

BLINDAJE JURÍDICO CONTRA AMENAZAS DIGITALES

Joel A. Gómez Treviño

Presidente Fundador de la Academia Mexicana de Derecho Informático, A.C.,
Coordinador del Comité de Derecho de las TIC y Protección de Datos Personales de la
Asociación Nacional de Abogados de Empresa, Colegio de Abogados, A.C.
Profesor Universidad Panamericana, ITESM, INFOTEC y UDLAP Jenkins Graduate School
Socio Director de Lex Informática Abogados, S.C.



SEGURIDAD... ¿PARA QUÉ? ¿PARA QUIÉN?

@AbogadoDigital



¿DÓNDE RESIDEN LOS DATOS/INFORMACIÓN?

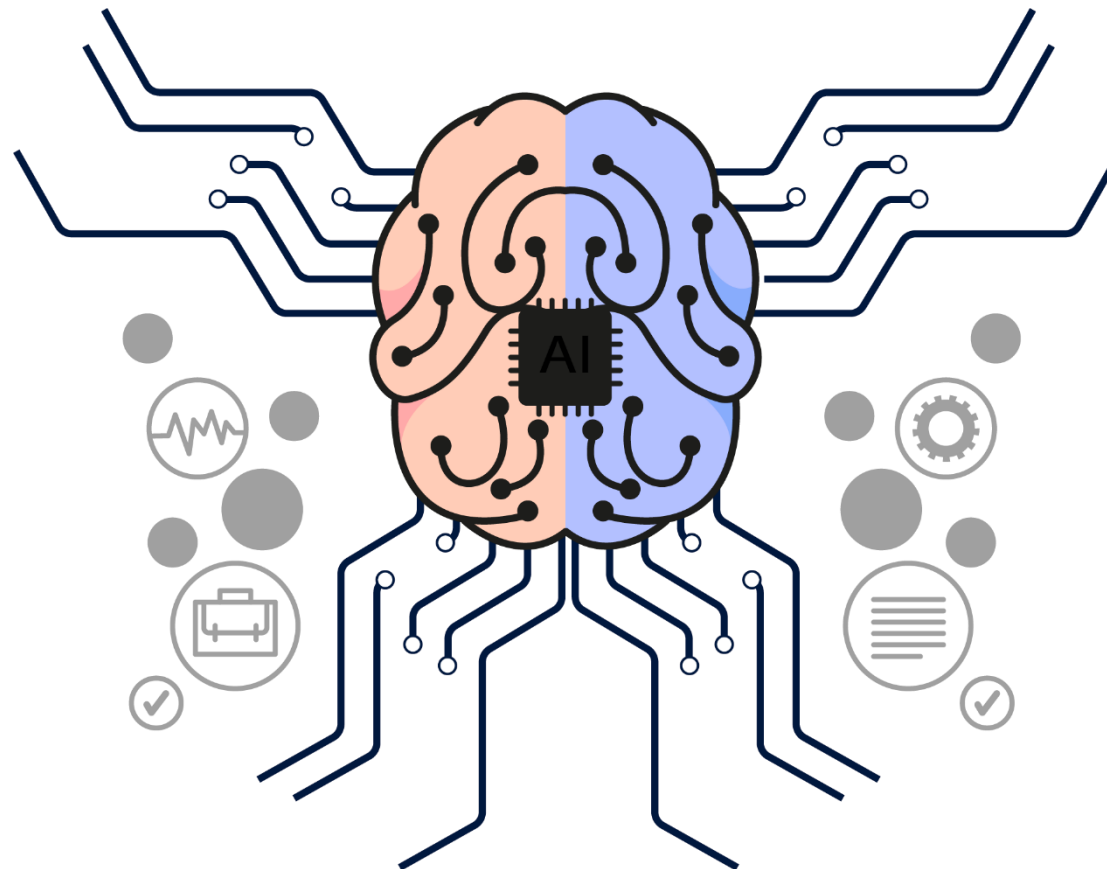
@AbogadoDigital



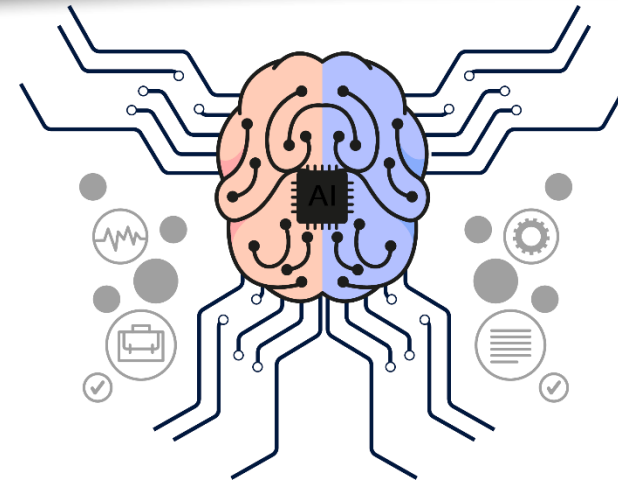
</lexinformatica>
</abogados>

¿QUIÉN TIENE ACCESO A LOS DATOS / INFO?

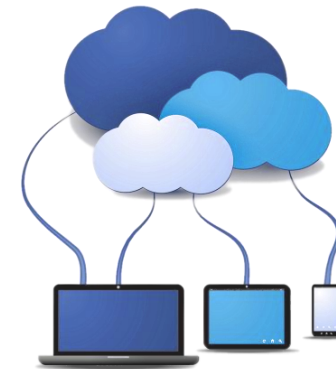
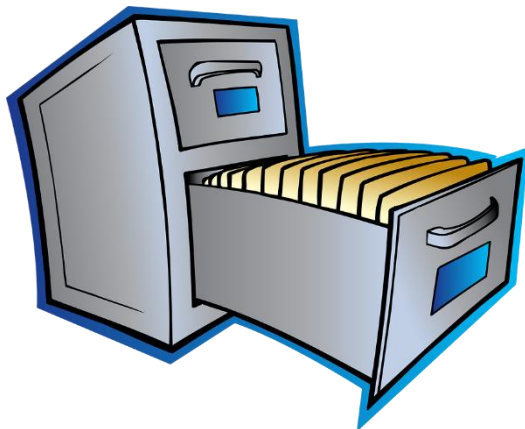
@AbogadoDigital



¿A QUIÉN Y QUÉ TENEMOS QUE CUIDAR?

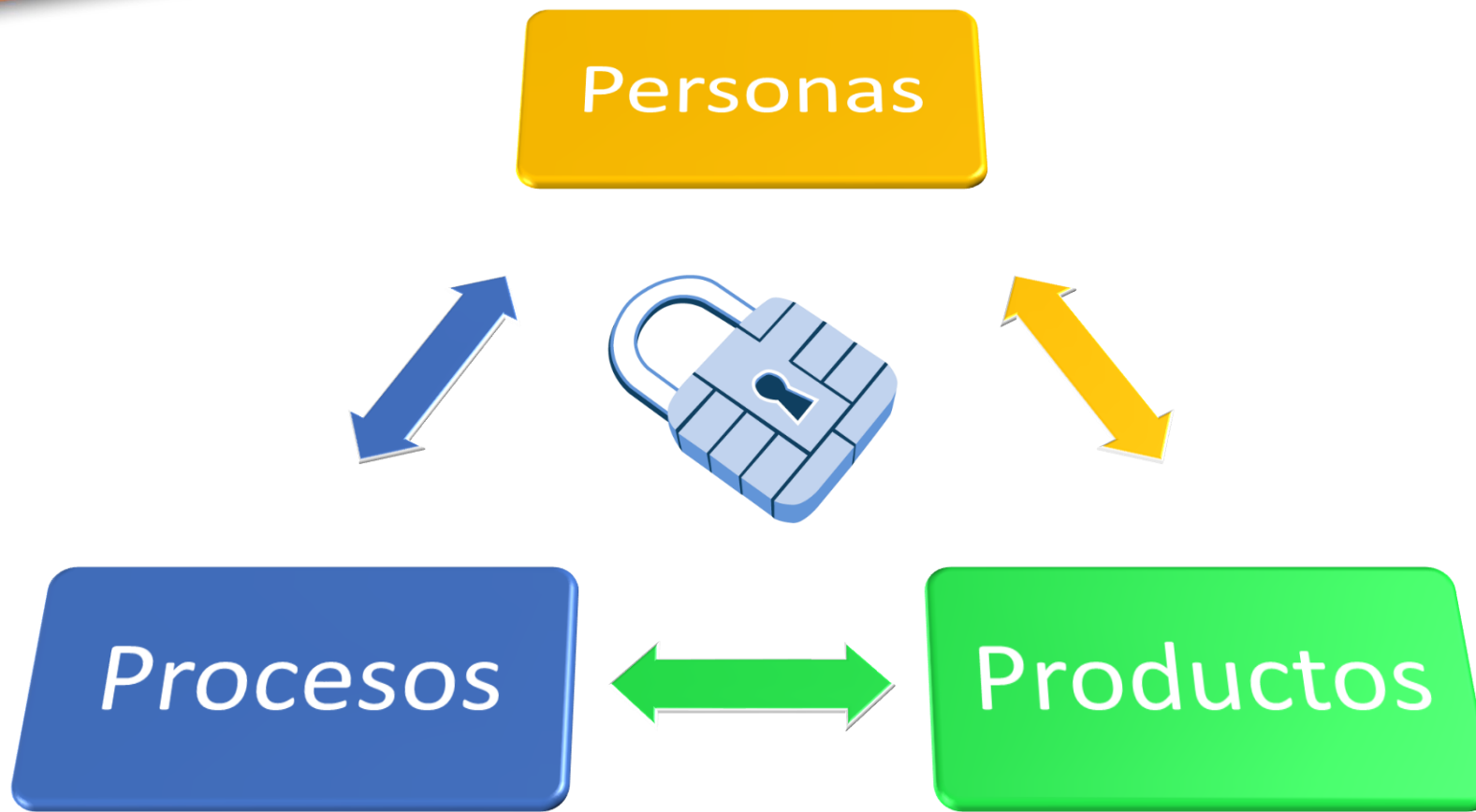


@AbogadoDigital



BUSCAMOS LA SEGURIDAD DE:

@AbogadoDigital



Constitución Política de los EUM

- 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.

Ley Federal de Seguridad Privada

- **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

Proyecto de Ley General de Seguridad Privada

- **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.

- 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.

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.

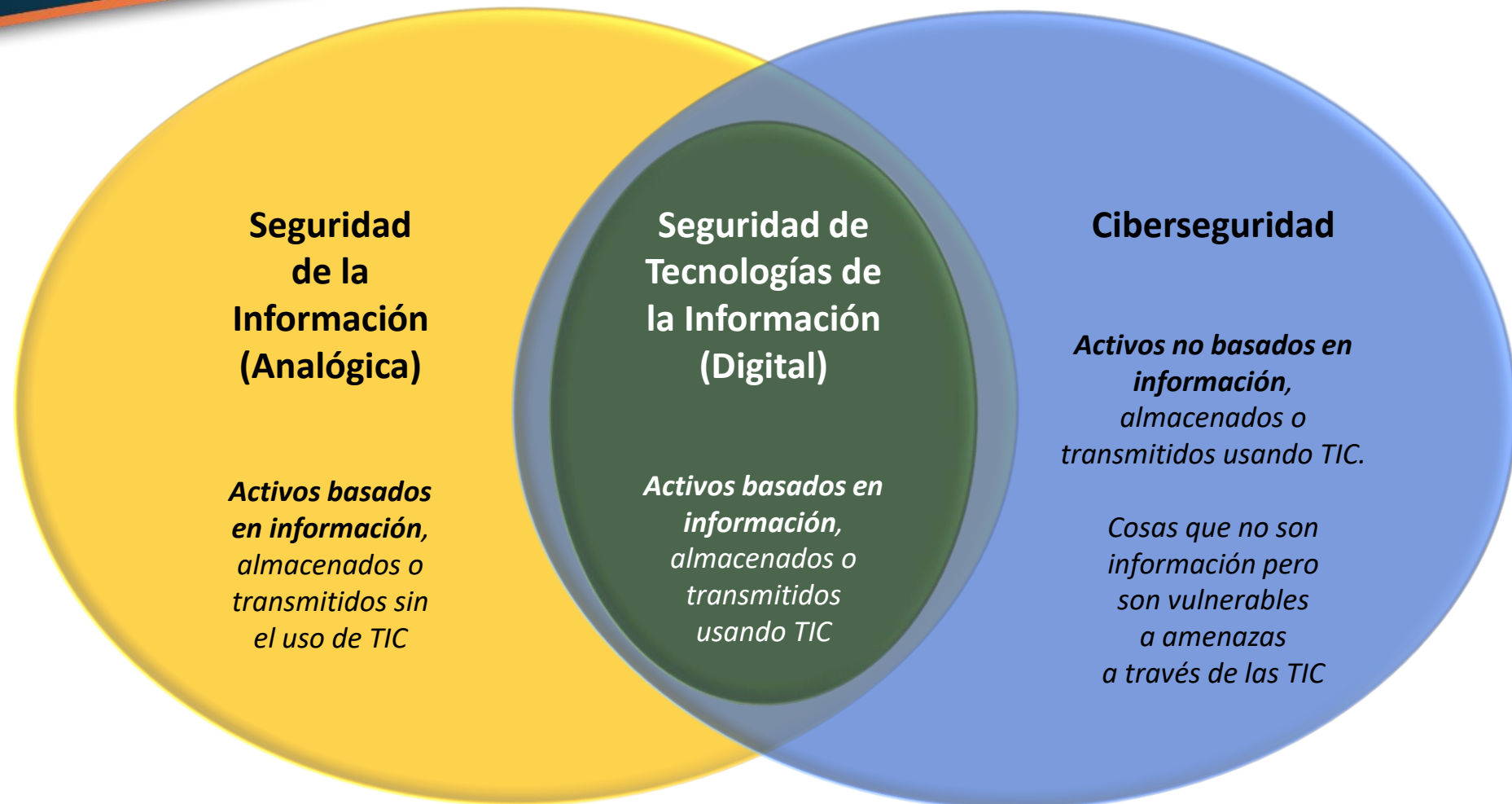
Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. Es el mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados.

Fuente:



¿SEGURIDAD DE... CIBER... SEGURIDAD?

@AbogadoDigital



DERECHO DE LA SEGURIDAD DE LA INFORMACIÓN

Joel A. Gómez Treviño

Presidente Fundador de la Academia Mexicana de Derecho Informático, A.C.,
Coordinador del Comité de Derecho de las TIC y Protección de Datos Personales de la
Asociación Nacional de Abogados de Empresa, Colegio de Abogados, A.C.
Profesor Universidad Panamericana, ITESM, INFOTEC y UDLAP Jenkins Graduate School
Socio Director de Lex Informática Abogados, S.C.

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

- ARTICULO 36 LEP.- Todo profesionalista 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.



- **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 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

@AbogadoDigital



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;

Conjunto de acciones y mecanismos, ya sea que empleen o no la tecnología, destinados para:

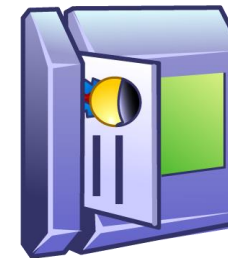
- Prevenir el acceso no autorizado, el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, equipo e información;
- Proteger los equipos móviles, portátiles o de fácil remoción, situados dentro o fuera de las instalaciones;
- Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento que asegure su disponibilidad, funcionalidad e integridad, y
- Garantizar la eliminación de datos de forma segura;





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;

- 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

@AbogadoDigital



NEGLIGENCIA



**ESPIONAJE
HACKER**



HACKER



**VIRUS
HACKER**



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;



SECRETO TÉCNICO, COMERCIAL Y DE FABRICACIÓN LEY FEDERAL DEL TRABAJO

@AbogadoDigital

- 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 concurren 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.

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;



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;

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, [...].**

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.**

- 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**.

- **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;

- **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.

- **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.

- **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.

- **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.**

- **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;



BLINDAJE JURÍDICO CONTRA AMENAZAS DIGITALES

¿Cómo proteger nuestra información y activos digitales contra amenazas internas y externas?

¿EN QUIÉN RESIDE LA FUNCIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LAS ORGANIZACIONES?

@AbogadoDigital



#1: NO TODO ES “SECRETO INDUSTRIAL”

- Ejemplos: CLÁUSULA CLÁSICA 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.

- 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”* ...



#1: IDENTIFICA QUÉ TIPO DE INFORMACIÓN SENSIBLE MANEJAS Y SU MARCO JURÍDICO

- 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:**
 - Secreto industrial
 - Secreto técnicos y/o comercial
 - Datos del consumidor
 - Datos personales
 - Secreto profesional
 - Secreto bancario
 - Secreto fiduciario
 - Secreto financiero
 - Datos personales sensibles
 - Datos de salud

#2: ¿FIRMAR CLÁUSULAS DE CONFIDENCIALIDAD ES SUFICIENTE?

@AbogadoDigital

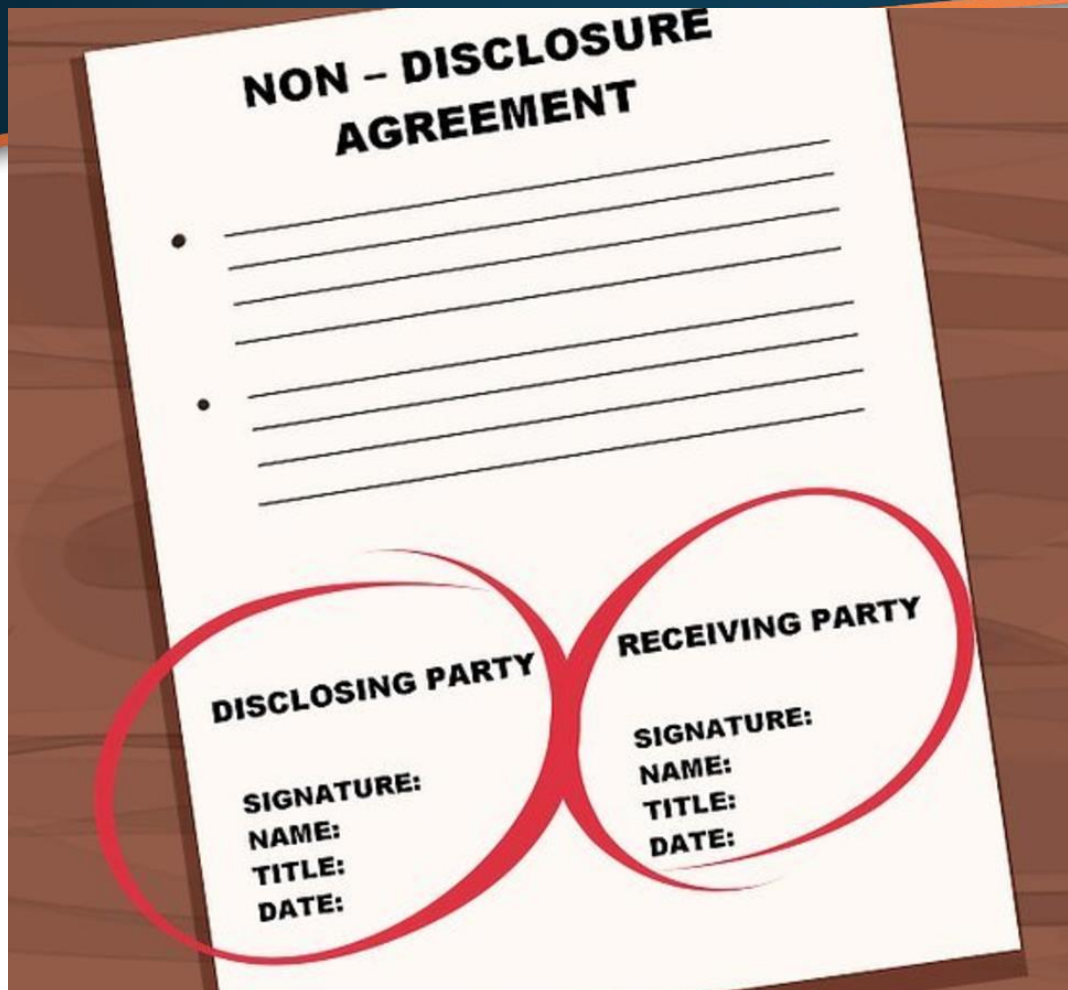
- Existe la mítica creencia de que una vez firmado el contrato o cláusula de confidencialidad, todo está listo, **la información mágicamente quedará protegida por siempre.**
- *“Si alguien viola el convenio irá a la cárcel seguramente...”.*





#2: FIRMAR UN “NDA” ES SOLO EL PRIMER PASO

@AbogadoDigital



- 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!

#3: ¿PONERLE A TODO “INFORMACIÓN CONFIDENCIAL” ES SUFICIENTE?

@AbogadoDigital

- 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”.





#4: ¿MIS CONTRATOS DE CONFIDENCIALIDAD SON UNILATERALES O BILATERALES?

@AbogadoDigital



- 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.

#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.



#6: NO TRAZABILIDAD DE DISPOSITIVOS

@AbogadoDigital

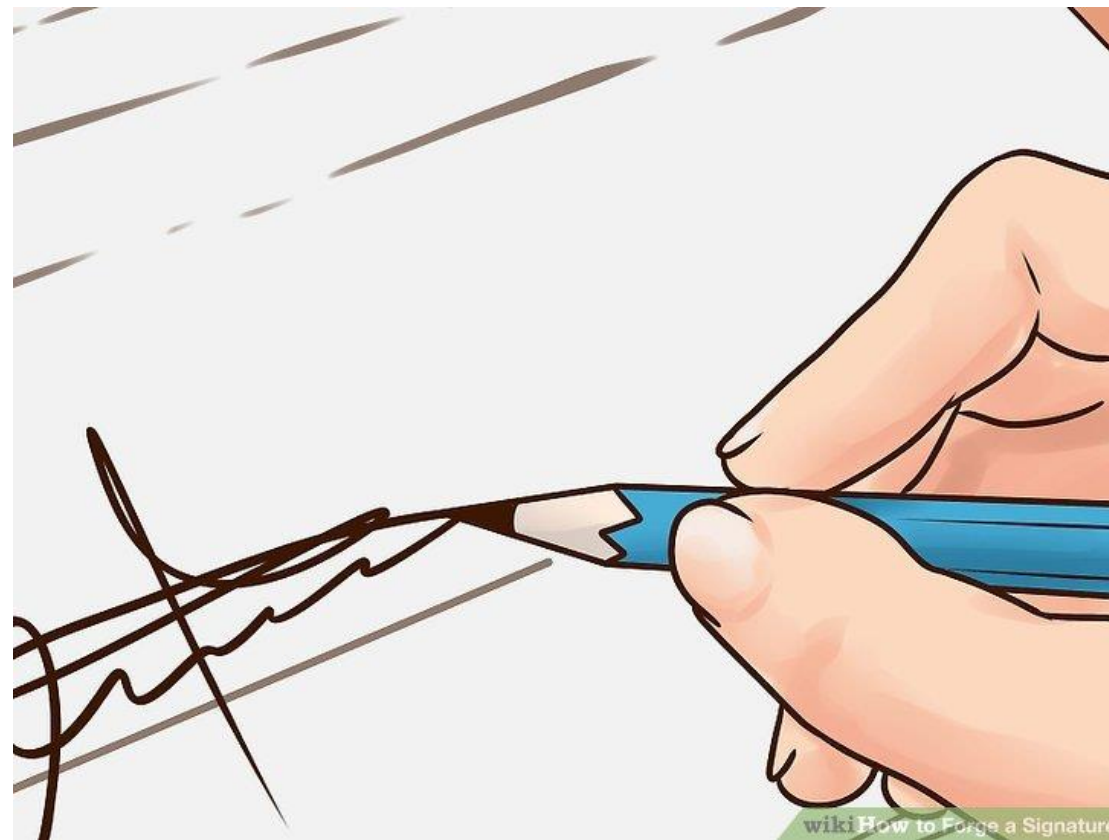


- Tienes una política BYOD, o no la tienes, pero entregaste laptops, tabletas y/o celulares a tus empleados.
- En un eventual ilícito cometido por alguno de ellos ¿cómo probarás que cada empleado tenía asignado determinado equipo?

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

@AbogadoDigital

- Cualquier empleado firmará lo que le des a firmar, **¡quiera 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.



#8: DESCUIDAR EL ESLABÓN MÁS DÉBIL...

@AbogadoDigital



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.

#9: EXCESO DE CONFIANZA

@AbogadoDigital

- 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.



#10: CHECKLIST PARA BLINDAR LEGALMENTE TU INFORMACIÓN Y ACTIVOS INTANGIBLE

1. Identifica qué tipo de información sensible tienes y por ende el marco regulatorio aplicable.
2. Firma cláusulas de confidencialidad y dale seguimiento a obligaciones de confidencialidad (dentro y fuera de la empresa).
3. Permea al interior de la empresa la cultura de la seguridad y confidencialidad de la información. Toma acciones preventivas y correctivas si detectas violaciones.
4. Dale trazabilidad a los dispositivos y a la información.
5. Evalúa periódicamente tus obligaciones en esta materia.

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

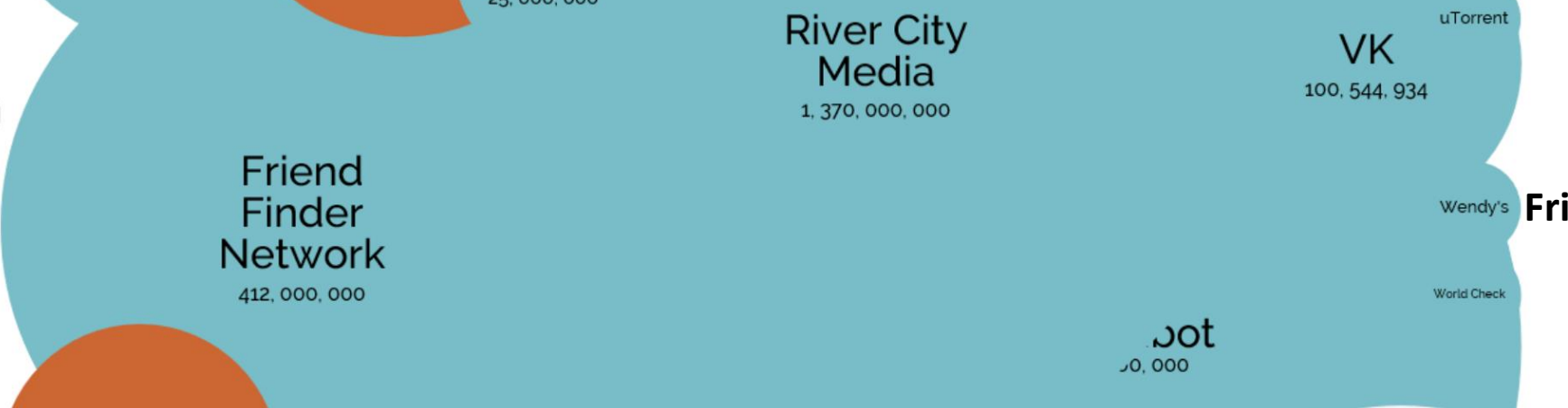
DATA SENSITIVITY

SHOW FILTER

2017



2016



2015



gadoDigital

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

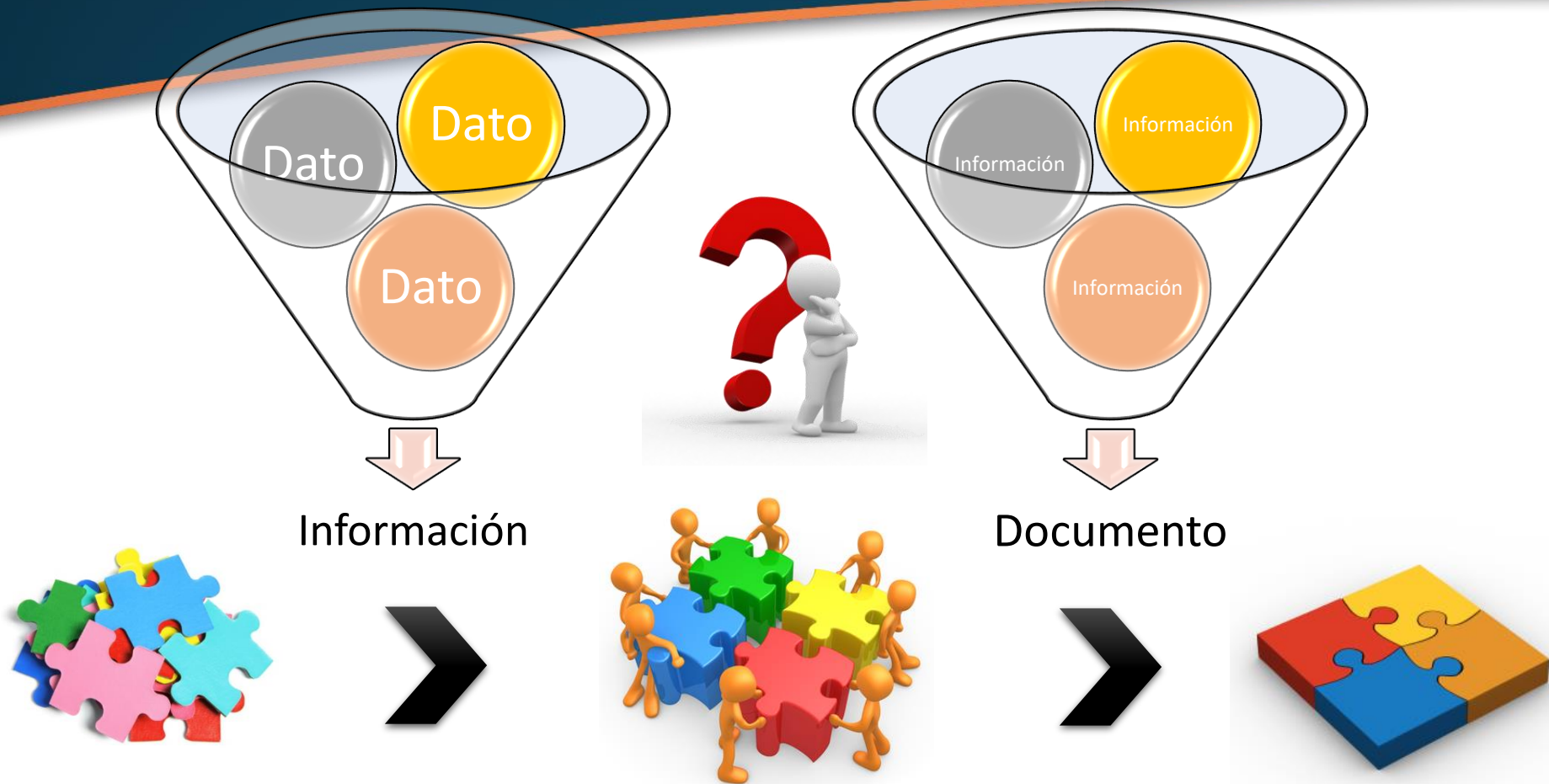
2015

- Uber 57,000,000
- JP Morgan Chase 76,000,000

2014

- Yahoo 500,000,000
- Ebay 145,000,000
- Target 70,000,000

www.Abogado.Digital



Derechos de autor, marcas, patentes, escrow

@AbogadoDigital



¿CÓMO SE PUEDE PROTEGER LA INFORMACIÓN Y RECURSOS TECNOLÓGICOS?

@AbogadoDigital





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

Joel A. Gómez Treviño
LEX INFORMÁTICA ABOGADOS, S.C.
ACADEMIA MEXICANA DE DERECHO INFORMÁTICO, A.C.

- www.LexInformatica.com
- JoelGomez.Abogado.Digital
- 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

[Twitter.com/AbogadoDigital](https://twitter.com/AbogadoDigital)

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.