Aspectos Legales y Éticos de la Seguridad Informática©
Una reflexión local y global.
Autora: Lic. Ivonne V. Muñoz Torres

La seguridad informática, no sólo en México sino a nivel mundial, es uno de los temas que mayor auge comienza a tener en la actualidad, visto ya sea desde las necesidades de promoverla así como de implementarla.

Lo anterior atiende a centrar esta disertación en una premisa importante: la seguridad informática no implica en forma única y específica a Internet, la seguridad informática se refiere a todo lo que hace referencia a la preservación, respeto y buen manejo de la información. Para ello, es de vital importancia aclarar que el valor protegido, tanto tangible como intangible, será siempre la información.

Sin embargo, el tema de preservar, respetar y manipular en la forma más correcta a la información, al día de hoy no es un tema fácil de entender, dado que se tiene pensado en el mayor de los casos, que la seguridad informática es un tema que sólo debe aplicarse a casos específicos y no a un "todo" empresarial, Vg:

a. *la importancia de proteger los archivos electrónicos de un alto ejecutivo en una empresa vs. la falta de importancia de proteger los archivos electrónicos de la persona encargada de llevar el registro de entrada y salida del personal.*

b. *la constante actualización de programas antivirus en las computadoras personales de los altos ejecutivos en una empresa vs. la ausencia de un programa antivirus en las computadoras personales de las secretarias de dichos ejecutivos.*

Ambos ejemplos nos permiten entender la forma en que es visto, en muchos de los casos, el cómo deben ser implementados algunos de los controles en materia de seguridad de la información, ahora veamos las consecuencias de pensar en esta forma:

a. *el viernes 20 de febrero una descarga de alto voltaje recae en la empresa, como consecuencia, el procesador y disco duro de la computadora personal del Director de Recursos Humanos sufren daños y por ende pierde su información, sin embargo la consecuencia no es grave dado que su información sí tenía implementado un sistema de respaldo, permitiéndole así no comprometer la integridad y disponibilidad de la misma. Por otra parte, como consecuencia de la descarga, la computadora del encargado de mantener un registro electrónico del control de entradas y salidas del personal así como de personas externas a la empresa, también sufre daños y la información se pierde. ¿qué sucederá con el control de asistencias del personal?, ¿cómo determinar quién asistió que días y en qué horario?, en caso de una investigación por robo, ¿en base a qué registro se podrá saber quién accedió a las instalaciones de la empresa?, ¿quién será el responsable ante la ausencia de esta información: el encargado del control o el encargado de sistemas? Más importante aún: ¿a quién despedir por esta negligencia?*

b. *El lunes 04 de enero a las 9 h, un nuevo virus ataca a las computadoras, en esa hora es cuando las secretarias de los altos ejecutivos de una empresa están revisando agendas y ajustando las actividades de la semana laboral. Una de las computadoras de las secretarias es infectada por el nuevo virus, obviamente sin tener conocimiento de que dicho hecho sucede dado que no tiene instalado un antivirus. Al momento de intercambiar información con las demás secretarias y con su propio jefe, ella infecta las computadoras de las otras secretarias y afortunadamente la computadora de su jefe no es afectada. Las consecuencias de ejecutar el virus son fatales dado que empieza a borrar la información así como el acceso a ciertos programas en la computadora,*

situación que sucede en todas las computadoras de las secretarias de los altos ejecutivos de la empresa. Consecuencia fatal: al inicio de una semana laboral, el área operativa más importante de una empresa es detenida en sus actividades aún cuando la toma de decisiones permanece intacta, sin embargo… ¿cómo pueden ejecutarse las decisiones si el área operativa es inoperable?

De los dos ejemplos anteriores, mismos que reflejan consecuencias mínimas, (existen más graves, como el robo de información, fraudes, revelación de secretos, difamación, etc.) surge la pregunta más utilizada en el tema: ¿quién es el responsable de que sucedan estos hechos?

Para abrir las opciones en esta respuesta, la abordare desde dos puntos de vista: uno será el de los aspectos éticos y el otro de los aspectos legales, no sin antes mencionar que aún cuando separare los puntos de vista, se debe dejar claro que la ética y el derecho son dos temas que siempre van unidos.

Aspectos éticos

Los *medios* y el *fin*, la premisa principal cuando de ética se habla. *El fin justifica los medios* o *los medios justifican el fin*, ambas frases son las que salen a relucir cuando estamos frente a un conflicto ético.

Con la intención de no entrar en teorías filosóficas, partamos de una definición objetiva de lo que la palabra *ética* significa de acuerdo a lo que la Real Academia Española indica:

> *- Parte de la filosofía que trata de la moral y de las obligaciones del hombre.*
> *- Conjunto de normas morales que rigen la conducta humana*.[1]

[1] *Real Academia Española. http://www.rae.es/ Fuente consultada: 10 de Marzo de 2005.*

De ahí que cuando nos enfrentamos a un conflicto ético no es más que cuando uno mismo está en una situación que compromete por una parte a su moral y por la otra a sus obligaciones, es decir, el ser y el deber ser.

Lo que siempre menciono con respecto a este tema, es que indudablemente los valores éticos no son universales, sería imposible asegurar que existe un manual único que enliste como debe ser la ética de todos los seres humanos, es por ello que ante las preguntas: ¿quién me dice sí soy ético o no? y ¿quién me enseña como ser ético?, existe para la primer pregunta sólo una respuesta: **uno mismo**; mientras que para la segunda pregunta, la respuesta es que los valores éticos los vamos aprendiendo de nuestro entorno (familia, trabajo y núcleo social) aún así, retornando al 'yo', es uno mismo quien construye su propia ética y por ende, la aplica en forma distinta ante casos específicos.

Para lo que respecta al tema de seguridad informática, el cómo ser ético es definido desde varios aspectos, principalmente por los Códigos de Ética estipulados por Instituciones dedicadas al tema de la Seguridad Informática[2] e incluso por Autoridades[3] (no gubernamentales, precisamente) dedicadas al tema de las Tecnologías de Información.

En el tema de Seguridad Informática, el Consorcio para la Certificación Internacional de Seguridad en Sistemas de Información (*ISC*^{2} – *International Information Systems Security Certification Consortium*) emite una de las más importantes certificaciones en el tema de Seguridad Informática, conlleva como requisito indispensable el compromiso y conocimiento del Código de Ética establecido por el Consorcio[4]. Dentro de los cánones a seguir, se indica lo siguiente:

- Proteger a la sociedad, a la comunidad y a la infraestructura
- Actuar en forma honorable, honesta, justa, responsable y legal

---

[2] *ISC*^{2} *– International Information Systems Security Certification Consortium* https://www.isc2.org/

[3] *Request for Comments Editor* http://www.rfc-editor.org/

[4] *Código de Ética de ISC*^{2} https://www.isc2.org/cgi/content.cgi?category=12

- Proveer servicios diligentes y competitivos a sus superiores
- Actuar siempre protegiendo y promoviendo el crecimiento de la profesión

Con respecto a Autoridades no Gubernamentales que establecen políticas y costumbres en materia de Tecnologías de Información, el Request for Comments 1087: Ética e Internet[5], generado desde enero de 1989 por DARPANET (Defense Advanced Research Projects Agency, Internet Activities Board) define, a *contrario sensu*, lo que se entiende como un comportamiento no ético en Internet de la siguiente forma:

- Conseguir accesos no autorizados a los recursos de Internet
- Entorpecer el uso intencionalmente de Internet
- Gasto de recursos en forma innecesaria
- Destruir la integridad de la información basada en computadoras
- Comprometer la privacidad de los usuarios

Aspectos legales

En lo que respecta al mundo jurídico, es obvio que las personas en ningún momento se encuentran sujetos a normas morales, la situación requiere de un ambiente de obligatoriedad especificada a través de disposiciones y sanciones, es decir: las normas jurídicas.

La relación entre la Seguridad Informática y el Derecho, se ciñe a las preocupaciones existentes en materia de implementación, todas ellas en torno de los siguientes cuestionamientos:

a. ¿qué pasa si mis programas de cómputo no tienen una licencia de uso?
b. ¿cómo puedo hacer responsable al personal de proteger la integridad de la información?

[5] *RFC 1087* http://www.rfc-editor.org/cgi-bin/rfcdoctype.pl?loc=RFC&letsgo=1087&type=ftp&file_format=txt

c. ¿en qué forma puedo evitar que la información confidencial de la empresa no sea revelada a terceros?
d. ¿cómo protejo mis secretos industriales?
e. ¿cómo responsabilizo a mi personal cuando les entrego una computadora para que trabajen con ella?
f. Etcétera…

La situación a resolver con los aspectos legales son sólo dos:

1. Promover una cultura jurídica en materia de TI que en consecuencia impacte en un robustecimiento de las normas jurídicas existentes al día de hoy, y
2. Fortalecer la normatividad interna de las empresas con apego siempre a derecho

Seguridad de la Información vs Sociedad de la Información

¿información o datos? ¿sociedad y seguridad? …

Hace no muchos años que el concepto information society empezaba a oírse en el mundo de las TIC, en su momento orientado a embanderar una lucha ideológica y política con el fin de incrementar la brecha digital y en consecuencia la brecha de conocimiento.

Actualmente es viable asegurar que en países como el nuestro, la brecha digital se ha visto enriquecida y ampliada, fortaleciendo así el concepto de Information Society.

En materia de seguridad, ¿cómo ha afectado este avance?

A. La brecha digital era ‘angosta’ y por ende, el número de usuarios con acceso a datos era más controlable, reduciendo así un índice de riesgos.
B. La brecha digital es ‘amplia, y por ende, el número de usuarios con acceso a datos en menos controlable, incrementando así un índice de riesgos.

El desajuste que conlleva esta evolución, se ve reflejado actualmente en los nuevos campos de estudio y reflexión analizados por la Information Society, específicamente en la Cumbre Mundial de la Sociedad de la Información (World Summit on the Information Society).

Los tópicos en materia de seguridad de la información, que se están estudiando por parte del Working Group On Internet Governance, incluidos en el “Cluster 2 of WGIG Key Issues relating to the use of the Internet” y en el “Cluster Three Assessment Report”, son los siguientes :

- Spam
- Cybersecurity,
- Cybercrime,
- Security of network and information systems,
- Critical infrastructure protection
- Applicable jurisdiction,
- Cross border coordination,
- Exemption for ISPs of third party liabilities
- National policies & regulations
- Intelectual Property Rights
- E-commerce

Los puntos en común con respecto a dichos temas y por obvias razones, revisados con la lupa jurídica, son: la jurisdicción, los sistemas legales de cada

país, la existencia y a su vez la inexistencia de legislación y por supuesto la parte de “cultura” del usuario, que obviamente forma parte de la Sociedad de la Información.

Nuestra participación en este proceso de discusión, queda sujeta a ver los resultados después de la siguiente Cumbre a llevarse a cabo a finales del presente año, momento en el que las acciones independientes de cada gobierno serán las de adecuarse y/o tomar las mejores prácticas de lo recomendado por los grupos de trabajo que la conforman.

O igual, a esperar a que sigan discutiéndose estos temas en el corazón de los trabajos de la Cumbre y a su vez, promoviendo la generación de un marco jurídico robusto en nuestros países.

Conclusión

El derecho y la ética, en conjunto, son una herramienta que permite fortalecer la implementación de estrategias de seguridad informática.

¿En qué momento interactúa la ética?

En el momento en que se determina que la seguridad informática es un tema que involucra a todos los miembros de una organización y no sólo a ciertos puestos específicos dentro de la misma. La ética se refleja en la responsabilidad de considerarse parte de un proceso que tiene como fin único el preservar y conservar la integridad y buen manejo de la información frente al mundo actual lleno de tecnología y, por ende, de riesgos que comprometen a la información.

¿En qué momento interactúa el derecho?

En el momento en que son implementados los procedimientos estipulados en la legislación vigente, ya sea en los procesos como en los marcos normativos internos de las empresas.

¿Sabía usted que…

… el daño a la información (vista esta como un bien mueble) puede ser causa de una rescisión laboral – justificada -?

… la revelación de un secreto industrial es un delito?

… el hecho de no contar con licencias en sus programas de cómputo puede afectarle con una multa equivalente a 5,000 días de SMGV[6] o hasta de 10,000 días de SMGV en México?

… la firma electrónica avanzada le permitirá tener un ambiente legal seguro en sus transacciones realizadas a través de medios electrónicos?

es visible como el concepto de *Information Society* no es ajeno al de *Information* Security, en si, el segundo es parte intrínseca del primero ya que todos al formar parte de la *Information Society* adquirimos no sólo privilegios, sino también obligaciones, muchas de ellas (sino es que todas) deben estar encuadradas en un marco jurídico que convierta a el uso de las TIC´s en una práctica segura, tal y como lo hacemos cuando salimos a convivir en una sociedad tangible, misma que se encuentra regida por normas de conducta (tanto morales, sociales como jurídicas)

Piense éticamente y actué legalmente si lo que usted realmente desea es dar soluciones de seguridad informática a su empresa… NO se arrepentirá.

[6] SMGV – Salario Mínimo General Vigente

¿Cuál es el marco jurídico que en materia de seguridad informática existe en México?

A manera de síntesis, en la siguiente tabla se resumen las normas jurídicas, entre otras, que en México permiten darle un soporte legal a la implementación y seguimiento de estrategias de Seguridad Informática:

- Delitos informáticos - Comercio electrónico - Protección de programas de cómputo - Responsabilidad de personal de TI - Intercepción de comunicaciones - Estándares de Seguridad Física y Lógica - Firma electrónica - Confidencialidad de la información - Secretos industriales	- Código Civil - Código Federal de Procedimientos Civiles - Código de Comercio - Ley Federal de Protección al Consumidor - Reglamento de Prestadores de Servicios de Certificación - Reglas del Reglamento de Prestadores de Servicios de Certificación - NOM 151 SCFI 2002 - Código Penal Federal - Códigos penales estatales (D.F., Sinaloa, otros) - Ley Federal del Derecho de Autor - Ley de Seguridad Nacional - Ley Federal contra la Delincuencia Organizada - Ley Federal del Trabajo - Ley Federal de Responsabilidades Administrativas de los Servidores Públicos - Acuerdo que establece las normas que determinan como obligatoria la presentación de las declaraciones de situación patrimonial de los servidores públicos, a través de medios de comunicación electrónica. - Ley de Propiedad Industrial - Ley Federal de Telecomunicaciones

	- Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental

*****La autora es Licenciada en Derecho (UAM, 1999) titulándose con el trabajo: *Reconocimiento y certificación de la firma electrónica ante Notario Público*. Maestra en Comercio Electrónico (ITESM, 2004) titulándose con la tesis: *La importancia de la seguridad informática para el sano desarrollo del comercio electrónico en México - Propuesta legal*.

Desde agosto de 2002 es profesora del Diplomado en Seguridad Informática en los Campus: Ciudad de México, Estado de México, Hidalgo y Santa Fe, así como en las versiones especiales para la Comisión Nacional Bancaria y de Valores de México y la Comisión Nacional Bancaria y de Seguros de Honduras, impartiendo el módulo de *Aspectos Legales y Éticos en la Seguridad Informática*.

Es autora de los rediseños educativos de las materias: Informática Jurídica (2002) y Legislación en Informática (2003) del Instituto Tecnológico y de Estudios Superiores de Monterrey a nivel Sistema.

En sus membresías es: Coordinadora de Publicaciones de la Academia Mexicana de Derecho Informático, Miembro de: Consejo Directivo de la Organización Mundial de Derecho e Informática; del Consejo Editorial de la revista B-Secure y de la mesa directiva de ALAPSI.

Actualmente es consultora externa de la Dirección General de Clasificación y Datos Personales del Instituto Federal de Acceso a la Información Pública. Para el presente año, es responsable de actualizar el reporte de privacidad en México que anualmente publica el Electronic Privacy Information Center