@AbogadoDigital

CIBERSEGURIDAD Y DELITOS INFORMÁTICOS EN MÉXICO

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.

POLICÍA FEDERAL

CONSEJO DE LA JUDICATURA FEDERAL
INSTITUTO DE LA JUDICATURA FEDERAL
ESCUELA JUDICIAL

¿QUÉ SE MUEVE EN INTERNET?

Dinero

Información

¿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.

¿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.

REFLEXIONES PREVIAS...

"El hacha sirve para cortar cabezas; pero también la utilizamos para cortar árboles y hacer casas con su madera. Has de aprender a descubrir lo mucho bueno que hay en lo malo y lo malísimo que puede resultar lo bueno."

- Don Cesar de Echague by Jose Marllorquí

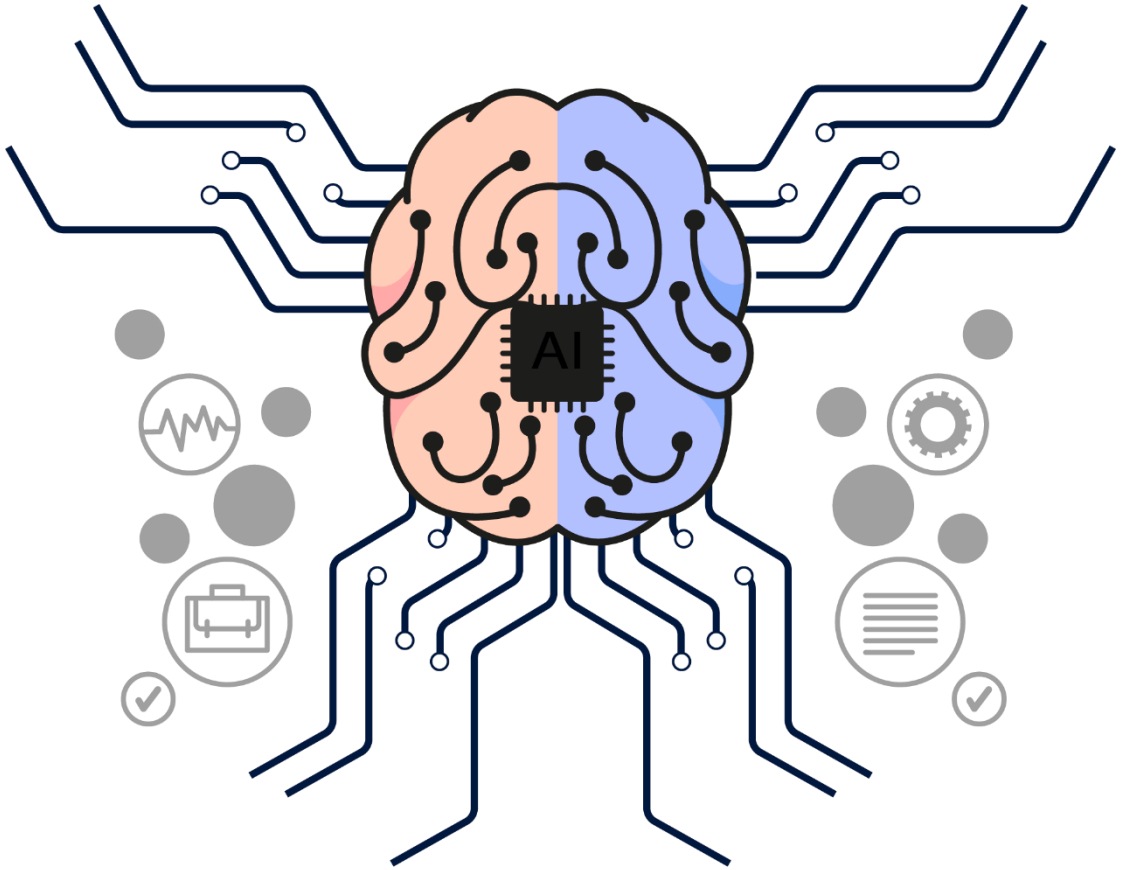
LA SEGURIDAD INFORMÁTICA...

¿ES OPCIONAL?

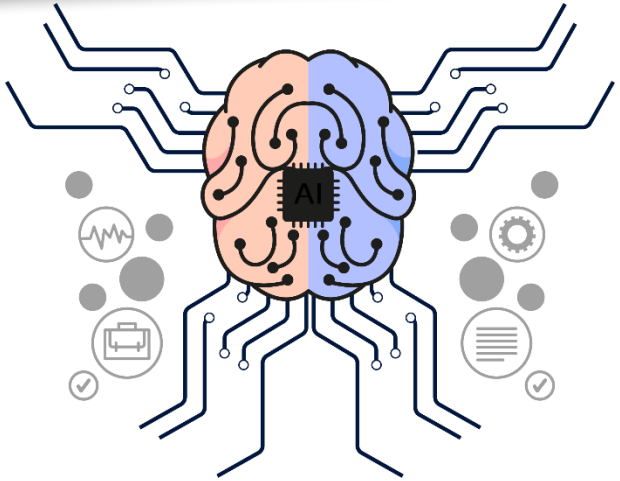
SEGURIDAD... ¿PARA QUÉ? ¿PARA QUIÉN?

¿DÓNDE RESIDEN LOS DATOS/INFORMACIÓN?

¿QUIÉN TIENE ACCESO A LOS DATOS / INFO?



¿A QUIÉN Y QUÉ TENEMOS QUE CUIDAR?



¿PUEDE LA INFORMACIÓN DAÑAR A ALGUIEN?

¿La FALTA (temporal o permanente) de información puede dañar a alguien?

¿La información FALSA, INCORRECTA o INEXACTA puede dañar a alguien?

¿La información ALTERADA o MANIPULADA puede dañar a alguien?

¿La información DAÑADA puede perjudicar a alguien?

¿La información en EXCESO puede dañar a alguien?

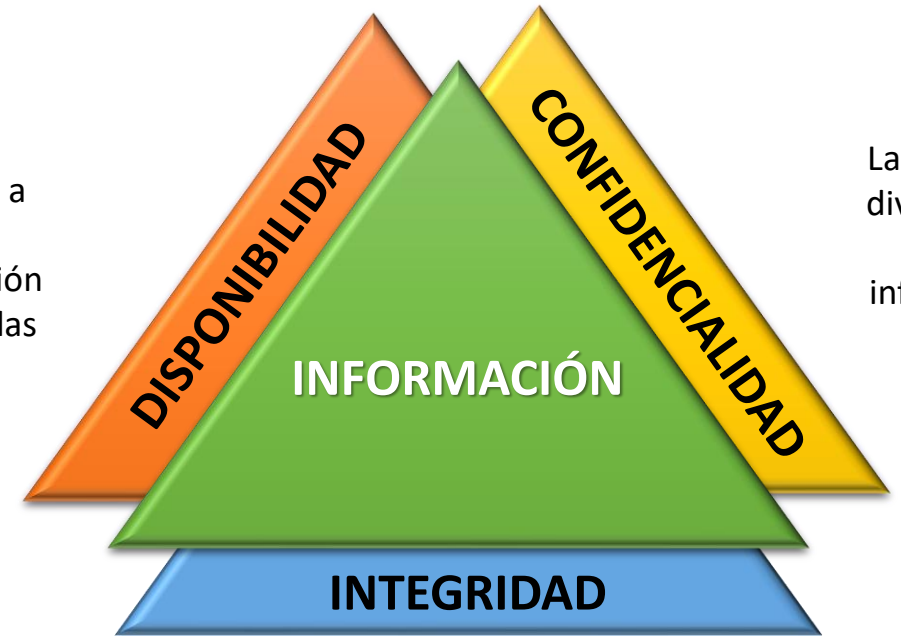
LA SEGURIDAD DE LA INFORMACIÓN Y SUS PARIENTES

Conceptos

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.



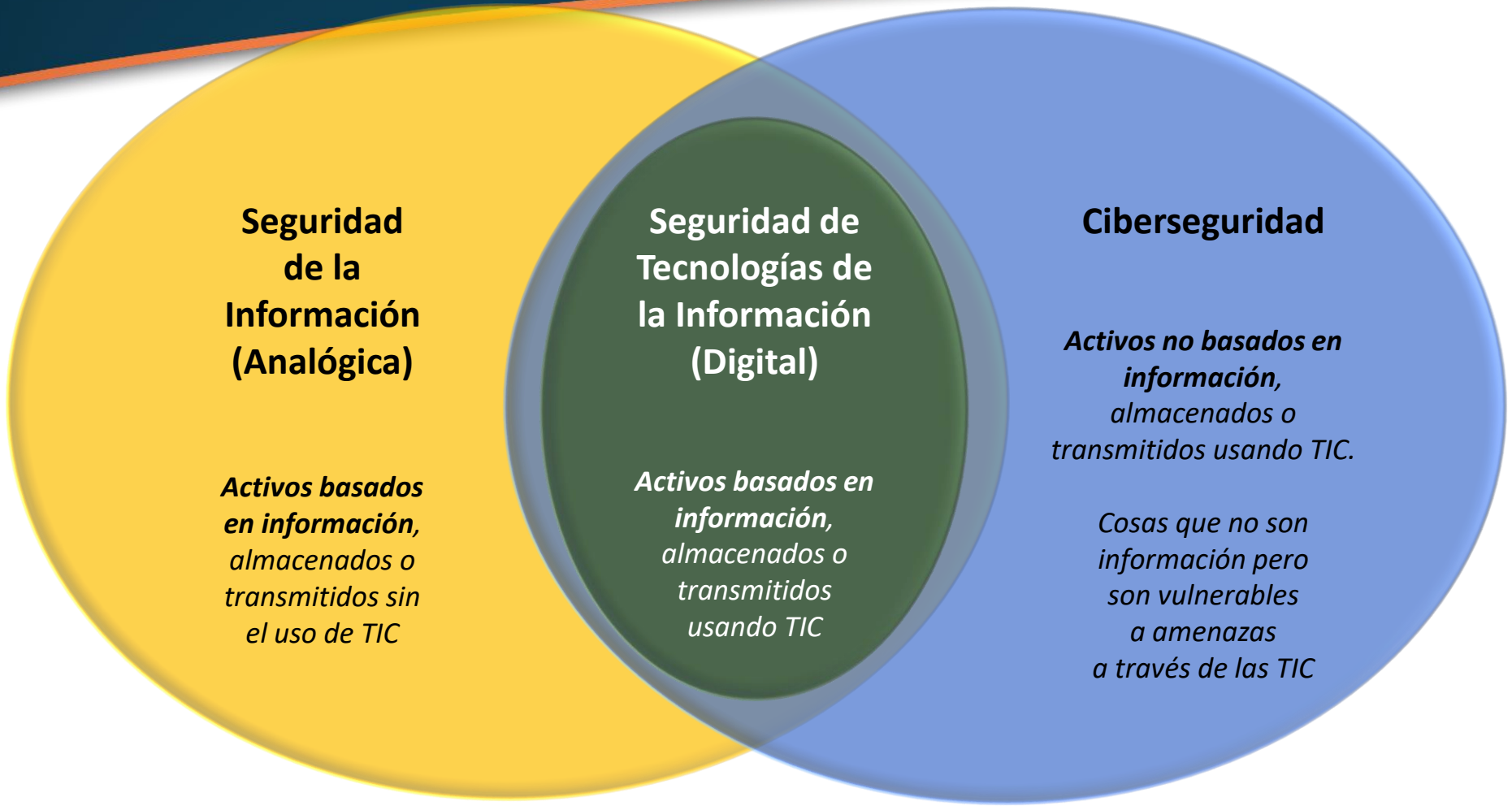
La confidencialidad es la propiedad que impide la divulgación de información a personas o sistemas no autorizados. Asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización.

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

¿SEGURIDAD DE... CIBER... SEGURIDAD?



DERECHO DE LA SEGURIDAD DE LA INFORMACIÓN

Definición y marco jurídico mexicano

Seguridad pública y seguridad privada

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 (Expedido por el Senado el 25 abril de 2018)
  - 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 (Expedido por el Senado el 25 abril de 2018)

  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.

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.

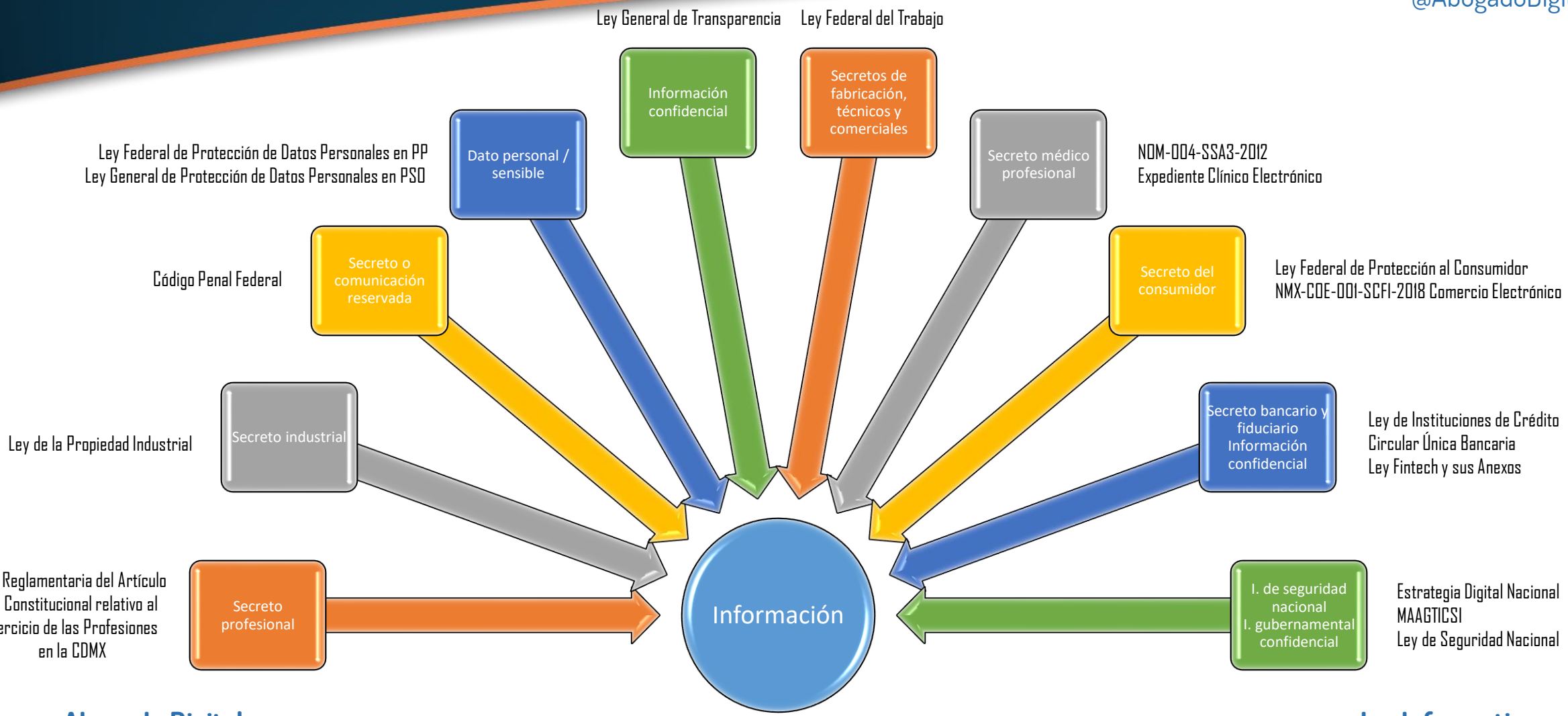
DERECHO DE LA SEGURIDAD DE LA INFORMACIÓN

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.

TIPOS DE INFORMACIÓN PROTEGIDA



PROBLEMAS EN LA WEB

Motivaciones cibercriminales

Razones por las que abundan las víctimas

¿QUÉ MOTIVACIONES PUEDE TENER UN CRIMINAL?

- Obtener dinero (lucro)
- Causar un daño o perjuicio
- Venganza
- Satisfacción personal (orgullo)
- Razones políticas

¿QUIÉN QUIERE HACERNOS DAÑO EN LA WEB?

- Cibercriminales (hackers)
- Hacktivistas
- Troles
  - Competencia
  - Clientes insatisfechos
  - Adversarios políticos
- Personas cercanas
  - Familiares
  - Amistades / examistades
  - Pareja / expareja
  - Compañeros del trabajo / escuela

¿POR QUÉ ES TAN FÁCIL DAÑAR O APROVECHARSE DE ALGUIEN EN INTERNET?

EN LA WEB ES MUY FÁCIL SER ANÓNIMO

¿POR QUÉ ES TAN FÁCIL DAÑAR O APROVECHARSE DE ALGUIEN EN INTERNET?

EN LA WEB ES MUY FÁCIL SUPLANTAR IDENTIDADES

¿POR QUÉ ES TAN FÁCIL DAÑAR O APROVECHARSE DE ALGUIEN EN INTERNET?

EN LA WEB ES MUY FÁCIL ENGAÑAR

¿POR QUÉ ES TAN FÁCIL DAÑAR O APROVECHARSE DE ALGUIEN EN INTERNET?

EN LA WEB ES MUY FÁCIL SER UN TROL

¿POR QUÉ HAY TANTAS VÍCTIMAS?

AVARICIA
LA GENTE QUIERE

- DINERO
  - FÁCIL
  - RÁPIDO
- COSAS GRATIS

¿POR QUÉ HAY TANTAS VÍCTIMAS?

EXCESO DE CONFIANZA

INGENUIDAD

¿POR QUÉ HAY TANTAS VÍCTIMAS?

FALTA DE SENTIDO COMÚN

¡Y DE INTELIGENCIA TAMBIÉN!

¿POR QUÉ HAY TANTAS VÍCTIMAS?

HEMOS PERDIDO EL CONTROL DE NUESTRA INFORMACIÓN

DELITOS INFORMÁTICOS Y CIBERATAQUES

No todo lo que parece un ciberdelito es un delito informático

¿QUÉ ES UN DELITO INFORMÁTICO?

Los delitos informáticos son aquellas actividades ilícitas que:

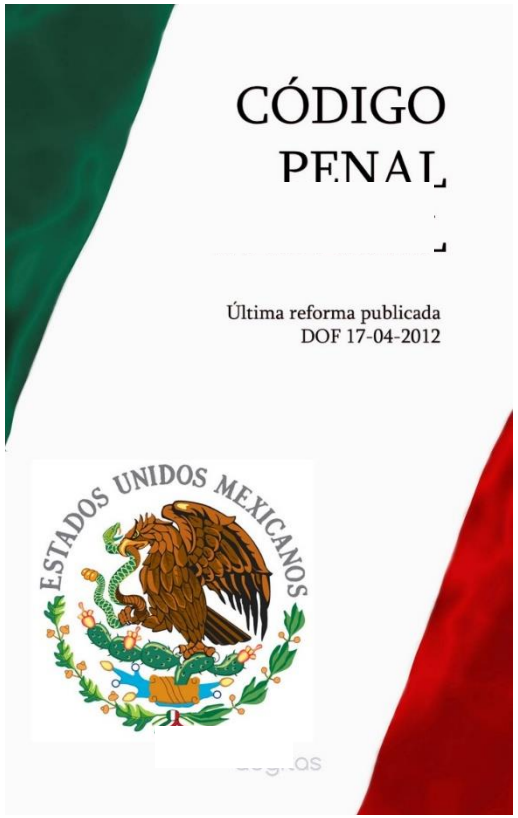
- **Se cometen mediante** el uso de computadoras, sistemas informáticos u otros dispositivos de comunicación, pero el daño o impacto es "off-line".
  - La informática es el medio o instrumento para realizar un delito "off-line"; o
- **Tienen por objeto** entrar sin autorización a un sistema informático, provocar pérdidas, causar daños, o impedir el uso de sistemas informáticos.
  - Delitos informáticos "*per se*" – *en sí mismos*. "La informática" es el fin del delito.

DELITO VS. ATAQUE INFORMÁTICO

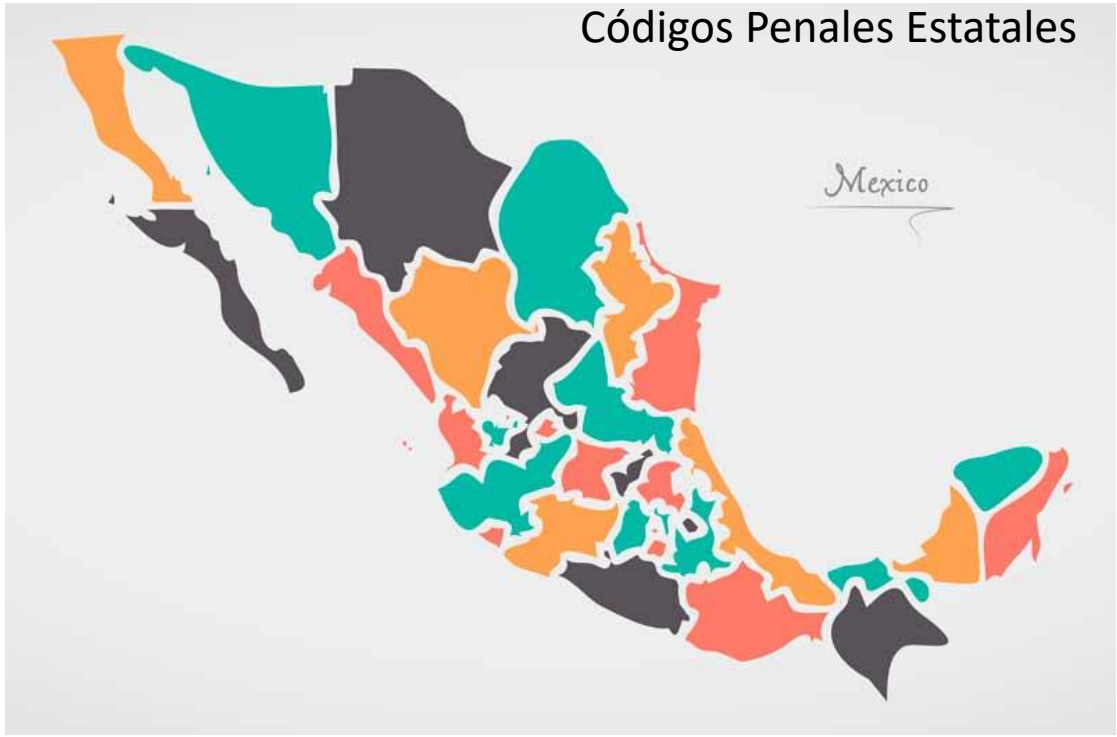
- Delito informático es la conducta típica, antijurídica, culpable y punible, en que se tiene a las computadoras como instrumento o fin.

- Ataque informático es la conducta indebida que también causa daños informáticos pero no esta contemplada en la legislación como delito.

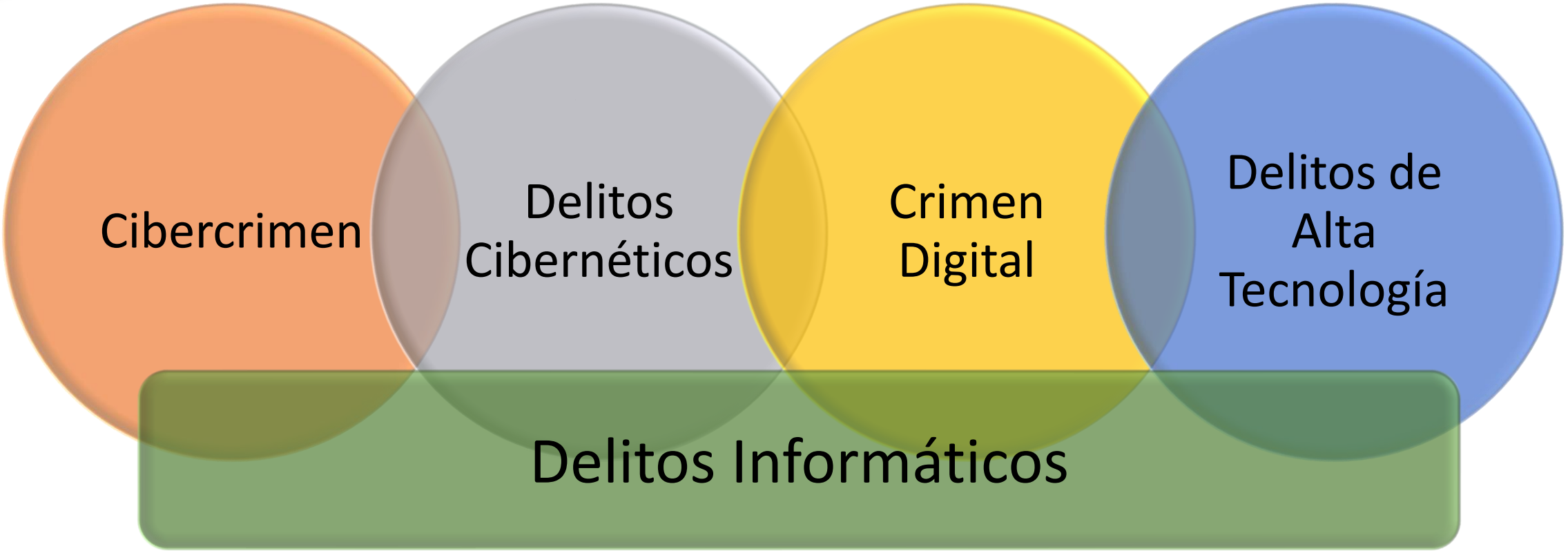
MUCHOS CÓDIGOS, MUCHOS DELITOS...



+



MUCHOS TÉRMINOS...



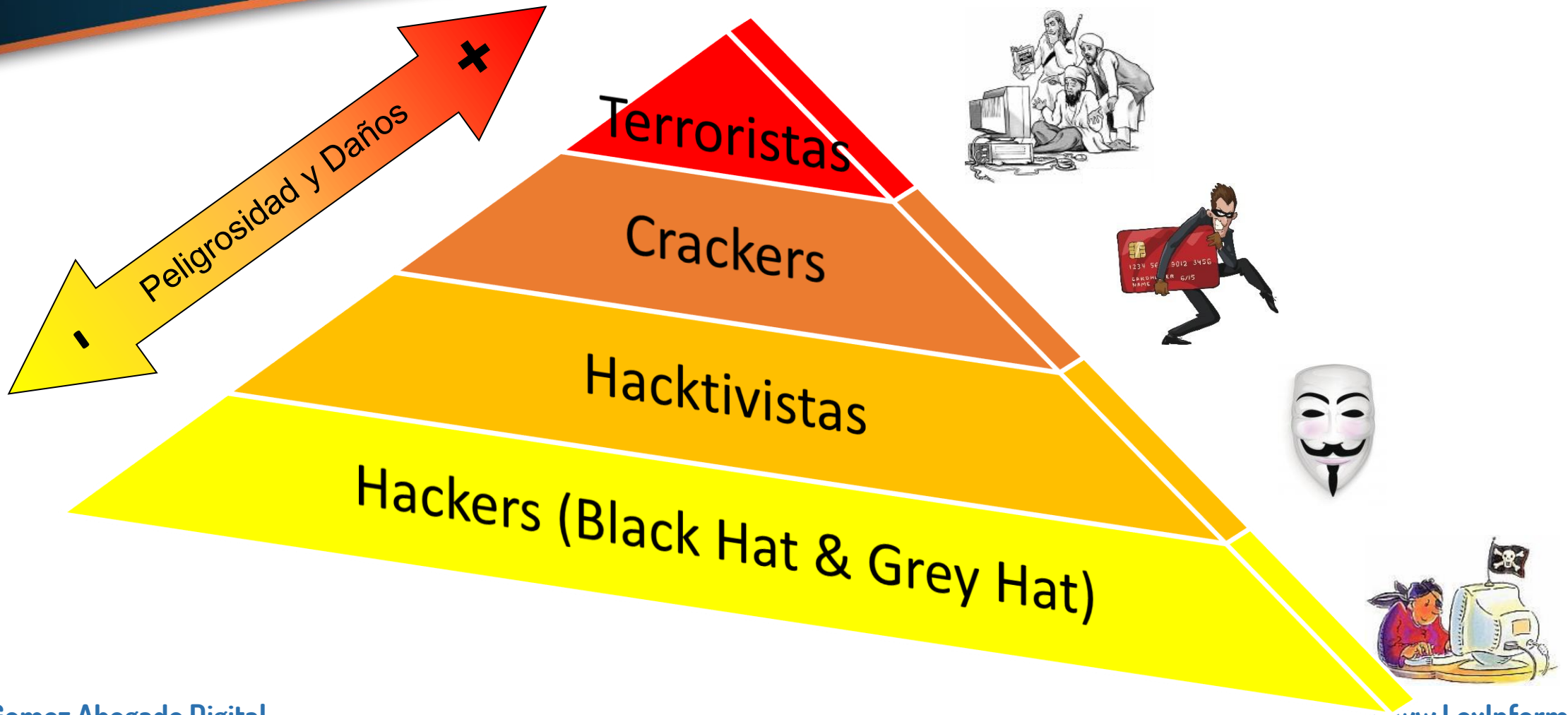
PROBLEMÁTICA

Los ataques más significativos son transnacionales por diseño y con víctimas en todo el mundo

Los ciberdelincuentes explotan las debilidades existentes en las leyes y prácticas de aplicación de la ley de los países (“*enforcement*”)

La velocidad y complejidad técnica de las actividades cibernéticas requiere de procedimientos pre-acordados entre la comunidad internacional

PIRÁMIDE DEL DELINCUENTE INFORMÁTICO



LOS DELINCUENTES Y LAS VÍCTIMAS (MÁS COMÚNES)

- Hackers y Crackers → Personas físicas al azar y eventualmente empresas
- Mercenarios y traficantes de información → Empresas, grandes corporativos y personas físicas a nivel masivo
- Terroristas y Grupos Extremistas → Gobierno y eventualmente grandes empresas

DIFERENCIAS ENTRE TÉRMINOS

Hacker

- Individuo que accede a un sistema informático sin autorización. Usualmente no tiene fines delictivos graves este tipo de intrusión, mediante la cual el hacker puede tener tres objetivos: practicar o probar sus habilidades, conocer y/o copiar información privada o secreta, o (en el peor de los casos) modificar, eliminar o provocar pérdida de información.
- El término puede tener connotaciones:
  - positivas (hacker = experto en informática) o
  - negativas (hacker = delincuente informático).
- Sin embargo, cualquier intrusión sin autorización a un sistema informático suele considerarse delictiva.

DIFERENCIAS ENTRE TÉRMINOS

Cracker

- Persona que penetra un sistema informático con el fin de robar o destruir información valiosa, realizar transacciones ilícitas, o impedir el buen funcionamiento de redes informáticas o computadoras. Este término fue acuñado por los "hackers" que se sentían criminalizados al asociarse dicho término en prensa a actividades delictivas-informáticas.

- Es poco utilizado el término "cracker".
- También se les puede conocer como "black hat hacker" (hacker de sombrero negro).

DIFERENCIAS ENTRE TÉRMINOS

Hacker Ético

- Profesional dedicado a brindar servicios de seguridad informática dentro del marco de la ley.
- También se les conoce como "white hat hackers" (hackers de sombrero blanco).

DIFERENCIAS ENTRE TÉRMINOS

Cibergrafitti

- Penetrar sitios web para modificar su contenido, desplegando imágenes obscenas, amenazas, mensajes ridiculizantes, burlas, etc.

Phreak

- Penetrar ilícitamente sistemas telefónicos o de telecomunicaciones con el fin de obtener beneficios o causar perjuicios a terceros.

DIFERENCIAS ENTRE TÉRMINOS

Warez (vs. Propiedad Intelectual)

- Grupo de personas fanáticos de la piratería de software. Su meta es violar códigos de seguridad (cracking) o generar, obtener o compartir números de registro (regging) de programas de computo, para luego subirlos a Internet y compartirlos con el mundo.

CiberPandillerismo

- Grupos de hackers o extremistas se reúnen para cometer o planear delitos, o para expresar ideas racistas, discriminatorias o xenofóbicas.

CIBERATAQUES COMUNES

Ataques contra la información o los sistemas (redes)

- Hacking
- Robo de información confidencial
- Ransomware
- DoS y DDoS

Ataques contra las personas

- Ciberacoso
- Robo de identidad
- Usurpación de identidad
- Violaciones a la intimidad

Ataques contra las empresas

- Cracking
- Espionaje
- Robo de secretos industriales
- Ransomware

Ataques contra el gobierno

- Hacktivismo
- Robo de información confidencial gubernamental
- Revelación de secretos
- Ciberterrorismo

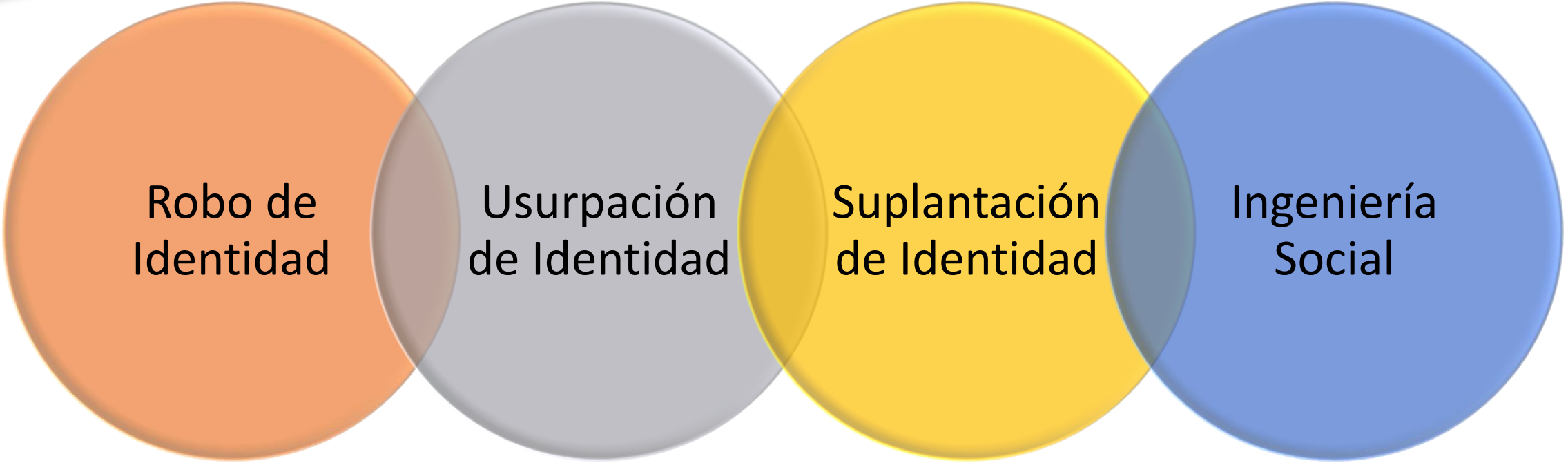
CLASIFICACIÓN DE D.I. POR MOTIVACIÓN

- **D.I. de entretenimiento, orgullo y exploración:**
  - Phreaking
  - Web defacement
  - Hacking
  - Warez
  - Virus
- **D.I. con causa:**
  - Hacktivismo
  - CiberTerrorismo
  - CiberAcoso
  - DDoS
- **D.I. motivados por lucro:**
  - Cracking
  - Fraude electrónico
  - Robo informático
  - Robo de Identidad
  - Ingeniería Social
  - Phishing
  - Cartas Nigerianas
  - Wi-Fi hacking
  - WarDriving
  - Clonación de tarjetas
  - DDoS, Virus, etc.

D.I. E ILÍCITOS VS. LA PRIVACIDAD, INTIMIDAD Y CONFIDENCIALIDAD INDUSTRIAL

- Contra las empresas, instituciones y gobierno
  - Virus
  - Spyware / Malware
  - Sniffing / packet sniffers
  - Keyloggers
  - Hacking / Cracking
  - Ingeniería Social
  - Robo informático de información confidencial o secretos industriales
- Contra las personas
  - Robo de identidad
  - Phishing
  - Carding y clonación
  - CiberAcoso
  - “Spamming”
  - Difamación y calumnia en redes sociales y cadenas de correos electrónicos
  - Pornografía infantil
  - Corrupción de menores

ROBO DE IDENTIDAD, MÚLTIPLES TÉRMINOS



¿ROBO O SUPLANTACIÓN DE IDENTIDAD?

- El término con el que internacionalmente se le reconoce a esta figura delictiva es "robo de identidad" (ID theft), aunque técnicamente es más correcto llamarle "usurpación de identidad" o "suplantación de identidad".
- **La usurpación o suplantación de identidad** es la apropiación indebida de datos (personales y/o financieros) de una persona física con el objeto de hacerse pasar por ella para:
  - Afectar su reputación o imagen en sociedad (simulación de identidad, creación perfiles falsos en redes sociales, esparcir datos falsos); y/o
  - Recabar datos de un tercero mediante engaño (phishing, vhising, ciberacoso, extorsión) ; y/o
  - Adquirir un beneficio económico (obtención de créditos, compras por internet, robo cibernético).

TÉCNICAS PARA PERPETRAR EL "ID THEFT"

- Para llegar al robo de identidad, el atacante pudo haber utilizado diversas técnicas o estrategias para apoderarse de tus datos financieros y personales, entre ellas:
  - **Skimming (clonación de tarjetas de crédito/débito):** apoderamiento de los datos de una tarjeta de crédito durante el momento de la transacción. Esta labor se logra gracias a pequeños aparatos llamados "skimming devices", que son portátiles o pueden ser colocados sobre los propios lectores de tarjetas de los cajeros automáticos (más una microcámara para captar el número PIN).
  - **Dumpster diving:** en Estados Unidos y otros países existen empresas que se dedican legalmente a ejecutar esta práctica. Consiste en acudir a los botes de basura de edificios u oficinas y llevarse la misma antes de que pase el camión recolector. Estas empresas tienen personal y equipo sofisticado para volver a "armar" papel previamente triturado.
  - **Ingeniería social**…

FACTORES QUE FACILITAN LA USURPACIÓN

- Engaño + ciberdelincuencia (ingeniería social, phising, vishing).
- Descuido (clonación de tarjetas) o negligencia (mal manejo de nuestra información personal y financiera).
- Accesibilidad de la información (mucha información está al alcance de muchos).
- Ausencia de controles en las empresas (medidas de seguridad técnicas, físicas y administrativas).
- Falta de sentido común de las personas. No cumplimiento de leyes aplicables.
- Leyes insuficientes e inadecuadas que la tipifiquen.

¿ESTÁ CONTEMPLADO EL R.I. COMO DELITO?

- Pocos códigos penales tipifican como delito la usurpación o suplantación de identidad. Algunos congresos estatales, como el de Jalisco, han recibido varias propuestas para incluir esta conducta en sus códigos penales pero hasta ahora no lo han logrado.
- **Código Penal para el Estado de Colima:**
- ARTÍCULO 234.- Se considera fraude y se impondrá pena de tres a nueve años de prisión y multa hasta por 100 unidades…:
  - VII.- **Al que por algún uso del medio informático**, telemático o electrónico alcance un **lucro indebido** para sí o para otro valiéndose de alguna **manipulación informática**, instrucciones de código, predicción, intercepción de datos de envío, reinyecte datos, use la red de redes montando sitios espejos o de trampa captando información crucial para el empleo no autorizado de datos, **suplante identidades**, modifique indirectamente mediante programas automatizados, imagen, correo o vulnerabilidad del sistema operativo cualquier archivo principal, secundario y terciario del sistema operativo **que afecte la confiabilidad, y variación de la navegación** en la red o use artificio semejante para obtener lucro indebido.

¿ESTÁ CONTEMPLADO EL R.I. COMO DELITO?

- **Código Penal para la Ciudad de México:**
- Artículo 211 Bis.- Al que por cualquier medio **usurpe, con fines ilícitos, la identidad de otra persona**, u otorgue su consentimiento para llevar a cabo la usurpación en su identidad, se le impondrá una pena de **uno a cinco años de prisión** y de cuatrocientos a seiscientos días multa. Se aumentaran en una mitad las penas previstas en el párrafo anterior, a quien se valga de la **homonimia**, parecido físico o **similitud** de la voz para cometer el delito establecido en el presente artículo.

¿ESTÁ CONTEMPLADO EL R.I. COMO DELITO?

- **Código Penal para el Estado de Morelos:**
- ARTÍCULO 189 Bis.- Al que por cualquier medio, **suplante la identidad de otra persona**, u otorgue su consentimiento para llevar a cabo la suplantación en su identidad, causando con ello un daño o perjuicio u obteniendo un lucro indebido, se le impondrá una pena de uno a cinco años de prisión, de cuatrocientos a seiscientos días multa y, en su caso, la reparación del daño que se hubiere causado. Serán equiparables al delito de suplantación de identidad y se impondrán las mismas penas previstas en el párrafo que precede, las siguientes conductas:
  - I. Al que, por algún uso de los medios informáticos o electrónicos, valiéndose de alguna manipulación informática o intercepción de datos de envío, cuyo objeto sea el empleo no autorizado de datos personales o el acceso no autorizado a bases de datos automatizadas para suplantar identidades, con el propósito de generar un daño patrimonial u obtener un lucro indebido para sí o para otro;
  - II. A quien transfiera, posea o utilice, sin autorización, datos identificativos de otra persona, con la intención de causar un daño patrimonial a otro u obtener un lucro indebido, o
  - III. Al que **asuma, suplante, se apropie o utilice** a través de internet, cualquier sistema informático, o medio de comunicación, l**a identidad de una persona física o jurídica que no le pertenezca**, causando con ello un daño o perjuicio u obteniendo un lucro indebido.

¿ESTÁ CONTEMPLADO EL R.I. COMO DELITO?

- 29-11-2016.- La Cámara de Diputados aprobó, con 414 votos a favor, el dictamen que adiciona un **artículo 430** (Título Vigésimo Séptimo "Delitos contra la identidad de las personas) al **Código Penal Federal**, para sancionar la usurpación de identidad con una pena de uno a seis años de prisión y 400 a 600 días de multa y, en su caso, la reparación del daño que se hubiere causado.
- El dictamen, enviado al Senado de la República para sus efectos constitucionales, destaca que **comete el delito de usurpación de identidad** quien por sí o por interpósita persona, usando cualquier medio lícito o ilícito, se apodere, apropie, transfiera, utilice o disponga de datos personales sin autorización de su titular o, bien, suplante la identidad de una persona, con la finalidad de cometer un ilícito o favorecer su comisión.
- Las penas aumentarán hasta en una mitad cuando el ilícito sea cometido por un servidor público que, aprovechándose de sus funciones, tenga acceso a bases de datos que contengan este tipo de información, así como a los particulares responsables del tratamiento de datos personales sensibles, en términos de la ley en la materia.

INGENIERÍA SOCIAL

- **Es el arte de atacar al eslabón más débil en la cadena de la seguridad informática: el ser humano.**
- Práctica consistente en obtener información confidencial, secreta o medios de acceso (claves y nombres de usuario) a sistemas informáticos mediante el engaño.
- No es necesario tener amplios conocimientos en informática para ejercer la ingeniería social, basta con ser convincente o tener habilidad para disuadir a personas.

INGENIERÍA SOCIAL

- La ingeniería social puede practicarse de muy diversas maneras:
  - *Personalmente*: el ingeniero social se presenta en una empresa u oficina y finge ser empleado de una empresa que repara computadoras o impresoras, para conseguir acceso a las instalaciones y una vez ahí poder instalar USB's infectados, keyloggers o tener acceso a computadoras de manera directa.
  - *Vía correo electrónico o telefónicamente*: estas prácticas son conocidas como "**phishing**" y "**vishing**" respectivamente.
  - *Empresas fantasma*: Defraudadores profesionales tienen la capacidad de crear sitios web que aparentemente pertenecen a empresas reales. Con apoyo de bases de datos robadas, envían correos o hacen llamadas telefónicas a clientes de estas empresas para ofrecerles un gran negocio, por ejemplo, "comprarles sus semanas de tiempo compartido" a cambio del pago de impuestos o cuotas de mantenimiento.

¿LA INGENIERÍA SOCIAL ES DELITO?

- Ninguna de las conductas antes descritas como ejemplos de "ingeniería social" están específicamente contempladas como delitos en nuestro Código Penal Federal. Sin embargo, estas conductas podrían caer en la figura conocida como "fraude genérico".
  - ***Artículo 386 del Código Penal Federal****.- Comete el delito de fraude el que engañando a uno o aprovechándose del error en que éste se halla se hace ilícitamente de alguna cosa o alcanza un lucro indebido.*
- Sin embargo, dada la modalidad y características de las conductas anteriormente descritas, es muy difícil localizar a los ciberdelincuentes para poder procesarlos.

PHISHING, SMISHING Y VISHING

- El phishing es una forma de **ingeniería social** que tiene por objetivo apoderarse de tus datos financieros mediante el engaño (**suplantación de identidad de una empresa u organización**). El phishing nace siempre con un correo electrónico que los atacantes envían a miles o millones de direcciones gracias a bases de datos de spammers. Dicho correo tiene la "identidad corporativa" usualmente de un banco o institución financiera.
- En su texto, el remitente suele identificarse como "el área de seguridad informática del Banco X" e informa al destinatario que su cuenta bancaria ha sido vulnerada ya que han detectado "movimientos sospechosos" en ella. Crean un sentido de urgencia en el destinatario para entrar de inmediato al portal del "Banco X" para identificarse (con nombre de usuario y contraseña) y así poder generarle una nueva cuenta o contraseña.

PHISHING, SMISHING Y VISHING

- Para hacer este procedimiento le ofrecen al destinatario una vía rápida: un enlace o botón que aparece al final del correo para entrar fácilmente al sitio web del banco. Al hacer clic en dicho botón o enlace, se abre en el navegador de la computadora una página apócrifa del banco, es decir, luce igual o muy similar a la de la institución financiera. La mayoría de los usuarios no saben leer o interpretar nombres de dominio, por lo que con que lean en cualquier parte de la barra de navegación el nombre de su banco, creerán que están en su sitio oficial.
- Una vez que se han ganado la confianza del usuario (al utilizar mismos logotipos, colores e identidad corporativa de la institución), y haberle creado el sentido de urgencia (invitándolo a actuar de inmediato para evitar que su cuenta sea "vaciada"), el destinatario finalmente introduce sus datos bancarios en el falso portal, de los cuales se apodera el atacante para luego poder disponer de los fondos de la víctima.

EJEMPLO DE PHISHING

ESTIMADO CLIENTE DE BANAMEX

Banamex le comunica que los servidores de procesos bancarios Banamex estan actualizados y estan ya operativos.
Sin embargo nos vemos en la obligación de pedirle su colaboración para una rápida restauración de los datos en las nuevas plataformas.

Si no ha entrado en su cuenta bancaria en las últimas 48 horas se recomienda entrar.

Puede entrar a su cuenta desde Banamex o para mayor comodidad hacer click sobre la imagen correspondiente a su tipo de cuenta.

BancaNet BancaNet Empresarial

Este sitio está diseñado para navegadores I.E. 6.0 y superiores

Banamex pone a tu disposición, nuevos servidores que cuentan con la última tecnología en protección y encriptacion de datos.
Una vez mas Banamex líder en el ramo.

Le recordamos que últimamente se envian e-mails de falsa procedencia con fines fraudulentos y lucrativos. Por favor **nunca** ponga los datos de su tarjeta bancaria en un mail y siempre compruebe que la procedencia del mail es de @banamex.com

Para cualquier duda o aclaración comuníquese con nosotros
al Tel. (5255) 1 226 3990

EJEMPLOS DE PHISHING

Banamex

Grupo Financiero Banamex le comunica:

Estimado cliente su cuenta de BancaNet de Banamex no ha podido cerrarse con exito ya que hay problemas con los servidores y hay fallos con el sistema, estamos trabajando para no tener mayores problemas con su inicio la siguiente vez que ingrese a BancaNet por lo tanto le pedimos por su seguridad que Ingrese de Inmediato a su sesion, esto le llevara solo un minuto de su tiempo Grupo Banamex le ofrece una disculpa y le ruega atienda este comunicado.

Numero de reporte: ID 091283563-0987-4253

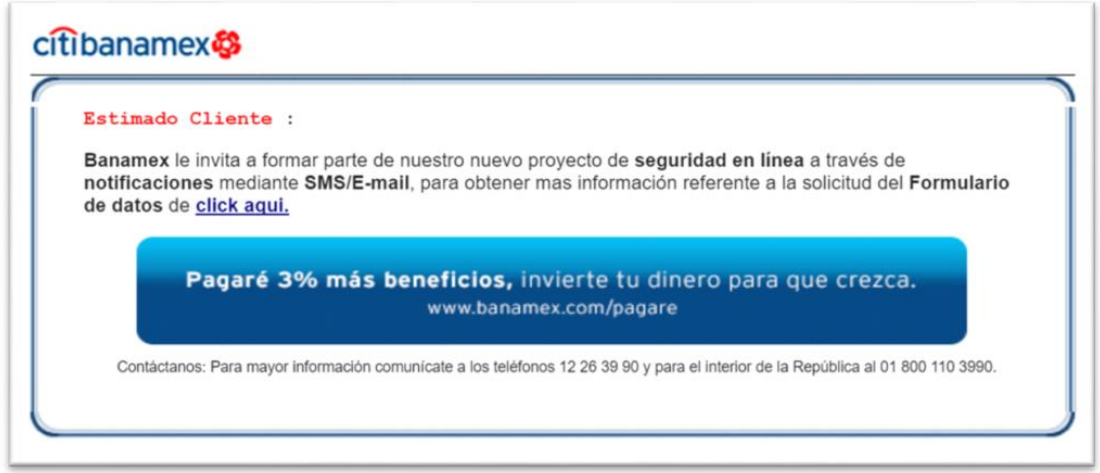
Recuerde que su Clave NETKEY expira, para realizar esta operacion es necesario utilizar una nueva.

Ingrese rapidamamente desde el siguiente Enlace:

Sesion BancaNet

PERSONAS **EMPRESAS**

Usted recibira un Email de Confirmacion al terminar su sesion para mayor Informacion acuda a cualquier Centro Banamex mas cercano.
Atte. Grupo Financiero Banamex



citibanamex

Estimado Cliente :

Banamex le invita a formar parte de nuestro nuevo proyecto de **seguridad en línea** a través de **notificaciones** mediante **SMS/E-mail**, para obtener mas información referente a la solicitud del **Formulario de datos** de click aqui.

Pagaré 3% más beneficios, invierte tu dinero para que crezca.
www.banamex.com/pagare

Contáctanos: Para mayor información comunícate a los teléfonos 12 26 39 90 y para el interior de la República al 01 800 110 3990.

EJEMPLO DE PHISHING

From: VISA Mexico <soporte.clientes@visa.com>
Date: 2006-08-24 0:41 GMT-05:00 Subject:
Atencion tarjetahabientes VISA To: abogado@*******.com

- Estimado Tarjetahabiente de Visa, Usted ha sido automaticamente registrado para darse de alta en el programa Verified by Visa. El programa de protección Verified by Visa le ofrece un nivel de seguridad sin paralelos. El programa Verified by Visa protege todas las tarjetas de crédito Visa emitidas por todas las instituciones bancarias del país y su protección se extiende sobre todas las transacciones procesadas por Visa - tanto en el mundo virtual, como en el mundo real. Es muy simple y eficiente. Haga compras en línea y en persona con absolutamente cero riesgo. Use su tarjeta Visa para adquirir productos y servicios en línea, en una tienda local o en cualquier lugar del mundo y usted está protegido contra el uso no autorizado de su tarjeta o de la información de su cuenta.
- Verified by Visa le ofrece:
  - Seguridad de acuerdo a los últimos avances tecnológicos
  - Protección completa contra el fraude
  - Cero deuda en caso de las transacciones fraudulentas
- Para evitar la interrupción de la cobertura antifraude de su tarjeta y de otros servicios provistos por Visa le pedimos verificar su tarjeta a más tardar 72 horas a la recepción y lectura de este correo.
- Haga click aquí para verificar su tarjeta ahora mismo: **http://www.verificado-por-visa.org.mx**
- Este correo ha sido enviado automáticamente por el sistema Soporte a Clientes de Visa México. Favor de no responder a este correo.

EJEMPLO DE PHISHING

Quien es quien en las gasolineras Inbox x Phising x

Profeco <profeco@camaradecomercio.com.mx>
to abogado

Por una cultura de consumo inteligente...

Estimado Ciudadano Le informamos que La Escuela Tec De Monterrey y Profeco Tienen Como Proyecto Informale a los Ciudadanos de Mexico Un Servicio Que le Informa Que Gasolineras De la ciudad de Mexico son irregulares por lo tanto seria aconsajable que usted tome medidas de su provedor de gasolina mas cercano o tenga en otras opciones algunas que si se ajusten a su precio y cantidad por litro.

Descargar Verificador de Gasolineras

profecomexico.webspacemania.com/profeco.exe

PROFECO - Procuraduría Federal del Consumidor - México © Todos Los Derechos Reservados

México, 24 Setiembre 2007

¿CUÁNTAS VÍCTIMAS DE PHISHING EXISTEN?

- Según un reporte publicado en el mes de marzo de 2017, el porcentaje de personas que hacen clic en un email con phishing es entre el 10 y el 24%. De ellas, entre un 34 y un 74% proporcionaron datos personales o financieros, y de este porcentaje entre el 17 y el 81% descargaron un archivo malicioso.
- Si usted cree que de todas maneras es un porcentaje muy bajo de personas que cae en este engaño (10 a 24%), piense que estos correos son enviados a millones de personas en el mundo. Solo por poner un ejemplo, en una base de datos de 5,000,000 de correos caen en este fraude de 500,000 (10%) a 1,200,000 (24%) personas.

VARIANTE 1: SPEAR PHISHING

- Existe una variante de este fenómeno delictivo llamada "spear phishing" (pesca con lanza). A diferencia del phishing que no tiene un destinatario específico (se lanza el "anzuelo" a miles o millones de correos electrónicos), el spear phishing si tiene un objetivo específico.
- Digamos que te acaban de correr de tu trabajo o te peleaste con tus socios. Conoces bastante información sobre tu ex-jefe o ex-socio. Le envías un correo electrónico desde un servicio gratuito de "envío de correos falsos" para que parezca que proviene de un cliente que sabes que tiene. Conoces qué clase de negocios tiene con el cliente e incluso detalles específicos (cotizaciones pendientes, negociaciones de precios, etc.) Le envías un correo muy convincente, pidiéndole que revise de inmediato el archivo adjunto pues mañana tomará una decisión al respecto.
- El archivo, aunque parece un PDF legítimo, en realidad se trata de malware o código que te llevará a una página web apócrifa. A pesar de que el spear phishing siempre va dirigido solo a una persona, suele ser mucho más efectivo que el phishing convencional, ya que al conocer detalles de la víctima, es altamente probable que caiga en el engaño.

VARIANTE 2: SMISHING

- Otra variante del phishing es el "SMiShing". La diferencia es el medio de propagación del "anzuelo" para concretar en engaño. En el phishing y spear phishing el "anzuelo" se lanza a través de correo electrónico. En SMiShing se lanza a través de un mensaje de texto que llega a tu teléfono (SMS). El ciberdelincuente te envía un SMS, usualmente pretendiendo ser una empresa conocida o legítima. En ocasiones también pueden enviarte una clásica oferta tentadora: "te acabas de ganar un premio" o "te ofrecemos un 50% de descuento en la compra de X".
- En cualquier caso, te piden que te comuniques a un número telefónico para conseguir tu premio (lo cual se puede transformar en "vishing") o que hagas clic en un enlace para que te otorguen el descuento deseado. Al hacerlo, podrías descargar una aplicación maliciosa para que el ciberdelincuente consiga acceso a tu teléfono y así obtenga datos personales o financieros.

VARIANTE 3: VISHING

- El vishing es otra forma de ingeniería social, derivada del phishing, pero en lugar de utilizar un correo electrónico para engañar al usuario, lo hacen a través de llamadas telefónicas realizadas mediante el Protocolo Voz sobre IP (VoIP). El atacante realiza llamadas a números telefónicos de determinada región, cuando la persona contesta le alerta que "su tarjeta de crédito ha sido clonada" o cualquier otra situación similar, por lo que le invita a llamar a un número telefónico de emergencia para reportar el hecho.
- Ese número suele ser gratuito y obviamente falso, donde se pretende suplantar la identidad de cierta institución comercial o financiera. Contesta una grabadora de voz pidiendo al cliente introduzca mediante el teclado de su teléfono toda la información sobre su tarjeta de crédito lo cual es requerido para verificarla y "bloquear" posibles cargos no autorizados. Una vez hecho lo anterior, el "visher" ha obtenido toda la información necesaria para realizar cargos fraudulentos a la víctima.

¿ESTAS CONDUCTAS SON DELITOS?

- Ninguna de las conductas antes descritas como ejemplos de "ingeniería social" están específicamente contempladas como delitos en nuestro Código Penal Federal. Sin embargo, estas conductas podrían caer en la figura conocida como "fraude genérico".
- Artículo 386 del Código Penal Federal.- Comete el delito de fraude el que engañando a uno o aprovechándose del error en que éste se halla se hace ilícitamente de alguna cosa o alcanza un lucro indebido.
- Sin embargo, dada la modalidad y características de las conductas anteriormente descritas, es muy difícil localizar a los ciberdelincuentes para poder procesarlos.

FRAUDE ELECTRÓNICO

- En la actualidad es muy sencillo comprar un nombre de dominio y diseñar una página web. Estas dos actividades suelen ser muy económicas, e incluso llegan a ser gratuitas en algunos casos. Otra cosa que suele ser muy fácil en internet es ser anónimo o crear identidades falsas. Los cibercriminales aprovechan estos factores para cometer fraudes electrónicos en la web.

F.E.: TRANSACCIONES CON DINERO AJENO

- Un ciberdelincuente tiene en su poder una gran cantidad de datos de tarjetas de crédito o débito que han sido clonadas (vía ***skimming*** o ***phishing***). Entre la información con la que cuenta están los datos personales de los titulares de las tarjetas clonadas. Ello le permite hacer cargos por internet como si fuera la víctima.
- Si compra productos físicos -que deban de ser enviados a una dirección postal-, se estaría arriesgando a ser descubierto, salvo que use un "PO Box" (buzón postal) o direcciones que no le pertenezcan para recibir los artículos comprados. En ambos casos, aunque el riesgo de ser ubicado disminuye, de todas maneras existe.
- ¿Cómo hacer dinero con tarjetas de crédito clonadas de manera 100% segura? Hay dos opciones principalmente:
  - Vender esos datos en portales de hackers (*carding forums*) y dejar que otros encuentren maneras para hacer dinero con esa información, o
  - Venderle a terceros productos comprados con esas tarjetas clonadas.

F.E.: FALSOS VENDEDORES, FALSAS VENTAS

- Los cibercriminales se aprovechan de portales de avisos clasificados, sitios web apócrifos (creados por ellos mismos), redes sociales o mercados de compradores (como Mercadolibre) para publicar anuncios de venta de productos muy atractivos por su precio.

- Caso: Compraventa de Autobuses a “bajo costo” o con descuentos atractivos.

OTROS FRAUDES ELECTRÓNICOS

- El fraude escrow: “el auto de tus sueños a un precio increíble”.
- Las vacaciones de tus sueños (ofertas de tiempos compartidos).
- Fraudes nigerianos / cartas nigerianas / fraude amoroso.

- Ninguna de las conductas antes descritas como ejemplos de "fraude electrónico" están específicamente contempladas como delito(s) en nuestro Código Penal Federal. Sin embargo, estas conductas podrían tipificarse como fraude genérico.
- ***Artículo 386 del Código Penal Federal***.- *Comete el delito de fraude el que engañando a uno o aprovechándose del error en que éste se halla se hace ilícitamente de alguna cosa o alcanza un lucro indebido.*
- Sin embargo, dada la modalidad y características de los fraudes electrónicos anteriormente descritos, es muy difícil localizar a los ciberdelincuentes para poder procesarlos.

DELITOS INFORMÁTICOS EN MÉXICO

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**.

LEY DE LA PROPIEDAD INDUSTRIAL

- Para que se considere que existe un secreto industrial es necesario que concurran los siguientes requisitos (art. 82 y 83):
  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;

LEY DE LA PROPIEDAD INDUSTRIAL

- Para que se considere que existe un secreto industrial es necesario que concurran los siguientes requisitos (art. 82 y 83):
  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.

CÓDIGO PENAL FEDERAL

REVELACIÓN DE SECRETOS

- **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.

CÓDIGO PENAL FEDERAL

ART. 211 BIS 1

- Al que sin autorización **modifique, destruya o provoque pérdida de información** contenida en sistemas o equipos de informática **protegidos por algún mecanismo de seguridad**, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

- Al que sin autorización **conozca o copie información** contenida en sistemas o equipos de informática **protegidos por algún mecanismo de seguridad**, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

CÓDIGO PENAL FEDERAL

ART. 211 BIS 2

- Al que sin autorización **modifique, destruya o provoque pérdida de información** contenida en sistemas o equipos de informática **del Estado**, **protegidos por algún mecanismo de seguridad**, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.

- Al que sin autorización **conozca o copie información** contenida en sistemas o equipos de informática **del Estado**, **protegidos por algún mecanismo de seguridad**, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

CÓDIGO PENAL FEDERAL

ART. 211 BIS 2

- A quien sin autorización **conozca, obtenga, copie** o **utilice** información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos **de seguridad pública**, **protegido por algún medio de seguridad**, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal.

- Las sanciones anteriores se duplicarán **cuando la conducta obstruya, entorpezca, obstaculice, limite o imposibilite la procuración o impartición de justicia**, o recaiga sobre los registros relacionados con un procedimiento penal resguardados por las autoridades competentes.

CÓDIGO PENAL FEDERAL

ART. 211 BIS 3

- Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, **indebidamente modifique, destruya o provoque pérdida de información** que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.

- Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, **indebidamente copie información** que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

CÓDIGO PENAL FEDERAL

ART. 211 BIS 3

- A quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, **indebida-mente obtenga, copie o utilice información que contengan**, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal.

- Si el responsable es o hubiera sido **servidor público** en una **institución de seguridad pública**, se impondrá además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública multa.

CÓDIGO PENAL FEDERAL

ART. 211 BIS 4

- Al que sin autorización **modifique, destruya o provoque pérdida de información** contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, **protegidos por algún mecanismo de seguridad**, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

- Al que sin autorización **conozca o copie información** contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, **protegidos por algún mecanismo de seguridad**, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

CÓDIGO PENAL FEDERAL

ART. 211 BIS 5

- Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, **indebidamente modifique, destruya o provoque pérdida de información** que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

- Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, **indebidamente copie información** que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

CÓDIGO PENAL FEDERAL

ART. 211 BIS 5 Y 7

- **Artículo 211 bis 5**.- Las penas previstas en este artículo se incrementarán en una mitad cuando las **conductas sean cometidas por funcionarios o empleados** de las instituciones que integran el sistema financiero.

- **Artículo 211 bis 7**.- Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la **información obtenida se utilice en provecho propio o ajeno**.

¿QUÉ FALTA REGULAR?

- Virus, gusanos, troyanos
  - Creación, inserción, diseminación o comercialización de cualquier tipo de código malicioso
- CiberAcoso o CyberBullying
- Grooming / Acoso Sexual
- Phishing / ID Theft
- Cybercrime as a Service
- Comercialización de información obtenida ilícitamente a través de intrusiones informáticas
- Secuestro de Datos Informáticos
  - Ransomware
- Hacktivismo
  - Ataques DoS / DDoS
- Ciberterrorismo

DELITOS INFORMÁTICOS EN CÓDIGOS PENALES ESTATALES

Anexo

CAPÍTULO II **La Obtención Ilícita de Información Electrónica**

- Artículo 143-Bis. Al que sin autorización y de manera dolosa, **copie, modifique, destruya o provoque pérdida de información** contenida en sistemas o equipos de informática, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días de multa.
- Las penas previstas en este artículo se incrementarán en una mitad cuando el sujeto pasivo del delito sea una entidad pública o institución que integre el sistema financiero.

CAPÍTULO III **Utilización Ilícita de información Confidencial**

- Artículo 143-Ter. Se impondrán de tres a seis años de prisión a la persona que, **teniendo acceso a bases de datos con información confidencial de instituciones o personas**, emplee esta información para fines ilícitos, o transmita esta información a terceros para ser empleada con fines ilícitos.

CAPÍTULO IV **Suplantación de Identidad**

- Artículo 143-Quáter. Comete el delito de **suplantación de identidad** quien **suplante con fines ilícitos o de lucro**, se atribuya la identidad de otra persona por cualquier medio, u otorgue su consentimiento para llevar la suplantación de su identidad, **produciendo con ello un daño moral o patrimonial**, u **obteniendo un lucro o un provecho indebido** para sí o para otra persona.
- Este delito se sancionará con prisión de tres a ocho años y multa de mil a dos mil salarios.

CÓDIGO PENAL DE JALISCO

Serán equiparables al delito de suplantación de identidad y se impondrán las penas establecidas en este artículo:

I. Al que por algún uso de medio electrónico, telemático o electrónico obtenga algún lucro indebido para sí o para otro o genere un daño patrimonial a otro, **valiéndose de alguna manipulación informática o intercepción de datos de envío**, cuyo objeto sea el empleo no autorizado de datos personales o el acceso no autorizado a base de datos automatizados para suplantar identidades;

II. Al que transfiera, posea o utilice datos identificativos de otra persona con la intención de cometer, favorecer o intentar cualquier actividad ilícita; o

III. Al que asuma, suplante, se apropie o utilice, a través de internet, cualquier sistema informático o medio de comunicación, **la identidad de una persona física o jurídica que no le pertenezca**, produciendo con ello un daño moral o patrimonial, u obteniendo un lucro o un provecho indebido para sí o para otra persona.

Se aumentará hasta en una mitad las penas previstas en el presente artículo, a quien se valga de la homonimia, parecido físico o similitud de la voz para cometer el delito; **así como en el supuesto en que el sujeto activo del delito tenga licenciatura, ingeniería o cualquier otro grado académico en el rubro de informática, computación o telemática**.

CAPÍTULO VIII **Falsificación de Medios Electrónicos o Magnéticos**

- Artículo 170-Bis. Se impondrán de tres a nueve años de prisión y multa por el equivalente de doscientos a cuatrocientos días de salario mínimo general vigente en la época y área geográfica en que se cometa el delito, al que, sin consentimiento de quien esté facultado para ello:
  - I. Produzca, imprima, enajene, distribuya, altere o falsifique, aún gratuitamente, adquiera, utilice, posea o detente, sin tener derecho a ello, **boletos, contraseñas, fichas, tarjetas u otros documentos que no estén destinados a circular y sirvan exclusivamente para identificar** a quien tiene derecho a exigir la prestación que en ellos se consigna, siempre que estos delitos no sean de competencia federal;
  - **II. Altere, copie o reproduzca, indebidamente, los medios de identificación electrónica de boletos, contraseñas, fichas u otros documentos** a los que se refiere la fracción I de este artículo;

CAPÍTULO VIII **Falsificación de Medios Electrónicos o Magnéticos**

- Artículo 170-Bis. (continuación):

III. Acceda, obtenga, posea o detente indebidamente **información de los equipos electromagnéticos o sistemas de cómputo de las organizaciones emisoras** de los boletos, contraseñas, fichas u otros documentos a los que se refiere la fracción I de este artículo, y los destine a alguno de los supuestos que contempla el presente artículo; y

IV. Adquiera, utilice, posea o detente **equipos electromagnéticos o electrónicos para sustraer en forma indebida la información contenida** en la cinta magnética de los boletos, contraseñas, fichas u otros documentos a los que se refiere la fracción I del artículo.

CÓDIGO PENAL DE NUEVO LEÓN

CAPITULO UNICO VIOLACION DE CORRESPONDENCIA
ARTÍCULO 178.- COMETE EL DELITO DE VIOLACIÓN DE CORRESPONDENCIA:

- I.- **QUIEN ABRA INDEBIDAMENTE UNA COMUNICACIÓN ESC**RITA O QUE SE ENCUENTRE EN CUALQUIER **MEDIO MATERIAL O ELECTRÓNICO** QUE NO LE ESTÉ DIRIGIDA; O
- II.- **QUIEN INDEBIDAMENTE INTERCEPTE UNA COMUNICACIÓN** ESCRITA O QUE SE ENCUENTRE EN CUALQUIER MEDIO MATERIAL O ELECTRÓNICO QUE NO LE ESTÉ DIRIGIDA, AUNQUE LA CONSERVE CERRADA Y NO SE IMPONGA DE SU CONTENIDO.
- AL RESPONSABLE DE ESTE DELITO SE LE IMPONDRÁ UNA PENA DE PRISIÓN DE TRES DÍAS A SEIS MESES Y MULTA DE CINCO A CIEN CUOTAS.

CÓDIGO PENAL DE NUEVO LEÓN

- ARTÍCULO 242 BIS.- SE IMPONDRÁN DE TRES A NUEVE AÑOS DE PRISIÓN Y MULTA DE CIENTO CINCUENTA A CUATROCIENTAS CINCUENTA CUOTAS AL QUE, SIN CONSENTIMIENTO DE QUIEN ESTÉ FACULTADO PARA ELLO, INCURRA EN CUALQUIERA DE LAS SIGUIENTES CONDUCTAS:
- I.- PRODUZCA, REPRODUZCA, INTRODUZCA AL ESTADO, ENAJENE, AÚN GRATUITAMENTE, O ALTERE, **TARJETAS DE CRÉDITO O DE DÉBITO**, O LA INFORMACIÓN CONTENIDA EN ÉSTAS, ESQUELETOS DE CHEQUE O DOCUMENTOS UTILIZADOS PARA EL PAGO DE BIENES Y SERVICIOS O PARA DISPOSICIÓN DE EFECTIVO;
- IV.- **ALTERE LOS MEDIOS DE IDENTIFICACIÓN ELECTRÓNICA** DE CUALQUIERA DE LOS OBJETOS A QUE SE REFIERE LA FRACCIÓN I DE ESTE ARTÍCULO ; O
- V.- **ACCEDA INDEBIDAMENTE A LOS EQUIPOS ELECTROMAGNÉTICOS DE LAS INSTITUCIONES EMISORAS** DE CUALQUIERA DE LOS OBJETOS A QUE SE REFIERE LA FRACCIÓN I DE ESTE ARTÍCULO.

CÓDIGO PENAL DE NUEVO LEÓN

- ARTÍCULO 249.- COMETE EL DELITO DE FALSEDAD DE DECLARACIONES Y EN INFORMES DADOS A UNA AUTORIDAD QUIEN, BAJO PROTESTA DE DECIR VERDAD, INCURRA EN ALGUNO DE LOS SIGUIENTES SUPUESTOS:
- …
- ADEMÁS, COMETE EL DELITO DE FALSEDAD **QUIEN PROPORCIONE DATOS O INFORMACIÓN A INSTITUCIONES DE SEGURIDAD PÚBLICA** O CUALQUIER AUTORIDAD PÚBLICA EN EJERCICIO DE SUS FUNCIONES, UTILIZANDO INTERNET O CUALQUIER OTRO MEDIO DE COMUNICACIÓN TELEFÓNICO O ELECTRÓNICO, **AFIRMANDO UNA FALSEDAD O NEGANDO LA VERDAD EN TODO O EN PARTE**, ASÍ COMO TAMBIÉN LA PERSONA QUE PERMITA O FACILITE SU APARATO O EQUIPO DE COMUNICACIÓN A SABIENDAS DE ESTA CIRCUNSTANCIA. PARA EFECTOS DE ESTE PÁRRAFO, NO SE LE REQUERIRÁ LA TOMA DE PROTESTA DE DECIR VERDAD QUE SEÑALA ESTE ARTÍCULO.

CÓDIGO PENAL DE NUEVO LEÓN

- ARTICULO 271 BIS 5.- **TRATANDOSE DE DELITOS SEXUALES**, SE INCREMENTARA LA PENA EN UNA MITAD MÁS, **CUANDO SE UTILICE EL INTERNET, O CUALQUIER OTRO MEDIO DE COMUNICACIÓN ELECTRÓNICA**, RADIAL O SATELITAL PARA CONTACTAR A LA VICTIMA.
- ARTICULO 365.- **SE EQUIPARA AL ROBO**, Y SE CASTIGARA COMO TAL:
- IV.- **EL APODERAMIENTO MATERIAL O MEDIANTE VÍA ELECTRÓNICA DE LOS DOCUMENTOS QUE CONTENGAN DATOS EN COMPUTADORAS**, O EL APROVECHAMIENTO O UTILIZACIÓN DE DICHOS DATOS, SIN DERECHO Y SIN CONSENTIMIENTO DE LA PERSONA QUE LEGALMENTE PUEDA DISPONER DE LOS MISMOS;

CÓDIGO PENAL DE NUEVO LEÓN

- ARTICULO 395.- **COMETE EL DELITO DE CHANTAJE** EL QUE, CON ANIMO DE CONSEGUIR UN LUCRO O PROVECHO, AMENAZARE A OTRO CON DAÑOS MORALES, FISICOS O PATRIMONIALES, QUE AFECTEN AL AMENAZADO O A PERSONA FISICA O MORAL CON QUIEN ESTE TUVIERA LIGAS DE CUALQUIER ORDEN, QUE LO DETERMINEN A PROTEGERLA.
- SE INCREMENTARÁ LA PENA EN UNA MITAD MÁS, CUANDO LA COMISIÓN DEL DELITO SE REALICE EN ALGUNA DE LAS SIGUIENTES MODALIDADES:
- VIII. **SE REALICE POR** VÍA TELEFÓNICA O **CUALQUIER MEDIO DE COMUNICACIÓN ELECTRÓNICA**, RADIAL O SATELITAL, PARA COMETER EL DELITO;

CÓDIGO PENAL DE NUEVO LEÓN

- ARTÍCULO 408 BIS.- **CUANDO PARA COMETER LOS DELITOS DE ROBO, FRAUDE, ABUSO DE CONFIANZA, USURA, CHANTAJE O ADMINISTRACIÓN FRAUDULENTA**, SE UTILICEN TARJETAS DE CRÉDITO O DÉBITO, **O CUALQUIER MEDIO O INSTRUMENTO ELECTRÓNICO O BANCARIO**, LA PENA SE AUMENTARÁ HASTA EN UNA TERCERA PARTE DE LA QUE CORRESPONDA IMPONER.

CÓDIGO PENAL DE NUEVO LEÓN

- TÍTULO VIGÉSIMO SEGUNDO **DE LOS DELITOS POR MEDIOS ELECTRÓNICOS**
- ARTÍCULO 427.- **A QUIEN INDEBIDAMENTE ACCESE A UN SISTEMA DE TRATAMIENTO O DE TRANSMISIÓN AUTOMATIZADO DE DATOS**, SE LE IMPONDRÁ DE 2 MESES A 2 AÑOS DE PRISIÓN Y MULTA DE 200 A 1000 CUOTAS.
- ARTÍCULO 428.- **A QUIEN INDEBIDAMENTE SUPRIMA O MODIFIQUE DATOS CONTENIDOS EN EL SISTEMA**, O **ALTERE EL FUNCIONAMIENTO DEL SISTEMA** DE TRATAMIENTO O DE TRANSMISIÓN AUTOMATIZADO DE DATOS, SE LE IMPONDRÁ DE 2 A 8 AÑOS DE PRISIÓN Y MULTA DE 300 A 1500 CUOTAS.
- ARTÍCULO 429.- **A QUIEN INDEBIDAMENTE AFECTE O FALSEE EL FUNCIONAMIENTO DE UN SISTEMA DE TRATAMIENTO** O DE TRANSMISIÓN AUTOMATIZADA DE DATOS, SE LES IMPONDRÁ DE 2 A 8 AÑOS DE PRISIÓN Y MULTA DE 350 A 2000 CUOTAS.

CÓDIGO PENAL DE BAJA CALIFORNIA

- TÍTULO TERCERO **DELITOS CONTRA LA INVIOLABILIDAD DEL SECRETO Y DE LOS SISTEMAS Y EQUIPOS DE CÓMPUTO Y PROTECCIÓN DE LOS DATOS PERSONA**LES CAPÍTULO PRIMERO
- ARTÍCULO 175.- Tipo y punibilidad.- **Al que sin consentimiento de quien tenga derecho a otorgarlo revele un secreto, de carácter científico, industrial o comercial, o lo obtenga a través de medios electrónicos o computacionales**, se le haya confiado, conoce o ha recibido con motivo de su empleo o profesión y obtenga provecho propio o ajeno se le impondrá prisión de uno a tres años y hasta cincuenta días multa, y en su caso, suspensión de dos meses a un año en el ejercicio de su profesión; si de la revelación del secreto resulta algún perjuicio para alguien, la pena aumentará hasta una mitad más. Al receptor que se beneficie con la revelación del secreto se le impondrá de uno a tres años de prisión y hasta cien días multa.
- REVELACION DEL SECRETO: Se entiende por revelación de secreto cualquier información propia de una fuente científica, industrial o comercial donde se generó, que sea transmitida a otra persona física o moral ajena a la fuente.

CÓDIGO PENAL DE BAJA CALIFORNIA

- CAPÍTULO SEGUNDO
- ARTÍCULO 175 BIS.- A quien sin autorización o indebidamente, modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y multa equivalente de cien a trescientos días.
- ARTÍCULO 175 TER.- A quien sin autorización o indebidamente, copie o accese a información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y multa equivalente de cincuenta a ciento cincuenta días de salario mínimo vigente.
- ARTÍCULO 175 QUATER.- Agravación de la pena.- Las penas previstas en los artículos anteriores se duplicarán cuando las conductas delictivas se ejecuten en contra de sistemas o equipos de informática del Estado o Municipios.

CÓDIGO PENAL DE BAJA CALIFORNIA

- CAPÍTULO SEGUNDO
- ARTÍCULO 175 QUINQUIES.- Tipo y punibilidad.- Al que por cualquier medio usurpe o suplante con fines ilícitos o de lucro, la identidad de otra persona, u otorgue su consentimiento para llevar a cabo la usurpación o suplantación en su identidad, se le impondrá pena de seis meses a seis años de prisión y de cuatrocientos a seiscientos días multa.
- Se aumentarán en una mitad las penas previstas en el párrafo anterior, a quien además se valga de la homonimia, parecido físico o similitud de la voz para cometer el delito así como en el supuesto de que el sujeto activo del delito tenga licenciatura, ingeniería o cualquier otro grado académico reconocido en el rubro de la informática, telemática o sus afines.

CÓDIGO PENAL DE BAJA CALIFORNIA

- CAPÍTULO SEGUNDO
- Serán equiparables al delito de usurpación o suplantación de identidad y se impondrán las penas establecidas por este artículo, cuando se actualicen las siguientes conductas:
- I.- Al que por algún uso del medio informático, telemático o electrónico alcance un lucro indebido o genere un daño patrimonial para sí o para otro valiéndose de alguna manipulación informática o intercepción de datos de envío, cuyo objeto sea el empleo no autorizado de datos personales o el acceso no autorizado a base de datos automatizados para suplantar identidades;
- II.- Al que transfiera, posea o utilice datos identificativos de otra persona con la intensión de cometer, intentar o favorecer cualquier actividad ilícita, y
- III.- Al que asuma, suplante o se apropie o utilice a través del internet, cualquier sistema informático, o medio de comunicación, la identidad de una persona física o jurídica que no le pertenezca.

CAPITULO III VIOLACION DE CORRESPONDENCIA

- ARTÍCULO 257.- Tipo y punibilidad.- Al que dolosamente abra o intercepte una comunicación escrita, electrónica, magnética, óptica o informática que no esté dirigida al inculpado, se le impondrá de veinte a cuarenta días multa.
- Exclusión de pena, por razón de la patria potestad, tutela o custodia.- No se impondrá pena a los que ejerciendo la patria potestad, la tutela o custodia, abran o intercepten las comunicaciones escritas a sus hijos menores de edad o a las personas que se hallen bajo su tutela o guarda.

CÓDIGO PENAL DE SONORA

- CAPÍTULO IX PORTACIÓN Y USO INDEBIDO DE DISPOSITIVOS DE COMUNICACIÓN ELECTRÓNICA
- ARTÍCULO 144 TER.- Se impondrá pena de 3 a 5 años de prisión y multa de cien a trescientas Unidades de Medida y Actualización al interno, reo, visitante o abogado que porte, posea o utilice un dispositivo portátil de comunicación electrónica en el interior de un centro de readaptación social.
- En el caso a que se refiere este artículo, además de las sanciones señaladas en el mismo, serán decomisados los dispositivos portátiles de comunicación electrónica.

CÓDIGO PENAL DE SONORA

- TITULO QUINTO DELITOS CONTRA EL DESARROLLO Y DIGNIDAD DE LAS PERSONAS CAPÍTULO I EXPOSICIÓN PÚBLICA DE PORNOGRAFÍA, EXHIBICIONES OBSCENAS Y SEXTING
- ARTÍCULO 167 BIS.- A quien reciba u obtenga de una persona, imágenes, textos o grabaciones de voz o audiovisuales de contenido erótico, sexual o pornográfico y las revele o difunda sin su consentimiento y en perjuicio de su intimidad, a través de mensajes por teléfono, publicaciones en redes sociales, correo electrónico o cualquier otro medio, se le impondrá de uno a cinco años de prisión y de ciento cincuenta a trescientas Unidades de Medida y Actualización.

CÓDIGO PENAL DE SONORA

- Artículo 241 Bis 1.- Cometerá también el delito de Usurpación de Personalidad o identidad y se impondrá una pena de dos a seis años de prisión y multa de cuatrocientos a seiscientas Unidades de Medida y Actualización, el que con el objeto de suplantar a otro con fines ilícitos, se acredite con la personalidad de éste, alterando, reproduciendo, falsificando, utilizando o proporcionando, ante terceros, cuando menos alguna de la siguiente información o documentos personales del suplantado:
- VI.- Números de Tarjeta de Crédito, números confidenciales y/o claves de acceso a servicios de banca por Internet, telefónicos o cualquier otro dato o elemento que permita el acceso a los servicios bancarios del afectado;
- XXVI.- Firma Electrónica; o
- XXVII.- Cualquier otra información o documento que identifique física o electrónicamente a un individuo; o permita el acceso a sus bienes o patrimonio o responsabilidades.

CÓDIGO PENAL DE CHIHUAHUA

- CAPÍTULO IV DEL USO Y ACCESO ILÍCITO A LOS SISTEMAS Y EQUIPOS INFORMÁTICOS Y DE COMUNICACIÓN
- Artículo 327 Bis. A quien sin la debida autorización o excediendo la que tenga y con ánimo de lucro, en beneficio propio o de un tercero, acceda, copie, modifique, destruya, deteriore, intercepte, interfiera, o use, información contenida en equipos informáticos o de comunicación, se le impondrán de seis meses a tres años de prisión y de cien a cuatrocientos días multa.
- Artículo 327 Ter. Al que diseñe, programe, fabrique, introduzca, importe, comercialice o distribuya programas de cómputo, aparatos, sistema, códigos de acceso, o cualquier dispositivo físico, que tengan por objeto violar uno o más mecanismos de seguridad de equipos informáticos, de comunicación, de programas de cómputo, en beneficio propio o de un tercero, se le impondrán de seis meses a cuatro años de prisión y de doscientos a quinientos días multa.

CÓDIGO PENAL DE CHIHUAHUA

- CAPÍTULO IV DEL USO Y ACCESO ILÍCITO A LOS SISTEMAS Y EQUIPOS INFORMÁTICOS Y DE COMUNICACIÓN
- Artículo 327 Quater. Al que valiéndose de equipos informáticos o de comunicación, utilice indebidamente, datos o información personal de otro para ostentarse como tal sin consentimiento de éste, ya sea en beneficio propio o de un tercero, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.
- Artículo 327 Quinquies. Las penas previstas en este Capítulo se incrementarán en una mitad cuando las conductas sean cometidas en contra de una entidad pública estatal o municipal.

CÓDIGO PENAL DE QUERÉTARO

- TÍTULO SÉPTIMO DELITOS CONTRA LA INVIOLABILIDAD DEL SECRETO Y EL ACCESO ILÍCITO A SISTEMAS DE INFORMÁTICA
- CAPÍTULO I REVELACIÓN DE SECRETO
- ARTÍCULO 159 BIS. El que para descubrir los secretos o vulnerar la intimidad de otro, sin el consentimiento de éste, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen o de cualquier otra señal de comunicación, se le impondrán de seis meses a tres años de prisión y de cien a trescientos días multa.

CÓDIGO PENAL DE QUERÉTARO

- TÍTULO SÉPTIMO DELITOS CONTRA LA INVIOLABILIDAD DEL SECRETO Y EL ACCESO ILÍCITO A SISTEMAS DE INFORMÁTICA
- CAPÍTULO II ACCESO ILÍCITO A SISTEMAS DE INFORMÁTICA
- ARTÍCULO 159 TER. Al que sin autorización, por cualquier medio ingrese a sistemas informáticos, destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos protegidos o no por algún sistema de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.
- Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos o no por algún sistema de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa. Las penas señaladas en el párrafo anterior se aplicarán a aquellos que teniendo autorización para ingresar al sistema informático, hagan uso indebido de la información, para sí o para otro.

CÓDIGO PENAL DE QUERÉTARO

- TÍTULO SÉPTIMO DELITOS CONTRA LA INVIOLABILIDAD DEL SECRETO Y EL ACCESO ILÍCITO A SISTEMAS DE INFORMÁTICA
- CAPÍTULO II ACCESO ILÍCITO A SISTEMAS DE INFORMÁTICA
- ARTÍCULO 159 QUATER. Al que sin autorización, por cualquier medio ingrese a sistemas informáticos, destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos del Estado, protegidos o no por algún sistema de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.
- Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos o no por algún medio de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

CÓDIGO PENAL DE QUERÉTARO

- TÍTULO SÉPTIMO DELITOS CONTRA LA INVIOLABILIDAD DEL SECRETO Y EL ACCESO ILÍCITO A SISTEMAS DE INFORMÁTICA
- CAPÍTULO II ACCESO ILÍCITO A SISTEMAS DE INFORMÁTICA
- A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido o no por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a setecientos cincuenta días multa. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en cualquier empleo, puesto, cargo o comisión de carácter público.

- **Artículo 403.-** El delito de fraude se sancionará: …
- **Artículo 404.-** Las mismas sanciones señaladas en el artículo anterior, se impondrán:
- **XIX.-** Al que dolosamente y con el propósito de procurarse un lucro ilícito, para sí o para un tercero, dañe o perjudique el patrimonio de otro, mediante el uso indebido de mecanismos cibernéticos, que provoque o mantenga un error, sea manipulando datos de entrada a un equipo de informática con el fin de producir o lograr movimientos falsos en transacciones de una persona física o moral, sea presentando como ciertos hechos que no lo son, o deformando o disimulando hechos verdaderos; y

CÓDIGO PENAL DE PUEBLA

- **CAPÍTULO VIGÉSIMO QUINTO DELITOS INFORMÁTICOS**
- **ARTICULO 475.** Se impondrá prisión de uno a cinco años, multa de cincuenta a quinientos días de salario 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.

- **CAPÍTULO VIGÉSIMO QUINTO DELITOS INFORMÁTICOS**
- **ARTICULO 476.** Al que sin autorización modifique, destruya o provoque perdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días de multa.
- Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

CÓDIGO PENAL DE PUEBLA

- **CAPÍTULO VIGÉSIMO QUINTO DELITOS INFORMÁTICOS**
- **ARTICULO 477.** Al que sin autorización modifique, destruya o provoque perdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a dos años de prisión y de doscientos a seiscientos días multa.

CÓDIGO PENAL DE PUEBLA

- **CAPÍTULO VIGÉSIMO QUINTO DELITOS INFORMÁTICOS**
- **ARTICULO 478**. Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque perdida de información que contengan, se le impondrán de dos a cuatro años de prisión y de trescientos a novecientos días multa.
- Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a dos años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

CÓDIGO PENAL DE PUEBLA

- **CAPÍTULO VIGÉSIMO QUINTO DELITOS INFORMÁTICOS**
- **ARTICULO 478**. (continuación…) A quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de dos a cinco años de prisión y multa de quinientos a mil días de salario mínimo general vigente. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública.

CÓDIGO PENAL DE SINALOA

- CAPÍTULO III SUPLANTACIÓN DE IDENTIDAD.
- ARTÍCULO 177 BIS. A quien por cualquier medio suplante la identidad de otra persona, con fines ilícitos o de lucro para sí o para otra, u otorgue su consentimiento para llevarla a cabo, se le impondrá prisión de seis meses a tres años y de cuatrocientos a seiscientos días multa.
- ARTÍCULO 177 BIS A. Será equiparable al delito de suplantación de identidad y se impondrán las mismas penas previstas en el artículo anterior:
- I. Al que por algún uso de medio informático, telemático o electrónico, obtenga algún lucro indebido para sí o para otro o, genere un daño patrimonial, mediante el empleo no autorizado de datos personales o el acceso no autorizado a bases de datos automatizadas para suplantar identidades;
- III. Al que asuma, se apropie o utilice indebidamente a través de internet, cualquier sistema informático, o medio de comunicación, la identidad de una persona física o jurídica que no le pertenezca para ostentarse como tal sin consentimiento de éste, ya sea en beneficio propio o de un tercero.

CÓDIGO PENAL DE SINALOA

- CAPÍTULO V DELITO INFORMÁTICO
- ARTÍCULO 217. Comete delito informático, la persona que dolosamente y sin derecho:
- I. Use o entre a una base de datos, sistema de computadores o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información; o
- II. Intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red. Al responsable de delito informático se le impondrá una pena de seis meses a dos años de prisión y de noventa a trescientos días multa.

CÓDIGO PENAL COAHUILA

- Artículo 401 (Conductas punibles relacionadas con la falsificación de documentos crediticios privados y acceso no autorizado a equipos emisores) Se impondrá de cuatro a seis años de prisión y de quinientos a cinco mil días multa a quien:
- III. (Alteración o manipulación de medios de identificación electrónica) Altere o manipule un mecanismo o sistema de identificación electrónico, magnético, electromagnético, computacional o telemático, de tarjetas de crédito o de débito, de títulos, vales u otros documentos utilizados para el pago de bienes y servicios o para disposición de efectivo, de tal modo que arroje uno o más resultados falsos.

CÓDIGO PENAL COAHUILA

- Artículo 401 (Conductas punibles relacionadas con la falsificación de documentos crediticios privados y acceso no autorizado a equipos emisores) Se impondrá de cuatro a seis años de prisión y de quinientos a cinco mil días multa a quien:
- V. (Acceso no autorizado a equipos electromagnéticos o electrónicos de instituciones emisoras) Sin consentimiento de quien esté facultado para ello, acceda al equipo electrónico, magnético, electromagnético, computacional o telemático de alguna institución emisora de tarjetas de crédito o de débito, de títulos, vales u otros documentos utilizados para el pago de bienes y servicios o para disposición de efectivo, y obtenga o use la información confidencial o reservada de los mismos para lograr un beneficio para sí o para otro, o perjudicar a la institución emisora, al titular de aquellos documentos o a otra persona.

CÓDIGO PENAL COAHUILA

- Artículo 273 (Delitos contra la información privada en medios informáticos)
- Los delitos contra la información privada en medios informáticos serán los siguientes:
- I. (Acceso y transmisión o divulgación ilícitas de información contenida en un sistema informático) Se impondrá de seis meses a tres años de prisión y de doscientos a quinientos días multa, o de seis meses a tres años de libertad supervisada y de quinientos a mil días multa, a quien sin consentimiento de quien tenga derecho de disponer de datos o información privados contenidos en un sistema informático, acceda al sistema y transmita a una o más personas o divulgue los referidos datos o información, perjudicando a quien tenga derecho a disponer de ellos o a otra persona.
- II. (Afectación de datos o información contenidos en un sistema informático) Se impondrá de cuatro meses a cuatro años de prisión y de setecientos cincuenta a mil quinientos días multa, a quien sin consentimiento de quien tenga derecho de disponer de datos o información privada contenidos en un sistema informático, a propósito, altere, dañe, borre, destruya o de cualquier otra manera provoque a propósito la pérdida de datos o información contenidos en el sistema. Si en los supuestos del párrafo precedente hubiera algún resguardo o copia de los datos o información afectados, solo se impondrá al autor de cuatro meses a un año de libertad supervisada y de quinientos a mil días multa.

CÓDIGO PENAL DEL ESTADO DE MÉXICO

- Artículo 168.- El delito de falsificación de documentos se comete por alguno de los medios siguientes:
- II. Aprovechando indebidamente una firma o rúbrica en blanco ajena, la firma electrónica avanzada o el sello electrónico en su caso, extendiendo una obligación o liberación o cualquier otro documento que pueda comprometer los bienes, la honra, la persona o la reputación de otra, o causar un perjuicio a la sociedad, al Estado, al municipio o a un tercero.
- III. Alterando el contexto de un documento físico o electrónico verdadero, después de concluido y firmado o sellado, si esto cambiare su sentido sobre alguna circunstancia o punto substancial, ya sea que se haga añadiendo, enmendando o borrando, en todo o en parte, una o más palabras, cifras o cláusulas o variando la puntuación.
- V. Atribuyéndose el que extienda el documento físico o electrónico o a la persona en cuyo nombre lo hace, un nombre o una investidura, calidad o circunstancia que no tenga y que sea necesaria para la validez del acto.

GRACIAS

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

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.