SALUD, TECNOLOGÍA Y DERECHO

José Manuel Muñoz Vela

Vicepresidente de ISACA Valencia
Abogado experto en Technology, Corporate & Compliance
CO, CISA, CISM, CGEIT, CRISC, ACP

ISACA
Sistemas de información fiables y valiosos
Valencia Chapter

ISACA

Sistemas de información fiables y valiosos
Valencia Chapter

ISACA nació en EEUU en 1969, y es una asociación global sin ánimo de lucro que aglutina a más de **140 000 profesionales en 180 países**, con más de 200 capítulos en todo el mundo.

Certificaciones reconocidas de prestigio internacional de habilidades y conocimientos críticos para el negocio:

CISA® (Certified Information Systems Auditor)
CISM® (Certified Information Security Manager)
CGEIT® (Certified in the Governance of Enterprise IT)
CRISC® (Certified in Risk and Information Systems Control)

Marcos y recursos:

Cybersecurity Nexus TM (CSX): Un marco integral y global en ciberseguridad
COBIT®: Un marco de negocio para el gobierno de las TI en las organizaciones

ISACA Valencia

Asociación de Auditoría y Control de los Sistemas de Información de la C.V.

ISACA Valencia Chapter

Entidad sin ánimo de lucro que aglutina a los profesionales de gobierno, auditoría, seguridad y control de los sistemas no sólo de nuestra comunidad sino de otras comunidades como Galicia, Andalucía, Aragón o Murcia.

ISACA
Sistemas de información fiables y valiosos
Valencia Chapter

Health, Technology & Compliance

ISACA
Sistemas de información fiables y valiosos
Valencia Chapter

Nuevas realidades globales

Nuevas necesidades

Nuevas exigencias

Nuevas respuestas

Nuevas tecnologías en constante cambio

ISACA
Sistemas de información fiables y valiosos
Valencia Chapter

¿Nuevos instrumentos?

¿Locales, autonómicos, estatales, comunitarios, internacionales?

CÓDIGO CIVIL (1888)

TRLPI (1996)

LSSI-CE (2002)

CÓDIGO DE COMERCIO (1889)

CONSTITUCIÓN ESPAÑOLA (1978)

LOPD (1999)

CÓDIGO PENAL (1995)

ISACA
Sistemas de información fiables y valiosos
Valencia Chapter

¿Son suficientes y eficaces?

ISACA
Sistemas de información fiables y valiosos
Valencia Chapter

Objetivo

Garantista
Protección eficaz y salvaguarda de derechos

ISACA
Sistemas de información fiables y valiosos
Valencia Chapter

Legal Compliance by Design 360°

ISACA
Sistemas de información fiables y valiosos
Valencia Chapter

¿”Privacy” by design? y/o ¿”Security” by design?

¿Qué buscamos?

Integrar negocio con tecnología, Derecho, seguridad y protección de la información.

Previsión y análisis del impacto en la privacidad con anterioridad a la implementación de un sistema,, proceso, programa o servicio.

Definir e integrar desde la fase inicial (no a posteriori) las medidas y controles de seguridad necesarios para mantener la seguridad de la información.

Garantizar la privacidad de forma constante en el sistema físico, tecnológico o proceso de negocio involucrado.

ISACA
Sistemas de información fiables y valiosos
Valencia Chapter

¿Por qué y Cómo?

COMPLIANCE

a) Corporativo

Códigos de gobierno y éticos
Códigos de Conducta, Códigos Tipo, BCR's
Estándares y códigos de buenas prácticas internacionales–nacionales
COBIT (Control Objectives for Information and Related Technology) del Instituto de Gobierno TI (ITGI)
ISO/IEC 27001 (17799) (Information Technology Security Techniques-Code of Practice for Information Security Management) de la Organización Internacional para la Estandarización/Normalización (ISO)
UNE-EN ISO27799 Gestión de la Seguridad de la Información en sanidad utilizando la norma ISO/IEC 27002
Generales-sectoriales

b) Legal

Acuerdos y tratados internacionales, Derecho comunitario, Derecho estatal, Derecho autonómico

c) Contractual

Acuerdos, contratos, concursos, pliegos, licitaciones

eHealth & Apps

Smartphones, tablets and smartTVs

ISACA
Sistemas de información fiables y valiosos
Valencia Chapter

EJEMPLOS

ISACA
Sistemas de información fiables y valiosos
Valencia Chapter

Expansión.com
Martes, 26.08.14. Actualizado a las 19:52

Expansión Mercados

Expansión en ORBYT.

Ahorro | Empresas | Economía | Sociedad | Tecnología | Jurídico | Directivos | Motor | Tendencias | Multimedia | Pymes | Emprendedores&Empleo | Más

Entrevistas | Opinión | Sentencias

IBEX 35 10.773,2 (+0,25%) | I.G. BOLSA MADRID 1.098,1 (+0,18%) | DOW JONES 17.098,4 (+0,00%) | EURO STOXX 3.

Portada » Jurídico

Tabletas y 'smartphones' aumentan los ciberataques a empresas

Más noticias sobre: juridico, tecnología

26.08.2014 Mercedes Serraller

Los trabajadores con el correo interno e información corporativa en sus dispositivos móviles personales se convierten en blanco fácil para los 'hackers' que quieran acceder a información de sus compañías.

Los empleados con acceso a redes corporativas en sus dispositivos móviles son blanco de 'hackers'.

Tabletas y smartphones aumentan los ciberataques a empresas. Los empleados con correos internos e información de su compañía en sus dispositivos móviles personales se convierten en un blanco fácil para los piratas informáticos con sed de información sensible. Así lo advierten los expertos, que se apoyan en datos de un estudio de Norton, que revela que el 49% de los consumidores usa sus dispositivos móviles personales tanto para trabajar como para entretenerse.

Esto genera nuevos riesgos de seguridad para las empresas puesto que, cuanto mayor sea el número de puntos de acceso a sus sistemas, mayor será también el riesgo de fugas.

Última hora — CaixaBank

14:30 Fitch aplaude la compra de Barclays por CaixaBank pero duda del recorte de costes

14:23 Norwegian compra Prestige Cruises por 3.000 millones de dólares

14:17 Juncker entrevistará a Cañete el jueves antes de decidir qué cartera le adjudica

Lo + leído | Lo + comentado

1 ¿Existe el trabajo perfecto?

2 Sidney, la ciudad con mejor calidad de vida del mundo

3 La plantilla de Barclays se reducirá a la mitad tras la compra por CaixaBank

4 Cómo es el nuevo comprador de vivienda

Las Apps pueden plantear serios riesgos para la confidencialidad de la información corporativa así como para la privacidad de las personas.

Aumentan los ataques a las organizaciones y personas. Mayor número de puntos de acceso, mayor riesgo de fugas

Trabajadores con correo interno o información corporativa. Estudio Norton:

- 49% de consumidores los utiliza para trabajar y como entretenimiento.
- El 48 % ni contraseñas, ni software de seguridad, ni copias

Ejemplos:

Caso Snowden vs EEUU. WhatsApp, Instagram, FourSquare, etc….

Mensajería instantánea (Whatsapp, Line, Wechat…) y vulnerabilidades (Ej: Se puede cambiar al remitente).

"Cámara de visión nocturna" comercializada para Android. Obtiene teléfono de Whatsapp, Telegram o Chaton y suscribe al usuario a servicios SMS Premium.

Dictamen conjunto sobre la privacidad en aplicaciones móviles
Grupo de Trabajo del Artículo 29*
Opinion 02/2013 on apps on smart devices
Adopted on 27 February 2013

Informe Análisis coordinado sobre las condiciones de privacidad de las aplicaciones móviles

(*) El grupo de autoridades europeas de protección de datos -denominado "Grupo de Trabajo del Artículo 29"- es el grupo consultivo compuesto por representantes de las autoridades nacionales de protección de datos de los Estados miembros, el Supervisor Europeo de Protección de Datos y la Comisión Europea. Sus funciones están descritas en el Artículo 30 de la Directiva 95/46/EC y el Artículo 15 de la Directiva 2002/58/EC.

Dictamen conjunto sobre la privacidad en aplicaciones móviles

- El **marco legal aplicable a cualquier tipo de App dirigida a los usuarios europeos**, dejando a un lado las normativas locales que resulten de aplicación, es la Directiva de Protección de Datos 95/46, en combinación con la Directiva 2002/58/CE de Privacidad y Comunicaciones Electrónicas. Este marco normativo **es aplicable con independencia de dónde esté ubicado el desarrollador de la aplicación o la tienda que la comercialice, debido a que estos programas recurren a medios ubicados en la UE, como son los propios terminales de los usuarios**.

- La mayoría de las **conclusiones y recomendaciones del Dictamen se dirigen a desarrolladores de aplicaciones** ya que son los que tienen mayor control sobre cómo se gestiona y presenta la información dentro de la aplicación.

- El dictamen presta **especial atención al uso de aplicaciones por parte de menores** (en España 14 años, en EEUU y en el futuro reglamento europeo de protección de datos, 13)

- ***"Los desarrolladores deben adoptar las necesarias medidas técnicas y organizativas para asegurar la protección de los datos personales que procesen en todas las fases del diseño e implementación de la App (Privacy by Design)".***

- ***Los fabricantes de sistemas operativos y dispositivos deben "Emplear la privacy by design para evitar la vigilancia secreta del usuario y garantizar la seguridad del tratamiento***".

Ejemplo: “Consentimiento previo e informado”

Según el estudio, sólo el 61% de las 150 aplicaciones más descargadas cuenta con una política de privacidad.

Conclusiones del Dictamen:

- Los desarrolladores deben proporcionar información suficiente sobre los datos que van a tratar antes de hacerlo, de forma que se pueda obtener un consentimiento válido.
- El usuario no debe enfrentarse a una pantalla única cuya única opción es la “Sí, acepto”. También debería mostrarse un botón que permitiera cancelar la instalación.
- El hecho de hacer clic en el botón “Instalar” no implica necesariamente un consentimiento válido para el tratamiento de datos personales si no va acompañado de suficiente información, tanto sobre las condiciones de ese tratamiento como sobre el hecho de que al pulsar “instalar” se presta el consentimiento para tratar los datos en esas condiciones.

Principales obligaciones:

- Obtención del consentimiento previo e informado del usuario
- Limitación de la finalidad para la que se recoge la información
- Minimización de la información a recabar
- Adopción de medidas de seguridad adecuadas
- Obligación de información al usuario sobre sus distintos derechos
- Períodos de retención de datos
- Tratamiento adecuado de datos de menores. En este sentido conviene recordar que, en España, la legislación no permite el tratamiento de datos de menores de 14 años sin el consentimiento de padres o tutores.

Algunos retos:

- La *privacy by design va* más allá de los requerimientos regulatorios vigentes según la legislación local de cada país. Puede no constituir un requerimiento regulatorio.
- Concienciación
- Cambio cultural a nivel corporativo: Incentivar el valor de la privacidad
- Liderazgo de la dirección
- Políticas y procedimientos
- Recursos
- Valoración en términos de eficacia y eficiencia
- Involucrar a la organización a todos los niveles, especialmente área clave.
- Conversión de una buena práctica en un requerimiento:
  - Corporativo
  - Contractual
  - Legal
- Formación
- Guías y estándares por parte de autoridades y organismos reguladores que respondan a la necesidad del mercado, negocio y tecnología

ISACA
Sistemas de información fiables y valiosos
Valencia Chapter

¡Gracias por su atención!

vicepresidente@isacavalencia.org

www.isaca.org
www.isacavalencia.org