PONCEKURI

LAW FIRM

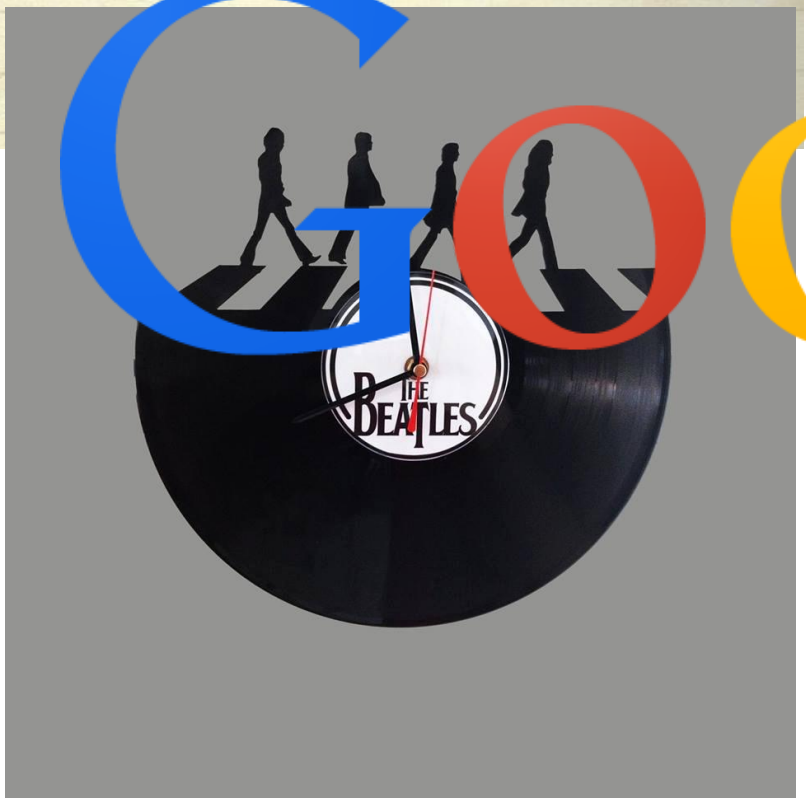
Seguridad de la información

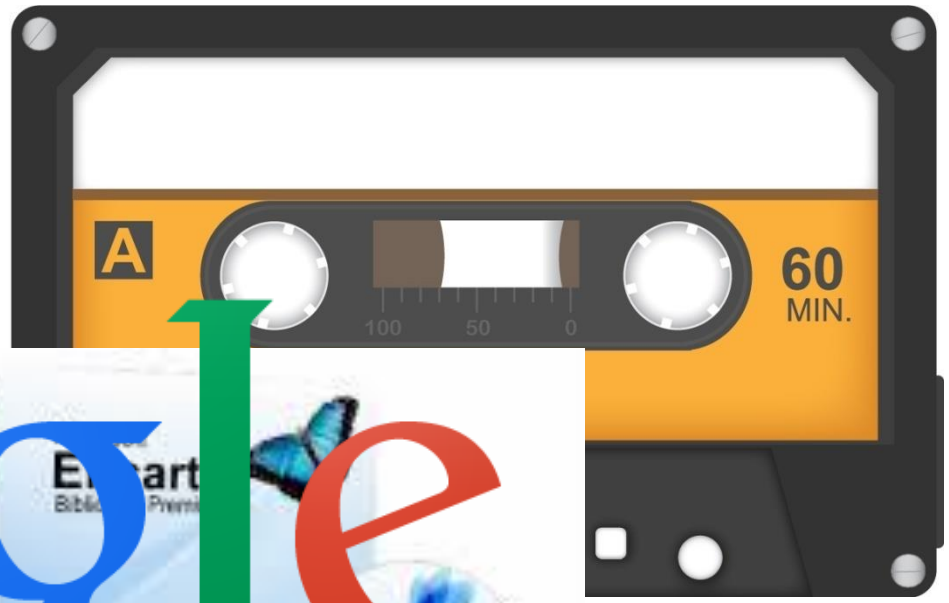
Nuhad Ponce Kuri
nponce@poncekuri.com
@nuhadsita13

Oscar Andrés Castillo Caamal
ocastillo@poncekuri.com
@oscar_castillo4

Antecedentes

Para recordar…





Google

PONCEKURI
LAW FIRM

Algunas Noticias

sabado 09, junio 2012 b:Secure

INICIO INTERNET OPINIÓN REPORTES SEGURIDAD

30 March, 2012

Visa y MasterCard alertan por brecha de seguri

Por Sergio

Email | ¿De

11 June, 2012

LinkedIn desactivará contraseñas comprometidas

Por Sergio López

Email | ¿Desea imprimir? Regístrese ahora

La red social para profesionales,

esactivará

ñas

taque

r hackers

és de su

Hackers roban 75 mdd a cuentahabientes

Delincuentes cibernéticos lograron ingresar a perfiles de millonarios en el mundo, advierte McAfee; los principales países afectados fueron Italia, Alemania, Holanda, Estados Unidos y Colombia.

Publicado: Martes, 26 de junio de 2012 a las 14:23

Por: Francisco Rubio

CIUDAD DE MÉXICO (CNNExpansión) — Una operación delictiva realizada por delinci

robado cuando menos 75 mi

cuentahabientes de cinco pa

empresa especializada en se

El 51% de las organizaciones sufre la pérdida de móviles

Un estudio de Unisys confirma que las empresas no han tomado hasta el momento las debidas medidas de **seguridad** en la adopción de los **dispositivos móviles** para el ámbito profesional. En concreto, un 51% de las **empresas** encuestadas ha experimentado pérdida de datos corporativos durante los últimos 12 meses a partir del uso inseguro de **dispositivos móviles**.

La movilidad es una tendencia cada vez más consolidada y los datos apuntan a que seguirá siéndolo en

móviles que personas y en 2020 habrá más de 50.000 millo

trata de datos que ilustran el crecimiento imparable de la m

IN

De

cr

El

el

28 June, 2012

Hackers roban y publican información sensible de empleados de AT&T

Por Ángel Álvarez

Email | ¿Desea imprimir? Regístrese ahora

Follow @bsecuremagazine 3,846 followers

El grupo hackers The WikiBoat robó y publicó en línea información de los empleados del servicio de cuentas de la compañía telefónica AT&T.

Los hacktivistas obtuvieron los nombres de los empleados, edad, salario, correos electrónicos y contraseñas, datos que posteriormente publicaron en Pastebin.

"Hola a todos. En este basurero de

ICANN publica por error información personal sobre los solicitantes de dominios

Christel Borgna hace 3 horas +1 1 Me gusta Twittear 188 0

sabado 09, junio 2012 b:Secure

INICIO INTERNET OPINIÓN REPORTES SEGURIDAD

23 April, 2012

Emplea

los man

y

las

a

es

SecurID 800 de RSA comprometidos, hackeados en 15 minutos

26/06/2012 | Jesús Maturana | 0 comentarios Twittear 23 +1 1

ESET descubre primer caso de ciberespionaje por malware en América Latina

Lunes 25 junio 2012 | 8:16

Tv Azteca rompe con IBOPE por supuesta fuga de información

Azteca anunció que dejará a un lado las

ediciones de IBOPE debido a la desconfianza

ue le genera la supuesta filtración de datos

ue sufrió la empresa encargada de este tipo

sondeos.

televisora del Ajusco acusó a IBOPE de

ber sido víctima de una filtración de

formación en la que se publicaron los datos

3,400 telehogares que participan en el

a, Los telehogares son las casas en las que

conocer cuáles son los programas más

PONCEKURI LAW FIRM

¿Por qué una ley de protección de datos?

By @juan_carrillo

Estructura de la legislación

Ley Federal de Protección de Datos Personales en Posesión de los Particulares (Ley)

Reglamento de la LFPDPPP (Reglamento)

Lineamientos del aviso de privacidad (lineamientos)

Recomendaciones de Seguridad (recomendaciones)

Recomendaciones para la designación de la persona o Departamento de Datos Personales

Guía para implementar un SGSDP

Parámetros de autorregulación en materia de protección de datos personales

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados

PONCEKURI
LAW FIRM

- *Artículo 16...*

  *Toda **persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción** a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.*

- *Artículo 73. El Congreso tiene facultad:*

  *XXIX-O. **Para legislar en materia de protección de datos personales en posesión de particulares**.*

PONCEKURI
LAW FIRM

GENERALIDADES

- Principios de protección de datos: licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad.

- Derechos de los titulares de los datos de: acceso, rectificación, cancelación y oposición (derechos ARCO) y mecanismo para ejercerlos.

- Implicación en caso de la negativa de particulares, solicitud ante el Instituto Nacional de Acceso a la Información Pública y Protección de Datos Personales (INAI).

PONCEKURI
LAW FIRM

- La Ley tiene por objeto:

  La protección de los datos personales en posesión de los particulares, con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas.

PONCEKURI
LAW FIRM

El tratamiento de datos debe ser legítimo, controlado e informado.

Ley define tratamiento: Obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio.

Uso: Cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos.

PONCEKURI
LAW FIRM

- Art. 3.- Distinción en la Ley:
  - *Datos personales:* Cualquier información concerniente a una persona física identificada o identificable.

  - *Datos personales sensibles:* Aquellos datos personales **que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste.** En particular, se consideran sensibles aquellos que puedan **revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual**.

PONCEKURI
LAW FIRM

- Artículo 2.- Además de las definiciones del Art. 3 de la Ley, se entenderá por:

  - Persona física identificable: Toda persona física cuya identidad pueda determinarse directa o indirectamente mediante cualquier información.

PONCEKURI
LAW FIRM

- Art.- 7 Los datos obtenidos, únicamente podrán ser utilizados para los fines para los cuales se haya dicho que fueron recabados, previa autorización en los términos de la Ley.

PONCEKURI
LAW FIRM

Creando un plan para atender la Ley

Fase 1. Adquisición de contexto

Fase 2. Ciclo de vida de datos personales

Fase 3. Clasificación de datos personales

Fase 4. Análisis de riesgos de datos personales

Fase 5. Análisis legal

Fase 6. Análisis organizacional

Fase 7. Análisis de cumplimiento

Fase 8. Plan estratégico

PONCEKURI
LAW FIRM

PRINCIPIOS

- **Licitud:** No engaños o fraude
- **Consentimiento:** (Art. 8) Expreso o tácito
- **Información:** Datos correctos y actualizados
- **Calidad:** Datos pertinentes. Cuando ya no sean necesarios cancelar.
- **Finalidad:** Cumplimiento de fines señalados en aviso de privacidad.

PONCEKURI
LAW FIRM

- **Lealtad:** fin distinto, nuevo consentimiento.

- **Proporcionalidad:** Tratamiento necesario, adecuado y relevante en relación con las finalidades.

- **Responsabilidad:** Cumplimiento de los principios de protección. Medidas de seguridad para su aplicación.

PONCEKURI
LAW FIRM

Consentimiento

Todo tratamiento de datos personales requiere consentimiento de su titular, salvo las excepciones.

El consentimiento **será expreso cuando la voluntad se manifieste verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos.**

El consentimiento será **tácito cuando habiéndose puesto a disposición del titular el aviso de privacidad, no manifieste su oposición**.

PONCEKURI
LAW FIRM

- Excepciones al consentimiento:
  - Esté previsto en una Ley;
  - Los datos figuren en fuentes de acceso público;
  - Los datos personales se sometan a un procedimiento previo de disociación;
  - Tenga el propósito de cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable

PONCEKURI
LAW FIRM

- Excepciones al consentimiento:
  - Exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;
  - Sean indispensables para la atención médica, la prevención, diagnóstico, tratamientos médicos, mientras el titular no esté en condiciones de otorgar el consentimiento
  - Se dicte resolución de autoridad competente.

Derechos ARCO

- ¿Qué son los derechos ARCO?

- **Acceso:** Acceder a sus datos personales, así como al Aviso de Privacidad.
- **Rectificación:** Derecho de rectificar los datos cuando sean inexactos o incompletos.
- **Cancelación:** Derecho para la supresión del dato tras un periodo de bloqueo.
- **Oposición:** Derecho de oponerse por causa legitima al tratamiento de sus datos.

PONCEKURI
LAW FIRM

¿De que forma se ejercen los derechos ARCO?

El titular de los datos personales o su representante legal podrán solicitar al responsable en cualquier momento el ejercicio de sus derechos ARCO a través de una solicitud que deberá contener lo siguiente:

1. Nombre del titular y domicilio u otro medio para comunicar la respuesta.
2. Documentos que acrediten su personalidad.
3. Descripción clara y precisa de los datos respecto de los que se busca ejercer alguno de los derechos ARCO.
4. Cualquier otro elemento o documento que facilite la localización de los datos personales

PONCEKURI
LAW FIRM

Obligaciones del responsable

¿Qué obligaciones tengo como responsable del tratamiento de datos personales?

- Obtener el consentimiento del titular de los datos, salvo cuando aplique alguna excepción.
- Proporcionar información sobre el tratamiento al titular de los datos a través del Aviso de Privacidad.
- Guardar confidencialidad respecto a los datos personales
- Adoptar y mantener medidas de organización y seguridad respecto de los datos evitando su modificación, pérdida y tratamiento o acceso no autorizado.
- Establecer procedimientos para que el titular de los datos pueda ejercer sus derechos.

PONCEKURI
LAW FIRM

Aviso de privacidad

AVISO DE PRIVACIDAD

¿Qué es?

Documento físico, electrónico o en cualquier otro formato generado por el responsable, y puesto a disposición del titular previo al tratamiento de sus datos personales a través de medios físicos, digitales, visuales, sonoros o de cualquier otra tecnología.

PONCEKURI
LAW FIRM

Contenido mínimo (artículo 16):

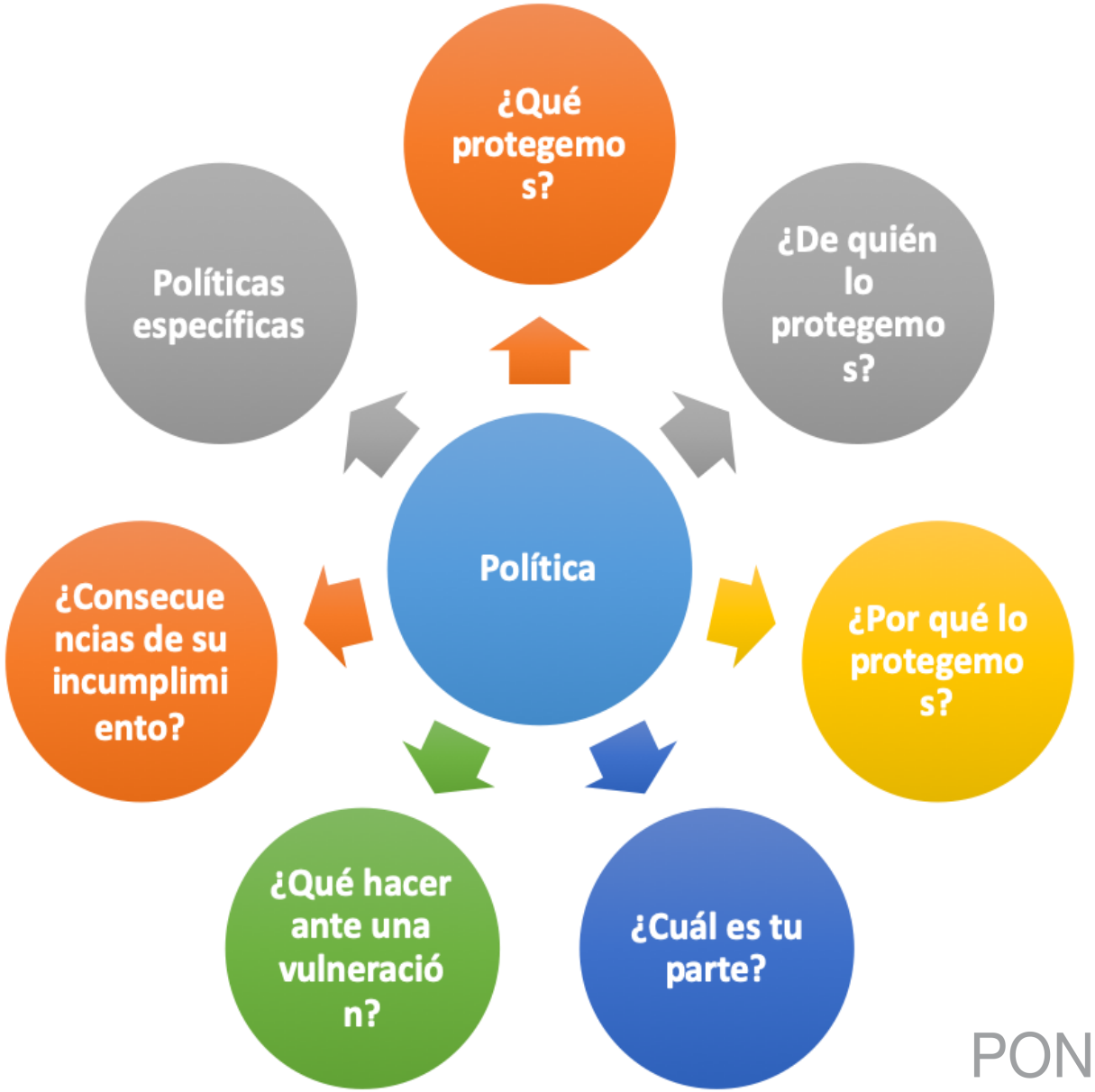
1. Identidad y domicilio del responsable.
2. Finalidades del tratamiento de datos.
3. Opciones y medios para limitar el uso o divulgación de los datos.
4. Medios para ejercer los derechos ARCO.
5. Las transferencias de datos que se efectúen.
6. Procedimiento por el que el responsable comunicara a los titulares de cambios al aviso de privacidad.

Políticas

Política

Protegemos la integridad, confidencialidad y disponibilidad de la información que manejamos y los activos relacionados.

Firma del Director

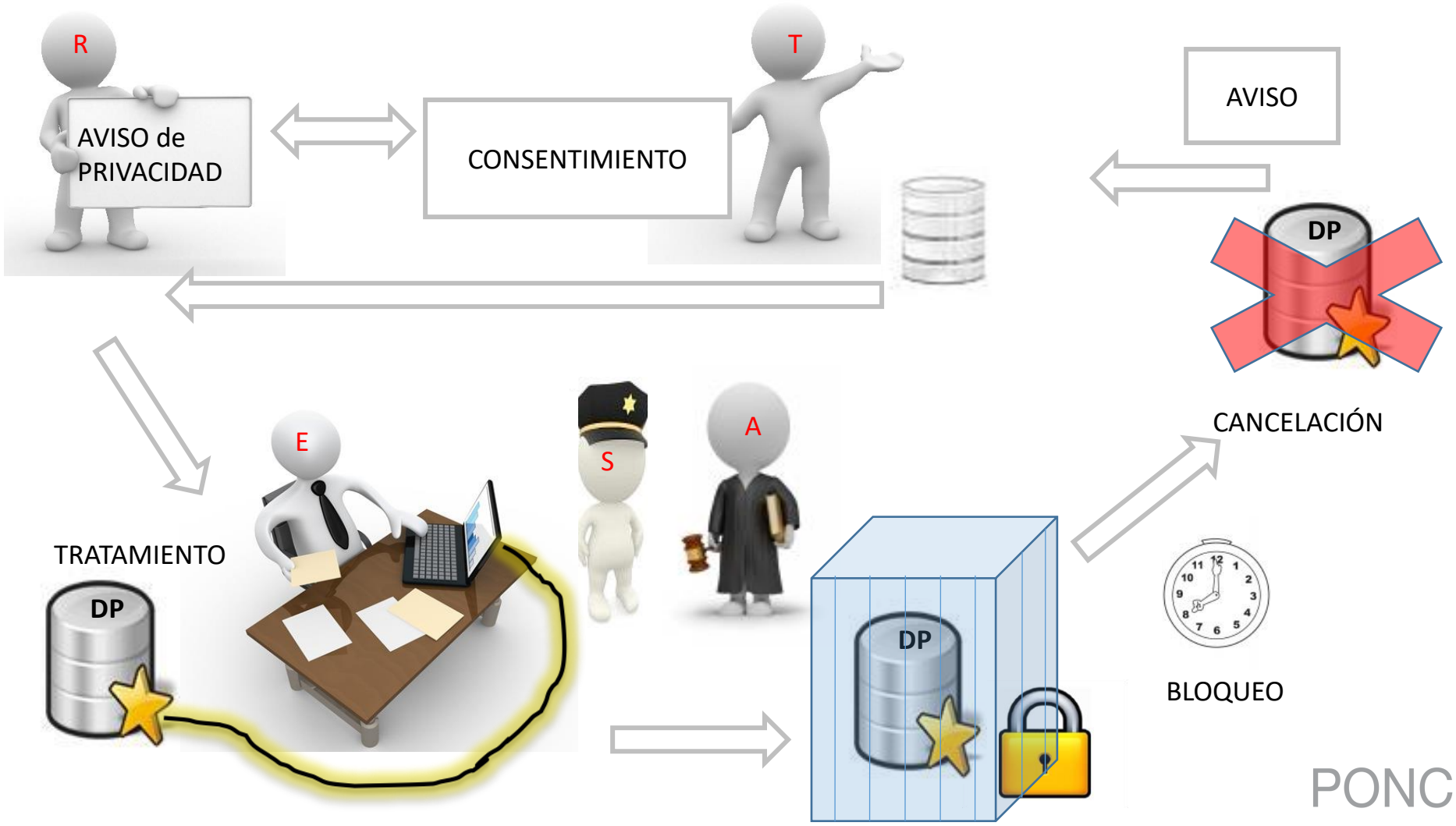


PONCEKURI
LAW FIRM

- **Comité de Privacidad:**

  - Nombrar a la persona(s) encargada(s) de:
    - El manejo de las bases de datos
    - Dar atención a solicitudes de ejercicio de derechos ARCO
    - Atender visitas IFAI
    - Conocer los avisos de privacidad y las políticas de la empresa
    - Firmar convenio confidencialidad

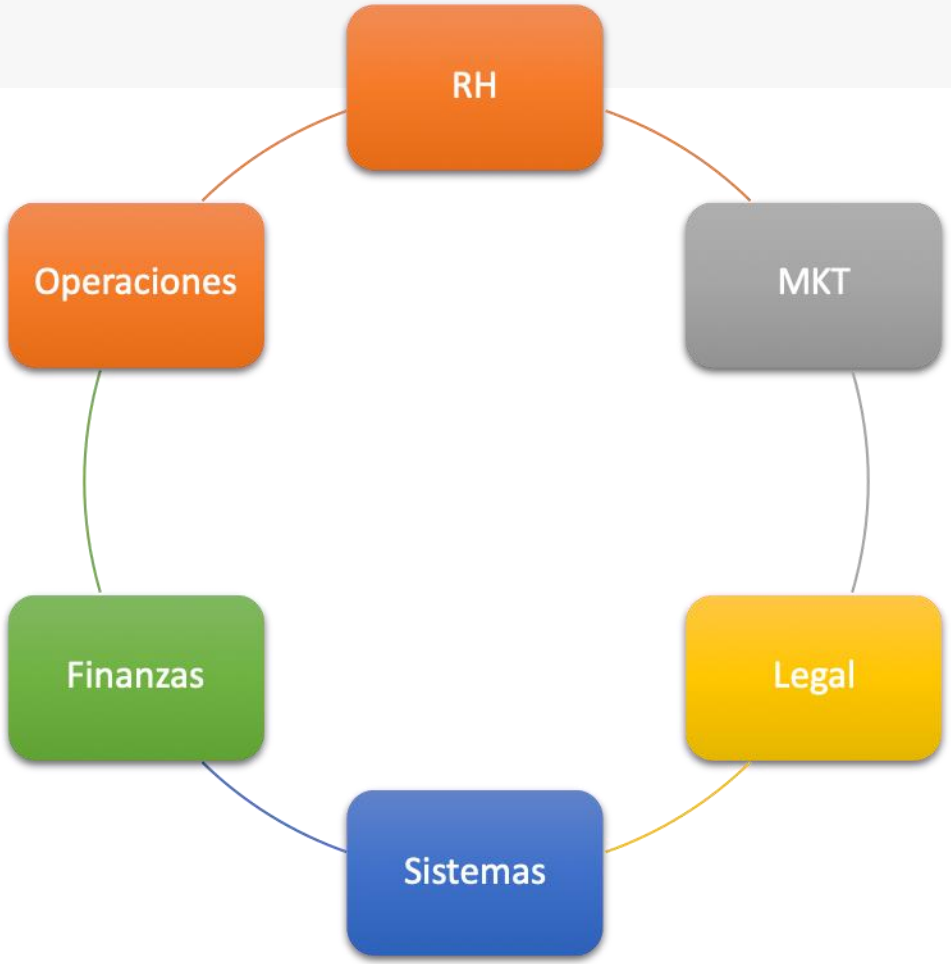
  - Saber que hacer en caso de:
    - Recibir solicitud de algún titular
    - Recibir oficio de alguna autoridad
    - Consultas



PONCEKURI
LAW FIRM


Aviso de privacidad
Procedimientos para atención de derechos ARCO
Designación de responsable o departamento al interior
Políticas de Seguridad y protección de datos
Convenios de confidencialidad y contratos
Acciones y procedimientos en caso de vulneración
Capacitar al personal involucrado
Inventario de Datos personales y sistemas de tratamiento
Identificación de personas que tratan los datos, privilegios, roles y responsabilidades
Análisis de riesgos
Datos
Finalidades
Tratamientos
Consentimiento
Privilegios de Acceso y transferencias
Identificar
¿Para qué?
¿Qué voy a hacer con ellos?
Evidencia
Internos
Externos
Medidas de seguridad Administrativas
Medidas de seguridad Físicas
Medidas de seguridad Técnicas

¿A quién debo involucrar en mi organización?



"involucrar a todas las áreas que manejen los datos"

PONCEKURI
LAW FIRM

Robo de identidad

Robo de identidad en México

El robo de identidad es la recopilación de datos personales relativa a la identidad de una persona con la finalidad de realizar un fraude

Algunos datos:

- Delito con mayor crecimiento en México.
- Ocupamos el octavo lugar a nivel mundial (Banco de México).
- Diario se envían 18 millones de correos falsos (Buró de Crédito).
- En México hay 80.6 millones de usuarios en internet (INEGI).

PONCEKURI
LAW FIRM

PONCEKURI
LAW FIRM

¿Cómo evitar el robo de identidad?

- Evitar llevar documentos que contengan datos personales como nombre, CURP, dirección, firma, huella digital (INE).
- Solicitar el envío de estados de cuenta a través de correos electrónicos ya que de forma física pueden ser robados con mayor facilidad.
- Evitar conectarse con dispositivos electrónicos a una red WiFi gratuita ya que pueden haber softwares robando tu información.
- Cambiar de forma constante contraseñas y no usar la misma para todas las plataformas.

PONCEKURI
LAW FIRM

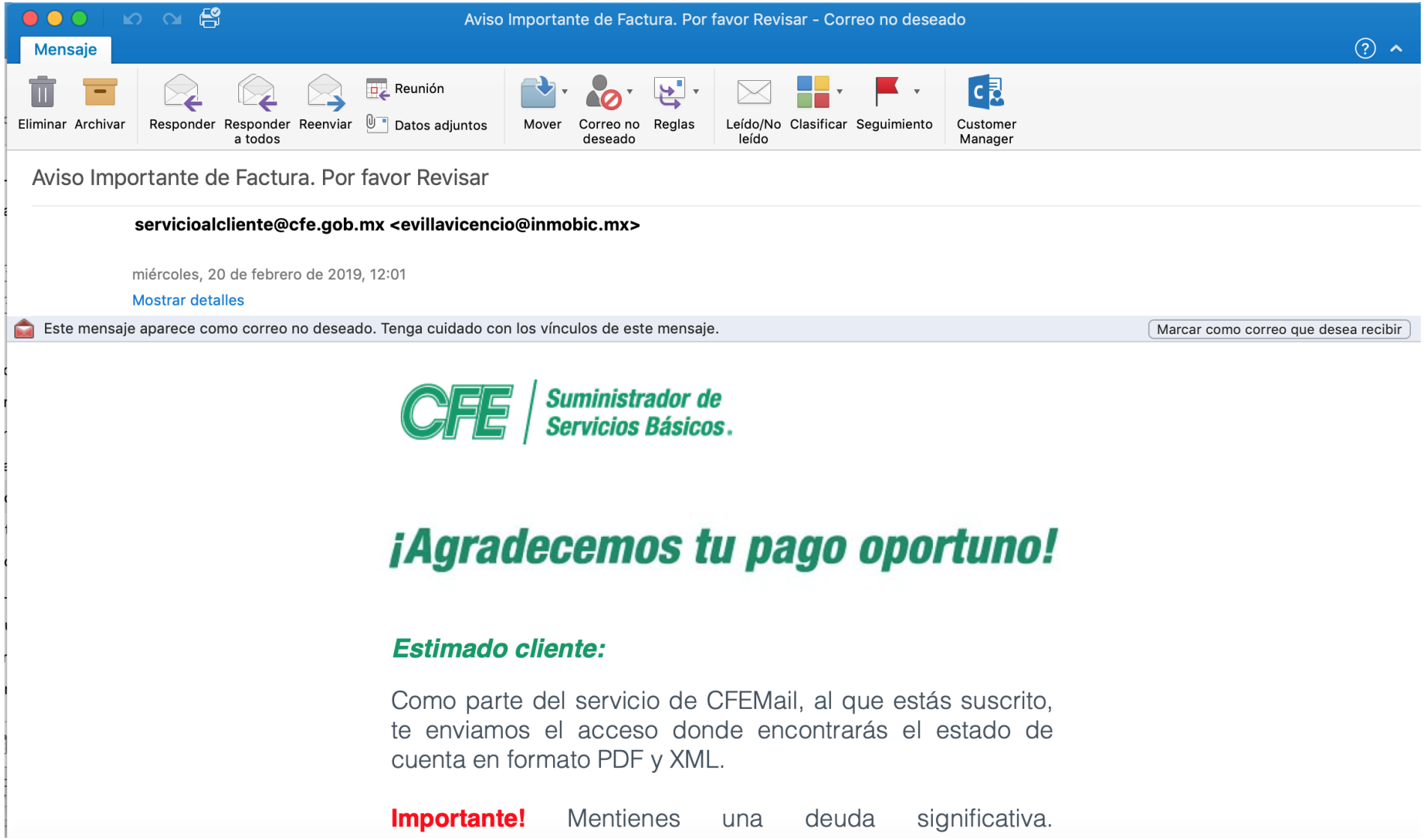
Amenazas contra la seguridad de la información

Phishing

Es phishing es un tipo de fraude en donde el atacante envía una comunicación (correo electrónico, redes sociales, SMS, etc.) con la finalidad de que la víctima haga clic en un enlace, descargue un archivo adjunto o envíe información solicitada.

El ataque tiene 3 componentes:

1. Se realiza mediante comunicaciones electrónicas.
2. El atacante se hace pasar por una persona/organización de confianza.
3. El objetivo es obtener información personal confidencial.



PONCEKURI
LAW FIRM

CFE | Suministrador de Servicios Básicos.

¡Agradecemos tu pago oportuno!

Estimado cliente:

Como parte del servicio de CFEMail, al que estás suscrito, te enviamos el acceso donde encontrarás el estado de cuenta en formato PDF y XML.

Importante! Mentienes una deuda significativa. Recomendamos revisar el documento a la brevedad para evitar sanciones en tu contra.

Archivo PDF	Archivo XML

PONCEKURI
LAW FIRM

Estimado cliente:

Como parte del servicio de CFEMail, al que estás suscrito, te enviamos el acceso donde encontrarás el estado de cuenta en formato PDF y XML.

Importante! Mentienes una deuda significativa. Recomendamos revisar el documento a la brevedad para evitar sanciones en tu contra.

Archivo PDF	Archivo XML
Ver	Ver

Te invi https://www.cazaoportunidades.com.mx/images/2/CFE_Factura.zip?rpu=972020100593&serie=MA&folio=0000995 98389&hash=62bc06f7204e9959b63d767af9d ***os medios de pago***

PONCEKURI
LAW FIRM

Ransomware

Hace referencia a un software de extorsión el cual tienen la finalidad de impedir el uso de un dispositivo o de ciertos archivos dentro de un dispositivo hasta que se haya pagado un rescate.

Usualmente, una infección con ransomware ocurre a partir de que el virus se introduce al dispositivo y posteriormente cifra por completo el sistema operativo o solo algunos de los archivos. Finalmente se le exige el pago a la víctima para poder obtener la llave de acceso a sus propios archivos.

WANNACRY

12 de mayo de 2017, ordenadores en toda Europa ven afectados sus sistemas, encriptados sus archivos y bloqueados los accesos de administrador a sus usuarios.

Cunde el pánico.

Miles de empresas quedan paralizadas en cuestión de minutos debido a un ransomware distribuido en la red llamado WannaCryptor (conocido como WannaCry). El que,probablemente, por alcance a sistemas afectados y perdidas económicas, ha sido el virus más destructor de la época actual. El malware se coló por una vulnerabilidad de un parche de seguridad instaurado semanas antes que infectó a más de 360.000 equipos. Se calcula que el impacto en pérdidas directas e indirectas alcanzó la suma de 4.000 millones de euros.

WannaCry ha supuesto un antes y un después en el mundo de la seguridad cibernética.

¿Qué puede pasar si roban mis datos?

Robo físico

PONCE KURI
LAW FIRM

Robo digital

US largest card incident hacker has track record says Miami Herald

21 August 2009

As the fall-out in the Albert Gonzalez credit card hacking case - in which the card hacker was charged earlier this week with gaining unauthorized access to 130 million people's card details from major ...erchants - continues. the Miami Herald

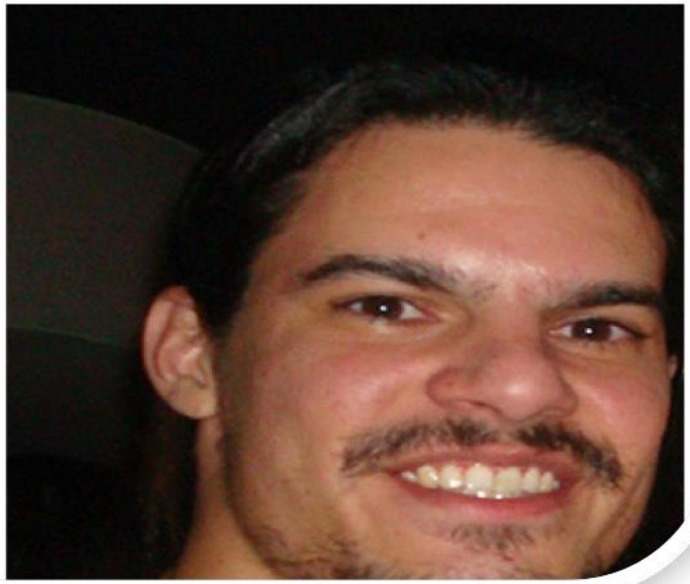
...l posts tagged 'Albert Gonzalez'

In Surprise Appeal, TJX Hacker Claims U.S. Authorized His Crimes

By Kim Zetter ✉ April 7, 2011 | 4:07 pm | Categories: Breaches, Hacks and Cracks, The Courts

Albert Gonzalez, the hacker who masterminded the largest credit card heists in U.S. history, is asking a federal judge to throw out his earlier guilty pleas and lift his record-breaking 20-year prison sentence, on allegations that the government authorized his years-long crime spree.

Gonzalez, 29, admitted last year that he and accomplices hacked into TJX, Office Max, Dave & Busters, Heartland Payment Systems and other companies to steal more than 130 million credit and debit card numbers, in what the government deemed the biggest computer crime case ever prosecuted in the United States. He's currently serving time at the Milan low-security federal prison in southeastern Michigan, with a release date in the year 2025.



PONCEKURI
LAW FIRM

La mejor herramienta

PONCEKURI
LAW FIRM

Acciones para la seguridad

Datos	Sensibilidad	Sistemas	Roles
Nombre	Dato personal	Sistema de RH	RH Director del Área
Teléfono	Dato personal	Sistema de Nominas	Finanzas
Numero de empleado	Dato personal	Sistemas de Nominas	Finanzas RH
Salario	Dato personal sensible	Expediente físico	RH Archivo

PONCEKURI
LAW FIRM

Medidas de seguridad

Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares

- Artículo 2.- Además de las definiciones del Art. 3 de la Ley, se entenderá por:

  - Medidas de Seguridad Administrativas: Acciones y mecanismos para establecer la gestión, soporte y revisión de la seguridad de la información a nivel organizacional…

  - Medidas de Seguridad Físicas: Acciones y mecanismos que pueden emplear o no la tecnología. Ej. Proteger laptops, garantizar eliminación de forma segura.

  - Medidas de Seguridad Técnicas: Actividades, controles o mecanismos con resultado medible que se valen de la tecnología para asegurar los accesos a las bases de datos.

PONCEKURI
LAW FIRM

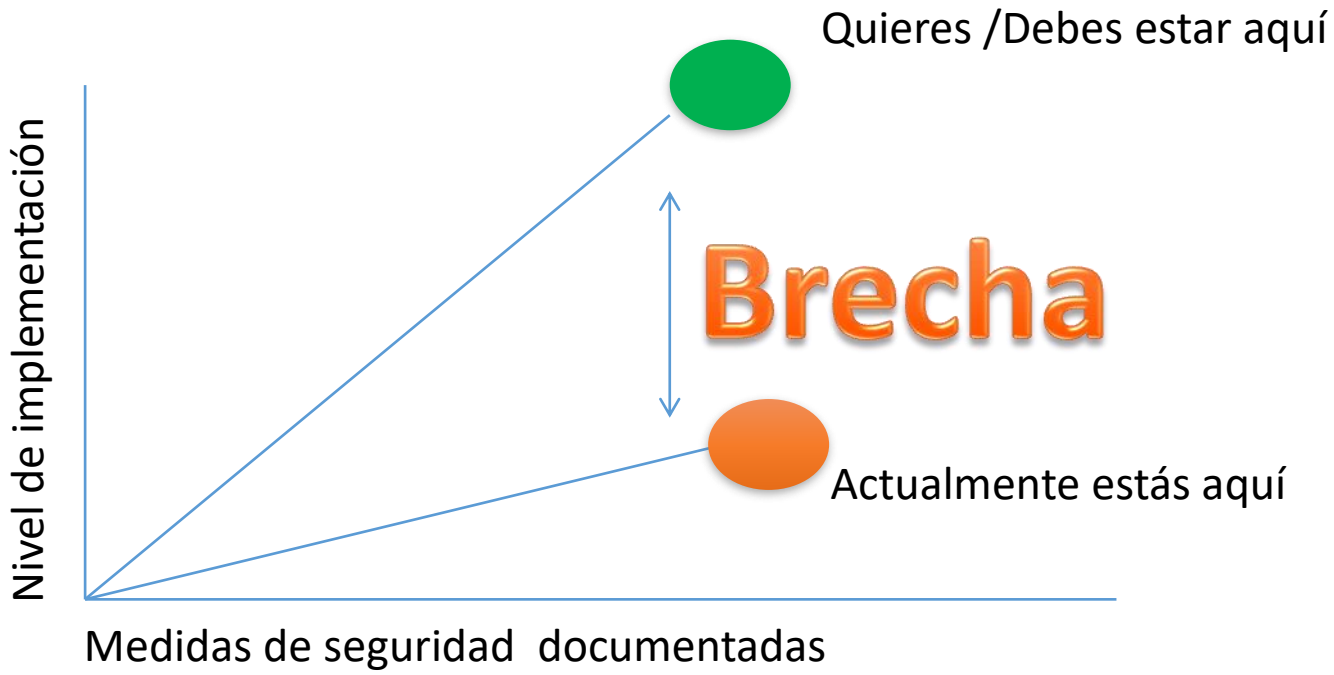
La clave

Análisis de riesgos

- El valor de los datos personales para los titulares
- La exposición de los activos involucrados con los datos personales
- El valor potencial para un atacante o tercera persona no autorizada para la posesión de los datos personales
- La trazabilidad y posibilidad de identificar quién tuvo acceso a los datos personales.

PONCEKURI
LAW FIRM

Análisis de brecha



PONCEKURI
LAW FIRM

Infracciones, sanciones y delitos

- Art 63.- INFRACCIONES:

I. No cumplir con la solicitud del titular para ejercer los derechos ARCO al tratamiento de sus datos personales, sin razón fundada;

II. Actuar con negligencia o dolo en la tramitación y respuesta de solicitudes ARCO;

III. Declarar dolosamente la inexistencia de datos personales, cuando exista total o parcialmente en las bases de datos del responsable;

IV. Dar tratamiento a los datos en contravención a los principios de la Ley.

V. Omitir en el aviso de privacidad, alguno o todos los elementos a que se refiere el artículo 16;

VI. Mantener datos inexactos, o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan;

VIII. Incumplir el deber de confidencialidad establecido Art. 21;

IX. Cambiar sustancialmente la finalidad originaria del tratamiento de los datos, sin observar lo dispuesto por el Art.12;

X. Transferir datos a terceros sin comunicarles el aviso de privacidad;

XI. Vulnerar la seguridad de bases de datos, locales, programas o equipos;

XII. Llevar a cabo la transferencia o cesión de los datos, fuera de los casos en que esté permitida por la Ley;

XIII. Recabar o transferir datos personales sin el consentimiento expreso

XIV. Obstruir los actos de verificación de la autoridad;

XV. Recabar datos en forma engañosa y fraudulenta;

XVI. Continuar con el uso ilegítimo de los datos cuando se solicito el cese;

XVII. Tratar los datos afectando o impidiendo el ejercicio de los derechos ARCO;

XVIII. Crear bases de datos en contravención a lo dispuesto por el Art. 9

XIX. Cualquier incumplimiento del responsable a las obligaciones establecidas a su cargo en términos de lo previsto en la presente Ley.

PONCEKURI
LAW FIRM

- Art. 64.- SANCIONES:
  - Apercibimiento (fracción I).
  - Multa de 100 a 160,000 UMA (fracciones II a VII).
  - Multa de 200 a 320,000 UMA (fracciones VIII a XVIII).
  - En caso de que persistan las infracciones de manera reiterada, el Instituto podrá imponer una multa adicional que irá de 100 a 320,000 UMAs.

PONCEKURI
LAW FIRM

- Delitos:

  - Artículo 67.- De 3 meses a 3 años de prisión al autorizado para tratar datos que con ánimo de lucro, provoque una vulneración de seguridad a las bases de datos bajo su custodia.

  - Artículo 68.- Prisión de 6 meses a 5 años al que, con el fin de lucro, trate datos personales mediante el engaño, aprovechándose del error del titular o persona autorizada para transmitirlos.

  - Artículo 69.- Tratándose de datos personales sensibles, las penas a que se refiere este Capítulo se duplicarán.

Pharma Plus, S.A. de C.V. con **$2,045,000** por omitir el elemento de identidad en el Aviso de Privacidad.

Caja Popular Cristo Rey, S.C. de R.L. de C.V., con **$2,181,550** por recabar datos de carácter financiero y patrimonial, sin contar con el consentimiento del titular.

PONCEKURI
LAW FIRM

TELCEL (2 multas $6,264,165)

Sin consentimiento del titular Telcel accedió a los contactos de su cliente , a quienes les hizo llamadas y envió mensajes, para ponerlos al tanto del adeudo y gestionar por medio de ellos la cobranza del servicio.

Universidad Intercontinental

(7 multas que suman $8,725,750)

Por transcribir las sesiones de las terapias psicológicas de un particular y publicarlas en un sitio de internet.

PONCEKURI
LAW FIRM

Oceánica multa por $2,493,200

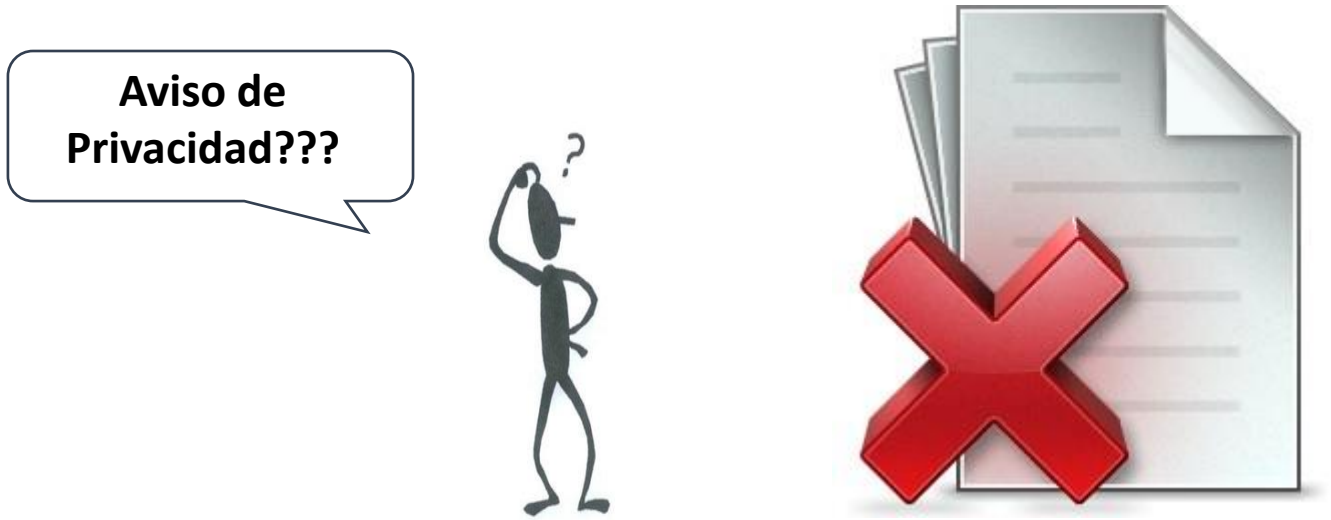
Fue multado por hacer públicos los datos de un paciente del y posteriormente obstruir actos de verificación ordenados por el Instituto.

PONCEKURI
LAW FIRM

Creaciones Textiles de Mérida, S.A. de C.V.

multa de $129,520.00

Fue multado por obtener datos personales sin haber dado a conocer, mediante el aviso de privacidad, la existencia de los mismos y el tratamiento que se les darían.



PONCEKURI
LAW FIRM

Nada es GRATIS!!!

PONCEKURI
LAW FIRM

PONCEKURI

LAW FIRM

Nuhad Ponce Kuri
nponce@poncekuri.com
@poncekuri
@nuhadsita13

Oscar Andrés Castillo Caamal
ocastillo@poncekuri.com
@poncekuri
@oscar_castillo4