DERECHO DE LA SEGURIDAD DE LA INFORMACIÓN EN MÉXICO; MARCO JURÍDICO

Joel A. Gómez Treviño

Presidente Fundador de la Academia Mexicana de Derecho Informático, A.C.

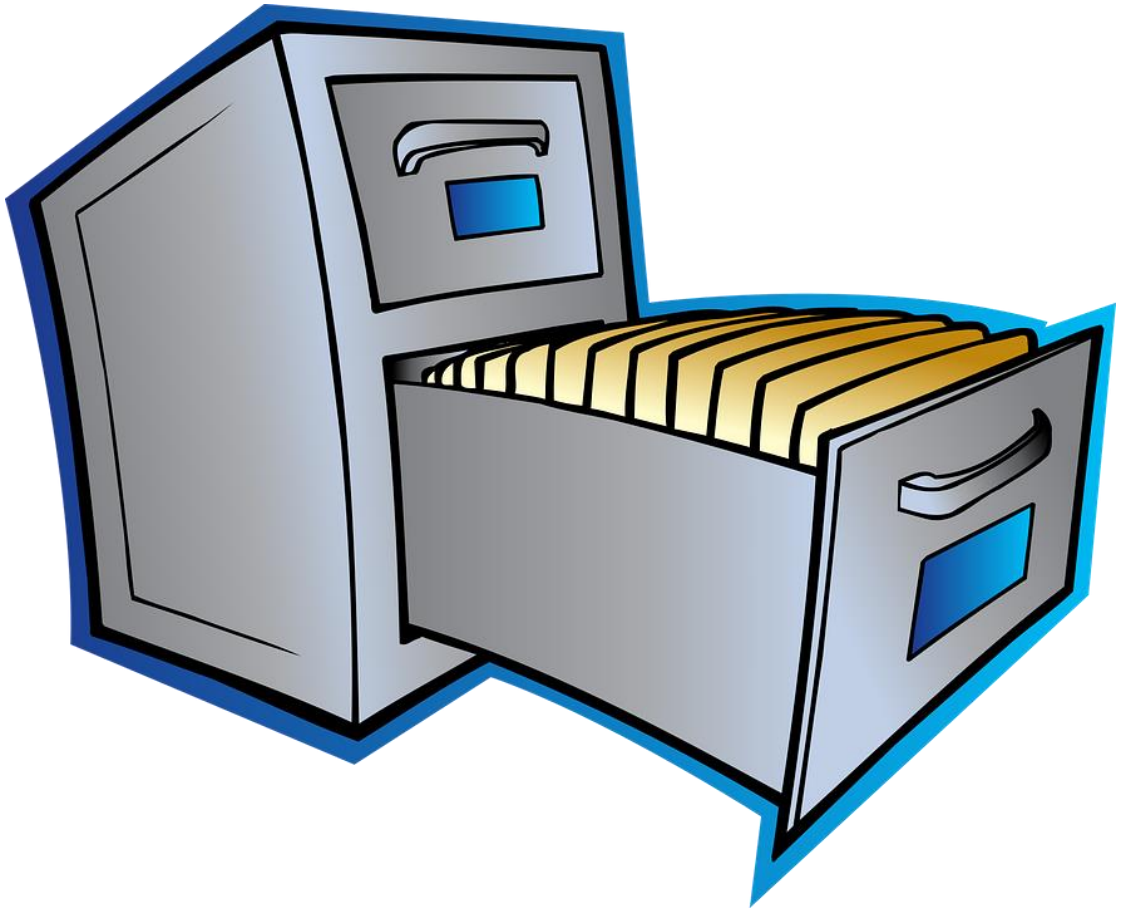
Socio Director de Lex Informática Abogados, S.C.

ACADEMIA MEXICANA DE DERECHO INFORMÁTICO

SEGURIDAD... ¿PARA QUÉ? ¿PARA QUIÉN?

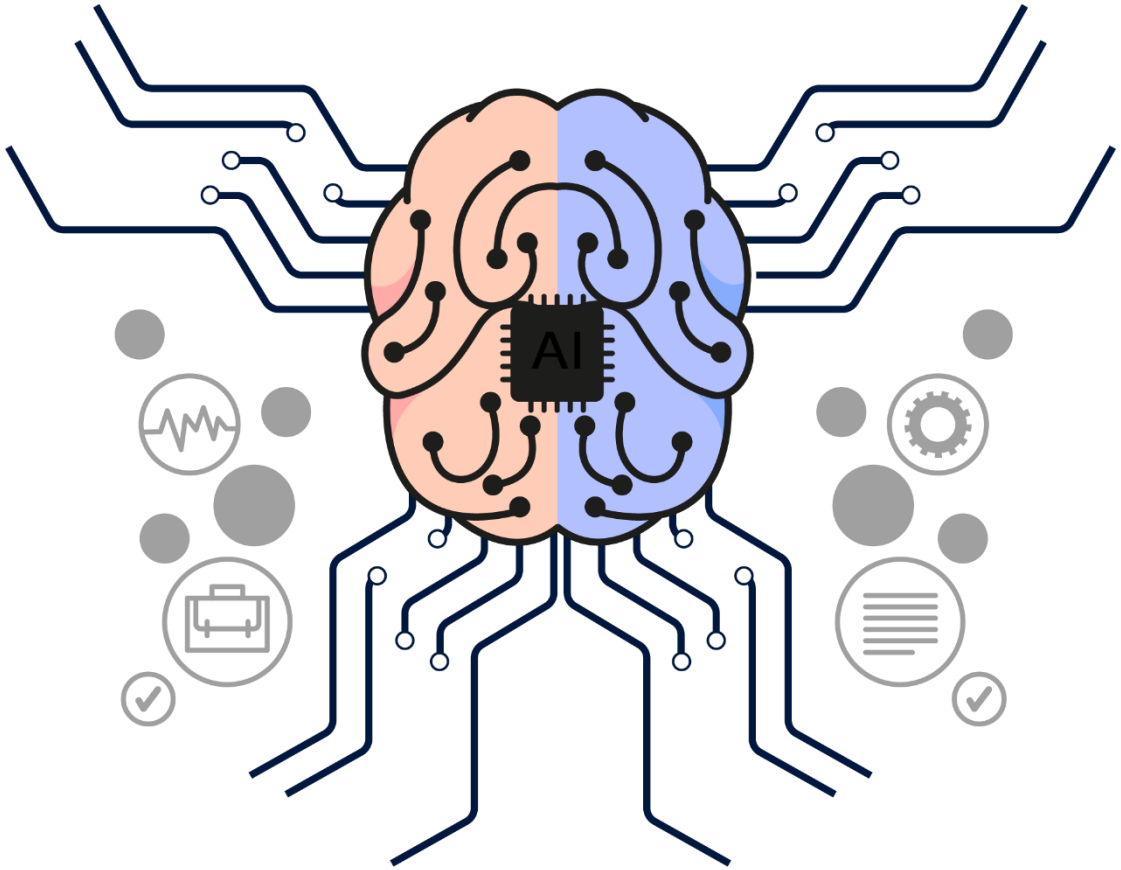
ACADEMIA MEXICANA DE DERECHO INFORMÁTICO

¿DÓNDE RESIDEN LOS DATOS/INFORMACIÓN?

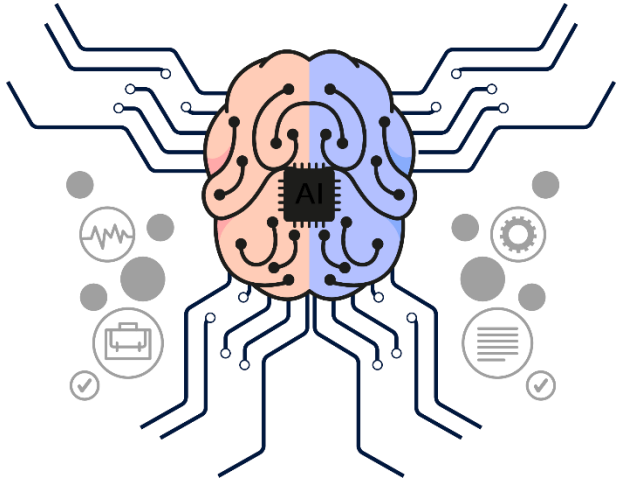


ACADEMIA MEXICANA DE DERECHO INFORMÁTICO

¿QUIÉN TIENE ACCESO A LOS DATOS / INFO?



¿A QUIÉN Y QUÉ TENEMOS QUE CUIDAR?



ACADEMIA MEXICANA DE DERECHO INFORMÁTICO

¿QUÉ ES "INFORMACIÓN"?

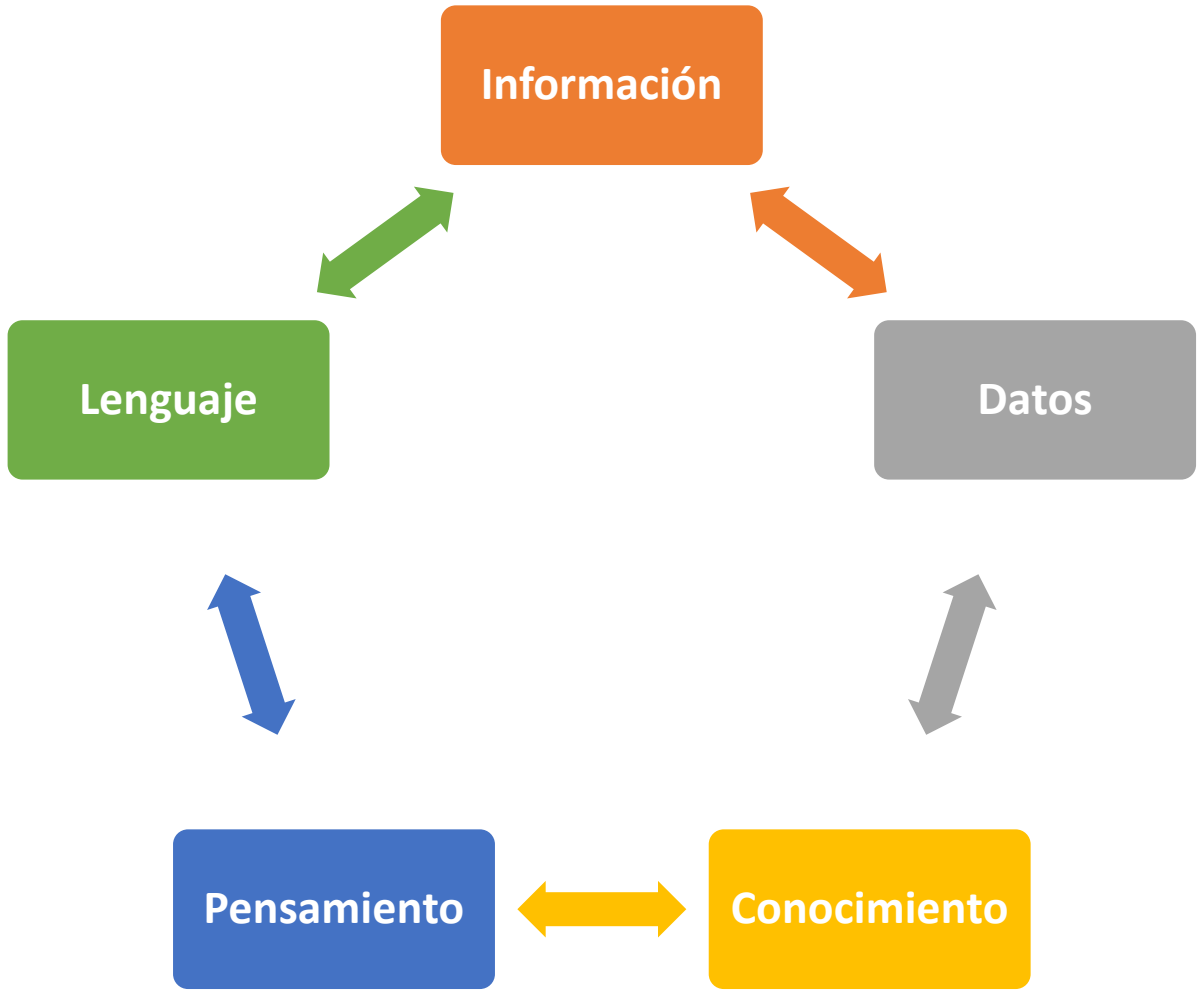
- La palabra *información* deriva del sustantivo latino ***informatio(-nis)*** (del verbo ***informare***, con el significado de "dar forma a la mente", "disciplinar", "instruir", "enseñar").
- La **información** es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.
- La **información** está constituida por un **grupo de datos ya supervisados y ordenados**, que sirven para construir un **mensaje** basado en un cierto fenómeno o ente.
- Desde el punto de vista de la ciencia de la computación, la **información** es un conocimiento explícito extraído por seres vivos o sistemas expertos como resultado de interacción con el entorno o percepciones sensibles del mismo entorno.

ACADEMIA MEXICANA DE DERECHO INFORMÁTICO

¿QUÉ ES "INFORMACIÓN"?

- **Idalberto Chiavenato** afirmaba que la información consiste en un **conjunto de datos** que poseen un significado.
- **Ferrell y Hirt**, por su parte, dicen que esos **datos y conocimientos** están estrictamente ligados con mejorar nuestra **toma de decisiones**.
- **Czinkota y Kotabe**, que dicen que la información consiste en un **conjunto de datos** que han sido clasificados y ordenados con un **propósito determinado**.
- Como **información** denominamos al **conjunto de datos**, ya procesados y ordenados para su comprensión, que aportan nuevos conocimientos a un individuo o sistema sobre un asunto, materia, fenómeno o ente determinado.

VÍNCULO INDISOLUBLE



MARCO JURÍDICO DE LA SEGURIDAD EN MÉXICO

- Constitución Política de los Estados Unidos Mexicanos:
  - Art. 21.- […] **La seguridad pública es una función a cargo de la Federación, las entidades federativas y los Municipios, que comprende la prevención de los delitos; la investigación y persecución para hacerla efectiva, así como la sanción de las infracciones administrativas**, en los términos de la ley, en las respectivas competencias que esta Constitución señala. La actuación de las instituciones de seguridad pública se regirá por los principios de legalidad, objetividad, eficiencia, profesionalismo, honradez y respeto a los derechos humanos reconocidos en esta Constitución. […]

MARCO JURÍDICO DE LA SEGURIDAD EN MÉXICO

- Ley General del Sistema Nacional de Seguridad Pública:
  - La presente Ley **es reglamentaria del artículo 21 de la Constitución Política de los Estados Unidos Mexicanos en materia de Seguridad Pública** y tiene por objeto regular la integración, organización y funcionamiento del Sistema Nacional de Seguridad Pública, así como establecer la distribución de competencias y las bases de coordinación entre la Federación, los Estados, el Distrito Federal y los Municipios, en esta materia.
  - DE LOS SERVICIOS DE SEGURIDAD PRIVADA: Además de cumplir con las disposiciones de la Ley Federal de Armas de Fuego y Explosivos, **los particulares que presten servicios de seguridad, protección, vigilancia o custodia de personas, lugares o establecimientos, de bienes o valores**, incluido su traslado y monitoreo electrónico; **deberán obtener autorización previa de la Secretaría, cuando los servicios comprendan dos o más entidades federativas**; o de la autoridad administrativa que establezcan las leyes locales, cuando los servicios se presten sólo en el territorio de una entidad.

MARCO JURÍDICO DE LA SEGURIDAD EN MÉXICO

- Ley Federal de Seguridad Privada y su Reglamento:
  - La presente ley tiene por objeto **regular la prestación de servicios de seguridad privada, cuando estos se presten en dos o más entidades federativas**, en las modalidades previstas en esta ley y su reglamento, así como la infraestructura, equipo e instalaciones inherentes a las mismas.
  - Para los efectos de esta ley, **se entenderá por "Seguridad Privada" aquella actividad a cargo de los particulares**, autorizada por el órgano competente, con el objeto de desempeñar acciones relacionadas con la seguridad en materia de protección, vigilancia, custodia de personas, información, bienes inmuebles, muebles o valores, incluidos su traslado; instalación, operación de sistemas y equipos de seguridad; aportar datos para la investigación de delitos y apoyar en caso de siniestros o desastres, en su carácter de auxiliares a la función de Seguridad Pública.

MARCO JURÍDICO DE LA SEGURIDAD EN MÉXICO

- Proyecto de Ley General de Seguridad Privada
  - La presente **Ley es reglamentaria del artículo 21 constitucional** y tiene por objeto regular la seguridad privada como actividad auxiliar de la función de Seguridad Pública en materia de prevención del delito, así como establecer la distribución de competencias y las bases de coordinación entre la Federación y las Entidades Federativas, en esta materia.
  - Para los efectos de esta ley, **se entenderá por "Seguridad Privada" la actividad auxiliar de la función de Seguridad Pública a cargo de los particulares**, con el objetivo de desempeñar acciones relacionadas con la seguridad en materia de protección, vigilancia, custodia de personas, información, bienes inmuebles, muebles o valores, incluidos su traslado; instalación, operación de sistemas y equipos de seguridad; que requiere autorización única expedida por el Servicio Nacional Regulador de Seguridad Privada en los términos de la presente Ley.

MARCO JURÍDICO DE LA SEGURIDAD EN MÉXICO

- Proyecto de Ley General de Seguridad Privada:

  T4. De los servicios de seguridad privada y su autorización única.

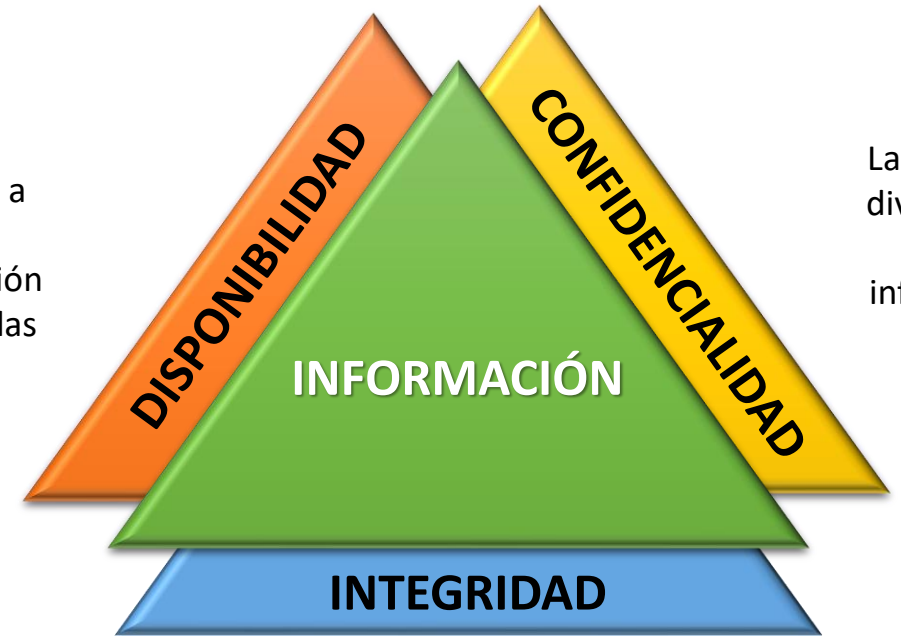
  C1. De las modalidades de los servicios de seguridad privada y sus requisitos.

  - Art. 20. Para prestar servicios de seguridad privada en cualquier entidad federativa, se requiere de la autorización única otorgada por el Servicio Nacional, previo cumplimiento de los requisitos correspondientes.
  - Es facultad del Servicio Nacional autorizar los servicios de Seguridad Privada que se presten dentro del territorio nacional, de acuerdo a las modalidades y submodalidades siguientes:
  - VI. 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.
  - VII. SISTEMAS O BIENES TECNOLÓGICOS PARA LA SEGURIDAD: Consiste en todo producto o servicio tecnológico que sea utilizado como medio de apoyo para realizar las actividades de seguridad.

SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la:

La información debe encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. Es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.



La confidencialidad es la propiedad que impide la divulgación de información a personas o sistemas no autorizados. Asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización.

Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. Es el mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados.

Fuente:

WIKIPEDIA

ACADEMIA MEXICANA DE DERECHO INFORMÁTICO

DERECHO DE LA SEGURIDAD DE LA INFORMACIÓN

Joel A. Gómez Treviño

Presidente Fundador de la
Academia Mexicana de Derecho Informático, A.C.
Socio Director de Lex Informática Abogados, S.C.

DERECHO DE LA SEGURIDAD DE LA INFORMACIÓN

Rama de las ciencias jurídicas que:

- Protege a la información contenida en medios físicos, electrónicos y sistema informáticos, contra daño, pérdida, alteración, destrucción, accesos y usos no autorizados, con la finalidad de conservar su confidencialidad, integridad y disponibilidad.

- Brinda confidencialidad y seguridad 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.

Definición de © Joel Gómez Treviño

ACADEMIA MEXICANA DE DERECHO INFORMÁTICO

SECRETO PROFESIONAL E INDUSTRIAL

- *ARTICULO 36 LEP.- 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.*

- *Artículo 85 LPI.- 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.*

CÓDIGO PENAL FEDERAL

REVELACIÓN DE SECRETOS

- **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**.

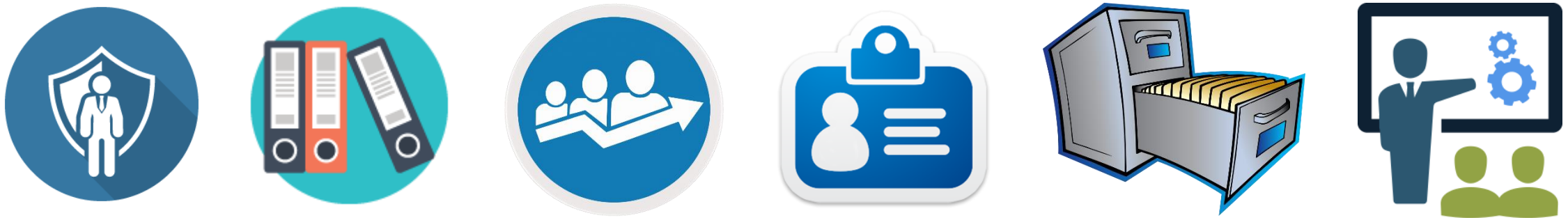
- **Artículo 211**.- La sanción será de uno a cinco años, multa de cincuenta a quinientos pesos y suspensión de profesión en su caso, de dos meses a un año, cuando la revelación punible sea hecha por persona que presta servicios profesionales o técnicos o por funcionario o empleado público o cuando el **secreto revelado o publicado sea de carácter industrial**.

PROTECCIÓN DEL DATO PERSONAL (LFPDPPP)

- *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.*

MEDIDAS DE SEGURIDAD ADMINISTRATIVAS



Conjunto de acciones y mecanismos para 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;

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;





ACADEMIA MEXICANA DE DERECHO INFORMÁTICO

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;

ACADEMIA MEXICANA DE DERECHO INFORMÁTICO

ACCIONES PARA LA SEGURIDAD DE LOS DATOS PERSONALES

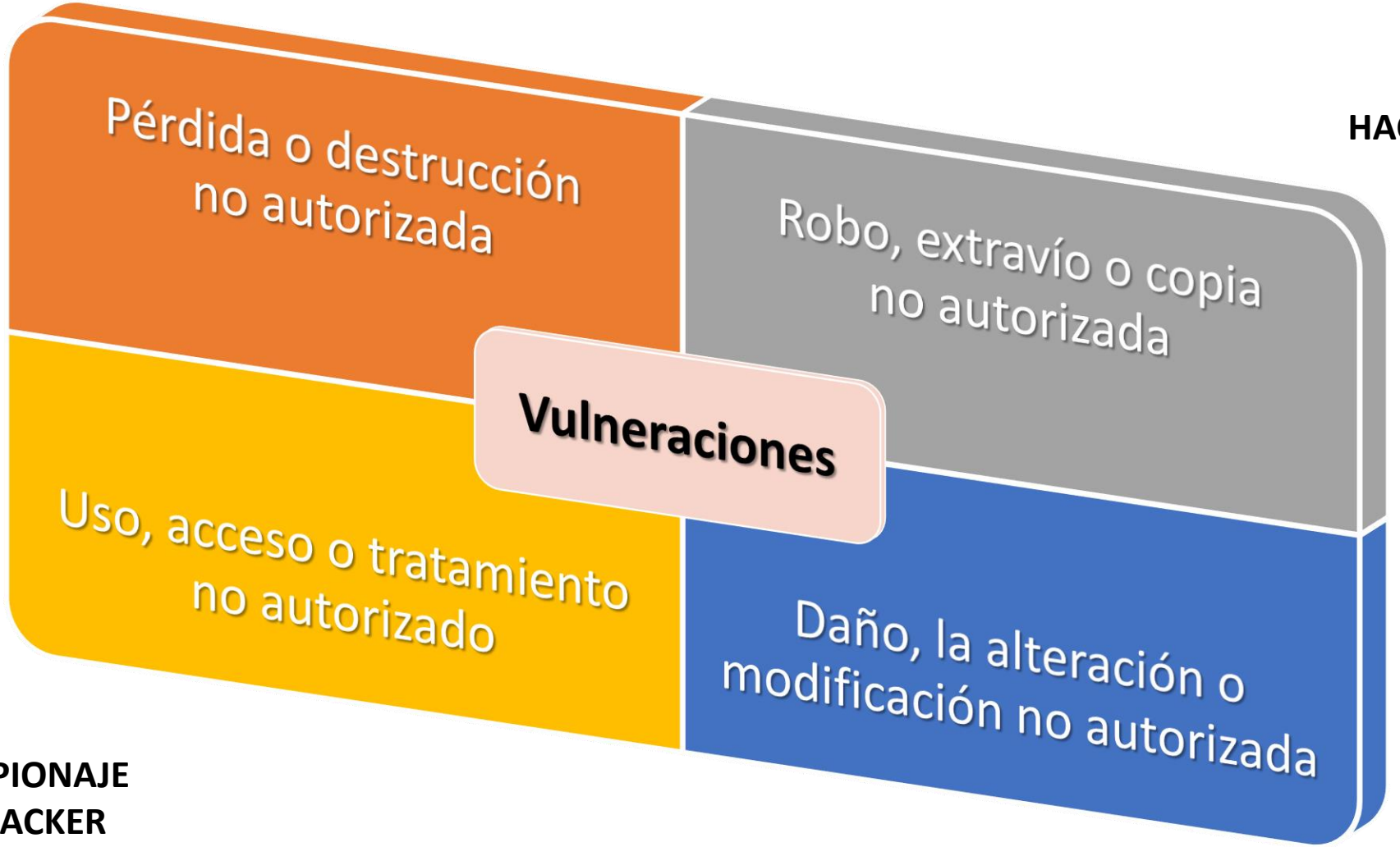
- I. Elaborar un **inventario de datos personales** y de los sistemas de tratamiento;
- II. Determinar las **funciones y obligaciones** de las personas que traten datos personales;
- III. Contar con un **análisis de riesgos** de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales;
- IV. **Establecer las medidas de seguridad** aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva;

- V. Realizar el **análisis de brecha** que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales;
- VI. Elaborar un plan de trabajo para la **implementación de las medidas de seguridad faltantes**, derivadas del análisis de brecha;
- VII. Llevar a cabo revisiones o **auditorías**;
- VIII. **Capacitar al personal** que efectúe el tratamiento, y
- IX. Realizar un **registro de los medios de almacenamiento** de los datos personales.

VULNERACIONES DE SEGURIDAD

NEGLIGENCIA

ESPIONAJE
HACKER



HACKER

VIRUS
HACKER

SEGURIDAD DE DATOS PERSONALES EN LA NUBE

- Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor:

- **Guarde la confidencialidad respecto de los datos personales** sobre los que se preste el servicio;
- **Establezca y mantenga medidas de seguridad** adecuadas para la protección de los datos personales sobre los que se preste el servicio;

ACADEMIA MEXICANA DE DERECHO INFORMÁTICO

INFORMACIÓN CONFIDENCIAL
LEY GENERAL DE TRANSPARENCIA…

- Artículo 116. Se considera información confidencial la que contiene **datos personales** concernientes a una persona identificada o identificable. La información confidencial no estará sujeta a temporalidad alguna y sólo podrán tener acceso a ella los titulares de la misma, sus representantes y los Servidores Públicos facultados para ello.

- Se considera como información confidencial: **los secretos bancario, fiduciario, industrial, comercial, fiscal, bursátil y postal**, cuya titularidad corresponda a particulares, sujetos de derecho internacional o a sujetos obligados cuando no involucren el ejercicio de recursos públicos.

ACADEMIA MEXICANA DE DERECHO INFORMÁTICO

SECRETO TÉCNICO, COMERCIAL Y DE FABRICACIÓN 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.*

SECRETO DEL CONSUMIDOR

Artículo 76 bis de la Ley Federal de Protección al Consumidor.- *En la celebración de transacciones electrónicas 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;

SECRETO FINANCIERO (ENGLOBA AL SECRETO BANCARIO, BURSÁTIL Y FIDUCIARIO)

- Artículo 46 Bis 1 (**LIC**).- **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.

- **Las disposiciones de carácter general** a que se refiere el primer párrafo de este artículo, deberán contener, entre otros, los siguientes elementos:
- I. Los lineamientos técnicos y operativos que deberán observarse para la realización de tales operaciones, así como para salvaguardar la confidencialidad de la información de los usuarios del sistema bancario y proveer que en la celebración de dichas operaciones se cumplan las disposiciones aplicables;

SECRETO FINANCIERO (ENGLOBA AL SECRETO BANCARIO, BURSÁTIL Y FIDUCIARIO)

Artículo 142 de la Ley de Instituciones de Crédito (LIC).-

- **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.

SECRETO FINANCIERO (ENGLOBA AL SECRETO BANCARIO, BURSÁTIL Y FIDUCIARIO)

Artículo 142 de la Ley de Instituciones de Crédito (LIC).-

- *(Continuación…)* Los empleados y funcionarios de las instituciones de crédito serán responsables, en los términos de las disposiciones aplicables, por violación del secreto que se establece y las instituciones estarán obligadas en caso de revelación indebida del secreto, a reparar los daños y perjuicios que se causen.

SECRETO FINANCIERO…

- Artículo 112 Quáter (**LIC**).- **Se sancionará** con prisión de tres a nueve años y de treinta mil a trescientos mil días multa, **al que sin causa legítima o sin consentimiento** de quien esté facultado para ello:
  - **I. Acceda a los equipos o medios electrónicos, ópticos o de cualquier otra tecnología del sistema bancario mexicano**, para obtener recursos económicos, información confidencial o reservada, o
  - **II. Altere o modifique el mecanismo de funcionamiento de los equipos o medios electrónicos**, ópticos o de cualquier otra tecnología para la disposición de efectivo de los usuarios del sistema bancario mexicano, para obtener recursos económicos, **información confidencial o reservada**.

LEY FINTECH

- **Artículo 39.- Las solicitudes para obtener las autorizaciones de la CNBV** previstas en el presente Capítulo (para realizar actividades atribuidas a las instituciones de financiamiento colectivo o de fondos de pago electrónico) **deberán acompañarse de lo siguiente**:
  - VI. **Las medidas y políticas** en materia de control de riesgos operativos, así como **de seguridad de la información**, **incluyendo las políticas de confidencialidad**, con la evidencia de que cuentan con un **soporte tecnológico seguro, confiable** y preciso para sus Clientes y con los **estándares mínimos de seguridad que aseguren la confidencialidad, disponibilidad e integridad de la información** y **prevención de** fraudes y **ataques cibernéticos**, de conformidad con lo establecido en las disposiciones de carácter general aplicables;

LEY FINTECH

- **Artículo 48.-** La **CNBV** deberá emitir disposiciones de carácter general orientadas a preservar la estabilidad y correcto funcionamiento de las ITF […] Asimismo, tratándose de instituciones de financiamiento colectivo podrá emitir **disposiciones de carácter general** en materia de **seguridad de la información**, **incluyendo las políticas de confidencialidad**, **uso de medios electrónicos**, ópticos o de cualquier otra tecnología, sistemas automatizados de procesamiento de datos y redes de telecomunicaciones, ya sean privados o públicos y continuidad operativa.

LEY FINTECH

- **Artículo 48.-** [*Continuación…*] Tratándose de instituciones de fondos de pago electrónico, la **CNBV** y el **Banco de México** emitirán conjuntamente **disposiciones de carácter general** en materia de **seguridad de la información**, **incluyendo las políticas de confidencialidad** y registro de cuentas sobre movimientos transaccionales, el **uso de medios electrónicos**, ópticos o de cualquier otra tecnología, sistemas automatizados de procesamiento de datos y redes de telecomunicaciones, ya sean privados o públicos y continuidad operativa.

LEY FINTECH

- **Artículo 48.-** [*Continuación…*] Las instituciones de fondos de pago electrónico deberán, de conformidad con las disposiciones de carácter general que para tal efecto emitan conjuntamente la CNBV y el Banco de México, **evaluar con la periodicidad que señalen dichas disposiciones, por medio de terceros independientes, el cumplimiento de los requerimientos de seguridad de información, uso de medios electrónicos** y continuidad operativa que dichas instituciones deben observar conforme a las referidas disposiciones.

LEY FINTECH

- **Artículo 58.-** […] **La Secretaría**, considerando las características de las Operaciones y actividades llevadas a cabo por las ITF, **en las disposiciones de carácter general a que se refiere este artículo, emitirá los lineamientos sobre el procedimiento y criterios**, así como los casos, la forma, los términos y los plazos **en que las ITF deberán observar respecto de**:

  - III. La forma en que las ITF deberán resguardar y garantizar la seguridad de la información y documentación relativas a la identificación de sus Clientes o quienes lo hayan sido, así como la de aquellos actos, Operaciones y servicios reportados conforme al presente artículo;

LEY FINTECH

- **Artículo 76.-** [… OPEN BANKING / API's …] El intercambio de datos e información que podrán compartirse en términos de este artículo estará **sujeto a las disposiciones de carácter general que emita la Comisión Supervisora, o el Banco de México** para el caso de las sociedades de información crediticia y las cámaras de compensación a que se refiere el primer párrafo de este artículo, **en las cuales podrán establecerse los estándares necesarios para** la interoperabilidad de interfaces de programación de aplicaciones; el diseño, desarrollo, mantenimiento y **mecanismos de seguridad** de estas interfaces para el acceso, envío u obtención de datos e información, **la información considerada crítica para el buen funcionamiento de las aplicaciones** que requieran el uso de estas interfaces, así como los **mecanismos** por medio de los cuales **se obtendrá el consentimiento del cliente**.

LEY FINTECH

- **Artículo 83.-** En la solicitud de autorización temporal, las sociedades que pretendan **operar con Modelos Novedosos** deberán incluir lo siguiente:

  - III. Las políticas de análisis de riesgo, incluyendo aquellas **políticas a seguir en materia de seguridad** en la Infraestructura Tecnológica y de **seguridad de la información**;

LEY FINTECH

- **Artículo 87.- Para otorgar la autorización a** que se refiere este Capítulo (De los **Modelos Novedosos en entidades reguladas**), los interesados deberán presentar su solicitud acompañando la documentación e información siguiente:

  - II. Las **políticas** de análisis de riesgo, incluyendo aquellas políticas a seguir en materia de **seguridad en la Infraestructura Tecnológica** y de **seguridad de la información**;

LEY FINTECH

- **Artículo 103.-** Las multas previstas en esta Ley que le corresponde imponer a la CNBV serán las siguientes:
  - IV.- Multa de 30,000 ($2,418,000) a 150,000 ($12,090,000) UMA ($80.60) por lo siguiente:
    - b) **Por no cumplir con los requisitos de seguridad** y continuidad de la operación de los registros de cuenta a que se refiere el artículo 48 de esta Ley;

ACADEMIA MEXICANA DE DERECHO INFORMÁTICO

Manual
Administrativo de
Aplicación
General en las materias de
Tecnologías de la
Información y
Comunicaciones y de
Seguridad de la
Información

www.amdi.org.mx @JoelGomezMX

MAAGTICSI

Designar

Al responsable de la seguridad y GESI*

Operar y mantener

El modelo de Seguridad de la Información

Diseñar

La estrategia para establecer el SGSI

Actualizar

El catálogo de infraestructura esencial y activos clave

Analizar

El riesgo e impacto sobre procesos y servicios

Definir

Los Controles de Seguridad de salvaguarda de TIC

Mejorar

El Sistema de Gestión de la Seguridad de la Información

*GESI Grupo Estratégico de Seguridad de la Información.

Roles

1. Responsable de la seguridad de la información en la Institución o RSII.
2. Grupo estratégico de seguridad de la información o GESI.
3. Equipo de respuesta a incidentes de seguridad o ERISC.

Entregables

1. Documento de integración y operación del grupo estratégico de seguridad de la información. ASI F1.
2. Catálogo de infraestructuras de información esenciales y/o críticas. ASI F2
3. Documento de resultados del análisis de riesgos. ASI F3.
4. Documento de definición del SGSI. ASI F4.

ESTRATEGIA DIGITAL NACIONAL

ACUERDO que tiene por objeto emitir las políticas y disposiciones para la **Estrategia Digital Nacional**, en materia de **tecnologías de la información y comunicaciones**, **y en la de seguridad de la información**, así como establecer el Manual Administrativo de Aplicación General en dichas materias.

Capítulo IV

Disposiciones generales para la seguridad de la información

Sección I

Seguridad de la información

- **Artículo 21.-** Las Instituciones deberán observar, implementar y operar los criterios generales de seguridad de la información conforme a los procesos de administración de la seguridad de la información y, de operación de los controles de seguridad de la información y del ERISC, establecidos en el MAAGTICSI.

ESTRATEGIA DIGITAL NACIONAL

- **Artículo 22.- Las Instituciones establecerán un modelo de gobierno de seguridad de la información**, el cual incluirá la **designación del responsable de la seguridad de la información de la Institución** y la constitución de un **grupo estratégico de la seguridad de la información**, que serán responsables de operar el sistema de gestión de seguridad de la información.
- Dicho modelo deberá contar con un **equipo de respuesta a incidentes de seguridad en TIC**, de acuerdo a lo que se señala en el MAAGTICSI.

ESTRATEGIA DIGITAL NACIONAL

- **Artículo 23.** Las Instituciones elaborarán su catálogo de infraestructuras de información esenciales y activos clave e **identificarán**, en su caso, las que tengan el carácter de infraestructuras críticas de información. El catálogo deberá mantenerse actualizado a fin de facilitar la definición de los controles que se requieran para protegerlas, en términos de lo previsto en el MAAGTICSI.
- **Artículo 24.** Las Instituciones desarrollarán un análisis de riesgos, que identifique, clasifique y priorice los mismos de acuerdo a su impacto en los procesos y servicios en la Institución.

ESTRATEGIA DIGITAL NACIONAL

- **Artículo 25.-** Las Instituciones instrumentarán un proceso de fortalecimiento de la cultura de la seguridad de la información, así como de mejora continua sobre los controles de seguridad de la información y del sistema de gestión de seguridad de la información, con base en lo señalado en el MAAGTICSI.

- **Artículo 26.-** Las Instituciones conforme a lo indicado en el MAAGTICSI, **previo al inicio de la puesta en operación de un aplicativo de cómputo**, realizarán el análisis de vulnerabilidades correspondiente, el cual preferentemente será realizado por un tercero, distinto a quién desarrolló el aplicativo. El resultado del análisis deberá preservarse para efectos de auditoría.

ESTRATEGIA DIGITAL NACIONAL

- **Artículo 27.-** Las Instituciones mantendrán los componentes de software y de seguridad de los dominios tecnológicos actualizados para evitar vulnerabilidades, de acuerdo a lo que se establece en el MAAGTICSI, para lo cual implementarán, entre otros, elementos de seguridad de la información, los siguientes:
  - **I.** **Establecer directrices de seguridad de la información**, mismas que podrán ser complementadas con base en mejores prácticas y estándares internacionales en la materia;
  - **II.** **Establecer controles de seguridad en los Activos de TIC**, priorizando aquellos de mayor nivel de riesgo, entre éstos los dispositivos móviles que acceden a la red o interactúen con los dispositivos conectados a la infraestructura, incluyendo aquellos propiedad de terceros que sean utilizados al interior de las Instituciones;

ESTRATEGIA DIGITAL NACIONAL

- **Artículo 27.-** [*Continuación…*]:

III. Mantener, evidencia auditable del proceso de borrado seguro;

IV. Utilizar mecanismos de autenticación y cifrado de acuerdo a estándares internacionales, con un grado no menor a 256 bits para la protección de la comunicación inalámbrica;

V. Utilizar redes abiertas únicamente al proporcionar servicios a la población, las cuales deberán estar separadas y aisladas de su red de datos;

VI. Implementar mecanismos de cifrado en los medios de almacenamiento en Centros de Datos centralizados, determinando que la administración de dichos mecanismos de cifrado esté a cargo de servidores públicos;

VII. Implementar medidas y procedimientos para el respaldo de información, y

VIII. Establecer herramientas de filtrado de contenido, que incluya búsquedas e imágenes en Internet, y permitan la segmentación en distintas categorías, reportes y soporte de sitios de nueva generación y/o micro-aplicaciones.”

ESTRATEGIA DIGITAL NACIONAL

Sección II

Seguridad de la información considerada de seguridad nacional

- **Artículo 28.-** Las Instancias de Seguridad Nacional observarán las disposiciones siguientes:
  - III. Al diseminar la información identificada conforme a los niveles señalados en la fracción I, deberán asegurarse que aquélla que se contenga en medios magnéticos, ópticos o electrónicos, cuente al menos, con las medidas de protección siguientes:
    - b) El documento electrónico deberá diseminarse en un **formato de archivo que no permita su edición o manipulación y protegido de origen contra impresión o copiado no autorizado**, parcial o total, de su contenido;

ESTRATEGIA DIGITAL NACIONAL

- **Artículo 28.-** [*Continuación…*]: III. …
  - c) Se utilizarán **mecanismos de cifrado de llave pública y privada**, canales cifrados de comunicación y, cuando corresponda, de **firma electrónica avanzada**, que permitan la diseminación de la información únicamente al destinatario autorizado al que esté dirigida;
  - e) Comunicar a los destinatarios sobre la responsabilidad que éstos adquieren al recibir la información a que se refiere este artículo, por lo que estarán obligados a:
    - i. Acusar de recibido al remitente, utilizando los mismos mecanismos de cifrado de llave pública y privada, canales cifrados de comunicación y, cuando corresponda, de firma electrónica avanzada;
    - ii. Resguardar la información que reciban en repositorios de información cifrados y controlados con mecanismos de autenticación, para usuarios autorizados y, en los cuales, se lleve un registro sobre los accesos a la información contenida en los mismos;
    - iii. Abstenerse de efectuar reproducciones totales o parciales de los documentos electrónicos

ACADEMIA MEXICANA DE DERECHO INFORMÁTICO

ERRORES COMUNES EN EL *COMPLIANCE* EN SEGURIDAD DE LA INFORMACIÓN

Joel A. Gómez Treviño

Presidente Fundador de la
Academia Mexicana de Derecho Informático, A.C.
Socio Director de Lex Informática Abogados, S.C.

ACADEMIA MEXICANA DE DERECHO INFORMÁTICO

ERROR #1: TODO ES "SECRETO INDUSTRIAL"

- CONTRATO / CLÁUSULA DE CONFIDENCIALIDAD
  - **Toda la información** que se conozca con motivo de su trabajo, puesto, cargo, desempeño de su profesión o relación de negocios **será considerada secreto industrial**, por lo que la parte que revele dicha información sin autorización incurrirá en el delito señalado en el artículo 223 fracción IV de la Ley de la Propiedad Industrial.

ACADEMIA MEXICANA DE DERECHO INFORMÁTICO

ERROR #1: TODO ES "SECRETO INDUSTRIAL"

- Para que se considere que existe un **secreto industrial** es necesario que **concurran los siguientes requisitos** (art. 82, 83 y 223 de la LPI):
  1. Que la información resguardada tenga **aplicación industrial o comercial**;
  2. Que la persona resguarde la información **con carácter confidencial**;
  3. Que la información le signifique **obtener o mantener una ventaja competitiva o económica** frente a terceros en la realización de actividades económicas;
  4. Que el beneficiario de la información haya **adoptado los medios o sistemas** suficientes para **preservar su confidencialidad y el acceso restringido** a la misma;
  5. La información de un secreto industrial necesariamente **deberá estar referida a la naturaleza, características o finalidades de los productos; a los métodos o procesos de producción**; o a los medios o formas de distribución o comercialización de productos o prestación de servicios.
  6. La información deberá **constar en documentos, medios electrónicos** o magnéticos, discos ópticos, microfilmes, películas u otros instrumentos similares.
  7. **Para que sea delito**: … "*habiendo sido prevenido de su confidencialidad*" …

ACADEMIA MEXICANA DE DERECHO INFORMÁTICO

ENTONCES… ¿TODO ES SECRETO INDUSTRIAL?

- En toda cláusula, convenio o contrato de confidencialidad debe identificarse claramente lo que se considera "**información confidencial**".
  - ¿Qué leyes me aplican que tengan obligaciones relacionadas con seguridad y/o confidencialidad de la información?
  - Entre otros tipos, **será considerada información confidencial la siguiente**:
    - Secretos industriales
    - Secretos técnicos y/o comerciales
    - Datos personales
    - Datos del consumidor
    - Secreto profesional
    - Secretos bancarios
    - Secreto fiduciario
    - Datos personales sensibles
    - Datos de salud

ACADEMIA MEXICANA DE DERECHO INFORMÁTICO

ERROR #2: ¡YA FIRMÉ EL N.D.A!

- Existe la mítica creencia de que una vez firmado el contrato o cláusula de confidencialidad, todo está listo, **la información mágicamente quedará protegida por siempre**.
- *"Si alguien viola el convenio irá a la cárcel seguramente..."*.

ACADEMIA MEXICANA DE DERECHO INFORMÁTICO

FIRMAR UN "NDA" ES SOLO EL PRIMER PASO

- Firme actas de entrega – recepción de información confidencial.
- Clasifique e identifique toda información que sea confidencial.
- Adopte medidas técnicas, físicas y administrativas para proteger la información confidencial.
- Capacite a su personal.
- Realice auditorías periódicamente.
- Si hay fuga, ¡presente denuncia!

ACADEMIA MEXICANA DE DERECHO INFORMÁTICO

ERROR #3: A TODO LE PONGO LA LEYENDA MÁGICA "INFORMACIÓN CONFIDENCIAL"

- Poner la leyenda "confidencial" en la firma de un correo o en el encabezado de un documento **no genera obligaciones automáticas ni unilaterales**.
- Si no hay una ley y/o una obligación contractual, de nada servirá colocar la "leyenda de confidencialidad".

ACADEMIA MEXICANA DE DERECHO INFORMÁTICO

ERROR #4: MIS "NDA" SON UNILATERALES

- Es muy poco probable que en una relación de negocios de tracto sucesivo solamente una de las partes revele información a la otra.
- Si ofreces de inicio un NDA con obligaciones bilaterales será mucho más fácil su firma.
- No valúes el monto del daño si hay divulgación en el contrato, que lo haga el juez.

ACADEMIA MEXICANA DE DERECHO INFORMÁTICO

ERROR #5: SOLO DIRECTIVOS SE ENTERAN DE LA EXISTENCIA DE OBLIGACIONES DE CONFIDENCIALIDAD

- Todo el personal debe conocer la existencia de las obligaciones de seguridad y confidencialidad que adquiere la empresa, ya sea por virtud de una ley o derivado de una relación contractual.
- No es suficiente con decirles “aquí todo es confidencial”.
- La capacitación y advertencias al interior de la organización deben ser continuas.

ACADEMIA MEXICANA DE DERECHO INFORMÁTICO

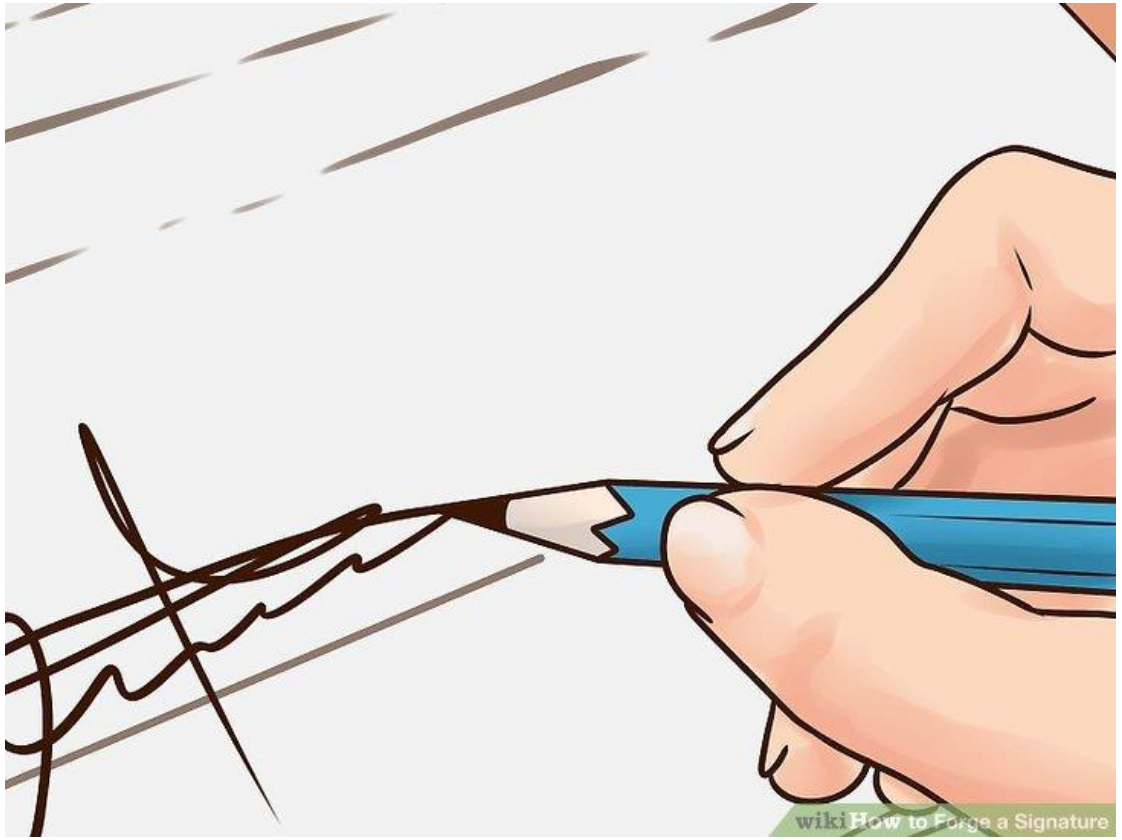
ERROR #6: NO TRAZABILIDAD DE DISPOSITIVOS

- Tienes una política BYOD, o no la tienes, pero entregaste laptops, tabletas y/o celulares a tus empleados.
- En un eventual ilícito cometido por alguno de ellos ¿cómo probarás que cada empleado tenía asignado determinado equipo?

ACADEMIA MEXICANA DE DERECHO INFORMÁTICO

ERROR #7: MIS EMPLEADOS YA FIRMARON… ¡Y MIS PROVEEDORES TAMBIÉN!

- Cualquier empleado firmará lo que le des a firmar, **¡quiere el trabajo!** Eso no significa que vaya a cumplir su contrato o a respetar la ley.
- Es necesario implementar políticas, auditorías anuales y mecanismos de control y revisión cotidianos, de ser posible automatizados.



ACADEMIA MEXICANA DE DERECHO INFORMÁTICO

ERROR #8: DESCUIDAR EL ESLABÓN MÁS DÉBIL…

Estadísticamente quienes generan mayores riesgos para la empresa son los empleados. Suelen ser ellos los hackers o los que provocan fugas de información.

- Desconocimiento.
- Falta de conciencia.
- Mentalidad “no pasa nada”.
- Falta de persecución / denuncias contra empleados que infringen la ley / políticas / contratos.

ACADEMIA MEXICANA DE DERECHO INFORMÁTICO

ERROR #9: EXCESO DE CONFIANZA

- El tener avisos de privacidad, políticas y contratos revisados, elaborados o evaluados por expertos suele dejar a las empresas en un estado de confianza que pone en peligro el cumplimiento con las leyes aplicables.
- Las mejores políticas, instrumentos y herramientas no pueden prevenir todas las posibles conductas de infracción.

World's Biggest Data Breaches

Selected losses greater than 30,000 records

(updated 10th Sep 2017)

interesting story

YEAR | *BUBBLE COLOUR* YEAR | METHOD OF LEAK | *BUBBLE SIZE* NO OF RECORDS STOLEN | DATA SENSITIVITY | SHOW FILTER

2017

Yahoo 32,000,000

Equifax 143,000,000

River City Media 1,370,000,000

Dailymotion 85,200,000

2016

Friend Finder Network 412,000,000

MySpace 164,000,000

Spambot 711,000,000

2015

Uber 57,000,000

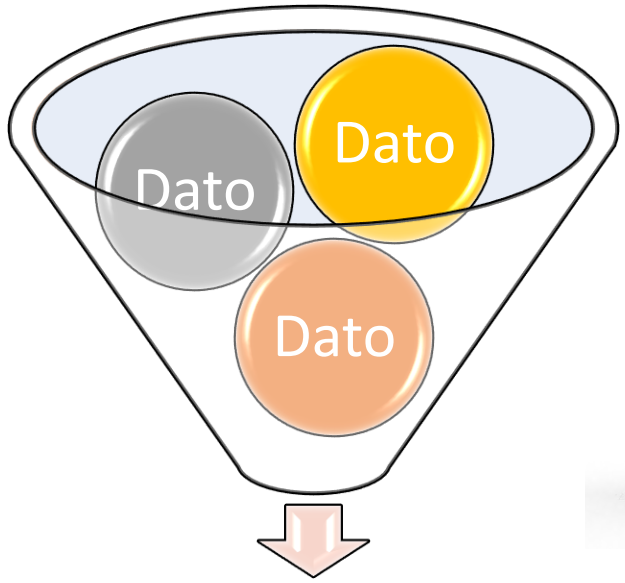
JP Morgan Chase 76,000,000

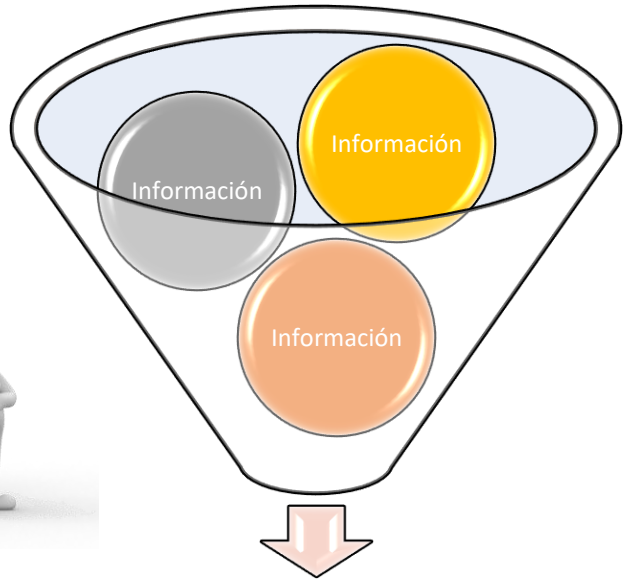
2014

Yahoo 500,000,000

Ebay 145,000,000

Target 70,000,000

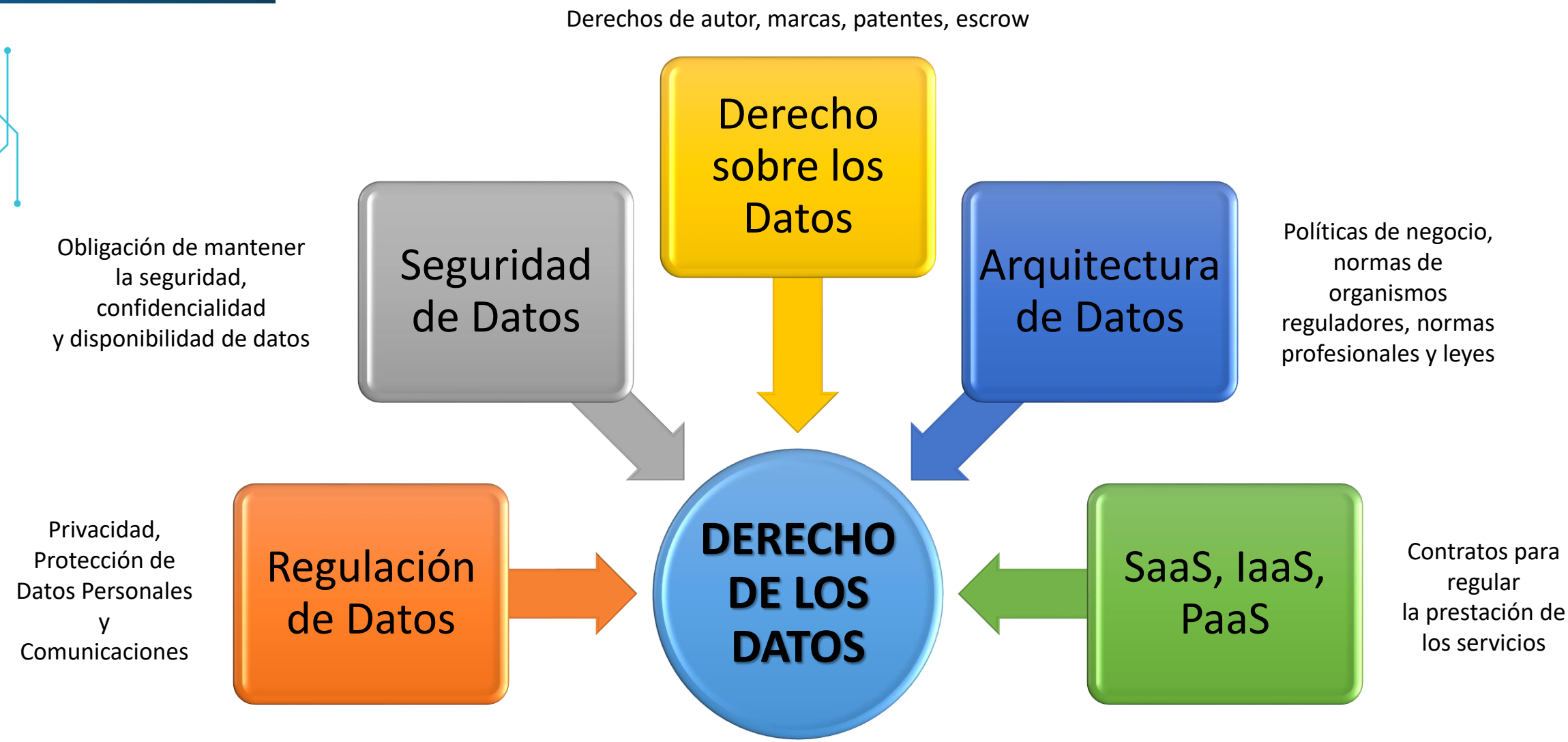




Información

Documento

DERECHO DE LOS DATOS



¿CÓMO SE PUEDE PROTEGER LA INFORMACIÓN Y RECURSOS TECNOLÓGICOS?

ACADEMIA MEXICANA DE DERECHO INFORMÁTICO

CONCLUSIÓN: ECOSISTEMA DE CIBERSEGURIDAD

Cooperación entre todas las partes involucradas, a nivel nacional, regional e internacional

Industria local

- Profesionales capacitados para orientar a empresas y entidades públicas para protegerlas en el entorno digital

Tecnología para el Monitoreo, Protección y Defensa

- Preventiva
- Reactiva

Medidas de Seguridad adoptadas en todos los sectores

- Administrativas
- Técnicas
- Físicas

Leyes y Políticas Públicas

- Leyes estrictas en materia de seguridad de la información y ciberdelincuencia

Autoridades y Abogados

- Capacitados para implementar normas y perseguir delincuentes

Concientización de toda la sociedad respecto de los riesgos en entornos digitales

ACADEMIA MEXICANA DE DERECHO INFORMÁTICO

GRACIAS

Joel A. Gómez Treviño

Lex Informática Abogados, S.C.

Academia Mexicana de Derecho Informático, A.C.

- www.LexInformatica.com
- www.JoelGomez.Abogado
- www.amdi.org.mx
- www.AbogadoDigital.tv
- www.Abogado.Digital

Boulevard Anillo Periférico Adolfo López Mateos No.4293, Piso 3, Int. 300.
Col. Jardines de la Montaña. C.P. 14210.
Ciudad de México.

Conmutador.- (55) 4774-0597

joelgomez@lexinformatica.com

abogado@joelgomez.com

ACADEMIA MEXICANA DE DERECHO INFORMÁTICO

SOBRE EL AUTOR

Joel Gómez Treviño

- Es Abogado egresado del Tecnológico de Monterrey y tiene una Maestría en Derecho Internacional por la Universidad de Arizona. Es Doctor Honoris Causa. Cuenta con 24 de años de trayectoria como especialista en derecho de las tecnologías de la información, privacidad y propiedad intelectual.
- Es Presidente fundador de la Academia Mexicana de Derecho Informático y Coordinador del Comité de Derecho de las TIC y Datos Personales de la Asociación Nacional de Abogados de Empresa, Colegio de Abogados (ANADE).
- Ha recibido 18 reconocimientos (nacionales e internacionales) debido a su desempeño profesional y su contribución al crecimiento de la industria de Internet en México.
- Ha sido invitado a impartir más de 450 conferencias y cursos en programas profesionales y académicos de Brasil, Canadá, Colombia, Costa Rica, Ecuador, España, Estados Unidos, Guatemala, Italia, Panamá, México y Asia.
- Es profesor del ITESM, Universidad Panamericana, INFOTEC y UDLAP.