EL DERECHO INFORMÁTICO Y LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
UNA PERSPECTIVA CON BASE EN LA NORMA ISO 27 001

Arean Hernando Velasco Melo*

* Abogado de la Universidad del Norte de Barranquilla. Magíster en Informática y Derecho de la Universidad Complutense de Madrid (España). Especialista en Regulación y Gestión de las Telecomunicaciones de la Universidad Externado de Colombia. Estudios de Negociación Avanzada en Harvard Law School. Estudios de Propiedad Intelectual en la OMPI. Asesor y consultor en temas de Derecho de Tecnologías de la Información y las Comunicaciones y en Seguridad de la Información. Miembro de la firma Velasco, Calle & D´Alleman. *Abogados. www.iustic.net*

REVISTA DE DERECHO
Nº 29, Barranquilla, 2008
ISSN: 0121-8697

Resumen

Este artículo pretende informar sobre la existencia y diversas modalidades que incluye el Derecho informático y crear conciencia acerca de la posición que deben tomar los diversos actores económicos en la era de la información para asegurar una adecuada política de seguridad de la información que, ante la falta de una legislación nacional sobre el tema, debe basarse en los estándares internacionales, el derecho comparado y autonomía de la voluntad. La metodología empleada para explicar las diversas áreas de impacto es la seguida por la norma ISO 27001 en el dominio que hace referencia al cumplimiento y que comprende: La protección de datos personales; la contratación de bienes informáticos y telemáticos; el derecho laboral y prestación de servicios, respecto de la regulación de aspectos tecnológicos; los servicios de comercio electrónico; la propiedad intelectual, y el tratamiento de los incidentes informáticos.
Palabras claves: TIC's, información, seguridad, derecho informático.

Abstract

This article seeks to provide information about the existence and various disciplines of Information Technology Law and to create awareness about the position to be taken by the various economic players in the information age to ensure an adequate information security policy that, in the absence of a national regulation on the matter, has to be based on international standards, comparative law and the autonomy of will. The methodology employed to explain the various areas of impact is that of the ISO 27001 standard in its domain about Compliance which includes: The protection of personal data, the contracting of IT goods and computer data transmission; labor law and provision of services, regarding the regulation of technological aspects; electronic commerce services; intellectual property rights, and the treatment of IT incidents.
Key words: TIC's, information, security, Information & Communications Technology Law.

Fecha de recepción: 10 de sep 07
Fecha de aceptación: 29 de oct 07

INTRODUCCIÓN

El impacto de las Tecnologías de la Información y las Comunicaciones –TIC– no es ajeno al Derecho, por el contrario, cada día los avances de la tecnología imponen mayores retos a los operadores jurídicos, a los cuales hay que responder desde la legislación nacional –si ésta existe –, la legislación internacional, el derecho comparado, la autonomía de la voluntad privada, las mejores prácticas existentes en la industria y las normas que permitan dar un tratamiento uniforme a problemáticas que experimentan las organizaciones, cualquiera que sea la latitud en que estén ubicadas.

Para enfrentar de manera adecuada los retos que las TIC plantean al Derecho se requiere como punto de partida por el operador jurídico, la comprensión de los aspectos tecnológicos que, desde la informática, las telecomunicaciones y la convergencia, están presentes en el tráfico de bienes y servicios, así como en la e-conomía, pues sin esta comprensión es difícil entender los problemas que giran en torno al desarrollo de *software*, integración de sistemas informáticos, diseño de *hardware*, voz IP, servicios y redes de telecomunicaciones, propiedad intelectual de intangibles digitalizables, bases de datos, servicios convergentes, entre otras problemáticas.

Adicional a ello, se requiere el estudio de las relaciones entre las TIC y el Derecho. De esta reflexión ha hecho carrera la existencia de un área encargada de la regulación del fenómeno informático y telemático que ha sido denominada Derecho Informático, término adoptado por tratadistas como Emilio Suñe, Michel Vivant, Julio Núñez, Miguel Davara, entre otros.

Al respecto afirma el profesor Suñe (2000):

> *El Derecho de la informática, por seguir aportando razones singulares que avalan su autonomía, tiene mucho de Derecho Global, al tratarse de un Derecho muy internacionalizado, probablemente por el tipo de comunidades humanas que están en su base. La regulación jurídica de Internet, por ejemplo, plantea problemas globales, que requieren soluciones globales. Las grandes multinacionales del sector teleinformático, que lo dominan casi todo por completo, no pueden –ni quieren– adap-*

tarse a regulaciones estatales injustificadamente diversas y dispersas, cuando el mercado no es nacional, sino global (p. 7).

El desarrollo en nuestro país de normas jurídicas que respondan a los problemas que surgen del fenómeno de las TIC´s es mínimo. La Ley 527 de 1999 constituye uno de los pocos desarrollos importantes en este sentido. Esta situación genera un grado importante de inseguridad e incertidumbre no sólo para las organizaciones, sino para también los ciudadanos, en su condición de usuarios, consumidores y titulares de datos personales.

La información se ha convertido no sólo en un activo valioso, sino también estratégico en las organizaciones. Las bondades de los sistemas de información, por ejemplo, al procesar información económica de las empresas permite predecir los riesgos financieros de las mismas, con una precisión tal, que podría incluso diagnosticarse, en términos de tiempo, la fecha en la que un ente empresarial puede estar en situación de insolvencia o iliquidez.

La información puede ser protegida de muchas maneras. Desde el Derecho pudiera pensarse que se logra contar con un adecuado nivel de protección, con la encriptación, teniendo en cuenta que la mayor de las veces la compresión del tema tecnológico es poca; sin embargo, la encriptación es un mecanismo para otorgar a la información atributos de confidencialidad, integridad, autenticidad, y dependiendo del mecanismo de encriptación, podría reputarse el no repudio. En la protección de la información intervienen diferentes disciplinas, desde la informática, la gerencial, la logística, la matemática hasta la jurídica, entre muchas otras.

El objetivo de este artículo es analizar cómo el Derecho participa en la gestión de la protección de la información, máxime cuando este tema es para las organizaciones uno de los que mayor preocupación genera para las áreas directivas. La participación del Derecho en la protección de la información no es un querer arbitrario de los operadores jurídicos, es el resultado de un estudio profundo y concienzudo del sector real de la economía, al punto que organizaciones como la OCDE han formulado

recomendaciones en este sentido, las cuales hoy día están consignadas en la ISO 27 001.

Así pues, el punto de partida de este estudio será acudir a los conceptos de Información y Seguridad, para lo cual se tendrá en cuenta las definiciones otorgadas por el Diccionario de la Real Academia de la Lengua Española, ello con el fin de partir de conceptos básicos.

En este orden de ideas, se ha de entender como "información" la "Comunicación o adquisición de conocimientos que permiten ampliar o precisar los que se poseen sobre una materia determinada" (Diccionario de la Real Academia de la Lengua Española, última edición).

De otra parte, la "Seguridad" "Se aplica también a ciertos mecanismos que aseguran algún buen funcionamiento, precaviendo que este falle, se frustre o se violente" (Diccionario de la Real Academia de la Lengua Española, última edición).

De estas definiciones se puede concluir el valor que tiene la información como resultado de un conocimiento especializado en un área determinada, que a su vez requiere de ciertos mecanismos para garantizar su buen funcionamiento, en aras de protegerlo y asegurar su permanencia frente a los actos violentos que se pueden perpetrar contra la información.

Anteriormente la seguridad de la información estaba entendida como la aplicación de un conjunto de medidas de orden físico y lógico a los sistemas de información, para evitar la pérdida de la misma, siendo ésta una tarea de responsabilidad exclusiva de los departamentos de informática de las organizaciones.

Cambiar la perspectiva del problema de la seguridad de la información que pueden tener los responsables de ésta en las organizaciones no es una tarea fácil; para ello es importante acudir a criterios objetivos que demuestren la importancia que tiene el Derecho en esta problemática, y demostrar cómo el tema, por ejemplo, de los incidentes informáticos puede tener una vocación judicial, siempre y cuando las evidencias de los mismos hayan sido adecuadamente recabadas.

Hoy día, el Derecho es un invitado importante en la gestión de la información; en este sentido, es la herramienta ideal para aportar una serie de recomendaciones y controles jurídicos, en ocasiones matizados por la tecnología, para la gerencia adecuada de aquellos activos tangibles e intangibles que involucren información relevante y valiosa para una organización, sea esta pública o privada.

Tratándose de proyectos informáticos o telemáticos, que la mayoría de las veces son desarrollados por terceros para una organización, es importante tener en cuenta que éstos no pueden ejecutarse al margen de las políticas generales de seguridad del ente empresarial. En la medida en que se trata de terceras personas que tienen acceso a las redes, sistemas informáticos, infraestructura e información estratégica de la compañía, se debe tener presente que estos terceros, al interactuar con la organización, deben asumir una serie de obligaciones, cargas y deberes, así como los riesgos y responsabilidades que conlleva el indebido tratamiento de la información para el titular de tales activos; sin esta concepción holística del tema, es frágil cualquier sistema de gestión de la seguridad de la información.

Antecedentes

La seguridad siempre ha sido una preocupación para el hombre, los deseos de proteger la información de una manera segura no es una preocupación exclusiva de esta era; por el contrario, a lo largo de la historia del hombre se han usado diversos mecanismos para alcanzar este cometido.

La trascendencia de la seguridad de la información en las organizaciones públicas o privadas radica en que: (i) el volumen de información crece día a día; (ii) la información es un intangible con un valor bastante apreciable en la economía actual; (iii) la información es una ventaja estratégica en el mercado, que la convierte en algo atractivo para la competencia, como elemento generador de riqueza, (iv) la frecuencia de los ataques a los activos de una organización es cada vez mayor, cualquiera que sea el medio al que se acuda, y (v) no existe una cultura de seguridad en los usuarios de la información, lo que conduce

a que las organizaciones empiecen a incorporar prácticas seguras de protección de la información, advirtiendo que este proceso habrá de impactar la cultura de la organización; aspecto que requiere de tiempo y compromiso, empezando por la dirección de la misma.

El origen reciente de la seguridad la información, entendida como un proceso que se debe gestionar, nace en el Reino Unido, donde el Departamento de Industria y Comercio y las empresas del sector privado trabajaron de manera conjunta en esta problemática, lo cual dio origen a la norma BS7799 en el primer lustro de la década pasada; norma que no pretendía ser más que un Código de Buenas Prácticas para la Gestión de la Seguridad de la Información.

A finales de la década pasada esta norma fue actualizada y complementada, lo cual dio como resultado una norma que establecía las recomendaciones para que una empresa evaluará y certificará su sistema de gestión de seguridad de la información. Esta nueva versión de la norma se convirtió en la norma ISO 17 999 de diciembre de 2000, la cual estaba alineada con las directrices de la OCDE (Organización para la Cooperación y el Desarrollo Económico) en materia de privacidad, seguridad de la información y Criptología, hecho de gran trascendencia, pues le otorgaba un carácter global a la norma. En el 2002, la norma adquiere la denominación de ISO 27 001, luego de una nueva actualización.

> (…) *la gestión de la seguridad de la información debe ser revisada (¿complementada?) para no solamente cubrir las fallas de seguridad, sino para comprender la manera estructural y sistemática las tensiones entre los elementos que componen el sistema de gestión de la seguridad. En este sentido, consecuente con las tendencias internacionales y la realidad de un mundo global, la seguridad de la información se convierte en un elemento activo y estratégico para las empresas del siglo XXI* (Cano, 2007).

Problema

La seguridad informática ha hecho tránsito de un esquema caracterizado por la implantación de herramientas de *software*, que neutralicen el acceso ilegal y los ataques a los sistemas de información, hacia un modelo de gestión de la seguridad de la información en el que prima lo dinámico sobre lo estacional.

Para lograr niveles adecuados de seguridad se requiere el concurso e iteración de las disciplinas que tengan un impacto en el logro de este cometido, teniendo siempre presente que un sistema de gestión no garantiza la desaparición de los riesgos que se ciernen con mayor intensidad sobre la información.

Entonces, el problema es determinar cómo desde una disciplina como el Derecho se contribuye a la gestión de la seguridad de la información. Los enfoques de intervención jurídica podrían ser muchos; de hecho no existe limitación alguna, para que una organización adopte las medidas que considere pertinentes con el fin de neutralizar un riesgo.

Sin embargo, el Derecho Informático se convierte en un enfoque adecuado de intervención, teniendo en cuenta que los temas que plantea el profesor Suñe (2000, p. 15 y ss.) en sus estudios están subsumidos en la norma ISO 27.001. Al respecto, advierte que son temas propios del Derecho Informático: a) Contratación Informática; b) Derecho a la intimidad y libertades; c). Flujo transnacional de datos; d). Propiedad Intelectual del *software*; y e) Otros temas del Derecho Informático (delitos penales, valor probatorio de los soportes informáticos, transmisión de datos).

El Derecho Informático comprende entonces las múltiples iteraciones entre las TIC y el Derecho, de donde surgen aspectos propios como la contratación de intangibles digitalizables, la propiedad intelectual sobre ellos, el comercio electrónico, la protección de datos personales, el tratamiento jurídico de los incidentes informáticos, los aspectos tecnológicos que impactan las relaciones laborales y la prestación de servicios.

El fenómeno de la convergencia introduce en este nuevo sector del derecho aspectos propios del derecho de las telecomunicaciones, como son la voz sobre IP, la Televisión sobre IP, los servicios de valor agregado y servicios telemáticos que empiezan a ser unificados con las TIC bajo en nombre de servicios convergentes.

El desarrollo cada vez más acelerado de la tecnología, y el incremento de la penetración de Internet en la vida social, económica y cultural,

además de los beneficios que reflejen para la sociedad, incrementarán los retos para los operadores jurídicos en materia de seguridad de la información y de regulación de estos fenómenos.

La ISO 27 001 es una herramienta de gestión estratégica que conduce a lograr la protección de la información, bien en un contexto en el cual la empresa pretenda alcanzar una certificación, o bien que sólo pretenda incorporar buenas prácticas de seguridad de la información, no sólo en sus procesos internos, sino también en sus procesos externos.

Aspectos jurídicos

La norma consagra un conjunto significativo de dominios que pretenden establecer un ciclo de seguridad lo más completo posible, advirtiendo que no todos ellos tienen impacto jurídico. Desde ya es importante mencionar que el enfoque que se propone se alimenta tanto de normatividad nacional como internacional, así como de otras fuentes del Derecho, en razón de la escasa legislación que existe.

La norma ISO 27 001, contempla diez dominios:

1. Política de Seguridad de la Información
2. Organización de la Seguridad de la Información
3. Gestión de Activos
4. Seguridad de Recursos Humanos
5. Seguridad Física y del Entorno
6. Gestión de Comunicaciones y Operaciones
7. Control de Acceso
8. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información
9. Gestión de Incidentes de la Seguridad de la Información
10. Cumplimiento

Estos dominios están compuestos por un conjunto de subdominios y sus correspondientes controles, los cuales han de ser abordados adoptando un modelo PHVA (Planificar, Actuar, Verificar y Actuar).

El enfoque basado en procesos para la gestión de la seguridad de la información, presentado en esta norma, estimula a los usuarios a hacer énfasis en la importancia de:

a) Comprender los requisitos de seguridad de la información del negocio, y la necesidad de establecer la política y objetivos en relación con la seguridad de la información;
b) Implementar y operar controles para manejar los riesgos de seguridad de la información de una organización en el contexto de los riesgos globales del negocio de la organización;
c) El seguimiento y revisión del desempeño y eficacia del SGSI, y
d) La mejora continua basada en la medición del objetivos.

La comprensión de la finalidad y de los procesos involucrados en la aplicación de la norma ISO 27 001 es un requisito fundamental para la adecuada contribución desde el Derecho al Sistema de Gestión de Seguridad de la Información en una organización, tema que no puede obviar el operador jurídico que como consultor intervenga.

Al respecto se identifican seis grandes temas desde la perspectiva jurídica: La protección de datos personales; la contratación de bienes informáticos y telemáticos; el derecho laboral y prestación de servicios, respecto de la regulación de aspectos tecnológicos; los servicios de comercio electrónico; la propiedad intelectual y el tratamiento de los incidentes informáticos.

Para el éxito de las recomendaciones jurídicas en materia de seguridad de la información es clave que las mismas estén alineadas con la estrategia y política general que la organización adopte en esta materia.

De los dominios consignados en la norma ISO 27 001 se tendrán en cuenta para efectos de las relaciones entre el Derecho y las TIC los siguientes tópicos:

Política de seguridad de la Información

El punto de partida para la gestión de la seguridad de la información dentro de una organización se encuentra en la **política de seguridad**

que se formule; esta carta de navegación habrá de definir el marco tecnológico, gerencial, logístico y jurídico dentro del cual se administren los activos de información.

El dominio A.5 de la Norma ISO 27 001 establece como objetivo de la política de seguridad de la información, el "brindar apoyo y orientación a la dirección con respecto a la seguridad de la información, de acuerdo con los requisitos del negocio y los reglamentos y las leyes pertinentes".

En un medio en el cual la legislación aplicable a los problemas propios de las Tecnologías de la Información y las Comunicaciones es escasa cobra mayor importancia el contenido y desarrollo de la política que en esta materia formule una organización. Adicionalmente, la presencia de las compañías en diferentes sectores económicos implica el cumplimiento de una serie de disposiciones legales, lo que supone dificultades al deber armonizar estas disciplinas particulares con las novedosas tendencias del Derecho Informático.

Desde esta perspectiva, la política de seguridad que formule una organización puede ser el punto de encuentro de todas las disposiciones legales y reglamentos a que pueda estar sometida una organización en desarrollo de su actividad económica en diferentes países.

Cuando la ley no existe o se presentan vacíos en su alcance, corresponde a la política de seguridad servir de guía a la organización en el cumplimiento de sus obligaciones, deberes o cargas. Esta situación ofrece un espacio interesante de autorregulación, en la medida que la organización podrá incorporar las mejores practicas o estándares en una determinada materia; situación, que por demás, facilitará el cumplimiento de la normatividad que deba acatar en diferentes países en los cuales tenga presencia, siempre que las mismas no sean contradictorias.

Adoptar un estándar o una práctica foránea, que no esté normada en un país, implica un cumplimiento más allá de la ley, lo cual en nada perjudica a la organización, sino, por el contrario, puede generar un beneficio importante tanto para ella como para sus grupos de interés.

A manera de ejemplo, tal podría ser el caso de la organización que incorpore una política de protección de datos personales, siguiendo la Directiva 95/46/CE, en el supuesto en el cual el país donde tenga presencia no exista normatividad sobre protección de datos personales, o la existente sea menos exigente al desarrollo que existe en la Unión Europea en la materia.

El reto para los encargados de proteger la información en una organización es comprender que la política de la seguridad tiene la necesidad de considerar aspectos tecnológicos que impactan la ciencia jurídica, y viceversa; por tanto, de manera permanente habrá de revisarse y ajustarse en las guías o directrices que desarrollan la política de seguridad, la evolución del derecho predicable a los asuntos jurídicos y tecnológicos allí contemplados.

La formulación de la política de seguridad en cada organización seguramente habrá de ser diferente, pues la misma debe ser formulado sobre la base de los múltiples riesgos que pesen sobre la información, así como sobre la clase de activos involucrados, y las personas que tengan acceso a la información; factores que no pueden ser dejados al margen de una adecuada gestión de seguridad de la información.

Protección de Datos Personales

Este tema, de gran trascendencia para los seres humanos en la sociedad de la información, aún tiene poca relevancia en el medio latinoamericano, a pesar de constituir un derecho fundamental contenido en la mayoría de las constituciones políticas del mundo[1]. De forma lamentable en el continente americano, con excepción de Argentina, los países no cuentan con una ley que regule de manera integral el derecho fundamental a la

[1] En Colombia, desde 1991, la Constitución Política consagró en su artículo 15 el derecho a la protección de los datos personales, así como al *habeas data*. Como derechos fundamentales requieren de una ley estatutaria que los desarrolle. Después de múltiples intentos, recientemente el Congreso de la República expidió la ley y se encuentra en estudio de la Corte Constitucional para su análisis de constitucionalidad.

intimidad y al *habeas data*, que permita garantizar las libertades públicas de los nacionales de cada país, y en esa medida ser vistos como lugares seguros para la transferencia y tratamiento internacional de datos.

La norma ISO 27 001 señala en el dominio A.15.1.4., referido a la protección de datos, como control el siguiente: "Se debe garantizar la protección de los datos personales y la privacidad, de acuerdo con la legislación y los reglamentos pertinentes y, si se aplica con las cláusulas del contrato".

Para el cumplimiento de este control, quizás el referente internacional más representativo en materia de Protección de Datos Personales es la Directiva 95/46/CE, la cual establece el marco de regulación para los países miembros de la Unión Europea; norma que ha sido desarrollada en cada uno de esos países, producto de la conciencia de los ciudadanos sobre el destino de sus datos y el compromiso del Estado de garantizar las libertades públicas vinculadas a la derecho fundamental a la intimidad.

En este orden de ideas, para ilustrar la problemática de la intimidad[2] y el habeas data ha de entenderse el concepto de dato de carácter personal como "cualquier información concerniente a personas físicas identificadas o identificables"[3], los cuales pueden ser generales, como nombre, domicilio y documento de identidad; hasta información sensible como ideología política, estado de salud, tendencias sexuales, credo religioso, grupo étnico, entre otros.

En la economía actual, los datos de carácter personal están sometidos a tratamientos o procedimientos técnicos que permitan recabarlos,

[2] SUÑE (2000, p. 29). El derecho a la intimidad es un derecho de configuración relativamente reciente en términos de históricos, al menos si se le contempla como un derecho autónomo, desgajado del derecho al honor, puesto que su punto de referencia inicial máas comúnmente aceptado se halla en la obra señera que, con el título "The Right to Privacy", fue publicada en la *Harvard Law Review,* N° 5 de 1890. Este artículo fue redactado por S.D. Warren y L.D. Brandeis.
[3] Ley Orgánica 15/1999 de España. Artículo 3, literal a).

modificarlos, bloquearlos, cancelarlos, cederlos o transferirlos a terceros, así como definir perfiles de distinta naturaleza según la información que se desee obtener, acudiendo para ello a programas de minería de datos, que terminan entregando información valiosa sobre los hábitos de consumo de un individuo.

Esta posibilidad de que terceros puedan acceder sin control a la información personal de un individuo es lo que busca proteger el *habeas data*[4], en el sentido de que la información personal que sea confiada a una organización[5] por su titular, esté amparada y protegida de usos ilegítimos que desconozca ese tutela constitucional que cada individuo tiene sobre su información, así como sobre los perfiles diseñados a partir de sus hábitos, comportamientos y tendencias.

En consecuencia, en materia de seguridad de la información y en desarrollo de este Derecho Fundamental, consignado en el dominio de la norma ISO 27 001 antes citado, debe procurarse por la organización que toda base de datos, tenga connotación comercial o no, cuente con las medidas jurídicas, tecnológicas y físicas que aseguren su protección.

La ausencia de una norma como la europea antes mencionada, en un determinado país, conduce a que gran parte de las bases de datos en poder de entidades públicas como privadas sean explotadas de manera ilegítima, a partir del abuso, ignorancia o desconocimiento de los derechos que tienen los individuos sobre la información confiada.

Lo anterior no pretende limitar el uso de las bases de datos, sino llamar la atención sobre la posibilidad de explotar la información dentro de unos

[4] SUÑE (2000, p. 29). Citando a Warren y Bradeis dice: "El common law garantiza a cada persona el derecho a decidir hasta que punto pueden ser comunicados a otros sus pensamientos, sentimientos y emociones".

[5] OLLATILU (2006). Organizations that collect personal identifiable information, including, but no limited to, consumer reporting companies, lenders, insurers, employers, landlords, government agencies, mortgage brokers, automobile dealers, attorneys, private investigators and debt collectors, are responsible for safeguarding this resources.

parámetros legítimos, que atiendan los principios de consentimiento, finalidad, calidad, veracidad, conservación, entre otros, que caracterizan el tratamiento responsable de la información personal.

En materia de seguridad de la información, tratándose de datos personales, ha de recordarse que la protección a brindar se predica tanto de personas naturales como de personas jurídicas[6]. En cumplimiento del postulado del dominio de la norma ISO 27 001, las organizaciones en la ejecución de proyectos contratados con terceros no pueden dejar al margen la regulación contractual de las obligaciones que éstos deben acatar para asegurar que las medidas de seguridad de la información personal adoptadas por ella sean realmente eficaces.

Los deberes, cargas, obligaciones, riesgos y sanciones[7] que puedan pesar sobre los titulares de las bases de datos personales no desaparecen por encargar a terceros el tratamiento de tales datos, por el contrario, pueden incrementar el valor de estas por no haber tomado las medidas adecuadas. Igualmente, los terceros a los cuales se encomiende el tratamiento de bases de datos con información personal son responsables por el uso ilegítimo que hagan de los mismos, y en consecuencia serán responsables de los perjuicios que irroguen a los individuos titulares de los datos personales.

[6] Sentencia T-46 de 1997. Si las personas jurídicas son titulares del derecho fundamental al buen nombre, en consecuencia, lo son también del derecho al *habeas data*, toda vez que este último derecho, reconocido por el artículo 15 de la Carta Política, existe justamente como garantía de aquél y del derecho a la intimidad personal y familiar. En efecto, la sola lectura del texto constitucional mencionado pone de relieve que el *habeas data*, entendido por el constituyente como el derecho de las personas a "conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y archivos de entidades públicas y privadas", se vincula directamente con los derechos a la intimidad y buen nombre a los que se refiere el primer enunciado del artículo superior en comento. De esta manera, el *habeas data* viene a ser como una garantía de estos dos derechos, siendo por lo tanto accesorio de ellos. Así, si le es reconocido a las personas jurídicas el derecho al buen nombre, forzoso es concluir que les debe ser reconocido igualmente el derecho al *habeas data*, ya que en este caso lo accesorio debe seguir la suerte de lo principal.

[7] La Ley 221 de 1007, aprobada recientemente en Colombia, pendiente del examen de constitucionalidad, contempla sanciones de hasta 650 millones de pesos por cada violación a lo dispuesto en ella. La ley argentina establece sanciones de hasta 32 mil dólares y la española contempla sanciones de hasta 30 mil euros.

El no dotar a las bases de datos personales de la seguridad y medidas de protección adecuadas por parte de las organizaciones que las poseen, en primer lugar implica un desconocimiento de lo dispuesto en la norma ISO 27 001; segundo, la violación a un derecho constitucional, el cual puede ser garantizado a través de acciones de tutela, con el riesgo de indemnizar los perjuicios causados; tercero, es una limitante en el comercio internacional, pues los países europeos y algunos latinoamericanos impiden la transferencia internacional de datos con países o empresas que no garanticen un nivel adecuado de protección de datos (no debe olvidarse el origen europeo de esta norma ISO), y por último, las sanciones que tienden a imponerse por violación a este derecho fundamental de la protección de datos personales y habeas data son muy cuantiosas en términos económicos.

Contratación de bienes informáticos y servicios telemáticos

El Derecho Privado tiene sus fuentes más importantes en los códigos civiles y en los códigos de comercio de cada país, normas que por su antigüedad obviamente no prevén la **contratación de bienes informáticos y servicios telemáticos.** La contratación típica está estructurada sobre una economía de bienes tangibles, los cuales no representan problemática desde la perspectiva de las tecnologías de la información y las comunicaciones.

En el dominio A.10 de la gestión de comunicaciones y operaciones y en el dominio A.12 la norma ISO 27 001 habla de la adquisición, desarrollo y mantenimiento de sistemas de información. Estos dominios representan una parte importante de las falencias que se identifican en el análisis de riesgos en una organización, por cuanto existe el error de tratar de tipificar los proyectos informáticos en contratos como la compraventa, el arrendamiento, el suministro, entre otros, los cuales por razones obvias no responden de manera segura ni apropiada a la regulación de los múltiples aspectos tecnológicos que han de regularse en un contrato informático[8] o telemático.

[8] CALLE (2002). El contrato informatico sobre bienes inmateriales susceptibles de digitalizacion (p. 187). Tesina de grado, Universidad Complutense de Madrid.

Las características propias de los proyectos informáticos conducen a regulaciones no contempladas por la legislación positiva, que encuentran su fuente de regulación en la autonomía de la voluntad privada; esta realidad ratifica la concepción atípica[9] de los contratos sobre bienes intangibles susceptibles de digitalización.

Por tanto, la regulación de estos contratos debe ser suplida por la voluntad de las partes, los principios generales de contratación, el derecho internacional y demás fuentes, de manera que cada uno de los aspectos de la relación jurídica a ejecutar entre las partes sea definido y consignado en el cuerpo del contrato y sus anexos respectivos, advirtiendo la importancia de regular de manera independiente las diferentes prestaciones jurídicas que puedan estar vinculadas al contrato principal.

En la práctica se encuentra que los equipos de informática trabajan al margen de los equipos jurídicos dentro de las organizaciones en lo que tiene que ver con los procesos de contratación informática, situación que genera una ruptura en la tarea de gestionar de manera eficaz la seguridad de los activos de la información. No son extraños los casos en los cuales aspectos sencillos como la definición de la propiedad intelectual sobre los intangibles contratados no están formalizados, o existen reclamaciones sobre la propiedad de los mismos por quienes los han desarrollado.

Ante esta realidad se aconseja que exista un proceso de comunicación clara entre las áreas involucradas en la contratación de intangibles

---

El contrato informático, como una entidad negocial independiente y autónoma, se presenta cuando el objeto de contratación recae exclusivamente sobre bienes inmateriales susceptibles de digitalización, como lo es el *software*, en todas sus formas y vertientes, como lo son las bases de datos y también las obras o productos multimedia.

[9] JORDANO (1993, p. 20). Para que exista un contrato atípico tiene que faltar al menos uno de los elementos esenciales del negocio determinado o de un esquema legal para que pueda decirse que se está frente a un contrato típico. Por tanto será atípico aquel contrato que, aun mencionado por la Ley, está desprovisto de una normación específica, a menos que la mención del contrato se haga por la ley en tal lugar que se pueda inducir por vía de remisión la disciplina jurídica aplicable.

digitales, en aras de que las inversiones en tecnología para la organización sean seguras. Los operadores jurídicos de la organización, responsables de la contratación de esta clase de bienes y servicios, han de tener en cuenta que la adquisición, desarrollo y mantenimiento de obras digitalizadas requieren de regulaciones apropiadas a la naturaleza incorpórea del objeto contratado, que exigen armonizar lo jurídico con lo técnico.

Otra buena práctica es la participación de los abogados –conocedores de la tecnología– en los procesos de negociación del proyecto informático o telemático, participación que seguramente permitirá definir de manera clara el alcance del objeto contratado, el cual en ocasiones es bastante abstracto; desechar esta práctica puede conducir a disputas futuras o costo innecesarios para las partes contratantes. En igual sentido, es válida la presencia de un operador jurídico, con el perfil recomendado, en la etapa de ejecución del proyecto, aspecto de dotará de seguridad el compromiso de las obligaciones pactadas.

La contratación de desarrollo de programas de ordenador o integración de sistemas de información, por las dificultades que supone dimensionar el alcance de los mismos y los valores asociados, apunta a separar las etapas de toma de requerimientos, análisis y diseño, de las etapas de desarrollo, pruebas y puesta en producción de la aplicación informática. Lo anterior permite a las partes contratantes cumplir con los tiempos previstos, recursos económicos comprometidos, identificación plena de requerimientos, cumplimiento de las funcionalidades pretendidas al contratar, entre otros aspectos.

En términos de contratos de licencia de uso sobre aplicaciones informáticas normalmente media la entrega de la correspondiente licencia y del ejecutable que permite la instalación de sistema de información. La ISO 27 001 plantea la importancia de que la organización pueda garantizar el acceso al código fuente de la aplicación cuyo uso se concede, en caso de que el titular del programa de ordenador desaparezca del mercado; situación que exige regular tal hipótesis en términos de seguridad de la información.

Igualmente, las organizaciones contratan servicios telemáticos de diversa naturaleza, como puede ser la instalación de redes de comunicaciones privadas, la gestión, soporte y mantenimiento de las mismas, así como servicios que se soporten en éstas; servicios que particularmente son provistos por terceros.

Por tanto, la **gestión de redes** de comunicaciones, tratándose de servicios de telecomunicaciones, aconseja adoptar medidas que vayan más allá de la prestación eficiente de tales servicios, siendo fundamental que a nivel tecnológico se adopten medidas que otorguen estabilidad a la red, ofrezcan la velocidad requerida para el funcionamiento de los diferentes equipos y sistemas, y gocen de protocolos seguros que permitan reaccionar a los ataques a los sistemas o a las redes mismas. En los contratos de esta naturaleza no es extraño encontrar omisiones en este sentido, las cuales pueden ser resultado del desconocimiento de lo tecnológico o de la ausencia de reflexiones sobre el impacto jurídico que en materia de responsabilidad derivan para las partes involucradas. Obviar la regulación de aspectos como los mencionados puede ser fuente de conflictos o interpretaciones ambiguas sobre el alcance de las obligaciones que corresponden a las partes.

En este tópico de la seguridad de la información vale cuestionarse sobre lo siguiente: ¿Cómo verificar la estabilidad de la red? ¿Cuáles son los parámetros aceptables de acuerdo con la tecnología y la robustez de la misma? ¿Cuáles son los niveles de servicios pactados? ¿Son éstos suficientes acorde con la naturaleza del negocio? El protocolo de los equipos de comunicaciones ¿es suficiente para seguridad de la información que se trasmite, o se requiere adoptar medidas de seguridad adicionales? ¿Cuáles pueden ser los factores exógenos que disminuyan la eficiencia de las comunicaciones?

Estos asuntos han de ser regulados en los contratos telemáticos, advirtiendo que la mayoría de ellos son de corte tecnológico, pero no por ello, se insiste, deben ser desatendidos en la relación contractual, salvo que dentro de la organización no exista preocupación por la seguridad de la información y por la gestión que la misma empresa o terceros le proporcionen.

Políticas Laborales y Prestación de Servicios por Terceros

Las relaciones laborales son aspectos también comprendidos en el alcance de la norma ISO 27 001. En este sentido, existe un dominio específico –A.8.– denominado Seguridad de los Recursos Humanos, el cual establece un conjunto de controles que se deben tener presentes antes, durante y después de la terminación de la contratación laboral[10]. Este componente involucra las relaciones de servicios con terceros, advirtiendo que las obligaciones aplican no sólo a las personas jurídicas o naturales con quienes se contrata, sino también a las relaciones laborales con sus empleados o relaciones de servicios con sus subcontratistas; ello con el fin de dotar de seguridad todo el ciclo de personas involucradas con los activos de información de una organización.

El dominio A.8.1., referido a la seguridad de los recursos humanos antes de la contratación laboral, dispone como objetivo:

> Asegurar que los empleados, contratistas y usuario por tercera parte entienda sus responsabilidades y son adecuados para los roles para los que se los considera, y reducir el riesgo de robo, fraude o uso inadecuado de las instalaciones.

El dominio A.8.2., referido a la seguridad de los recursos humanos durante la contratación laboral, establece como objetivo:

> Asegurar que todos los empleados, contratistas y usuarios de terceras partes estén conscientes de las amenazas y preocupaciones respecto de la seguridad de la información, sus responsabilidades y sus deberes, y que estén equipados para apoyar la política de seguridad de la organización en el transcurso de su trabajo normal, al igual que reducir el riesgo de error humano.

[10] La palabra "contratación laboral" para efectos de la interpretación de la norma cubre las siguientes situaciones: Empleo de personas (temporal o indefinido), asignación de roles de trabajo, cambio de roles de trabajo, asignaciones de contratos y la terminación de cualquiera de estos acuerdos.

El dominio A.8.3., referido a la seguridad de los recursos humanos, tiene el siguiente objetivo en la norma:

> Asegurar que los empleados, contratistas y los usuarios de terceras partes salen de la organización o cambian su contrato de forma ordenada.

Estos tres momentos de la contratación laboral o de servicios han de verse en el contexto de la relación entre los recursos humanos y los activos de la información a los que éstos tengan acceso.

Pensar en estos tres momentos de la relación laboral o de servicios requiere focalizar la adopción de las medidas de seguridad con relación a los retos que las tecnologías de la información y las comunicaciones plantean al Derecho en esta materia.

Existen problemáticas nada pacíficas respecto del uso de herramientas de trabajo como el correo electrónico de la organización por parte de los empleados, en el sentido de establecer si la información allí contenida puede ser auditada por la empresa, o si tiene carácter personal, o cuál es el justo medio que pueda dar una respuesta justa a la problemática.

La tecnología permite al administrador del sistema tener conocimiento sobre los sitios de la red que un usuario visita durante su jornada laboral o de servicios, puede establecer el tiempo que éste ha estado navegando un contenido determinado; entonces, se pregunta si esta vigilancia atenta contra los derechos de la persona ¿Se vulnera la intimidad del empleado? ¿El empleado está incumpliendo con sus obligaciones? ¿Esta es una justa causa para imponer la suspensión o la terminación de la relación? La respuesta está determinada en la definición de las políticas laborales y sus desarrollos que adopte una organización en relación con sus empleados o con los contratistas.

El uso de las herramientas tecnológicas es un proceso cultural, en el sentido que las personas desconocen los riesgos que devienen de su uso. De hecho, las fallas de seguridad o la pérdida de la información, la mayoría de las veces obedecen al desconocimiento de los riesgos que conlleva el uso inadecuado de las mismas por parte de los mismos operadores de la organización.

Es deber de la organización capacitar al personal sobre los riesgos inherentes al uso de las tecnologías de la información y las comunicaciones, dar a conocer la importancia que los activos de la información tienen, comunicar los riesgos que pesan sobre la información, las prácticas de ingeniería social de la que se aprovechan los *hackers* y *crackers* para atentar contra la seguridad de la organización; aspectos que exigen el trabajo en equipo entre los diferentes actores para consolidar un sistema eficaz de gestión de la seguridad de la información.

No menos importante es asegurarse de que las personas tengan acceso a los sistemas con base en los perfiles y autorizaciones definidas, y que a la desvinculación éstos sean cancelados efectivamente, tareas de los administradores de los sistemas de información de una compañía.

Del análisis de riesgos que se hace como punto de partida de la aplicación de la norma ISO 27 001, corresponde al operador jurídico sugerir los tópicos que se deben tener presentes en los contratos laborales y en los contratos de prestación de servicios, en lo que se refiere al manejo, administración, uso, entrega y devolución de los activos de información a los que se otorga acceso, así como a las consecuencias derivadas de la perdida, hurto, alteración o modificación de la información entregada y confiada a estas personas.

Las reflexiones expuestas constituyen sólo la punta de iceberg de muchos otros temas que desde la tecnología impactan las relaciones laborales o de prestación de servicios, los cuales han de ser identificados y regulados, con el fin de poder cumplir la finalidad que esta materia proponen los tres objetivos concebidos por la norma ISO 27 001.

Servicios de Comercio Electrónico

Para efectos de la norma ISO 27 001, el comercio electrónico debe entenderse más allá del intercambio electrónico de bienes y servicios, sea éste directo o indirecto; ha de entenderse dentro de esta acepción la transmisión de información por vías electrónicas, sean éstas públicas como Internet o privadas como una Intranet, EDI, Swift, entre otras.

El control de la norma ISO que hace referencia a esta materia es el A.10.9, cuyo objetivo consiste en "Garantizar la seguridad de los servicios de comercio electrónico y su utilización segura".

Conforme a este control, el cual hace parte de un dominio superior como es la gestión de comunicaciones y operaciones –A.10–, corresponde al operador jurídico en los temas de su competencia tener presente que: (i) que la información que se trasmite por las redes públicas debe estar protegida contra actividades fraudulentas; (ii) las eventuales disputas por contratos; y (iii) la divulgación o modificación no autorizada de la información.

El referente colombiano que se debe tener en cuenta en este dominio es la Ley 527 de 1999, la cual hace referencia a la validez de los mensajes de datos y a la firma digital, que tiene como objetivo principal dar validez a los mensajes de datos remitidos por vías electrónicas, cosa diferente de regular las actividades de comercio electrónico que puedan celebrarse por la red.

La preocupación para las organizaciones, en términos de seguridad de la información, respecto de las transacciones que operan a través de canales electrónicos, es que éstas cuenten con los atributos de integridad, disponibilidad, confidencialidad, y no repudio, atributo, este último, que se logra con la implementación de herramientas como las firmas digitales de clave pública y privada, de carácter asimétrico.

El crecimiento del comercio electrónico en Colombia no es representativo, situación que atiende a la escasa confianza del consumidor en los medios electrónicos a través de los cuales se surten las transacciones de bienes y servicios. Sumado a lo anterior, existe un desconocimiento en el consumidor sobre la existencia de protocolos seguros que permiten minimizar los riesgos al suministrar información, sea esta personal o económica.

De otra parte, se requiere crear en el consumidor la confianza en este nuevo canal de negocios; para ello éste debe sentir las misma tranquilidad que percibe cuando adquiere bienes o servicios en el mundo

real; sin embargo, los portales o sitios virtuales, incluso de grandes organizaciones, guardan silencio sobre información tan básica como puede ser la ubicación geográfica de la misma, sobre el responsable de atender las peticiones, quejas y reclamos de los consumidores, sobre los mecanismos o escenarios en los cuales se puedan ventilar las diferencias nacidas de la adquisición de bienes y servicios relacionadas con las garantías de estos, entre otros aspectos.

El crecimiento del comercio electrónico está determinado sólo por el consumidor, y para lograr la confianza de éste se requiere garantizar sus derechos, y concienciar a quienes comercializan bienes y servicios en la red que éstos tienen deberes y obligaciones respecto de estos protagonistas. Por su parte, es hora que el Estado modernice las disposiciones relacionadas con el derecho del consumo, que el consumidor encuentre respuestas ágiles y oportunas en la autoridad competente en esta materia; sin estos cambios será lento el crecimiento de este nuevo canal de negocios.

Las mismas organizaciones proveedoras de bienes y servicios por vías electrónicas tienen la capacidad y los medios para autorregular su comportamiento económico. En este orden de ideas, en el portal de las organizaciones se puede: informar acerca de las condiciones generales de contratación, la responsabilidad que asume el proveedor, dar a conocer los derechos que tiene el consumidor, generar la factura electrónica correspondiente, establecer las condiciones para la materialización de las garantías, informar sobre la territorialidad del impuesto, entre otros aspectos que se deben tener en cuenta para conquistar al consumidor.

En Europa Continental los gremios han avanzado en la adopción de códigos de conducta empresarial, que buscan dotar de seguridad a las actividades de comercio electrónico, incorporando en algunos de ellos procedimientos de solución de controversias que delegan en terceros la decisión final, obligándose previamente las empresas titulares de los portales a someterse a las decisiones que se adopten por árbitros o amigables componedores.

En este sentido, se han adoptado sellos que generan confianza en el consumidor, los cuales son divulgados en los portales Web, de suerte que el consumidor al adquirir bienes y servicios sabe de antemano que cualquier disputa puede ser resuelta de manera ágil, oportuna y en forma vinculante para el proveedor.

Las acciones que se adopten en materia de seguridad, en términos de la ISO 27 001, respecto de los servicios de comercio electrónico han de atender la naturaleza del modelo de negocio, de las transacciones que se realicen, los datos que se transmitan y de los riesgos inherentes a las actividades mismas; por tanto, en cada caso habrá que identificar un catálogo de acciones a aplicar.

Propiedad Intelectual

En la era industrial, los activos productivos de carácter tangibles pueden ser asegurados mediante pólizas, de suerte que en el evento de un siniestro el propietario puede afectar la póliza de seguros para recuperar su inversión; hoy día, en la era de la sociedad de la información, los activos productivos son intangibles, incorpóreos, entonces, ¿cómo protegerlos? Uno de los mecanismos que sirven para proteger este tipo de bienes es la **propiedad intelectual**.

El dominio A.15.1.4 de la norma ISO 27 001 establece en materia de cumplimiento la necesidad de acatar las disposiciones sobre propiedad intelectual en aras de la seguridad de la información. El control que establece la norma consiste en "implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legales, reglamentarios, y contractuales sobre el uso del material con respecto al cual puedan existir derechos de propiedad intelectual y sobre el uso de productos de software patentados".

Bienes como el *software*[11], las bases de datos[12], las obras multimedia, los sistemas inteligentes son activos de valor incalculable para cualquier

[11]Artículo 3 de la Decisión 351 de 1993 de la CAN. Expresión de un conjunto de instrucciones mediante palabras, códigos, planes o en cualquier otra forma que, al ser

organización, que ameritan adoptar medidas especiales para lograr una protección eficaz.

En materia de protección del *software* es importante tener en cuenta que algunas legislaciones, como la europea, establecen que también es objeto de protección la documentación preparatoria de los programas de ordenador, consideración que aclara uno de los aspectos que pueden ser fuente de controversia en el sector, máxime cuando existen incumplimientos o terminaciones anticipadas de los contratos informáticos.

La protección de los bienes intangibles susceptibles de digitalización encuentra vacíos importantes en la regulación aplicable en términos de propiedad intelectual, pues la asimilación que las leyes hacen a obras literarias para efectos de protección plantea cuestionamientos importantes sobre su eficacia.

En materia de seguridad de la información se requiere imprimir claridad a los contratos de desarrollo de aplicaciones informáticas en lo que respecta a la titularidad de los derechos de propiedad intelectual, los cuales en ocasiones son vagos, abstractos o no son formalizados. Es preciso tener en cuenta que en la legislación colombiana se requiere expresar de manera clara cuáles son los derechos patrimoniales que se ceden, así como cumplir con la formalidad de la escritura pública o del documento privado con reconocimiento del contenido del documento ante notario, formalidades que en la mayoría de las veces son obviadas, con lo cual se afecta la correcta protección de activos susceptibles de digitalización.

---

incorporadas en un dispositivo de lectura automatizada, es capaz de hacer que un ordenador –un aparato electrónico o similar capaz de elaborar informaciones–, ejecute determinada tarea u obtenga determinado resultado. El programa de ordenador comprende también la documentación técnica y los manuales de uso.

[12] Directiva 96/9/CE. Tendrán la consideración de 'bases de datos' las recopilaciones de obras, de datos o de otros elementos independientes dispuestos de manera sistemática o metódica y accesible individualmente por medios electrónicos o de otra forma. La protección prevista por la presente Directiva no se aplicará a los programas de ordenador utilizados en la fabricación o en el funcionamiento de las bases de datos accesibles por medios electrónicos.

Ergo, la propiedad intelectual, en sus modalidades de Derechos de Autor y Propiedad Industrial, son temas transversales a la seguridad de la información corporativa, la cual exige de medidas que aseguren la protección de la misma.

Una organización, además de velar por asegurar la titularidad de los derechos patrimoniales sobre las obras informáticas encargadas, debe preocuparse también porque sus sistemas de información tengan las licencias correspondientes; preocupación que debe extenderse a exigir que sus proveedores cuenten con las licencias de uso de los programas informáticos, que soportan la prestación de los servicios informáticos contratados.

El equipo de seguridad de la organización debe informar sobre la prohibición de instalar en los ordenadores programas que no tengan licencias, o programas que puedan poner en riesgos la seguridad de los sistemas o de los equipos; eventualidades que deben estar reguladas en el marco de la política laboral y de servicios que tenga la organización.

El cumplimiento de las normas sobre propiedad intelectual debe ser una de las cláusulas principales en todo proyecto de la organización; no de otra forma puede extenderse a terceros la obligación de respeto sobre los derechos de propios o de terceros.

Otra recomendación en desarrollo de la norma ISO 27 001 es otorgar transparencia en la titularidad de los desarrollos, descubrimientos, adelantos, innovaciones y nuevas creaciones de los empleados en desarrollo de la relación laboral, los cuales pertenecen a la empresa, salvo acuerdo en contrario. Al respecto se cuestiona si las cláusulas que se acostumbran pactar en los contratos laborales, previa la existencia de los desarrollos o innovaciones, dotan de seguridad adecuada la propiedad que tiene la empresa sobre la información desarrollada, o si se requiere de acuerdos posteriores a la creación de la obra o patente.

A pesar de que la norma ISO 27 001 hace referencia a derechos de propiedad intelectual, es importante tomar medidas de seguridad respecto de información que puede no estar cobijada por esta regulación,

como puede ser la información empresarial, *know how* estratégico o secretos empresariales de la organización.

Las normas de propiedad intelectual establecen cuáles bienes son sujetos de protección, cuáles derechos asisten a sus titulares, la duración de la protección y demás aspectos inherentes a su seguridad jurídica.

Ahora bien, además de las normas de propiedad intelectual es importante en el desarrollo de proyectos informáticos tener presente que la relación entre las partes debe atender los principios de buena fe y lealtad contractual, en el sentido que debe evitarse incurrir en prácticas que la ley considera como contrarias a la sana y leal competencia.

En consecuencia, las normas sobre competencia desleal[13] se convierten en herramientas de protección de la seguridad de la información de las organizaciones, complementando así la protección que deriva de las normas nacionales y comunitarias sobre propiedad intelectual.

Tratamiento Legal de los Incidentes Informáticos

El concepto de seguridad informática es de reciente data, y tal vez fue en los últimos 15 años en los que adquirió un nombre propio. El fenómeno de atacar las redes de comunicaciones se inicia en los albores del siglo XX, cuando piratas del mundo eléctrico/ electrónico empezaron a vulnerar los sistemas de terceros, tras la aparición de las líneas de comunicaciones telegráficas (Álvarez y otros, p. 20).

> (…) el estudio sobre seguridad y crimen informático del Computer Security Institute (en adelante CSI), arroja datos de los que se estiman las perdidas de los sistemas analizados en más de 141 millones de dólares por problemas de seguridad. Esta cantidad nada despreciable impulsa la teoría de que en seguridad informática el dinero siempre se gasta: o bien antes, en proteger, o bien posteriormente en recuperar (Álvarez y otros, p. 20).

[13] Ley 256 de 1996. Esta ley es concordante con el numeral 1º del artículo 10 bis del Convenio de París, aprobado mediante la Ley 178 de 1994.

Una de las mayores preocupaciones de las organizaciones, y en particular de los responsables del área informática, es el tratamiento de los incidentes informáticos, es decir, de aquellas situaciones que atentan, vulneran o destruyen información valiosa de la organización, además del impacto psicológico y económico que puede generar en el mercado accionario o en los accionistas cuando se informa sobre intrusiones y pérdidas[14] de información en un ente empresarial.

Quizás lo descrito en los párrafos anteriores refleja la importancia del concepto de seguridad de la información. Sin embargo, para terminar de reforzar la importancia del tema para las empresas, si aún existiese alguna duda, basta conocer un listado de los delitos cometidos por el *cracker* más reconocido en la historia reciente, Kevin Mitnick. Fue acusado de diversos crímenes: creación de números telefónicos no tarificables; robo de más de 20 000 números de tarjetas de crédito; precursor de la falsificación de dirección IP conocida como IP Spoofing; burla al FBI durante más de 2 años; robo de *software* de terminales telefónicos; control de varios centros de conmutación en USA; acceso ilegal a múltiples sistemas del gobierno de USA; entre otros incidentes de seguridad.

Los delitos cometidos por este ex delincuente informático –quien hoy es un experto consultor en seguridad, después de purgar varios años de prisión– reflejan no sólo los tipos de conductas que configuran un incidente informático, sino también la posibilidad de que cualquier empresa sea víctima de un ataque a sus activos, sistemas o redes de información.

Entrando en materia, se tiene que el dominio A.13 de la norma ISO 27 001 establece como objetivo de la gestión de los incidentes de seguridad de la información la necesidad de "asegurar que los eventos y las debilidades de la seguridad asociados con los sistemas de información se comunican de forma tal que permiten tomar las acciones correctivas oportunamente…"

[14] Un estudio del año 2003 indicaba que en ese período se habían producido 100 000 incidentes de seguridad y se habían informado mas de 3000 vulnerabilidades en sistemas de información.

En los asuntos de competencia del Derecho en materia de incidentes informáticos, descritos en el dominio A.13.2.3., se invita a que las organizaciones sean proactivas en la recolección de la evidencia de los mismos; en este sentido, el control establece que cuando una acción de seguimiento contra una persona u organización después de un incidente de seguridad de la información implica acciones legales (civiles o penales), "la evidencia se debe recolectar, retener y presentar para cumplir con las reglas para la evidencia establecidas en la jurisdicción competente".

Se puede decir que un "incidente de seguridad" consiste en una conducta criminal o no desarrollada por un individuo contra sistemas de información, redes de comunicaciones, activos de información, con el fin de alterar, copiar, simular, hurtar, destruir, indisponer, bloquear y/o sabotear éstos. Estos comportamientos pueden ser desplegados por intrusos informáticos, extorsionistas, terroristas, espías industriales, usuarios de los sistemas o de las redes, ex empleados y millones de adolescentes con conocimientos meridianos en ataques informáticos.

Para el cumplimiento de la norma en materia de recolección de las pruebas de un incidente es importante tener en cuenta que tales actividades requieren del apoyo de la informática forense[15]. Ante la sospecha de la comisión de un incidente informático, el análisis forense permitirá capturar, procesar e investigar información procedente de sistemas informáticos, mediante la aplicación de una metodología que permita dar mismidad y autenticidad a la prueba a ser utilizada en una causa judicial.

Frente a la presencia de un incidente informático corresponde al equipo de seguridad reaccionar frente al incidente siguiendo este esquema de 4 pasos: identificar los equipos que pueden contener evidencia del

[15] Es la encargada de analizar sistemas informáticos en busca de evidencia que colabore en llevar adelante una causa judicial. Esta práctica suele ser usada en la persecución de criminales, litigios civiles, investigación de seguros; y en organizaciones, con el fin de recolectar pruebas de comportamientos contrarios a la ley, a los estatutos, a los reglamentos o a las políticas existentes en materia de seguridad.

incidente acaecido; preservar la evidencia de los daños accidentales o intencionales, lo cual se logra efectuando una copia o imagen espejada exacta del medio analizado; examinar la imagen de la copia original, buscando evidencia o información sobre los hechos que suponen la existencia de un incidente de seguridad; y por último, escribir un reporte, finalizada la investigación, en el cual debe hacerse referencia de los hallazgos a la persona indicada para tomar una decisión, bien sea a un juez o al presidente de la compañía.

El problema de la recolección de incidentes informáticos radica en aplicar protocolos que permitan un tratamiento probatorio conforme a la ley, de manera que la prueba obtenida tenga la legalidad requerida para ser aceptada en una causa judicial, sea ésta de naturaleza penal, civil, administrativa o disciplinaria.

En términos gráficos, el tratamiento que se debe realizar respecto de la comisión de un incidente informático demanda aplicar técnicas equivalentes a las practicadas para buscar la evidencia de un delito cometido en el mundo real.

No obstante, existen diferencias sustanciales al recabar la evidencia de incidentes informáticos, pues la prueba de tales acciones muchas de las veces pueden desaparecer o ser eliminadas por su volatilidad; característica que exige que la intervención del equipo de seguridad se realice tan pronto como se tenga conocimiento o sospecha de la ocurrencia de un ataque a los activos de información de una organización.

Corresponde precisar que no sólo se trata de encontrar la evidencia del delito, ataque o intrusión, de carácter informático, sino que además se precisa la limpieza en la práctica de la misma, pues en caso de alterarla o desaparecer ésta, será imposible demostrar la comisión del incidente, y por esta vía, aplicar las sanciones o penas a que haya lugar, así como el resarcimiento de los perjuicios que se causen.

Ahora bien, un incidente informático puede o no tener carácter judicial, y una organización seguramente definirá por razones estratégicas hacer pública o no su condición de víctima de un ataque a sus

activos de información. Así mismo, la definición de si un incidente informático tiene carácter judicial es determinada por la tipicidad legal de la conducta del infractor; para el efecto habrá de contrastarse la misma contra los tipos penales consagrados en la legislación de cada país.

Los sistemas acusatorios permiten que los particulares puedan participar en la recolección de la evidencia de la comisión de determinados hechos potencialmente punibles, previo cumplimiento de los requisitos que exige la ley procesal. Esta facultad es fundamental en materia de oportunidad y pericia a la hora de recabar la evidencia de un incidente de naturaleza informática.

La recolección de la evidencia de un incidente informático, por las particularidades y características del mismo, implica la participación de un equipo interdisciplinario de profesionales capacitados en identificar, recolectar, documentar y proteger las evidencias del incidente, apoyándose en técnicas de criminalísticas forenses, que permitan iniciar las acciones penales y civiles derivadas de la ocurrencia de estos incidentes.

Al respecto es importante conocer las medidas que en el marco del sistema acusatorio de cada país existan para que los mismos particulares, en este caso las organizaciones afectadas, puedan recabar las pruebas de los hechos punibles cometidos, teniendo en cuenta la cadena de custodia, entre otras herramientas, que asegure las características originales de los elementos físicos de la prueba del incidente, desde la protección de la escena, recolección, embalaje, transporte, análisis, almacenamiento, preservación, recuperación y disponibilidad final de éstos, identificando al responsable en cada una de sus etapas y los elementos que correspondan al caso investigado.

En materia de gestión de la seguridad de la información, éste es quizás uno de los mayores retos que enfrenta una organización, en particular, por la facilidad y creciente tendencia a atentar contra los sistemas de información, así como el desconocimiento y la escasa formación en la recolección de la evidencia de los incidentes informáticos.

CONCLUSIONES

El siglo XXI, caracterizado por la sociedad de la información, implica que todas las organizaciones, sean éstas públicas o privadas, nacionales o transnacionales, cualquiera que sea el sector económico en que desarrollen su objeto social, están relacionadas con la tecnología informática, sea que adquieran o desarrollen activos de información; realidad que hace que la seguridad sea algo que demande su permanente atención.

Las Tecnologías de la Información y las Comunicaciones reclaman del Derecho respuestas innovadoras y globales respecto de los retos que le son intrínsecos; por tanto, los operadores jurídicos deben estar capacitados y entrenados para apoyar a la sociedad en la solución de las problemáticas propias de la relación Informática-Derecho.

El Derecho, como administrador de riesgos, se encarga de dotar de seguridad los diferentes activos de información de una organización; desde esa perspectiva se requiere una gestión jurídica permanente de los riesgos, amenazas y vulnerabilidades, como medio para adoptar las medidas y controles que disminuyan los mismos.

Así como en la sociedad el Derecho es el agente regulador de la convivencia entre los seres humanos, la Norma ISO/NTC 27 001 imparte las reglas y parámetros para que las organizaciones reglamenten y autorregulen la gestión de sus activos de información de manera segura.

Referencias

Libros

ÁLVAREZ, G. y otros. *Seguridad Informática para empresas y particulares*. Madrid: McGraw-Hill.

CALDER, A. (2006). *Nueve claves para el Éxito. Una visión general de la implementación de la norma NTC-ISO/IEC 27001*. Icontec.

CALLE, S. (2002). *El contrato informatico sobre bienes inmateriales susceptibles de digitalizacion*. Tesina de grado, Universidad Complutense de Madrid.

JORDANO, J.B. (1953). *Los contratos atípicos* (p. 20). Madrid: Instituto Editorial Reus.

SUÑE, E. (2000). *Tratado de Derecho Informático. Introducción y Protección de datos personales* (1ª ed., vol. I, p. 7). Editorial Universidad Complutense de Madrid.

Revistas

CANO, J. (2007). Inseguridad Informática y Computación Antiforense: Dos conceptos emergentes de la Seguridad de la Información. *Information System Control Journal*, vol 4,.

OLLATILU, O. (2006). Identifity Theft and Corporations' Due Diligence. *Information Systems Control Journal*, vol. 6.

Leyes y normas

Decisión 351 de 1993 CAN. Artículo 3
Directiva 96/9/CE
Ley Orgánica 15/1999 de Protección de Datos Personales. España
Ley 256 de 1996
Norma ISO 27 001

Sentencias

Sentencia T-46 de 1997