CIBERSEGURIDAD EN COSTA RICA

CAPÍTULO 10

Roberto Lemaítre Picado

El objetivo de este capítulo es describir y establecer la situación de la ciberseguridad en Costa Rica. Incluye ocho secciones, las primeras tres brindan el contexto de la ciberseguridad, lo que se comprende por ciberespacio, ciberseguridad y las amenazas informáticas.

En la sección cuatro se describe el marco internacional de la ciberseguridad se conocerán las diferentes instancias mundiales donde el país es miembro y los acuerdos que existen en torno a este tema.

La quinta sección presenta y analiza el marco regulatorio de la ciberseguridad a nivel nacional, tanto leyes, decretos ejecutivos. En la sección seis se ofrece un aspecto fundamental, la opinión de los entes estatales involucrados en el tema como lo son: Banco Central, Poder Judicial en la Sección de Delitos Informáticos, la Superintendencia de Telecomunicaciones (Sutel) Ministerio de Ciencia y Tecnología con las direcciones de Firma Digital y el Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR), la Agencia de Protección de Datos (Prodhab) y Gobierno Digital por medio de la dirección de la Secretaría Digital.

En la sección siete se analiza la ciberseguridad en los sistemas en la nube describiendo sus conceptos, aspectos normativos y examinando los riesgos jurídico-informáticos que se vislumbran con esta modalidad de servicio en el país. En la sección ocho se plasman los resultados relevantes de las encuestas realizadas sobre la ciberseguridad a las empresas, realizada por el Prosic, en el mes de diciembre del 2012. La novena y última sección se ocupa de las principales conclusiones del estudio.

El momento que vive el país, en que la tecnología de la computación ha penetrado todos los ámbitos de la Sociedad de la Información o Cibersociedad, que entendida como un desarrollo social caracterizado por la capacidad de sus miembros para obtener y compartir cualquier información, instantáneamente, desde cualquier lugar y en la forma que se prefiera (Joyanes Aguilar, 2006). En esta nueva realidad surgen interrogantes acerca de la seguridad de dicha información, de los equipos tecnológicos de cada ciudadano y empresa, de los aspectos jurídicos que respaldan para denunciar situaciones anómalas que ocurran en el ciberespacio y cuáles son las instituciones que trabajan en pro de la seguridad cibernética del país. Estos aspectos hacen que se torne fundamental conocer el estado de la ciberseguridad. Para comprender la Ciberseguridad resulta necesario entender el "ecosistema" donde se desarrollan los delitos informáticos.

10.1 ¿QUÉ ES EL CIBERESPACIO?

El término ciberespacio se hace más común dentro del vocabulario actual, pero muchas veces no se puede definir. El vocablo fue desarrollado por primera vez por William Gibson, quien lo define como el "espacio libre donde nos movemos a través de las redes de telecomunicaciones" (Joyanes Aguilar, 2006), este espacio libre de movimiento en redes encuentra su máxima expresión en la red de redes: Internet. Tal situación hace que no se pueda determinar un centro, debido a su estructura técnica desde el origen de Internet, remontándonos a los años 60, en el Departamento de Defensa de los Estados

Unidos, específicamente en la Agencia de Proyectos de Investigación Avanzada (Advanced Research Project Agency, ARPA).

De igual forma este ciberespacio trabaja en lo que se denomina redes informáticas, según Lemaître (2011, págs. 50-60) podemos encontrar:

Redes de área local: *Las redes de área local, son las que se conocen como redes LANs (local area network), estas tienen la característica de ser de propiedad privada, esta se encuentra en un sólo edificio o en un área de pocos kilómetros de longitud.*

Redes de área metropolitana: *Una red de área metropolitana, MAN (Metropolitan Area Network), es una red que abarca una ciudad.*

Redes de Área Amplia: *Las redes de área amplia, WAN (Wide Area Network), abarcan una gran área geográfica, con frecuencia un país o un continente (Tanenbaum, 2003).*

Redes Inalámbricas: *Las redes inalámbricas (wireless network), son las que su medio de transmisión es no guiado y la estructura de la red, se realiza por medio de antenas incorporadas en los equipos para la emisión y recepción de los datos.*

Ahora bien, desde el punto de vista jurídico, el ciberespacio es el área donde se desarrollen muchos de los delitos informáticos que se efectúan actualmente, en él es donde se realiza la recolecta de la evidencia digital, junto al proceso de investigación judicial y de informática forense que se realiza para buscar los responsables de las posibles acciones delictuales.

10.2 ¿QUÉ ES LA CIBERSEGURIDAD?

Se debe comprender la ciberseguridad como la seguridad informática. La Unión Internacional de Telecomunicaciones en su recomendación UIT-TX 1205 define el concepto de ciberseguridad como…

> *(...) el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/ aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno* (Unión Internacional de Telecomunicaciones).

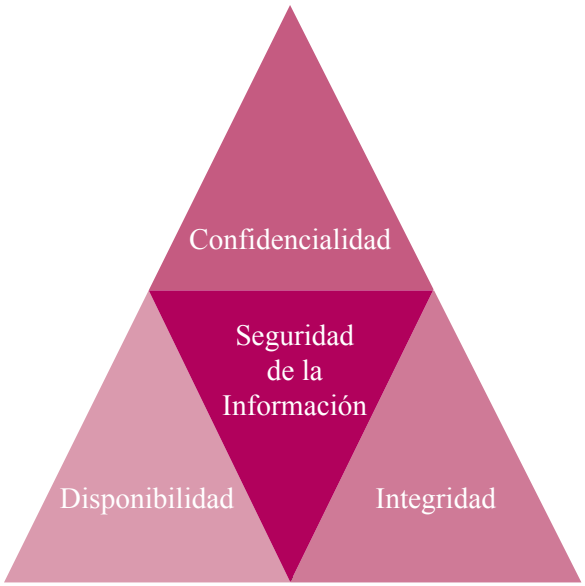
La ciberseguridad tanto de instituciones públicas como empresas privadas requiere basarse en dos aspectos: la protección de bienes, activos, servicios y la responsabilidad compartida con otros Estados, utilizando organismos en que las partes sean partícipes o por medio de acuerdos o tratados internacionales sobre la ciberseguridad.

Como se podrá notar al existir una Cibersociedad global enmarcada en el ciberespacio donde las fronteras se han eliminado, la dificultad de establecer una ciberseguridad efectiva no puede basarse solamente en un Estado, debe ser un trabajo global y coordinado; siendo necesario un constante análisis y gestión de los riesgos de la seguridad informática.

Desde el punto de vista técnico la ciberseguridad va a buscar tres aspectos: confidencialidad, integridad y disponibilidad. Debe existir en la seguridad informática un balance adecuado de estos tres aspectos, y tener presente que nada puede ser 100% seguro, se debe adecuar al contexto de cada institución y empresa realizando un análisis del riesgo, (ver figura 10.1).

Figura 10.1

Triángulo de la Seguridad de la Información



Fuente: Elaboración propia. Prosic, 2012.

Los organismos nacionales miembros de ISO o IEC (la Organización Internacional para la Estandarización y la Comisión Electrotécnica Internacional, respectivamente) participan en el desarrollo de estándares internacionales a través de comités técnicos establecidos por la organización respectiva para trabajar campos particulares de la actividad técnica; este estándar internacional ha sido preparado para proporcionar un modelo con el fin de establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).

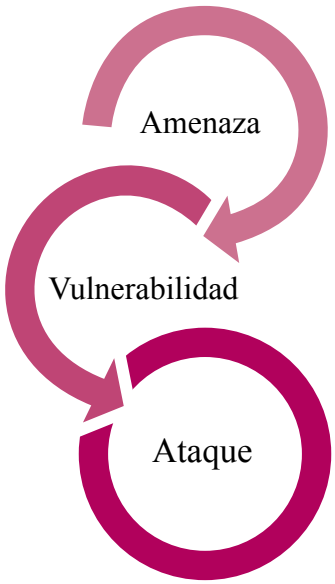
10.3 ¿QUÉ SON LAS AMENAZAS INFORMÁTICAS?

Las amenazas en general podemos definirlas como "*cualquier ocurrencia potencial, maliciosa o no que pueda tener un efecto indeseable en los recursos de una organización"* (Barrantes Sliesarieva, 2010, pág. 42). Siempre las amenazas van relacionadas con las vulnerabilidades, siendo estas las que dentro de un sistema potencian que el ataque se concrete. En este hilo de relación el atraco informático aprovecha esta vulnerabilidad para realizar la ofensiva. (Ver Figura 10.2). Se establecen tres tipos de amenazas (Barrantes Sliesarieva, 2010, págs. 43-44):

- **La revelación de información:** *se refiere a la amenaza de un ente que no cuenta con autorización para el acceso a ciertos recursos.*

Figura 10.2

Relación Amenaza, Vulnerabilidad y Ataque



Fuente: Elaboración propia. Prosic, 2012.

- **La denegación de servicio, o repudio**: *corresponde a los entes que sí cuentan con autorización de acceso a los recursos no consigan entrar (esto es, sean repudiados a la entrada).*

- **La corrupción de la integridad:** *se trata del acceso directo a los recursos, comprende muchos aspectos, más allá de la definición de daño, pérdida o inserción de información falsa. Es la más agresiva.*

Ejemplos de amenazas tenemos el robo y publicación de información clasificada o sensible, el robo y publicación de datos personales, el robo de identidad digital, el fraude, los ataques contra infraestructuras críticas, contra las redes y sistemas, contra servicios de Internet, contra sistemas de control y redes industriales, además infección con malware y ataques contra redes, sistemas o servicios a través de terceros.

Entre los más comunes tenemos las infecciones con malware, esta palabra es un acrónimo en inglés: malicious y software, por tanto establecemos que va a ser cualquier software (programa informático) que sea malicioso. Los malware y las amenazas informáticas se van a clasificar en:

- **Adware:** este va a ser un programa malicioso, cuya función es descargar o mostrar anuncios publicitarios en la pantalla del usuario infectado.

- **Botnets:** es una red de equipos infectados por códigos maliciosos, son controlados por un atacante, logrando de esta manera disponer los recursos informáticos de estos equipos para que trabajen y realicen ataques de forma conjunta.

- **Gusanos:** este tipo de malware pueden reproducirse utilizando diferentes medios de comunicación como las redes locales o el correo electrónico, busca infectar la mayor cantidad de equipos, transportar otros tipos de malware, y agotar los recursos del sistema mientras intenta distribuirse e infectar más equipos.

- **Hoax:** este es un correo electrónico distribuido como cadena, buscando hacer creer que lo que señala es real a pesar de ser falso.

- **Phishing:** La base de este malware es el robo de información personal del usuario, a través de la falsificación de un ente de confianza, donde la persona cree ingresar los datos a un sitio verdadero, pero en su lugar son enviados a la persona atacante.

- **Ransomware:** Es un código malicioso que encripta la información del ordenador, el usuario para obtener la contraseña que libera la información, debe pagar al atacante una suma de dinero.

- **Rogue:** simula ser una aplicación anti-malware, pero en realidad lo que hace es instalar un programa malware.

- **Rootkit:** son herramientas diseñadas para mantener en forma el control de una computadora sin que el usuario se entere.

- **Scam:** son estafas a través de medios tecnológicos, provocando un perjuicio patrimonial a alguien mediante engaño y con ánimo de lucro.

- **Spam:** es un correo no solicitado que se envía masivamente a los usuarios, también conocido como correo no deseado o correo basura.

- **Spyware:** son programas espías que recopilan información del usuario sin que éste se entere.

- **Troyanos:** son archivos que simulan ser normales para lograr hacer que los usuarios los ejecuten de manera confiada y así instalarse en el sistema.

- **Virus:** es un programa informático creado para producir algún daño en el ordenador, tiene la capacidad de reproducirse por sí mismo.

10.4 MARCO INTERNACIONAL DE LA CIBERSEGURIDAD

10.4.1 Unión Internacional de las Telecomunicaciones

Fundada en 1865, la UIT es la agencia especializada de la Organización de las Naciones Unidas para tecnologías de la información y la comunicación,

organizando principalmente foros mundiales. Dentro de su misión encontramos la creación de estándares técnicos, promoción y coordinación de una correcta distribución del espectro radioeléctrico, así como brindar asistencia técnica y promover la creación de capacidades en países en desarrollo.

La ITU ha formado parte de los procesos internacionales de regulación de la ciberseguridad desde larga data, toma un rol activo en el tema desde el año 2007 cuando lanza la llamada "Global Cybersecurity Agenda" (GCA), la cual se plantea como "un marco global para el diálogo y la cooperación internacional para coordinar la respuesta internacional a los crecientes desafíos a la ciberseguridad y para fomentar la confianza y la seguridad en la sociedad de la información." (International Telecommunications Union, 2007).

Con miras al cumplimiento de sus objetivos, en el año 2009 la UIT publicó un documento titulado "ITU Toolkit for Cybercrime Legislation" (International Telecommunications Union, 2009), que brinda a los países un ejemplo de marco legislativo y materiales de referencia que les asistan en la creación de leyes y reglas procedimentales harmónicas. El desarrollo de éste se basó en un análisis comprensivo de las leyes de naciones desarrolladas así como de la Convención sobre el Cibercrimen del Consejo de Europa.

La UIT también ha dictado varias resoluciones relacionadas con la ciberseguridad, a saber:

- Resolución 130 de la Conferencia Plenipotenciaria de la UIT dada el año 2006 en Antalya, Turquía titulada "Reforzando el rol de la UIT en la creación de confianza y seguridad en el uso de las tecnologías de la información y comunicación" (International Telecommunications Union, 2006).
- Resoluciones de la Asamblea Mundial de Estandarización de Telecomunicaciones dadas en Johannesburgo en el año 2008:
    - Resolución 50 sobre "Ciberseguridad" (International Telecommunications Union, 2008).
    - Resolución 52 sobre "Lucha contra el Spam" International Telecommunications Union, 2008.
    - Resolución 58 sobre "Los incentivos para la creación de equipos nacionales de respuesta a incidentes, particularmente para países en desarrollo" (International Telecommunications Union, 2008).
- Resoluciones de la Conferencia Mundial de Desarrollo de las Telecomunicaciones realizadas en Hyderabad.
    - Resolución 45 titulada "Mecanismos para mejorar la cooperación en ciberseguridad, incluyendo la lucha contra el spam" (International Telecommunications Union, 2010).
    - Resolución 69 titulada "Creación de equipos nacionales de respuesta a incidentes informáticos, particularmente para países en desarrollo y la cooperación entre ellos" (International Telecommunications Union, 2010).
- Resoluciones de la Conferencia Plenipotenciaria de la UIT en la Cumbre Mundial sobre la Sociedad de la Información realizada en Guadalajara en el 2010:
    - Resolución 130 titulada "Reforzando el rol de la UIT en la creación de confianza y seguridad en el uso de tecnologías de información y comunicación" (International Telecommunications Union, 2010).
    - Resolución 179 titulada "El rol de la UIT en la protección en línea de los niños" (International Telecommunications Union, 2010).
    - Resolución 181 titulada "Definiciones y terminología relacionada con la construcción de confianza y seguridad en uso de tecnologías de información y comunicación" (International Telecommunications Union, 2010).

Cabe resaltar también las labores que en Ciberseguridad ha realizado el sector de estandarización de las telecomunicaciones de la UIT (ITU-T), el cual ataca los riesgos informáticos mediante la normalización y la emisión de recomendaciones.

Debido a que nuestro país se encuentra suscrito a la UIT, sus resoluciones deberían ser tomadas en cuenta (según la Ley) por nuestros legisladores al formular normativa relativa al tema, además los entes encargados de la ciberseguridad de nuestro país, y especialmente para los diversos actores del sector Telecomunicaciones deben tomarlas en consideración para el desarrollo de las políticas de ciberseguridad.

10.4.2 Organización de las Naciones Unidas

La Organización de las Naciones Unidas, fundada en 1945, con miras a la eliminación de la guerra entre países y proveer una plataforma para el diálogo y cuyos objetivos giran en torno a la cooperación en derecho internacional, el desarrollo económico, el progreso social, los derechos humanos, la seguridad internacional y la búsqueda de la paz mundial se caracteriza también por su relación con la regulación internacional de la ciberseguridad.

La Asamblea General, ente deliberativo principal de la ONU, se configura también como foro internacional para la discusión y adopción de resoluciones relacionadas con el ciberespacio, así como con la creación de conciencia internacional en materia de ciberseguridad, lo cual realiza por lo general por medio de la emisión de Resoluciones, las cuales poseen carácter no vinculante (con la excepción de algunas de las Resoluciones emitidas por el Consejo de Seguridad) y pueden ser comprendidas como recomendaciones, meramente dirigidas a manifestar acuerdos relativos a los objetivos que deberían ser perseguidos por los países miembros a nivel interno.

Algunas de las resoluciones más relevantes emitidas por la Asamblea General que se relacionan con la ciberseguridad son las siguientes:

- Resoluciones A/RES/53/70 del 4 de diciembre del 1998; A/RES/54/49 del 1 de diciembre de 1999; A/RES/55/28 del 20 de noviembre de 2000; A/RES/57/53 del 22 de noviembre de 2002; A/RES/63/37 del 2 de diciembre de 2008; A/RES/66/24 del 2 de diciembre de 2011; todas las cuales se refieren a "Desarrollos en el sector de la información y las telecomunicaciones en el contexto de la seguridad internacional" (Organización de las Naciones Unidas, 2011) .

- Resoluciones A/RES/55/63 del 4 de diciembre de 2000 y A/RES/56/121 del 23 de enero del 2002, las cuales hacen referencia al "Establecimiento de bases legales para combatir el mal uso criminal de las tecnologías de la información", así como al "Combate al mal uso criminal de la tecnología de la información" (Organización de las Naciones Unidas, 2002)

- Resolución A/RES/ 57/239 del 20 de diciembre de 2002, que hace referencia a la "Creación de una cultura global de ciberseguridad" (Organización de las Naciones Unidas, 2002), la cual en su anexo establece los elementos necesarios para lograr tal fin e invita a las organizaciones internacionales a tomar en cuenta tales elementos.

- Resolución A/RES/58/199 del 30 de enero de 2004 hace referencia a la "Creación de una cultura global de ciberseguridad y la protección de infraestructuras de información críticas" (Organización de las Naciones Unidas, 2004), la cual en su anexo establece los elementos para proteger tales infraestructuras e invita a las organizaciones internacionales a tomar en cuenta tales elementos.

La "Oficina sobre Drogas y Crimen" se constituye como foros adicionales donde se discuten los nuevos enfoques a utilizarse para tratar temas de trascendencia internacional, como el cibercrimen. Dentro de esta oficina la "Comisión de Prevención del Crimen y Justicia Criminal", en su doceavo congreso de prevención del crimen y Justicia Criminal celebrado en Brasil en el año 2010 culminó

con la adopción de la "Declaración de Salvador" (UNODC, 2012), en la cual se hace un llamado a los estados miembros a adaptar sus sistemas de justicia criminal a un mundo cambiante" y en su artículo 42, hace un llamado a la conformación de un grupo de expertos internacionales que analicen el problema de la ciberseguridad con miras a facilitar tal adaptación.

Costa Rica es uno de los estados fundadores de tal organización y ha formado parte de su "Consejo de Seguridad" a lo largo de tres períodos, por lo que las resoluciones y declaraciones anteriormente mencionadas deberían, en principio, ser tomadas en consideración al definir las políticas de ciberseguridad nacionales.

10.4.3 Organización de Estados Americanos

La Organización de Estados Americanos es una organización intergubernamental compuesta por 34 naciones independientes del Caribe, así como de Norte, Centro y Sur América, dentro de las cuales se encuentra nuestro país.

La OEA contempla dentro de los fines establecidos, el reforzamiento de la paz y seguridad del continente, para lo cual la Comisión de Seguridad Hemisférica del Consejo Permanente de la Organización de los Estados Americanos ha buscado, crear ámbitos de discusión sobre temas de seguridad en la forma de conferencias tales como la Conferencia Especial sobre Seguridad realizada en Ciudad de México en el año 2003, en la cual se adopta la "Declaración sobre seguridad en las Américas", en la cual se reconocen los ataques a la seguridad cibernética como amenazas a la seguridad de los Estados del Hemisferio (Organización de los Estados Americanos, 2003).

Asimismo, en 2004 los países de la OEA adoptaron la resolución AG/RES.2004 (XXXIV-O/04) titulada: "Estrategia Comprehensiva Interamericana para la Ciberseguridad" (Organización de Estados Americanos, 2004), en la cual se identifica la importancia de la ciberseguridad y requiere la acción conjunta de tres entidades de la OEA para dirigir aspectos tales como la creación de "Equipos de respuesta a incidentes de seguridad informática" (Csirt por sus siglas en inglés) por parte del "Comité contra el Terrorismo" y la evaluación por parte de la Comisión Interamericana de Telecomunicaciones (Citel) de los estándares técnicos actualmente vigentes.

La estrategia dirige la acción conjunta de los Ministros de Justicia de las Américas a través del grupo de expertos gubernamentales en cibercrimen para proveer asistencia a los estados miembros en la redacción y aplicación de leyes efectivas contra los delitos informáticos.

Especial mención merece la "Convención Interamericana sobre Asistencia Mutua en Materia Penal", conocida como "Convención de Nassau" (Asamblea Legislativa de la República de Costa Rica, 2011), adoptada por los estados miembros de la OEA en Nassau, Bahamas, el 23 de mayo de 1993 y entró en vigor el 14 de abril de 1996. Esta fue firmada por nuestro país el 08 de marzo de 2002, ratificada por la Asamblea Legislativa el 03 de enero del 2012 y depositada ante la Secretaría General de la OEA el 14 de marzo de 2012.

Asegura el compromiso de los estados partes prestar "asistencia mutua en investigaciones, juicios y actuaciones en materia penal" (Asamblea Legislativa de la República de Costa Rica, 2011), comprende la remisión de "documentos, informes, información y elementos de prueba" (Asamblea Legislativa de la República de Costa Rica, 2011), incluyendo dentro de tal información tanto documentos e información de carácter público como privado.

Esta Convención ha tomado gran relevancia para nuestro país en tanto se ha constituido en la principal herramienta con la que cuenta nuestro sistema de justicia para recabar información en crímenes informáticos, esto debido a la naturaleza usualmente transfronteriza de los mismos, y si bien no extiende de manera alguna la jurisdicción de nuestro país, ha sido de suma utilidad para la "Oficina de Asesoría Técnica y Relaciones Internacionales de la Fiscalía General de la República", ente encargado de su aplicación.

10.4.4 Unión Europea

La Unión Europea es una comunidad política y económica con características supranacionales e intergubernamentales, compuesta por veintisiete estados miembros, la base de su marco legal fue establecida en 1993 por medio del tratado

de Maastricht (Comunidad Europea, 1992). Su cuerpo ejecutivo, llamado "Comisión Europea" es responsable del desarrollo e implementación del cuerpo legal Europeo, así como actividades relacionadas con la ciberseguridad dirigidas a la preparación y prevención, detección y respuesta, mitigación, recuperación y cooperación internacional.

A la fecha no existen en Europa Directivas Europeas que versen específicamente sobre ciberseguridad, pero cuenta con Directivas sobre temas relacionados, como la "Protección de Datos" (Directiva 95/46/EC), la "Retención de Datos" (Directiva 2006/24/EC), la "Privacidad y Comunicaciones Electrónicas" (Directiva 2002/58/EC), la "Responsabilidad del ISP" (*2000/31/EC)*, los "Servicios de la sociedad de la información" (Directiva 2006/123/EC), y la "Protección a la infraestructura crítica" (Directiva 2008/114/EC).

En tanto el mayor problema relacionado con las Directivas Europeas antes mencionadas es su total enfoque en el mercado común y no implican un efecto directo en asuntos de seguridad nacional, resultaría difícil considerarlas parte fundamental de la regulación internacional relacionada con la ciberseguridad, no obstante lo cual, varias reformas y nuevas propuestas están siendo generadas actualmente por la Comisión Europea para atacar por esta vía el problema (Comisión Europea, 2012).

El "Consejo de Europa", es una organización con carácter consultativo que actúa como foro para el estudio de una amplia gama de problemas tales como la integración de inmigrantes, la amenaza a la vida privada que implica la tecnología, el terrorismo, las actividades criminales y la ciberseguridad.

Sobre este tema el principal logro del Consejo de Europa corresponde a la adopción, en el 2001 de la "Convención sobre el Cibercrimen" (Consejo de Europa, 2001), conocida como el "Convenio de Budapest", entró en vigencia en el año 2004 y posee la particularidad de estar abierta a su ratificación tanto por parte de estados miembros como no miembros.

El Convenio de Budapest trata el acceso ilegal, la intercepción ilegal, la interferencia de datos, la interferencia de sistemas, el mal uso de dispositivos, la falsificación informática, el fraude informático, las ofensas relacionadas con pornografía infantil y las ofensas relacionadas con violación de propiedad intelectual y derechos conexos y contempla aspectos tan importantes como la territorialidad[180], la protección de la información y la protección del funcionamiento de un sistema informático. (Salas Ruiz, 2010)

Por otro lado, el Consejo de Europa utilizó[181] también como herramientas para el combate de la ciberdelincuencia las llamadas "Decisiones Marco" (Framework Decision), las cuales fueron utilizadas exclusivamente dentro de las competencias de cooperación policial y judicial europeas, dos de las más relevantes fueron la 2002/475/JHA del 13 de junio de 2002 relativa al combate al terrorismo y la 2005/222/JHA del 24 de febrero de 2005 sobre ataques a sistemas informáticos.

El impacto directo del marco Europeo en materia de ciberseguridad se ha visto gravemente limitado en nuestro país por la falta de voluntad política y legislativa, la cual ha rezagado nuestra integración dentro de los países miembros del Convenio de Budapest. Cabe resaltar que nuestro país recientemente ha tomado pasos hacia la adhesión a tal convenio mediante la publicación del proyecto de ley N. º 18484 "Aprobación de la adhesión al convenio sobre la ciberdelincuencia", la cual se dio el viernes 24 de agosto de 2012.

10.4.5 Estados Unidos de América

En los últimos años el tema de la ciberseguridad y la ciberdefensa ha adquirido un nivel de atención inusitado en los Estados Unidos de América. Pese a contar con un panorama diverso de Leyes Federales relacionadas con Ciberseguridad, (vigentes y relevantes para el tema leyes tan antiguas como la Posse Comitatus Act

180 Capacidad de un país que haya suscrito el Convenio y haya sufrido un crimen, de perseguir el caso en cualquier otro país suscriptor, extendiendo efectivamente su jurisdicción.

181 Fueron abolidas como figura legislativa con la ratificación del tratado de Lisboa, el cual entró en vigencia el 01 de diciembre de 2009 y actualmente se encuentran en un período de transición que culmina en el año de 2014, cuando el Parlamento Europeo adquiera de manera definitiva mayores funciones legislativas.

de 1879 (Fischer, 2012)), un estudio del sistema actual Estadounidense debe dar inicio en el año 2000, cuando la Casa Blanca emite su "Plan nacional para la protección de sistemas de información", el cual constituyó el primer esfuerzo gubernamental de crear una estrategia nacional de ciberseguridad y ciberdefensa (Oficina ejecutiva del Presidente de los Estados Unidos de América, 2000).

A raíz de los atentados terroristas del 11 de septiembre de 2001, es aprobada la "Uniting and Strenghtening America by Providing Appropiate Tools to Intercept and Obstruct Terrorism Act of 2001" (USA Patriot Act) conocida como Ley Patriota, la cual disminuyó restricciones en las habilidades del gobierno para recabar información sobre las actividades y conversaciones de los individuos, aplicable tanto para investigaciones legales domésticas e internacionales como para el contexto de la seguridad nacional.

En el año 2002, fue aprobada la "Homeland Security Act of 2002" (HSA), la cual crea el Departamento de Seguridad Patria y le transfiere funciones relacionadas con la protección de la infraestructura de información con miras a la reducción de la vulnerabilidad nacional y evitar ataques terroristas.

Esta ley fue seguida por la "Cyber Security Enhancement Act of 2002", la cual modifica la ley patriota para disminuir aún más las restricciones impuestas a los proveedores de internet con respecto a cuándo y a quién pueden liberar información sobre sus subscriptores y los contenidos de las comunicaciones, estableciéndose ahora tan solo el requisito de contar con la creencia de buena fe (en lugar de razonable como lo establecía la ley patriota) de que existe una emergencia que involucra peligro (en lugar de peligro inmediato) o muerte o afectación física seria. Los contenidos pueden ser descubiertos ante una entidad gubernamental federal, estatal o local (en lugar de una agencia de aplicación de la ley).

Más adelante se ven llegar una serie de leyes federales tales como la "Federal Information Security Management Act of 2002 (Fisma)", la "E-Government Act of 2002", la "Identity Theft Penalty Enhancement Act" y la "Intelligence Reform and Terrorism Prevention Act of 2004 (Irtpa)", todas las cuales se encuentran dirigidas a la construcción de un marco legislativo, administrativo y ejecutivo capaz de disminuir la vulnerabilidad de los sistemas de información estadounidenses mediante la correcta planificación, distribución de funciones y análisis de riesgos (Fischer, 2012).

En el año 2011 se publicó el que sin duda alguna es el documento más representativo de la visión estadounidense en materia de ciberseguridad. Titulado "Estrategia Internacional para el Ciberespacio: Prosperidad, seguridad y apertura en un mundo interconectado", dibuja cinco principios que deben ser apoyados por las naciones, en los cuales se encuentra la protección contra el crimen, y bajo el cual las naciones "identifiquen y procesen legalmente a los cibercriminales para asegurar la eliminación de refugios seguros y la cooperación con las investigaciones internacionales criminales de manera oportuna" (Oficina ejecutiva del Presidente de los Estados Unidos de América, 2011), brinda además propuestas de acción para lograr tales ideales y compromete al gobierno estadounidense a fomentar acciones de otras naciones tales como la participación en la Convención de Bruselas.

Si bien es cierto que los efectos de la estrategia estadounidense antes mencionada sobre nuestro país aún son difíciles de dilucidar, y que desde el punto de vista del derecho internacional ni las leyes federales ni las estatales de este país tienen efecto alguno en Costa Rica, resulta importante resaltar que, debido a la naturaleza misma de las tecnologías de la información y la comunicación, (la cual requiere de la conectividad de las redes y no hace diferencias con base en el territorio) se dificulta seriamente que nuestro país pueda afirmar encontrarse fuera del área de influencia de leyes como la Ley Patriota o de decisiones estratégicas tomadas por los Estados Unidos de América como las antes señaladas.

Finalmente, resulta importante recordar que actualmente contamos con un instrumento internacional que nos vincula de manera directa con el gobierno estadounidense, el cual no es otro que el Tratado de Libre Comercio entre Norte América, Centro América y República Dominicana (DR-Cafta). El cual pese a no poseer disposiciones específicas relativas a ciberseguridad a nivel nacional y estar enfocado en el mercado interior (específicamente en el mercado

de telecomunicaciones), establece en sus cláusulas de manera reiterada la capacidad de una de las partes de "tomar medidas necesarias para (…) Garantizar la seguridad y confidencialidad de los mensajes" así como de "Proteger la integridad técnica de las redes o servicios públicos de telecomunicaciones" (Asamblea Legislativa de la República de Costa Rica, 2008).

10.5 REGULACIÓN DE LA CIBERSEGURIDAD EN COSTA RICA

El marco jurídico relacionado con ciberseguridad en el país presenta un desarrollo más amplio a partir del año 2000, producto del crecimiento en las conexiones de internet y el aumento de delitos cometidos por medios informáticos principalmente en el tema de fraude informático; a continuación se presenta el estado actual del país en esta materia jurídica.

10.5.1 Leyes

Ley de la Administración Financiera de la República y Presupuestos Públicos (Asamblea Legislativa de la República de Costa Rica, 2001).

Establece dos artículos relacionados con el tema de ciberseguridad, sentando responsabilidades por acciones en contra del hardware como del software dentro del ámbito de aplicación del régimen económico-financiero de los órganos y entes administradores o custodios de los fondos públicos:

> *Artículo 110.- Hechos generadores de responsabilidad administrativa*
>
> *Además de los previstos en otras leyes y reglamentaciones propias de la relación servicio, serán hechos generadores de responsabilidad administrativa, independientemente de la responsabilidad civil o penal a que puedan dar lugar, los mencionados a continuación:*
>
> *n) Obstaculizar el buen desempeño de los sistemas informáticos de la Administración Financiera y de Proveeduría, omitiendo el ingreso de datos o ingresando información errónea o extemporánea.*
>
> ñ) *Causar daño a los componentes materiales o físicos de los aparatos, las máquinas o los accesorios que apoyan el funcionamiento de los sistemas informáticos de la Administración Financiera y de Proveeduría.*
>
> *Artículo 111.- Delito informático*
>
> *Cometerán delito informático, sancionado con prisión de uno a tres años, los funcionarios públicos o particulares que realicen, contra los sistemas informáticos de la Administración Financiera y de Proveeduría, alguna de las siguientes acciones:*
>
> *a) Apoderarse, copiar, destruir, alterar, transferir o mantener en su poder, sin el debido permiso de la autoridad competente, información, programas o bases de datos de uso restringido.*
>
> *b) Causar daño, dolosamente, a los componentes lógicos o físicos de los aparatos, las máquinas o los accesorios que apoyan el funcionamiento de los sistemas informáticos.*
>
> *c) Facilitar a terceras personas el uso del código personal y la clave de acceso asignados para acceder a los sistemas.*
>
> *d) Utilizar las facilidades del Sistema para beneficio propio o de terceros.*

Ley de Certificados, Firmas Digitales y Documentos Electrónicos y su Reglamentos (Asamblea Legislativa de la República de Costa Rica, 2005)**.**

Esta ley crea un aspecto fundamental en el marco normativo jurídico-informático costarricense: seguridad jurídica y técnica, debido a que se garantiza la autoría e integridad de los documentos digitales, equiparándolos a los documentos realizados en papel, lo cual se denomina equivalencia funcional, en su artículo 3 lo señala expresamente:

Artículo 3.- Reconocimiento de la equivalencia funcional.

> *Cualquier manifestación con carácter representativo o declarativo, expresada o transmitida por un medio electrónico o informático, se tendrá por jurídicamente equivalente a los documentos que se otorguen, residan o transmitan por medios físicos.*

De igual forma le da fuerza probatoria a estos documentos firmados digitalmente, aspecto fundamental para en caso de procesos judiciales exista el respaldo jurídico de documentos, situación que han comenzado a aprovechar principalmente el sector financiero del país:

Artículo 4.- Calificación jurídica y fuerza probatoria.

> *Los documentos electrónicos se calificarán como públicos o privados, y se les reconocerá fuerza probatoria en las mismas condiciones que a los documentos físicos.*

Artículo 10.- Presunción de autoría y responsabilidad.

> *Todo documento, mensaje electrónico o archivo digital asociado a una firma digital certificada se presumirá, salvo prueba en contrario, de la autoría y responsabilidad del titular del correspondiente certificado digital, vigente en el momento de su emisión.*

Artículo 11.- Alcance.

> *Entiéndase por certificado digital el mecanismo electrónico o digital mediante el que se pueda garantizar, confirmar o validar técnicamente:*
>
> *a) La vinculación jurídica entre un documento, una firma digital y una persona.*
>
> *b) La integridad, autenticidad y no alteración en general del documento, así como la firma digital asociada.*
>
> *c) La autenticación o certificación del documento y la firma digital asociada, únicamente en el supuesto del ejercicio de potestades públicas certificadoras.*

Ley de protección de la niñez y la adolescencia frente al contenido nocivo de internet y otros medios electrónicos (Asamblea Legislativa de la República de Costa Rica, 2011).

Esta ley busca proteger a la niñez y adolescencia que utilizan medios tecnológicos en los locales con acceso al público, destinados al uso público de computadoras conectadas a Internet u otras formas de comunicación en red, sea por medio de computadoras y de cualquier otro medio electrónico, que sean utilizados por personas menores de edad. La ley establece que los locales deberán tener filtros para evitar el acceso a los siguientes contenidos, según lo establecido en su artículo 3:

> *a) Sitios que muestren o promuevan la pornografía en general y la infantil, en particular.*
>
> *b) Sitios que promuevan el lenguaje obsceno.*
>
> *c) Sitios que promuevan la agresión y la violencia física, sexual y emocional.*
>
> *d) Sitios que promuevan la construcción de armas o explosivos.*
>
> *e) Sitios que promuevan e inciten el uso de drogas de uso no autorizado.*
>
> *f) Sitios que promuevan actividades bélicas.*
>
> *g)Sitios que promuevan el racismo, la xenofobia o cualquier otra forma de discriminación contraria a la dignidad humana, de conformidad con el artículo 33 de la Constitución Política y los instrumentos internacionales de derechos humanos vigentes en Costa Rica.*
>
> *h) Los programas o la información que puedan ser usados para mirar, descargar, distribuir, adquirir e intercambiar pornografía en general e infantil, en particular.*

Según la normativa indicada, en sus artículos 4, 5 y 6, los encargados de la supervisión será la Superintendencia de Telecomunicaciones, que tendrá la fiscalización, regulación y control de los requerimientos y las

estipulaciones establecidos en la ley, además de resolver los procedimientos administrativos por incumplimientos y sus sanciones, certificar los locales libres de pornografía y contenidos nocivos. Además, en su artículo 7, se establece una obligación de los proveedores de servicios de Internet referente a los filtros de contenido, y se agrega otra de fiscalización a la Sutel:

> *Todo proveedor de servicios de acceso a Internet que ofrezca o venda estos servicios al público deberá incluir, dentro de su oferta de servicios, la opción de adquirir los filtros y demás programas especiales para bloquear el acceso a sitios con los contenidos indicados en el artículo 2 de esta Ley. La Sutel fiscalizará el cumplimiento de esta obligación. (Asamblea Legislativa de la República de Costa Rica, 2011).*

Resulta extraño estas atribuciones asignadas a la Sutel, debido a que sus funciones son de regular el mercado de telecomunicaciones, pero con esta ley los hacen inspectores, lo cual por ahora la Sutel no está realizando. Un aspecto fundamental en los temas tecnológicos es el tema de la educación tecnológica, lo cual lo contempla la ley:

Artículo 8.- Educación

> *El Patronato Nacional de la Infancia, en coordinación con el Ministerio de Educación Pública, el Ministerio de Ambiente, Energía y Telecomunicaciones, el Ministerio de Ciencia y Tecnología y la Sutel desarrollarán campañas de educación para concienciar a los padres y madres de familia, las personas tutoras o las encargadas de las personas menores de edad, sobre la importancia de velar por la información a la que acceden estos, vía Internet o por algún otro medio electrónico de comunicación.*

Ley de protección de la persona frente al tratamiento de sus datos personales (Asamblea Legislativa de la República de Costa Rica, 2011).

Actualmente, los datos de las personas en los diferentes sistemas de bases de datos toman vital importancia, debido al robo de este tipo de información. Bajo este panorama nuestro país creo esta ley, en búsqueda de brindar al ciudadano el respaldo jurídico para denuncias por mal manejos de su información, y a las empresas públicas y privadas les establece el marco de trabajo de las bases de datos que manejan.

ARTÍCULO 1.- Objetivo y fin

> *Esta Ley es de orden público y tiene como objetivo garantizar a cualquier persona, independientemente de su nacionalidad, residencia o domicilio, el respeto a sus derechos fundamentales, concretamente, su derecho a la autodeterminación informativa en relación con su vida o actividad privada y demás derechos de la personalidad, así como la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes.*

ARTÍCULO 2.- Ámbito de aplicación

> *Esta Ley será de aplicación a los datos personales que figuren en bases de datos automatizadas o manuales, de organismos públicos o privados, y a toda modalidad de uso posterior de estos datos.*
>
> *El régimen de protección de los datos de carácter personal que se establece en esta Ley no será de aplicación a las bases de datos mantenidas por personas físicas o jurídicas con fines exclusivamente internos, personales o domésticos, siempre y cuando éstas no sean vendidas o de cualquier otra manera comercializadas.*

Hay que resaltar que la ley establece el principio de autodeterminación informativa el cual es en general el derecho de toda persona a decidir qué información brinda, lo que se realice con ella y en general el manejo y tratamiento de sus datos, así lo señala el artículo 4, 5. También es importante resaltar de la ley el principio de calidad de la información, el cual establece a las instituciones públicas y privadas que la información que maneje debe cumplir ciertas características de actualidad,

veracidad y exactitud, buscando asegurar que la información de las personas sea la correcta, verdadera y actualizada.

Es importante hacer notar que de igual forma se le solicita a las empresas e instituciones protocolos de actuación y adoptar las medidas de índole técnica y de organización necesarias para garantizar la seguridad de los datos de carácter personal y evitar su alteración, destrucción accidental o ilícita, pérdida, tratamiento o acceso no autorizado, señalando la norma que "dichas medidas deberán incluir, al menos, los mecanismos de seguridad física y lógica más adecuados de acuerdo con el desarrollo tecnológico actual, para garantizar la protección de la información almacenada." (Asamblea Legislativa de la República de Costa Rica, 2011)

Si no se reúnen estos requisitos no podrán registrar estas bases de datos ante la Agencia de Protección de Datos Personales (Prodat), la cual también se crea en esta ley, siendo la institución que velará por los datos de todos los ciudadanos en el mundo digital costarricense; con esta figura la norma tendrá un respaldo en la praxis.

Por ahora se está a la espera de la publicación del Reglamento a esta ley para que la Agencia comience a trabajar, a pesar de que la misma ley estableció transitorios en donde para este 2013 debería estar en funcionamiento, todavía sin la publicación de dicho Reglamento no ha podido comenzar la Agencia su labor.

Código Penal Ley 9048 Reforma de varios artículos y modificación de la sección VIII, denominada Delitos Informáticos y Conexos, del título VII del Código Penal (Asamblea Legislativa de la República de Costa Rica).

Merece especial atención este tema por la situación jurídicamente particular que estamos viviendo sobre el tema penal en materia de ciberseguridad. Para el año 2001, a raíz de la aparición de delitos en materia económica utilizando tecnología, surge la reforma en el Código Penal y aparición de los primeros artículos sobre delitos informáticos en el Código Penal, se crean tres figuras: la primera la Violación de Comunicaciones Electrónicas (artículo 196 bis del Código Penal). La segunda el Fraude Informático (artículo 217 bis del Código Penal) y la Alteración de Datos y Sabotaje Informático (artículo 229 bis del Código Penal).

Es claro que estos tres tipos penales no eran suficientes para abarcar la variada gama de delitos informáticos que en otros países se regulan, es por esto que 11 años después Costa Rica realiza un proceso de reforma en el tema de Delitos Informáticos, creando la Ley 9048 Reforma de varios artículos y modificación de la sección VIII, denominada Delitos Informáticos y Conexos, del título VII del Código Penal. Esta nueva normativa contempla, penas más altas al delito de corrupción de menores si el ofensor utiliza redes sociales, establece nuevos tipos penales como la suplantación de identidad, el espionaje informático, la propagación de malware, falsificación de sitios web. Veamos algunos de los artículos:

Artículo 217 bis.- Estafa informática

> *Se impondrá prisión de tres a seis años a quien, en perjuicio de una persona física o jurídica, manipule o influya en el ingreso, en el procesamiento o en el resultado de los datos de un sistema automatizado de información, ya sea mediante el uso de datos falsos o incompletos, el uso indebido de datos, programación, valiéndose de alguna operación informática o artificio tecnológico, o bien, por cualquier otra acción que incida en el procesamiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta, con la cual procure u obtenga un beneficio patrimonial o indebido para sí o para otro. La pena será de cinco a diez años de prisión, si las conductas son cometidas contra sistemas de información públicos, sistemas de información bancarios y de entidades financieras, o cuando el autor es un empleado encargado de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tenga acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.*

Artículo 229 bis.- Daño informático

Se impondrá pena de prisión de uno a tres años al que sin autorización del titular o excediendo la que se le hubiera concedido y en perjuicio de un tercero, suprima, modifique o destruya la información contenida en un sistema o red informática o telemática, o en contenedores electrónicos, ópticos o magnéticos. La pena será de tres a seis años de prisión, si la información suprimida, modificada, destruida es insustituible o irrecuperable.

Artículo 230.- Suplantación de identidad

Será sancionado con pena de prisión de tres a seis años quien suplante la identidad de una persona en cualquier red social, sitio de Internet, medio electrónico o tecnológico de información. La misma pena se le impondrá a quien, utilizando una identidad falsa o inexistente, cause perjuicio a un tercero. La pena será de cuatro a ocho años de prisión si con las conductas anteriores se causa un perjuicio a una persona menor de edad o incapaz. Indiscutiblemente, es un gran avance en la legislación costarricense, la ciudadanía podrá disponer de nuevas figuras penales para poder denunciar los delitos que principalmente se llevan a cabo en Internet y que antes no podían denunciar; no obstante, es necesario acompañarlo de otras acciones como el fortalecimiento de la sección de Delitos Informáticos del Organismo de Investigación Judicial.

Artículo 231.- Espionaje informático

Se impondrá prisión de tres a seis años al que, sin autorización del titular o responsable, valiéndose de cualquier manipulación informática o tecnológica, se apodere, transmita, copie, modifique, destruya, utilice, bloquee o recicle información de valor para el tráfico económico de la industria y el comercio.

Artículo 233.- Suplantación de páginas electrónicas

Se impondrá pena de prisión de uno a tres años a quien, en perjuicio de un tercero, suplante sitios legítimos de la red de Internet.

La pena será de tres a seis años de prisión cuando, como consecuencia de la suplantación del sitio legítimo de Internet y mediante engaño o haciendo incurrir en error, capture información confidencial de una persona física o jurídica para beneficio propio o de un tercero.

Esta ley ha sido fuertemente cuestionada por algunos de sus artículos por parte del Colegio de Periodistas principalmente. Se cuestiona en dicha ley el artículo 288 y el artículo 230:

Artículo 288.- Espionaje

Será reprimido con prisión de cuatro a ocho años al que procure u obtenga indebidamente ***informaciones secretas políticas*** *o de los cuerpos de policía nacionales o de seguridad concernientes a los medios de defensa o a las relaciones exteriores de la nación, o afecte la lucha contra el narcotráfico o el crimen organizado. La pena será de cinco a diez años de prisión cuando la conducta se realice mediante manipulación informática, programas informáticos maliciosos o por el uso de tecnologías de la información y la comunicación.*

En este caso se ha discutido el tema del concepto informaciones secretas políticas, señalando que existirá una mordaza a la libertad de prensa, por señalar la figura penal, la obtención de informaciones secretas políticas; asimismo se dice que esta nueva ley va a afectar a los medios informativos y la manera en que realicen periodismo investigativo.

Primeramente, es importante señalar que este concepto jurídico indeterminado (informaciones secretas políticas) existe desde el Código Penal de 1970 por tanto no era una novedad en la normativa, además que las estadísticas del Poder Judicial señalan que el mismo nunca se ha aplicado, pero si se hace necesario su modificación debido a que en Costa Rica este concepto no existe, nuestra Constitución contempla el Secreto de Estado, por tanto si es necesaria su reforma. El artículo 230 de la nueva normativa indica:

Artículo 230.- Suplantación de identidad

> *Será sancionado con pena de prisión de tres a seis años quien suplante la identidad de una persona en cualquier red social, sitio de Internet, medio electrónico o tecnológico de información.* ***La misma pena se le impondrá a quien, utilizando una identidad falsa o inexistente, cause perjuicio a un tercero.*** *La pena será de cuatro a ocho años de prisión si con las conductas anteriores se causa un perjuicio a una persona menor de edad o incapaz. Indiscutiblemente, es un gran avance en la legislación costarricense, la ciudadanía podrá disponer de nuevas figuras penales para poder denunciar los delitos que principalmente se llevan a cabo en Internet y que antes no podían denunciar; no obstante, es necesario acompañarlo de otras acciones como el fortalecimiento de la sección de Delitos Informáticos del Organismo de Investigación Judicial.*

En este caso los blogueros y cibernautas en general esta preocupados por que la norma sanciona el uso de una identidad falsa o inexistente en Internet lo que señala la posibilidad de no permitir realizar denuncias de manera anónima en redes sociales, es innegable que en Internet la mayoría utiliza, en muchos casos, un nombre ficticio, por lo que puede prestarse dicho artículo para persecución de este tipo de acciones de los cibernautas.

Esta redacción puede prestarse para este tipo de denuncias y afectar la libertad de expresión por lo que si es necesaria su modificación. Bajo estas protestas que se han generado en el país, esta reciente ley presenta en la Asamblea Legislativa tres propuestas de reforma que están siendo estudiadas para reformar dicha ley.

Independientemente de estos aspectos, esta ley es un gran avance en la legislación costarricense, la ciudadanía y las empresas podrán disponer de nuevas figuras penales para poder denunciar los delitos que principalmente se llevan a cabo en Internet y que antes no podían denunciar; nos ponemos a la vanguardia de los países que han realizado una reforma integral de la normativa penal en materia de delitos informáticos.

10.5.2 Decretos Ejecutivos

Directrices relativas al empleo ilegal de software en las oficinas gubernamentales y autorización para el empleo de software libre DECRETO 30151-J
(Poder Ejecutivo y Ministerio de Justicia y Gracia, 2002).

En este caso se crea una directriz con el fin de asegurar el mantenimiento del equipo de cómputo que tiene el Estado, buscar la seguridad de la información, prevenir virus y asegurar la eficiente custodia de los archivos informáticos de las instituciones públicas y cumplir la normativa referente a Derechos de Autor y Derechos Conexos, entre su articulado destaca:

> *Artículo 1—Se ordena que todo el Gobierno Central se proponga diligentemente prevenir y combatir el uso ilegal de programas de cómputo, con el fin de cumplir con las disposiciones sobre derecho de autor que establece la Ley N° 6683 y sus reformas y la Ley N° 8039, acatando las provisiones pertinentes de los acuerdos internacionales, incluyendo el Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio y también las otras disposiciones de la normativa nacional vigente.*
>
> *Artículo 2°—Cada Ministerio deberá realizar un inventario inicial de los equipos existentes y de los programas que tengan las computadoras y el número de copias autorizadas de cada programa, determinando la fecha de instalación y versión de cada uno. El término para el cumplimiento de este inventario inicial no será mayor de diez (10) meses a partir de la entrada en vigencia de este decreto.*
>
> *Artículo 3°—Posterior al levantamiento del inventario, cada Ministerio del Gobierno Central deberá establecer sistemas y controles dentro de un término de dieciocho (18) meses para garantizar la utilización en sus computadoras única y exclusivamente de aquellos programas que cumplan con los derechos de autor correspondientes. Cualquier programa que exceda el*

número autorizado o que no cuente con la licencia correspondiente deberá removerse inmediatamente.

El Ministro designará a una persona como responsable, entre otras cosas, de presentar un informe anual ante el Registro Nacional de Derechos de Autor y Derechos Conexos, en el que hará constar que el respectivo Ministerio cumple con la protección de los derechos de autor relativos a los programas de cómputo.

Artículo 5°—El Registro Nacional de Derechos de Autor y Derechos Conexos obligatoriamente llevará a cabo auditorías, para lo cual coordinará con cada Ministerio del Gobierno Central, debiendo realizar inventarios periódicos de las computadoras, al menos una vez al año, para determinar la fidelidad del sistema de información y el acatamiento a las normas sobre derecho de autor. Para esto, dicho registro contará con el auxilio y colaboración del Departamento de Informática del Registro Nacional, y podrá además, en caso necesario solicitar a la Junta Administrativa del mismo Registro, aprobación para la contratación de personal externo adecuado para este cumplimiento.

Es importante esta directriz debido a que el tener software ilegal produce que no se actualicen los equipos adecuadamente, manteniendo vulnerabilidades, lo cual aumenta la posibilidad de ataques a los equipos y en este caso a equipos del estado que pueden producir perdida de información valiosa de todos los ciudadanos.

Creación Comisión Internet Costa Rica, CI-CR (Poder Ejecutivo, Ministerio de Ciencia y Tecnología, 2004). Esta Comisión busca, según lo establece el mismo decreto, al existir…

"*ausencia natural de fronteras nacionales en Internet requiere de una perspectiva global para el desarrollo de políticas públicas. Internet constituye un medio excepcional, debido a que toda información que se publica en la red, instantáneamente es accesible en todo el mundo, desde cualquier parte y su impacto se percibe globalmente"*, además señala *"que es fundamental promover la investigación, el desarrollo transparente, la expansión técnica y la evolución tecnológica de Internet y su arquitectura, y su apoyo a las organizaciones, proyectos y programas que se puedan realizar conjuntamente para el futuro de Internet. Además de participar en el desarrollo de actividades en materia de creación de estándares, políticas públicas y educación".*

Su artículo 1 señala el fin de esta Comisión:

Artículo 1°—Créase la Comisión Internet Costa Rica, CI-CR, adscrita al Ministerio de Ciencia y Tecnología (Micit) con el fin de recomendar las políticas y directrices estratégicas relacionadas con el uso y desarrollo de Internet en Costa Rica. Para el funcionamiento de la CI-CR se utilizarán los recursos tanto financieros como humanos ya existentes en la Institución y en las demás instituciones que la conformen.

Esta Comisión es importante en el tema de ciberseguridad en el tanto cumpla lo que estipula su fin el artículo 3 inciso c, en el campo de recomendaciones técnicas y de seguridad en el uso de Internet en el país:

Artículo 3°—Los objetivos específicos de la CI-CR serán:

c) Promover estudios y recomendar procedimientos y normas técnicas y operacionales para asegurar el funcionamiento eficiente de las redes y servicios de Internet, así como su adecuada y creciente utilización por la sociedad costarricense.

Sobre el establecimiento de sitios web en las entidades públicas (Poder Ejecutivo, Ministerio de Ciencia y Tecnología, 2005)

En este caso este decreto hace referencia a la creación y desarrollo de de sitios web en el sector público, lo cual lo establece claramente en su artículo 1:

> *Artículo 1º—Instruir a las instituciones públicas que aún no tienen presencia en Internet a tomar las medidas necesarias para que en un plazo de seis meses logren dicha presencia mediante el desarrollo de sitios Web institucionales. Para la realización de esto deberán cumplir con todos los trámites y procedimientos que establece nuestro ordenamiento jurídico vigente.*

En el tema de ciberseguridad señala en su artículo 2 que dichos sitios deben cumplir "estándares de eficiencia, seguridad y amigabilidad", contemplando (a pesar de que no explica cómo) el tema de sitios seguros.

> *Artículo 2º—Instruir a las instituciones públicas que ya cuentan con presencia en Internet que deberán tomar las acciones necesarias para que un plazo de 18 meses ofrezcan a través de sitios web los servicios institucionales estratégicos de acuerdo con sus prioridades y la demanda de servicios de sus usuarios; lo anterior en forma interactiva y cumpliendo con estándares de eficiencia,* ***seguridad*** *y amigabilidad. Para la realización de esto deberán presentar al Ministerio de Ciencia y Tecnología a más tardar tres meses después de la entrada en vigencia de esta directriz un plan de acción institucional en donde se incluya el cronograma de actividades que se estarán llevando a cabo y que incorpore un plan de seguridad y un plan de contingencias además de todos los trámites y procedimientos que establece nuestro ordenamiento jurídico vigente.*

Creación de la Comisión Nacional de Seguridad En Línea (Poder Ejecutivo, Ministerio de Ciencia y Tecnología, 2010)**.**

Para el 2010 se crea la Comisión Nacional de Seguridad en Línea, con el fin de diseñar las políticas necesarias sobre el buen uso de Internet y las Tecnologías Digitales, además hacerle frente a los riesgos que se presentan en esta red, también, y uno de los aspectos más importantes que plantea este decreto, es que esta Comisión participará en el diseño y posterior coordinación, para la implementación del Plan Nacional de Seguridad en Línea.

Esta Comisión la conforman: el Ministerio de Ciencia y Tecnología, quien la presidirá. El Ministerio de Educación Pública, el Ministerio de Cultura y Juventud, la Superintendencia de Telecomunicaciones, el Poder Judicial, el Patronato Nacional de la Infancia, Fundación Paniamor, Fundación Omar Dengo (FOD), Cámara Costarricense de Tecnologías de la Información y la Comunicación (Camtic).

Creación del "Centro de Respuesta de Incidentes de Seguridad Informática (Csirt-CR)" (Poder Ejecutivo, Ministerio de Ciencia y Tecnología, 2012)**.**

El fin de este Centro, como lo indica el decreto Nº 37052-Micit en su artículo 1, es coordinar con los poderes del Estado, instituciones autónomas, empresas y bancos del Estado todo lo relacionado con la materia de seguridad informática y cibernética y concretar el equipo de expertos en seguridad de las Tecnologías de la Información que trabajará para prevenir y responder ante los incidentes de seguridad cibernética e informática que afecten a las instituciones gubernamentales.

Es claro que esta es una de las instancias más importantes para el tema de ciberseguridad, en su artículo 2 se le asigna una gran cantidad de objetivos donde se le integra a este Centro un alto grado de responsabilidad y múltiples actividades. Desde el punto de vista de acción administrativa el Centro está a cargo del Ministerio de Ciencia y Tecnología, que deberá coordinar, planificar, administrar y ejecutar los acuerdos del Consejo Directivo, este último conformado por:

- Ministro de Ciencia y Tecnología o su representante, quien lo presidirá. Ministro de la Presidencia o su representante. Ministro de Seguridad Publica o su representante. Fiscal General de la República o su representante. Ministro de Relaciones Exteriores o su representante. Ministro de Justicia y Paz o su representante. Presidente de la Academia Nacional de las Ciencias o su representante.

Este centro se torna en el país como una de las instancias principales en la lucha contra la ciberdelincuencia.

Creación de la Comisión Interinstitucional de Gobierno Digital (Poder Ejecutivo, Ministros de la Presidencia, Planificación Nacional y Política Económica, 2009).

En el 2009 la Presidencia de la República crea por medio del decreto Nº 35139-MP-Mideplan la Comisión Interinstitucional de Gobierno Digital. Para el 2010, se da una reforma a este decreto por medio del decreto Nº 36176-MP-PLAN (Poder Ejecutivo, Ministro de la Presidencia,Ministra de Planificación Nacional y Política Económica, 2010), modificando la conformación de la Comisión quedando de la siguiente manera:

A) La Presidenta de la República, quien la presidirá. Podrá ser sustituida por el Segundo Vicepresidente de la República, quien presidirá la Comisión ante esa eventualidad;

B) El Ministro o el Viceministro de Planificación Nacional y Política Económica;

C) El Ministro o el Viceministro de Ciencia y Tecnología;

D) El Ministro o el Viceministro de Economía, Industria y Comercio;

E) El Presidente Ejecutivo del Instituto Costarricense de Electricidad (ICE).

Con derecho a voz pero sin voto el Gerente de la Secretaría Técnica de Gobierno Digital y Los representantes de otras instancias que determine la Comisión.

En el artículo 2 del Decreto del 2009 se crea la Secretaría Técnica de Gobierno Digital, siendo el *"órgano ejecutor de las políticas, estándares y proyectos que defina la Comisión para incrementar la eficiencia y la transparencia en el Sector Público por medio del uso estratégico de las tecnologías digitales con el fin de empoderar a los habitantes en el uso de servicios públicos"*. (Poder Ejecutivo, Ministros de la Presidencia, Planificación Nacional y Política Económica, 2009).

Bajo esta normativa la Comisión y por medio de la Secretaria Técnica son los encargados de buscar la conformación de un Gobierno Digital por medio de la Comisión y la Ejecución de los proyectos por parte de la Secretaría, por tanto esta secretaria es el llamado a "orquestar" el tema digital de Costa Rica.

10.6 CIBERSEGURIDAD EN COSTA RICA

Para conocer a fondo el tema de ciberseguridad en el país es importante consultar a los principales actores institucionales su opinión con respecto a esta materia, por lo que se realizó una entrevista a directores (o representantes designados) de las siguientes instituciones:

- Gobierno Digital, Secretaría Digital
- Ministerio de Ciencia y Tecnología: Dirección Firma Digital
- Poder Judicial, Sección de Delitos Informáticos
- Agencia de Protección de Datos (Prodhab)
- Banca Estatal (Banco Central)
- Centro de Respuesta de Incidentes de Seguridad Informática (Csirt-CR)
- Superintendencia de Telecomunicaciones (Sutel)

10.6.1 Banco Central

> *El Banco Central de Costa Rica es la organización cuyo principal objetivo es controlar la inflación, realiza labores conjuntamente con el Consejo Nacional de Supervisión de Sistema Financiero para cumplir con sus objetivos. Se encarga también de la emisión y administración de los billetes y monedas, entre otras tareas*. (Banco Central de Costa Rica, 2011).

Además, el Banco Central tiene a su cargo (por medio de un Convenio con el Ministerio de Ciencia y Tecnología con la Dirección de Firma Digital) albergar el nodo superior o raíz del sistema de certificación nacional, con lo cual se logra el aprovechamiento de infraestructura

Cuadro 10.1
Certificados Emitidos por entidades financieras costarricenses

Entidad de Registro	2009	2010	2011	2012	Total
Banco Nacional de Costa Rica	10	3.228	6.466	7.514	17.218
Banco Popular	85	1.223	1.591	1.845	4.744
BCCR	544	825	315	911	2.595
Banco de Costa Rica	3	50	594	1.511	2.158
Banco BAC de San José S.A.	20	522	572	853	1.967
Banco BCT S.A.	6	324	349	231	910
Instituto Nacional de Seguros		11	423	261	695
COOOPENAE			42	460	502
Grupo Mutual Alajuela La Vivienda		27	51	220	298
Banco Promérica				195	195
Banco Crédito Agrícola de Cartago		4	89	55	148
Banco Lafise			24	108	132
Total	668	6.214	10.516	14.164	31.562

Fuente: Banco Central de Costa Rica

física y recursos tecnológicos existentes (Ministerio de Ciencia y Tecnología), además las diferentes entidades bancarias generan firmas y certificados digitales para los clientes que lo soliciten dentro de la red bancaria.

También, el Reglamento de la Ley 8454 "Ley de Certificados, Firmas Digitales y Documentos Electrónicos" faculta que el Director de la Dirección de Certificadores de Firma Digital cuente con la asesoría de un comité de políticas, entre los cuales se cuenta el Banco Central de Costa Rica. Tomando en consideración este panorama y que muchos de los Fraudes Informáticos ocurren o pueden ocurrir dentro de las plataformas informáticas bancarias es importante conocer la opinión de este sector.

El Banco Central señala (Carvajal Chavarría, 2012) que desde la óptica del sistema de pagos y la seguridad, desde hace aproximadamente 3 o 4 años donde se tuvo una alta incidencia de phishing, lo cual provocó muchos desfalcos a los clientes y que al ser llevados a instancias judiciales los bancos terminaron asumiendo las perdidas teniendo que reponer el dinero a los clientes; la banca comenzó a implementar medidas de seguridad para evitar esta situación, además de un enfoque de crear conciencia a los clientes, lo que provocó la disminución de la incidencia de estos tipos de delitos.

Asimismo, indican que se han apoyado con el tema de firma digital y certificados digitales, que brindan un mayor respaldo jurídico y mayor seguridad, donde muchas instancias financieras están comenzando a utilizar y brindar al usuario la posibilidad de este medio de seguridad, permitiendo identificar con mayor certeza al cliente y lograr jurídicamente establecer en los usuarios la responsabilidad de las transacciones bancarias que realizan.

Sobre la coordinación mencionan que sí mantienen una relación con la Dirección de Firma Digital, pero que a nivel país no aparece quién brinde el norte, indican que se pensó que la Secretaria Digital iba a tener este papel

pero se ha dedicado a ejecutar, no a fijar un proyecto país de ciberseguridad y otros temas, ni a coordinar todas las instancias estatales para un trabajo conjunto, consideran que actualmente cada institución tiene un trabajo independientemente sin coordinación, o es muy poca la existente. Acerca de la normativa vigente en el país sobre el tema ciberseguridad, señalan que la falta de normativa era insuficiente para enfrentar lo que estaba ocurriendo y que además el tema tecnológico avanza muchísimo más veloz que la modernización de la normativa relacionada, y que estos vacíos los afectan. (Ver cuadro 10.1).

10.6.2 Poder Judicial: Sección de Delitos Informáticos

Esta sección nace en 1997 como Unidad de Investigación Informática, pero debido al crecimiento de este tipo de delincuencia para el año 2002 pasa a ser la Sección de Delitos Informáticos. Su labor es fundamental en esta nueva era de Cibersociedad; es realizar las investigaciones de los delitos en los cuales los medios informáticos son los principales o únicos indicios existentes, además apoyar en el ámbito informático en las investigaciones relacionadas con otros delitos.

La Sección de Delitos Informáticos señala (Lewis Hernández, 2012)que el gran problema en la ciberseguridad es la falta de cultura informática, tanto de usuarios normales, como de los informáticos, provocando brechas en cuanto a la aplicación y creación de medidas de seguridad, generando que en muchos casos recabar la prueba sea mucho más complicado, ejemplo de esta falta de políticas es la no presencia de bitácoras de registros de lo que realizan los usuarios en las redes.

Además, ponen de manifiesto que las personas a pesar de conocer en muchos casos los riesgos de ciertas acciones en Internet no toman precauciones, por ejemplo no leen lo que les aparece en la pantalla de sus equipos, se presentan muchos excesos de confianza. Así mismo, se encuentra el problema de la inversión en la seguridad informática, donde en muchas empresas es poco, considerando que no se ha desarrollado esa visión de la importancia que representa este tipo de seguridad.

La Sección de Delitos Informáticos cuenta con 21 personas (informáticos) más el personal administrativo, esperan que se apruebe el presupuesto ordinario en la Asamblea Legislativa para continuar con esta cantidad. Preocupa a la Sección que con la nueva ley de Delitos Informáticos va a aumentar la cantidad de denuncias y procesos que deberán realizar, por lo que debería contarse con más personal y convenios internacionales que permitan el apoyo en las investigaciones, que en muchos de estos casos se trasladan a otros países.

En el caso de las herramientas que requieren para la informática forense, señalan que no están mal, pero siempre faltan recursos, el presupuesto es limitado, principalmente porque las herramientas son muy caras y los equipos para este tipo de análisis requieren gran capacidad, y se ocupa que la sección se mantenga actualizada, además señalan el problema que en la nueva ley de Delitos Informáticos no se contempló un aumento al presupuesto de la Sección de Delitos Informáticos.

Indican que sobre el tema de ciberseguridad es necesaria una política de capacitación constante a jueces, fiscales, investigadores, etc. para que conozcan mucho más del tema; de igual forma mencionan que la sección en específico le falta presupuesto para capacitación, la cual en general es cara.

En el tema de colaboración a nivel nacional se coordina con el Csirt-ICE, la Asociación Bancaria Costarricense para temas como phishing y farming, pero si falta una mejor coordinación con las demás instancias relacionadas con la ciberseguridad como el Csirt-CR, además de que sigue faltando el establecimiento de un norte en el país en materia de ciberseguridad, donde consideran que nadie ha asumido ese rol, el cual en algún momento se pensó que Gobierno Digital ocuparía.

10.6.3 Superintendencia de Telecomunicaciones

Sutel es un órgano de desconcentración máxima, adscrito a la Autoridad Reguladora. A esta institución le corresponde la aplicación de la regulación al sector de telecomunicaciones. Se creó mediante la Ley 8660, publicada el 13 de agosto del 2008. Le toca asegurar la eficiencia, igualdad, continuidad, calidad, mayor y mejor cobertura e información, así como mejores alternativas en la prestación de los servicios de telecomunicaciones. (Superintendencia de Telecomunicaciones, 2011).

Sus funciones son: (Superintendencia de Telecomunicaciones, 2011)

- *Imponer a los operadores la obligación de dar libre acceso a redes y servicios*
- *Incentivar la inversión en el sector.*
- *Otorgar autorizaciones y rendir dictámenes técnicos al Poder Ejecutivo para otorgar, ceder, prorrogar o extinguir concesiones o permisos.*
- *Administrar y controlar el uso eficiente del espectro radioeléctrico.*
- *Resolver conflictos entre operadores y proveedores de servicios de telecomunicaciones.*
- *Homologar contratos de adhesión entre proveedores y abonados.*
- *Elaborar las normas técnicas.*
- *Fijar las tarifas de telecomunicaciones, según la ley.*

La Sutel tiene hasta hace dos años un departamento de Tecnologías de la Información, anteriormente los servicios se los brindaba la Aresep, por ahora son 3 personas los que están en este departamento, el tema de ciberseguridad si lo toman en cuenta a lo interno pero no han establecido estas políticas de manera escrita.

Señalan que (Herrera Céspedes & Fonseca Salazar, 2012) la Sutel no tiene la potestad legal para establecer normas de ciberseguridad a los operadores, no está establecido que deban brindarlas, podría proponer recomendaciones a nivel técnico pero no ha sido considerado realizarlas, los proveedores deben cumplir estándares internacionales, pero la Sutel no les impone un estándar de seguridad Mucha de la información que manejan es información pública por lo que el robo de información no es tan preocupante, pero si tienen desarrollado un esquema de seguridad en busca de disminuir cualquier intento de ataque.

Además indica que a la Sutel no se le ha invitado a participar en los grupos de seguridad a nivel nacional, además señalan al Micitt por medio del Csirt-CR como los encargados de velar por la seguridad cibernética a nivel nacional. Mencionan que sí han coordinado con el Poder Judicial para apoyos en procesos de investigación de llamadas por medio de telefonía celular. Han trabajado en campañas para crear conciencia acerca de qué debe hacer la persona en caso de robos de celulares y cómo bloquearlos.

Como parte de lo que se requiere para una estructura de seguridad, las empresas proveedoras tendrían que brindar información sobre su infraestructura y esto está considerado como confidencial, por lo que también es otro aspecto que se torna difícil a la hora de trabajar el tema de ciberseguridad

Con Gobierno Digital se ha tenido algunos contactos para analizar posibles trabajos conjuntos, pero no en el tema de ciberseguridad. Indican que no aparece quién defina un trabajo conjunto entre las instituciones, ni un proyecto en tema digital a nivel de país, como debería ser. Sobre la tarea de velar por la pornografía en Cafés Internet en protección a menores se le asignó por ley, pero no están claros de cómo deben realizar esta tarea.

10.6.4 Ministerio de Ciencia y Tecnología, Dirección de Firma Digital

En Costa Rica el concepto de certificación digital se remonta a un proyecto de Ley presentado por el Poder Ejecutivo a la Asamblea Legislativa en 29 de febrero 2002, tramitado bajo el expediente 14.276, mismo que pretendía legislar lo relacionado con la firma digital en nuestro país, al cabo años de deliberaciones acerca del tema,

> *y varios textos sustitutos el día 22 de agosto del 2005 el proyecto de marras, culminó con la aprobación de la Ley de Certificados, Firmas Digitales y Documentos Electrónicos* (Dirección Firma Digital).

Por medio de la firma digital, se asocia la identidad de una persona o equipo, con un mensaje o documento electrónico, para asegurar la autoría y la integridad del mismo, es en la Dirección de Certificadores de Firma Digital que recae administrar y supervisar el sistema de certificación, adscrita al Ministerio de Ciencia y Tecnología.

La Dirección de Firma Digital señala que (Barquero Elizondo, 2012) el tema de ciberseguridad tiene muchas aristas, entendiendo dicho tema como la seguridad de todos los involucrados en el acceso a las tecnologías: proveedores, usuarios, intermediarios. Además, consideran que la ciberseguridad va muy relacionada con los aspectos legales y es necesario un respaldo de este tipo, lo cual con firma digital se ha logrado.

Señalan que éste es el mecanismo idóneo para brindar seguridad a los involucrados y tener certeza de quién es la persona que se identifica en la red con completo respaldo jurídico; señalando un aspecto fundamental: sin importar la debilidad técnica la firma digital va a funcionar y proveer la seguridad jurídica de las comunicaciones, de igual forma indican que las personas jurídicas también van a poder tener esta confianza.

La Dirección autoriza y supervisa a las entidades certificadoras emisoras (Banco Central) y busca oportunidades para masificar el uso de la firma, además promueve su uso, por lo cual han trabajado para ampliar las aplicaciones que pueden utilizar firma digital, con el fin de que las personas se interesen por obtenerla, lo cual se ha ampliado en el 2012, solamente en ese año, se adquirieron más firmas digitales que en otros años; actualmente se han emitido alrededor de 33000 certificados.

Indican además que la dirección de Firma Digital está adscrita al Ministerio de Ciencia y Tecnología y a este Ministerio es de los que menos presupuesto se le asigna, el trabajo de firma digital se realiza con dos personas; consideran que en general no se le está dando la importancia al tema tecnológico en el país y se ve reflejado en los apoyos presupuestarios, no es prioridad estos temas.

Sobre la coordinación con otras instancias, la Dirección asiste con las que requieran colaboración en la firma digital, pero consideran que en el país no existe un orquestador en el tema tecnológico como proyecto común, ni la interoperabilidad entre las instituciones del estado, que en su momento se pensó que sería asumido por Gobierno Digital por medio de su Red Intersectorial; sí señalan que los desarrollos que se están brindando por medio de este incluyen Firma Digital lo cual es positivo.

La dirección de firma digital menciona que se colabora con todos los que requieran de su apoyo, pero los esfuerzos no responden a un proyecto en común ni lineamientos de cómo deben hacerse las cosas a nivel país, consideran que cada instancia está trabajando independientemente.

10.6.5 Ministerio de Ciencia y Tecnología, Csirt-CR

Csirt significa Computer Security Incident Response Team (equipo de respuesta a incidentes de seguridad informática), este es un equipo dedicado a la implantación y gestión de medidas tecnológicas con el objetivo de mitigar el riesgo de ataques contra los sistemas de la comunidad a la que se proporciona el servicio (Ministerio de Ciencia y Tecnología, 2012). Busca incorporar el sistema de seguridad cibernética y tecnologías de información a la protección del Gobierno Central y las Entidades Autónomas como un factor minimizador de riesgos y amenazas cibernéticas a través de un CSIRT.

La dirección del Csirt señala (Núñez Corrales, 2012) que esta instancia es parte de la Estrategia Nacional Digital, donde se ha buscado definir esta estrategia debido a la falta de visión integral de tecnologías en el estado. Asimismo se indica que es necesario darle el estatus adecuado a la tecnología del estado, como herramienta indispensable de los sectores, que es necesaria una inversión fuerte en tecnología y de

políticas públicas que es donde entra el Csirt. Indica que han buscado enfocarse en mitigar los riesgos en el sector gobierno, realizando un proceso de análisis de estos. También expresa que el país presenta un atraso en tecnologías de la comunicación lo cual provoca un amplio espectro de huecos de seguridad.

EL Csirt-CR busca esa protección del gobierno central en tema cibernético, donde han logrado coordinar con equipos de vigilancia de las instituciones del estado, además de coordinar con los Csirt de la región y a nivel mundial al ser un problema global, esto se ha conseguido por medio de la OEA. Actualmente solo se cuenta con dos personas trabajando en el Csirt-CR, no se ha asignado presupuesto para las nuevas plazas.

El Csirt ha desarrollado protocolos y procedimientos de acción en casos de ataques, en donde los peligros que han detectado en su gran mayoría han sido externos. Señalan que se ocupan los recursos para tener efectivamente el Centro de Respuesta, con el personal y equipo adecuado para coordinar efectivamente la protección cibernética del país, acciones que deben llevarse a cabo por haber aceptado y firmado acuerdos internacionales.

Indica que la coordinación de Gobierno Digital y Csirt-CR no se ha dado, exponiendo que la estrategia de Gobierno Digital es distinta a la que realiza el Csirt-CR. Considera que no aparece un coordinador del tema de ciberseguridad, y que es necesario un "chief information Officer" a nivel país para que maneje este tema fuera de las instancias actuales.

10.6.6 Agencia de Protección de Datos de los Habitantes

Esta instancia es un órgano de desconcentración máxima adscrito al Ministerio de Justicia y Paz, sus atribuciones por ley se resumen en su artículo 16 inciso a "*velar por el cumplimiento de la normativa en materia de protección de datos, tanto por parte de personas físicas o jurídicas privadas, como por entes y órganos públicos"* (Asamblea Legislativa, 2011). La función de esta agencia se torna trascendental en la protección de la información de todos los ciudadanos que se encuentra en las bases de datos.

La Dirección de la Agencia indica que (González Castillo, 2012) la ciberseguridad es parte de los temas que la ley del todo no fue amplia en regular, que tendrá que irse aclarando con el Reglamento que está en proceso de revisión y publicación, pero por la coyuntura en que se encuentra la Agencia, al no existir reglamento, no se está trabajando el tema, pero que será uno de los aspectos a tratar y analizar.

Señalan que se presentó el presupuesto a la Contraloría, en espera de aprobación por parte de la Asamblea Legislativa, además que los que están ejerciendo funciones actualmente son por recargo, los puestos y presupuesto se esperan para el 2013. Además, indican que en estos meses de funcionamiento ha sido más de brindar información sobre la protección de datos a las otras instancias del estado, que sepan que ya existe esta agencia y la ley.

Internacionalmente señalan que tienen muchos aliados, Costa Rica pertenece a la Red Iberoamericana de Protección de Datos (desde hace 6 años), además es parte del Comité Ejecutivo de la Ley de Protección de Datos, también a nivel de Centroamérica somos el primer país en tener una ley de Protección de Datos. Asimismo se tiene una buena relación con la Agencia Española de Protección de Datos, la Agencia Uruguaya de Protección de Datos, de igual forma en México, Chile, Colombia.

10.6.7 Gobierno Digital, Secretaría Técnica

La Misión y Visión de Gobierno Digital son (Gobierno Digital-Secretaria Técnica):

- *Misión: Mejorar la competitividad nacional con una responsabilidad ambiental a través de la prestación de servicios transparentes y de alto nivel a los ciudadanos, basados en un gobierno interconectado y el desarrollo de las TIC.*

- *Visión: Ser un país líder en gobierno electrónico en América Latina a través de:*
    - *Servicio centrado en el ciudadano*
    - *Servicio transparente*
    - *Gobierno interconectado basado en un ambiente favorable para las TIC y construir una sociedad segura y equitativa*

Señala la dirección (Avendaño Rivera, 2012) que Gobierno Digital trabaja en ofrecer servicios digitales, que inserto en éstos va el tema de seguridad, buscan mejorar los servicios a los ciudadanos de las instituciones y que éstos mantengan esquemas de seguridad robusta, pero que su rol no es regular, considera que para esas funciones está el Micitt y Csirt, que en Gobierno Digital las políticas que emiten es de ejecución.

Indican que ellos tienen un plan de acción con una cartera de proyectos, ese es el norte que siguen, y que a pesar de siempre faltar dinero, buscan recursos de auto sustentabilidad. De la misma forma apoyan a las instituciones para que desarrollen sus proyectos, cada uno de estos debe estar con niveles de seguridad que son considerados en su desarrollo, esto en razón de proteger al usuario y no perder credibilidad. También exponen que a nivel país existe el problema de no aprovechar los desarrollos realizados como Merlink, siendo necesario que se brinde una estrategia para aprovechar como un todo las plataformas existentes y que no cada institución haga su propio desarrollo.

Sobre la coordinación con otras instancias, asegura que si requieren ayuda, participan y colaboran, pero no propiamente en temas de ciberseguridad debido a que no existe claridad de que es lo que se quiere. Considera que hay que tener claro la instancia de trabajo de cada institución; existe una Comisión de Coordinación Interinstitucional, donde participan diferentes instancias en las cuales se dan las políticas de coordinación; propiamente el tema de ciberseguridad considera que le corresponde al Ministerio de Ciencia y Tecnología.

Plantea que es necesario dar un paso más, crear una Agencia de Infocomunicación, para que se encargue de las áreas faltantes, que vea telecomunicaciones, brecha digital, ciberseguridad; definir políticas públicas, entre otras; señala que es necesario que alguien orqueste el norte digital del país, pero que no le corresponde a Gobierno Digital.

10.7 LA CIBERSEGURIDAD EN LA NUBE, COSTA RICA

10.7.1 Concepto de "La Nube"

Los servicios de computación en la nube han llegado para quedarse. Este servicio ofrece muchas ventajas a las empresas y a las personas, pero también encierra riesgos, además de existir vacíos jurídicos en nuestra legislación que deben buscar resolverse en pro de la seguridad jurídica de las personas físicas y jurídicas, principalmente en aspectos relacionados con la protección de datos.

Pero ¿qué es la computación en la nube?

"La computación en la nube o Cloud Computing, (término en inglés), es una modalidad que ofrece servicios y aplicaciones desde Internet y en la cual se puede obtener el equipo de cómputo, los programas y el software a través de una empresa externa o proveedora de servicios desde la nube, la cual ofrece además, procesar y almacenar los datos de la persona o empresa que compre este servicio". (Universidad de Costa Rica. Programa de la Sociedad de la Información y el Conocimiento, 2010, pág. 160).

Sobre el concepto de nube, el mismo Informe menciona que se basa en el hecho de que toda la tecnología (infraestructura, aplicaciones, software, etc.) está ubicada en los grandes centros de datos que tienen las compañías alrededor del mundo. Esta es una de las principales diferencias con la computación tradicional, dado que no es necesario conocer la infraestructura que hay detrás, sino que pasa a ser una nube donde las aplicaciones y los servicios pueden crecer y funcionar rápidamente (Universidad de Costa Rica. Programa de la Sociedad de la Información y el Conocimiento, 2010, pág. 161).

10.7.2 Aspectos Normativos

Luego de comprender el marco general de los servicios en la nube, es importante establecer que a pesar de los beneficios que conllevan se tienen vacíos en aspectos jurídicos. Tomando en consideración que actualmente el robo de información se encuentra en la mira de la ciberdelincuencia y que las empresas a nivel mundial han comenzado una tendencia a trasladar sus plataformas y servicios a sistemas en la nube, se hace necesario analizar la situación jurídica de la protección de los datos en Costa Rica bajo este nuevo panorama.

En el país se publicó en La Gaceta N. 170 del 5 de setiembre de 2011 la Ley N. 8968 denominada "Ley de protección de la persona frente al tratamiento de sus datos personales", la cual busca regular y proteger la información (los datos) de todos los ciudadanos que se encuentren en las bases de datos (principalmente digitales).

Es necesario primeramente recordar que en nuestro país el derecho a la Intimidad se encuentra regulado en los numerales 23, 24, y 28 del articulado de la Constitución Política, por tanto la protección de nuestra información tiene rango constitucional. En esta nueva ley, contempla el concepto de autodeterminación informativa, que podemos definirlo como el derecho a saber qué hacen con nuestra información. El objetivo de la ley se establece en su artículo 1 el cual señala:

> *Artículo 1.- Objetivo y fin*
>
> Esta ley es de orden público y tiene como objetivo garantizar a cualquier persona, independientemente de su nacionalidad, residencia o domicilio, el respeto a sus derechos fundamentales, concretamente, su derecho a la autodeterminación informativa en relación con su vida o actividad privada y demás derechos de la personalidad, así como la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes (Asamblea Legislativa, 2011, pág. 1).

Por tanto la protección de la información de las personas en los sistemas en la nube también está regulada por esta ley, lo cual se confirma con su artículo 2 el cual señala:

> *Artículo 2.- Ámbito de aplicación*
>
> Esta ley será de aplicación a los datos personales que figuren en bases de datos automatizadas o manuales, de organismos públicos o privados, y a toda modalidad de uso posterior de estos datos. El régimen de protección de los datos de carácter personal que se establece en esta ley no será de aplicación a las bases de datos mantenidas por personas físicas o jurídicas con fines exclusivamente internos, personales o domésticos, siempre y cuando estas no sean vendidas o de cualquier otra manera comercializadas (Asamblea Legislativa, 2011, pág. 2).

La ley prevé que cualquier información que se solicite y se registre en la base de datos deberá informarse a la persona, esto en busca de cumplir el derecho de todo ciudadano de autodeterminación informativa.

10.7.3 Riesgos Jurídico-Informáticos

La nueva ley se encuentra a la espera de la publicación de su reglamento para que comience a aplicarse la misma por medio de la Agencia de Protección de Datos (que la misma ley crea), se vislumbran problemas en la aplicación de la misma para los casos de los sistemas en la nube, entre los problemas que podemos citar están:

Además, en el Artículo 5- Principio de consentimiento informado se menciona:

> 1.- Obligación de informar
>
> Cuando se soliciten datos de carácter personal será necesario informar de previo a las personas titulares o a sus representantes, de modo expreso, preciso e inequívoco:
>
> **h) De la identidad y dirección del responsable de la base de datos**
> (Asamblea Legislativa, 2011, pág. 4)**.**

Es de señalar del punto h, ¿qué sucede en estos casos cuando el responsable de la base de datos no está en el país?; como es muy común en los servicios de proveedores en la nube estos no están dentro de Costa Rica, por lo que aplicarle este aspecto comienza a tener muchas complicaciones, comenzando que podrían alegar que el alcance de la ley no les aplica por no tener su empresa dentro de nuestro ámbito de acción. Otro problema que se puede presentar en las bases de datos con este servicio es con el artículo 7 el cual señala:

Artículo 7.- Derechos que le asisten a la persona

> Se garantiza el derecho de toda persona al acceso de sus datos personales, rectificación o supresión de estos y a consentir la cesión de sus datos.
>
> La persona responsable de la base de datos debe cumplir lo solicitado por la persona, de manera gratuita, y resolver en el sentido que corresponda en el plazo de cinco días hábiles, contado a partir de la recepción de la solicitud.
>
> **1.- Acceso a la información**
>
> La información deberá ser almacenada en forma tal que se garantice plenamente el derecho de acceso por la persona interesada (Asamblea Legislativa, 2011, pág. 6).

La pregunta en este caso será ¿estarán las empresas proveedoras de servicios en la nube dispuestas a brindar acceso a sus bases para que las personas verifiquen la información que tengan sobre ellos? Además ¿quién va a cubrir los costos de estos procesos extras de cumplimiento de esta ley, la empresa proveedora o el cliente nacional? Otro aspecto a señalar es el artículo 11 sobre confidencialidad:

Artículo 11.- Deber de confidencialidad

> La persona responsable y quienes intervengan en cualquier fase del tratamiento de datos personales están obligadas al secreto profesional o funcional, aun después de finalizada su relación con la base de datos. La persona obligada podrá ser relevado del deber de secreto por decisión judicial en lo estrictamente necesario y dentro de la causa que conoce (Asamblea Legislativa, 2011, pág. 11).

Surge la duda de ¿cómo garantizar la confidencialidad de los datos cuando no tenemos control sobre los empleados de la empresa proveedora? Y mucho menos si la empresa no está en el país, va a ser complicado el poder asegurar tal aspecto. Un aspecto muy preocupante va a ser el registro de estas bases en la Agencia de Protección de Datos (encargada de la vigilancia y cumplimiento de esta ley), el artículo 21 indica;

Artículo 21.- Registro de archivos y bases de datos

> Toda base de datos, pública o privada, administrada con fines de distribución, difusión o comercialización, debe inscribirse en el registro que al efecto habilite la Prodhab. La inscripción no implica el trasbase o la transferencia de los dato... (Asamblea Legislativa, 2011, pág. 16).

Empresas en otros países podrían negarse a registrarse en la Agencia, lo cual pondría en desventaja a los ciudadanos para poder defenderse en caso de alguna situación anómala con su información. En general la Agencia de Protección de Datos enfrenta un gran reto para lograr cumplir la ley en servicios como este, además las empresas que utilizan este medio también se encuentran en un problema jurídico que deberán comenzar a clarificar en los contratos que realicen, con el fin de evitar no cumplir con la normativa, los contratos de servicios que realicen desde ahora tendrán que contemplar cumplimiento y cláusulas de responsabilidad encaso de incumplimientos con el fin de evitar responsabilidades por acciones ajenas a la empresa, en las cuales se les afecte la imagen y económicamente por procesos judiciales en que sean condenados a indemnizaciones por un mal manejo de los datos o por robos de información.

10.8 CIBERSEGURIDAD DE LAS EMPRESAS

Dentro de la encuesta a empresas realizada por el Prosic en colaboración con ITS-Infocom, se introdujo una sección para conocer los tipos de controles de seguridad informática que utilizan las empresas, así como los tipos de problemas informáticos que las han afectado.[182] Este apartado describe los principales resultados de dicha sección, con el fin de mostrar el estado de la Ciberseguridad en las empresas.

10.8.1 Principales resultados

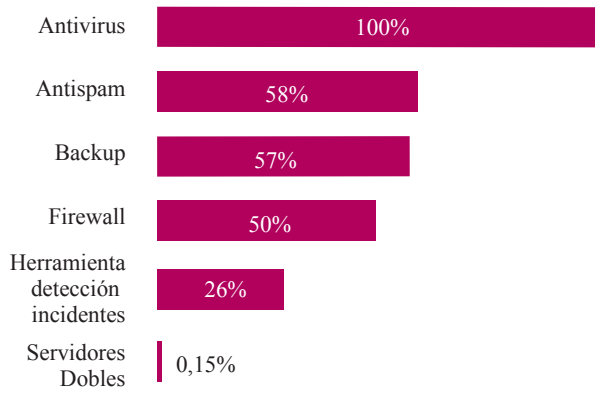
El 68% de las empresas consultadas afirmaron haber implementado medidas de seguridad informática, mientras que un 32% contesto negativamente. Sin embargo, al preguntar directamente si utiliza ciertos tipos de control de seguridad informática (software antivirus, antispam, bloqueo de acceso no autorizado, entre otros) el total de los encuestados indicó que hacía uso de al menos uno de estos.

Según el gráfico 10.1 los tipos de controles de seguridad informática más utilizados por las empresas son: antivirus, antispam y el backup. El 100% de los encuestados hace uso del antivirus, aunque un tercio de estos no lo identifican como una medida de seguridad informática. El 58% de los informantes indicaron hacer uso de un filtro antiSpam, de los cuales el 18% no reconoce éste como un control seguridad. De la misma manera sucede con el 57% las empresas, quienes señalaron hacer respaldo de información (backup), el 26% de estos respondió que no llevaba a cabo una medida de seguridad informática. Se puede notar que medidas como los servidores dobles son menos implementadas dentro de las empresas, puesto que este tipo de medidas implica cierto grado de conocimiento técnico así como una cantidad de recursos mayor.

182 Encuesta mencionada en el capítulo *"Acceso y uso de las TIC en la Administración Pública, las Empresas y los Hogares"* de este informe. Como se describe en dicho capítulo, ésta es una encuesta llevada a cabo por medio de una consulta telefónica durante el mes de diciembre 2012. La muestra fue tomada a partir del directorio de establecimientos del Instituto Nacional de Estadística y Censo (INEC) que inicialmente incluía 800 empresas clasificadas por tamaño de empresa y actividad económica, de las cuales respondieron 108.

Gráfico 10.1

Uso de controles de seguridad por parte de las Empresas



Fuente: Elaboración propia con base en la encuesta a empresas realizada por PROSIC en colaboración con ITS-Infocom, 2012.

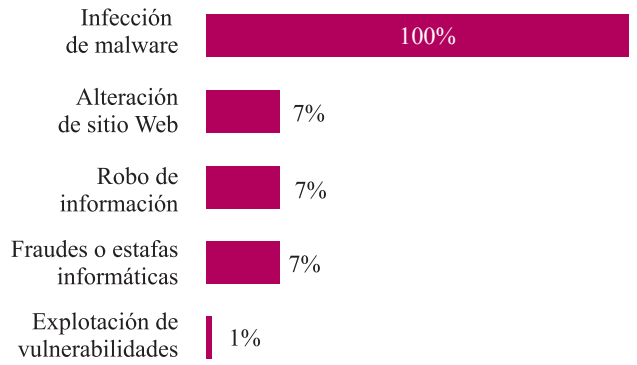
De las empresas que mencionaron no aplicar medidas de seguridad informática el 53% posee un departamento de cómputo o mantienen una persona encargada. El 43% de las que si llevan a cabo dichas medidas no cuentan con este recurso. Esto sugiere que tener con un departamento o personal especialista en el tema no asegura la implementación de control de seguridad dentro de las empresas.

En cuanto a los problemas de seguridad informática, el 24% de las empresas indicó haberse visto afectado mientras que el restante 76% manifestó lo contrario. No obstante, un 16% de las empresas que señalaron no haber tenido dichos problemas contestaron haber sufrido infecciones de malware, por este motivo al preguntar individualmente sobre ciertos problemas el 40% de empresas manifestaron haber sido afectadas por al menos uno.

De las empresas que han padecido algún problema de seguridad informática, el 87% corresponde a infecciones de malware; los fraudes o estafas informáticas, robos de información y alteración de sitios Web son los siguientes problemas de seguridad informática que se presentan más comúnmente dentro de las empresas (7% cada uno, gráfico 10.2).

Gráfico 10.2

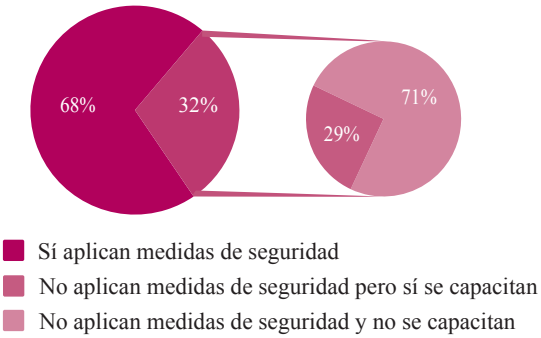
Problemas de seguridad informática que afectan a las empresas



Fuente: Elaboración propia con base en la encuesta a empresas realizada por PROSIC en colaboración con ITS-Infocom, 2012.

Gráfico 10.3

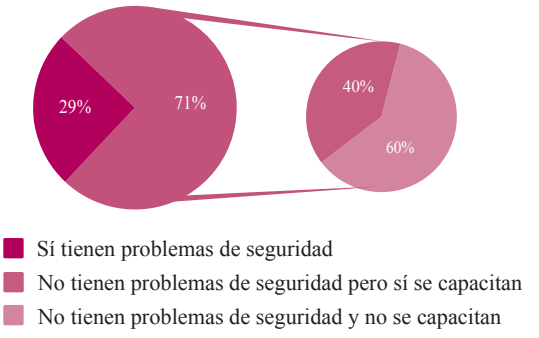
Medidas de seguridad informática versus capacitación



Fuente: Elaboración propia con base en la encuesta a empresas realizada por PROSIC en colaboración con ITS-Infocom, 2012.

Gráfico 10.4

Problemas de seguridad informática versus capacitación



Fuente: Elaboración propia con base en la encuesta a empresas realizada por PROSIC en colaboración con ITS-Infocom, 2012.

Es importante hacer notar que las demás afectaciones se dieron en una menor proporción, aunque la infección de malware puede generar todas los demás problemas, siendo en muchos casos la primera acción para lograr desde fraudes hasta las alteraciones del sitio web.

Al igual que con las medidas de seguridad informática, parece no existir una relación entre los problemas de seguridad informática y la tenencia de un departamento de cómputo o una persona encargada. Los datos reflejan que el 44% de las empresas que contestaron sí haberse visto afectadas por estos problemas poseen un departamento o persona encargada del área de informática. Mientras que el 40% que no se vieron afectadas por alguna situación de este tipo no contaba con personal especializado.

Por otra parte, un porcentaje importante de las empresas que si ha recibió capacitación no está implementando medidas de seguridad. Como se menciono anteriormente el 32% de las empresas no implementa medidas de seguridad, de las cuales el 71% no han recibido capacitación en el uso de computadoras y de internet, el restante 29% si la han recibido (gráfico 10.3).

En el caso de las empresas que no han tenido problemas de seguridad informática el 60% de estas no recibieron ningún tipo de capacitación, por el contrario el 40% sí (gráfico 10.4). Por lo tanto, no se evidencia una relación entre la capacitación y los problemas de seguridad informática.

10.8.2 Principales conclusiones de los resultados

El uso de antivirus es uno de los controles de seguridad informática, sin embargo éste no es suficiente puesto que no puede detectar ciertas amenazas; de igual forma sucede con el uso de cualquier otro control de seguridad. Por tanto, es necesario aplicar varias herramientas para contar con un alto nivel de seguridad.

Como se puede observar el 87% de las empresas han sufrido alguna afectación por malware, lo cual es un problema grave en la seguridad informática; se debe tener en cuenta que las tendencias para el 2013 consisten en un aumento exponencial en la propagación de este tipo de infección. Este tipo de ataques buscan obtener un beneficio económico con la creación, difusión y utilización de malware, e información de la empresa o persona atacada para conseguir datos de acceso u obtener información confidencial o privada.

Que existan empresas que manifiestan no haber tenido problemas de seguridad informática habiendo sido afectadas por infecciones de malware hace sospechar que estas buscan no dañar su imagen. A nivel mundial cada segundo se estiman 18 víctimas de un crimen informático, dichos crímenes generan pérdidas que ascienden a $110.000 millones por año.[183]

Pero hay un tema más preocupante, a pesar de están sufriendo estas afectaciones, las empresas no invierten en capacitar a su personal o las inversiones que realizando no están teniendo un impacto positivo en temas de seguridad. Ante aumento de riesgos de seguridad y la tendencia creciente de ataques informáticos, el no tener un personal preparado para enfrentar dichas amenazas es un riesgo. Bajo el modelo actual, es necesario profesionales con conocimientos avanzados en seguridad informática para mantener la confidencialidad, integridad y disponibilidad de la información de la empresa.

183 Symantec (2012). *"El informe de Norton 2012 revela que el coste anual del Cibercrimen es de 85.000 millones de euros"*. En: News Release. Disponible en: http://www.symantec.com/es/es/about/news/release/article.jsp?prid=20121030_01

10.9 CONSIDERACIONES FINALES

Costa Rica no dispone de una gestión sólida que permita realizar una dirección, control y gestión eficaz en ciberseguridad. El Gobierno deberá asumir la responsabilidad por la Ciberseguridad, además es fundamental dejar claro a qué ente le corresponde este tema (sea creando una entidad superior a las ya existentes o lo asigne a alguna de las actuales) y que este ente brinde el "norte país" en ciberseguridad como proyecto nacional.

Asimismo, es necesario desarrollar y aprobar una Estrategia Nacional de Ciberseguridad, la cual debe convertirse en un instrumento que guíe a los responsables de la Dirección, control y gestión de la Ciberseguridad Nacional así como a todas las entidades del país, esto para eliminar el trabajo como "islas" que se está realizando en este momento en el plano de ciberseguridad. Queda claro que Gobierno Digital no ha asumido el papel de "director de orquesta" que en teoría todos esperaban que ocupara, su papel se ha centrado en ser ejecutor de proyectos.

La situación en las diferentes instituciones y empresas muestran que la tecnología no es el problema, son parte de la solución y su protección y empleo seguro no son sólo responsabilidad del Gobierno, sino de las demás instituciones autónomas junto con el sector privado y empresarial; todos son corresponsables, no obstante, le corresponde al Gobierno el liderazgo y la dirección de la ciberseguridad.

Se debe considerar el ciberespacio como un elemento clave en la gestión global de riesgos de la seguridad nacional y otorgarle la importancia necesaria a la ciberseguridad, y que se vea reflejado en asignar recursos suficientes a las instituciones para que enfrenten esta nueva delincuencia y al mismo tiempo que se acompañe de convenios internacionales y leyes que permitan un eficaz enfrentamiento contra los ciberlincuentes, teniendo en consideración el tema transfronterizo; al respecto se torna como una gran opción para el país ser parte del "Convenio de Budapest".

Es preciso que las normativas relacionadas con tecnología deban pasar por una revisión de su aplicación desde la perspectiva informática, con el objetivo de que la parte jurídica sea factible aplicarla en el "mundo informático", es necesario un equilibrio entre ambas áreas para tener normas realmente eficientes y eficaces.

Es fundamental para las instituciones y empresas invertir en capacitación para sus trabajadores tanto en el ámbito técnico como jurídico, el desconocimiento de las normativas existentes relacionadas al ámbito tecnológico junto a una inadecuada actualización profesional y técnica de conocimientos en temas de seguridad informática pone en riesgo los datos de las empresas, los expone a procedimientos administrativos y judiciales, y además podría dañar su imagen; es por esto que el tema de cultura digital es necesario incluirlo en los planes de las empresas e instituciones acompañado de un desarrollo y puesta en práctica de políticas internas de buen uso de las tecnologías de la información.

Lic. Ing. Roberto Lemaître Picado

Abogado e Ingeniero Informático. Especialista en Delitos Informáticos. Miembro de Internet Society. Representante para Costa Rica en la Red Iberoamericana de Derecho Informático.
roberto.lemaitre@ucr.ac.cr