SEMINARIO NUEVAS TECNOLOGÍAS:
PRIVACIDAD VS SEGURIDAD
Cartagena de Indias, 21-23 julio 2010

Respuestas a los delitos informáticos:

su visión desde la privacidad

y la seguridad de la información

Dra. Esc. Prof. María José Viega[(*)]

Dr. Federico Carnikian[(**)]

[(*)] **Directora de la Dirección de Derechos Ciudadanos de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC)**. Doctora en Derecho y Ciencias Sociales y Escribana Pública por la Universidad Mayor de la República Oriental del Uruguay (UDELAR). Profesora de Informática Jurídica, Derecho Informático y Derecho Telemático (UDELAR). Ex - Profesora de Derecho de las Telecomunicaciones en Universidad de la Empresa. Cursos del Posgrado de Derecho Informático: Contratos Informáticos, Contratos Telemáticos y Outsourcing en la Universidad de Buenos Aires. Miembro Honorario de la Asociación Paraguaya de Derecho Informático y Tecnológico. Miembro de la International Technology Law Association. Miembro del Colegio de Abogados del Uruguay y de la Comisión de Derecho Tecnológico de la Asociación de Escribanos del Uruguay. Miembro del Instituto de Derecho Informático (UDELAR) y Coordinadora del Grupo de Jurisprudencia del mismo Instituto. Co-editora del Boletín Electrónico de Derecho y Tecnologías (www.viegasociados.com). Autora de múltiples trabajos de su especialidad y conferencista a nivel nacional e internacional.

[(**)] **Asesor Jurídico de la Dirección de Derechos Ciudadanos de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC)**. Dr. en Derecho y Ciencias Sociales por la Universidad Mayor de la República Oriental del Uruguay (UDELAR). Miembro del Grupo de Jurisprudencia del Instituto de Derecho Informático (UDELAR).

1. Introducción

Las tecnologías de la información y las comunicaciones son, sin lugar a dudas, una herramienta fundamental en el desarrollo de la sociedad actual. Sus beneficios son innumerables y se vinculan con todas las áreas de nuestra vida. Pero también son un arma potente para causar daño y en este sentido, podemos decir que, la criminalidad en Internet es la parte negativa del desarrollo informático.

El presente trabajo tiene como objeto conceptualizar las amenazas existentes en la red, especialmente las vinculadas a la privacidad, analizar el derecho penal uruguayo a la hora de dar respuestas a las mismas, así como hacer referencia a los proyectos de reforma del Código Penal y al presentado por el Senador Tabaré Viera, que se encuentran a estudio del Parlamento. Pero también se pretende dar un enfoque práctico al tema, a través del análisis del CERTuy en la esfera pública y la referencia a la División de Delitos Informáticos perteneciente al Departamento de Delitos Complejos de la Policía de Montevideo para aspectos relativos a la criminalidad en general.

Se abordará la conceptualización de la criminalidad en la red con una clasificación realizada por Marlon Fetzner, quien divide las principales amenazas en tres sectores[1]:

1. Para los niños

    a. Predadores: usan internet para engañar a los niños, lograr citas, les solicitan fotos.

    b. Cyberbullying: matones cibernéticos, pueden ser otros niños o adultos que utilizan internet para acosar

    c. Abuso de archivos compartidos: intercambiar canciones o videos puede ser ilegal o incluso traer riesgos como virus

    d. Invasión de privacidad: los niños puedes exponer información personal, como direcciones, teléfonos, etc.

    e. Contenido inapropiado: los niños puedes estar expuestos a fotos o videos que no deberían ver.

2. Para seguridad personal

    a. Spam

    b. Phishing o fraude en línea

[1] FETZNER, Marlon. “Internet y privacidad. Las amenazas a los niños”. I Seminario Euro-Iberoamericano de Protección de Datos. Cartagena de Indias (Colombia), 26 a 28 de mayo de 2009.

c. Robo de identidad

3. Para seguridad del PC

    a. Virus

    b. Gusanos

    c. Troyanos

    d. Spyware

Entre las conductas delictivas vinculadas con el robo o suplantación de identidad o con la violación de la privacidad concretamente, se quieren destacar las siguientes:

Ciberbullying

El Bullying cibernético es una variante del Bullying o acoso escolar y es protagonizado por uno o varios acosadores hacia uno o varios de sus compañeros. Consiste en utilizar medios electrónicos como la computadora y el celular para acosar, intimidar y agredir psicológicamente a las víctimas. (…) Es aún más peligroso que el abuso escolar dentro del aula ya que las víctimas pueden ser también blanco para los pederastas quienes navegan por internet buscando a este tipo de víctimas[2].

Esta conducta se define como acoso entre iguales en el entorno TIC e incluye actuaciones de chantaje, vejaciones e insultos de niños a otros niños. En una definición más exhaustiva, se puede decir que el *ciberbullying* supone el uso y difusión de información lesiva o difamatoria en formato electrónico a través de medios de comunicación como el correo electrónico, la mensajería instantánea, las redes sociales, la mensajería de texto a través de teléfonos o dispositivos móviles o la publicación de videos y fotografías en plataformas electrónicas de difusión de contenidos[3].

Un elemento a considerar es la sensación de anonimato que otorga Internet a los acosadores. Pero debe tenerse en cuenta que existen medios informáticos suficientes para poder determinar el lugar exacto y el equipo informático desde el que se llevó a cabo el presunto delito, a través de la detección de la dirección IP.

Phishing

Los ataques de estafa a través de Internet por el método "phishing", que significa "pesca" en el argot informático, se han ido incrementando.

---

[2] TAPIA Edna. El ciberbullying, consecuencias de las libertades en Internet.

[3] INTECO, Instituto Nacional de Tecnologías de la Comunicación. “Guía legal sobre 0ciberbullying y gooming”.

El sistema más utilizado por los cyber-estafadores es el envío de correos electrónicos con falsos remitentes, como por ejemplo de entidades financieras, de forma tal que las víctimas cliquearan en un link y de esa forma podían obtener información personal[4].

En junio de 2005, se celebró en las instalaciones de la Dirección General de la Policía en Madrid unas jornadas sobre fraude en Internet, concretamente sobre phishing bancario. Se ha definido al phishing como "un acto de crimen organizado, y como tal debe ser tratado, que los actores que participan en el escenario del fraude tienen todos su porción de responsabilidad y que es preciso transmitir y recordar a los usuarios de banca electrónica que no deben desconfiar del canal bancario electrónico, sino que deben ser conscientes de que han de contemplarse medidas preventivas para evitar ser víctimas de los engaños. La banca electrónica es, salvo excepciones extraordinarias, segura y confiable[5].

Pero ya se habla de una nueva generación de phishing. Hispasec[6] demuestra cómo es posible realizar ataques phishing en servidores seguros de entidades bancarias, aun cuando el usuario visualice que la URL comienza por https:// seguido del nombre de la entidad y que el icono del candado que aparece en la parte inferior del navegador certifique que se encuentra en el servidor seguro del banco, lo que constituían hasta el momento las recomendaciones que se hacían para acceder de forma segura a la banca electrónica[7].

Como podemos ver esto se ha vuelto inseguro y el Pharming es la confirmación de esta afirmación.

Pharming

Es una modalidad de fraude online, que ataca la vulnerabilidad del software de los servidores DNS o de los equipos de los propios usuarios, redireccionando el nombre de dominio a un sitio web falso, diseñado por el atacante.

El pharming deriva del término *farm* (granja en inglés), expresión utilizada cuando el atacante ha conseguido acceso a un servidor DNS o varios servidores (granja de servidores o DNS).

Esta modalidad delictual se utiliza normalmente para realizar ataques de *phishing*, redirigiendo el nombre de dominio de una entidad de confianza a una página web, en apariencia idéntica, pero que en realidad ha sido creada por el atacante para obtener los datos personales del usuario, generalmente datos bancarios.

---

[4] VIEGA, María José. "El problema de los datos personales y el espionaje en Internet", presentada al Cuarto Congreso Internacional de Derecho (CIDER 2005) en las Sedes de Cochabamba, Santa Cruz y La Paz. Bolivia, 23 al 25 de noviembre de 2005. Publicada en el Libro de Ponencias.

[5] http://www.hispasec.com/unaaldia/2421 Página visitada 13 de junio 2005.

[6] http://www.hispasec.com/unaaldia/2406 Página visitada 13 de junio 2005.

[7] VIEGA, María José. "Privacidad Vs. Espionaje en Internet". Anuario de "Derecho Informático". Tomo VI Jurisprudencia correspondiente al año 2005 y en el Boletín de Derecho y Tecnologías Nº 16 Enero 2005 http://viegasociados.com/moodle//mod/forum/discuss.php?d=440

Si el phishing engaña a los usuarios uno por uno, conduciéndolos a visitar un sitio apócrifo de su banco o comercio preferido, el pharming interviene las comunicaciones entre el usuario y su proveedor de Internet (ya sea un proveedor de comunicaciones, o un servidor corporativo) para lograr que cuando un usuario teclea en su navegador una dirección legítima, éste sea conducido a una falsificación de la página Web que quiere visitar y sea ahí donde introduzca los datos de su cuenta[8].

Por tanto, el riesgo para el usuario en los casos de pharming es diferente, mientras que en el phishing requiere una actitud activa, hacer click en el link del correo electrónico, en el pharming el fraude se produce sin participación directa del usuario.

La utilización de medidas técnicas de seguridad en un sistema, como por ejemplo un firewall, herramientas de protección contra adware y spyware, contrarrestan este tipo de amenazas.

La finalidad de ambas conductas delictivas es la captura ilegítima de datos confidenciales, difiriendo en el modo de ejecutarlo.

El pharming se realiza modificando el software, lo cual puede realizarse en forma remota o introduciendo un programa que lo realice en forma automática. Para ello es necesario introducir un troyano en el disco duro de la víctima, el cual puede autoeliminarse, borrando del disco duro las huellas del ataque.

“La respuesta es muy delicada para el banco, si hace responsable al cliente y el "pharming" se generaliza, los usuarios abandonaremos en masa la banca online por insegura y peligrosa, pero si el banco carga con los gastos. ¿A cuánto tendrá que subir las comisiones por operación el banco online para cubrir este riesgo? ¿Seguirá siendo competitivo? Si no se atajan estos riesgos, quizá el porvenir de la e-banca no sea después de todo tan brillante como se auguraba”[9].

Scam

A este tipo de fraude también se lo conoce como phishing laboral, porque tiene como objetivo obtener datos confidenciales de usuarios, para acceder a sus cuentas bancarias.

Las modalidades utilizadas consisten en envíos masivos de correos electrónicos o la publicación de anuncios en webs, en los que se ofrecen empleos muy bien remunerados. Cuando el usuario acepta la oferta de trabajo, se le solicita que facilite datos de sus cuentas bancarias, a través de un e-mail o accediendo a una web, para ingresarle los supuestos beneficios.

---

[8] http://www.mx.terra.com/tecnologia/interna/0,,OI889426-EI4906,00.html Página visitada 21 de junio de 2010. El Pharming: amenaza de fraude a negocios. Trend Micro. 21 de febrero de 2006.

[9] http://www.laflecha.net/canales/seguridad/articulos/pharming/ El Pharming, un peligro para la e-banca. Página visitada 21 de junio de 2010.

Smishing

Esta es otra variante del phishing, pero el ataque se realiza a través de los mensajes a teléfonos móviles. El resto del procedimiento es igual al del phishing, el estafador suplanta la identidad de una entidad de confianza para solicitar al usuario que facilite sus datos, a través de otro SMS o accediendo a una página web falsa, idéntica a la de la entidad en cuestión.

Spear Phishing

También estamos, en este caso, ante un sub tipo de phishing en el que, en lugar de realizar un envío masivo de correos electrónicos, se envían correos con mayor grado de personalización, a destinatarios concretos, consiguiendo que los mensajes resulten más creíbles que los del phishing tradicional.

Vishing

Esta clase de fraude también persigue la obtención de datos confidenciales de los usuarios, pero a través de la telefonía IP. Los ataques de vishing se suelen producir siguiendo dos esquemas[10]:

- Envío de correos electrónicos, en los que se alerta a los usuarios sobre algún tema relacionado con sus cuentas bancarias, con el fin de que éstos llamen al número de teléfono gratuito que se les facilita.

- Utilización de un programa que realice llamadas automáticas a números de teléfono de una zona determinada.

En ambos casos, cuando se logra contactar telefónicamente con el usuario, un mensaje automático le solicita el número de cuenta, contraseña, código de seguridad, etc.

Grooming

El grooming es un nuevo tipo de problema relativo a la seguridad de los menores en Internet, consistente en acciones deliberadas por parte de un adulto de cara a establecer lazos de amistad con un niño o niña en Internet, con el objetivo de obtener una satisfacción sexual mediante imágenes eróticas o pornográficas del menor o incluso como preparación para un encuentro sexual, posiblemente por medio de abusos.

El grooming habitualmente es un proceso que puede durar semanas o incluso meses, y que suele pasar por las siguientes fases, de manera más o menos rápida según diversas circunstancias:

[10] http://www.delitosinformaticos.info/delitos_informaticos/glosario.html Página visitada 21 de junio de 2010.

1. El adulto procede a elaborar lazos de amistad con el menor simulando ser otro niño o niña.

2. El adulto va obteniendo datos personales y de contacto del menor.

3. Utilizando tácticas como la seducción, la provocación, el envío de imágenes de contenido pornográfico, consigue finalmente que el menor se desnude o realice actos de naturaleza sexual frente a la webcam o envíe fotografías de igual tipo.

De esta forma se inicia un proceso de cyberacoso, en el cual se chantajea a la víctima para obtener cada vez más material pornográfico o tener un encuentro físico con el menor para abusar sexualmente de él.

Scavenging

Es la apropiación de informaciones residuales, la que consiste en la obtención de información a partir de lo que desechan los usuarios legítimos de un sistema informático.

Suplantación de identidad

"Puede ser entendida como la suplantación de personalidad fingiendo ser una persona que no es imitándola e inclusive remedándola. El caso más común es el robo de tarjetas de crédito y de cajeros automáticos. Los autores del delito se hacen pasar por empleados de la central de tarjetas de crédito, llamando telefónicamente al titular para solicitarle que con el objeto de anular la posibilidad de utilización fraudulenta de la tarjeta robada le revele su clave secreta o personal"[11].

Hoy por hoy, con el desarrollo de las redes sociales en Internet, una nueva modalidad es la creación de páginas o usuarios suplantando a otra persona.

2. Normativa penal uruguaya

Debemos preguntarnos acerca de la posibilidad de aplicar los delitos tipificados en nuestro Código Penal a los delitos informáticos.

a) Hurto

El artículo 340 dice: "*El que se apoderare de cosa ajena mueble, sustrayéndosela a su tenedor, para aprovecharse o hacer que otro se aproveche de ella, será castigado con tres meses de prisión a seis años de penitenciaría*."

El problema está planteado con el objeto, o sea la cosa ajena mueble. En nuestro derecho fue necesario agregar por el artículo 316 de la Ley Nº 13.737

[11] BLOSSIERS MAZZINI Juan José. CALDERON GARCIA Sylvia B. "Los Delitos inform@ticos". Editora RAO SRL Lima, 2000. páginas 53 y 54.

de 9 de enero de 1969 el Hurto de Energía y Agua Potable (art. 343 del Código Penal).

Teniendo presente el principio de legalidad, este artículo no es aplicable a los casos de hurto de información, por ejemplo, donde la misma no se sustrae a su tenedor, sino que este sigue conservándola, no produciéndose el desapoderamiento[12].

b) Estafa

La estafa está tipificada en el artículo 347, que establece: "*El que con estratagemas o engaños artificiosos, indujere en error a alguna persona, para procurarse a sí mismo o a un tercero, un provecho injusto, será castigado con seis meses de prisión a cuatro años de penitenciaría*".

Se ha discutido acerca de si se puede engañar a una máquina, o si por el contrario la víctima de la estafa debe ser una persona. Actualmente, la doctrina y jurisprudencia son contestes en admitir que la estafa mecánica se encuentra comprendida en este tipo penal.

c) Daño

El artículo 358 dispone que: "*El que destruyere, deteriorare o de cualquier manera inutilizare, en todo o en parte, alguna cosa mueble o inmueble ajena, será castigado, a denuncia de parte, cuando el hecho no constituya delito más grave con multa de .....*"

Nuevamente el problema lo plantea el objeto, ya que el objeto del daño debe ser una cosa mueble o inmueble, los delitos informáticos dañan los datos, la información, los programas, pero no a la computadora en sí. En virtud de esto sería imposible aplicar este artículo al daño informático.

Independientemente de la posibilidad de aplicación de los artículos señalados anteriormente a las nuevas conductas delictuales, existen en nuestro país legislados algunos delitos informáticos.

La primer norma uruguaya que tipifica un delito informático es la Ley Nº 16.002 del 25 de noviembre de l988, la cual en el artículo 130 establece: "*El que voluntariamente trasmitiere a distancia entre dependencias oficiales un texto del que resulte un documento infiel, incurrirá en los delitos previstos por los artículos 236 a 239 del Código Penal, según corresponda*".

Los artículos 129 y 130 de dicha norma regulan la autenticidad y prueba de los documentos trasmitidos a distancia por medios electrónicos entre dependencias oficiales. Y los delitos a que alude son los que penalizan la falsificación documentaria.

[12] VIEGA María José y DELPIAZZO Carlos. Lecciones de Derecho Telemático. Tomo I. Lección 13. Página 189.

Dice el artículo 129: "*La documentación emergente de la transmisión a distancia, por medios electrónicos, entre dependencias oficiales, constituirá, de por sí, documentación auténtica y hará plena fe a todos sus efectos en cuanto a la existencia del original trasmitido*".

Y el artículo 130 establece: "*El que voluntariamente trasmitiere a distancias entre dependencias oficiales un texto del que resulte un documento infiel, incurrirá en los delitos previstos por los artículos 236 a 239 del Código Penal, según corresponda*".

La Ley Nº 16.736 de 5 de enero de 1996 amplía el artículo 129 de la Ley Nº 16.002 en dos aspectos: sustituye el término "medios electrónicos" por "medios informáticos y telemáticos" y elimina la frase "entre dependencias oficiales", lo que convierte a la norma en aplicable para la generalidad.

El inciso segundo establece: "*El que voluntariamente transmitiere un texto del que resulte un documento infiel, adultere o destruya un documento almacenado en soporte magnético, o su respaldo, incurrirá en los delitos previstos por los artículos 236 a 239 del Código Penal, según corresponda*".

Comparando con el art. 130 de la Ley Nº 16.002 podemos observar que en primer lugar hay una ampliación de los comportamientos reprimibles, en segundo lugar se elimina también aquí la expresión "*entre dependencias oficiales*" y se tiene en cuenta para quien adultere o destruya el "*documento almacenado en soporte magnético o su respaldo*".

La Ley Nº 18.600 de 21 de setiembre de 2009 de documento electrónico y firma electrónica establece en el artículo 4 inciso 2º establece: "*El que voluntariamente transmitiere un texto del que resulte un documento infiel, adultere o destruya un documento electrónico, incurrirá en los delitos previstos por los artículos 236 a 245 del Código Penal, según corresponda*".

Respecto a la Propiedad Intelectual, el 13 de enero de 2003 se promulgó la Ley de Protección del Derecho de Autor y Derechos Conexos Nº 17.616 de 17 de enero 2003, la cual modifica el texto de la Ley Nº 9.739 de 17 de diciembre de 1937, incluyendo en forma expresa al software como una de las obras objeto de su protección, regulando de esta forma la reproducción ilícita de software.

Por otra parte, la Ley Nº 17.815 de 6 de setiembre de 2004, regula delitos referente a violencia sexual comercial cometida contra niños, adolescentes o incapaces, estableciendo tipo amplios que implica la utilización de diferentes tecnologías.

Actualmente, en nuestro país se está trabajando en un proyecto de reforma del Código Penal, a cuyos efectos, el artículo 22 de la Ley N° 17.897 de 14 de setiembre de 2005 creó una Comisión, la que se integrará por representantes de distintos organismos y organizaciones, tomando en consideración para su elaboración principios modernos de política criminal, introduciendo modificaciones y agregando conductas no tipificadas en el código penal vigente.

El proyecto citado, más precisamente en el capítulo de delitos contra la inviolabilidad del secreto contempla algunas hipótesis de espionaje informático.

En el delito de violación de correspondencia escrita -art. 296 del Código vigente- se incluyó la modalidad de mensajes de correo electrónico o cualquier otro documento cerrado[13].

Los delitos de interceptación de noticia telegráfica o telefónica -art. 297 código penal vigente- incluyen la noticia electrónica y por su parte el delito de revelación de secreto de la correspondencia y de la comunicación epistolar, telegráfica o telefónica -art.298- también se le agregó la modalidad electrónica.

El proyecto añade dentro de los delitos contra la propiedad, un tipo penal denominado "Menoscabo al derecho a disposición de datos" el que se relaciona directamente con la protección de datos personales.

El texto del proyecto dispone que: "…*al que por medio de copia, supresión, inutilización o cambio, menoscabare el derecho de disposición de otro, sobre datos, cuando éstos sean protegidos contra acceso no autorizado y que sean almacenados o se transmitan electrónicamente o en otra forma no inmediatamente visible*".

En este sentido, la circunstancia de verse privado de disponer de la información personal y por tanto perder el control en el procesamiento y comunicación de los datos personales, afecta indudablemente los derechos de los titulares. De esta manera, se busca la protección de un derecho humano reconocido por la Ley N° 18.331, de Protección de Datos Personales y Acción de Habeas Data, como un derecho inherente a la persona humana.

Se considera que el delito incluido, debería hacer alusión a sistema informático, a efectos de ser omnicomprensivo de situaciones que no afectan solamente la disposición de los datos, sino a un sistema, comprendiendo de esta manera la integridad, confidencialidad y disponibilidad de la información contenida en éste. (…) En estos casos se podría abarcar ataques de hacking o cracking -como intrusión o interferencia en un sistema-, incluyendo también la introducción de un virus en el sistema informático[14].

Concomitantemente, hace pocos días, se publicó una nota de prensa bajo el título: Proponen duros castigos a la "ciberdelincuencia", en la cual se anuncia un proyecto de ley del senador Tabaré Viera, que plantea penas de prisión escalonadas para las falsificaciones informáticas, accesos ilícitos, interceptación de datos, pornografía infantil y fraude.

[13] RODRIGUEZ, María José. "Comentarios al Proyecto de Reforma del Código Penal". Trabajo Inédito de junio de 2010.
[14] RODRIGUEZ, María José. "Comentarios al Proyecto de Reforma del Código Penal". Trabajo Inédito de junio de 2010.

El texto del proyecto propone castigar de forma escalonada una decena de delitos relacionadas con el manejo informático (muchos ya previstos en la ley), con multas que van de las 50 a 500 Unidades Reajustables ($231.500), o penas de prisión de entre tres meses y siete años. Luego de definir lo que entiende por sistema informático, datos y proveedores de servicios, entre otras cosas, el proyecto detalla los casi diez delitos que componen la "ciberdelincuencia"[15].

3. CERTuy

El centro de la coordinación de CERT® (CERT/CC) es un Centro de Maestría de la seguridad de Internet, que fue creado en 1988 en Estados Unidos y forma parte del Software Engineering Institute de la Universidad de Carnegie Mellon. Su información pretende proteger nuestros sistemas contra problemas potenciales y reaccionar a los problemas actuales y a problemas futuros. Su trabajo implica estudiar los sistemas de seguridad de la computadora y las vulnerabilidades, alarmas de seguridad, investigar cambios a largo plazo en sistemas networked, y proporcionar la información y entrenamiento para ayudarle a mejorar la seguridad en su sitio[16].

Los problemas relativos a la seguridad de la información guardan una estrecha relación con los activos de información, los que en términos generales pueden estar determinados por el tipo de datos manejados, la calidad de los servicios prestados, el mercado donde se desempeñan, las actividades y vínculos establecidos.

Es por ello, que no solo es importante definir y establecer cuáles son los activos de información que el Estado posee, sino gestionar su reutilización y dotar de un marco de seguridad adecuado orientado a la confidencialidad, integridad y disponibilidad de la información.

Para lograr un marco adecuado de seguridad, es necesaria la aplicación de un conjunto de medidas técnicas y organizativas a efectos de lograr un entorno seguro para los datos, la información, y los sistemas que los sustentan[17].

La norma ISO/IEC 27001 define a la seguridad de la información como la preservación de la confidencialidad, la integridad, y la disponibilidad, pudiendo además, abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio.

A estos efectos, una buena gestión de seguridad puede ser obtenida a través de la concreción de un conjunto de controles, tales como políticas, prácticas, procedimientos, estructuras organizativas y software adecuados.

---

[15] http://www.observa.com.uy/actualidad/nota.aspx?id=99214&ex=25&ar=2&fi=1&sec=8 Información del día 8 de julio de 2010.

[16] VIEGA, María José y DELPIAZZO Carlos. Lecciones de Derecho Telemático. Tomo I. Lección 13. Página 177.

[17] Curso CEDDET. Módulo 3: Seguridad, confidencialidad, transferencias internacionales y autorregulación. Página 43.

En este sentido, es necesario que el Estado -como uno de los principales sujetos que almacena y transmite información- adopte medidas de seguridad adecuadas a fin de proteger aquella información sustancial para el desarrollo de sus actividades y cometidos, y que en definitiva es fundamental a efectos de la protección de sus intereses como Estado y la salvaguarda de los derechos de los ciudadanos.

Como contrapartida de lo mencionado, también existen quienes, ya sea con intenciones de daño o no, efectúan un uso malintencionado de la información y los sistemas, lo que es capaz de producir importantes daños de gran escala que afecten los servicios públicos prestados por los organismos y entidades estatales.

El Estado, al igual que los particulares, pueden ser víctimas de ataques de estos "delincuentes informáticos", los que muchas veces atentan contra un sistema de información por el simple hecho de divertirse, o como forma de realizar publicidad de ellos mismos.

Conforme a esto, existe la necesidad de contar con políticas, prácticas, medidas de seguridad adecuadas, entre otras, y la existencia de un equipo de trabajo que, a nivel estatal, centralice las competencias al respecto y dé respuestas inmediatas a las amenazas que la propia red pueda ocasionar.

Es por ello que, con la finalidad de dar respuesta a los incidentes informáticos de seguridad de activos críticos de información del Estado y teniendo como objetivo la instalación de políticas y buenas prácticas para la seguridad de la información a nivel estatal, se creó el CERTuy dentro de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica la Sociedad de la Información y del Conocimiento (Agesic), dotándolo de competencias y cometidos acordes al efecto.

Los incidentes informáticos están definidos por el Decreto Nº 451/009 de 28 de septiembre de 2009 -que reglamenta el funcionamiento del CERTuy- como una violación o amenaza inminente de violación a una política de seguridad de la información implícita o explícita, que comprometa la seguridad de un sistema (confidencialidad, integridad o disponibilidad).

La sigla CERT deviene de "Computer Emergency Response Team", esto es, un equipo de trabajo responsable del desarrollo de medidas preventivas y reactivas relacionadas con los incidentes de seguridad en los sistemas de información[18].

3.1 Marco regulatorio

[18] http://cert.inteco.es/Acerca_de/. Página visitada 29 de junio de 2010.

La creación del Centro Nacional de Respuestas a Incidentes de Seguridad Informática (en adelante CERTuy) es producto de un esquema normativo lógico y sistemático que lo provee de coherencia en cuanto a su funcionamiento.

La Agesic posee potestades legales para la concepción y el desarrollo de políticas en materia de seguridad de la información, a los efectos de la prevención, detección y respuesta frente a los incidentes que pudieran afectar los activos críticos del país[19].

Por el artículo 119 de la Ley Nº 18.172 de 7 de septiembre de 2007 se creó el Consejo Asesor Honorario de Seguridad de Informática del Estado dotado de una integración variada el que apoyará en esta materia a la Agesic, contribuyendo también con su opinión para la clasificación y diagnóstico de incidentes realizada por el CERTuy.

A través del artículo 73 de la Ley Nº 18.362 de 15 de octubre de 2008 se creó el CERTuy dentro del ámbito de la Agesic en virtud de las potestades legales asumidas por este órgano.

Es dable destacar que, el ámbito objetivo de aplicación del CERTuy alcanza a los sistemas informáticos que soportan activos críticos de información y aquellos sistemas circundantes a éstos mantenidos dentro de la órbita de la Administración Central del Estado.

En cuanto a las obligaciones legales que posee, mencionamos el deber de intervención ante un posible incidente de seguridad informática, debiendo llevar un registro de los reportes al efecto y debiendo también publicar las recomendaciones en materia de seguridad informática que realice.

En cuanto a la definición de los activos críticos de información, el propio Decreto que regula el funcionamiento y organización del CERTuy contiene un capítulo de definiciones el que establece en su artículo 2 literal b) que, los activos de información críticos del Estado son aquellos activos de información necesarios para asegurar y mantener el correcto funcionamiento de los servicios vitales -servicios de salud, banca, energía, telecomunicaciones, entre otros- para la operación del gobierno y la economía del país.

Posteriormente, se aprueba el Decreto Nº 451/2009 de 28 de septiembre de 2009 que reglamenta el funcionamiento del CERTuy, otorgándole diversas competencias y obligaciones, así como también regulando todos los aspectos necesarios para la mejor ejecución de sus cometidos legales.

Asimismo, por Decreto Nº 452/2009 de 28 de septiembre de 2009 y con motivo de impulsar un sistema de gestión de la seguridad de la información, se aprobó el documento denominado “Políticas en la Seguridad en la Información para los Organismos del Estado”, de aplicación obligatoria para los organismos públicos integrantes de la Administración Central, exhortándose su cumplimiento a los restantes órganos del Estado.

[19] Inciso agregado por el artículo 118 de la Ley Nº 18.172 al artículo 55 de la Ley 18.046.

El decreto precitado, además de aprobar el documento sobre políticas de seguridad en la información, consagra otras disposiciones que guardan relación directa tanto con el Decreto que regula la creación y funcionamiento del CERTuy como aquellas concernientes a la protección de los datos personales (Resultando Nº IV).

El mencionado documento dispone que los Organismos deberán contar con una política de gestión de incidentes de seguridad de la información de acuerdo con los lineamientos dados por el CERTuy, y clasificar los activos de información en relación a la importancia que posean, de acuerdo con la normativa vigente, entre ellas, la relativa al CERTuy.

Por lo tanto, como ya hiciéramos referencia, la normativa reglamentaria vigente de seguridad de la información guarda coherencia temporal, lógica y sistemática, contribuyendo a la salvaguarda de información de sustancial importancia para el desarrollo del país.

3.2 Cometidos

Todos los Organismos del Estado manejan, intercambian, almacenan y son pasibles de amenazas y ataques informáticos, contra los activos de información, que pongan en riesgo el cumplimiento de sus objetivos.

Por lo tanto, es de radical importancia definir y clasificar los activos de información que poseen, diagnosticar el nivel de seguridad de la información que desarrollan, y apuntar a la concreción de políticas, prácticas y otras medidas tendientes a la mejora en la gestión de la seguridad de la información.

Es importante destacar que el artículo 73 de la Ley Nº 18.362 faculta al CERTuy a: regular la protección de los activos críticos de información del Estado, difundir las mejores prácticas, centralizar y coordinar la respuesta a incidentes informáticos y realizar las tareas preventivas que correspondan.

En este sentido, tanto los cometidos como las potestades asignadas reglamentariamente al CERTuy apuntan a fomentar el trabajo conjunto de éste con todos los organismos estatales, con el fin de obtener una buena gestión de políticas de seguridad de la información que coadyuve a la ejecución efectiva y eficiente de los proyectos que dichos organismos pretendan llevar a cabo.

Podemos diferenciar los cometidos otorgados al CERTuy, en dos grupos: a) los relativos al trabajo en conjunto con los restantes organismos del Estado; y b) los relacionados con los incidentes de seguridad y las medidas atinentes a su control y prevención.

a) Se trata de tareas de asistencia, coordinación, colaboración entre los organismos públicos con la finalidad de proporcionar una asistencia eficaz en los casos de incidentes de seguridad informática, proponer normas destinadas

a incrementar los niveles de seguridad en los recursos y sistemas relacionados con las TIC.

Además de los verbos nucleares utilizados por la norma reglamentaria descrita, se desprende que se trata de un proceso donde los distintos niveles de seguridad que los Organismos posean se van a ir acompasando con la normativa vigente gracias a la colaboración, asistencia, coordinación y asesoramiento que el CERTuy les provea.

En este sentido, la norma se encuentra en armonía con el Decreto Nº 450/009 que aprueba un documento de políticas de seguridad de la información para los organismos públicos.

b) El CERTuy posee cometidos relacionados con la alerta ante amenazas y vulnerabilidades informáticas dando respuesta a los incidentes ocurridos. Estos servicios son denominados como reactivos, esto es, servicios diseñados para dar respuestas a solicitudes de asistencia, como por ejemplo a los incidentes de seguridad, investigación forense tendiente a determinar las huellas informáticas que los ataques informáticos generan.

El CERTuy documenta y registra los reportes de los incidentes ocurridos.

3.3 Funcionamiento del CERTuy

Luego de haber analizado las razones de su creación, su marco regulatorio en cuanto a sus obligaciones, cometidos y potestades, destacaremos en primer lugar algunas de las tareas y procedimientos que el CERTuy tiene asignados legalmente y en segundo lugar los aspectos prácticos de como éste se está desenvolviendo en la actualidad.

3.3.1 Respuestas a incidentes de seguridad informática

Al comienzo de este apartado hicimos referencia a que los organismos públicos son pasibles de ataques a sus sistemas de información, que originan un evento o incidente de seguridad informática.

En cuanto al alcance del tipo de información que salvaguarda, podríamos decir que dicho centro de respuestas protege de las violaciones o amenazas a una política de seguridad de la información, así como un hecho que comprometa la seguridad de un sistema, sean activos críticos o no de información, esto se desprendería de la definición de incidente de seguridad informática proporcionada por el propio Decreto que reglamenta el CERTuy.

Además, el artículo 1º del Decreto dispone que el CERTuy protegerá tanto los sistemas informáticos como los sistemas circundantes a éstos.

La respuesta a incidentes puede significar la realización de análisis forense sobre el sistema o sistemas informáticos circundantes al analizado, tales como

la descripción de aquellas “huellas informáticas” que el atacante, dejó en el sistema.

Ante una alerta de amenaza o vulnerabilidad el CERTuy puede actuar, tanto por la detección que el propio centro efectúe o por la puesta en conocimiento por parte de los Organismos de un eventual ataque. Al respecto aparece como relevante la designación de un Responsable de seguridad de la información establecida en el documento sobre “Políticas de Seguridad en la Información para Organismos de la Administración Pública” que tenga a su cargo las tareas concernientes a la seguridad de la información.

Sin perjuicio de ello, es lógico que ante la eventualidad de una violación al sistema informático no sea el Responsable de seguridad necesariamente el que informe al CERTuy al respecto (art. 8 literal a), siendo fundamental el conocimiento por parte de todos los empleados de un Organismo público acerca de este tipo de sucesos que puedan ocurrir (último ítem del documento “Políticas de seguridad de la información…”).

Siguiendo la misma línea de pensamiento, se destaca que ante la eventualidad de una posible violación al sistema informático de seguridad, se recomienda que la persona realice una descripción del incidente, indicando al menos la siguiente información general:

- fecha y hora del incidente
- métodos y herramientas utilizadas para la intrusión al sistema
- niveles de software utilizados
- detalle de las vulnerabilidades explotadas
- origen del ataque[20]

Ante la intervención en un evento o incidente informático, el CERTuy deberá guardar reserva de la información relativa a éste y llevar un registro de los reportes de incidentes, tal como lo dispone el literal A), B) y C) del artículo 7 del Decreto Nº 451/009.

Simplemente a título informativo decir, que el capítulo V del Decreto de marras, establece un cuerpo normativo destinado a la regulación del procedimiento relativo a la respuesta a reportes de incidentes de seguridad informática.

3.3.2 Tareas preventivas

El Decreto le asigna al CERTuy tareas de corte preventivas por lo que, ante este tipo de incidentes y a través del resultado de la coordinación y comunicación con los Organismos públicos se recomiende la ejecución de un conjunto de medidas tendientes a proteger los activos de información que se posea.

[20] http://www.arcert.gov.ar/. Página visitada el 1 de julio de 2010.

Las tareas preventivas implementadas por el CERTuy, son ejercidas a través de un procedimiento establecido y regulado en los artículos 9 a 13 de la reseñada norma.

También la ejecución de este tipo de tareas es necesaria para la posterior detección, manejo y recopilación de información sobre incidentes de seguridad que puedan resultar de relevancia ante eventuales sucesos futuros.

Por último cabe agregar que dentro de las potestades conferidas al CERTuy se encuentra la destinada a recuperar los servicios afectados tras un ataque informático, identificando y mitigando la causa de éste, preservando al efecto la información forense emanada.

3.4 Aspectos prácticos

En el presente apartado se dará un panorama actual de las actividades que realiza el CERTuy que a nuestro juicio interesa destacar.

Como hemos mencionado a lo largo del presente trabajo, entre las principales competencias otorgadas legalmente al CERTuy se encuentra la relativa a la protección de los activos críticos de información, protegiendo los sistemas informáticos y los sistemas circundantes a éstos.

Asimismo, se informa que el CERTuy viene trabajando en base a tres columnas de trabajo:

1) Actividades Reactivas: tales como la respuesta a incidentes de seguridad informática e investigación forense;

2) Actividades Proactivas: por ejemplo el asesoramiento en seguridad y alerta de incidentes;

3) Actividades en materia de Seguridad e Infraestructura, es decir, la seguridad en la red y sobre la plataforma de gobierno electrónico.

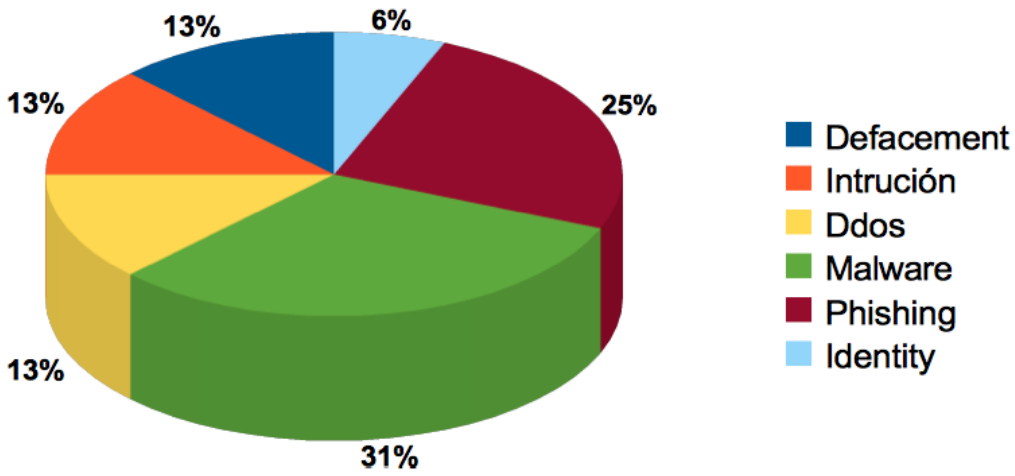
La plataforma de gobierno electrónico es un facilitador de trámites y servicios en línea y un instrumento para lograr la interoperabilidad y el intercambio de información entre los Organismos del Estado. Dicha plataforma conecta a los distintos Organismos a través de la Reduy, la cual es supervisada por el CERTuy.

Para ello se instalaron firewalls -en el límite de la red local y la Reduy- en los Organismos públicos a efectos de que el CERTuy, reciba aquella información que resulte relevante para la detección de posibles amenazas o incidentes informáticos, y con ello lograr una actuación más efectiva y eficiente, teniendo como meta fundamental la búsqueda directa de incidentes, sin necesidad de que éstos se reporten.

La información recolectada por el CERTuy, es tratada con reserva en virtud de lo dispuesto en el literal B) del artículo 7 de su Decreto reglamentario.

En cuanto a datos estadísticos, el CERTuy en la actualidad gestiona un promedio de dos incidentes mensuales.

A nivel de ataques tenemos[21]:



Se han registrados casos de correos electrónicos enviados a nombre de otro, consumándose robos de identidad.

En la actualidad, se está trabajando en temas de identidad digital y los riesgos que conlleva las identidades duplicadas (Digital Indentity Managment) y en aspectos relacionados con la dirección de eventos de seguridad informática, esto es todo el "Managment" en lo que refiere a este tipo de eventos. En este sentido, el Decreto reglamentario del CERTuy en su artículo 3 literal B), define los eventos de seguridad informática como toda ocurrencia identificada de un estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información, la falla de medidas de seguridad o una situación previamente desconocida, que puede ser relevante para la seguridad.

En cuanto a los aspectos técnicos se viene trabajando en el dispositivo IDS/IPS testing, el cual es una versión ligeramente simplificada de un Unified Threater Managment (UTM), el que no sólo dispone de funcionalidades IDS/IPS -funcionalidad que monitorea la red por actividades maliciosas o violaciones de las políticas de seguridad- sino también posee una herramienta de evaluación de vulnerabilidad pudiendo ser configurado como firewall o un router, y permitiendo además la protección de las redes contra otras amenazas informáticas[22].

4. Seguridad de la información y Privacidad

[21] PAZ Santiago. Presentación del CERTuy

[22] http://www.securecomputing.net.au/Review/90967,idsips.aspx. Página visitada el 3 de julio de 2010.

El Estado como sujeto que recolecta, trata y transfiere información debe poseer un sistema de gestión de activos de información y un conjunto de medidas técnicas y organizativas de seguridad que permitan una gestión adecuada de dichos activos.

Los puntos de conexión entre la seguridad y privacidad son variados, sin embargo haremos referencia a aquellos relativos a la seguridad de la información en el Estado uruguayo, haciendo especial énfasis en las actividades del CERTuy.

En el manejo de la información, y por el riesgo que su revelación no autorizada pueda producir, es necesario contar no sólo con políticas adecuadas en materia de seguridad, sino también que se debe tomar en consideración todas aquellas medidas pertinentes para la protección de los datos personales.

Estos constituyen activos de información que pueden poseer un alto valor para todo tipo de organizaciones, debiendo ser protegidos ante eventuales ataques informáticos que perjudiquen la competitividad o eficacia de las tareas realizadas.

Muchas veces, las aplicaciones contenidas en un software pueden eventualmente atentar contra el derecho a la protección de datos personales, por ejemplo, recogiendo más información que la permitida o no habiendo informado a la persona de dicha recolección.

Es por ello que la introducción de nuevas tecnologías en la sociedad no puede realizarse sin antes garantizar el derecho a la protección de los datos tutelando la seguridad de los mismos.

La metodología MAGERIT V2 de análisis y gestión de riesgos de los sistemas de seguridad de información define la seguridad como: “la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes o las acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos u de los servicios que dichas redes y sistemas ofrecen o hacen accesibles”.

Las definiciones de seguridad de la información consagran la existencia de los tres pilares básicos para que ésta se cumpla, la confidencialidad, integridad y disponibilidad de la información.

4.1 Principio de Seguridad

Ahora bien, como presupuesto básico para la protección de los datos personales, el tratamiento de éstos debe ser realizado fundamentalmente, bajo el cumplimiento estricto de los principios generales.

El principio de seguridad de los datos personales, se enmarca dentro del grupo de principios de protección de datos consagrados en la normativa internacional.

El Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas respecto al tratamiento automatizado de datos de carecer personal establece un marco mínimo de seguridad de los datos y en su artículo 7 dispone: “se tomarán medidas de seguridad apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados”.

Asimismo, la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de Octubre de 1995, relativa a la protección de las personas físicas en los que respecta al tratamiento de datos personales y a la libre circulación de estos datos, en su artículo 17 determina la obligación de garantizar la seguridad de los datos de carácter personal.

Los Estándares Internacionales sobre la Protección de Datos Personales y Privacidad, aprobados en Madrid, el 5 de noviembre de 2009, en el marco de la 31º Conferencia Internacional de Protección de Datos y Privacidad, en el que se hace hincapié en que tanto la persona responsable como los prestadores de servicios de tratamiento deberán proteger los datos de carácter personal mediante aquellas medidas técnicas y organizativas que resulten idóneas en cada momento para garantizar su integridad, confidencialidad y disponibilidad.

Tales medidas dependerán del riesgo existente, de sus posibles consecuencias para los interesados, del carácter especialmente sensible de los datos de carácter personal, del estado de la técnica y del contexto en el que se efectúe el tratamiento, así como de las obligaciones establecidas en la legislación nacional aplicable[23].

El instrumento normativo reseñado agrega, que los titulares de datos personales deberán ser informados por parte de todos aquellos que intervengan en cualquier fase del tratamiento al respecto de cualquier infracción de seguridad que pueda afectar de forma significativa a sus derechos patrimoniales o extramatrimoniales, así como de las medidas adoptadas para su resolución, y que ésta información se facilite con antelación suficiente, para permitir la reacción de los interesados en defensa de sus derechos [24].

4.2 Situación uruguaya

A los efectos de brindar un panorama general de la situación de nuestro país, comenzaremos con el marco normativo en materia de seguridad de los datos personales, para luego realizar algunas consideraciones generales al respecto.

---

[23] Curso CEDDET. Módulo 3: Seguridad, confidencialidad, transferencias internacionales y autorregulación. Página 9.

[24] Curso CEDDET. Módulo 3: Seguridad, confidencialidad, transferencias internacionales y autorregulación. Página 9.

La Ley Nº 18.331 de 11 de agosto de 2008, de Protección de Datos Personales y Acción de Habeas Data (en adelante LPDP), dispone en su artículo 10 que: “el responsable o usuario de la base de datos debe adoptar las medidas que resultaren necesarias para garantizar la seguridad y confidencialidad de los datos personales. Dichas medidas tendrán por objeto evitar su adulteración, pérdida, consulta o tratamiento no autorizado, así como detectar desviaciones de información, intencionales o no, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado. “Los datos deberán ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular. Queda prohibido registrar datos personales en base de datos que no reúnan condiciones técnicas de integridad y seguridad”.

El artículo 20 de la LPDP, en sede de datos personales especialmente protegidos y bajo el nombre iuris de datos relativos a las telecomunicaciones, establece: “los operadores que exploten redes públicas o que presten servicios de comunicaciones electrónicas disponibles al público deberán (…) adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad en la explotación de su red o en la prestación de sus servicios, con el fin de garantizar la protección de los datos personales que sean exigidos por la normativa de desarrollo de esta ley en esta materia. En caso que exista un riesgo particular de violación de la seguridad de la red pública de comunicaciones electrónicas, el operador que explote dicha red o preste el servicio de comunicaciones electrónicas informará a los abonados sobre dicho riesgo y sobre las medidas a adoptar”.

En materia de inscripción registral el artículo 29 de dicha ley dispone que los responsables de base de datos o del tratamiento deben identificar las medidas de seguridad y descripción técnica de la base de datos.

Por su parte, el Decreto Nº 414/009 de 31 de agosto de 2009, contiene algunas disposiciones en materia de seguridad que interesa resaltar.

El mencionado reglamento contiene un capítulo específico para la regulación de las medidas de seguridad compuesto por dos artículos.

En primer lugar el artículo 7º dispone: “tanto el responsable como el encargado de la base de datos o del tratamiento deberán proteger los datos personales que sometan a tratamiento, mediante aquellas medidas técnicas y organizativas que resulten idóneas para garantizar, su integridad, confidencialidad y disponibilidad”.

En segundo lugar, el artículo siguiente establece: “cuando el responsable o encargado de la base de datos o del tratamiento conozca de la ocurrencia de vulneraciones de seguridad en cualquier fase del tratamiento que realice, que sean susceptibles de afectar de forma significativa los derechos de los interesados, deberán informarles de ese extremo”.

El artículo 23 del Decreto Nº 414/009 al regular las atribuciones que posee el Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales (URCDP), establece que entre sus cometidos estará el de dictar normas y

reglamentaciones que se deben cumplir en el desarrollo de las actividades comprendidas por la ley que se reglamenta; incluyendo las medidas de seguridad en el tratamiento…".

El principio de seguridad de los datos personales, se enmarca dentro del concepto de seguridad de la información, en virtud que los principios y normas relativas a la seguridad de los datos personales tutelan la salvaguarda de activos de información valiosos para el Estado, como lo son los datos personales, por lo que podríamos decir que la seguridad de la información es el género y el principio de seguridad en materia de protección de datos es una especie de ésta.

Las normas internacionales en materia de seguridad de los datos personales, se erigen hacia su protección, teniendo como fundamento dos postulados: las medidas técnicas y organizativas que los responsables y encargados de tratamiento deben tomar para garantizar el cumplimiento de los tres pilares básicos en esta materia: la confidencialidad, la integridad y la disponibilidad, y aquellas relativas a los derechos del titular del dato.

4.3 Características del concepto de Seguridad de los datos personales

Con relación a los tres pilares mencionados:

a) la confidencialidad significa que la información solo es accesible para aquellos autorizados a tener acceso a ella,

b) la integridad es la garantía que la información es exacta, correcta y completa, así como los métodos de su procesamiento,

c) la disponibilidad es la disposición de los servicios a ser usados cuando se requiera la información.

La confidencialidad, deviene de la propia finalidad de la protección de los datos personales, ya que si el acceso a los datos sólo lo realiza la persona autorizada para ello, no existiendo accesos intermedios, filtrados de información o comunicación a terceros, no se ve violentada la autodeterminación informativa del titular del dato.

En el mismo sentido, encontramos el principio de reserva dispuesto en el artículo 11 de la LPDP por el cual las personas que por su situación laboral tengan acceso legítimo o intervengan en cualquier fase del tratamiento, deberán tratarlos exclusivamente para las operaciones habituales de su giro o actividad, estando prohibida toda difusión a terceros de la información.

La integridad de la información se condice con el principio de veracidad de los datos ya que este obliga a que los datos sean veraces, adecuados y no excesivos para los fines para los cuales fueron recogidos, lo que conlleva a protegerlos contra alteraciones que pueda sufrir la información, en este sentido

son importantes los procedimientos de actualización que existan sobre los datos[25].

El artículo 7º de la LPDP establece que cuando se constate la inexactitud o falsedad de los datos, el responsable deberá suprimirlos, sustituirlos o completarlos, siendo estos mecanismos en los casos donde la integridad de la información se pueda ver afectada, por no ser exacta o por haber sufrido algún tipo de manipulación.

La disponibilidad de la información va de la mano con el ejercicio de los derechos de los titulares del dato. Una correcta gestión de la información garantiza que ésta se encuentre disponible en cualquier momento, y así facilitar el ejercicio de los derechos de los titulares. A estos efectos, el inciso 2 del artículo 10 de la LPDP establece que "los datos deberán ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular".

4.4 Medidas de seguridad en la LPDP: su relación con los principios de protección de datos

En oportunidad de enumerar las características de las normas internacionales en materia de seguridad, dijimos que la confidencialidad, integridad y disponibilidad de la información se cumple con la adopción de un conjunto de medidas técnicas y organizativas tendientes a ello.

Se debe tener en cuenta que las medidas de seguridad se encuentran inmersas en una política de seguridad de la información, con carácter general, es decir, un conjunto de criterios acordados en la organización de que se trate para la consecución de dichos objetivos, generando consenso, capacitación y documentos de seguridad.

Las medidas organizativas suponen: la gestión de la información, determinar los activos que se disponen, los niveles de riesgos, la formación y alineación del personal del organismo, así como también el almacenamiento y documentación de la información.

Las medidas técnicas son aquellas relativas a la adecuación y adaptación de los sistemas, equipos y programas tendientes a efectivizar la seguridad de los datos personales protegiéndolos antes eventuales amenazas de seguridad y coadyuvando a la concreción de las medidas organizativas.

En cuanto a los criterios para establecer las medidas de seguridad, se considera que ésta debe atender a: la naturaleza de los datos, siendo las más exigentes las relativas a los datos especialmente protegidos; la finalidad del tratamiento, el tipo de soporte donde se almacene y registre dicha información[26].

---

[25] Curso CEDDET. Módulo 3: Seguridad, confidencialidad, transferencias internacionales y autorregulación. Página 13.

[26] Curso CEDDET. Módulo 3: Seguridad, confidencialidad, transferencias internacionales y autorregulación. Página 15.

La normativa uruguaya contiene los principios básicos en materia de seguridad de la información.

Las medidas de seguridad para la protección de los datos personales dependerá del tipo de organización, del volumen de los datos tratados, de los sistemas que utilicen, del responsable o encargado de tratamiento y de las personas que participen en cualquier fase del procesamiento de los datos personales.

El principio de seguridad se encuentra inmerso dentro del conjunto de los principios establecidos en la LPDP, por lo que la aplicación e interpretación del mismo debe guardar estrecha relación con ellos.

A través del principio de responsabilidad dispuesto en el artículo 12, se puede responsabilizar al responsable de una base de datos por la violación a una norma de seguridad.

El artículo 8 del Decreto reglamentario de la LPDP dispone a texto expreso que, el responsable o el encargado de tratamiento cuando conozca la ocurrencia de vulneraciones de seguridad deberá informar al titular la existencia de éstas así como también los riesgos que dichas vulnerabilidades puedan producir y las medidas que se pretenden adoptar para eliminarlas o mitigarlas.

En el caso del principio de legalidad, las bases de datos que no cumplan con las condiciones de seguridad no podrán ser inscriptas en el registro de base de datos que al efecto lleva la URCDP. La normativa de protección de datos en este aspecto, es contundente, ya que parte de la prohibición de registro en los casos que no se cumplan con medidas de seguridad adecuadas.

Es interesante destacar, que la obligación de adoptar medidas de seguridad alcanza también al encargado del tratamiento, en cualquiera de sus fases, cumpliendo con la normativa de protección de datos.

Luego de un primer análisis de las medidas de seguridad para la protección de los datos personales, podemos decir que en su adopción e implementación, intervienen varios factores y sujetos, y que su cumplimiento atiende a un proceso de evaluación y gestión de los activos de información en todos sus aspectos.

4.5 CERTuy: seguridad en la información y protección de datos

El Decreto que regula el funcionamiento del CERTuy y el Decreto que obliga la adopción de políticas en seguridad en la información, se aprueban conjuntamente.

Asimismo, y con un año aproximadamente de antelación, se sancionan las Leyes de Protección de Datos y Acceso a la Información pública.

El Resultando VI del Decreto Nº 451/009 de seguridad de la información alude a la Ley Nº 18.331, la cual dispone que el responsable o usuario de la base de datos debe adoptar las medidas que resultaren necesarias para garantizar la seguridad y confidencialidad de los datos personales.

El deber de inscripción de base de datos personales, alcanza a aquellas creadas, modificadas o suprimidas por Organismos públicos, estatales o no, salvo las excepciones que al efecto establece la propia LPDP.

El Órgano de control se encargará de verificar si la base de datos contiene las medidas de seguridad adecuadas, pudiendo tener en cuenta el tipo de soporte donde se registran los datos, la calidad de los datos tratados, las políticas y documentos que posea la institución, los planes de contingencia ante amenazas informáticas, destrucción o pérdida de la información, entre otros.

La publicación de recomendaciones que realice el CERTuy en su sitio web y refieran a incidentes de seguridad informática, deben realizarse con arreglo al procedimiento de disociación de los datos.

Asimismo, dentro de sus obligaciones se encuentra la de guardar reserva acerca de la información relativa a estos incidentes.

EL CERTuy posee capacidades suficientes y acordes al ámbito de su competencia y muy similares a las de otros “Cert” internacionales.

En su labor diaria, de recomendar o hasta de analizar fallas o vulnerabilidades informáticas, el CERTuy debe guardar especial cuidado en el manejo de todo los datos personales que se recolecten, traten y comuniquen en los Organismos públicos.

4. Policía especializada en Delitos Informáticos

La División de Delitos Informáticos perteneciente al Departamento de Delitos Complejos de la Policía de Montevideo, fue creada por Decreto N° 254/003, y comenzó a funcionar en el año 2005, con dos funcionarios y escasísimos recursos. Hoy en día cuenta con nueve funcionarios.

El Jefe de Delitos Informáticos, Gabriel Lima, aseguró a El País que hoy en día los delitos informáticos más comunes en Uruguay son las amenazas de muerte por correo electrónico y páginas web. Los delitos informáticos han aumentado, se han perfeccionado y son más difíciles de aclarar ya que las pistas no están "al alcance de la mano", explicó Lima agregando que "en una rapiña los investigadores tienen a la víctima que aporta datos, testigos y posibles pruebas en el lugar; en los delitos informáticos las pruebas que nosotros necesitamos no están físicamente en nuestras manos y el 90% de las veces tenés que ir a servidores extranjeros para ver si hay algún respaldo"[27].

[27] Alerta: crece el peligro de delitos a través de Internet. http://www.elpais.com.uy/09/02/11/lault_398189.asp El País Digital del 2 de febrero de 2009.

"Delitos informáticos" es una nominación para que se entienda, pues no existe una legislación en Uruguay que los defina. "Lo que hacemos es combatir los ilícitos como estafa, hurto, amenaza, y en que el medio para cometerlos sea Internet", explicó el subjefe de la división, el oficial Roberto Ferreira. La unidad se creó "de urgencia" en 2005 y cuenta con siete policías que enfrentan el desafío de combatir una modalidad de delito en expansión en el mundo[28].

Un caso que se destacó en la prensa uruguaya en el mes de mayo fue el siguiente: "Eduardo jamás usó Facebook. Por una cuestión de principios, no forma parte de "redes que carecen de un director responsable o en las que la gente puede escudarse en el anonimato". Sin embargo, un día recibió la noticia de que alguien había creado un perfil suyo en la popular red social, en el que se le atribuían preferencias políticas y sexuales que no compartía. Sin dudarlo, inició un proceso de investigación que finalizó con un resultado poco habitual en estos casos"[29].

El día 7 de julio de 2010 mantuvimos reunión con el Agente Walter Mario Calleros de la Policía de Montevideo, Dirección de Investigaciones Departamento de Delitos Complejos Sección Delitos Informáticos, quien manifestó su preocupación acerca de la falta de normativa existente en delitos informáticos, sobre todo en lo que tiene que ver con la regulación de los cibercafés, responsables de teléfonos celulares, concretamente de los chips, ya que la venta de teléfonos tarjeteros no permite identificar al titular del servicio.

Por otra parte, destacó la importancia de guardar información de telecomunicaciones, tanto de las empresas prestadoras de servicios de telefonía celular, como los ISP, resultando fundamental contar con los log de registro, no siendo necesario los contenidos de los mensajes. Con el dato del log es posible que Antel informe a quien le asignó la IP en ese día y hora. También es relevante guardar la información de servicios 3G, entendiendo como un plazo razonable entre 6 meses y un año para todos los casos.

Los casos más comunes son de difamación e injurias a través de Internet o de teléfonos celulares prepagos, en igual porcentaje y la suplantación de identidad a través de la creación de sitios web.

Se entiende relevante legislar delitos concretos como el hurto de información, el fraude electrónico, la suplantación de identidad, así como también ratificar la Convención de Budapest sobre Cybercrime.

A vía de ejemplo se hizo referencia a algunos casos investigados en nuestro país, que se comentan a continuación.

Respecto al grooming, es fundamental tener en cuenta la edad de las niñas, distinguiendo si tienen más de 10 años. Se planteó una denuncia por una

---

[28] Ciberpolicías patrullan la web. http://www.elpais.com.uy/Suple/DS/07/04/22/sds_276418.asp El País Digital del 22 de abril de 2007.

[29] Los peligros en las redes sociales: cuando la impunidad es la norma. http://www.espectador.com/1v4_contenido.php?id=182602&sts=1 El Espectador, entrevista del 21 de mayo de 2010.

madre de una adolescente de 14, que se había fotografiado y filmado y a quien la persona de contacto en la web se había negado a conocer personalmente (18 años) al enterarse de la edad de la menor.

La denominada "Operación Peón" refiere a un uruguayo que se encuentra procesado y al que se le incautaron materiales de pornografía infantil. No se le ha podido probar la producción de pornografía, que es el delito más severamente tipificado. Este caso tiene ramificaciones internacionales.

Phishing en el Banco Santander. Se había puesto un teléfono de contacto en el mensaje que no era del Banco, sino de una casa de familia a la cual llamaban a toda hora solicitando préstamos. Los mensajes se originaban en la India por lo cual la investigación se derivó a Interpol.

Hurto de correspondencia. Un funcionario de la Intendencia Municipal de Canelones, personal de confianza del Intendente, intervino los correos electrónicos de personas de los partidos blanco y colorado para enemistarlos.

Caso Velásquez. Es un hacker argentino que realizó un phishing mediante el cual ingresó a correos electrónicos de diputados y senadores enviando mensajes diciendo que necesitaba el usuario y password para el restablecimiento de la casilla. De esta forma lograba tener acceso a los correos electrónicos. Se encontró en su computador un listado de claves, todas las direcciones de correo electrónico que había intervenido. Es interesante desatacar que las casillas no fueron robadas, sino que estaban intervenidas, entraba y salía para leer los correos y obtener la información. Fue procesado por el Juez Letrado de Primera Instancia en lo Penal de 7º turno el 25 de enero de 2009.

"Tal fue el delito cometido por el espía argentino Iván Velásquez, quien robó información secreta sobre 60 policías de la Jefatura de Policía de Montevideo, relativa a su identidad y armamento"[30].

Sobre este caso, destaca el auto de procesamiento que: mediante la utilización de medios fraudulentos el encausado accedió a información reservada ocasionando un perjuicio a la seguridad. El encausado posee habilidades suficientes al efecto en virtud de ocupar cargos de inteligencia en la policía Argentina, teniendo información de este tipo en su poder, a la cual accedió de forma no autorizada. El engaño se produce al simular hacer entrega de una computadora en donación a una de las dependencias del Ministerio del Interior argentino. La información contenía datos personales de los policías argentinos y uruguayos, sus armamentos, así como también información de personas vinculadas con la política de Uruguay.

El sentenciante entiende que la conducta encarta plenamente en la figura tipificada en el artículo 300 del Código Penal Uruguayo "Conocimiento fraudulento de documentos secretos".

---

[30] http://www.ultimasnoticias.com.uy/hemeroteca/040210/prints/act13.html Diario Ultimas Noticias del 4 de febrero del 2010.

Además de las investigaciones policiales relatadas, interesa referir a casos resueltos judicialmente.

Por Sentencia del Juzgado Letrado en lo Penal de 20º Turno Nº 225 de 26 de agosto de 2009, se condenó por delito de violación de correspondencia con un ilícito de falsificación de documento privado por interceptación de correos electrónicos. En este caso, a través de la obtención por medios ilegítimos de la contraseña de la cuenta de correo electrónico de la denunciante, la procesada divulgó noticias falsas de ésta última a sus contactos personales.

Mediante orden judicial dirigida a “Anteldata”, se obtuvo la información con la que se pudo determinar el número IP asignado al contrato de adsl de la procesada, siendo más sencilla su determinación en virtud de que no existían conexiones inalámbricas a Internet.

Se considera que la conducta desplegada encarta plenamente en la figura representada en el artículo 296 del Código Penal Uruguayo, al haberse interceptado la correspondencia escrita electrónica con intención de interrumpir su curso normal.

Por Sentencia del Tribunal de Apelaciones en lo Penal de 2º Turno Nº 63 de 19 de marzo de 2009 se confirma procesamiento por un delito continuado de violencia privada mediante amenazas por mensajes de texto, correos electrónicos y llamadas telefónicas. A través del envío de mensajes de texto y correos electrónicos, la imputada amenazó de forma continuada a un hombre de estado civil casado, con el cual mantuvo una relación amorosa.

A pesar de que la defensa argumentó que la conducta desplegada no constituye una violencia o amenaza, la Sala desestimó los agravios, considerando que existió una transgresión al bien jurídico que la ley protege, es decir, la libre determinación de la voluntad, circunstancia la cual se vio alterada por la recepción de sendos mensajes de textos y correos electrónicos agraviantes.

5. Conclusiones

El Dr. Palazzi analiza el robo de identidad vinculado a ficheros sobre solvencia crediticia, manifestando que: “El robo de identidad es entonces algo muy nuevo, pero las soluciones legales están presentes desde hace mucho tiempo (aunque en mayor parte de los casos son de carácter paliativo y no preventivo), como lo evidencian los fallos que responsabilizan a entidades financieras. Lo que se necesita, entonces, no es una nueva ley sino un cambio de la arquitectura del sistema en materia de manejo de información; lo que se requiere, y lo examinaremos en detalle más adelante, es mejorar las protecciones a la difusión y acceso a la información en poder de entidades financieras por parte de terceros que intentan cometer delitos. (…) Lo que necesitamos es hacer más efectivas las normas de protección de datos, y a la

vez mejorar las prácticas relacionadas con la obtención de créditos bancarios para evitar el uso de datos falsos"[31].

Uruguay se encuentra trabajando, desde un punto de vista teórico en la actualización de marcos legales, pero también realizando tareas de campo, a través del CERTuy en el sector público y de la policía especializada en delitos informáticos con carácter general.

Desde Agesic, estamos comprometidos con la seguridad de la información, en todos sus aspectos, partiendo de la protección de los datos personales, como impulsores de la ley vigente y trabajando en la gestión y consolidación del derecho, como también en la salvaguarda de los activos críticos de información del Estado, siendo por mandato legal sus custodios.

Montevideo, 16 de julio de 2010

[31] PALAZZI, Pablo. "Robo de identidad, protección de datos personales y ficheros sobre solvencia crediticia", capítulo del libro Derecho a la intimidad y a la protección de datos personales. Heliasta, Argentina, 2009. Página 132.