asignación de funciones entre el personal que administra, opera, mantiene y en general manipula el sistema usado, ya que se ha evidenciado que por la falta de esta correcta asignación ha generado robos de información. Así mismo, se implementarán procedimientos para impedir que funcionarios de la entidad que no cuenten con la autorización debida tengan acceso a información confidencial de clientes. Se contará con un registro de acceso sobre las consultas realizadas por los funcionarios a la información con su código, sistema utilizado, registro IP, fecha, hora e información consultada. (JB-2012-2148, 2012)

Otro aspecto, es el de mantener un historial de todas las transacciones realizadas por un cliente como un mínimo de 12 meses con el fin de tener constancia de las operaciones realizadas, llevar monitoreo y control de las mismas. (JB-2012-2148, 2012)

En la Resolución JB-2014-3066 se destacan disposiciones que permitan la continuidad del negocio bajo la normativa ISO/IEC 27000 por lo que describe las funciones del responsable de la información, que será la persona encargada de velar por la integridad, confiabilidad y disponibilidad de información. Así mismo, decreta la implementación de un plan de continuidad que garantice la satisfacción del cliente a pesar de eventos inesperados. Especifica el concepto de incidente de tecnología de la información e incidente de seguridad de la información. (JB-2014-3066, 2014)

Dispone la creación de un comité de tecnología que realice las tareas de planificación, coordinación y supervisión de las actividades del área de tecnología. De igual manera, dispone la creación de:

(i) Políticas, procesos, procedimientos y metodologías de tecnología de la información definidos bajo estándares de general aceptación.
(ii) Procedimientos de gestión de incidentes de tecnología de la información
(iii) Inventario de la infraestructura tecnológica
(iv) Procedimientos de respaldo de información periódicos
(v) Procedimientos que establezcan las actividades y responsables de la operación y el uso de las instalaciones de procesamiento de información (JB-2014-3066, 2014)

Así también, dispone establecer un proceso de administración de la continuidad del negocio utilizando la metodología ISO/IEC 27000 realizando:

(i) definición de objetivos, políticas, estrategias, procedimientos, metodología, planes y presupuesto para la administración de la continuidad
(ii) Creación de un comité de continuidad encargado de:
(iii) Monitoreo de la implementación del plan alineado a la metodología.
(iv) Cambios, actualizaciones y mejoras del plan
(v) Revisar el presupuesto del plan
(vi) Seguimiento de potenciales amenazas
(vii) Seguimiento de medidas adoptadas
(viii) Análisis de impacto por la interrupción de procesos
(ix) Análisis de identificación de principales riesgos
(x) Evaluación y selección de estrategias para la continuidad
(xi) Realización de pruebas del plan de continuidad
(xii) Difusión, comunicación, entrenamiento, conciencia y cumplimiento del plan
(xiii) Integración del proceso de administración de continuidad al proceso integral de riesgos. (JB-2014-3066, 2014)

Las disposiciones más relevantes de esta resolución se plantean en el Artículo 21 y 22 en los que se describe la gestión de la seguridad de la información. Por su parte el Artículo 21 establece que con el fin de satisfacer las necesidades de la entidad y salvaguardar la información contra el uso, revelación y modificación no autorizada, así como daños y pérdidas, las instituciones deben al menos:

(i) Determinar funciones y responsables de la implementación y administración de un sistema de gestión de seguridad de la información que cumpla con los criterios de confidencialidad, integridad y disponibilidad, acorde al tamaño y complejidad de los procesos administrados por el negocio
(ii) Establecer las políticas, procesos, procedimientos y metodologías de seguridad de la información.
(iii) Difundir las políticas de seguridad de la información y propiciar actividades de concienciación y entrenamiento en estos temas. (JB-2014-3066, 2014)

Así mismo, el artículo 22 dispone la implementación, ejecución, monitoreo, mantenimiento y documentación de un sistema de gestión de seguridad de la información considerando:

(i) Implementación de un inventario de la información, realizando las siguientes actividades:
   a. Clasificación de la información en términos de su valor, requerimientos legales, sensibilidad y criticidad para la entidad.
   b. Definición y revisión periódica de las restricciones y clasificaciones de acceso.
   c. Autorización de los cambios funcionales a las aplicaciones
   d. Monitorización del cumplimiento de los controles establecidos

(ii) Identificación y documentación de los requerimientos mínimos de seguridad para cada tipo de información aplicando la metodología.

(iii) Establecer procedimientos para eliminar información crítica de forma segura y bajo los requerimientos legales y regulatorios.

(iv) Definir procedimientos de gestión de cambios en los sistemas de información, hardware y software base, elementos de comunicaciones, entre otros.

(v) Procedimientos que permitan identificar los solicitantes, autorizadores, y motivo de la modificación a la información, así como el registro de pistas de auditoría que facilite la trazabilidad del cambio al presentar incidentes en bases de datos.

(vi) Determinar los sistemas de control y autenticación que eviten accesos no autorizados y ataques externos a información crítica.

(vii) Realización de las auditorías de seguridad de la infraestructura tecnológica con base en el perfil de riesgo de la institución, por lo menos una vez al año, con el fin de identificar vulnerabilidades y mitigar los riesgos que podrían afectar a la seguridad de los servicios que se brindan.

(viii) Controles para detectar y evitar la instalación de software no autorizado o sin la respectiva licencia, detección y desinfección de virus informáticos y demás software malicioso

(ix) Medidas para proteger la información contenida en: documentos, medios de almacenamiento u otros dispositivos externos e intercambio electrónico,

contra: robo, utilización o divulgación no autorizada de información para fines contrarios a los intereses de la entidad, por parte de su personal o de terceros

(x) Un procedimiento para el control de accesos a la información que considere la concesión; administración de derechos y perfiles para el registro, eliminación y modificación de la información, que garanticen una adecuada segregación de funciones y reduzcan el riesgo de error o fraude; así como la revocación de usuarios;

(xi) Establecer un procedimiento para el monitoreo periódico de accesos, operaciones privilegiadas, intentos de accesos no autorizados, para asegurar que los usuarios solo estén realizando actividades para las cuales han sido autorizados;

(xii) Implementar procedimientos que permitan contar con pistas de auditoría a nivel de aplicativos y bases de datos que registren los cambios realizados a la información crítica de la entidad. Los administradores no deben tener permiso para borrar o desactivar las pistas de sus propias actividades

(xiii) Aplicar técnicas de encriptación sobre la información crítica, confidencial o sensible

(xiv) Considerar en la definición de requerimientos para nuevos sistemas o mantenimiento, aquellos relacionados con la seguridad de la información;

(xv) Establecer procedimientos de gestión de incidentes de seguridad de la información, en los que se considere al menos su registro, priorización, análisis, escalamiento y solución

(xvi) Definir y mantener un sistema de registros históricos que permitan verificar el cumplimiento de las políticas, procesos, procedimientos y controles definidos para gestionar la seguridad de la información

(xvii) Evaluar periódicamente el desempeño del sistema de gestión de la seguridad de la información, a fi n de tomar acciones orientadas a mejorarlo. (JB-2014-3066, 2014)

En la resolución JB-2012-2090 se obliga a la contratación de un seguro privado que cubra a la entidad contra fraudes generados a nivel de su tecnología de la información, cubriendo los siguientes riesgos:

(i) Alteraciones de bases de datos

(ii) Acceso ilícitos a sistemas informáticos y de información

(iii) Falsedad informática

(iv) Estafa informática

(v) Daño informático

(vi) Destrucción de infraestructura que permita la transmisión, recepción y procesamiento de la información. (JB-2012-2090, 2012)

Referencias

R3D Red en Defensa de los Derechos Digitales. (2016). Los Cinco Ojos, la alianza de espionaje del mundo anglosajón. . *Red en Defensa de Derechos Digitales*.

AEDIT Asociación Ecuatoriana de Derecho Informático y Telecomunicaciones. (2003). *AEDIT.org.* Obtenido de AEDIT.org: http://www.aedit.org.ec/index_archivos/Page398.htm

Aguilera, P. (2010). *Seguridad Informática.* Editorial EDITEX.

AIDP. (2015). *AIDP Asociación Internacional de Derecho Penal* . Obtenido de AIDP Asociación Internacional de Derecho Penal : http://www.penal.org/es/node/167

Ayllón Gutiérrez, J. A. (2014). Aspectos Legales de la Seguridad Informática: Nuevos retos en la tutela de la Propiedad Intelectual. *TFM Aspectos Legales de la Seguridad Informática*.

Carvallo, D. L. (3 de marzo de 2014). Obtenido de http://dlcarballo.com/2014/03/03/presente-y-futuro-de-la-normativa-de-proteccion-de-datos-en-ecuador/

Carvallo, D. L. (2014). Protección de datos y habeas data en la legislación ecuatoriana: presente y futuro. *Tribuna de la Red Iberoamericana de Protección de Datos*.

Castellanos, P. (18 de mayo de 2014). *Comunidad Todo comercio exterior.* Obtenido de Comunidad Todo comercio exterior: http://comunidad.todocomercioexterior.com.ec/profiles/blogs/ley-de-comercio-electr-nico-firma-electr-nica

Chiriboga Rosales, L. A. (2007). *Sistema Financiero.* Quito: Cámara Ecuatoriana del Libro - Núcleo de Pichincha.

Corera, G. (2013). Escándalo de espionaje: qué es el "Club de los cinco ojos". *BBC Mundo*.

Corletti Estrada, A. (2006). Análisis de ISO-27001:2005. *Documento Digital*.

Davara, M. R. (2004). *Anuario del Derecho de las Tecnologías de la Información y las Comunicaciones*, 3.

DDI. (2015). *Departamento de Derechos Intelectuales*. Obtenido de Departamento de Derechos Intelectuales: http://www.propiedadintelectual.cl/623/w3-propertyvalue-40378.html

DE ESPAÑA. (2013). Ley Orgánica 15/1999 de 13 de diciembre, de Protección de datos de Carácter Personal. *BOE num. 298199*.

Delgado, J. A. (2014). Gorbenanza de Internet en Ecuador: Infraestructura y acceso. *Encuentro Nacional de Gobernanza de Internet en Ecuador*.

Díaz, P., Jackson, M., & Motz, R. (2015). Learning Analytics y protección de datos. Recomendaciones. *Anais dos Workshops do Congresso Brasileiro de Informática na Educação, 4*(1), 981.

Freire, J. (3 de octubre de 2015). Ecuador, el cuarto país de la región que recibe más ataques cibernéticos. *EL COMERCIO*.

García, J. (2011). La protección de datos personales . *Revista Judicial derechoecuador.com*.

Gordón, A. (14 de julio de 2016). Ataques cibernéticos crecen en América Latina. *El Comercio*.

IEPI . (2016). *IEPI INSTITUTO ECUATORIANO DE LA PROPIEDAD INTELECTUAL*. Obtenido de IEPI INSTITUTO ECUATORIANO DE LA PROPIEDAD INTELECTUAL: http://www.propiedadintelectual.gob.ec/propiedad-intelectual/

INEN. (2015). *TECNOLOGÍAS DE LA INFORMACIÓN - TÉCNICAS DE SEGURIDAD-CODIGO DE PRÁCTICA PARA LOS CONTROLES DE LA SEGURIDAD DE LA INFORMACIÓN (ISO/IEC 27002:2013 + COR 1:2014 + COR 2:2015, IDT).* Quito.

InfoLEG. (2016). *Información Legislativa y Documental*. Obtenido de Información Legislativa y Documental : http://www.infoleg.gob.ar/

ISACA. (2011). *ISO 31000:2009 Herramienta para evaluar la gestión de riesgos.*

ISO International Standar Organization. (2009). *ISO 31000.* Obtenido de http://www.fecoopse.com/files/iso_31000_-_gestion_de_riesgos_-_espaol.pdf

ISO International Standar Organization. (2016). Obtenido de http://www.iso.org/iso/home/about.htm

ISO Tools Excellence . (2016). *Software ISO Riesgos y Seguridad.*

ISO27000.es. (2012). *ISO 27000.* Obtenido de http://www.iso27000.es/download/doc_iso27000_all.pdf

Jaramillo Albuja, J. P. (2016). Evolución de la Banca Privada Ecuatoriana. *Revista Perspectiva*.

Juste, M. (2015). Ciberdelincuencia: ¿Cuáles serán las principales amenazas en 2016? *Expansión: Economía Digital*.

Juste, M. (2016). Las amenazas de banca móvil, entre los ataques informáticos más extendidos. *Expansión: economía digital*.

LSSI. (2015). *LSSI, Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico.* Obtenido de LSSI, Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico: http://www.lssi.gob.es/la-ley/aspectos-basicos/Paginas/ambito-aplicacion-lssi.aspx

Matalobos Vega, J. M. (2009). Análisis de Riesgos de Seguridad de la Información.

Miño Grijalva, W. (2013). *Historia del Cooperativismo en el Ecuador.* Quito: Editogran S.A.

Morán Carvajal, W. S. (2004). Establecimiento y Estandarización de Procesos y Programas de Auditoría en el Sector Bancario. 12.

NAmestnikov, Y. (2016). *GREAT de Kasperky Lab.*

NovaGob La red de administración pública. (2015). *La red social NovaGob.org*. Obtenido de La red social NovaGob.org: http://www.novagob.org/pages/view/207046/proteccion-de-datos-personales-en-chile

NovaGob La red de administración pública. (2015). *La red Social NovaGob.org*. Obtenido de La red Social NovaGob.org: http://www.novagob.org/pages/view/206966/proteccion-de-datos-personales-en-colombia

NovaGob La red social de administración pública. (2015). *Red Social NovaGob.org*. Obtenido de Red Social NovaGob.org: http://www.novagob.org/pages/view/207061/proteccion-de-datos-personales-en-bolivia

Núñez , J. A. (2007). Importancia de la Protección de Datos de Caracter Personal en las Relaciones Comerciales. Aproximación del Derecho Venezolano. *Derecho Privado*, 12,109.

Nuñez, Á. C. (2013). Conceptos de seguridad informática y su reflejo en la Cámar de Cuentas de Andalucía. *Auditoría pública: revista de los Organos Autónomos de Control Externo*, (61), 111-117.

OCDE. (2016). *OCDE: Mejores políticas para una vida mejor*. Obtenido de OCDE: Mejores políticas para una vida mejor: http://www.oecd.org/centrodemexico/laocde/

OMPI. (2015). *OMPI*. Obtenido de http://www.wipo.int/madrid/es/how_madrid_works.html

OMPI. (2015). *Organismo Mundial de la Protección Intelectual*. Obtenido de Organismo Mundial de la Protección Intelectual: http://www.wipo.int/about-ip/es/

PDP Protección de Datos Personales. (2016). *PDP* . Obtenido de http://www.jus.gob.ar/datos-personales/normativa.aspx

Perez, J. S. (16 de Diciembre de 2008). *Universitat do Valencia.* Obtenido de Universitat do Valencia: http://www.uv.es/selva/guiaempleo/NT_1d.htm

Restrepo Figueroa, A. M. (2015). El documento electrónico como medio de prueba en el procedimiento laboral colombiana.

Romero, B. (2015). *TusFinanzas.ec*. Obtenido de TusFinanzas.ec: http://tusfinanzas.ec/el-rol-de-la-superintendencia-de-bancos-del-ecuador/

Salas, M. P. (2014). ¿Y de qué sirve un país OCDE? . *El DEfinido*.

Seguros, S. d. (Febrero de 2008). *SuperBancos.* Obtenido de SuperBancos : http://www.superbancos.gob.ec/medios/PORTALDOCS/downloads/cultura_financiera/info_0011.pdf

SEPS. (2015). *SEPS, Superintendencia de Economía Popular y Solidaria*. Obtenido de SEPS, Superintendencia de Economía Popular y Solidaria: http://www.seps.gob.ec/interna?-que-es-la-seps-

Solorzano, K. J. (203). El impacto de las nuevas tecnologíasen el derecho de autor: Tratados Internet de la OMPI y la Ley de Propiedad Intelectual Ecuatoriana.

SPUTNIK . (21 de mayo de 2015). *Mundo.SPUTNIKnew*. Obtenido de Mundo.SPUTNIKnew: https://mundo.sputniknews.com/seguridad/201505211037608485/

Tola, D., & Freire, L. (2015). Implementación de un sistema de Gestión de Seguridad de la Información para una empresa de Consultoría y Auditoría, aplicando la Norma ISO/IEC 27001.

Ulloa, S. J. (2015). Seguridad Informática para la red de datos en la Cooperativa de Ahorroy Crédito Unión Popular LTDA. 8.

Constitución política del Ecuador [Const.](2008) Artículo 92.

Constitución política del Ecuador [Const.](2008) Artículo 66

Congreso Nacional de Ecuador. (2002). Artículo 1. [Título Preliminar]. Ley De Comercio Electrónico, Firmas Electrónicas Y Mensajes De Datos 67.

Congreso Nacional de Ecuador. (2002). Artículo 13 [Título II].Capítulo I. Ley De Comercio Electrónico, Firmas Electrónicas Y Mensajes De Datos 67.

Congreso Nacional de Ecuador. (2002). Artículo 14 [Título II].Capítulo I. Ley De Comercio Electrónico, Firmas Electrónicas Y Mensajes De Datos 67.

Congreso Nacional de Ecuador. (2002). Artículo 15 [Título II].Capítulo I. Ley De Comercio Electrónico, Firmas Electrónicas Y Mensajes De Datos 67.

Congreso Nacional de Ecuador. (2002). Artículo 48 [Título III].Capítulo III. Ley De Comercio Electrónico, Firmas Electrónicas Y Mensajes De Datos 67.

Congreso Nacional de Ecuador. (2002). Artículo 49 [Título III].Capítulo III. Ley De Comercio Electrónico, Firmas Electrónicas Y Mensajes De Datos 67.

Congreso Nacional de Ecuador. (2002). Artículo 50[Título III].Capítulo III. Ley De Comercio Electrónico, Firmas Electrónicas Y Mensajes De Datos 67.

Asamblea Nacional. (2011). Artículo 3. [Título I]. Ley Orgánica de la Economía Popular y Solidaria del Sector Financiero Popular Solidario

Congreso Nacional de Ecuador. (1994). Artículo 1. [Título I]. Ley General de Instituciones del Sistema Financiero N.55

Congreso Nacional de Ecuador. (2011). Artículo 3. [Título I].Ley Orgánica de la Economía Popular y Solidaria del Sector Financiero Popular Solidario

Constitución de la República del Ecuador (2008). Artículo 283.

Constitución de la República del Ecuador (2008). Artículo 309.

Junta Bancaria del Ecuador. (2014). Resolución JB-2014-3066

Junta Bancaria del Ecuador. (2014). Resolución JB-2012-2148

Junta Bancaria del Ecuador. (2012). Resolución JB-2012-2090

Asamblea Nacional. (2011). Artículo 3. [Título I]. Ley Orgánica de la Economía Popular y Solidaria del Sector Financiero Popular Solidario

Congreso Nacional de Ecuador. (1994). Artículo 1. [Título I]. Ley General de Instituciones del Sistema Financiero N.55

Congreso Nacional de Ecuador. (2011). Artículo 3. [Título I].Ley Orgánica de la Economía Popular y Solidaria del Sector Financiero Popular Solidario

Constitución de la República del Ecuador (2008). Artículo 283.

Constitución de la República del Ecuador (2008). Artículo 309.

Junta Bancaria del Ecuador. (2014). Resolución JB-2014-3066

Junta Bancaria del Ecuador. (2014). Resolución JB-2012-2148

Junta Bancaria del Ecuador. (2012). Resolución JB-2012-2090

Asamblea Nacional. (2011). Artículo 3. [Título I]. Ley Orgánica de la Economía Popular y Solidaria del Sector Financiero Popular Solidario

Congreso Nacional de Ecuador. (1994). Artículo 1. [Título I]. Ley General de Instituciones del Sistema Financiero N.55

Congreso Nacional de Ecuador. (2011). Artículo 3. [Título I].Ley Orgánica de la Economía Popular y Solidaria del Sector Financiero Popular Solidario

Constitución de la República del Ecuador (2008). Artículo 283.

Constitución de la República del Ecuador (2008). Artículo 309.

Junta Bancaria del Ecuador. (2014). Resolución JB-2014-3066

Junta Bancaria del Ecuador. (2014). Resolución JB-2012-2148

Junta Bancaria del Ecuador. (2012). Resolución JB-2012-2090

Dra. Jenny Ríos Coello, Secretaria de la Facultad de Ciencias de la Administración de la Universidad del Azuay

C E R T I F I C A:

Que el Consejo de Facultad en sesión del 10 de junio de 2016, conoció la petición del estudiante **MARCOS VINICIO CALLE AREVALO** con código 48057, quien presenta su trabajo de titulación denominado **"ENTORNO LEGAL SOBRE SEGURIDAD INFORMATICA DEL SECTOR FINANCIERO COOPERATIVO ECUATORIANO"**, previo a la obtención del título de Ingeniero de Sistemas y Telemática. El Consejo de Facultad acoge el informe de la Junta Académica y aprueba el diseño. Designa como ***Director al ingeniero Esteban Crespo Martínez*** *y como miembros del Tribunal Examinador a los ingenieros Francisco Salgado Arteaga y Diego Astudillo Guillén.* De acuerdo a las disposiciones reglamentarias el peticionario para presentar su trabajo de titulación, tiene un plazo de SEIS MESES, esto es hasta el 10 de diciembre de 2016.

Cuenca, junio 15 de 2016

Dra. Jenny Ríos Coello
Secretaria de la Facultad

CONVOCATORIA

En mi calidad de Decano de la Facultad de Ciencias de la Administración, convoco a los Miembros del Tribunal Examinador, a la sustentación del Protocolo del Trabajo de Titulación: **"LEGISLACIÓN SOBRE SEGURIDAD INFORMÁTICA DEL SECTOR FINANCIERO ECUATORIANO"**, presentado por el estudiante Marcos Vinicio Calle Arévalo con código 48057, previa a la obtención del grado de Ingeniero de Sistemas y Telemática, para el Martes, 24 de mayo de 2016 a las 08h30.

Cuenca, 18 de mayo de 2016

Ing. Xavier Ortega Vásquez
Decano de la Facultad

Ing. Esteban Crespo Martínez .....

Ing. Francisco Salgado Arteaga ..... Francisco Salgado

Ing. Diego Astudillo Guillén .....

Comunicado 20/05/2016 11:27 am

OK

Oficio Nro. 061-2016-DIST-UDA

Cuenca, 10 de Mayo de 2016

Señor Ingeniero
Xavier Ortega Vázquez
DECANO DE LA FACULTAD DE CIENCIAS DE LA ADMNISTRACIÓN
Presente.-

De mis consideraciones:

La Junta Académica de la Escuela de Ingeniería de Sistemas y Telemática, reunida el día 10 de mayo del 2016, recibió el proyecto de tesis titulado "Legislación sobre Seguridad Informática del Sector Financiero Ecuatoriano", presentado por el estudiante Marcos Vinicio Calle Arévalo, estudiante de la Escuela de Ingeniería de Sistemas y Telemática, y revisado por el Ingeniero Esteban Crespo, previo a la obtención del título de Ingeniero de Sistemas y Telemática.

Por lo expuesto, y de conformidad con el Reglamento de Graduación de la Facultad, recomienda como director y responsable de aplicar cualquier modificación al diseño del trabajo de graduación posterior al Ingeniero Esteban Crespo y como miembros del Tribunal a Francisco Salgado Ph.D. e Ingeniero Diego Astudillo. → consultar Jenny

Atentamente,

Ing. Marcos Orellana Cordero
Director Escuela de Ingeniería de Sistemas y Telemática
Universidad del Azuay

UNIVERSIDAD DEL AZUAY

ACTA
SUSTENTACIÓN DE PROTOCOLO/DENUNCIA DEL TRABAJO DE TITULACIÓN

1.1 **Nombre del estudiante:** Marcos Vinicio Calle Arévalo
1.2 **Códigos:** 48057
1.3 **Director sugerido:** Ing. Esteban Crespo Martínez
1.4 **Codirector (opcional):** _____
1.5 **Tribunal:** Ing. Francisco Salgado Arteaga Ing. Diego Astudillo Guillén
1.6 **Título propuesto:** *"LEGISLACIÓN SOBRE SEGURIDAD INFORMÁTICA DEL SECTOR FINANCIERO ECUATORIANO"*
1.7 **Resolución:**

1.7.1 Aceptado sin modificaciones _____

1.7.2 Aceptado con las siguientes modificaciones:

Se acepta totalmente, con el cambio de título a: "Entorno legal sobe seguridad informática del sector financiero cooperativo ecuatoriano".

1.7.3 No aceptado
- Justificación:

_____
_____
_____

Tribunal

Ing. Esteban Crespo Martínez	Ing. Francisco Salgado Arteaga	Ing. Diego Astudillo Guillén
Sr. Marcos Vinicio Calle Arévalo	Dra. Jenny Ríos Coello Secretaria de Facultad	

Fecha de sustentación: Martes, 24 de mayo de 2016 a las 08h30 .

UNIVERSIDAD DEL AZUAY

RÚBRICA PARA LA EVALUACIÓN DEL PROTOCOLO DE TRABAJO DE TITULACIÓN

1.1 **Nombre del estudiante:** Marcos Vinicio Calle Arévalo
1.2 **Códigos:** 48057
1.3 **Director sugerido:** Ing. Esteban Crespo Martínez
1.4 **Codirector (opcional):**
1.5 **Título propuesto:** *"LEGISLACIÓN SOBRE SEGURIDAD INFORMÁTICA DEL SECTOR FINANCIERO ECUATORIANO"*
1.6 **Revisores (tribunal):** Ing. Francisco Salgado Arteaga e Ing. Diego Astudillo Guillén
Recomendaciones generales de la revisión:

	Cumple totalmente	Cumple parcialmente	No cumple	Observaciones (*)
Línea de investigación				
1. ¿El contenido se enmarca en la línea de investigación seleccionada?				
Título Propuesto				
2. ¿Es informativo?				
3. ¿Es conciso?				
Estado del arte				
4. ¿Identifica claramente el contexto histórico, científico, global y regional del tema del trabajo?				
5. ¿Describe la teoría en la que se enmarca el trabajo				
6. ¿Describe los trabajos relacionados más relevantes?				
7. ¿Utiliza citas bibliográficas?				
Problemática y/o pregunta de investigación				
8. ¿Presenta una descripción precisa y clara?				
9. ¿Tiene relevancia profesional y social?				
Hipótesis (opcional)				
10. ¿Se expresa de forma clara?				
11. ¿Es factible de verificación?				
Objetivo general				
12. ¿Concuerda con el problema formulado?				
13. ¿Se encuentra redactado en tiempo verbal infinitivo?				
14. ¿Se encuentra redactado en tiempo verbal infinitivo?				

Objetivos específicos				
15.¿Concuerdan con el objetivo general?				
16.¿Son comprobables cualitativa o cuantitativamente?				
Metodología				
17.¿Se encuentran disponibles los datos y materiales mencionados?				
18.¿Las actividades se presentan siguiendo una secuencia lógica?				
19.¿Las actividades permitirán la consecución de los objetivos específicos planteados?				
20.¿Los datos, materiales y actividades mencionadas son adecuados para resolver el problema formulado?				
Resultados esperados				
21.¿Son relevantes para resolver o contribuir con el problema formulado?				
22.¿Concuerdan 23.con los objetivos específicos?				
24.¿Se detalla la forma de presentación de los resultados?				
25.¿Los resultados esperados son consecuencia, en todos los casos, de las actividades mencionadas?				
Supuestos y riesgos				
26.¿Se mencionan los supuestos y riesgos más relevantes?				
27.¿Es conveniente llevar a cabo el trabajo dado los supuestos y riesgos mencionados?				
Presupuesto				
28.¿El presupuesto es razonable?				
29.¿Se consideran los rubros más relevantes?				
Cronograma				
30.¿Los plazos para las actividades son realistas?				
Referencias				
31.¿Se siguen las recomendaciones de normas internacionales para citar?				
Expresión escrita				
32.¿La redacción es clara y fácilmente comprensible?				
33.¿El texto se encuentra libre de faltas ortográficas?				

(*) Breve justificación, explicación o recomendación.

- Opcional cuando cumple totalmente,
- Obligatorio cuando cumple parcialmente y NO cumple.

.....

.....

.....

Ing. Esteban Crespo Martínez

Ing. Francisco Salgado Arteaga

Ing. Diego Astudillo Guillén

Cuenca, 2 de junio de 2016

Ingeniero

Xavier Ortega Vásquez

DECANO DE LA FACULTAD DE CIENCIAS DE LA ADMINISTRACION

Ciudad.

De mis consideraciones:

Yo, Ing. Esteban Crespo, profesor de la escuela de Sistemas, informo a Ud. que luego de las observaciones emitidas por el tribunal de tesis, he procedido a revisar los ajustes al diseño de tesis presentado por el señor Marcos Vinicio Calle Arévalo, con el tema **"ENTORNO LEGAL SOBRE SEGURIDAD INFORMÁTICA DEL SECTOR FINANCIERO COOPERATIVO ECUATORIANO"** como requisito previo a la obtención del título de Ingeniero en Sistemas y Telemática, sobre el que emito el siguiente informe:

Se han considerado los cambios solicitados por el tribunal examinador, además de mencionar que el proyecto tiene un alcance considerable, en el cual se realizará el estudio del marco legal internacional y nacional en cuanto a seguridad de la información, para luego compararlos, y determinar el grado de madurez del aspecto legal ecuatoriano en cuanto a delito informático, aplicado a las entidades financieras del sector cooperativo.

Por lo expuesto anteriormente, emito informe favorable y recomiendo su aprobación.

Muy atentamente:

Ing. Esteban Crespo, MBA

Cuenca, 10 de mayo de 2016

Ingeniero

Xavier Ortega Vásquez

DECANO DE LA FACULTAD DE CIENCIAS DE LA ADMINISTRACION

Ciudad.

De mis consideraciones:

Yo, Ing. Esteban Crespo, profesor de la escuela de Sistemas, informo a Ud. que he procedido a revisar el diseño de Tesis presentado por el señor Marcos Vinicio Calle Arévalo, con el tema **"LEGISLACIÓN SOBRE SEGURIDAD INFORMÁTICA DEL SECTOR FINANCIERO ECUATORIANO"** como requisito previo a la obtención del título de Ingeniero en Sistemas y Telemática, sobre el que emito el siguiente informe:

El proyecto tiene un alcance considerable, en el cual deberán realizar el estudio del marco legal internacional y nacional en cuanto a seguridad de la información, para luego compararlos, a manera de determinar el grado de madurez del aspecto legal ecuatoriano en cuanto a delito informático.

Por lo expuesto anteriormente, emito informe favorable y recomiendo su aprobación.

Muy atentamente:

Ing. Esteban Crespo, MBA

UNIVERSIDAD DEL AZUAY

Cuenca, 11 de Mayo de 2016

Señor Ingeniero
Xavier Ortega Vásquez
Decano de la Facultad de Ciencias de la Administración
Presente.

De mi consideración:

Yo, Marcos Vinicio Calle Arévalo, estudiante de la carrera de Ingeniería de Sistemas y Telemática, con código 48057, solicito mediante la presente se sirva disponer el trámite para la aprobación del diseño del trabajo de titulación denominado "Legislación sobre Seguridad Informática del Sector Financiero Ecuatoriano", previo a la obtención del título de Ingeniero de Sistemas y Telemática.

Adjunto el diseño correspondiente, que ha sido avalado por el Director propuesto y validado por la Junta Académica de la Escuela.

Con sentimientos de gratitud y estima.

Atentamente,

Marcos Vinicio Calle Arévalo

UNIVERSIDAD DEL AZUAY

DOCTORA JENNY RIOS COELLO SECRETARIA DE LA FACULTAD DE CIENCIAS DE LA ADMINISTRACION DE LA UNIVERSIDAD DEL AZUAY.

C E R T I F I C A :

Que, el señor **Marcos Vinicio Calle Arévalo,** registrado con código 48057 alumno de la Escuela de Ingeniería de Sistemas y Telemática, tiene aprobado más del 80 % de su plan de estudios, le falta aprobar las siguientes materias: Ingeniería de Software II, Calidad de Software, Producción II, Diseño de Trabajo de Graduación para egresar.

Cuenca, Marzo 21 del 2016

UNIVERSIDAD DEL AZUAY
FACULTAD DE ADMINISTRACION SECRETARIA

No. Derecho 045978
rgp.-

Edición autorizada de 30.000 ejemplares
Del 708.501 al 738.500
Nº 0723057

Universidad del Azuay

Facultad de Ciencias de la Administración

Escuela de Sistemas y Telemática

Entorno legal sobre Seguridad Informática del Sector Financiero Cooperativo Ecuatoriano.

Trabajo de graduación previo a la obtención del título de Ingeniero de Sistemas y Telemática

Autor: Marcos Vinicio Calle Arévalo

Director: Ing. Esteban Crespo

Cuenca, Ecuador

2016

UNIVERSIDAD DEL AZUAY

1. Datos generales

1.1 Nombre del estudiante: Calle Arévalo Marcos Vinicio

1.1.1 Código: 48057

1.1.2 Contacto:

Teléfono Convencional: 2870732

Celular: 0993393700

Correo Electrónico: marcos_calle_a@hotmail.com

1.2 Director sugerido: Crespo Martínez, Esteban

Título: Ingeniero en Informática

1.2.1 Contacto: ecrespo@uazuay.edu.ec

1.3 Asesor metodológico: Salgado Arteaga Francisco, PhD

1.4 Tribunal designado:

1.5 Aprobación:

1.6 Línea de Investigación de la carrera:

1.6.1 Código UNESCO 1203.99 "Sistemas de seguridad de la información"

1.6.2 Tipo de trabajo: Proyecto de Investigación

1.7 Área de estudio: Sistemas de seguridad de la Información

1.8 Título propuesto: Entorno legal sobre Seguridad Informática del Sector Financiero Cooperativo Ecuatoriano.

1.9 Estado del proyecto: El proyecto de investigación se concentrará en el análisis del Entorno legal sobre Seguridad Informática del Sector Financiero Cooperativo Ecuatoriano, con el fin de encontrar las leyes más relevantes que faciliten la elaboración de una metodología que se aplique en la gestión de riesgos informáticos del Ecuador.

Edición autorizada de 20.000 ejemplares Del 738.501 al 758.500 Nº 0748016

2. Contenido

2.1 Motivación de la investigación:

La seguridad informática en entidades financieras de ahorro y crédito es importante, debido a que la información que se maneja en este tipo de instituciones es valiosa y delicada. La falta de conocimiento del marco legal que rige actualmente en el Ecuador, ha provocado un sin número de delitos, contribuyendo al enriquecimiento ilícito. Debido a esta situación, es importante conocer el aspecto regulatorio exigido por la Superintendencia de Economía Popular Solidaria, conocido por sus siglas SEPS.

Así también, se convierte en motivación el proyecto de seguridad informática que viene desarrollando la Escuela de Sistemas y Telemática de la Universidad del Azuay. Finalmente, el análisis del marco legal de la seguridad informática permitirá conocer los derechos y deberes que tienen las entidades económicas de ahorro y crédito con el fin de salvaguardar sus bienes informáticos.

2.2 Problemática:

El desarrollo de la tecnología y la aplicación de la misma para la automatización de procesos y el almacenamiento de la información han contribuido, en gran medida, al surgimiento de nuevas técnicas para el robo de la información. Este delito se evidencia en gran medida en las instituciones financieras que se encargan de almacenar, manipular y generar información delicada y valiosa para las personas ya que se manejan cantidades de dinero y de bienes, es por esto que es necesario estudiar las leyes encargadas de la regulación de este problema. En el ámbito nacional estas leyes están presenten pero su desconocimiento es el principal problema como consecuencia se producen delitos que han quedado impunes, por ejemplo, el robo de números de tarjetas de crédito que han provocado fraudes económicos, entre otros. Con estos antecedentes, la evaluación de dicha legislación es de vital importancia y el fundamento de esta investigación.

2.3 Resumen:

La investigación tiene como objetivo estudiar los aspectos legales que regularizan la seguridad informática en el Ecuador aplicados al sector financiero de la economía popular y solidaria. Para realizar el estudio se fundamentará en conceptos de seguridad informática y seguridad de la información, ley orgánica de protección de datos, ley de

propiedad intelectual, leyes relacionadas con servicios de información y finalmente las disposiciones en el sector financiero ecuatoriano. Todas estas legislaciones serán analizadas con el fin de obtener el extracto de las leyes más relevantes para la gestión de riesgos en entidades de ahorro y crédito del Ecuador.

2.4 Indagación exploratoria y base conceptual

En la actualidad, el avance de la tecnología ha facilitado el desarrollo de nuevas formas de producción, consumo y gestión de la información cuyo objetivo es la generación de conocimiento, esto se conoce como la Sociedad de la Información. Así también, ha generado cambios en los métodos de almacenamiento, es decir, se dejó de almacenar en documentos físicos para almacenar en repositorios digitales, como los servidores o la nube.

La información que se almacena puede pertenecer a grandes entidades como a personas, no importa el ámbito en el que se genere puede ser comercial, militar, gubernamental, entre otros. El valor de esta información es muy grande y merece protección, es por esto que la información llega a ser considerada como el activo más importante de una organización. A partir de esta premisa se concluye que es necesario tener métodos que protejan la misma, ya que con el avance de la tecnología se han desarrollado técnicas de ataques para el robo de la información.

Es necesario conocer el concepto de Seguridad Informática, el cual se define como: "la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable" (Lopez, 2010). También se la entiende como cualquier medida que frene las actividades no autorizadas sobre un sistema informático que afecten la confidencialidad, autenticidad o integridad del mismo. (Mantilla Guerra, 2009)

Por otra parte, se conoce como delito informático a las acciones típicas, antijurídicas y culpables que atentan a la integridad, confidencialidad o disponibilidad de la información. (Maldonado Ortega, 2014)

Así también, han surgido normativas cuya función es salvaguardar la información generada por las personas o por las organizaciones. La primera propuesta de controlar los delitos informáticos surgió en Estados Unidos por parte del senador Ribicoff en 1977.

En París, en el año de 1983 la Organización de Cooperación y Desarrollo Económico, conocido por sus siglas como OCDE, integró los delitos informáticos a su legislación penal con el fin de contrarrestar el uso ilícito de programas computacionales. Para el año de 1989, el Consejo de Europa modificó la lista de delitos informáticos adecuándose al nuevo contexto. Finalmente, esta organización definió al delito informático como: "cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisión de datos." (Chungata Cabrera, 2015)

En otro contraste, el Real Decreto 1720/2007 y la Ley orgánica 15 de 1999 en España. (Chaparro Ronderos, 2014) Estados Unidos en 1994 estableció el Acta Federal de Abuso Computacional, en donde modificaba los términos técnicos que ocasionaban ambigüedades. Un extracto del acta es: "...la transmisión de un programa, información, códigos o comandos que causan daño a la computadora, al sistema informático, a las redes, a la información, datos o programas..." (Huilcapi Peñafiel, 2009)

~~A nivel regional, Chile fue el primer país en aprobar una ley de protección a la privacidad de los datos personales. Por otra parte, surge en Colombia la Ley 1581/2012 que protege la información que se almacena de forma digital. (Chaparro Ronderos, 2014)~~

En el entorno nacional es poco el conocimiento que se tiene sobre las leyes que salvaguardan la información digital, y se encuentra dando sus primeros pasos en relación a otros países. En Ecuador dentro de la ley de comercio electrónico, firmas electrónicas y mensajes de datos, existe un artículo de protección de datos en la que se detalla que es necesario el consentimiento expreso del titular de los datos, quien se encargará de seleccionar la información que quiera compartir con terceros. Sin embargo, si los datos son requeridos para el ejercicio de las funciones propias de la administración pública no es necesario el consentimiento del titular. (Ecuador, 2002)

Así también, en esta ley se decreta como infracción informática a la acción en la "...que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica" (Ecuador, 2002)

A través del desarrollo de estas normativas se ha buscado resguardar la información generada por las diferentes entidades que se encuentran en un país, ya sean estas públicas o privadas. Para un análisis concreto se estudiará la presencia de estas leyes en las entidades de ahorro y crédito que existen en la ciudad de Cuenca.

El organismo encargado de supervisar el comportamiento de las entidades de ahorro y crédito en el Ecuador es la Superintendencia de Economía Popular y Solidaria, es por esto que existe las "Normas generales para la aplicación de la Ley General de Instituciones del Sistema Financiero" JB-2014-3066, en donde se detalla el marco legal que rige para la generación, almacenamiento y manipulación de la información que generan las entidades de ahorro y crédito.

2.5 Objetivo general:

Estudiar los aspectos legales que regularizan la seguridad de la información en el Ecuador aplicados al sector financiero de la economía popular y solidaria.

2.6 Objetivos específicos:

- Evaluar los aspectos regulatorios sobre seguridad de la información a nivel local. Además evaluar los aspectos internacionales usando como referencia "Five Eyes", la Organización de Cooperación y Desarrollo Económico (OCDE), y la Asociación de Derecho Penal.
- Realizar un extracto de las leyes más relevantes que debería considerar una metodología para la gestión de riesgos en entidades de ahorro y crédito del Ecuador.

2.7 Metodología:

Para realizar la investigación teórica se utilizará repositorios digitales de Google Académico con el fin de sintetizar los conceptos de seguridad informática. Para la evaluación de la legislación de la seguridad informática se basará en los artículos correspondientes a dicha seguridad y en entrevistas realizadas a profesionales en la rama. Se realizará cuadros comparativos con legislaciones extranjeras y nacionales con el fin de encontrar el extracto de las leyes más importantes para la seguridad informática en el Ecuador en entidades financieras.

2.8 Alcances y resultados esperados:

El alcance de este trabajo será obtener un extracto de las leyes más importantes que deberían ser consideras para la gestión de riesgos en entidades de ahorro y crédito del Ecuador.

2.9 Supuestos y riesgos:

Supuestos	Riesgos	Posible Solución
El desarrollo de la investigación es factible ya que para realizar la indagación existen referencias bibliográficas en las cuales se va a basar la misma. Así también, el acceso a las leyes de la seguridad informática es posible.	La información no sea apta para facilitar el proceso de la investigación.	Recurrir a referencias bibliográficas en inglés.
Cumplir con el plazo establecido para el desarrollo de capítulos.	Presencia de inconvenientes que retrasan a la investigación.	Requerir prórroga para la culminación de la investigación.
Las legislaciones internacionales, regionales y nacionales son de libre acceso.	Existen limitaciones en cuanto al acceso de las legislaciones.	Realizar entrevistas a profesionales que brinden su guía respecto al tema.
El extracto de las leyes más relevantes cumple con los requerimientos del sector de ahorro y crédito.	El análisis no puede realizarse.	Establecer una metodología que pudiese ser adecuada para el caso.

UNIVERSIDAD DEL AZUAY

2.10 Presupuesto:

Rubro-Denominación	Costo USD	Justificación
Proveedor de internet	$150	Con el fin de realizar búsquedas en bibliotecas digitales para asegurar la calidad de la información recopilada para la investigación.
Impresiones	$200	Presentación del documento en formato físico y digital. Trámites dentro de la universidad.
Materiales de Oficina (papel, lápiz)	$20	Registrar ideas referentes al tema.

2.11 Financiamiento:

El estudiante financiará el desarrollo de la investigación.

2.12 Esquema tentativo:

Resumen

Introducción

Objetivos

Justificación

Alcance y Limitaciones

Capítulo I: Fundamentación teórica

1.1 Seguridad de la información y seguridad informática.

1.2 Riesgo

1.3 Ley de protección de datos

1.4 Ley de propiedad intelectual

1.5 Principio de no repudio

1.6 ISO 27001

1.7 ISO 27002

1.8 ISO 27005

Edición autorizada de 20.000 ejemplares
Del 738.501 al 758.500 Nº 0748019

2.13 Cronograma:

Objetivo Específico	Actividad	Resultado esperado	Tiempo (semanas)
Evaluar los aspectos regulatorios sobre seguridad de la información a nivel local.	Indagar sobre conceptos de seguridad informática.	Obtener fuentes bibliográficas valiosas que aporten al desarrollo y estudio de la investigación.	3semanas
	Enumerar los marcos internacionales de la seguridad informática (ISO 27001, 27002, 27005 y 31000).		
	Investigar marcos legales nacionales de la seguridad de la información (Ley de Propiedad Intelectual, Ley Orgánica de Protección de Datos, Leyes relacionadas con servicios de información).		11 semanas
	Analizar el marco legal del sector financiero ecuatoriano correspondiente a la seguridad de la información.		

	Evaluar el marco legal del sector financiero aplicado a las entidades de ahorro y crédito del Ecuador, relacionados con la seguridad de la información (JB-2014-3066 / JB-2014-2148)		3 semanas
Realizar un extracto de las leyes más relevantes que debería considerar una metodología para la gestión de riesgos en entidades de ahorro y crédito del Ecuador.	Entrevistar a profesionales en la seguridad de la información con su experiencia laboral.	Obtener extracto de las leyes más importantes para las entidades de ahorro y crédito del Ecuador.	
	Seleccionar las leyes más adecuadas para el sector de entidades de ahorro y crédito del Ecuador.		4 semanas
	Elaborar el extracto con las leyes más apropiadas para el sector de ahorro y crédito del Ecuador.		

UNIVERSIDAD DEL AZUAY

2.14 Referencias

Chaparro Ronderos, M. F. (2014). Legislación informática y protección de datos en Colombia, comparada con otros países. Revista Inventum, 17.

Chen Mok, S. (2010). Privacidad y protección de datos: un análisis de legislación comparada. . Diálogos Revista Electrónica de Historia, 11(1), 111-152.

Chungata Cabrera, A. M. (2015). El fraude como delito informático. 19.

Ecuador. (2002). Ley de comercio electrónico, firmas electrónicas y mensajes de datos. Corporación de Estudios y Publicaciones.

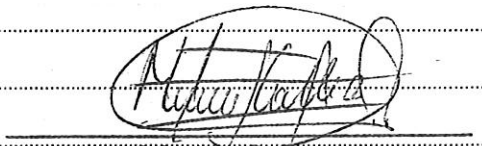
Huilcapi Peñafiel, A. O. (2009). El Delito Informático. Revista Judicial. La Hora.

Lopez, P. A. (2010). Seguridad Informática. Editex.

Maldonado Ortega, M. d. (2014). El delito informático, vulnera el principio de la garantía constitucional y legal, sobre el honor de las personas establecidos en la constitución de la república.

Mantilla Guerra, A. R. (2009). Diseño de un sistema de gestión de seguridad de la información para Cooperativas de Ahorro y Crédito en base a la norma ISO 27001.

2.15 Firma de responsabilidad del alumno



Marcos Calle

2.16 Firma de responsabilidad del director

Ing. Esteban Crespo

2.17 Fecha de entrega: 01/06/2016

Edición autorizada de 20.000 ejemplares Del 738.501 al 758.500 Nº 0748021