

Edita

Ediciones CODA, S.L.
 Doctor Esquerdo, 28; S-1º-D
 28028 Madrid (España)
 Tels: 91-401 06 26/91-309 04 99
 Fax: 91-401 09 90
 Correo-e: coda2@jet.es

Editor

Luis Guillermo Fernández Delgado

Director

José de la Peña Muñoz

Sección Laboratorio SIC

Javier Areitio Bertolin

Colaboran en este número:

Andrés Bermejo Miguel
 Oscar Conesa Ribelles
 Juan Carlos Cruellas
 Marta Cruellas
 Jorge Dávila Muro
 José de la Peña Sánchez
 José Mª González Zubieta
 Sandra Hernández
 Peter Höjerback
 Roberto López Navarro
 Marc Martínez
 Manel Medina Llinás
 Javier Jarauta Sánchez
 Ramón Pinuaga Cascales
 Benjamín Ramos Álvarez
 Arturo Ribagorda Garnacho
 Lluís Salas Areny

José María Sierra Cámara
 Manuel Tascón Álvarez

Coordinación de**Marketing/Publicidad:**

Maria Victoria Colino

Departamento de Suscripciones:

Susana Montero

Fotografía:

Jesús A. de Lucas

Ilustraciones:

Access360, Adecco, Allasso, Allianz,
 Amena, Axent, Bankpyme, Baltimore,
 C2, CA, Check Point, Danu, e-certchile,
 eVeritas, Ernst & Young, ESTIO,
 FESTE, GTA, Identix, ipsCA, ISS,
 Nakua, Precise Biometrics, Ra-Ma,
 SIA, Safelayer, StoneSoft, Symantec,
 TransIndigo, Trend Micro, Sybari,
 VeriSign

Diseño y Producción

EXTRA Comunicación Gráfica

Tel: 91-562 36 28/37 97

Diseño y Maquetación:

Miguel Salgueiro

Elena Suárez

Fernando Halcón

Imprime: Gráficas Ruiz Polo, S.A.

ISSN: 1136-0623

Depósito Legal: GU-132/96

SIC SEGURIDAD EN INFORMÁTICA Y COMUNICACIONES no comparte necesariamente las opiniones vertidas por los autores de los artículos. Prohibida la reproducción total o parcial de cualquier información gráfica o escrita publicada en SIC sin autorización escrita de la fuente.

Editorial



Imagen portada:
ESTIO

El largo camino hacia las normas internacionales

A nadie le resulta ajeno el hecho de que para hacer ciertas cosas con fundamento, convendría que en la mayoría de países todos estuviéramos interesados en hablar exactamente de lo mismo, que es la forma más humanamente razonable de conseguir una confluencia en el significado de los conceptos y el punto de partida para ponerse de acuerdo y mover las iniciativas globales en una suerte de coherencia entre los usuarios, los fabricantes y los intrincados matices de las leyes y sus consecuencias. Esto ha empezado ya a suceder en el mundo de la calidad. Pero, ¿qué pasa en el de la seguridad?

Hay, fundamentalmente, cuatro necesidades de contexto: primera, disponer de normas cualitativas de seguridad de la información; segunda, disponer de normas técnicas que garanticen la seguridad y la interoperabilidad de los productos; tercera: que con las dos anteriores se puedan cumplir las legislaciones, y cuarta, tiempo. No hay que engañarse, las cosas llevan su tiempo.

Vayamos por partes, y entendamos la idea en el conglomerado –a veces amorfo– formado por EE.UU./Canadá, Australia/Nueva Zelanda y la UE, aunque ello parezca muy restrictivo.

Normas cualitativas

Hay buenas noticias, ya que al parecer ISO, estaría adoptando el estándar británico BS 7799 como ISO 107799. Básicamente esto significa que se podrían implantar sistemas de alto nivel en la materia, y que, quizá, con el paso del tiempo y la experiencia, pueda alguna vez ‘certificarse’ la implantación de la norma con el alcance y las limitaciones pertinentes en una suerte de proceso continuado para, en última instancia, ir gestionando el riesgo ayudados por esas herramientas indispensables que son el control y las auditorías y/o revisiones.

Normas técnicas

Aquí la cosa está más negra, porque la onda de las necesidades de las organizaciones para apoyar en las TIC su negocio está algo desfasada –en términos generales– con la onda de las presiones que sufren los fabricantes y desarrolladores (*time-to-market*), deseosos legítimamente de comerse el mercado y elevar sus productos y enfoques tecnológicos a la categoría de estándares, con lo cual se tienen un montón de estándares de facto para cada cosa (algunos más de facto que otros, claro está). Este panorama afecta de forma irremisible a la interoperabilidad, gran caballo de batalla.

Ya lo resumió de modo contundente en la pasada edición de SIC (septiembre) el Responsable del Departamento de Seguridad de uno-e.com, Santiago Moral Rubio: «*Aunque los fabricantes y los organismos de estandarización están trabajando en esta línea (la estandarización y la interoperabilidad), la situación actual provoca la existencia de distintos mecanismos de*

seguridad que, o bien no pueden integrarse entre sí, o bien hacen muy compleja las tareas de integración e implantación. Al mismo tiempo, los procesos de toma de decisión, en el momento de incorporar mecanismos de seguridad a nuestras arquitecturas, se complican al contar con funcionalidades aparentemente diferentes en productos de distintos fabricantes que deberían tener un comportamiento homólogo». Siempre queda la esperanza.

En lo que compete específicamente a la seguridad de los productos de TIC, existen los Criterios Comunes (ISO 14408). Algunos países tienen estructuras de evaluación y certificación de la seguridad a efectos, digamos, civiles. En España, aunque estamos adheridos al Acuerdo de Reconocimiento Mutuo de Certificados, no tenemos esquema publicado, algo de todo punto impresentable en estas fechas para un Estado que quiere situarse en el grupo de cabeza de los de la UE. En seguridad, señores, también hay diferencias, para desgracia de la incipiente industria española dedicada al desarrollo de productos tecnológicos de seguridad, en general malhadada y huérfana de comprensión, apoyo e igualdad de oportunidades.

Leyes

Tercer asunto en juego. Hoy existe legislación sobre firma electrónica y prestadores de servicios de certificación electrónica, y sobre ‘privacidad’, lo que ha polarizado el debate de la seguridad de la información (aspectos penales aparte). En lo referente a las primeras hay un entendimiento razonable con EE.UU., justo lo que no pasa con la segunda, la ‘privacidad’. La idea continental de las garantías, de los derechos..., se lleva de patadas con la concepción anglosajona de los sistemas de control privados y los códigos éticos. Ejemplos de ello son los «Principios de Puerto Seguro», rechazados por el Grupo del Artículo 29 de la Directiva y por el Parlamento Europeo, aunque la Comisión haya dictado una Decisión que podría permitir las transferencias de datos personales a EE.UU., país sin legislación federal en la materia y sin órgano de control.

Sin embargo, aquí, en España, tenemos legislación sobre firma-e –eso sí, insuficientemente desarrollada y, en principio, sometida a un futuro cambio formal–, LOPD y Reglamento de Medidas de Seguridad, y las políticas de ‘privacidad’ de las organizaciones tienen que cumplir escrupulosamente las normas y lo que se pudiera indicar en posibles Instrucciones futuras de la Agencia de Protección de Datos. Y eso es, en síntesis, lo que hay al cierre de este número.

Tiempo

El cuarto asunto. Dicen que lo arregla todo. O lo estropea, según se mire. Por cierto, y ya que se habla de tiempo, quizá merezca la pena recordar que esta edición de SIC es la última del año postrero del siglo XX, segundo milenio. La próxima verá la luz, según lo previsto, en el primer año del siglo XXI, tercer milenio. Todo un acontecimiento. Feliz salida y entrada.