ISO/IEC 29100:2011
Una introducción al marco de trabajo de privacidad para la protección de información de identificación personal (PII)

Con la adopción del Reglamento General de Protección de Datos (Regulación de la Unión Europea 2016/679) [1] y los acontecimientos más recientes vinculados con exfiltración de datos personales (incluyendo la información publicada de forma no autorizada de 49,6 millones de ciudadanos turcos [2] y 93,4 millones de ciudadanos mexicanos [3], sin contar el robo de información de 37 millones de usuarios del sitio de citas para adultos "Ashley Madison" [4], por solo nombrar algunos ejemplos) se hace cada vez más necesaria la implementación organizacional de un marco de trabajo para la protección de la información de identificación personal (*Personally Identifiable Information* – PII) que defina los roles y responsabilidades de todos los actores involucrados dentro del ciclo de vida de este tipo de datos. En este artículo se analizará el estándar ISO/IEC 29100:2011 y otras propuestas previas similares que pueden servir como referencia para la definición de una estrategia para la protección de la privacidad en la organización.

David Acosta

Contexto histórico de las iniciativas de protección de la privacidad

Conforme con el artículo 12 de la "Declaración Universal de los Derechos Humanos" de las Naciones Unidas [5] y el artículo 8 de la "Convención para la Protección de los Derechos Humanos y las Libertades Fundamentales" de la Unión Europea [6], la "**privacidad**" –entendiéndose ésta como el derecho a la protección de la intromisión en la vida privada (intimidad) de un individuo– es uno de los pilares del desarrollo individual y social en una sociedad democrática. Debido al desarrollo continuo de las tecnologías de información y comunicación (*Information and Communication Technology* – ICT) y la evidente confluencia entre los entornos físicos y digitales, la protección de la información de identificación personal (*Personally Identifiable Information* – PII) se ha convertido en uno de los principales objetivos organizacionales desde la perspectiva de Seguridad de la Información debido a su valor legal y comercial en caso de un incidente.

A pesar de que la existencia de la necesidad de protección de esta información era tangible desde los comienzos de la informática, no fue sino hasta 1980 cuando se desarrolló un modelo que permitió la implementación de una estrategia para la protección de la privacidad. En ese año, la Organización para la Cooperación y el Desarrollo Económico – OCDE publicó el documento "*Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data*" [7]. Este documento se basaba en tres elementos principales:

- "**Controlador de datos**": Tercero que, de acuerdo con la legislación nacional, tiene competencia para determinar los contenidos y el uso de datos personales independientemente de si dicha parte o un agente en su nombre los recoge, guarda, procesa o divulga.
- "**Datos personales**": Cualquier información relacionada con un individuo identificado o identificable (sujeto de los datos).
- "**Flujo transfronterizo de datos personales**": Movimiento de datos personales a través de fronteras nacionales.

Con estas definiciones se enumeraban ocho principios generales para la protección de datos personales:

A pesar de la claridad y simplicidad en la definición de estos principios, había un gran problema subyacente en su implementación ya que su aplicación era únicamente recomendable sin obligaciones jurídicas vinculantes a los estados miembro del OCDE, por lo cual su grado de cubrimiento global estaba limitado.

Más adelante, en 2005 se realizó la "27ª Conferencia Internacional de Protección de Datos" en Montreux (Suiza) [8]. En esta conferencia, más de 300 participantes de todo el mundo debatieron acerca del derecho a la protección de datos, cuyas conclusiones quedaron registradas en la declaración "La protección de datos personales y de la intimidad en un mundo globalizado: un derecho universal que respeta diversidades" ("*The protection of personal data and privacy in a globalised world: a universal right respecting diversities*") en donde se establecían 11 principios generales para la protección de datos personales:

Adicionalmente, en esta declaración se apelaba a las Naciones Unidas para que preparara una serie de instrumentos jurídicos vinculantes para establecer los derechos a la protección de datos y a los gobiernos para la adopción de los mismos. Las mismas conferencias en ediciones siguientes hicieron un llamado a la mejora en la cooperación internacional para la protección de datos y privacidad (28ª Conferencia en Montreal), la necesidad de establecer estándares internacionales sobre protección de datos y privacidad (30ª Conferencia en Estrasburgo), la adopción de dichos estándares (31ª Conferencia en Madrid) [9] y su puesta en marcha (32ª Conferencia en Jerusalén) bajo el contexto de "*Privacy by Design*" (del cual se hablará más adelante), el aseguramiento de datos y privacidad mediante el Derecho Internacional (35ª Conferencia en Varsovia) y la protección de datos personales en entornos de Big Data aplicando los principios establecidos anteriormente (36ª Conferencia en Balaclava) [10].

Ejemplos de Información de Identificación Personal (PII)
Historial criminal
Información clínica
Datos financieros y números de tarjeta de pago
Identificadores biométricos
Fechas de nacimiento
Información de discapacidades
Datos de recursos humanos y salarios
Perfiles financieros
Posiciones GPS
Direcciones IP
Nombres y apellidos
Direcciones de correo electrónico
Información de navegación por internet
Fotografías y videos
Orígenes étnicos y raza
Creencias religiosas o filosóficas
Orientación sexual

Figura 1.- Ejemplos de Información de Identificación Personal (PII)

Iniciativas similares fueron desarrolladas de forma paralela por el Foro de Cooperación Económica Asia Pacífico (APEC), Federal CIO Council [11], la Red de Autoridades Francófonas, la Red Iberoamericana de Protección de Datos y la Red Global para hacer cumplir la ley de privacidad (*Global Privacy Enforcement Network* – GPEN).

Muchos de estos criterios fueron tenidos en cuenta para la redacción de los principios del Reglamento general de protección de datos de la Unión Europea, que indica que los datos personales deberán cumplir los siguientes principios relativos al tratamiento:

Privacidad y protección de datos por Diseño: Principios fundamentales

En la 32ª Conferencia Internacional de comisarios de protección de la privacidad y datos personales realizada en Jerusalén en 2010, se destacó el desarrollo de la "Resolución sobre la privacidad por diseño" (*Resolution on Privacy by Design*) [12] en donde se reconocía la "Privacidad por Diseño" (concepto desarrollado inicialmente por la Dra. Ann Cavoukian) [13] como componente para la protección fundamental de los datos personales. Bajo este criterio, no es suficiente con solo cumplir con los marcos regulatorios sino que además se deben establecer pautas para el desarrollo de la protección de la privacidad desde el inicio del ciclo de vida del desarrollo de un sistema hasta la puesta en producción y mantenimiento del mismo, convirtiéndose en el modo de operación predeterminado de la organización cubriendo los sistemas de tecnología de la información, las prácticas de negocio responsables y el diseño físico e infraestructura de red.

Principios de protección de privacidad de la OECD
1. Principio de **limitación de recogida**
2. Principio de **calidad de los datos**
3. Principio de **especificación del propósito**
4. Principio de **limitación de uso**
5. Principio de **salvaguardia de la seguridad**
6. Principio de **transparencia**
7. Principio de **participación individual**
8. Principio de **responsabilidad**

Figura 2.- Principios de protección de la privacidad del OECD.

Principios de protección de privacidad de la 27ª Conferencia Internacional de Protección de datos (Montreux – Suiza)
1. Principio de **recopilación y procesamiento justo y legítimo de datos**
2. Principio de **exactitud**
3. Principio de **especificación y limitación del objetivo**
4. Principio de **proporcionalidad**
5. Principio de **transparencia**
6. Principio de **participación individual** y, en concreto, la garantía del derecho de acceso de la persona en cuestión
7. Principio de **no discriminación**
8. Principio de **seguridad de los datos**
9. Principio de **responsabilidad**
10. Principio de **supervisión independiente y sanción legal**
11. Principio de **nivel adecuado de protección** en caso de flujos transfronterizos de datos personales

Figura 3.- Principios de protección de la privacidad de la 27ª Conferencia Internacional de Protección de datos.

Principios de protección de privacidad del Reglamento general de protección de datos de la Unión Europea
1. Principio de **licitud, lealtad y transparencia**
2. Principio de **limitación de la finalidad**
3. Principio de **minimización de datos**
3. Principio de **exactitud**
4. Principio de **limitación del plazo de conservación**
5. Principio de **integridad y confidencialidad**
6. Principio de **responsabilidad proactiva**

Figura 4.- Principios de protección de la privacidad del Reglamento de protección de datos de la Unión Europea.

Los principios sobre los cuales se fundamenta la "Privacidad por diseño" se muestran en la **Figura 5**.

La privacidad por diseño se ha convertido en una obligación legal desde la perspectiva del Reglamento general de protección de datos de la Unión Europea.

ISO/IEC 29100:2011: El marco de trabajo de protección de privacidad

Desde la 26ª Conferencia Internacional de comisarios de protección de la privacidad y datos personales que se desarrolló en Varsovia en 2004 ya se venía haciendo énfasis en la necesidad de trabajar de forma conjunta con la Organización Internacional de Normalización (*International Organization for Standardization* – ISO) para el desarrollo de un estándar orientado a la protección de la privacidad [14]. En 2007 en Lucerna (Suiza) como parte del WG5 de ISO/IEC/FIDIS/ITU-T de estándares de gestión de identidades se presentó el estándar ISO/IEC 29100, enfocado al establecimiento de un marco de trabajo para la protección de la privacidad.

El objetivo de este estándar es soportar a las organizaciones en la definición de los requerimientos para salvaguardar la privacidad en cualquier sistema en el que se procese información de identificación personal y servir como complemento en el caso que existan consideraciones legales relacionadas.

La información de identificación personal (PII) tratada por el estándar debe coincidir con alguno de los siguientes identificadores:

- Si contiene o está asociada con un identificador que se refiera a una persona natural (por ejemplo, un número de seguridad social)
- Si contiene o está asociada con un identifica-

dor que pueda estar relacionado con una persona natural (por ejemplo, un número de pasaporte o un número de cuenta, etc.)

• Si contiene o está asociado con un identificador que pueda ser usado para establecer una comunicación con una persona natural identificada (por ejemplo, una ubicación geográfica precisa, un número de teléfono, etc.)

• Si contiene una referencia que esté enlazada con cualquiera de los identificadores anteriores.

Así mismo, también se contempla cualquier dato que distinga a una persona natural de otra (por ejemplo, datos biométricos).

Para la gestión de este tipo de datos se definen los siguientes actores:

• **Titular de los datos** (PII Principal / Data Subject): Persona física titular de la información de identificación personal (PII).

• **Responsable de los datos** (PII Controller): Parte interesada que determina el propósito y los medios para el procesamiento de información de identificación personal.

• **Encargado del tratamiento** (PII Processor): Parte interesada ajena al responsable que trata los datos como consecuencia de una relación jurídica que delimita su ámbito de actuación en la prestación de un servicio

• **Tercero** (Third Party): Parte interesada diferente del titular, el responsable o el encargado.

La interacción de estos actores y la información de identificación personal (PII) puede dar resultado a los siguientes flujos que definen las responsabilidades en el tratamiento de los datos:

Siendo así, el marco de trabajo para la protección de estos datos para la gestión de las anteriores interacciones está compuesto por 11 principios (ver **Figura 7**). A continuación se describen cada uno de estos principios:

1. Consentimiento y opción: El titular de los datos debe poder elegir el procesamiento o no de sus datos a través de un consentimiento y se le debe informar acerca de sus derechos de participación y acceso.

Principios de la "Privacidad por Diseño"
Proactivo, no reactivo; Preventivo, no correctivo
Privacidad como la configuración predeterminada
Privacidad incrustada en el diseño
Funcionalidad total: "todos ganan", no "si alguien gana, otro pierde"
Seguridad extremo-a-extremo: Protección del ciclo de vida completo
Visibilidad y transparencia
Respeto por la privacidad de los usuarios. Mantener el enfoque centrado en el usuario

Figura 5.- Principios de la "Privacidad por diseño".

Escenario	Titular	Responsable	Encargado	Tercero
A	Entrega PII	Recibe PII		
B		Entrega PII	Recibe PII	
C	Entrega PII		Recibe PII	
D	Recibe PII	Entrega PII		
E	Recibe PII		Entrega PII	
F		Recibe PII	Entrega PII	
G		Entrega PII		Recibe PII
H			Entrega PII	Recibe PII

Figura 6.- Interacción entre los actores del tratamiento de datos personales.

2. Legitimidad de propósito y especificación: El propósito de tratamiento de datos debe cumplir con las leyes aplicables y debe ser informado al titular antes de que la información sea recolectada a través de un lenguaje claro y adaptado a las circunstancias.

3. Limitación en la recolección: La recolección de datos personales deben ser limitada estrictamente a las necesidades del propósito especificado y bajo las consideraciones de las leyes aplicables.

4. Minimización de datos: Adoptar el principio de "necesidad de saber" (Need-to-know) para darle acceso a los datos únicamente al personal requerido y eliminar los datos cuyo propósito haya expirado o que no exista requerimiento legal para retenerlo.

5. Limitación de uso, retención y divulgación de los datos personales conforme con los propósitos específicos, explícitos y legítimos establecidos.

6. Exactitud y calidad: Garantizar que los datos procesados son exactos, completos, actualizados, adecuados y relevantes para el propósito de uso, validando su confiabilidad si son provistos por alguien diferente del titular, así como establecer procedimientos de control en la recolección y mecanismos periódicos para la validación de los datos recolectados y almacenados.

7. Apertura, transparencia y notificación: Proveer al titular de información de las políticas de procesamiento y de cualquier cambio en el procedimiento del tratamiento de datos.

8. Participación individual y acceso: Permitirle al titular acceder y revisar sus datos y definir procedimientos para que los titulares puedan ejercer sus derechos de forma rápida y eficiente.

9. Rendición de cuentas: Asignarle la responsabilidad de implementación de políticas de privacidad a un individuo en la organización, informarle al titular en caso de una brecha de seguridad que haya afectado sus datos, gestionar los terceros involucrados con los que se comparten los datos a través de consideraciones contractuales y efectuar formación al personal que tenga acceso a los datos.

10. Seguridad de la información: Implementar controles operativos, funcionales y estratégicos para garantizar la integridad, confidencialidad y disponibilidad de los datos personales y protegerlos contra riesgos como acceso no autorizado, destrucción, divulgación o pérdida a través del ciclo de vida, así como realizar análisis de riesgos para identificar el estado de controles físicos, técnicos y organizacionales.

11. Cumplimiento con

Principios de protección de privacidad de ISO/IEC 29100:2011
1. Consentimiento y opción
2. Legitimidad de propósito y especificación
3. Limitación en la recolección
4. Minimización de datos
5. Limitación de uso, retención y divulgación
6. Exactitud y calidad
7. Apertura, transparencia y notificación
8. Participación individual y acceso
9. Rendición de cuentas
10. Seguridad de la información
11. Cumplimiento con la privacidad

Figura 7.- Principios de protección de privacidad de ISO/IEC 29100:2011.

la privacidad: Verificar y demostrar los niveles de protección de los controles de seguridad a través de auditorías periódicas con auditores internos o de terceros y monitorizar el cumplimiento de los requerimientos de privacidad.

El estándar en formato digital puede ser descargado sin costes del sitio web de la Fuerza de Tarea de Tecnologías de la Información de ISO/IEC (Information Technology Task Force – ITTF) [15].

¿Por qué es importante la implementación de un marco de trabajo como ISO/IEC 29100:2011?

La información de identificación personal es claramente uno de los activos de información más confidenciales en una organización y debe ser empleado de forma exclusiva bajo controles específicos. Precisamente, algunas de las razones por las cuales una organización que no tenga implementado un marco de trabajo de privacidad debería proceder con su despliegue inmediatamente son:

- Protección de la privacidad de la información personal delegada por los titulares como parte de la estrategia de responsabilidad corporativa
- Cumplimiento de requerimientos legales y regulatorios (por lo general vinculados con la región geográfica en donde se capturen y procesen los datos personales)
- Incremento de la confiabilidad de marca y credibilidad por parte del usuario
- Minimización y gestión de cualquier incidente de seguridad vinculado a estos datos

Con estas bases, se logran minimizar las potenciales consecuencias vinculadas con la negligencia en la protección de datos personales (multas, procesos legales, daños a la reputación, demandas, pérdida de la confianza de inversores, aumento en los costes de respuesta a incidentes, etc.).

Si se cuenta con regulaciones legales orientadas a la protección de Información de Identificación Personal (PII), ¿Para qué es necesaria la implementación de ISO/IEC 29100:2011?

Tal como se ha descrito anteriormente, el estándar ISO/IEC 29100:2011 provee un marco de trabajo de alto nivel para la protección de la Información de Identificación Personal (PII) que le permite a las organizaciones la definición de sus requerimientos de protección de la privacidad mediante la especificación de una terminología común, la definición de actores y sus roles en el procesamiento de datos, los requerimientos de privacidad y la referencia de una serie de principios orientados a la gestión de los aspectos organizativos, técnicos y procedimentales de esta estrategia.

Figura 8.- Factores que influencian la gestión de riesgos de privacidad.

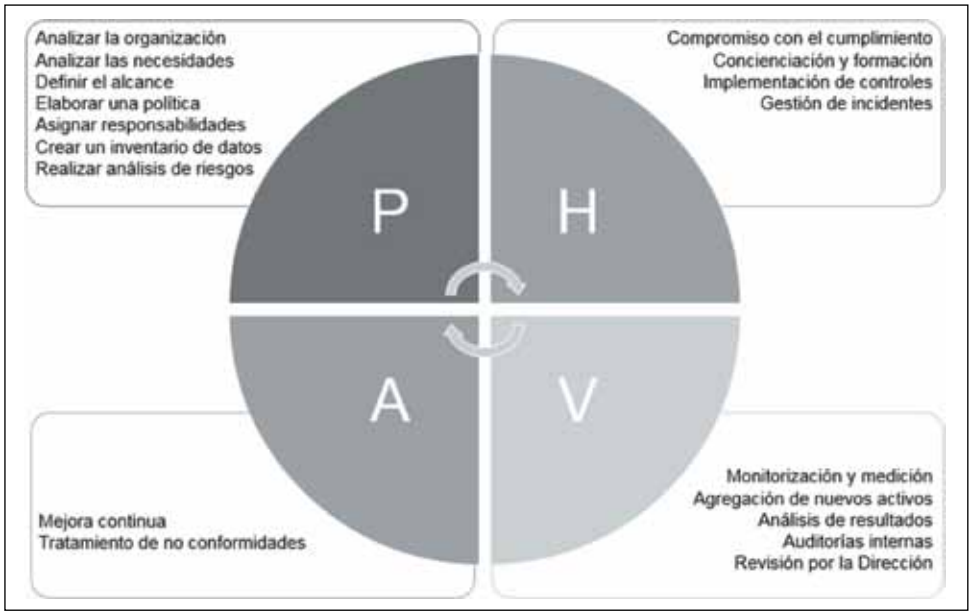

Figura 9.- Círculo de Deming (PHVA) de despliegue de ISO/IEC 29100:2011.

No obstante, el estándar no remplaza o entra en conflicto con la legislación local o internacional orientada a la protección de la privacidad. Al contrario, complementa estas acciones y las consolida mediante el establecimiento de acciones globales trasversales y estratégicas que le permiten a la organización no solo cubrir los requerimientos legales vigentes sino también otro tipo de variables contractuales, de negocio y otros factores vinculados con datos personales que deberían ser detectados dentro del proceso de gestión de riesgos corporativo.

Por otro lado, con la definición de un marco de trabajo de alto nivel para la protección de la privacidad se facilita la adopción del concepto de "Privacidad por Diseño", evitando que la organización acarree con costes excesivos cuando se realiza el despliegue de acciones correctivas

Correspondencia de conceptos entre ISO/IEC 29100 e ISO/IEC 27000	
ISO/IEC 29100	ISO/IEC 27000
Parte interesada (privacidad)	Parte interesada
Información de identificación personal	Activo de información
Violación de la privacidad	Incidente de seguridad de la información
Control de privacidad	Control
Riesgo de la privacidad	Riesgo
Gestión de riesgos de la privacidad	Gestión de riesgos
Requerimientos para protección de la privacidad	Objetivos de control

Figura 10.- Correspondencia de conceptos entre ISO/IEC 29100 e IO/IEC 27000.

después de que el sistema se encuentre en producción y remplazándolas con acciones preventivas y detectivas desde las fases iniciales de implementación, a través del ciclo PHVA (Planificar-Hacer-Verificar-Actuar) del cual se hablará enseguida.

Siendo así, no se debe entender el estándar ISO/IEC 29100:2011 como un remplazo de la legislación o como un estándar orientado exclusivamente al cumplimiento legal. Al contrario, se trata de un marco holístico enmarcado dentro de una estrategia organizacional de alto nivel para la protección de la privacidad en cualquier ámbito que afecte a la empresa.

Implementación de ISO/IEC 29100:2011

Al igual que con otros estándares de ISO, los principios de protección de datos personales definidos en la ISO/IEC 29100:2011 pueden ser implementados a través de las fases del círculo de Deming o PHVA (Planificar-Hacer-Verificar-Actuar) dentro de las actuaciones de mejora continua.

Partiendo del criterio de "Privacidad por Diseño" descrito anteriormente, la necesidad de protección de datos personales debería estar presente desde la fase de diseño del sistema de gestión. Con esta idea en mente, el despliegue de las acciones de alineación no dista de las realizadas en otros estándares similares como ISO/IEC 27001, ISO/IEC 9001 o ISO/IEC 14001.

Integración de ISO/IEC 29100 con ISO/IEC 27001

Cuando se habla de "información de identificación personal" desde la perspectiva de seguridad de la información, solamente se está refiriendo a una categoría (subconjunto) del grupo de activos de información global de la organización. El estándar ISO/IEC 29100 tiene su entorno de aplicación en ese subconjunto de activos en particular. Tal como se explicó anteriormente, su implementación se puede llevar a cabo empleando PHVA, estableciendo acciones transversales de gestión estratégica.

Con esto en mente, cuando se pretende establecer un sistema de gestión de seguridad de la información (SGSI) empleando el estándar ISO/IEC 27001:2013, el estándar ISO/IEC 29100 complementaría los controles de seguridad asociados con la privacidad.

Bajo la premisa que ambos estándares se complementan en vez de excluirse, el estándar ISO/IEC 29100:2011 incluye el Anexo A (informativo) que establece una correspondencia entre los conceptos de privacidad empleados en los principios de protección de datos de dicho estándar y los conceptos de seguridad de la familia de estándares ISO/IEC 27000.

De esta manera, la integración entre ambos estándares (ISO/IEC27000 de forma global para todos los activos de información e ISO/IEC 29100 para el subconjunto de activos de información de identificación personal) es transparente y directa, sin solapar acciones.

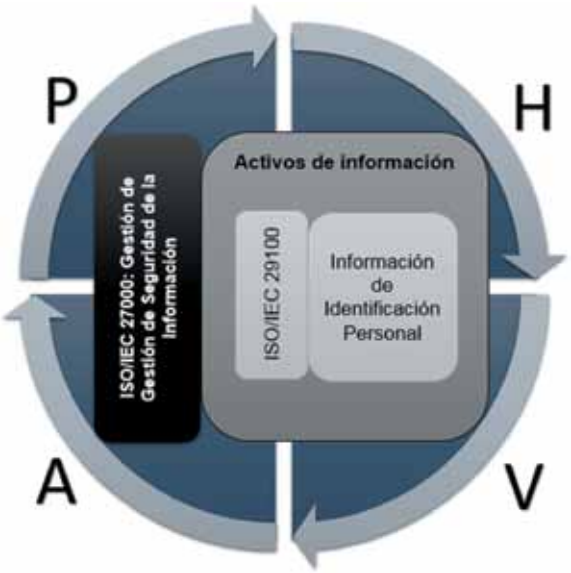

Figura 11.- Activos de información y los estándares de ISO/IEC asociados.

Conclusión

Cuando una compañía se enfrenta con la necesidad de proteger los datos personales de sus usuarios –ya sea por requerimientos legales o contractuales o por iniciativas internas de mejoramiento de la seguridad de la información– una de las decisiones clave es la elección de un marco de trabajo que le permita tomar elementos comunes y estándares y adaptarlos a sus propias necesidades.

Es obvio que no existe un modelo único que pueda cubrir las expectativas de todas las organizaciones desde la perspectiva de privacidad. No obstante, se puede hacer uso de los criterios descritos en iniciativas globales y estandarizadas para evitar empezar de cero.

ISO/IEC 29100:2011 ha centralizado la gran mayoría de criterios de protección de información de identificación personal establecidos en regulaciones y mejores prácticas anteriores (OCDE, APEC, GPEN, etc.) y los ha puesto en contexto para servir como base en la definición de requerimientos de protección de la privacidad a nivel organizacional, técnico, procedimental, físico y regulatorio, empleando una terminología común, un conjunto de principios de procesamiento y las acciones necesarias para el despliegue de la estrategia organizacional. ■

David Acosta
Consultor Senior de Seguridad
INTERNET SECURITY AUDITORS

REFERENCIAS

[1] Reglamento general de protección de datos http://www.consilium.europa.eu/es/policies/data-protection-reform/data-protection-regulation/

[2] The entire Turkish citizenship database has allegedly been leaked online http://www.businessinsider.com/turkish-citizenship-database-allegedly-hacked-and-leaked-2016-4?r=UK&IR=T

[3] Personal info of 93.4 million Mexicans exposed on Amazon https://www.databreaches.net/personal-info-of-93-4-million-mexicans-exposed-on-amazon/

[4] Online Cheating Site Ashley Madison Hacked http://krebsonsecurity.com/2015/07/online-cheating-site-ashleymadison-hacked/

[5] The Universal Declaration of Human Rights http://www.un.org/en/universal-declaration-human-rights/index.html

[6] Convention for the Protection of Human Rights and Fundamental Freedoms https://www.coe.int/es/web/conventions/full-list/-/conventions/rms/0900001680063765

[7] Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html

[8] Declaración de Montreux: "La protección de datos personales y de la intimidad en un mundo globalizado: un derecho universal que respeta diversidades" https://icdppc.org/wp-content/uploads/2015/06/montreux_declaration-Spanish.pdf

[9] Declaración de Madrid: https://icdppc.org/wp-content/uploads/2015/02/The-Madrid-Resolution.pdf

[10] Declaración de Balaclava: "Resolución sobre Big Data" https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Big-Data-Spanish-version.pdf

[11] FEA SPP Versión 2 http://cio.gov/documents/Security_and_Privacy_Profile_v2.pdf

[12] Declaración de Jerusalén: "Resolución sobre privacidad por diseño" http://privacyconference2012.org/wps/wcm/connect/pvconference/a88f0a12-022c-4482-804d-d55fc18d2d06/2010_J5.pdf?MOD=AJPERES

[13] Privacidad por Diseño - Los 7 principios fundamentales http://mediascope.nl/wp-content/uploads/2015/08/privacidad-por-dise%C3%B1o.pdf

[14] Propuesta de la Resolución sobre el proyecto de normas ISO de protección de la privacidad https://icdppc.org/wp-content/uploads/2015/02/Propsoed-Resolution-of-Draft-ISO-Privacy-Framework-Standard-Spanish.pdf

[15] ISO/IEC Information Technology Task Force (ITTF) web site http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html