ESPECIAL

"Marcos y Normas"

Tecnología & Sentido Común

DE

ESPECIAL

AGOSTO 2024

ESPECIAL

"Marcos y Normas"

Tecnología & DE Sentido Común

EDITA
Business, Technology & Best Practices, S.L.
Av. San Onofre, 20
46930-Quart de Poblet (Valencia)
Teléfono: 96 109 44 44
Fax: 96 109 44 45
https://tecnologiaysentidocomun.com
soluciones@businessandcompany.com

Renato Aquilino

Licenciado en Informática por la Universitat Politécnica de Catalunya. E.U. en Protección de Datos y Privacidad por la Facultad de Derecho de la Universidad de Murcia. CISA, CISM, CGEIT, COBIT 5 Implemen- ter, Lead Auditor ISO 27001-TC y Auditor del Esquema Nacional de Seguridad. Carrera profesional desarro- llada en Ingeniería de sistemas, DBA y, principalmente, consultoría y auditoría sobre marcos y normas asociadas a la seguridad de la información, tanto en sector público como privado. Colaborador de ISACA HQ desde 2004, autor de numerosas publicaciones, cursos y ponencias sobre estas materias, miembro del COIICV, ISACA, itSMF España, APEP e ISMS Forum.

LinkedIn:
https://www.linkedin.com/in/renatoaquilino

ISSN 2951-8180

Escuela de Gobierno
eGob®
https://escueladegobierno.es

LIVE STREAMING

Sesión de Formación y Certificación en:

Sistema de Gestión de la Inteligencia Artificial

Director Académico:

Javier Peris

- Duración 5 horas
- Sesión única
- Miércoles de 16:00 a 21:00 horas
- En Directo y en Remoto
- Basado en la norma ISO 42001:2023
- Examen de Certificación Incluido
- Certificación ISO 42001 Leader
- Plazas limitadas

MPPM® MGEIT® eGob®

Miércoles 10 de Abril

+ 34 96 109 44 44
campus@escueladegobierno.es

ESPECIAL AGOSTO 2024

índice

DE CONTENIDOS

https://tecnologiaysentidocomun.com

¡ndice

#TYSC

Premios recibidos

Premio 2016 a la Difusión de los Valores de la Gestión y Gobierno TI

El Foro de Profesionales de la Gestión del Servicio en España itSMF otorga a «Tecnología y Sentido Común» el Galardón 2016 a la Difusión de los Valores de la Gestión y Gobierno de Tecnologías de la Información.

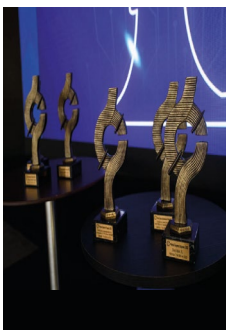
itSMF ESPAÑA

Premio Medio de Comunicación 2018 de la Asociación Profesional Española de Privacidad

La Junta Directiva de la Asociación Profesional Española de Privacidad durante su VI Congreso Nacional de Privacidad APEP celebrado en Madrid otorga el Premio Medio de Comunicación 2018 a Tecnología y Sentido Común #TYSC

apep

Tecnología y Sentido Común "Premio Sapiens" Medio de Comunicación 2022



El Colegio Oficial de Ingeniería Informática de la Comunidad Valenciana entregó el Premio Sapiens Medio de Comunicación 2022 a nuestra Revista "Tecnología y Sentido Común #TYC". El Colegio Oficial de Ingeniería Informática de la Comuni- dad Valenciana COIICV alabó tanto la gran labor de difusión que viene realización Tecnología y Sentido Común desde hace siete temporadas como su capacidad de adaptación y resiliencia adaptándose a nuevos formatos con los que continuar en su labor de evangelización en Buenas Prácticas al conjunto de los profesionales a pesar de la alerta sanitaria con nuevos formatos que partiendo de un programa de Radio y Podcast han permitido seguir llevando su mensajes a través de la Revista Mensual, o el informativo televisivo "El Semanal" de Tecnología y Sentido Común.

COLEGIO OFICIAL DE INGENIERÍA INFORMÁTICA DE LA COMUNITAT VALENCIANA

Premio 2022 ESET al Periodismo y Divulgación eb Seguridad Informática

VI Premios ESET Periodis- mo y Divulgación: Tecnología y Sentido Común Premiada en la Categoría Blogs por el Articulo de Ricard Martínez "Seguridad en el Smartphone".
Los Premios ESET apuestan por la educación y la concienciación de la sociedad en materia de ciberseguridad, y los medios de comunicación son esenciales en este cometido.
Los periodistas y divulgadores son fundamentales para difundir el conocimiento necesario que permita a los usuarios disfrutar de la tecnología de una manera más segura.
Estos VI Premios ESET pretenden fomentar la divulgación de la ciberseguridad.

eset

Agradecimiento de la Asociación Valenciana de Informática Sanitaria AVISA

La Asociación Valenciana de Informática Sanitaria AVISA durante las XIV Jornadas Técnicas que bajo el título "20 Años Implantando TIC en Sanidad" se celebraron en Benidorm en febrero de 2024 hizo entrega de su agradecimiento a Tecnología y Sentido Común por su apoyo y visibilidad a la profesión.

AVIS@ ASOCIACIÓN VALENCIANA DE INFORMÁTICA SANITARIA

Escuela de Gobierno

eGob®

https://escueladegobierno.es

Curso de Doble Certificación en:

Gestión Documental y Gestión del Conocimiento

ISO 30301:2021
ISO 30401:2021

Dirección Académica:
Javier Peris

- Dos formatos para tu comodidad
- Opción A: Remoto en Directo
- Opción B: Virtual con Tutoría
- Basado en las Últimas Normas ISO
- Exámenes de Certificación Incluidos
- Certificación ISO 30300 Leader
- Certificación ISO 30401 Leader
- Solicita tu admisión

MPPM® MGEIT® eGob®

Próxima Convocatoria en Directo
Septiembre 2024

Solicita tu admisión en:

+ 34 96 109 44 44
admisiones@escueladegobierno.es

MAGERIT V3 y PILAR en el Reino de los Riesgos.

Abordamos una nueva temporada analizando la metodología MAGERIT V3 para el desarrollo del proceso de análisis y gestión de riesgos, así como PILAR, plataforma de automatización del proceso que, con sus fans y haters, aporta un alto valor añadido y ayudas automatizadas al modelado de todos los acores y a los cálculos relacionados. Yo soy fan.

METODOLOGÍA MAGERIT V3

MAGERIT, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) fue creada por el Consejo Superior de Administración Electrónica del Gobierno de España y, a la fecha, está vigente su versión 3.

Está incluida en el catálogo de metodologías de Análisis y Gestión de Riesgos (AGR en adelante) de ENISA (European Union Agency for Cibersecurity): https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_magerit.html)

Ha sido adoptada principalmente por la Administración Pública, si bien es aplicable a todos los sectores.

En mi opinión, es una metodología muy completa que permite representar en detalle los activos de una organización **y sus dependencias,** lo que facilita unas valoraciones precisas de dichos activos en base a su criticidad.

La documentación de MAGERIT es completa y detallada, contenida en tres documentos (Método, Catálogo y Guía de Técnicas), ofreciendo información relevante sobre los fundamentos y bases matemáticas que sustentan la metodología.

ACTIVIDADES MAGERIT V3 (Libro I – Método)

Las actividades propuestas son las habituales en todas las metodologías AGR de referencia, si bien MAGERIT V3 distingue entre "activos esenciales" y "activos de soporte".

1.Identificación de los activos esenciales: es decir, la información que se trata y los servicios que se prestan

2.Valoración de las necesidades o niveles de seguridad requeridos por cada activo esencial en cada dimensión de seguridad (confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad).

3.Identificación de los demás activos del sistema, denominados activos de soporte, incluyendo personal, aplicaciones, servidores, comunicaciones / redes, servicios en la nube, CPDs, etc, que materializan los activos esenciales. **Debe determinarse un nivel de granularidad de los activos que permita una gestión adecuada de sus riesgos sin generar un número de activos inmanejable.**

4.Establecimiento del valor (o nivel requerido de seguridad) de los demás activos en función de su relación con los activos esenciales (idealmente mediante identificación de las dependencias).

5.Identificación de amenazas posibles sobre los activos (ver documento "Catálogo").

6.Estimación de las consecuencias que se derivarían de la materialización de dichas amenazas.

7.Estimación de la probabilidad de que dichas amenazas se materialicen

8.Estimación de los impactos y riesgos potenciales, inherentes al sistema.

9.Identificación de las salvaguardas apropiadas para atajar los impactos y riesgos potenciales.

10.Valoración del despliegue de las salvaguardas identificadas.

11.Estimación de los valores de impacto y riesgo residuales = nivel de impacto y riesgo que aún soporta el sistema tras el despliegue de las salvaguardas.

12.Comparación de los valores de riesgo residual con los valores aceptables por la Organización. En caso de no ser aceptables, iterar nuevamente desde el punto 9 hasta llegar a niveles aceptables. Estos niveles aceptables deben establecerse, modificarse (en su caso) y aprobarse por los estamentos directivos de la Organización.

MAGERIT V3 EN SU CONTEXTO

Dentro del concepto "análisis y gestión de riesgos" existen diferentes metodologías y aproximaciones para su materialización, principalmente OCTAVE, CRAMM, NIST SP800-30, CLUSIF MEHARI e ISO/IEC 31000:2018+ISO/IEC 27005:2022. Los fundamentos de todas ellas contienen numerosas similitudes, si bien este artículo no tiene como objetivo analizarlas ni compararlas.

Los marcos normativos y estándares para la construcción de un SGSI **no están asociados a metodología AGR concretas**, siendo decisión de cada entidad la elección de aquélla que consideren adecuada a su SGSI concreto. Sin embargo, es una realidad que los SGSI de la Administración Pública española, basados en el ENS, suelen seleccionar MAGERIT V3, mientras que los SGSI basados en ISO/IEC 27001:2022 suelen desarrollar su AGR sobre ISO/IEC 31000:2018+ISO/IEC 27005:2022.

CONTINÚA EN PRÓXIMA PÁGINA

AUTOMATIZACIÓN DEL PROCESO
El desarrollo, mantenimiento y evolución del AGR sólo puede gestionarse adecuadamente mediante un sistema de información específico que permita el modelado de activos, dependencias, niveles de seguridad, asociación de amenazas, determinación de probabilidades e impactos inherentes, asociación de salvaguardas y los iterativos cálculos del impacto y riesgo residual.

Existen en el mercado diferentes soluciones que ofrecen estas funcionalidades, pero en este artículo me centro en PILAR, muy especialmente por **ser gratuita para la Administración Pública y ser la más utilizada en este sector.**

PILAR es una de las aportaciones más relevantes de José Antonio Mañas, catedrático de la UPM y una de las personas con mayores contribuciones en materia de métodos, guías, normativas y herramientas para los SGSI.

PILAR es una plataforma binaria: o la amas o la odias, aunque admite amor – odio por temporadas o casos.

En mi caso le profeso mucho amor dado que, una vez "aterrizado" su peculiar interfaz de usuario y comprendido sus razonamientos (ver Libro III – Guía de Técnicas de MAGERIT V3) PILAR ofrece una valiosa colección de ayudas automatizadas para el AGR, incluyendo medidas y controles para referenciales del SGSI como ENS e ISO/IEC 27001, así como los riesgos sobre los derechos y libertades de las personas asociados al RGPD y también el Análisis de Impacto en el negocio (BIA) en su versión BCM.

Su nivel de aportación y proactividad para facilitar el proceso permite acortar los tiempos de desarrollo del AGR, dado que propone de forma automática valores, amenazas y salvaguardas, siendo este comportamiento plenamente configurable para ajustarlo a las preferencias de cada Organización.

Por otra parte, permite analizar el resultado de diferentes procesos AGR en el tiempo, con lo cual puede evaluarse la evolución de sus resultados, ayudando a la toma de decisiones mediante una información relevante y proyectada en el tiempo.

Permite elegir entre visión cuantitativa y cualitativa. Yo siempre utilizo la visión cuantitativa, dado que permite una mayor precisión en los resultados que la cualitativa, si bien ésta última es útil para entornos sencillos con un pequeño volumen de activos implicados.

CONCLUSIONES
Este inicio de temporada empieza con una confesión: **me gusta PILAR**. Por favor, no disparen.

Escuela de Gobierno

eGob®

https://escueladegobierno.es

Curso de Doble Certificación en:

Inteligencia Estratégica y Gestión de la Innovación

ISO 56002:2019
ISO 56006:2021

Dirección Académica:
Javier Peris

- Dos formatos para tu comodidad
- Opción A: Remoto en Directo
- Opción B: Virtual con Tutoría
- Basado en las Últimas Normas ISO
- Exámenes de Certificación Incluidos
- Certificación ISO 56002 Leader
- Certificación ISO 56006 Leader
- Solicita tu admisión

MPPM® MGEIT® eGob®

Próxima Convocatoria en Directo
Septiembre

Solicita tu admisión en:

+ 34 96 109 44 44
campus@escueladegobierno.es

OWASP – Marco de referencia para la securización de aplicaciones (AppSec)

Open Worldwide Application Security Project **(OWASP)** es una **fundación sin ánimo de lucro** que trabaja para mejorar la seguridad del software. Sus diferentes proyectos aportan una amplia cantidad de criterios y utilidades de verificación, hasta el punto de convertirse en una plataforma de conocimiento universalmente aceptada como estándar para AppSec.

CONTEXTO

El desarrollo de aplicaciones seguras es una necesidad indiscutible ante la dependencia prácticamente absoluta de toda organización, pública o privada, de sus sistemas de información para el desarrollo de su modelo de negocio o servicio. Las aplicaciones materializan este modelo dotando a la organización de las funcionalidades adecuadas para la realización de las transacciones de negocio y todas sus derivadas.

RIESGOS RELACIONADOS CON APLICACIONES

Este escenario, trasladado a una evaluación simplificada de riesgos, asigna a los activos de tipo "aplicación" un valor alto en la dimensión "disponibilidad" debido a la mencionada dependencia e incapacidad de suplir su indisponibilidad por medios manuales. Por supuesto, esta es una generalización por motivos de espacio en el artículo que debe, en los escenarios reales, ser estudiada y formar parte de un Análisis de Impacto en el Negocio (BIA) donde las aplicaciones son activos de soporte a los servicios corporativos. En la dimensión "confidencialidad" de la información, debe tenerse el modelo de clasificación de datos que asigne valor corporativo (p.e. desarrollo de productos), regulatorio (p.e. datos personales), etc, a la confidencialidad. A su vez, la dimensión "integridad" de la información recibe valor alto dado que la falta de integridad puede corromper, alterar y desvirtuar su exactitud y completitud, originando un grave problema a la organización al desarrollar su modelo basándose en una información incorrecta. En la ecuación del riesgo interviene fundamentalmente el valor del activo, la probabilidad de que se materialicen las amenazas a las que puede estar expuesto, explotando sus vulnerabilidades, y el impacto que supondría su materialización. Posteriormente, deben identificarse las salvaguardas aplicables para mitigar la probabilidad y el impacto y calcular el riesgo residual tras su aplicación, hasta llegar a un nivel de riesgo aceptable para la organización. Aquí entra OWASP.

OWASP TOP 10

Este "ranking", cuya última versión está datada en 2021, clasifica las 10 vulnerabilidades más comunes para la seguridad de las aplicaciones, y es un referente muy utilizado para priorizar las iniciativas de securización. El catálogo de vulnerabilidades que utiliza es el CWE. En la versión de 2021 la clasificación es:

A01 – Pérdida del control de acceso.
A02 – Errores criptográficos.
A03 – Inyección.
A04 – Diseño inseguro.
A05 – Configuración incorrecta de seguridad.
A06–Componentes vulnerables y/o desactualizados.
A07 – Errores de identificación y autenticación.
A08 – Problemas de integridad en el software y/o los datos
A09 – Carencias en registro y monitorización.
A10 – Falsificación de solicitudes en el lado del servidor.

La elaboración de esta clasificación está basada en un gran número de pruebas y reportes, lo que le confiere un razonable grado de confiabilidad. La información ofrecida es significativa y puede ampliarse mediante otros proyectos de OWASP. El acceso completo está en https://owasp.org/Top10/es/

OWASP APPLICATION SECURITY VERIFICATION STANDARD (ASVS)

Un complemento de OWASP TOP 10 es el ASVS, proyecto que ofrece un marco referencial para la verificación de la seguridad de las aplicaciones. Debe tenerse en cuenta que OWASP TOP 10 es un marco enumerativo, descriptivo y "medicinal", pero no ofrece en sí mismo unos indicadores de verificación de las recomendaciones ofrecidas, algunas de ellas complicadas de evaluar (p.e. A04-Diseño inseguro).

El ASVS ofrece, en su versión vigente a la fecha (4.0.3 de octubre de 2021), un amplio conjunto de criterios de verificación, basados principalmente en NIST y PCI-DSS y, al igual que otros marcos referenciales, dispone de una clasificación L1 a L3 que aporta proporcionalidad a los requerimientos. Está estructurado en 14 capítulos, cubriendo una amplia temática de auditoría:

V1 Arquitectura, Diseño y Modelado de Amenazas
V2 Autenticación
V3 Gestión de sesiones
V4 Control de Acceso

CONTINÚA EN PRÓXIMA PÁGINA

V5 Validación, Sanitización y Codificación
V6 Criptografía
V7 Manejo y Registro de Errores
V8 Protección de Datos
V9 Comunicaciones
V10 Código Malicioso – Integridad del código
V11 Lógica de Negocio
V12 Archivos y Recursos
V13 API y Servicios Web
V14 Configuración

El ASVS puede ser muy útil para la elaboración de listas de auditoría para la seguridad de aplicaciones dentro de la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en otras normas, como ENS y familia ISO/IEC 27K. En la norma ISO/IEC 27002:2022 se mencionan diferentes documentos OWASP como referencia, así como en la norma ISO/IEC 27031:2023 – *Guidelines for Internet Security y otras, mientras que la medida del ENS mp.s.2 - Protección de servicios y aplicaciones web* requiere un conjunto de verificaciones plenamente alineadas con las contempladas en el ASVS e incluidas en OWASP TOP 10.

OTROS PROYECTOS OWASP

En este artículo he mencionado los dos proyectos que, a mi juicio, aportan mayor valor añadido a la securización de aplicaciones, pero la lista es amplia y recomiendo encarecidamente su consulta, ya que el valor añadido que aportan, **a coste cero**, es inmenso. Accesibles en: https://owasp.org/projects/

CONCLUSIONES

Los marcos normativos y estándares referenciales en materia de SGSI, incluyan o no catálogo propio de medidas, **no excluyen en absoluto** la adopción de otras medidas que puedan complementar las propias. En el caso de las aplicaciones web, OWASP ofrece una cantidad ingente de información valiosa para la implementación y auditoría de la seguridad en las aplicaciones, muy especialmente en las aplicaciones web, arquitectura que, a la fecha, constituye el estándar "de facto" y, por ello, son objetivo de ataques especializados que pueden comprometer su disponibilidad y la confidencialidad e integridad de su información.

OWASP ofrece gratuitamente estos referenciales, pero admite suscripciones y donaciones para reforzar sus capacidades. Yo pago mi suscripción y lo seguiré haciendo, pocas inversiones tiene un ROI tan elevado e inmediato como OWASP.

OWASP CHAPTERS

Al igual que otras organizaciones, OWASP se estructura geográficamente en Chapters. A la fecha, el único Chapter de OWASP en España está en Sevilla: https://owasp.org/www-chapter-sevilla/

Escuela de Gobierno
eGob®
https://escueladegobierno.es

LIVE STREAMING

Curso de
Doble Certificación

Gobierno del Tiempo y Gestión de la Productividad

Director Académico:
Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación TSG4® Yellow Belt
- Certificación UNE 71404 Executive
- Módulo 1: MasterGEIT®
- Módulo 1: MasterPPM®

MPPM® MGEIT® eGob®

Del 15 al 23 de marzo

+ 34 96 109 44 44
campus@escueladegobierno.es

Certificaciones sobre “seguridad”. Seamos realistas.

Los continuos ataques informáticos exitosos que están sufriendo entidades públicas y privadas que disponían de certificaciones en materia de seguridad para sus sistemas de información cuestionan la confianza en dichas certificaciones.

CONFIANZA EN LA SEGURIDAD

La “necesidad de confianza” en la seguridad de la información y los servicios ha conllevado la creación de normativas y estándares (p.e. ENS, ISO/IEC 27K) con el fin de ofrecer referenciales y certificaciones sobre una materia nuclear como ésta. Las certificaciones generan una alta expectativa - interna y externa - de seguridad, ya que suponen la construcción de un Sistema de Gestión de Seguridad de la Información (SGSI) que supera un proceso de auditoría reglado por un esquema de certificación formal. Todo ello aporta en principio la confianza en la seguridad que toda organización requiere.

En la realidad se producen brechas de seguridad, algunas de alto impacto, sobre organizaciones certificadas, algo que lleva invariablemente a cuestionar el valor de las certificaciones conseguidas al verse defraudadas las expectativas de seguridad generadas. En este contexto, **seamos realistas**.

DEBILIDADES DEL PROCESO DE CERTIFICACIÓN – FOTO vs PELÍCULA

Voy a centrarme sobre el ENS e ISO 27K y voy a expresar mi opinión como implantador y auditor de ambas.

En primer lugar quiero mencionar una obvia debilidad del proceso de certificación, ya que certifica una “foto” de la organización en una fecha determinada, cuando la seguridad de la información y los servicios es una película continua en la que una escena romántica puede convertirse en un drama posteriormente. Es cierto que todas las normas certificables requieren un proceso de mejora continua y monitorización permanente, pero la casuística de los ataques y las brechas de seguridad consecuentes pueden dejar obsoleto un “fotograma de conformidad” con el paso del tiempo.

La validez de una certificación ENS es de 2 años, mientras que, en el caso de ISO/IEC 27001 es de 3 años, si bien existen auditorías de seguimiento anuales que auditan una parte del SGSI. Estos periodos de tiempo entre auditorías de certificación tienen un efecto muy diferente en las organizaciones, y aquí **es importante hablar muy claro.**

CONTINÚA EN PRÓXIMA PÁGINA

• **Organizaciones concienciadas.** Su objetivo fundamental es la implementación de un SGSI que aporte garantías de seguridad a su modelo de negocio o servicio. La obtención de la certificación es una consecuencia directa de su objetivo fundamental y existe un compromiso institucional, emanado desde su Dirección, de mantener y mejorar su SGSI como un activo corporativo. Estas organizaciones no están inmunizadas en absoluto contra las amenazas, pero la evolución permanente y continua de su SGSI permite prevenir, detectar, actuar y aprender de sus brechas de seguridad, aprobando las inversiones necesarias.

• **Organizaciones "interesadas".** Su objetivo fundamental es obtener la certificación al ser un requerimiento normativo o condición de sus clientes o proveedores. Habitualmente no valoran el SGSI por su valor intrínseco sino por las consecuencias comerciales que puede tener la pérdida de la certificación. En estos casos el periodo entre certificaciones suele derivar en una sustancial "relajación" de las medidas de seguridad acreditadas en la auditoría, con el consecuente aumento de las brechas de seguridad. Este tipo de organización suele percibir el SGSI como "burocracia", minimizan las inversiones en materia de seguridad y, en caso de que desaparezca el requerimiento de certificación, no renuevan ésta.

La certificación ENS o ISO/IEC 27001 es igualmente válida para ambos tipos de organización, pero, obviamente, la **confianza en la seguridad** que debería aportar es muy diferente en cada caso.

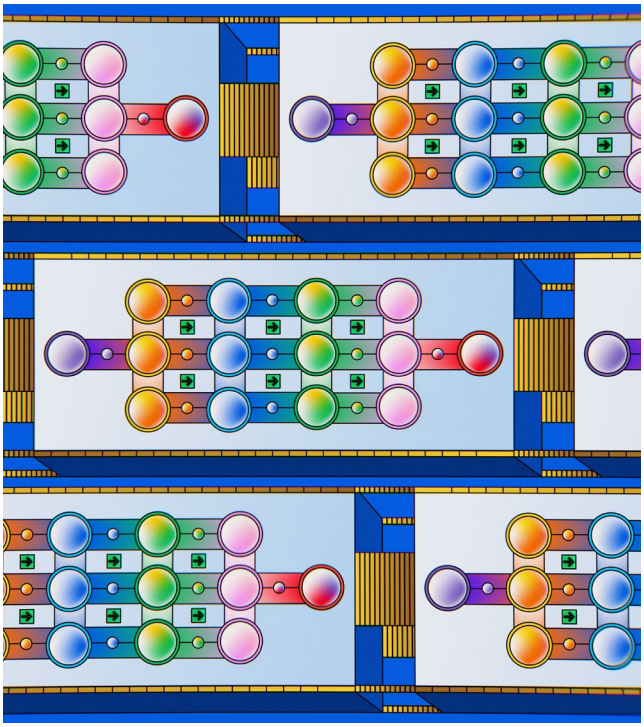
DEBILIDADES DEL PROCESO DE CERTIFICACIÓN INHERENTES AL PROCESO

Las auditorías de certificación ENS e ISO/IEC 27001 se centran, expresado en forma muy simplificada, en verificar que la organización cumple con los requerimientos de la norma en su aspecto documental – **di lo que haces** – y en su correspondiente aspecto material – **haz lo que dices** – documentando los hallazgos de conformidad y no conformidad y las evidencias que los sustentan.

No es objeto de este artículo analizar las diferencias (significativas) entre la auditoría del ENS y de ISO/IEC 27001, pero ambas tienen un punto en común: **las jornadas de auditoría de certificación**. El número mínimo de jornadas y el precio por jornada que cada entidad certificadora oferta está acotado en el caso del ENS en función de la categoría del sistema a auditar, mientras que, en el caso de ISO/IEC 27001 no existe un estándar predeterminado.

Es decir, el número de jornadas **es un factor comercial** que, en un entorno de mercado competitivo, suele derivar en ofertas donde se ajusta este parámetro al máximo ya que la adjudicación depende del presupuesto ofertado y éste depende sustancialmente del número de jornadas. Obviamente, los conocimientos y la experiencia del auditor son factores clave.

Este escenario deriva frecuentemente en auditorías de certificación donde el tiempo necesario real para una auditoría completa y profunda sería superior a las jornadas contratadas, resultando en diferentes niveles de profundidad en las verificaciones del auditor y, con ello, en la calidad de las evidencias y opiniones de auditoría.



Por otra parte, las personas auditoras están a, su vez, acreditadas para desarrollar esta función, pero su "percepción de conformidad" ante un mismo escenario auditado puede variar sustancialmente y, en algunas ocasiones, estar sujeto a presiones a las que cada persona puede responder de forma muy diferente.

Existen mecanismos de auditoría sobre muestras de auditorías de certificación, que han conllevado en ocasiones a la retirada de la acreditación, pero son claramente insuficientes.

CONCLUSIONES

Disponer de una certificación ENS e/o ISO/IEC 27001 aporta un alto valor añadido a cualquier organización, pública o privada, pero no supone en absoluto inmunidad ante ataques sobre la seguridad de la información y/o servicios que la organización certificada aporta.

El proceso de implantación y certificación de un SGSI siempre mejora los niveles de seguridad y aporta una mayor confianza en la seguridad, pero la frase "estoy certificado" no implica en absoluto que deba confiarse ciegamente en los niveles de seguridad de quien la pronuncia, máxime si pertenece al modelo "organización interesada", algo relativamente fácil de detectar.

Escuela de Gobierno

eGob®

https://escueladegobierno.es

LIVE STREAMING

Curso de
Doble Certificación

Análisis de Negocio y Gestión por Procesos

Director Académico:

Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación BPA Leader
- Certificación BPM Executive
- Módulo 2: MasterGEIT®
- Módulo 2 MasterPPM®

MPPM® MGEIT® eGob®

Del 5 al 13 de abril

+ 34 96 109 44 44
campus@escueladegobierno.es

Cóctel de Contratación Pública, LOPDGDD y ENS. Ingredientes problemáticos. Parte I.

La contratación pública de productos y servicios afectados por el Esquema Nacional de Seguridad (Real Decreto 311/2022 de 3 de mayo, ENS en adelante) está generando situaciones rocambolescas, impugnaciones de concursos y una inseguridad manifiesta para licitadores y licitantes.

LAS EMPRESAS PRIVADAS Y EL ENS DENTRO DEL ENS

En el artículo 2-*Ámbito de aplicación del ENS se incluyen explícitamente requerimientos de cumplimiento del ENS para "los sistemas de información de las entidades del sector privado, …, cuando, de acuerdo con la normativa aplicable y* ***en virtud de una relación contractual,*** *presten servicios o provean soluciones a las entidades del sector público …".*

Dentro de esta mismo artículo se enlaza directamente con la contratación pública cuando se requiere que:
"…los ***pliegos de prescripciones administrativas o técnicas*** *de los contratos que celebren las entidades del sector público incluidas en el ámbito de aplicación de este real decreto* ***contemplarán todos aquellos requisitos necesarios para asegurar la conformidad con el ENS de los sistemas de información en los que se sustenten los servicios prestados por los contratistas****, tales como la presentación de las correspondientes* ***Declaraciones o Certificaciones de Conformidad con el ENS****…"*

La necesidad de contemplar el ENS en la contratación pública queda así explicitada en el propio texto normativo, con poco margen para la interpretación, pero esto no es todo.

LAS EMPRESAS PRIVADAS Y EL ENS DENTRO DE LA LOPDGDD

La Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) intenta resolver en su Disposición adicional primera una "carencia" del Reglamento (UE) 2016/679 (RGPD) en cuanto a la concreción de las medidas de seguridad a aplicar.

Recordemos que el Real Decreto 1720/2007, Reglamento de desarrollo de la antigua Ley 15/1999 (LOPD), contenía en su Titulo VIII un conjunto de medidas de seguridad concretas que orientaban su implementación y, con ello, facilitaban el cumplimiento del requerimiento de securización. En la redacción de la LOPDGDD el legislador optó por señalar el ENS como marco de referencia para las medidas de seguridad a implantar, incluyendo una previsión para el sector privado:

"… En los casos en los que ***un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad****".*

La intención del legislador era elogiable al ofrecer un marco normativo con un amplio conjunto de medidas de seguridad enumeradas en su Anexo II, numerosas

CONTINÚA EN PRÓXIMA PÁGINA

Guías para su implementación desarrolladas por el Centro Criptológico Nacional (CCN) y un esquema de certificación que permite obtener acreditaciones oficiales de cumplimiento, por lo que, en la teoría, el escenario parecía ideal.

Esta Disposición de la LOPDGDD amplía automática y explícitamente el ámbito de aplicación del ENS a servicios que **tratan datos personales**, por lo que los procesos de contratación de estos servicios quedan también afectados.

EL ENS CERTIFICA "SISTEMAS DE INFORMACIÓN", NO EMPRESAS

Una de las cuestiones que más confusión generan, y con bastante razón, se centra en que el ENS certifica **sistemas de información,** un concepto extraordinariamente amplio que el propio texto normativo del ENS intenta aclarar, con escasa fortuna, en mi opinión:

Sistema de información: cualquiera de los elementos siguientes:
1.º Las redes de comunicaciones electrónicas que utilice la entidad del ámbito de aplicación de este real decreto sobre las que posea capacidad de gestión.
2.º Todo dispositivo o grupo de dispositivos interconectados o relacionados entre sí, en el que uno o varios de ellos realicen, mediante un programa, el tratamiento automático de datos digitales.
3.º Los datos digitales almacenados, tratados, recuperados o transmitidos mediante los elementos contemplados en los números 1.º y 2.º anteriores, incluidos los necesarios para el funcionamiento, utilización, protección y mantenimiento de dichos elementos.

Es muy habitual encontrar en los pliegos requerimientos de certificación ENS de "la empresa licitante", cuando el **ENS no certifica empresas sino sistemas de información**, propiedad de la empresa, que implementan uno o varios servicios, siendo impugnable el requerimiento de certificación que no se plantee en los términos adecuados.

EL ENS CERTIFICA "SISTEMAS DE INFORMACIÓN" CATEGORIZADOS

El Anexo I del ENS especifica la metodología para determinar el nivel (BAJO, MEDIO, ALTO) de cada una de las dimensiones de seguridad de un sistema (disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad), derivando la categoría global del sistema (BÁSICA, MEDIA, ALTA) y **esta categoría es la que figura en el certificado**, si bien los niveles por cada dimensión también deben aparecer.
Es muy habitual encontrar en los pliegos un requerimiento de certificación basado únicamente en

la categoría global (BÁSICA, MEDIA o ALTA), sin tener en cuenta que ésta se deriva del máximo nivel asignado a las dimensiones de seguridad, y esto puede llevar a un resultado no deseado en un proceso de licitación.

Imaginemos un caso de contratación de un sistema de información donde se tratarán masivamente categorías especiales de datos personales (artículo 9 RGPD) y, simplificando el proceso, la Administración contratante decide que las dimensiones "confidencialidad" e "integridad" asumen el nivel ALTO, por lo que la categoría global a requerir para la certificación de los licitantes será ALTA. Ahora bien, esta categoría ALTA puede haberla obtenido un licitante asignando el nivel ALTO a la dimensión "trazabilidad" y haber dejado el resto en nivel MEDIO o BAJO, lo que puede incumplir las expectativas de seguridad de la entidad contratarte, centradas en "confidencialidad" e "integridad".

Por tanto, **es fundamental que los pliegos contemplen los niveles requeridos por dimensión de seguridad, no solo una categoría global del ENS.**

CONTINÚA EN LA PARTE II

En la parte II expondré un caso de impugnación del resultado de una licitación a causa de esta problemática y sugerencias para abordar la redacción de pliegos (y el escenario de los contratos menores) de forma que las Administraciones Públicas y las entidades licitantes minimicen las probabilidades de impugnación del proceso debidas a una redacción inadecuada de los requerimientos respecto al ENS.

Escuela de Gobierno
eGob®
https://escueladegobierno.es

LIVE STREAMING

Curso de
Doble Certificación

Gestión de Proyectos

OpenPM² (PjM) + ISO 21502

Director Académico:
Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación OpenPM² (PjM) Executive
- Certificación ISO 21502 Leader
- Módulo 3: MasterGEIT®
- Módulo 3 MasterPPM®

MPPM® MGEIT® eGob®

Del 19 al 27 de abril

+ 34 96 109 44 44
campus@escueladegobierno.es

Cóctel de Contratación Pública, LOPDGDD y ENS. Ingredientes problemáticos(II)

Empecé a mezclar ingredientes para un gin tonic y me salió una paella estupenda.

CATÁLOGO DE PRODUCTOS Y SERVICIOS DE SEGURIDAD CERTIFICADOS

Las entidades públicas licitadoras disponen de la "*Guía de Seguridad de las TIC - CCN-STIC 105 -Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación*" (CPSTIC en adelante), la cual contiene la relación a su fecha de publicación de los productos y servicios de seguridad (switches, routers, cortafuegos, antimalware, servicios de gestión de identidades, SIEM, etc.) certificados por el CCN, con lo que la redacción de los pliegos recibe una ayuda relevante dado que, en cumplimiento de la medida "*Componentes certificados [op.pl.5]*" del ENS, **para sistemas de categoría MEDIA y ALTA es obligatorio que los productos y servicios licitados estén incluidos en esta guía**, a menos que pueda alegarse algún motivo que lo exceptúe.

Ahora bien, y tal como he publicado en un artículo anterior, esta guía **carece de certificaciones para las aplicaciones informáticas, servicios en la nube, servicios de comunicaciones**, etc, por lo que todo lo no incluido en el CPSTIC debe certificarse a través del esquema de certificación del ENS y, por tanto, como "sistema de información" con su alcance correspondiente, y aquí nos encontramos con una alta "creatividad".

LOS ALCANCES DE LAS CERTIFICACIONES DEL ENS SON "CREATIVAS"

Tal como publiqué en la parte (I) de este artículo, el ENS certifica sistemas de información que implementan uno o varios servicios, y el alcance de la certificación debe especificarlos. Hasta aquí todo bien. Sólo hasta aquí.

Si alguien tiene curiosidad en revisar los alcances de las certificaciones ENS actuales de numerosos proveedores de servicios a las Administraciones Públicas, cuyo Registro público está disponible en: https://gobernanza.ccn-cert.cni.es/certificados?link=private-tab-pane, puede observar alcances muy genéricos en cuanto a los servicios que contemplan. Dado que la certificación debe acreditar el cumplimiento del ENS para el objeto de la licitación a la que concurren las entidades licitantes, estos alcances genéricos hacen que no siempre resulte evidente que los servicios certificados incluyan el objeto de la licitación. En estos casos, queda en manos de la entidad licitadora "interpretar" el alcance y admitirlo o denegarlo.

OBLIGACIONES DE LAS ENTIDADES PÚBLICAS LICITADORAS

Las entidades públicas licitadoras deben incluir en la redacción de los pliegos, entre otros, los requerimientos técnicos y legales aplicables al objeto de la licitación, así como los criterios de evaluación de la solvencia técnica y posibles requisitos esenciales de ejecución.

CONTINÚA EN PRÓXIMA PÁGINA

La certificación del cumplimiento del ENS ha sido objeto de amplio debate, ya que, en función del criterio de la entidad licitadora, lo hemos leído como parte de la solvencia técnica, como parte de los requisitos esenciales de ejecución e incluso como parámetro valorable para la adjudicación.

Por otra parte, existen pliegos donde la certificación ENS es condición para poder licitar, en otros se exige sólo a la fecha de la firma del contrato para la entidad adjudicataria e incluso hemos leído algún pliego donde se requiere su obtención en un plazo temporal dentro del periodo de vigencia del contrato.

Este punto está generando serios problemas en las licitaciones, ya que se trata de procesos de concurrencia competitiva donde numerosas empresas presentan propuestas que deben cumplir con los requerimientos de ambos pliegos, técnico y administrativo y, por supuesto, van a defender sus derechos contra el resto de las concurrentes si detectan situaciones impugnables y/o recurribles, siendo el tema de la certificación ENS uno de los puntos candentes.

CASO CONCRETO – RECURSO CONTRA UNA ADJUDICACIÓN

El caso concreto que voy a exponer es público y puede consultarse íntegramente en el enlace:

https://irekia.araba.eus/es/-/resoluciones-ofarc-de-la-dfa-%C3%8Dndice-anual-2019-2020-1 en su Resolución 5/2023.

El objeto de la licitación incluye explícitamente una serie de servicios que debe ofrecer el sistema de información a contratar. Concretamente:

"Gestor de Expedientes / Sede Electrónica / Gestión de apoderamientos (o representación) / Gestión de Territorios y Personas / Registro Electrónico de Entrada y Salida / Escaneo certificado / Gestión de Notificaciones y Comunicaciones / Gestión Documental / Gestor de firma electrónica"

La licitación requiere que el sistema de información debe estar certificado en categoría MEDIA. La entidad adjudicataria presentó un certificado ENS en categoría MEDIA cuyo alance comprendía:

"Sistemas de información que dan soporte a los servicios de administración electrónica: • Gestión económico-financiera, contabilidad analítica y patrimonial. • Gestión de población, ingresos y recaudación."

La empresa recurrente adujo que el alcance de la certificación ENS no incluía algunas de las funcionalidades requeridas en el pliego y el **recurso fue estimado ordenando** "retrotraer las actuaciones hasta el momento de valoración de las ofertas técnicas para **proceder a la exclusión de la empresa propuesta como adjudicataria**".
Escenarios como éste son cada vez más frecuentes y estimo que se van a multiplicar ante el complicado cóctel expuesto.

SERVICIOS CON TRATAMIENTO DE DATOS PERSONALES

En este contexto, y dado que el cumplimiento del ENS es requerido para las entidades privadas que prestan servicios con tratamiento de datos personales a las entidades del sector público (Disposición adicional primera de la LOPDGDD), se debería exigir a todas las entidades licitantes su certificación ENS para poder optar a su adjudicación.
Esto supondría requerir esta certificación a todo autónomo o empresa que opte a ofrecer servicios donde trate datos personales, como podrían ser trabajadores/as sociales, asistentes para atención a persona dependientes, monitores o clubes deportivos, profesores/as contratadas, ONGs, entidades colaboradoras y, en general, toda entidad cuyos servicios traten datos personales. ¿Inviable? Así está la legislación actual. Como posible solución, generar perfiles de cumplimiento sectoriales o específicos que permitan racionalizar los requerimientos, ya que el uso de "sistemas de información" (p.e. Ofimática) es el medio utilizado para el desarrollo de cualquier prestación de este tipo.

CONTINÚA EN PARTE III

En la parte III (final) expongo una de las "preguntas del millón": ¿Puede exigir la AAPP certificaciones ENS a las empresas cuando la propia AAPP no está certi9ficada? Asimismo, expongo recomendaciones para la redacción de los pliegos en cuanto a los requerimientos respecto al ENS.

Escuela de Gobierno
eGob®
https://escueladegobierno.es

LIVE STREAMING

Curso de
Doble Certificación

Gestión de Programas

OpenPM² (PgM) + ISO 21503

Director Académico:
Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación OpenPM² (PgM) Executive
- Certificación ISO 21503 Leader
- Módulo 4: MasterGEIT®
- Módulo 4 MasterPPM®

MPPM® MGEIT® eGob®

Del 3 al 11 de mayo

+ 34 96 109 44 44
campus@escueladegobierno.es

Evento de Cierre de Temporada 2024 de las Revistas Tecnología y Sentido Común y Stakeholders.news

El 19 de julio de 2024, las revistas Tecnología y Sentido Común y Stakeholders.News celebraron el Cierre de su novena y tercera temporada respectivamente con un interesante evento en la sede de UNE Asociación Española de Normalización, en Madrid.

En una tradición que se inició el pasado año 2023, las revistas Tecnología y Sentido Común y Stakeholders.News prepararon un cierre de temporada a la altura tanto de la calidad de sus contenidos como del nivel de sus colaboradores. Con la inestimable colaboración de UNE Asociación Española de Normalización, el día 19 de julio de 2024 se reunió en Madrid un granado grupo de profesionales, entre los que estaban algunos de los colaboradores de nuestras revistas.

El evento comenzó con una bienvenida a cargo de Paloma García, Directora de Programas de Normalización y Grupos de Interés de UNE, y de Javier Peris, Director de las revistas Tecnología y Sentido Común y Stakeholders.News, en el que agradecieron a los presentes su asistencia, sobre todo a aquellos afectados por el incidente global en sistemas de información de grandes compañías de todo tipo que se dio en esa fecha.

CONTINÚA EN PRÓXIMA PÁGINA

Evento Protagonista

Tras la bienvenida, se dio paso al ponente principal del evento, Ramsés Gallego, primer español (y tercer europeo) en ser nombrado para el "Hall of Fame" de ISACA internacional, evento que tuvo lugar en este 2024. Renombrado conferenciante, deleitó al público asistente con su charla "De Gestionar a Gobernar …. con 'G' de Ganar", en la que glosó las bondades de dar ese salto hacia el gobierno de las Tecnologías de la Información, sobre todo en los aspectos relacionados con la ciberseguridad. Ciertamente, un lujo contar con él para el evento.

CONTINÚA EN PRÓXIMA PÁGINA

Evento Protagonista

El siguiente acto fue la mesa redonda con cinco de los autores que colaboran con la revista Tecnología y Sentido Común en el que participaron: Alejandro Aliaga líder de la seccion “Radio Security”, Renato Aquilino líder de la sección “Marcos y Normas”, Marlon Molina líder de la seccion “Es Tendencia”, Marcos Navarro líder de la seccion Ai Robot” que a partir de la proxima temporada pasará a llamarse “Ai Futuro” y Manuel Serrat líder de la seccion “Futuro y Seguridad”.

Durante la mesa redonda de Tecnologia y Sentido Común, estos cinco representantes respondieron a las preguntas del presentador y director de la revista, Javier Peris, acerca de los contenidos de la temporada que terminaba, y de qué se podía esperar de sus secciones en cuanto a contenidos y novedades en la décima temporada de la revista.

Alejandro Aliaga centró su intervención en recordad que el objetivo de su sección “Radio Security” es concienciar a los lectores de que existen vectores de ataque no convencionales asociados con las comunicaciones inalámbricas, y que, por la evolución tecnológica, es difícil que éstos se reduzcan.

Por su parte, Renato Aquilino, en su sección “Marcos y Normas” ha centrado sus contenidos en poner de manifiesto el gap existente entre las normas y quienes las escriben, frente a quienes las han de convertir en realidad en las organizaciones, algo que resulta extremadamente complejo en algunos casos.

Por lo que respecta a Marlon Molina, con su sección “Es Tendencia”, ha tratado de contar a los lectores en esta temporada que termina los temas que, mes a mes, han atraído la atención del sector por diferentes motivos.

Marcos Navarro anunció que su sección, a partir de la décima temporada, cambiaba de enfoque y de nombre, para explicar cómo es la vida en 2024, sólo dentro de diez años, gracias a tecnologías como la Inteligencia Artificial y la Robótica.

En cuanto a Manuel Serrat, explicó que con su sección “Futuro y Seguridad” ha tratado de poner el foco en aquellos aspectos de la evolución tecnológica que pueden suponer algún tipo de riesgo, y concienciar a los lectores para evitarlos.

CONTINÚA EN PRÓXIMA PÁGINA

Evento Protagonista

Finalizada esta mesa redonda, se llevó a cabo la segunda Mesa Redonda, que contó con cuatro de los colaboradores de la revista Stakeholders.News: Juan Manuel Domínguez líder de la Seccion "Organizaciones Resilientes", Luis Morán líder de la sección "Personas y Procesos", José Antonio Puentes líder de la seccion "Tendiendo Puentes" y Juan Jesús Urbizu líder de la seccion "Tecno-transformación".

Dada la temática de la revista, fundamentalmente dirigida a aquellos profesionales de la gestión de proyectos, programas y portfolios y áreas conexas, las preguntas para los participantes en la mesa redonda se centraron en poner de relieve la necesaria aplicación de estándares y buenas prácticas en cada uno de los ámbitos que tratan las diferentes secciones de la revista.

Juan Manuel Domínguez, a través de su sección "Organizaciones Resilientes", expuso aspectos tales como que, en Japón, con aproximadamente 120 millones de habitantes, hay 45.000 empresas centenarias, frente a las poco más de 5.000 que existen en España con 48 millones de habitantes.

Luis Moran comentó algunos de los temas que había tratado durante esta tercera temporada en su sección "Personas y Procesos", y avanzó alguna de las cuestiones que va a tratar en la cuarta temporada de la revista.

José Antonio Puentes (sección "Tendiendo Puentes") compartió con los presentes algunas vivencias personales, relacionadas con las dificultades que la gestión de proyectos enfrenta en determinadas organizaciones.

Por último, Juan Jesús Urbizu, que estas temporadas ha escrito en su sección "Tecno Transformación", apuntó algunas de las cuestiones más relevantes a las que se enfrenta el gestor de proyectos, programas y portfolios en relación con la digitalización de las organizaciones, y más desde la irrupción para el gran público de los sistemas de inteligencia artificial.

CONTINÚA EN PRÓXIMA PÁGINA

Tras las dos mesas redondas, Javier Peris anunció el nombramiento de los tres embajadores de la revista Stakeholders.News en Hispanoamérica más concretamente en Puerto Rico, Uruguay y El Salvador.
En Puerto Rico contaremos cada mes con la participacion de Nesty Delgado en Uruguay contaremos con Daniel Sorokins y en el pais de la eterna sonrisa "El Salvador contaremos con Luis Guardado quienes fueron nombrados y serán a partir de ahora Embajadores de Stakeholders.news.

Los actos de cierre de temporada terminaron con la entrega de los premios Tecnología y Sentido Común y Stakeholders. News, en esta ocasión en su edición de 2024.

El "Premio Tecnología y Sentido Común 2024" recayó en el Consejo General de Colegios Profesionales de Ingeniería Informática (CCII), por su aportación al progreso de la sociedad de la información, el impulso al desarrollo ético de los avances tecnológicos y la defensa y promoción de la ingeniería en informática. El premio fue recogido por José García Fanjul, secretario del CCII y vicedecano del Colegio Oficial de Ingenieros en Informática del Principado de Asturias.

Por otro lado, el "Premio Stakeholders.News 2024" fue otorgado a la Agencia para la Administración Digital de la Comunidad de Madrid, por haberse convertido en referente en la innovación y digitalización de la administración pública y por su compromiso con el cumplimiento y la excelencia del servicio al ciudadano. Este premio fue recogido por Zaida Sampedro Préstamo, subdirectora general de Transformación y Gestión del Cambio de la Agencia para la Administración Digital de la Comunidad de Madrid.

Al terminar el acto, todos los presentes pudieron disfrutar de un magnífico networking alrededor de un espectacular catering que se sirvió en las mismas instalaciones de UNE, con lo que se dio por cerrada la temporada de ambas revistas. ¡Nos vemos en septiembre!

Hace mucho tiempo que hablas.

¿Pero hace cuánto no dialogas?

Somos una organización global de beneficio para la comunidad cuya misión es crear normas para contribuir a la construcción de un mundo más seguro, sostenible y competitivo.

Creamos espacios de colaboración neutrales e inspiradores en los que compartir conocimiento para desarrollar, a través del diálogo y el consenso, normas que sirvan a los intereses de toda la sociedad y que movilicen a los que apuestan decididamente por la excelencia empresarial y la conciencia social.

UNE Normalización Española

Progreso compartido

une.org

Cóctel de Contratación Pública, RGPD, LOPDGDD y ENS. Ingredientes problemáticos. Parte III (final).

Recomendaciones para un cóctel indigesto.

ESTUDIO DE LAS AFECTACIONES NORMATIVAS

La Unidad Administrativa (UAD) que promueve la licitación debe realizar un estudio previo a la redacción de los pliegos donde se determine la afectación del objeto de la licitación en materia de tratamientos de datos personales y/o cuestiones de seguridad dentro del alcance del Esquema Nacional de Seguridad (ENS).

En esta fase debe participar el responsable de la UAD, el rol Delegado de Protección de Datos (DPD) y roles del ENS como Responsable de Seguridad (RSEG) y Responsable del Sistema (RSIS).

El estudio debe analizar no solo la posible afectación sobre RGPD, LOPDGDD y ENS en base a sus ámbitos de aplicación y alcance sino también un análisis de riesgos de naturaleza jurídica y técnica, **específico para la entidad contratante concreta y el objeto de la licitación**, identificando los requerimientos que deben trasladarse a los pliegos.

En la práctica, dicho estudio se realiza en contadas ocasiones, resultando en requerimientos inconsistentes con la realidad del Organismo público contratante, lo que puede afectar a la redacción de los pliegos y a la ejecución posterior del proyecto.

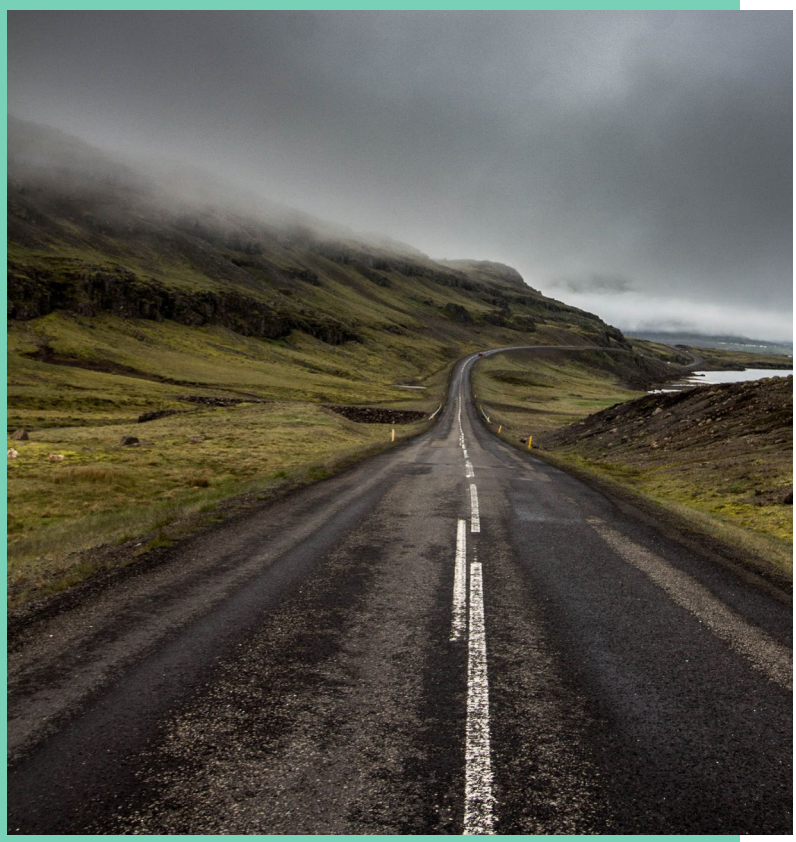
Es normal encontrar pliegos cuyos requerimientos se han basado únicamente en guías del Centro Criptológico Nacional (CCN) para las valoraciones ENS aplicables a los servicios e informaciones corporativas en los que, esgrimiendo "CCN dixit", **no evalúan su situación particular,** evaluación que puede influir sobre el planteamiento del PPT.

Particularmente cuestionables son las guías *CCN-STIC 890-A-C - "Requisitos Esenciales de Seguridad"* ya que, siendo muy loable su objetivo, incluyen en nivel BAJO de las dimensiones de seguridad del ENS servicios (en las EELL) tan sensibles como Policía Local o Servicios Sociales, sin especificar el análisis de riesgos efectuado para derivar tal calificación y sin incluir criterios de la Agencia Española de Protección de Datos (AEPD) al respecto. Por mi parte, estoy convencido de que la AEPD cuestionaría seriamente estos criterios del CCN.

Estas Guías están dedicadas a facilitar las certificaciones sobre ENS de los sistemas de información de los Organismos públicos considerándolos de categoría BÁSICA, forzando las costuras de las valoraciones de los servicios que los componen y la información que tratan, olvidando el artículo *3 del ENS –Sistemas de información que traten datos personales*, el cual deja muy clarito y diáfano que, en estos casos, debe realizarse un análisis de riesgos (y una Evaluación de Impacto si procede) y, explícitamente, requiere la adopción de medidas complementarlas a las del ENS si éstas fueran insuficientes. Si alguien considera que los datos personales que maneja, p.e., Servicios Sociales (violencia de género, conductas adictivas, menores, etc) merecen el nivel BAJO en confidencialidad e integridad … apaga y vámonos.

Por tanto, no es suficiente copiar-pegar criterios de una guía del CCN para determinar los niveles de seguridad a conseguir ni para identificar los requerimientos en materia de seguridad exigibles a las entidades licitantes, dado que la inmensa mayoría de servicios corporativos incluyen tratamientos de datos personales y deben analizarse desde esta perspectiva en el Organismo concreto.

CONTINÚA EN PRÓXIMA PÁGINA



PLIEGOS CLAROS Y COMPLETOS

En un proceso de licitación regido por pliegos, estos deben contener una descripción clara y completa del objeto de la licitación y, en el caso del Pliego de Prescripciones Técnicas (PPT), una exhaustiva enumeración de los requerimientos funcionales y técnicos aplicables a todos los componentes que deben materializar las prestaciones que constituyen dicho objeto. Esta exhaustividad es un factor crítico para evitar "interpretaciones" de las entidades licitantes que pueden derivar, posteriormente, en lagunas de cumplimiento que la entidad adjudicataria probablemente intentará achacar a la ausencia o ambigüedad de los requerimientos del pliego.

LICITACIONES CON TRATAMIENTO DE DATOS PERSONALES

Cuando la entidad adjudicataria, por el objeto del contrato, pueda tratar datos personales bajo la responsabilidad de la entidad contratante, aquélla asume la condición de "Encargado de Tratamiento" y, por ende, es necesario disponer del correspondiente contrato o acto jurídico vinculante que establece el artículo 28.3 del RGPD.
En este sentido, recomiendo incluir la asunción del rol Encargado de Tratamiento por parte de la entidad adjudicataria, el clausulado completo descriptivo de los tratamientos de datos personales a realizar dentro del objeto de la licitación y el clausulado requerido en este artículo 28.3 del RGPD dentro del PCAP, con lo que la entidad adjudicataria asume automáticamente su condición de Encargado de Tratamiento sin necesidad de firmar un documento separado.

REQUERIMIENTOS RESPECTO DEL ENS

En caso de que el objeto de la licitación incluya productos o servicios de seguridad, éstos deben estar incluidos en la *Guía de Seguridad de las TIC CCN-STIC 105-Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación* o fuente alternativa admitida (p.e. Common Criteria).
Si el objeto de la licitación incluye servicios afectados por el ENS o **incluye tratamientos de datos personales,** deben identificarse los niveles (BAJO, MEDIO, ALTO) para cada dimensión de seguridad que se deben implementar para el Organismo contratante como resultado de las prestaciones objeto de la licitación, lo cual redundará en su propio proceso de certificación.
Por otra parte, debe identificarse la certificación exigible para las entidades licitantes. En este caso, es fundamental requerir no solo una categoría certificada (BÄSICA, MEDIA, ALTA) sino también los niveles requeridos por cada dimensión de seguridad, y **muy especialmente, el alcance admisible de la certificación,** avisando explícitamente sobre la exclusión de las propuestas de las entidades licitantes cuyo alcance de su certificación sobre ENS no incluya claramente la cobertura del objeto de la licitación.

CONTRATOS MENORES

Este tipo de contratos no se gestionan mediante pliegos, pero todas las recomendaciones y consideraciones expuestas en el presente artículo son plenamente aplicables a las solicitudes de ofertas que se recaban de las posibles entidades a contratar o a cualquier documento contractual que formalice la adjudicación. Bajo ningún concepto sería admisible soslayar las cuestiones de cumplimiento normativo.

CONCLUSIÓN

El cóctel ya está provocando indigestiones, y su número y gravedad pueden aumentar, afectando a entidades licitadoras y licitantes.

Escuela de Gobierno

eGob®

https://escueladegobierno.es

LIVE STREAMING

Curso de
Doble Certificación

Service Management FitSM + ISO 20000

Director Académico:

Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación FitSM Executive
- Certificación ISO 20000 Leader
- Módulo 5 MasterGEIT®
- Módulo 5 MasterPPM®

MPPM® MGEIT® eGob®

Del 17 al 25 de mayo

+ 34 96 109 44 44
campus@escueladegobierno.es

La guerra de la biometría. Huellas borrascosas (Parte I)

La biometría se ha convertido en "casus belli" para los reguladores en materia de protección de datos personales, ignorando las medidas de seguridad aplicables para conseguir riesgos residuales aceptables.

LA CADENA DE MANDO

La última batalla fue librada en noviembre de 2023 por la Agencia Española de Protección de Datos (AEPD en adelante) en su "*Guía sobre tratamientos de control de presencia mediante sistemas biométricos*".

Esta guía (analizada en la segunda parte de este artículo) ha sido publicada por la AEPD pero no es de creación propia, dado que sigue los criterios interpretativos de su casa matriz, el Comité Europeo de Protección de Datos (CEPD en adelante), cuya función es "*garantizar que el Reglamento General de Protección de Datos (RGPD en adelante) y la Directiva sobre protección de datos en el ámbito penal se apliquen de manera coherente en los países de la UE*".

El CEPD está compuesto por el director de cada autoridad nacional de protección de datos y el Supervisor Europeo de Protección de Datos o sus representantes.

LA GUERRA CONTRA LA BIOMETRÍA

El Supervisor Europeo de Protección de Datos ya publicó en junio del 2020 un documento que la AEPD tradujo y publicó como "*14 equívocos con relación a la identificación y autenticación biométrica*". Este documento expone 14 escenarios en los que, indefectiblemente, los tratamientos de datos biométricos no solo no aportan ventajas en los procesos de identificación y autenticación sino que son señalados como fuente demoníaca de riesgos para quien ose utilizarlos. Su contenido ya denotaba una guerra sin cuartel contra los tratamientos biométricos y tuvo gran aceptación entre los enardecidos fans anti biométricos europeos, pero también dejó muy clara una postura que se ha mantenido en los documentos siguientes, como la mencionada Guía de la AEPD.
Es un documento que, en mi opinión, manipula y distorsiona el escenario real de los sistemas de tratamiento biométrico dado que sólo se centra en las amenazas que suponen para los derechos y libertades de las personas, construyendo un escenario completamente sesgado que, por supuesto, puede influir muy negativamente en la percepción de las personas que no dispongan de una visión holística de estos sistemas.

CONTINÚA EN PRÓXIMA PÁGINA

Ahora bien, su contenido es tan exageradamente sesgado que, como en el caso de una película de guión barato, ponen al "malo" tan absolutamente malo que se hace poco creíble.

El propio título del documento ya introduce una buena carga de prepotencia y "posesión de la verdad", ya que considera directamente "equivocados" a quienes piensen que las afirmaciones que contiene son muy debatibles. El CEPD se convierte a veces en organismo apostólico en lugar de garante de cumplimiento.

RIESGOS INHERENTES IGNORANDO RIESGOS RESIDUALES

La postura del CEPD y la AEPD se basa en la exposición exclusiva de los riesgos inherentes al tratamiento, **ignorando completamente las medidas de seguridad que se pueden y deben adoptar para mitigar dichos riesgos inherentes y transformarlos en riesgos residuales con niveles aceptables**.

Trasladando este absurdo escenario a otro contexto, si el CEPD y la AEPD recibieran las competencias en materia de seguridad aérea podrían decidir que no se debe volar dado que existe un alto riesgo de muerte en caso de accidente.

¿Absurdo? Efectivamente. Nadie creería tamañas afirmaciones dado que todos sabemos que los aviones disponen de medidas de seguridad activas y pasivas, obligatorias y certificables, que llevan su riesgo residual a valores aceptables por los reguladores. El CEPD ignora completamente las medidas aplicables al caso de la biometría y se limita a exponer sólo sus riesgos, impidiendo con esta carencia un análisis objetivo por parte de posibles usuarios de sistemas biométricos.

Por otra parte, tanto el CEPD como la AEPD meten en el mismo saco todos los tratamientos biométricos, cuando los riesgos inherentes son diferentes entre ellos. Tomando como base los más utilizados, el riesgo inherente asociado al tratamiento de la huella dactilar es inferior al tratamiento de reconocimiento facial. Mientras que la huella necesita un lector para ser procesada, el análisis biométrico de la cara de una persona puede realizarse masiva y automáticamente en cualquier espacio, por lo que la exposición es completamente distinta y así deberían ser también las consideraciones subsiguientes, incluyendo el conjunto de medidas específicas exigibles.
En cualquier caso, exponer únicamente riesgos inherentes a la biometría y no desarrollar el modelo completo de análisis y gestión de riesgos hasta llegar a sus riesgos residuales supone una falacia estelar. Por desgracia, la determinación de las medidas de seguridad **exigibles y certificables**, como en el caso de los aviones y otros sectores, choca con el perfil hiperjurídico del CEPD y el SEPD, con su **muy evidente desconexión de los entornos de conocimiento tecnológico que podrían aportar criterio para dichas medidas**.

COLABORACIÓN JURÍDICO - TECNOLÓGICA

Esta histórica división entre "lo jurídico" y "lo tecnológico" es uno de los grandes e históricos inhibidores de la legislación del siglo XXI. La Sociedad de la Información va muy por delante de los reguladores, y no se puede entender que las iniciativas jurídicas ignoren los entornos tecnológicos implicados, de la misma forma que las tecnologías no pueden ignorar el marco normativo aplicable. Este trabajo en equipo es un factor clave de éxito y, a la vez, una gran asignatura pendiente.

Decía una canción de Mago de Oz: "*Juicioso es el que ve que cielo y horizonte condenados están a tenerse que entender*". Llevo muchos años insistiendo en que sólo mediante equipos de trabajo con perfiles jurídicos y técnicos integrados se podrá desarrollar legislación del siglo XXI, pero está claro que sigo predicando en el desierto.

CUESTIONAMIENTO DE LA GUÍA DE LA AEPD

En la segunda parte de este artículo analizo la "*Guía sobre tratamientos de control de presencia mediante sistemas biométricos*" de la AEPD ante el enorme impacto que ha generado y los perjuicios que está ocasionando en las entidades que, atendiendo al criterio anterior de la propia AEPD, habían implementado sistemas biométricos para el control de presencia. Un "donde dije digo, digo Diego" de libro.

Escuela de Gobierno

eGob®

https://escueladegobierno.es

LIVE STREAMING

Curso de
Doble Certificación

Seguridad de la Información

CSX + ISO 27001

Director Académico:

Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación CSX Executive
- Certificación ISO 27001 Leader
- Módulo 6: MasterGEIT®

MGEIT® eGob®

Del 7 al 15 de junio

+ 34 96 109 44 44
campus@escueladegobierno.es

La guerra de la biometría (Parte II).

La guía "dondedijedigodigodiego" de la AEPD.

La "Guía sobre tratamientos de control de presencia mediante sistemas biométricos" de noviembre de 2023 deriva en un tsunami sobre la materia.

CAMBIO DE CRITERIO RADICAL 2021-2023

La guía de referencia supone un cambio de 180º en el criterio que la propia AEPD había mantenido en su propio documento de mayo de 2021, la guía "La Protección de Datos en las Relaciones Laborales", en la que se abordaba en el apartado "Los datos biométricos" del capítulo 4.6 el empleo de biometría en la implementación de los tratamientos de registro de presencia. En el texto se interpretaba la autenticación biométrica "fuera de las categorías especiales de datos".

Con esa premisa, avalada por la Autoridad de Control (AEPD), múltiples empresas y Administraciones Públicas (AAPP) invirtieron sustanciales sumas de dinero, privado **y público**, en la implementación de sistemas biométricos tras una Evaluación de Impacto sobre Protección de Datos (EIPD) que determinase la aceptabilidad del sistema tras su securización técnica y organizativa, a través de medidas (basadas en el ENS en las AAPP) adecuadas, sin olvidar, como ya escribí en la primera parte de este artículo, que el "almacenamiento biométrico" se limita a una secuencia alfanumérica derivada de un algoritmo de hash no reversible y **nunca se almacenan las propias características biométricas de la persona**.

La guía de noviembre de 2023 reconoce, sin rubor alguno:

> *"Sin embargo, esta interpretación ha sido superada por las Directrices antes citadas, por lo que la interpretación de esta AEPD ha de adaptarse a las Directrices del CEPD mencionadas de 26 de abril de 2023"*

Es curioso el eufemismo "esta interpretación ha sido superada", dado que, desde mayo de 2021 a abril de 2023 no han cambiado los marcos normativos referenciales de dicha "interpretación" y, por ende, el lugar de "superación" debería calificarse un cambio de criterio tan grave en contenido y **consecuencias** como una significativa inconsistencia que está generando graves perjuicios a entidades públicas y privadas.

Por otra parte, la guía de noviembre de 2023 ha sido publicada sin aviso ni consenso alguno, hecho que, por sí mismo, habla poco en favor de la pretendida "superación".

CONTINÚA EN PRÓXIMA PÁGINA

MEDIAS VERDADES NO SON VERDADES

El contenido de la guía de 2023 constituye un alegato en toda regla contra los sistemas biométricos "per se", asociando los tratamientos biométricos a riesgos prácticamente inasumibles y, en consecuencia, anatemizando su utilización si existen medios alternativos para el control de presencia o acceso.

En este escenario, la guía expone que "*se puedan inferir y recoger otras categorías especiales de datos y, en particular, datos relativos a la salud o datos que revelen el origen racial o étnico entre otros*". Esta posibilidad existe, por supuesto, pero los lectores biométricos utilizados para el control de presencia no disponen en su inmensa mayoría de esas funcionalidades, asociadas a lectores con un coste muy superior al de los lectores que únicamente ofrecen las funcionalidades necesarias para esa función.

En toda la guía subyace una premisa de "anatema biométrica" que ya permite adivinar el final de la película, absolutamente previsible ante la posición irreductible del guionista sobre la identidad y maldad del "malo" (la biometría) y su negativa a incluir en el guión medidas que permitan al "malo" ser percibido de otra forma. Al contrario, el texto sigue incidiendo en sus maldades y en el camino al infierno que llevamos quienes vemos alguna bondad y seguridad en estos tratamientos, admitidos hasta noviembre de 2023 y anatemizados tras esa fecha.

EL TÚNEL DEL TIEMPO

La guía desarrolla la historia del control de presencia desde el año 1890 y sus métodos, deduciendo que:

"El responsable de dichos tratamientos, a la hora de proponer operaciones biométricas, debe justificar las circunstancias por las que ya no es posible utilizar los sistemas de registro de presencia que se estaban empleando en el mismo centro hasta ese momento …."

Esta necesidad de justificación de la evolución de los métodos de control de presencia requiere demostrar que "ya no es posible utilizar sistemas anteriores", por lo que, dado que sí sería posible utilizarlos, inhibe dicha evolución al utilizar unos términos que, como mínimo, podrían calificarse como falaces. Este retorno al pasado se complementa con una gloriosa sugerencia de uso de "medios no tecnológicos", incidiendo en:

"No es obligatorio, ni recomendable, que la implementación de un tratamiento, se limite exclusivamente a la selección de recursos tecnológicos. En las opciones de implementar un tratamiento hay que considerar, entre otros, la utilización de recursos humanos, las garantías jurídicas y los procedimientos organizativos. Por lo tanto, en la evaluación de alternativas equivalentes y menos intrusivas se han de explorar opciones que no sean solo tecnológicas"

Esta sugerencia de involución genera un nuevo escenario de operaciones, las CLops, es decir, "Operaciones de Conserje y Libreta", todo ello bajo la inmutable consideración como "altamente intrusivo" de todo tratamiento biométrico, la cual preside inexorablemente toda la guía y condiciona sus contenidos bajo esta visión monofocal.

NO TODOS LOS RIESGOS ASOCIADOS A LA BIOMETRÍA SON IGUALES

Tomando como base los sistemas biométricos más utilizados, el riesgo inherente asociado al tratamiento de la huella dactilar es inferior al tratamiento de reconocimiento facial. Mientras que la huella necesita un lector para ser procesada, el análisis biométrico de la cara de una persona puede realizarse masiva y automáticamente en cualquier espacio, por lo que la exposición es completamente distinta y así deberían ser también las consideraciones subsiguientes, incluyendo el conjunto de medidas específicas exigibles y la consideración en cuanto a su intrusividad. Sin embargo, la guía obvia estas evidentes diferencias.

PRÓXIMO (Y ULTIMO) CAPÍTULO

En el siguiente capítulo acabo de analizar la guía de la AEPD y expongo las opiniones sobre la misma que personas referentes en la materia han expresado, así como la visión de la biometría desde la recientemente aprobada legislación europea sobre IA.
Es un tema candente y también preocupante ante la propia intrusión de la AEPD en aspectos legislativos que, en principio, no le corresponden.

Escuela de Gobierno
eGob®
https://escueladegobierno.es

LIVE STREAMING

Curso de
Doble Certificación

Continuidad de Negocio

BCI + ISO 22301

Director Académico:
Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación BCI Executive
- Certificación ISO 22301 Leader
- Módulo 7: MasterGEIT®

MGEIT® eGob®

Del 5 al 13 de julio

+ 34 96 109 44 44
campus@escueladegobierno.es

La guerra de la biometría (y III). Análisis final y propuesta de solución viable

El disenso puede ser consenso si todas las partes dialogan, debaten y no imponen.

NEGACIÓN DEL CONSENTIMIENTO

Uno de los aspectos más llamativos de la guía de la AEPD, proveniente del CEPD, es la interpretación que hace del concepto de "consentimiento" para negar su utilización como base jurídica legitimante del tratamiento biométrico para el control de presencia / registro de jornada.

"En el contexto de las relaciones laborales, de forma general, se produce un desequilibrio de poder entre empleado y empleador que hace que este consentimiento no se proporcione libremente por lo que no debe ser la base jurídica".

Este escenario supone una vulneración de algunos principios importantes, ya que, por definición y "en general", todo empleador es un malvado ente que presiona a sus empleados para prestar consentimientos que no desean, negando un principio tan básico como el de la presunción de inocencia y negando también el papel de los sindicatos en la defensa de los empleados en caso de sufrir presiones del empleador.

El tema no acaba aquí. En un punto posterior, la guía llega a admitir el consentimiento siempre y cuando el empleador demuestre que la falta de consentimiento no supone perjuicio alguno para el empleado y que le ofrece un método equivalente para poder cumplir sus obligaciones. Cuando parecía que teníamos una vía de solución llega la siguiente acrobacia interpretativa, en la que:

"Sin embargo, y respecto de este requisito de la posible "equivalencia de los tratamientos" hay que tener en cuenta que, si existen alternativas disponibles al tratamiento de datos biométricos que impliquen menor riesgo para los derechos y libertades de las personas cuyos datos personales se van a tratar, que permitan que en un momento dado todos los trabajadores opten por otras alternativas, ***el procesamiento de datos biométricos deja de ser necesario*** *para la implementación del tratamiento."*

Y aquí se acaba la historia, ya que si un tratamiento "no es necesario" no se puede llevar a cabo. Como siempre, la base de todo el argumentario es la anatemización de la biometría "per se", su consideración inherente como "alto riesgo" sin avanzar ni un milímetro en las medidas que pueden mitigar este riesgo hasta niveles incluso inferiores a otros métodos ni, por supuesto, entrar a considerar sus ventajas en materia de seguridad en los accesos o prevención del fraude.

CONTINÚA EN PRÓXIMA PÁGINA

Por otra parte, este CEPD y esta AEPD niegan el principio de "libre albedrío" de cada persona para tomar decisiones sobre determinados aspectos de su vida. Me resulta particularmente irritante (y preocupante) que se me impida otorgar el consentimiento para el tratamiento de mi huella dactilar si yo considero (como es el caso) que la seguridad del tratamiento es adecuada en la empresa donde trabajo y el método es idóneo para verificar mi identidad, evitando dispositivos externos y menos seguros ante la suplantación o el fraude, como las históricas tarjetas.

Organismos como el CEPD y la AEPD están invadiendo terrenos que no son de su propiedad ni de su competencia, con una deriva autoritaria nada compatible con los valores de una democracia en la UE, arrogándose la "defensa de los derechos y libertades" como otros se arrogan actuar "en nombre del pueblo" para defender iniciativas autocráticas.

OTRAS BASES JURÍDICAS

La guía de la AEPD desarrolla los supuestos de legitimación basados en otras bases jurídicas, pero su conclusión es la misma, no existe una norma con rango de Ley que recoja la "necesidad" de utilizar biometría para cumplir con los requerimientos legales del registro de jornada ni control de presencia, en una nueva acrobacia interpretativa que no solo resalta la inexistencia de esa necesidad en el ordenamiento actual sino que se permite el lujo de ordenar al poder legislativo cómo debe estar escrito un posible marco normativo que, hipotéticamente, lo pudiera recoger.

Por tanto, a la "no necesidad" se une el "consentimiento inválido" y la inexistencia de un marco legal que "requiera la biometría", además del argumentario clásico sobre los peligros de conocer a partir de una huella dactilar la temperatura y presión sanguínea del empleado, parámetros que los lectores del mercado del control de presencia no ofrecen en la realidad ni por objetivo de funcionalidad ni por precio.

AUTOCRACIA = IGNORAR OTRAS OPINIONES

En este escenario, donde la guía de la AEPD se ha publicado sin consenso alguno con los estamentos implicados o afectados, sin periodo de adaptación y sin tener en cuenta las implementaciones actuales realizadas bajo los criterios de la propia AEPD de 2021, cabría esperar que nuestra Autoridad de Control fuera receptiva a las solicitudes de diálogo sobre una materia tan debatible.
Entidades como la Asociación Profesional Española de Privacidad (APEP), empresas suministradoras, empresas y organismos con sistemas biométricos implementados han intentado, sin éxito hasta la fecha, dialogar y consensuar con la AEPD.

Recomiendo la lectura de las conclusiones del seminario "BIOMETRÍA, PROTECCIÓN DE DATOS E INTELIGENCIA ARTIFICIAL. LA GUÍA DE LA AEPD A DEBATE" de la Universidad de Alicante, celebrado en fecha 22/01/2024, con la participación de referentes como Julián Valero Torrijos. Esas conclusiones son demoledoras respecto a esta guía de la AEPD y solicitan su urgente retirada, aportando unos contundentes argumentos que señalan aspectos muy preocupantes de dicha guía en relación con la invasión de terrenos legislativos que no le corresponden.

Ver:
https://dpd.ua.es/es/seminario-de-investigacion-biometria-proteccion-de-datos-e-inteligencia-artificial.-la-guia-de-la-aepd-a-debate.html

CONCLUSIONES

La biometría no está exenta de riesgos, por supuesto, pero su prohibición "de facto" como se deduce de esta guía implica la ignorancia de las medidas técnicas y regulatorias que se podrían aplicar para minimizarlos.

Mi propuesta concreta, resumida, consiste en la elaboración de un conjunto "perfil de cumplimiento" (ENS/ISO27001) más "código de conducta" (RGPD) unidos, para los tratamientos biométricos, desarrollando un esquema de certificación específico para los dispositivos lectores que asegure unas medidas de seguridad adecuadas y acreditables, como ya dispone el CCN en su CPSTIC para productos de seguridad, incluyendo prohibiciones específicas sobre funcionalidades no relacionadas con su propósito de identificar y autenticar personas.

Escuela de Gobierno

eGob®

https://escueladegobierno.es

Curso de
Doble Certificación

Gobierno de I&T

COBIT + ISO 38500

Director Académico:

Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación COBIT Executive
- Certificación ISO 38500 Leader
- Módulo 8: MasterGEIT®

MGEIT® eGob®

Del 6 al 14 de septiembre

+ 34 96 109 44 44
campus@escueladegobierno.es


12
28

Yo, cuando sea mayor, quiero ser DPD (parte I)

El rol Delegado de Protección de Datos está siendo incorrectamente asociado a un modelo unipersonal inviable y "certificado" bajo un esquema poco realista.

DPD COMO OPORTUNIDAD PROFESIONAL

La figura del Delegado de Protección de Datos (DPO o DPD en adelante) se ha convertido en eje central del cumplimiento del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 (RGPD en adelante) y la Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD en adelante) ante la acumulación de funciones relevantes que estos marcos normativos le encomiendan, la protección de su independencia que dichos marcos le otorgan y la proyección que (presuntamente) puede suponer para quienes decidan optar por una carrera profesional dedicada a ejercer como tal.

Leyendo la posición, funciones y competencias del DPO, conferidas en los artículos 38 y 39 del RGPD y los artículos 35, 36 y 37 de la LOPDGDD, parece claro que "ser DPD" es una oportunidad de promoción y desarrollo para las personas que centran su carrera en el universo de la protección de datos personales, pero, como suele ocurrir, la teoría va por un camino y la realidad no siempre transcurre por el mismo.

INVIABILIDAD DEL DPO UNIPERSONAL

En base al Esquema de Certificación de Delegados de Protección de Datos de la Agencia Española de Protección de Datos (Esquema AEPD-DPD), el rol DPD (certificado o no) **debe "ser capaz de"** (sic):

a) recabar la información necesaria para determinar las actividades de tratamiento;
b) analizar y comprobar la conformidad de las actividades de tratamiento con la normativa aplicable;
c) informar, asesorar y emitir recomendaciones al responsable o el encargado del tratamiento;
d) recabar información para supervisar el registro de las operaciones de tratamiento;
e) asesorar en la aplicación del principio de la protección de datos por diseño y por defecto;

CONTINÚA EN PRÓXIMA PÁGINA

f) asesorar sobre si se debe llevar a cabo o no una evaluación de impacto de la protección de datos y qué áreas o tratamientos deben someterse a auditoría interna o externa, qué metodología debe seguirse al efectuar una evaluación de impacto de la protección de datos, si se debe llevar a cabo la evaluación de impacto de la protección de datos con recursos propios o mediante contratación externa, **qué salvaguardas (incluidas medidas técnicas y organizativas) aplicar para mitigar cualquier riesgo para los derechos e intereses de los afectados**, si se ha llevado a cabo correctamente o no la evaluación de impacto de la protección de datos y si sus conclusiones (seguir adelante o no con el tratamiento y qué salvaguardas aplicar) son conformes con el RGPD;

g) priorizar sus actividades y centrar sus esfuerzos en aquellas cuestiones que presenten mayores riesgos relacionados con la protección de datos;

h) asesorar sobre qué actividades de formación internas proporcionar al personal y a los directores responsables de las actividades de tratamiento de datos y a qué operaciones de tratamiento dedicar más tiempo y recursos;

i) intervenir en caso de reclamación ante las autoridades de protección de datos.

Esta enumeración de aquello que se espera del rol DPD ya puede dar una idea del planteamiento irreal sobre "DPD unipersonal".

Yo no suelo utilizar planteamientos taxativos ya que, en todo asunto, pueden existir matices, pero, en el caso del DPO, estoy defendiendo desde que leí un borrador del RGPD que ese rol es inviable como unipersonal dado que, **afirmo taxativamente**, no existe persona alguna que pueda concentrar todos los conocimientos jurídicos y técnicos necesarios, **simultáneamente**, que permitan ejercer su rol con la eficacia requerida. Por este motivo, he sido y soy crítico con el Esquema de Certificación de la AEPD dado que pretende "certificar" (ojo al verbo) que una persona que aprueba el examen y cumple los prerrequisitos ya es capaz de ejercer como DPD.

NO SE PUEDE EXIGIR LA CERTIFICACIÓN DPD-AEPD PARA EJERCER

Efectivamente, **para ejercer como DPD no hace falta certificación alguna**, tal como recoge la propia AEPD en su nota de 19 de abril de 2024 sobre su esquema de certificación:

Aunque esta certificación **no es obligatoria para poder ejercer como DPD y se puede ejercer la profesión sin estar certificado** bajo éste o cualquier otro esquema, la Agencia ha considerado necesario ofrecer un punto de referencia al mercado sobre los contenidos y elementos de un mecanismo de certificación que pueda **servir como garantía para acreditar la cualificación y capacidad profesional de los candidatos a DPD**.

Esta última frase es preocupante por el uso de la palabra "garantía de cualificación y capacidad profesional", dado que la aprobación del examen sólo garantiza la capacidad profesional para aprobar dicho examen, debido a las propias características del esquema de certificación.

¿CERTIFICACIÓN DPD SIN EXPERIENCIA PREVIA?

El esquema permite examinarse, y obtener el certificado DPO en caso de aprobar, a personas que, simplemente, acrediten la realización de un curso reconocido de 180 horas sin tener experiencia previa alguna en materia de protección de datos personales. Las personas que desarrollamos nuestra carrera profesional en estas materias desde hace años somos muy conscientes de que la experiencia y el aprendizaje en proyectos reales constituyen una base de conocimiento fundamental para poder ejercer las actividades encomendadas al rol DPD, y esa falta de experiencia, a la inversa, puede impactar seriamente sobre su aplicabilidad en los escenarios reales.

Este planteamiento sigue un camino contrario al que siguen otras certificaciones plenamente consolidadas, como las de ISACA (incluyendo Certified Data Privacy Solutions Engineer (CDPSE), donde el modelo "experiencia + conocimiento acreditado" es un binomio que aporta valor añadido a las entidades que se planteen contratar este tipo de perfiles.

PARTE II – PROPUESTA PARA EL MODELO DE ACREDITACIÓN

En la segunda parte de este artículo abordo los principales problemas del Esquema de Certificación DPD-AEPD y sugiero propuestas para que el rol DPD aporte mayor valor añadido, mediante un enfoque realista de su implementación práctica en las entidades públicas o privadas donde ejerce.

Escuela de Gobierno
eGob®
https://escueladegobierno.es

LIVE STREAMING

Curso de
Doble Certificación

Gobierno Corporativo COSO + ISO 37000

Director Académico:
Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación COSO Executive
- Certificación ISO 37000 Executive
- Módulo 10: MasterGEIT®
- Módulo 1:0 MasterPPM®

MPPM® MGEIT® eGob®

Del 22 al 30 de noviembre

+ 34 96 109 44 44
campus@escueladegobierno.es

Yo, cuando sea mayor, quiero ser DPD (y II)

El Esquema de Certificación AEPD-DPD contiene planteamientos cuestionables para la finalidad pretendida.

FORTALEZAS Y DEBILIDADES DEL ESQUEMA AEPD-DPD

El Esquema de Certificación de DPD (el esquema, en adelante) de la Agencia Española de Protección de Datos (AEPD) tiene una finalidad muy loable pero también excesivamente ambiciosa en función de sus planteamientos y los escenarios reales de trabajo que se encontrarán las personas certificadas.

La certificación de personas que promueve el esquema es correcta siempre y cuando el ámbito de aplicación del objeto de la certificación sea abarcable por un individuo, pero no es válida cuando la competencia que evalúa es inabarcable por una persona, resultando en certificados "teóricos" que no permiten una praxis adecuada al no profundizar en los temas, muy especialmente cuando se mezclan en la misma certificación conocimientos jurídicos y técnicos.

¿Sería lógico certificar un médico como oftalmólogo-cardiólogo requiriendo que sea experto en ambas disciplinas y que, adicionalmente, sea capaz de ejercer en ambas cuando acabe el examen? Inabordable. Pues parece que este criterio no se aplica en el esquema dado que mezcla el universo jurídico con el técnico, teniendo ambos un alcance inmenso claramente candidato a una especialización diferenciada que permita abordar los escenarios reales con unos conocimientos profundos y aplicables en la práctica.

No existe la figura "DPD junior". Las expectativas de las entidades que nombran o contratan un DPD certificado son muy altas y suelen rechazar cualquier intento de contratación de soporte externo, con su coste asociado, bajo el argumento "eres un DPD certificado por la AEPD y eso implica que sabes todo lo que tienes que saber", máxime cuando la propia AEPD afirma:

> "Este Esquema es un sistema de certificación que permite certificar que los DPD reúnen la cualificación profesional y los conocimientos requeridos para ejercer la profesión"

CONTINÚA EN PRÓXIMA PÁGINA

Este planteamiento y el uso del verbo "certificar" no ha tenido en cuenta la realidad y el volumen de trabajo que debe desarrollar el rol DPD.

ESPECIALIZACIONES NECESARIAS

El rol DPD en un organismo de la Administración Pública (AAPP) desarrolla su trabajo en un escenario legal diferente al de una entidad privada, cuestión que también debería ser objeto de especialización para evitar situaciones como las que encontramos habitualmente sobre todo en la AAPP, donde su DPD certificado, sobre todo si es externo, puede desconocer la legislación específica sobre procedimientos administrativos, gestión tributaria, urbanismo, Servicios Sociales, Policía Local, violencia de género, menores, etc, de un catálogo de tratamientos entre los que se encuentran algunos clasificables como de máxima sensibilidad.

Capítulo aparte merecen los conocimientos técnicos. Dentro del examen de certificación supone 30 preguntas de las 150 totales, un 20% del total, estando su contenido especificado en el denominado "dominio 3". Entre ellas:

……3.3. La gestión de la seguridad de los tratamientos. 3.3.1. Esquema Nacional de Seguridad, ISO/IEC 27001:2013 (UNE ISO/IEC 27001:2014: Requisitos de Sistemas de Gestión de Seguridad de la Información, SGSI). 3.3.2. Gestión de la Seguridad de los Activos. Seguridad lógica y en los procedimientos. Seguridad aplicada a las TI y a la documentación. 3.3.3. Recuperación de desastres y Continuidad del Negocio. Protección de los activos técnicos y documentales. Planificación y gestión de la Recuperación del Desastres…..

Simplemente con esta enumeración de contenidos ya queda claro que una persona que provenga del ámbito jurídico, perfil claramente mayoritario entre las personas que se presentan al examen, no puede abordar este caudal de conocimientos de forma efectiva y, con ello, observamos que el nivel de las preguntas del examen relacionadas con este dominio permite aprobar el examen, pero quedan a mucha distancia del nivel de conocimiento requerido para el perfil técnico del rol DPD.

En la práctica, encontramos DPDs provenientes del ámbito jurídico que no pueden entender un escenario técnico sobre el que deben asesorar y supervisar, ni siquiera con el soporte del área de IT, dado que no disponen de una base adecuada que, en el estado de la técnica y su constante evolución, les permita aportar criterio y supervisión en este contexto.

LA EXPERIENCIA NO ES UN GRADO, ES UNA NECESIDAD

El esquema de la AEPD permite presentarse al examen a personas sin experiencia alguna en materia de protección de datos personales, tras la realización de un curso homologado de un mínimo de 180 horas y, si aprueban el examen, se les concede la misma certificación que una persona con experiencia en los escenarios reales sobre la materia. En mi opinión, **este planteamiento supone un grave error que devalúa la propia certificación y su valor en el mercad**o, dado que, para estas actividades de asesoramiento y supervisión, es improbable que una persona sin experiencia previa real pueda aportar valor en los niveles que una entidad contratante de un "DPD certificado por la AEPD" espera.

PROPUESTAS PARA LA CERTIFICACIÓN DPD

Mis propuestas para un esquema de certificación DPD que considero acordes con la realidad, volumen y complejidad de los tratamientos de datos personales actuales y las proyecciones futuras consisten, a grandes rasgos, en:

Especializaciones por perfil.

1.Certificación DPD jurídica especializada. Incluye terminología y conceptos técnicos básicos, con el fin de contextualizar "lo técnico".

2.Certificación DPD técnica especializada, con una claro enfoque en la aplicación de normas y estándares en materia de seguridad de la información. Incluye contenido básico sobre conceptos y normativa legal en materia de protección de datos personales para su contextualización.

Especializaciones sectoriales tras la especialización por perfil.

1.Administración Pública.
2.Sanidad.
3.Empresa.

Requerimiento de experiencia.

ineludible, a menos que se plantee una certificación "DPD Candidate" para el curso de 180 horas y la aprobación del examen.

CONCLUSIÓN

Es fundamental considerar el rol DPD como un "equipo DPD" donde personas con perfil jurídico y técnico trabajan integradas para ejercer con propiedad las actividades que el RGPD y la LOPDGDD asignan a este rol, **suprimiendo la percepción del DPD unipersonal por inviable.**

FIN DE TEMPORADA

Con esta edición de TySC finaliza la temporada. Espero que las temáticas tratadas hayan sido de vuestro interés.

Escuela de Gobierno

eGob®

https://escueladegobierno.es

Curso de Doble Certificación en:

Gestión de Beneficios y Gestión de Portafolios

P4MGO!® BfM Leader
P4MGO!® PfM Leader

Dirección Académica:
Javier Peris

- Dos formatos para tu comodidad
- Opción A: Remoto en Directo
- Opción B: Virtual con Tutoría
- Metodología P4MGO!®
- Exámenes de Certificación Incluidos
- Certificación P4MGO!® BfM Leader
- Certificación P4MGO!® PfM Leader
- Solicita tu admisión

MPPM® MGEIT® eGob®

Próxima Convocatoria en Directo
Octubre 2024

Solicita tu admisión en:

+ 34 96 109 44 44
admisiones@escueladegobierno.es

P4MGO!

NUEVOS MASTERS

Escuela de Gobierno eGob®
admisiones@escueladegobierno.es
https://escueladegobierno.es