Publicado en enero de 2012 en la Revista:
www.bSecure.com.mx

La Ley y el Desorden 2.0
Unidad de Víctimas del Cibercrimen

Derecho de la Seguridad de la Información

Una rama de las ciencias jurídicas que busca brindar seguridad y confidencialidad a la información

***Por* Joel A. Gómez Treviño**

Desde el año 2006, el municipio de Westchester, Nueva York, se hizo famoso por aprobar la primera ley en su tipo que ordena a los negocios asegurar sus *hotspots*. Dicha ley requiere a todos los negocios comerciales que almacenen, usen o mantengan información personal en medios electrónicos, que tomen medidas mínimas de seguridad, tales como instalar un *firewall*, cambiar el nombre incluido en todos los paquetes de una red inalámbrica (***S****ervice* ***S****et* ***ID****entifier* - *SSID*), o deshabilitar la transmisión SSID. Los que incurran en una violación recibirán una amonestación la primera vez, una multa de $250 dólares la segunda vez y si hay una tercera, $500 dólares.

México no es la excepción. Cada vez existen más elementos para avistar el nacimiento de una nueva área del derecho a la que yo he optado por bautizar como "***derecho de la seguridad de la información***". Podríamos definir a esta rama de las ciencias jurídicas como aquella que busca brindar seguridad y confidencialidad a la información que sea: sensible, reservada, privada, secreto industrial, secreto bancario, secreto profesional, secreto técnico, secreto comercial, secreto de fabricación, dato personal, entre otros.

En términos generales, los propios abogados suelen visualizar solo dos o tres áreas en que se debe proteger o resguardar la información: secretos industriales, secreto bancario y datos personales. Sin embargo, son ya muchas las leyes, reglamentos, códigos y acuerdos que obligan a trabajadores, profesionistas, responsables de datos, empresarios, proveedores e instituciones de crédito a proteger la información contenida en medios físicos, electrónicos y sistema informáticos, contra accesos y usos no autorizados, con la finalidad de conservar su confidencialidad, integridad y disponibilidad.

A continuación le presento un amplio catálogo de obligaciones legales en materia de confidencialidad y seguridad de la información:

Ley Reglamentaria del Artículo 5° Constitucional, relativo al Ejercicio de las Profesiones en el D.F.	ARTICULO 36.- Todo profesionista estará obligado a guardar estrictamente el secreto de los asuntos que se le confíen por sus clientes, salvo los informes que obligatoriamente establezcan las leyes respectivas.
Ley de la Propiedad	Artículo 84.- La persona que guarde un secreto industrial podrá transmitirlo o

Industrial	autorizar su uso a un tercero. El usuario autorizado tendrá la obligación de no divulgar el secreto industrial por ningún medio. Artículo 85.- Toda aquella persona que, con motivo de su trabajo, empleo, cargo, puesto, desempeño de su profesión o relación de negocios, tenga acceso a un secreto industrial del cual se le haya prevenido sobre su confidencialidad, deberá abstenerse de revelarlo sin causa justificada y sin consentimiento de la persona que guarde dicho secreto, o de su usuario autorizado. Artículo 86.- La persona física o moral que contrate a un trabajador que esté laborando o haya laborado o a un profesionista, asesor o consultor que preste o haya prestado sus servicios para otra persona, con el fin de obtener secretos industriales de ésta, será responsable del pago de daños y perjuicios que le ocasione a dicha persona.
Código de Comercio	Artículo 20.- El Registro Público de Comercio operará con un programa informático y con una base de datos central interconectada con las bases de datos de sus oficinas ubicadas en las entidades federativas. Las bases de datos contarán con al menos un respaldo electrónico. Mediante el programa informático se realizará la captura, almacenamiento, custodia, seguridad, consulta, reproducción, verificación, administración y transmisión de la información registral. Artículo 30 bis.- La Secretaría podrá autorizar el acceso a la base de datos del Registro Público de Comercio a personas que así lo soliciten y cumplan con los requisitos para ello, en los términos de este Capítulo, el reglamento respectivo y los lineamientos que emita la Secretaría, sin que dicha autorización implique en ningún caso inscribir o modificar los asientos registrales. La Secretaría expedirá los certificados digitales que utilicen las personas autorizadas para firmar electrónicamente la información relacionada con el Registro Público de Comercio y demás usuarios; asimismo, podrá reconocer para el mismo fin certificados digitales expedidos por otras autoridades certificadoras siempre y cuando, a su juicio, presenten el mismo grado de confiabilidad y cumplan con las medidas de seguridad que al efecto establezca la Secretaría. Artículo 99.- El Firmante deberá: IV. Responder por las obligaciones derivadas del uso no autorizado de su firma, cuando no hubiere obrado con la debida diligencia para impedir su utilización, salvo que el Destinatario conociere de la inseguridad de la Firma Electrónica o no hubiere actuado con la debida diligencia. Artículo 102.- Los Prestadores de Servicios de Certificación que hayan obtenido la acreditación de la Secretaría deberán notificar a ésta la iniciación de la prestación de servicios de certificación dentro de los 45 días naturales siguientes al comienzo de dicha actividad. A) Para que las personas indicadas en el artículo 100 puedan ser Prestadores de

	Servicios de Certificación, se requiere acreditación de la Secretaría, la cual no podrá ser negada si el solicitante cumple los siguientes requisitos, en el entendido de que la Secretaría podrá requerir a los Prestadores de Servicios de Certificación que comprueben la subsistencia del cumplimento de los mismos: I. Solicitar a la Secretaría la acreditación como Prestador de Servicios de Certificación; II. Contar con los elementos humanos, materiales, económicos y tecnológicos requeridos para prestar el servicio, a efecto de garantizar la seguridad de la información y su confidencialidad; III. Contar con procedimientos definidos y específicos para la tramitación del Certificado, y medidas que garanticen la seriedad de los Certificados emitidos, la conservación y consulta de los registros; Artículo 104.- Los Prestadores de Servicios de Certificación deben cumplir las siguientes obligaciones: V. Guardar confidencialidad respecto a la información que haya recibido para la prestación del servicio de certificación; VII. Asegurar las medidas para evitar la alteración de los Certificados y mantener la confidencialidad de los datos en el proceso de generación de los Datos de Creación de la Firma Electrónica;
Ley Federal de Protección al Consumidor	Artículo 76 bis.- Las disposiciones del presente Capítulo aplican a las relaciones entre proveedores y consumidores en las transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología. En la celebración de dichas transacciones se cumplirá con lo siguiente: I. El proveedor utilizará la información proporcionada por el consumidor en forma confidencial, por lo que no podrá difundirla o transmitirla a otros proveedores ajenos a la transacción, salvo autorización expresa del propio consumidor o por requerimiento de autoridad competente; II. El proveedor utilizará alguno de los elementos técnicos disponibles para brindar seguridad y confidencialidad a la información proporcionada por el consumidor e informará a éste, previamente a la celebración de la transacción, de las características generales de dichos elementos;
Ley Federal de Protección de Datos Personales en Posesión de Particulares	Artículo 19.- Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. Artículo 21.- El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable. Artículos 63 y 64.- La multa por incumplir el deber de confidencialidad respecto de cualquier fase del tratamiento de datos personales puede ser de hasta $19,142,400 pesos (320,000 salarios mínimos).
Reglamento de la Ley Federal de Protección de	El artículo 2 define los siguientes términos: V. Medidas de seguridad administrativas: Conjunto de acciones y mecanismos para

Datos Personales en Posesión de Particulares	establecer la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación y clasificación de la información, así como la concienciación, formación y capacitación del personal, en materia de protección de datos personales; VI. Medidas de seguridad físicas: Conjunto de acciones y mecanismos, ya sea que empleen o no la tecnología, destinados para: a) Prevenir el acceso no autorizado, el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, equipo e información; b) Proteger los equipos móviles, portátiles o de fácil remoción, situados dentro o fuera de las instalaciones; c) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento que asegure su disponibilidad, funcionalidad e integridad, y d) Garantizar la eliminación de datos de forma segura; VII. Medidas de seguridad técnicas: Conjunto de actividades, controles o mecanismos con resultado medible, que se valen de la tecnología para asegurar que: a) El acceso a las bases de datos lógicas o a la información en formato lógico sea por usuarios identificados y autorizados; b) El acceso referido en el inciso anterior sea únicamente para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones; c) Se incluyan acciones para la adquisición, operación, desarrollo y mantenimiento de sistemas seguros, y d) Se lleve a cabo la gestión de comunicaciones y operaciones de los recursos informáticos que se utilicen en el tratamiento de datos personales; **Capítulo III.- De las Medidas de Seguridad en el Tratamiento de Datos Personales:** • Alcance • Atenuación de sanciones • Funciones de seguridad • Factores para determinar las medidas de seguridad • Acciones para la seguridad de los datos personales • Actualizaciones de las medidas de seguridad • Vulneraciones de seguridad • Notificación de vulneraciones de seguridad • Información mínima al titular en caso de vulneraciones de seguridad • Medidas correctivas en caso de vulneraciones de seguridad
Ley Federal del Trabajo	Artículo 47.- Son causas de rescisión de la relación de trabajo, sin responsabilidad para el patrón: IX. Revelar el trabajador los secretos de fabricación o dar a conocer asuntos de carácter reservado, con perjuicio de la empresa; Artículo 134.- Son obligaciones de los trabajadores: XIII. Guardar escrupulosamente los secretos técnicos, comerciales y de fabricación de los productos a cuya elaboración concurran directa o indirectamente, o de los cuales tengan conocimiento por razón del trabajo que desempeñen, así como de los asuntos administrativos reservados, cuya divulgación pueda causar perjuicios a la empresa.

Código Penal Federal	Artículo 210.- Se impondrán de treinta a doscientas jornadas de trabajo en favor de la comunidad, al que sin justa causa, con perjuicio de alguien y sin consentimiento del que pueda resultar perjudicado, revele algún secreto o comunicación reservada que conoce o ha recibido con motivo de su empleo, cargo o puesto. Artículo 211.- La sanción será de uno a cinco años, multa de cincuenta a quinientos pesos y suspensión de profesión en su caso, de dos meses a un año, cuando la revelación punible sea hecha por persona que presta servicios profesionales o técnicos o por funcionario o empleado público o cuando el secreto revelado o publicado sea de carácter industrial. Artículo 211 Bis.- A quien revele, divulgue o utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa.
Ley de Instituciones de Crédito	Artículo 117.- La información y documentación relativa a las operaciones y servicios a que se refiere el artículo 46 de la presente Ley, tendrá carácter confidencial, por lo que las instituciones de crédito, en protección del derecho a la privacidad de sus clientes y usuarios que en este artículo se establece, en ningún caso podrán dar noticias o información de los depósitos, operaciones o servicios, incluyendo los previstos en la fracción XV del citado artículo 46, sino al depositante, deudor, titular, beneficiario, fideicomitente, fideicomisario, comitente o mandante, a sus representantes legales o a quienes tengan otorgado poder para disponer de la cuenta o para intervenir en la operación o servicio. Artículo 46 Bis 1.- Las instituciones de crédito podrán pactar con terceros, incluyendo a otras instituciones de crédito o entidades financieras, la prestación de servicios necesarios para su operación, así como comisiones para realizar las operaciones previstas en el artículo 46 de esta Ley, de conformidad con las disposiciones de carácter general que expida la Comisión Nacional Bancaria y de Valores, previo acuerdo de su Junta de Gobierno. Lo dispuesto en el artículo 117 de esta Ley le será también aplicable a los terceros a que se refiere el presente artículo, así como los representantes, directivos y empleados de dichos terceros, aún cuando dejen de laborar o prestar sus servicios a tales terceros.
Ley Federal de Seguridad Privada	Artículo 15. Fracción V. Seguridad de la información. Consiste en la preservación, integridad y disponibilidad de la información del prestatario, a través de sistemas de administración de seguridad, de bases de datos, redes locales, corporativas y globales, sistemas de cómputo, transacciones electrónicas, así como respaldo y recuperación de dicha información, sea ésta documental, electrónica o multimedia.
Acuerdo por el que se establece el Esquema de Interoperabilidad y de Datos Abiertos de la Administración Pública Federal	Artículo 2. Para los efectos del presente Acuerdo, se entenderá por: Ciberseguridad: a la aplicación de un proceso de análisis y gestión de riesgos relacionados con el uso, procesamiento, almacenamiento y transmisión de información, así como con los sistemas y procesos usados para ello, que permite llegar a una situación de riesgo conocida y controlada;
Acuerdo por el que se expide el Manual	1. Definiciones y Términos: Seguridad de la información: La capacidad de preservación de la confidencialidad,

Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones	integridad y disponibilidad de la información. Vulnerabilidad: La debilidad en la seguridad de la información dentro de una organización que potencialmente permite que una amenaza afecte a un activo de TIC. SGSI: Sistema de Gestión de Seguridad de la Información, parte de un sistema global de gestión que basado en el análisis de riesgos, establece, implementa, opera, monitorea, revisa, mantiene y mejora la seguridad de la información. 5.9.4 Administración de la seguridad de los sistemas informáticos 5.9.4.1 Objetivos del proceso General: Establecer los mecanismos que permitan la administración de la seguridad de la información de la Institución contenida en medios electrónicos y sistemas informáticos. Específicos: Establecer un Sistema de Gestión de Seguridad de la Información (SGSI) que proteja la información de la Institución contenida en medios electrónicos y sistema informáticos, contra accesos y usos no autorizados, con la finalidad de conservar su confidencialidad, integridad y disponibilidad.
LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA GUBERNAMENTAL	**Capítulo III** **Información reservada y confidencial** Artículo 13. Como información reservada podrá clasificarse aquélla cuya difusión pueda: I. Comprometer la seguridad nacional, la seguridad pública o la defensa nacional; II. Menoscabar la conducción de las negociaciones o bien, de las relaciones internacionales, incluida aquella información que otros estados u organismos internacionales entreguen con carácter de confidencial al Estado Mexicano; III. Dañar la estabilidad financiera, económica o monetaria del país; IV. Poner en riesgo la vida, la seguridad o la salud de cualquier persona, o V. Causar un serio perjuicio a las actividades de verificación del cumplimiento de las leyes, prevención o persecución de los delitos, la impartición de la justicia, la recaudación de las contribuciones, las operaciones de control migratorio, las estrategias procesales en procesos judiciales o administrativos mientras las resoluciones no causen estado. Artículo 14. También se considerará como información reservada: I. La que por disposición expresa de una Ley sea considerada confidencial, reservada, comercial reservada o gubernamental confidencial; II. Los secretos comercial, industrial, fiscal, bancario, fiduciario u otro considerado como tal por una disposición legal; III. Las averiguaciones previas; IV. Los expedientes judiciales o de los procedimientos administrativos seguidos en forma de juicio en tanto no hayan causado estado; V. Los procedimientos de responsabilidad de los servidores públicos, en tanto no se haya dictado la resolución administrativa o la jurisdiccional definitiva, o VI. La que contenga las opiniones, recomendaciones o puntos de vista que formen parte del proceso deliberativo de los servidores públicos, hasta en tanto no sea adoptada la decisión definitiva, la cual deberá estar documentada. Cuando concluya el periodo de reserva o las causas que hayan dado origen a la

	reserva de la información a que se refieren las fracciones III y IV de este Artículo, dicha información podrá ser pública, protegiendo la información confidencial que en ella se contenga. No podrá invocarse el carácter de reservado cuando se trate de la investigación de violaciones graves de derechos fundamentales o delitos de lesa humanidad. Artículo 15. La información clasificada como reservada según los artículos 13 y 14, podrá permanecer con tal carácter hasta por un periodo de doce años. Esta información podrá ser desclasificada cuando se extingan las causas que dieron origen a su clasificación o cuando haya transcurrido el periodo de reserva. La disponibilidad de esa información será sin perjuicio de lo que, al respecto, establezcan otras leyes. Artículo 18. Como información confidencial se considerará: I. La entregada con tal carácter por los particulares a los sujetos obligados, de conformidad con lo establecido en el Artículo 19, y II. Los datos personales que requieran el consentimiento de los individuos para su difusión, distribución o comercialización en los términos de esta Ley. No se considerará confidencial la información que se halle en los registros públicos o en fuentes de acceso público. Artículo 19. Cuando los particulares entreguen a los sujetos obligados la información a que se refiere la fracción I del artículo anterior, deberán señalar los documentos que contengan información confidencial, reservada o comercial reservada, siempre que tengan el derecho de reservarse la información, de conformidad con las disposiciones aplicables. En el caso de que exista una solicitud de acceso que incluya información confidencial, los sujetos obligados la comunicarán siempre y cuando medie el consentimiento expreso del particular titular de la información confidencial.
Ley de Protección y Defensa al Usuario de Servicios Financieros	Artículo 8.- La Comisión Nacional establecerá y mantendrá actualizado, un Registro de Usuarios que no deseen que su información sea utilizada para fines mercadotécnicos o publicitarios. Queda prohibido a las Instituciones Financieras utilizar información relativa a la base de datos de sus clientes con fines mercadotécnicos o publicitarios, así como enviar publicidad a los clientes que expresamente les hubieren manifestado su voluntad de no recibirla o que estén inscritos en el registro a que se refiere el párrafo anterior. Las Instituciones Financieras que sean objeto de publicidad son corresponsables del manejo de la información de sus Clientes cuando dicha publicidad la envíen a través de terceros. Los usuarios se podrán inscribir gratuitamente en el Registro Público de Usuarios, a través de los medios que establezca la Comisión Nacional, la cual será consultada por las Instituciones Financieras.
Circular Única Bancaria de la CNBV (Disposiciones de Carácter General Aplicables a las Instituciones de Crédito)	Sección Cuarta.- De la seguridad, confidencialidad e integridad de la información transmitida, almacenada o procesada a través de Medios Electrónicos Artículo 316 Bis 10.- Las Instituciones que utilicen Medios Electrónicos para la celebración de operaciones y prestación de servicios, deberán implementar medidas o mecanismos de seguridad en la transmisión, almacenamiento y procesamiento de

	la información a través de dichos Medios Electrónicos, a fin de evitar que sea conocida por terceros. Para tales efectos, las Instituciones deberán cumplir con lo siguiente: I. Cifrar los mensajes o utilizar medios de comunicación Cifrada, en la transmisión de la Información Sensible del Usuario procesada a través de Medios Electrónicos, desde el Dispositivo de Acceso hasta la recepción para su ejecución por parte de las Instituciones, a fin de proteger la información a que se refiere el Artículo 117 de la Ley, incluyendo la relativa a la identificación y Autenticación de Usuarios tales como Contraseñas, Números de Identificación Personal (NIP), cualquier otro Factor de Autenticación, así como la información de las respuestas a las preguntas secretas a que se refiere el penúltimo párrafo del Artículo 316 Bis 3 de estas disposiciones. Para efectos de lo anterior, las Instituciones deberán utilizar tecnologías que manejen Cifrado y que requieran el uso de llaves criptográficas para asegurar que terceros no puedan conocer los datos transmitidos. Las Instituciones serán responsables de la administración de las llaves criptográficas, así como de cualquier otro componente utilizado para el Cifrado, considerando procedimientos que aseguren su integridad y confidencialidad, protegiendo la información de Autenticación de sus Usuarios. Tratándose de Pago Móvil, Banca Telefónica Voz a Voz y Banca Telefónica Audio Respuesta, podrán implementar controles compensatorios al Cifrado en la transmisión de información a fin de protegerla. II. Las Instituciones deberán Cifrar o truncar la información de las cuentas u operaciones de sus Usuarios y Cifrar las Contraseñas, Números de Identificación Personal (NIP), respuestas secretas, o cualquier otro Factor de Autenticación, en caso de que se almacene en cualquier componente de los Medios Electrónicos. III. En ningún caso, las Instituciones podrán transmitir las Contraseñas y Números de Identificación Personal (NIP), a través de correo electrónico, servicios de mensajería instantánea, Mensajes de Texto SMS o cualquier otra tecnología, que no cuente con mecanismos de Cifrado. Se exceptúa de lo previsto en esta fracción a las Contraseñas y Números de Identificación Personal (NIP) utilizados para acceder al servicio de Pago Móvil, siempre y cuando las Instituciones mantengan controles para que no se pongan en riesgo los recursos y la información de sus Usuarios. Las Instituciones que pretendan utilizar los controles a que se refiere el presente párrafo deberán obtener la previa autorización de la Comisión, para tales efectos. Asimismo, la información de los Factores de Autenticación Categoría 2 a que se refiere el Artículo 310 de las presentes disposiciones, utilizados para acceder a la información de los estados de cuenta, podrá ser comunicada al Usuario mediante dispositivos de audio respuesta automática, así como por correo, siempre y cuando esta sea enviada utilizando mecanismos de seguridad, previa solicitud del Usuario y se hayan llevado a cabo los procesos de Autenticación correspondientes. IV. Las Instituciones deberán asegurarse de que las llaves criptográficas y el proceso de Cifrado y descifrado se encuentren instalados en dispositivos de alta seguridad,

	tales como los denominados HSM (Hardware Security Module), los cuales deberán contar con prácticas de administración que eviten el acceso no autorizado y la divulgación de la información que contienen. Artículo 316 Bis 11.- Las Instituciones deberán contar con controles para el acceso a las bases de datos y archivos correspondientes a las operaciones y servicios efectuados a través de Medios Electrónicos, aún cuando dichas bases de datos y archivos residan en medios de almacenamiento de respaldo. Para efectos de lo anterior, las Instituciones deberán ajustarse a lo siguiente: I. El acceso a las bases de datos y archivos estará permitido exclusivamente a las personas expresamente autorizadas por la Institución en función de las actividades que realizan. Al otorgarse dichos accesos, deberá dejarse constancia de tal circunstancia y señalar los propósitos y el periodo al que se limitan los accesos. II. Tratándose de accesos que se realicen en forma remota, deberán utilizarse mecanismos de Cifrado en las comunicaciones. III. Deberán contar con procedimientos seguros de destrucción de los medios de almacenamiento de las bases de datos y archivos que contengan Información Sensible de sus Usuarios, que prevengan su restauración a través de cualquier mecanismo o dispositivo. IV. Deberán desarrollar políticas relacionadas con el uso y almacenamiento de información que se transmita y reciba por los Medios Electrónicos, estando obligadas a verificar el cumplimiento de sus políticas por parte de sus proveedores y afiliados. La obtención de información almacenada en las bases de datos y archivos a que se refiere el presente artículo, sin contar con la autorización correspondiente, o el uso indebido de dicha información, será sancionada en términos de lo previsto en la Ley, inclusive tratándose de terceros contratados al amparo de lo establecido en el Artículo 46 Bis 1 de dicho ordenamiento legal. Artículo 316 Bis 12.- En caso de que la Información Sensible del Usuario sea extraída, extraviada o las Instituciones supongan o sospechen de algún incidente que involucre accesos no autorizados a dicha información, deberán: I. Enviar por escrito a la Dirección General de la Comisión encargada de su supervisión, dentro de los cinco días naturales siguientes al evento de que se trate, la información que se contiene en el Anexo 64 de las presentes disposiciones. II. Llevar a cabo una investigación inmediata para determinar si la información ha sido o puede ser mal utilizada, y en este caso deberán notificar esta situación, en los siguientes 3 días hábiles, a sus Usuarios afectados a fin de prevenirlos de los riesgos derivados del mal uso de la información que haya sido extraída, extraviada o comprometida, debiendo informarle las medidas que deberán tomar. Asimismo, deberán enviar a la Dirección General de la Comisión encargada de su supervisión, el resultado de dicha investigación en un plazo no mayor a cinco días naturales posteriores a su conclusión.

Y si a estas leyes y regulaciones agregamos el conjunto de **Normas ISO** que tratan sobre temas de seguridad informática, la lista de "obligaciones, recomendaciones y requisitos" crece considerablemente:

- ISO/IEC 27000: Fundamentos y vocabulario.
- ISO/IEC 27001: Norma que especifica los requisitos para la implantación del Sistema de Gestión de Seguridad de la Información (SGSI).
- ISO/IEC 27002: Código de buenas prácticas para la gestión de Seguridad de la Información.
- ISO/IEC 27003: Directrices para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI).
- ISO/IEC 27004: Métricas para la gestión de Seguridad de la Información.
- ISO/IEC 27005: Gestión de riesgos de la Seguridad de la Información.
- ISO/IEC 27006: Requisitos para la acreditación de las organizaciones que proporcionan la certificación de los sistemas de gestión de la Seguridad de la Información.

Si usted es ingeniero o especialista en sistemas, tiene muchas leyes que aprender. Si usted es abogado, tiene muchas normas ISO que aprender. ¿No es este el pretexto perfecto para crear o formalizar una materia o rama jurídica que lleve por nombre "***Derecho de la Seguridad de la Información***"?

Joel Gómez (abogado@joelgomez.mx) es Abogado especialista en Derecho Informático y Propiedad Intelectual desde 1996. Receptor de dos Reconocimientos AMIPCI en 2011; uno en la categoría de "Personaje con Trayectoria Meritoria" debido a su desempeño profesional y su contribución al crecimiento de la industria del internet en México, y el otro por tener "el Mejor Blog Jurídico" del país. Profesor de Derecho Informático en La Salle, la Universidad Panamericana Campus Guadalajara y el INACIPE. Síguelo en Twitter: @JoelGomezMX y @LexInformatica.