LEGISLACIÓN, SALUD Y TECNOLOGÍA

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

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

Technology vs Compliance

- NUEVAS REALIDADES GLOBALES
- NUEVAS NECESIDADES
- NUEVAS EXIGENCIAS
- NUEVAS SOLUCIONES
- NUEVAS TECNOLOGÍAS EN CONSTANTE CAMBIO


SOCIEDAD DEL CONOCIMIENTO
COMPLIANCE OFFICER
GAMES
PRIVACY
SOCIEDADES VIRTUALES
APPS
IA
CONTENIDOS DIGITALES
COMPLIANCE
HACKERS
BIGDATA
DPO
CLOUD
BIA
CIBERBULLYING
REDES SOCIALES
PROPIEDAD VIRTUAL
DRP
SEXTING
BCP
BITCOIN
DATABROKERS

ISACA
Sistemas de información fiables y valiosos
Valencia Chapter

¿NUEVOS INSTRUMENTOS?

VIT SALUD VALENCIA | INNDEA VALENCIA | AJUNTAMENT DE VALÈNCIA
Red de Innovación en el Sector Salud

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

EJEMPLOS

PRIVACY

Artículo 13 RDLOPD Consentimiento para el tratamiento de datos de menores de edad

(…)

4. *Corresponderá al responsable del fichero o tratamiento articular los* ***procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado en su caso, por los padres, tutores o representantes legales****.*

CincoDías.com

Lunes, 28-06-2010 | Actualizado a las 16:29 h. Newsletter RSS Widgets Conectar Registro

Inicio Empresas Mercados Economía Profesionales Empleo y formación Tecnología Finanzas personales Tendencias Opinión Guías › Visor en PDF › Hemeroteca

buscar

MERCADOS Sigue la cotización de los 35 valores del Ibex

inversis BANCO Tu Inversis

Depuración

Tuenti borra casi 35.000 perfiles de menores de 14 años en 2010

Tuenti continúa con la identificación de jóvenes que no cumplan con la edad mínima exigida -14 años- y en los primeros cinco meses del año 2010 ya ha eliminado casi 35.000 perfiles de menores por debajo de ese umbral, según confirmó un portavoz de la red social.

¿Te interesa? Si Compartir: – más opciones

LO ÚLTIMO LO MÁS LEIDO LO MÁS VOTADO

16:20 - La inflación interanual en Alemania alcanzó en junio el 0,9%

16:07 - Los gigantes de Wall Street vuelven a contratar por primera vez en dos años

16:00 - Díaz Ferrán asegura que la reforma laboral encarece el despido

15:49 - Wall Street arranca la semana casi plano después de la reunión del G-20

ver más

publicidad

Conéctate a openbank y contrata el depósito a 12 meses

COMPLIANCE PROGRAMS

REFORMA DEL CÓDIGO PENAL

Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal

Antecedentes

a) EEUU
Watergate, FCPA 1977, Enron, SOX Act 2002

b) Europa
Italia: Decreto Legislativo 8 de junio de 2001, nº 231
UK: Bribery Act 2010

ASPECTOS ESENCIALES

Compliance Program – Programa de prevención de delitos
Compliance Officer (Supervisión del funcionamiento y cumplimiento)
Gestión de riegos (Identificación de riesgos, plan de acción, mapa de riesgos, revisión de controles y Manual de *Corporate Defense*)
Políticas y Procedimientos
Información y formación
Modelos de gestión de recursos financieros (Due Diligence)
Modelos de respuesta (instrucción y decisión)
Sistema de gestión de denuncias (Obligación)
Sistema disciplinario

REQUERIMIENTOS Y CUMPLIMIENTO
-COMPLIANCE-

REQUERIMIENTOS

A) CORPORATIVOS

CÓDIGOS DE GOBIERNO Y ÉTICOS
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 (Códigos Tipo)
CORPORATIVOS (Códigos de Conducta, Códigos Tipo, BCR's)

B) LEGALES

ACUERDOS Y TRATADOS INTERNACIONALES, DERECHO COMUNITARIO, DERECHO ESTATAL, DERECHO AUTONÓMICO

C) CONTRACTUALES

ACUERDOS, CONTRATOS, CONCURSOS, PLIEGOS, LICITACIONES

CONTRACTUALES

PROFESIONALES CERTIFICADOS
(Ejemplo: CISA, CISM)

AUDITORÍAS EXTERNAS CUALIFIFICADAS
(Ejemplo: CISA)

PROFESIONALES Y PERFILES ESPECIALIZADOS
(Ejemplo: Especialización en privacidad -Data Privacy Officer o DPO- o *compliance -Compliance Officer-*)

IMPLANTACIÓN DE ESTÁNDARES
(Ejemplo ISO/IEC 27001 Information Security, ISO 15378 Comercialización de Productos Farmacéuticos bien envasados, Sistema de Gestión de la Calidad para productos sanitarios UNE-EN ISO 13485, UNE-CEN-ISO/TR 14969:2006 Productos sanitarios, UNE-EN ISO 14971:2012 Productos sanitarios, ISO 27789:2013 Health informatics -- Audit trails for electronic health records, ISO/TS 21547:2010 Health informatics -- Security requirements for archiving of electronic health records – Principles, ISO 27799:2008 Health informatics -- Information security management in health using ISO/IEC 27002

SLAs y MEDIDAS DE SEGURIDAD

LEGALES

ACUERDOS Y TRATADOS INTERNACIONALES

DERECHO COMUNITARIO

- Privacidad, cookies y servicios de sociedad de la información
- Salud e historia clínica

DERECHO ESTATAL

- Privacidad, cookies y servicios de sociedad de la información
- Salud e historia clínica
- Farmacia

DERECHO AUTONÓMICO

ISACA
Sistemas de información fiables y valiosos
Valencia Chapter

PRIVACY

NORMATIVA BÁSICA

Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de julio de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Constitución Española, Artículo 18.

LOPD. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Reglamento de Desarrollo de la LOPD aprobado por R.D. 1720/2007, de 21 de diciembre (BOE 19.01.2008).

Novedades introducidas por la Ley 2/2011, de 4 de marzo, de Economía Sostenible

SECTORIAL

Sociedad de la Información, Telecomunicaciones, Salud y Gestión Sanitaria , Estadística, Electoral, Fuerzas y Cuerpos de Seguridad del Estado, etc... EJEMPLO. Ley 41/2002, de 14 noviembre, de Autonomía del Paciente (Ley básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica), Ley 1/2003, de 28 de enero, de derechos e información al paciente de la Comunidad Valenciana, Ley 14/2007, de 3 julio, de Investigación Biomédica, LO 3/1986 de 14 Abr. (medidas especiales en salud pública) , Ley 14/1986 de 25 Abr. (general de sanidad)

Ejemplos:

Ley 41/2002, de 14 noviembre, de Autonomía del Paciente (Ley básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica)

Artículo 14. Definición y archivo de la historia clínica
Artículo 15. Contenido de la historia clínica de cada paciente
Artículo 16. Usos de la historia clínica
Artículo 17. La conservación de la documentación clínica
Artículo 18. Derechos de acceso a la historia clínica
Artículo 19. Derechos relacionados con la custodia de la historia clínica

Ley 1/2003, de 28 de enero, de derechos e información al paciente de la Comunidad Valenciana

Ley 14/2007, de 3 julio, de Investigación Biomédica

Artículo 5. Protección de datos personales y garantías de confidencialidad

1. Se garantizará la protección de la intimidad personal y el tratamiento confidencial de los datos personales que resulten de la actividad de investigación biomédica, conforme a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Las mismas garantías serán de aplicación a las muestras biológicas que sean fuente de información de carácter personal.

2. La cesión de datos de carácter personal a terceros ajenos a la actuación médico-asistencial o a una investigación biomédica, requerirá el consentimiento expreso y escrito del interesado.

En el supuesto de que los datos obtenidos del sujeto fuente pudieran revelar información de carácter personal de sus familiares, la cesión a terceros requerirá el consentimiento expreso y escrito de todos los interesados.

3. Se prohíbe la utilización de datos relativos a la salud de las personas con fines distintos a aquellos para los que se prestó el consentimiento.

4. Quedará sometida al deber de secreto cualquier persona que, en el ejercicio de sus funciones en relación con una actuación médico-asistencial o con una investigación biomédica, cualquiera que sea el alcance que tengan una y otra, acceda a datos de carácter personal. Este deber persistirá aún una vez haya cesado la investigación o la actuación.

5. Si no fuera posible publicar los resultados de una investigación sin identificar a la persona que participó en la misma o que aportó muestras biológicas, tales resultados sólo podrán ser publicados cuando haya mediado el consentimiento previo y expreso de aquélla.

Artículo 8. Trazabilidad y seguridad

Deberá garantizarse la trazabilidad de las células, tejidos y cualquier material biológico de origen humano, para asegurar las normas de calidad y seguridad, respetando el deber de confidencialidad y lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

En el caso de la investigación con células y tejidos destinados a su aplicación en el ser humano, los datos para garantizar la trazabilidad deben conservarse durante al menos treinta años.

Las actividades relacionadas con la investigación biomédica se realizarán con estricta observancia del principio de precaución, con el fin de prevenir riesgos graves para la vida y la salud humanas.

Artículo 51. Deber de confidencialidad y derecho a la protección de los datos genéticos

1. El personal que acceda a los datos genéticos en el ejercicio de sus funciones quedará sujeto al deber de secreto de forma permanente. Sólo con el consentimiento expreso y escrito de la persona de quien proceden se podrán revelar a terceros datos genéticos de carácter personal.

Si no es posible publicar los resultados de una investigación sin identificar a los sujetos fuente, tales resultados sólo podrán ser publicados con su consentimiento.

2. En el caso de análisis genéticos a varios miembros de una familia los resultados se archivarán y comunicarán a cada uno de ellos de forma individualizada. En el caso de personas incapacitadas o menores se informará a sus tutores o representantes legales.

Artículo 51. Deber de confidencialidad y derecho a la protección de los datos genéticos

1. El personal que acceda a los datos genéticos en el ejercicio de sus funciones quedará sujeto al deber de secreto de forma permanente. Sólo con el consentimiento expreso y escrito de la persona de quien proceden se podrán revelar a terceros datos genéticos de carácter personal.

Si no es posible publicar los resultados de una investigación sin identificar a los sujetos fuente, tales resultados sólo podrán ser publicados con su consentimiento.

2. En el caso de análisis genéticos a varios miembros de una familia los resultados se archivarán y comunicarán a cada uno de ellos de forma individualizada. En el caso de personas incapacitadas o menores se informará a sus tutores o representantes legales.

DATOS DE CARÁCTER PERSONAL: Cualquier información concerniente a personas físicas identificadas o identificables, que incluye cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo.

FICHERO: Todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso, automatizado o no (papel).

TRATAMIENTO DE DATOS: Cualquier **o**peración o procedimiento técnico de carácter automatizado o no, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

COMUNICACIÓN O CESIÓN DE DATOS: Tratamiento de datos que supone su revelación a una persona distinta del interesado. Salvo excepciones, se exige el consentimiento previo del interesado para ceder sus datos personales.

RESPONSABLE DEL FICHERO O TRATAMIENTO: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente.

ENCARGADO DEL TRATAMIENTO: La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.

ISACA
Sistemas de información fiables y valiosos
Valencia Chapter

SALUD Y VIDA SEXUAL

ISACA
Sistemas de información fiables y valiosos
Valencia Chapter

TRATATAMIENTO DE DATOS ESPECIALMENTE PROTEGIDOS

IDEOLOGÍA, AFILIACIÓN SINDICAL, RELIGIÓN O CREENCIAS, ORIGEN RACIAL, SALUD O VIDA SEXUAL

- SE DEBE ADVERTIR AL INTERESADO DE SU DERECHO A NO PRESTAR SU CONSENTIMIENTO EN EL TRATAMIENTO DE ESTOS DATOS.
- SE NECESITA CONSENTIMIENTO EXPRESO Y POR ESCRITO DEL INTERESADO PARA EL TRATAMIENTO DE DATOS QUE REVELEN IDEOLOGÍA, AFILIACIÓN SINDICAL, RELIGIÓN Y CREENCIAS.
- SE NECESITA CONSENTIMIENTO EXPRESO O QUE LO DISPONGA UNA LEY PARA RECABAR, TRATAR O CEDER DATOS RELATIVOS A ORIGEN RACIAL, SALUD O VIDA SEXUAL.
- NO SE PERMITE CREAR FICHEROS CON LA ÚNICA FINALIDAD DE ALMACENAR DATOS DE CARÁCTER PERSONAL, QUE REVELEN IDEOLOGÍA, AFILIACIÓN SINDICAL, RELIGIÓN, ORIGEN RACIAL, SALUD O VIDA SEXUAL.
- SE PODRÁN TRATAR, NO OBSTANTE, LOS DATOS ANTERIORES SI RESULTA NECESARIO PARA EL DIAGNÓSTICO MÉDICO O LA ASISTENCIA SANITARIA.

VIT SALUD VALENCIA | INNDEA VALENCIA | AJUNTAMENT DE VALÈNCIA
Red de Innovación en el Sector Salud

PODRÁN SER TRATADOS:

A. Cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.

B. Cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.

PODRÁN SER TRATADOS:

a) Cuando dicho tratamiento resulte necesario para la **prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios**, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.

b) Cuando el tratamiento sea **necesario para salvaguardar el interés vital del afectado o de otra persona**, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.

c) Las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad.

d) Cuando la **cesión se produzca entre Administraciones públicas** y tenga por objeto el tratamiento posterior de los datos con **fines históricos, estadísticos o científicos** no será necesario el consentimiento.

e) Cuando la **cesión** de datos de carácter personal relativos a la salud sea **necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos** en los términos establecidos en la legislación sobre sanidad estatal o autonómica no será necesario el consentimiento.

f) **Cesión/comunicación** de datos a terceros sin consentimiento si están **disociados.**

CALIDAD

PROPORCIONALIDAD

SEGURIDAD

CONFIDENCIALIDAD

PRINCIPIOS Y DERECHOS

INFORMACIÓN PREVIA

CONSENTIMIENTO PREVIO PARA TRATAR O CEDER

SECRETO

ISACA
Sistemas de información fiables y valiosos
Valencia Chapter

ARCO (ACCESO, RECTIFICACIÓN, CANCELACIÓN, OPOSICIÓN)

REVOCACIÓN DEL CONSENTIMIENTO

DERECHO DE CONSULTA

DERECHO AL OLVIDO

DERECHOS DEL INTERESADO

TUTELA

INDEMNIZACIÓN

VIT SALUD VALENCIA | InnDEA VALENCIA | AJUNTAMENT DE VALÈNCIA

Red de innovación en el Sector Salud

ISACA
Sistemas de información fiables y valiosos
Valencia Chapter

REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS

VIT SALUD VALENCIA | INNDEA VALENCIA | AJUNTAMENT DE VALÈNCIA
Red de Innovación en el Sector Salud

ISACA
Sistemas de información fiables y valiosos
Valencia Chapter

COORDENADAS BÁSICAS

VIT SALUD VALENCIA | INNDEA VALENCIA | AJUNTAMENT DE VALÈNCIA
Red de Innovación en el Sector Salud

- Data Privacy Officer (DPO) - Responsable de Seguridad
- *Privacy by design/privacy by default*
- Evaluación de impacto de la privacidad (PIA)
- Auditoría
- Responsabilidad y *accountability* del responsable
- Derecho al olvido
- Portabilidad
- Seguridad
- Accesos en función de necesidad de saber
- Conservación durante el tiempo estrictamente necesario
- Autorizaciones y consultas previas a la autoridad de control
- Endurecimiento transferencias intenacionales
- Régimen sancionador (100.000.000€/5%volumen de negocio)
- *Compliance* global

POSIBLES MODIFICACIONES DEL TEXTO FINAL

Versión Consejo junio 2015

Pseudoanonimización: tratamiento de datos personales que no permite identificar a una persona sin otra información adicional que, a su vez, se encuentra separada, existiendo medidas técnicas que no permitan la identificación.

Minoración de competencias DPO

Brechas de seguridad (comunicación)

Modificaciones régimen sancionador

COORDENADAS BÁSICAS PARA PROYECTOS EN MATERIA DE SALUD ELECTRÓNICA

Intervención de expertos
Privacy/security by design/privacy by default
Información/consentimiento previo
Calidad y proporcionalidad
Seguridad
Confidencialidad y secreto
Portabilidad
Derechos
Investigación histórica, estadística o científica
Disociación/Anonimización como opción preferente, conservación separada y publicación limitada
Conservación (¿5-15-20-indefinida?)

ISACA
Sistemas de información fiables y valiosos
Valencia Chapter

OTRAS CUESTIONES DE ACTUALIDAD

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 Red Global de Control de la Privacidad (GPEN)

-**Proyecto CIPHER** (Recomendaciones y buenas prácticas para prevenir el cibercrimen)

-**Big Data**. Business Intelligence, Analítica predictiva. Privacy. Problemas: Almacenamiento, búsqueda, compartición, análisis, visualización, compliance.

(*) 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.

-***Privacy by Design, Privacy by Default, Privacy Impact Assesment (PIA)***

-**Proyecto europeo SURPRISE "*Vigilancia, privacidad y seguridad*"**

-Informe "***Responsabilidades legales ante un ciberataque***"

-Cookies. "***European Cookie Sweep***" (Septiembre 2014)

-**Dictamen sobre Internet de las cosas y sus riesgos** (Septiembre 2014)

Grupo de Trabajo del Artículo 29. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

ISACA
Sistemas de información fiables y valiosos
Valencia Chapter

¡Gracias por su atención!

vicepresidente@isacavalencia.org

www.isaca.org
www.isacavalencia.org

VIT SALUD VALENCIA | InnDEA VALENCIA
AJUNTAMENT DE VALÈNCIA
Red de Innovación en el Sector Salud