ESPECIAL

"Marcos y Normas"

de Tecnología & Sentido Común

ESPECIAL
AGOSTO
2023

ESPECIAL "Marcos y Normas" de Tecnología & Sentido Común

EQUIPO TYSC
Javier Peris - El Gobernauta
Manuel D. Serrat - Futuro y Seguridad
Maryna Danylyuk - Economía de la Salud
Miguel Angel Arroyo - Hack & News
Juan Carlos Muria - Diario de una Tortuga Ninja
Marlon Molina - Es Tendencia
Ricard Martínez - Ojo Al Dato
Catalina Valencia - Ecosistema Emprendedor
Marcos Navarro - Ai Robot
Víctor Almonacid - La Nueva Administracion
Tommi Lattu - Nordic Mindset
Jesús López Peláz - Consejo de Amigo
Renato Aquilino - Marcos y Normas
Pablo Molina - Ethics Today
Marta Martín - Mentes Divergentes
Lucio Molina - América Próxima
André Pitkowsky - Meu Brasil

PUBLICIDAD Y CONTRATACIÓN
Carmen Usagre
carmen.usagre@businessandcompany.com
Teléfono: +34 96 109 44 44

GABINETE JURÍDICO
Jesús López Peláz

ATENCIÓN AL LECTOR
soluciones@businessandcompany.com

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 Implementer, Lead Auditor ISO 27001-TC y Auditor del Esquema Nacional de Seguridad. Carrera profesional desarrollada 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

MasterGEIT®
Gobierno y Gestión de Información y Tecnología

TITULACIÓN
MasterGEIT®

CONTENIDO DEL MASTER

Módulo 01: Gestión del Tiempo
Curso de Doble Certificación TSG4® Yellow Belt + TSG4® Green Belt

Módulo 02: Gestión de Procesos de Negocio
Curso de Doble Certificación BPM Executive + ISO 19510 Leader

Módulo 03: Dirección y Gestión de Proyectos
Curso de Doble Certificación OpenPM² (PjM) Executive + ISO 21502 Leader

Módulo 04: Dirección y Gestión de Programas
Curso de Doble Certificación OpenPM² (PgM) Executive + ISO 21503 Leader

Módulo 05: Gestión de Servicios de Tecnología
Curso de Doble Certificación FitSM Executive + ISO 2000 Leader

Módulo 06: Gestión de Seguridad de la Información
Curso de Doble Certificación CSX Executive + ISO 27000 Leader

Módulo 07: Gestión de la Continuidad del Negocio
Curso de Doble Certificación CBCI Executive + ISO 22301 Leader

Módulo 08: Gobierno de Información y Tecnología
Curso de Doble Certificación COBIT 2019 Executive + ISO 38500 Leader

Módulo 09: Gobierno del Dato
Curso de Doble Certificación DAMA Executive + ISO 38505 Leader

Módulo 10: Gobierno Corporativo
Curso de Doble Certificación COSO Executive + ISO 37000 Leader

*Niveles de Certificación pertenecientes a los Esquemas de la Entidad de Certificación Business&Co.® y alineados con la Norma UNE-EN ISO/IEC 17024:2012 Evaluación de la Conformidad. Requisitos Generales para los Organismos que realizan Certificación de Personas. Más información: https://businessandcompany.com/certificacion-de-personas

MISIÓN

Nuestra misión consiste en instituir una nueva clase directiva capaz de liderar con éxito las oportunidades que nos brinda la era digital.

FORMACIÓN BUSINESS CLASS

- Formación experiencial y participativa en remoto y en directo para una mayor comodidad del alumno.
- Cursos de cuatro sesiones en formato tardes de martes y jueves o formato viernes tardes y sábados mañanas.
- Máximo doce alumnos por convocatoria para una mayor interacción y compartición de experiencias y anécdotas.
- Cursos de Doble Certificación convalidables por asignaturas del Master en Gobierno y Gestión de Información y Tecnología MasterGEIT®.

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

ESPECIAL AGOSTO 2023

#TYSC TECNOLOGIA Y SENTIDO COMÚN

índice
DE CONTENIDOS

https://tecnologiaysentidocomun.com

¡tyc

#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.

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

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 Comunidad 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.

Premio 2022 ESET al Periodismo y Divulgación en Seguridad Informática

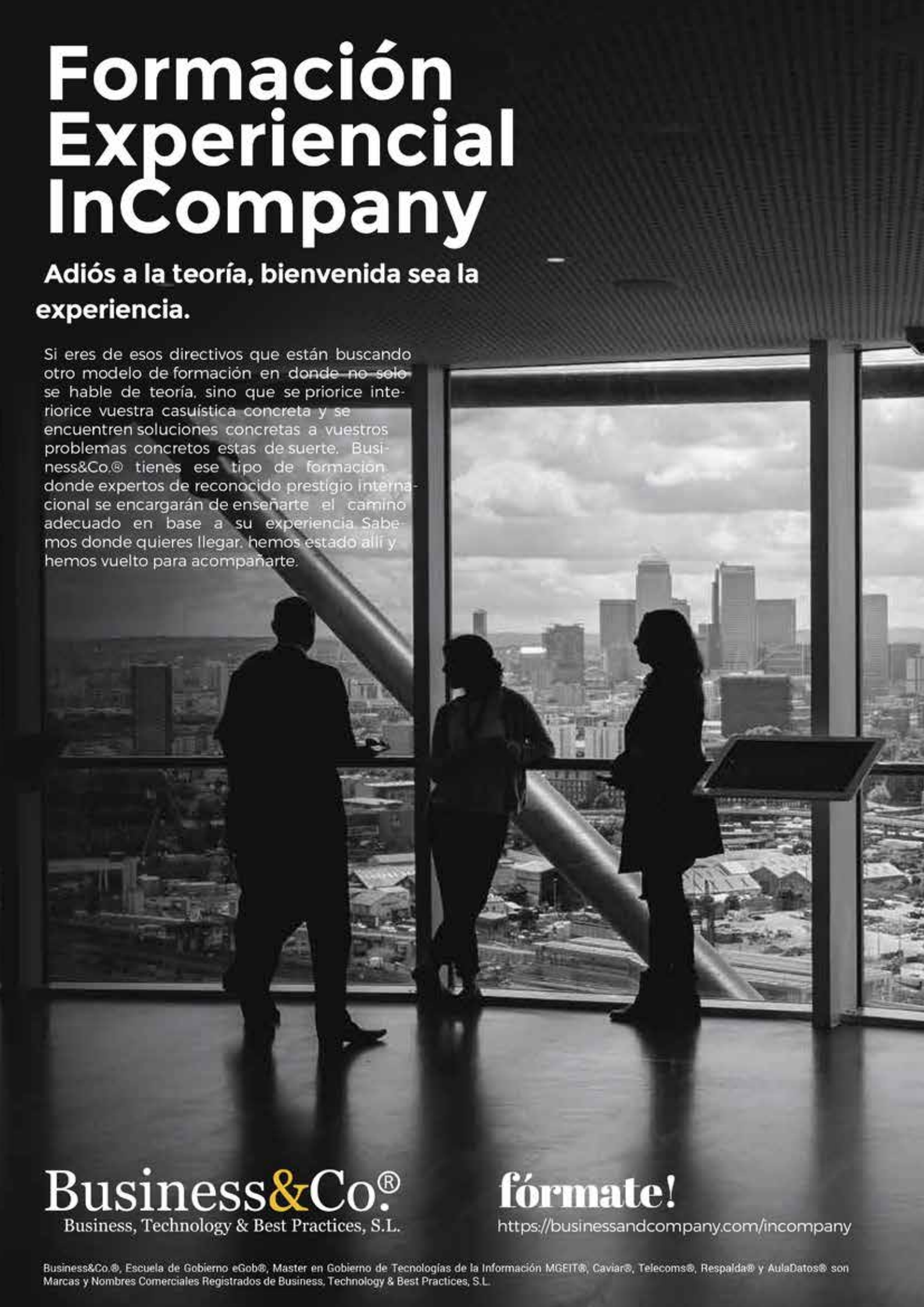
VI Premios ESET Periodismo y Divulgación: Tecnología y Sentido Común Premiada en la Categoría Blogs por el Articulo de Ricard Martínez "Seguridad en el Smartphone".
Los Premios ESET apuestan por la educación y la concienciación de la sociedad en materia de ciberseguridad, y los medios de comunicación 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.

Formación Experiencial InCompany

Adiós a la teoría, bienvenida sea la experiencia.

Si eres de esos directivos que están buscando otro modelo de formación en donde no solo se hable de teoría, sino que se priorice interiorice vuestra casuística concreta y se encuentren soluciones concretas a vuestros problemas concretos estas de suerte. Business&Co.® tienes ese tipo de formacion donde expertos de reconocido prestigio internacional se encargarán de enseñarte el camino adecuado en base a su experiencia. Sabemos donde quieres llegar, hemos estado allí y hemos vuelto para acompañarte.



Business&Co.®
Business, Technology & Best Practices, S.L.

fórmate!
https://businessandcompany.com/incompany

Evento Cierre de temporada y Premio Tecnología y Sentido Común 2023

El miércoles 13 de julio se celebro en la sede de UNE Asociación Española de Normalizacion el evento de Clausura de la 2ª Temporada de Stakeholders.news la Revista Líder de la Alta Dirección y los Profesionales en Gobierno, Dirección y Gestión de Porfolios Programas y Proyectos donde se dieron cita importantes directivos tanto de la Administracion Publica como de empresas privadas.

El Acto fue presentado por Paloma Garcia Lopez, Directora de Normalización y Grupos de Interés de la Asociación Española de Normalización UNE y Javier Peris Chief Knowledge Officer CKO de Business&Co. y director de la revista Stakeholders.news quienes agradecieron al público la fantástica acogida a esta clausura.

Tras una presentación de UNE, su gran actividad de fomento, y difusión de la normalización y su la importante proyección internacional de la entidad a cargo de Paloma Garcia se dio paso a una ponencia magistral a cargo de Marc Berghmans Embajador del Centro de Excelencia PM² (CoEPM²) de la Comisión Europea sobre Gestion de Porfolios (Portfolio Management) y Gestión de Programas (Programme Management) con metodología PM2 de la Comisión Europea.

Recientemente el Centro de Excelencia PM² (CoEPM²) de la Comisión Europea amplio su alcance para desarrollar, mantener y promover metodologías adicionales que incluyen Gestión de Porfolios y Gestión de Programas.

Tras la ponencia de Marc Berghmans los miembros del equipo de Stakeholders.news presentes en el evento ofrecieron una Mesa Redonda moderada por Javier Peris donde explicaron el contenido más significativo de todos los artículos publicados durante esta temporada en cada una de sus respectivas secciones.

CONTINÚA EN PRÓXIMA PÁGINA


Mesa Redonda "Tecnología y Sentido Común"
Manuel Serrat
Juan Carlos Miura
Marcos Navarro
Miguel Angel Arroyo
Sección Hack & News
Stakeholders

En primer lugar, Jose Luis Portela con la sección "Empleo y Futuro" hizo reflexionar al público sobre los importantes cambios de paradigma que van a producirse alrededor del empleo en las próximas décadas. Seguidamente Pedro Balsa, en la sección "Steering Committee" llevo a cabo importantes reflexiones sobre como valorar lo mejor poniendo como ejemplo el mundo del tenis profesional. Charo Fresneda desde su sección "El Lado Humano" puso como hace siempre a las personas en el centro poniendo el énfasis en una adecuada gestion de las emociones y la comunicación como factor determinante del logro de cualquier objetivo. Por su parte Juan Jesus Urbizu desde la sección "TecnoTransformación" nos hizo ver que por encima de la tecnología están las personas que son las que deben poder usar y hacer valer esa tecnología y produzca los resultados adecuados que permitan obtener los beneficios esperados con los que alcanzar los objetivos estratégicos. Por su parte Juan Manuel Dominguez nos habló desde la sección "Organizaciones Resilientes" de importantes reflexiones relativas a la resiliencia.

Javier Peris moderador de la mesa agradeció a todo el equipo de la Revista, tanto a los presentes como a Angela Plaza, Carlos Pampliega, Ricardo Sastre y Luis Guardado quienes que no pudieron asistir al evento por compromisos profesionales.

Tras la Primera Mesa Redonda dedicada al equipo de la Revista Stakeholders.news se dio paso a una segunda Mesa Redonda donde participo el equipo de la Revista hermana "Tecnología y Sentido Común" la Revista Líder de habla hispana de la Alta Dirección y los Profesionales en Gestión de Proyectos, Gestión de Servicios, Gestión de Procesos, Gestión de Riesgos y por supuesto Gobierno de Tecnologías de la Información también moderada por Javier Peris Director de ambas publicaciones y en la que participaron cuatro miembros del equipo de la revista.
La Mesa comenzó con Manuel Serrat y la sección "Futuro y Seguridad" donde se puso el énfasis en la necesidad de una mayor concienciación de la debilidad tecnológica y la importancia de invertir esfuerzos y recursos ante la enorme amenaza que representa el crimen organizado. Juan Carlos Muria de la sección Diario de una Tortuga Ninja hablo de la importancia de unos adecuados procesos y formacion en el ámbito de la Gestion y el Gobierno de las Organizaciones y hablo de su ultimo articulo dedicado a la motivación, esa energía tremendamente poderosa. Marcos Navarro desde su sección "Ai Robot" dedicada a Robotic Process Automation RPA e Inteligencia artificial IA nos lanzo un mensaje claro de un presente en el que los humanos vamos a convivir con robots no necesariamente humanoides tanto en el ámbito profesional como en el personal a modo de asistentes para multitud de tareas. Por último, Miguel Angel Arroyo de la sección "Hack&News" puso el énfasis en la Ciberseguridad y en la Inteligencia de Amenazas y como la inteligencia artificial tambien puede ayudar de una manera considerable a reducir el impacto en las organizaciones respecto de la ciberdelincuencia.

Javier Peris hizo notar la gran densidad de conocimiento de la Revista Tecnología y Sentido Común con 16 colaboradores qe generan mensualmente un documento de más de cien páginas repletas de Tecnología pero sobre todo de sentido común convirtiendo esta publicación en la revista menos friqui de tecnología de las que existen hoy en el mercado y finalizo agradeciendo a Maryna Danylyuk de "Economía de la Salud", Marlon Molina de "Es Tendencia, Ricard Martinez de "Ojo Al Dato", Catalina Valencia de "Ecosistema Emprendedor", Victor Almonacid de "La Nueva Administracion, Tommi Lattu de "Nordic Mindset" Jesus Lopez Pelaz de "Consejo de Amigo", Renato Aquilino de "Normas y Marcos", Pablo Molina de "Ethics Today", Marta Martín de "Mentes Divergentes" y Lucio Molina de "América Próxima" quienes con su trabajo y su absoluta generosa construyen mes a mes este impresionante documento que se puede disfrutar gratuitamente.

Siguiendo la agenda del evento, Javier Peris Director de ambas publicaciones invitó a participar a los nuevos fichajes de ambas revistas quienes explicaron ante la audiencia los contenidos que van a tratar dentro de cada una de sus respectivas secciones.

Los nuevos miembros del equipo que comenzarán a publicar en la próxima temporada que dará comienzo en setiembre son, por parte de Tecnologia y Sentido Común se incorporan Nacho Alamillo con la sección "Tecnoregulación en Prospectiva" quien nos traerá la actualidad reguladora tanto de España como de la Unión Europea en materia tecnológica con el foco en tecnologías disruptivas y basadas en cadena de bloques y entidad raíz de confianza. Y German Sanchis con la Sección "I'm IA" dedicada a la Inteligencia Artificial quien disculpó la asistencia al evento.

Por parte de la Revista Stakeholders.news se incorporan Jose Antonio Puentes, veterano Maestros y Director de Proyectos quien desde la sección "Tendiendo Puentes" se comprometió a compartir experiencias y consejos atesorados en su dilatada carrera profesional para que puedan

ser de utilidad al resto de profesionales y nuevas generaciones que se adentren en el maravilloso mundo del Cambio Organizacional. Luis Moran desde "Procesos y Personas" tambien ofreció todo su conocimiento alrededor de la Gestion de Procesos y Personas para ayudar al conjunto de la profesión desde su conocimiento y experiencia con el fin último de ayudar a crear mejores organizaciones. Para finalizar esta mesa redonda, Alejandro Aliaga desde "Radio Security" pondrá el acento mes a mes en desgranar nuevos vectores de amenazas que habitualmente pasan desapercibidos no por menos vulnerables y cuyos impactos en las organizaciones y en la vida de las personas pueden ser tremendamente significativos ¿Son los satélites vulnerables? nos anticipaba.

Llegado al punto álgido de la jornada se otorgaron los premios Tecnologia y Sentido Común 2023 y Stakeholders.news 2023" siendo entregados a UNE Asociación Española de Normalizacion y al Centro de Excelencia PM² (CoEPM²) de la Comisión Europea respectivamente.

Javier Peris, en nombre de todo el equipo de Tecnología y Sentido Común anunció como ganador del Premio "Tecnologia y Sentido Común 2023" a UNE Asociación Española de Normalizacion por su importante trabajo, su gran influencia y su elevada reputación mundial en el ámbito de la normalización, premio que fue recogido por Alfredo Berges, Presidente de UNE.

Alfredo Berges agradeció el Premio y elogio la labor de ambas publicaciones que se alienan con los objetivos de la asociación de crear un mundo mejor a través de la creación y difusión de Normas, Estándares, Metodologías y Bases de Conocimiento que permitan un futuro mejor. Alfredo Berges Presidente de UNE aseguró que "Es un reconocimiento que nos hace más ilusión si cabe al ser concedido por uno de nuestros miembros, Business&Co.®, Miembro Adherido Empresa de UNE, y que ha sido entregado por Javier Peris, quien preside el Comité de Gestión de servicios y Gobierno de la Tecnología de la Información y con el que tenemos una relación muy estrecha desde hace varios años".

Javier Peris, en nombre de todo el equipo de Stakeholders.news anuncio como ganador del premio "Stakeholders.news 2023" al Centro de Excelencia PM² (CoEPM²) de la Comisión Europea por haber ampliado su alcance para desarrollar, mantener y promover metodologías adicionales que incluyen Gestión de Porfolios y Gestión de Programas, premio que fue recogido por Marc Berghmans embajador de PM² de la Comisión Europea.

CONTINÚA EN PRÓXIMA PÁGINA

Marc Berghmans agradeció el premio y elogio la labor de difusión que viene llevando a cabo la revista no solo en el ámbito de Proyectos sino en el de Programas y Porfolios e invitó a la toda la audiencia a descargarse de manera gratuita y usar la metodología PM² que ha sido sufragada por todos los ciudadanos de la Unión Europea y ahora hay que aprovecharse de ello y usarla. Javier Peris le agradeció enormemente el esfuerzo que ha llevado a cabo Marc Berghmans con su presencia en el evento por encontrase en este momento de vacaciones.

Para finalizar el evento Javier Peris presentó a Antonio Galvez, Maestro Cortador de Jamón Ibérico quien realizaría una demostración de corete en vivo y degustación de un Jamon ibérico con el que deleitar el paladar de todos los asistentes e invito a todos a volvernos a leer la próxima temporada.

El Networking entre los asistentes, grandes profesionales tanto de la administración pública como de la empresa privada se extendió por mas de una hora y en donde además de degustar el Jamón Ibérico recién cortado por las manos expertas de un Maestro Cortador se pudieron compartir anécdotas, consejos y reflexiones entre todos los invitados.

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

¡Despegamos!

Nueva e ilusionante etapa de colaboración en Tecnología y Sentido Común.

Este artículo inicia mi aportación a la sección "Marcos y Normas", siendo para mí un honor colaborar en **Tecnología y Sentido Común** junto a un equipo de personas referentes en cada una de sus secciones. En esta publicación inicial expongo los contenidos y el enfoque de la sección, dedicada a los marcos normativos y normas estándares relacionados con el amplio concepto de "seguridad de la información".

Mi nombre es Renato Aquilino Pujol. Soy Licenciado en Informática por la Universitat Politécnica de Catalunya, Especialista Universitario en Protección de Datos y Privacidad por la Facultad de Derecho de la Universidad de Murcia, CISA, CISM, CGEIT, COBIT-5 Implementer, implantador / auditor del Esquema Nacional de Seguridad, ISO/IEC 27001:2013 e ISO 22301:2019.

Mi carrera ha evolucionado desde la ingeniería de sistemas, con los primeros despliegues del entonces novedoso sistema operativo UNIX, Windows NT Server, BBDD Informix. Oracle, etc, hacia la consultoría en sector público (SICAL, TAO, etc) y privado (ERP Navision, SAP R/3, etc) y, posteriormente, a la consultoría y auditoría sobre normas estándares en materia de seguridad y continuidad (aquellas BS 7799, BS 25999 posteriormente derivadas en las normas ISO/IEC 27001 e ISO 22301) y, desde el año 2010, en la implantación y auditoría del Esquema Nacional de Seguridad, todo ello en relación, adicionalmente, con los aspectos organizativos y técnicos de la legislación en materia de protección de datos personales, desde la LORTAD, LOPD, RGPD y LOPDGDD.

Esta carrera profesional me ha permitido profundizar en los diferentes marcos normativos y normas estándares relacionados con ese amplio concepto de "seguridad de la información", obteniendo de los numerosos proyectos desarrollados una gran cantidad de **escenarios prácticos** que espero trasladar a esta sección, la cual pretende exponer los marcos y normas sobre seguridad de la información bajo un enfoque **eminentemente práctico**, orientado a escenarios de aplicabilidad fácilmente "aterrizables" en casos reales de organizaciones públicas y privadas, huyendo de la "indigestión normativa" que podría provocar una exposición puramente enumerativa de marcos y estándares y procurando ofrecer una visión holística pero comprensible de los mismos. Es decir, esta sección no pretende ser un curso de marcos y normas sino una exposición de sus criterios y medidas sobre las diferentes casuísticas que voy a desarrollar, si bien podrá ser necesario en algún momento exponer texto concreto de sus preceptos para justificar o soportar el caso.

La sección va **dirigida tanto al sector público como al sector privado**, teniendo en cuenta los requerimientos específicos para el sector privado que ofrece productos y servicios para el sector público. A los efectos de esta sección, y dado que las normas estándares ISO e ISO/IEC mencionan la palabra "negocio" como contexto organizativo de las mismas, se asume que "negocio" es equivalente a "servicio" en el sector público.

CONTINÚA EN PRÓXIMA PÁGINA


("SpinnerPodium").GetComponent
("SpinnerPodium").GetComponent
followTransform.position);
spinnable
true) {
= false;
FindGameObjectsWithTag("Hotspots")) {
alwaysHideMe == false) {
();
followTransform.position);
startPosition, slerpVal);
= true;
WithTag("Hotspots")) {
closeButton> ().showMe ();
slerpVal);

DIMENSIONES DE LA SEGURIDAD

Soy consciente de que la mayoría de las personas que lean este artículo conocen sobradamente los conceptos que siguen, pero he considerado conveniente incluirlos principalmente para los perfiles menos habituados a su manejo. El alcance del término "seguridad de la información" es muy amplio y engloba visiones diferentes del mismo, denominadas por los marcos y normas como "dimensiones de la seguridad", cuyas definiciones son semánticamente iguales en todos ellos. Tomando como fuente el Anexo IV (glosario de términos) del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS en adelante):

•**Confidencialidad:** propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.
•**Disponibilidad:** propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.
•**Integridad:** propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.
•**Autenticidad:** propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
•**Trazabilidad:** propiedad o característica consistente en que las actuaciones de una entidad (persona o proceso) pueden ser trazadas de forma indiscutible hasta dicha entidad.

La norma ISO/IEC 27001:2013 contempla como dimensiones de seguridad la Confidencialidad, Integridad y Disponibilidad, si bien la Autenticidad y la Trazabilidad están contempladas también de forma explícita en sus controles.
La norma ISO 22301:2019 desarrolla la dimensión Disponibilidad en forma de Sistema de Gestión de la Continuidad de Negocio (SGCN en adelante).

MARCOS NORMATIVOS Y NORMAS ESTÁNDARES - CONTEXTO

No descubro nada nuevo al afirmar que la seguridad de la información se ha convertido en un factor clave para la viabilidad de cualquier organización, pública o privada, máxime cuando los modelos de negocio o servicio están basados en tecnologías de la información (TI en adelante) y dependen de las mismas.

Este escenario conlleva la necesidad de establecer unos criterios normalizados de apreciación de riesgos, implementación y mejora continua de medidas de seguridad, métricas e indicadores, y **certificación ante partes interesadas internas y externas** de un sistema de gestión que lo materializa. Este necesidad de normalización ha derivado en:

•**Normas estándares.** Cumplimiento no obligatorio, decisión de la organización por iniciativa propia o por requerimientos de partes interesadas en su modelo de negocio. Como ejemplo, ISO/IEC 27001 e ISO 22301 dentro del ámbito de esta sección. Su catalogación como "estándar" se basa en la amplia aceptación global de sus criterios y su certificación.

•**Marcos normativos.** Cumplimiento por obligación legal para las organizaciones dentro de su ámbito subjetivo, tanto públicas como privadas, dado que se trata de legislación vigente. Como ejemplo, Esquema Nacional de Seguridad (Real Decreto 311/2022) en esta sección.

ENFOQUE IMPLANTACIÓN / CERTIFICACIÓN DE MARCOS NORMATIVOS Y NORMAS ESTÁNDARES.

Tanto el ENS como ISO 27001 e ISO 22301 son **certificables.** Esta sección incluirá no solo **criterios de implantación** sino también **recomendaciones para el proceso de certificación**, todo ello, por supuesto, teniendo en cuenta las limitaciones de espacio inherentes a una publicación multidisciplinar como **Tecnología y Sentido Común**.

MasterPPM®

Gobierno, Dirección, Gestión y Ejecución de Porfolios, Programas y Proyectos

TITULACIÓN
MasterPPM®

CONTENIDO DEL MÁSTER

Módulo 01: Gestión del Tiempo
Curso de Doble Certificación TSG4® Yellow Belt + TSG4® Green Belt

Módulo 02: Gestión de Procesos de Negocio
Curso de Doble Certificación BPM Executive + ISO 19510 Leader

Módulo 03: Dirección y Gestión de Proyectos
Curso de Doble Certificación OpenPM² (PjM) Executive + ISO 21502 Leader

Módulo 04: Dirección y Gestión de Programas
Curso de Doble Certificación OpenPM² (PgM) Executive + ISO 21503 Leader

Módulo 05: Gestión de Servicios de Tecnología
Curso de Doble Certificación FitSM Executive + ISO 20000 Leader

Módulo 06: Gestión de Proyectos Ágiles
Curso de Doble Certificación OpenPM² (Ágil) Executive + KANBAN Leader

Módulo 07: Dirección y Gestión del Porfolio
Curso de Doble Certificación OpenPM² (PfM) Executive + ISO 21504 Leader

Módulo 08: Gobierno de Proyectos, Programas y Porfolios
Curso de Doble Certificación P3MGO® Executive + ISO 21505 Leader

Módulo 09: Gobierno de la Externalización
Curso de Doble Certificación SGF Executive + ISO 37500 Leader

Módulo 10: Gobierno Corporativo
Curso de Doble Certificación COSO Executive + ISO 37000 Leader

*Niveles de Certificación pertenecientes a los Esquemas de la Entidad de Certificacion Business&Co.® y alineados con la Norma UNE-EN ISO/IEC 17024:2012 Evaluación de la Conformidad. Requisitos Generales para los Organismos que realizan Certificación de Personas. Más información: https://businessandcompany.com/certificacion-de-personas

MISIÓN

Nuestra misión consiste en instituir una nueva clase directiva capaz de liderar con éxito las oportunidades que nos brinda la era digital.

FORMACIÓN BUSINESS CLASS

- Formación experiencial y participativa en remoto y en directo para una mayor comodidad del alumno.
- Cursos de cuatro sesiones en formato tardes de martes y jueves o formato viernes tardes y sábados mañanas.
- Máximo doce alumnos por convocatoria para una mayor interacción y compartición de experiencias y anécdotas.
- Cursos de Doble Certificación convalidable por asignatura del Master en Gobierno, Dirección, Gestión y Ejecución de Porfolios, Programas y Proyectos MasterPPM®.

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

Certificación del ENS Asignatura pendiente (I)

Luces y sombras en un proceso de certificación obligatorio

La situación actual del proceso de certificación del sector público y privado sobre el Esquema Nacional de Seguridad (ENS en adelante) expone un escenario preocupante y que incide seriamente en la acreditación de los niveles de ciberseguridad en ambos sectores, justamente cuando los ciberataques alcanzan frecuencias e impactos cada vez mayores.

La implantación y certificación del cumplimiento del ENS, al ser un proceso obligatorio emanado desde la Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad, se convierte en un **mecanismo de seguridad jurídica y no solo técnica**, ya que, si bien esta certificación no nos puede asegurar inmunidad ante los ataques, sí nos permite acreditar ante los organismos inspectores (p.e. AEPD) que la entidad certificada ha implementado los preceptos y las medidas de seguridad organizativas y técnicas requeridas en el ENS. De hecho, la AEPD ya ha instruido un procedimiento sancionador contra un Ayuntamiento por la carencia de estas medidas, a raíz de una brecha de seguridad que habían sufrido.

¿Obligatorio? Sí, para todas las Administraciones Públicas en sus diversas formas jurídicas, para sus tratamientos de datos personales y servicios afectados por el ámbito objetivo del ENS y/o los marcos normativos donde el ENS queda referenciado. Misma obligatoriedad para todas las entidades privadas que ofrezcan productos y/o servicios a las Administraciones Públicas cuando se tratan datos personales bajo responsabilidad de éstas o bien los servicios prestados queden afectados por el ámbito objetivo del ENS y/o los marcos normativos donde el ENS queda referenciado.

Expuesto el escenario, la realidad es radicalmente distinta entre el sector público y el privado. Mientras que en este último el número de sistemas de información certificados aumenta de forma constante, dado que ya es habitual que dicha certificación sea un requerimiento en las licitaciones (discutible en su forma y contenido, como veremos en una próxima entrega) el caso del sector público refleja una situación donde el número de certificaciones queda en niveles mínimos, sobre todo en las entidades donde se concentra un gran número de tratamientos sensibles de datos, los Ayuntamientos. El registro de entidades certificadas es público y está disponible en el portal web del Centro Criptológico Nacional (CCN), siendo ésta la fuente de las cifras expuestas a continuación, consultada en fecha 04/09/2022.

CONTINÚA EN PRÓXIMA PÁGINA

Número de Ayuntamientos en España: **8.131** (Instituto Nacional de Estadística).

Número de Ayuntamientos con un sistema de información certificado en el ENS: **21 de 8.131**, es decir, el **0'26% del total.** Si bien esta cifra ya es significativa en sí misma, analizando las entidades y los sistemas certificados extraemos
datos interesantes.

- Capitales de provincia:
1 (Donostia / San Sebastián) de 50 capitales

-Municipios con población > 75.000 habitantes: 2
-Municipios con población >= 20.000 y < 75.000 habitantes: 0
-Municipios con población >= 5.000 y < 20.000 habitantes: 4
-Municipios con población < 5.000 habitantes: 15. Entre éstos, 9 municipios tienen menos de 1000 habitantes.

Los datos sobre población han sido obtenidos de las estadísticas del INE correspondientes al año 2021. Los intervalos son los utilizados por el CCN para segmentar los perfiles de cumplimiento del ENS para Ayuntamientos.

Por otra parte, ¿Cuál es el alcance de estos sistemas certificados? Todos los Ayuntamientos menos uno han certificado "Los sistemas de información que dan soporte a la sede electrónica". El Ayuntamiento "discordante" ha certificado "Los sistemas de información que dan soporte a las actividades de la Policía local, administrativas y judiciales" y esto ya indica la insuficiencia de las certificaciones actuales, dado que, en la Sede Electrónica, no se gestionan todas las actuaciones municipales, quedando fuera de la misma, por ejemplo, intervenciones de Servicios Sociales en violencia de género, conductas adictivas, protección de infancia y adolescencia, intervenciones de la Policía Local en cuestiones de seguridad ciudadana, controles de alcoholemia y drogadicción, atestados, etc. Es decir, **las certificaciones actuales de los Ayuntamientos tampoco cubren los servicios que gestionan datos de la máxima sensibilidad y que no forman parte de la Sede Electrónica**.

Las Diputaciones Provinciales ofrecen servicios diversos a los Ayuntamientos, siendo habitual que, entre estos servicios, se ofrezcan prestaciones de sistemas de información como Padrón Municipal de Habitantes, gestión de nóminas y recursos humanos, contabilidad y finanzas, gestión tributaria y recaudación, etc. Es decir, una concentración de servicios a diversos Ayuntamientos que, sin embargo, no tiene un reflejo en el número de Diputaciones con sistemas certificados, ya que únicamente 2 de ellas (Albacete y Huesca) disponen de certificación.

La situación es igualmente preocupante en el resto del sector público.

-Administración General del Estado: 10 organismos con algún sistema certificado.

-Comunidades Autónomas: 10 Comunidades Autónomas han certificado 38 sistemas de información, si bien la Junta de Andalucía, por sí misma, dispone de 22 certificaciones.

-Universidades: Sólo 4 Universidades han certificado sistemas de información.

-Sector Público Institucional: 53 certificaciones de muy diversos organismos.

En el **sector privado** se han emitido 517 certificaciones de sistemas de información para 494 entidades.

Paralelamente, existe una "certificación de productos y servicios" 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, cuya última edición a la fecha data de agosto de 2022. Esta guía incluye un amplio inventario de productos como antivirus, sistemas operativos, cortafuegos, etc.

Las aplicaciones informáticas (como gestores de expedientes, gestión del Padrón,…), así como los servicios en la nube, comunicaciones, etc, deben buscarse en la página "Empresas certificadas" del portal web del CCN dedicado al ENS.

Por limitaciones de espacio, la problemática de la certificación del ENS y mi opinión sobre las causas de la situación expuesta será desarrollada en una próxima publicación de Tecnología y Sentido Común.

MGEIT® MPPM®

eGob®

TSG4® Yellow Belt + Green Belt
Time Slot Governance
Gestión del Tiempo

COMIENZA POR
ORGANIZARTE

Si vas desbordado, te cuesta cumplir con las necesidades de negocio, no eres capaz de evidenciar el valor que aportas y no te da la vida para implantar Buenas Prácticas comienza por organizarte tú y organizar tu equipo con Time Slot Governance TSG4® Porque lo que no es Método es Improvisación

NIVELES DE CERTIFICACIÓN

TSG4® YELLOW BELT*
Forma y Certifica a Resposables y Miembros del Equipo en la Metodología de Gestión del Tiempo Time Slot Governance TSG4®

TSG4® ORANGE BELT*
Reconoce y Certifica a Miembros del Equipo que aplican la Metodología de Gestión del Tiempo Time Slot Governance TSG4®

TSG4® GREEN BELT*
Forma y Certifica a Responsables de los Equipos en la Metodología de Gestión del Tiempo Time Slot Governance TSG4®

TSG4® BROWN BELT*
Reconoce y Certifica a Responsables de Equipos que aplican la Metodología de Gestión del Tiempo Time Slot Governance TSG4®

TSG4® BLACK BELT*
Forma y Certifica a Implementadores de Buenas Prácticas con la Metodología de Gestión del Tiempo Time Slot Governance TSG4®

*Niveles de Certificación pertenecientes a los Esquemas de la Entidad de Certificacion Business&Co.® y alineados con la Norma UNE-EN ISO/IEC 17024:2012 Evaluación de la Conformidad. Requisitos Generales para los Organismos que realizan Certificación de Personas. Más información: https://businessandcompany.com/certificacion-de-personas

MISION

Nuestra misión consiste en instituir una nueva clase directiva capaz de liderar con éxito las oportunidades que nos brinda la era digital.

FORMACIÓN BUSINESS CLASS

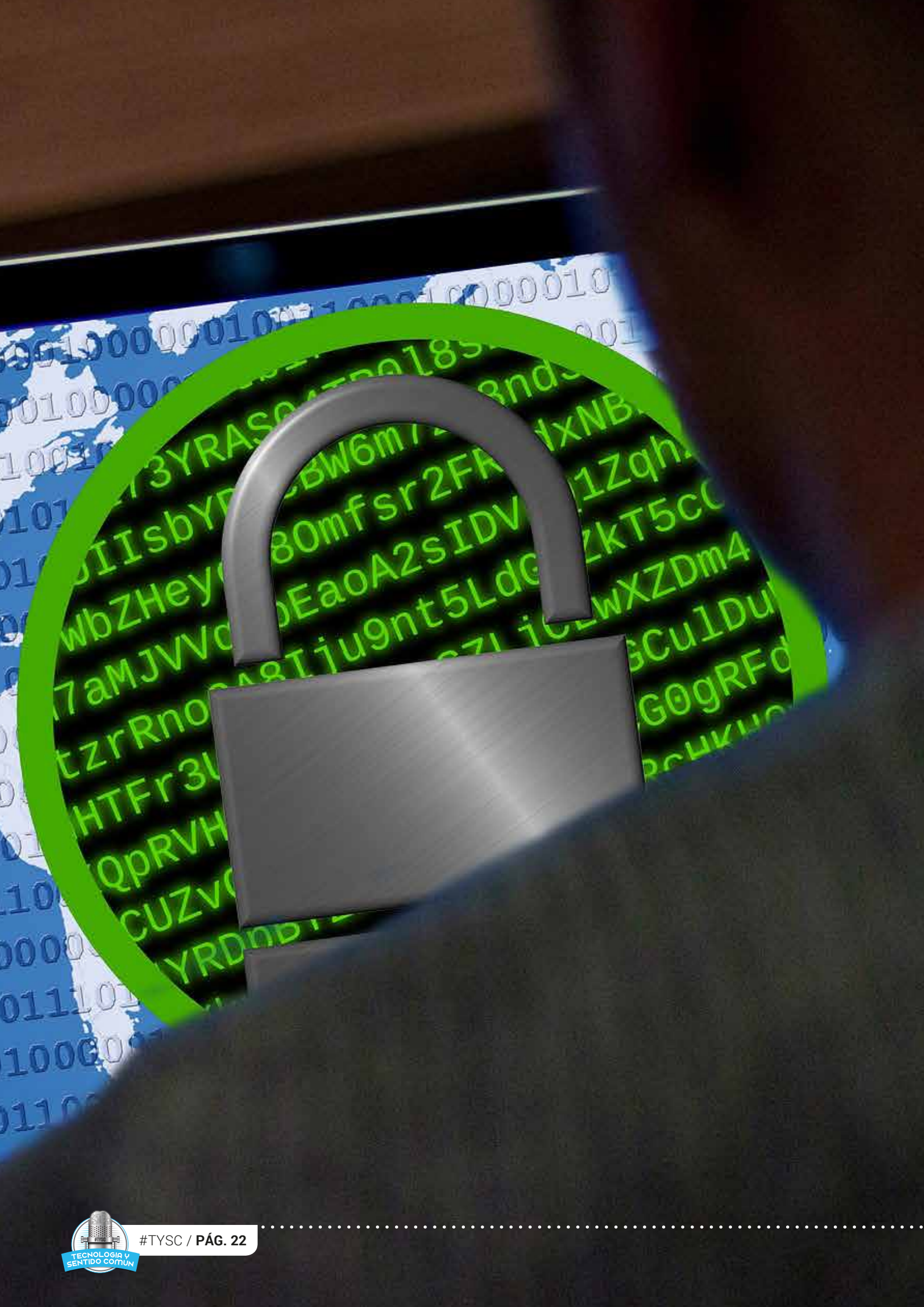
- Formación experiencial y participativa en remoto y en directo para una mayor comodidad del alumno.
- Cursos de cuatro sesiones de 5 horas en formato tardes de martes y jueves o formato viernes tardes y sábados mañanas.
- Máximo doce alumnos por convocatoria para una mayor interacción y compartición de experiencias y anécdotas.
- Cursos de Doble Certificación convalidables por asignaturas de los Masters MasterGEIT® y/o MasterPPM®.

CONVOCATORIAS 2022/23

- **TSG4® Yellow Belt + Green Belt (Martes y Jueves Tardes)**
  TSG4® Yellow Belt 15 de Septiembre de 2022 (Miércoles)
  TSG4® Green Belt 4, 6, 8 y 12 de Junio de 2023 (Martes y Jueves)
- **TSG4® Yellow Belt + Green Belt (Viernes Tardes y Sabados Mañana)**
  TSG4® Yellow Belt 1 de Octubre de 2022 (Sábado)
  TSG4® Green Belt 7, 8, 14 y 15 de Julio de 2023 (Viernes y Sábados)

eGob®

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



Certificación del ENS – Asignatura pendiente (y II)

Causas de la "no certificación" del ENS en el sector público

En la edición de octubre de TySC expuse el poco ejemplarizante número de entidades del sector público certificadas en el ENS, muy especialmente en la Administración Local. En esta edición expongo los que, en mi opinión y muy resumidos, son los motivos que nos llevan al escenario expuesto.

CAMBIOS NORMATIVOS Y FALTA DE REFERENTES

Esta situación viene de lejos, por lo que no es válido argumentar que no se ha abordado el proceso debido a la nueva edición del ENS 2022. Tampoco es válido argumentar la espera de "perfiles de cumplimiento" para Ayuntamientos, dado que estos perfiles están disponibles desde mayo del año 2020 y no han conseguido dinamizar las certificaciones.

Por parte del CCN se han desarrollado diferentes documentos de soporte al cumplimiento del ENS para Entidades Locales, todo ello con la participación activa de personas y entidades directamente implicadas en la casuística de la Administración Local. Documentos de alto valor para facilitar el proceso, por lo que sí existen referentes sectoriales.

LA SEGURIDAD, EN MAYOR O MENOR MEDIDA, SE TRADUCE EN EUROS.

Evidente, pero ¿quién tiene la llave de los euros? el órgano que ostente las máximas competencias ejecutivas (ENS 2022), denominado "órgano superior competente" en el texto del ENS 2010. En la guía "ENS-Preguntas frecuentes" publicada por el CCN se recoge un párrafo clarificador: "*… Obsérvese que los órganos superiores que menciona el ENS se corresponden con aquellos órganos administrativos* ***entre cuyas competencias se encuentra la determinación y asignación presupuestaria del organismo****, circunstancia lógica, a la vista de que el cumplimiento del ENS supondrá, en la mayoría de los casos,* ***la debida asignación presupuestaria*** *que requiere su implantación*". Ya tenemos identificado el dueño de la llave de los euros, pero observamos en general una escasa conciencia sobre los ciber-riesgos y sus consecuencias, excepto en los casos donde ya han sufrido un ataque con repercusión operativa y mediática. En estos casos asistimos a una auténtica reconversión de posturas al respecto, siempre acompañada de los típicos "in-bles": in-concebi-ble, in-asumi-ble, in-crei-ble, y una promesa de inversiones inmediatas para evitar la recurrencia. Estos órganos, en general, no tienen conocimiento previo de la existencia del ENS ni, por supuesto, de su obligatoriedad, tampoco de la relación directa entre ENS y LOPDGDD.

¿QUÉ ME PASA SI NO CUMPLO EL ENS?

El ENS no contiene procedimiento sancionador, por lo que las posibles consecuencias de los incumplimientos vendrían determinadas por normativas externas. Uno de los escenarios más habituales en Ayuntamientos y entidades supramunicipales proviene de brechas de seguridad afectando a datos personales, aplicando en este caso el régimen sancionador de la LOPDGDD, el cual, para las Administraciones Públicas, **no contempla sanciones económicas, únicamente apercibimiento**, con posible propuesta de actuaciones disciplinarias (a decidir por el Organismo) y diversas publicaciones del asunto. Es decir, **nada disuasorio**. Esta sensación de impunidad es un claro inhibidor de los proyectos de implantación y certificación del ENS, máxime en un contexto presupuestario restrictivo con priorizaciones a decidir.

CONTINÚA EN PRÓXIMA PÁGINA

ENS, ESE DESCONOCIDO

Observamos que el desconocimiento del ENS no afecta sólo al órgano superior competente, sino que se extiende también a funcionarios clave en el Organismo que podrían influir e impulsar su cumplimiento, sobre todo responsables de servicio y habilitados nacionales. En TySC tenemos un ejemplo extraordinario (Víctor Almonacid), Secretario implicado históricamente en estas cuestiones, desarrollando una ingente labor de formación y concienciación en toda la Administración Pública sobre estas cuestiones, junto a otras personas referentes en la materia, pero esa labor todavía no se ha traducido en proyectos integrales de cumplimiento y certificación en la mayoría de los Ayuntamientos.

EL ENS ES COSA DE LOS TÉCNICOS

Existe una percepción entre quienes conocen la existencia del ENS de que se trata de "temas técnicos del área de Informática", cuando este marco normativo contiene disposiciones que afectan a todo el Organismo en aspectos jurídicos, organizativos y técnicos, abordados como un sistema de gestión de seguridad de la información que involucra todos los estamentos corporativos, tal como recoge su artículo 6 – *La seguridad como un proceso integral*.

ÁREA DE INFORMÁTICA – EL ENS REQUIERE MUCHO TRABAJO ADMINISTRATIVO

Es muy habitual encontrar medidas técnicas de seguridad que cumplen con los requerimientos del ENS, pero, en numerosas ocasiones, están diseñadas, implementadas y mantenidas sin un análisis previo de riesgos que ayude a determinarlas, sin una adecuada interacción con los responsables de servicios para conocer sus requerimientos, sin indicadores de su eficacia y eficiencia, sin visión sobre la seguridad específica de los datos personales … Es decir, sin un sistema de gestión que permita abordar la ciberseguridad como un proceso integral y corporativo.

El ENS incluye "trabajos administrativos", efectivamente, ya que requiere políticas, normativas, procedimientos, instrucciones, registros, indicadores, procesos de autorización y otras actividades que conforman un entorno documentado, gestionado y controlado, donde el conocimiento persiste no solo en las mentes y notas del personal, pero nos encontramos en numerosas ocasiones con departamentos de Informática infradimensionados, sobrecargados de trabajo, y que ven el ENS como una carga adicional cuando deben soportar los "trabajos administrativos" que les afectan. Esta infradimensión de recursos humanos es otro claro inhibidor del cumplimiento y certificación del ENS.

¿CONCLUSIONES?

Las causas expuestas en los puntos anteriores **no son alternativas, sino acumulativas**, siendo habitual encontrarlas todas ellas en un mismo Organismo. Es por ello que la implicación del órgano superior competente es la condición "sine qua non" para que el proyecto consiga su objetivo, exigiéndose a sí mismo su participación activa (p.e. en el Comité de Seguridad) y exigiendo a todo el personal su implicación directa, así como dotando los recursos humanos y técnicos adecuados, internos y/o externos.

En estos artículos sólo pretendo exponer de forma resumida, por motivos de espacio, algunos de los aspectos que considero relevantes para comprender la precaria situación actual y sus motivos. En sucesivos artículos entraré en recomendaciones para su implantación y certificación con un objetivo de "mínimo impacto" sobre los recursos disponibles.

MGEIT® MPPM®

eGob®

BPM + ISO 19510

Business Process Management

Gestión de Procesos de Negocio

CERTIFÍCATE EN PROCESOS

Si quieres aportar valor al negocio comienza por Descubrir, Modelar, Implementar, Automatizar y Mejorar sus Procesos de Negocio con Busines Process Management BPM. Además la Gestión por Procesos es el origen del resto de Buenas Practicas relacionadas con Proyectos, Servicios, Productos o Riesgos pues todas ellas se basan exactamente en Procesos.

NIVELES DE CERTIFICACIÓN

Nivel de Certificación Board*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de la materia, su entorno y ámbito de aplicación, sus roles y responsabilidades que les permita participar en las inicativas.

Nivel de Certificación Executive*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de las Buenas Prácticas, Metodologías y Bases de Conocimiento aplicables con el fin de dirigir o participar en equipos de implementación.

Nivel de Certificación Leader*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de las normas y Estándares ISO aplicables con el fin de dirigir o participar en equipos de implementación.

Nivel de Certificación Skilled*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de la elaboracion de documentos, informes, planes, herramientas y/o artefactos que les permitan la aplicación práctica de los conocimientos.

*Niveles de Certificación pertenecientes a los Esquemas de la Entidad de Certificacion Business&Co.® y alineados con la Norma UNE-EN ISO/IEC 17024:2012 Evaluación de la Conformidad. Requisitos Generales para los Organismos que realizan Certificación de Personas. Más información: https://businessandcompany.com/certificacion-de-personas

MISION

Nuestra misión consiste en instituir una nueva clase directiva capaz de liderar con éxito las oportunidades que nos brinda la era digital.

FORMACIÓN BUSINESS CLASS

- Formación experiencial y participativa en remoto y en directo para una mayor comodidad del alumno.
- Cursos de cuatro sesiones en formato tardes de martes y jueves o formato viernes tardes y sábados mañanas.
- Máximo doce alumnos por convocatoria para una mayor interacción y compartición de experiencias y anécdotas.
- Cursos de Doble Certificación convalidables por asignaturas de los Masters MasterGEIT® y/o MasterPPM®.

CONVOCATORIAS 2022/23

- **SEPTIEMBRE 2022 (Formato Martes y Jueves Tardes)**
  Martes 20, jueves 22, martes 27 y jueves 29
- **OCTUBRE 2022 (Formato Viernes Tardes y Sábados Mañanas)**
  Viernes 21, sabado 22, viernes 28 y sábado 29
- **FEBRERO 2023 (Formato Viernes Tardes y Sábados Mañanas)**
  Viernes 3, sabado 4, viernes 10 y sábado 11

eGob

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

ISO/IEC 27001: 2022 y complementarias. La familia crece.

¿Sequía? Llueven normas y revisiones de la familia ISO 27XXX

Este año 2022 está siendo altamente productivo en cuanto a la publicación de normas y estándares relacionados con el amplio concepto de "seguridad de la información. En este artículo el protagonismo es para la norma **certificable** ISO/IEC 27001:2022 y el conjunto de normas asociadas y/o complementarias, principalmente las que considero "nucleares", ISO/IEC 27002:2022 e ISO/IEC 27005:2022, así como el nacimiento de nuevas normas en la familia, muy especialmente dedicadas a la privacidad.

¿QUÉ APORTAN ESTAS NORMAS?

Estas normas no aportan en sí mismas medidas organizativas y técnicas novedosas. Una primera lectura de su contenido, sobre todo en el caso de los controles de ISO/IEC 27002, suele llevar a reflexiones del tipo "eso ya lo hago yo". Otras personas expresan una cierta decepción al ver el escaso nivel de detalle de la guía de implementación de los controles (sobre todo cuando ven los 200€ que han pagado por ella) pero, siendo comprensibles estos planteamientos, su valor viene por otras vías.

En mi opinión, el mayor valor añadido de estas normas es la aportación de "**sentido común escrito y estructurado**", así como la implicación de los estamentos directivos de la organización en el SGSI (incluyendo el compromiso de dotación de los recursos necesarios en todo su ciclo de vida), el enfoque basado en riesgos, la disponibilidad del conocimiento como documentos de la organización, las mediciones de la eficacia y eficiencia del SGSI y el paradigma de mejora continua del sistema.

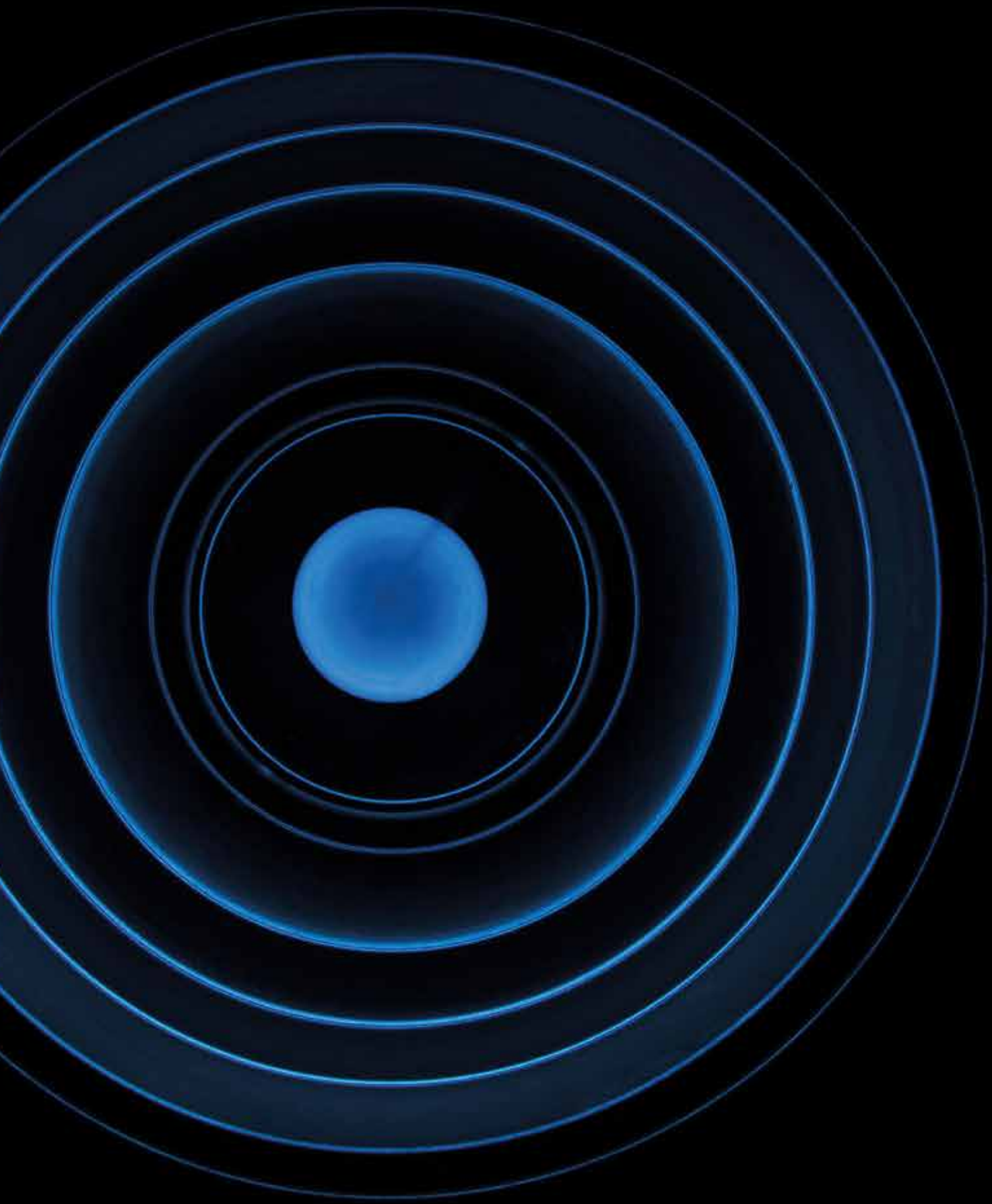
SOMOS UNA FAMILIA

El alcance del término "sistema de gestión de la seguridad de la información" no tiene cabida en estas dos normas, lo que ha llevado al desarrollo de normas complementarias,. específicas y temáticas, que aportan conocimiento y criterio en su objeto particular. A la fecha de redacción del presente artículo existen 69 normas en la "foto de familia" de ISO 27XXX (se esperan nuevos nacimientos en el corto plazo) destacando el número de normas dedicadas específicamente a la privacidad, aportando criterios sustanciales al cumplimiento normativo relacionado no solo con el RGPD sino con otras regulaciones internacionales en la materia.

La familia ISO/IEC 27XXX tiene conexiones estrechas con otras familias, y quiero destacar por su importancia sus primas hermanas ISO 223XX, dedicadas al concepto de "Continuidad de negocio".

Esta prolífica estructura familiar nos obliga a implementar el paradigma de las "tres A" (ADOPTAR, ADAPTAR, APLICAR) desde una visión holística presidida por una adecuada estructura de gobernanza de la seguridad de la información.

CONTINÚA EN PRÓXIMA PÁGINA



PASANDO LA ITV

Las normas "vehiculares" de la familia son ISO/IEC 27001 e ISO/IEC 27002 y, dado el enfoque basado en riesgos de la familia, también está en el "top" la norma ISO/IEC 27005 – Guía de gestión de riesgos de la seguridad de la información. Prescindo del sufijo ":2022" en adelante ya que siempre será la edición de 2022 la referenciada.

CAMBIOS EN ISO/IEC 27001

Cambia el nombre: Information security, cybersecurity and privacy protection — Information security management systems — Requirements.

Los otros cambios en ISO/IEC 27001 no son de gran entidad, centrados principalmente en la cláusula 6 (Planning), con un mayor énfasis en la identificación, análisis y tratamiento de riesgos, en la cláusula 8 (Operation) también con un mayor detalle en la evaluación y tratamiento de riesgos, así como en la gestión de cambios y la gestión documental. El Anexo A queda sincronizado con el nuevo conjunto de controles de ISO/IEC 27002.

CAMBIOS EN ISO/IEC 27002

Cambia el nombre: Information security, cybersecurity and privacy protection — Information security controls.

Esta es la norma que incluye el mayor número de novedades, ya que cada uno de sus 93 controles (reducción desde los 114 de la edición de 2013) ha sido actualizado en cuanto a su contenido y, adicionalmente, queda encuadrado en uno de los cuatro bloques temáticos (temas) de la norma y tiene asignados unos valores de una taxonomía definida para los denominados "atributos".

Los bloques temáticos son: **Personas** (controles relacionados con personas) – **Físicos** (controles relacionados con objetos o infraestructuras físicas) – **Tecnológicos** (controles relacionados con tecnología) – **Organizacionales** (controles no encuadrados en los tres temas anteriores).

Los atributos y sus valores son: **Tipo de control** (preventivo, detectivo, correctivo) – **Propiedades de seguridad de la información** (confidencialidad, integridad, disponibilidad) – **Conceptos de ciberseguridad** (identificar, proteger, detectar, responder, recuperar) – **Capacidades operativas** (equivalentes a los "objetivos de control" de las ediciones anteriores, p.e. seguridad de los recursos humanos, seguridad física, etc.) – **Dominios de seguridad** Visión de los controles desde cuatro dominios de seguridad (Gobernanza y ecosistema, Protección, Defensa y Resiliencia) teniendo cada uno de los cuatro subdominios que, por motivos de espacio, no se detallan aquí.

Estos atributos, así como los controles, no son obligatorios. Cada organización puede seleccionar éstos u otros controles y especificarlos en la Declaración de Aplicabilidad, así como adaptar la taxonomía de los atributos y sus valores según su criterio, documentando adecuadamente la taxonomía definitiva.

Esta nueva estructura proporciona, en mi opinión, una visión mucho más clara y flexible de los controles de la norma, permitiendo utilizar los valores de los atributos para agrupar controles y analizarlos desde diferentes perspectivas.

CAMBIOS EN ISO/IEC 27005

Cambia el nombre: Information security, cybersecurity and privacy protection — Guidance on managing information security risks.

En el caso de ISO/IEC 27005, los cambios incluyen un alineamiento de sus cláusulas con ISO/IEC 27001, alineamiento de la terminología con su "hermana mayor" (ISO 31000:2018) y, como cambios más relevantes, desarrolla el concepto de "escenario de riesgo" y se comparan de forma clara y muy útil el enfoque **basado en activos** y el **basado en eventos** en la fase de identificación de riesgos.

CONCLUSIONES

La familia ISO/IEC 27XXX crece y se renueva, si bien la renovación de los controles en ISO/IEC 27002 debería realizarse con mayor frecuencia para adaptarse a la evolución de las amenazas y sus riesgos asociados, así como desligarse del Anexo A de ISO/IEC 27001 para evitar renovaciones de ésta última cuyos cambios incidan únicamente en los que haya sufrido ISO/IEC 27002.

MGEIT® MPPM®

eGob®

FitSM + ISO 20000
Service Management
Gestión de Servicios de Tecnología

CERTIFICATE EN SERVICIOS

Estamos en un mundo cada vez más "As-a-Service" donde todo se comercializa como servicio con la ayuda de las nuevas tecnologías, pero las tecnologías que soportan los servicios deben ser adecuadamente gestionadas para dotarlas de capacidad, continuidad, disponibilidad, seguridad y resiliencia. Si quieres prepararte para la Era Digital fórmate en Servicios.

NIVELES DE CERTIFICACIÓN

Nivel de Certificación Board*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de la materia, su entorno y ámbito de aplicación, sus roles y responsabilidades que les permita participar en las inicativas.

Nivel de Certificación Executive*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de las Buenas Prácticas, Metodologías y Bases de Conocimiento aplicables con el fin de dirigir o participar en equipos de implementación.

Nivel de Certificación Leader*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de las normas y Estándares ISO aplicables con el fin de dirigir o participar en equipos de implementación.

Nivel de Certificación Skilled*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de la elaboracion de documentos, informes, planes, herramientas y/o artefactos que les permitan la aplicación práctica de los conocimientos.

*Niveles de Certificación pertenecientes a los Esquemas de la Entidad de Certificacion Business&Co.® y alineados con la Norma UNE-EN ISO/IEC 17024:2012 Evaluación de la Conformidad. Requisitos Generales para los Organismos que realizan Certificación de Personas. Más información: https://businessandcompany.com/certificacion-de-personas

MISION

Nuestra misión consiste en instituir una nueva clase directiva capaz de liderar con éxito las oportunidades que nos brinda la era digital.

FORMACIÓN BUSINESS CLASS

- Formación experiencial y participativa en remoto y en directo para una mayor comodidad del alumno.
- Cursos de cuatro sesiones en formato tardes de martes y jueves o formato viernes tardes y sábados mañanas.
- Máximo doce alumnos por convocatoria para una mayor interacción y compartición de experiencias y anécdotas.
- Cursos de Doble Certificación convalidables por asignaturas de los Masters MasterGEIT® y/o MasterPPM®.

CONVOCATORIAS 2022/23

- **SEPTIEMBRE 2022 (Formato Martes y Jueves Tardes)**
  Martes 6, jueves 8, martes 13 y jueves 15
- **ENERO 2022 (Formato Martes y Jueves Tardes)**
  Martes 17, jueves 19, martes 24 y jueves 26

eGob®

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

Continuidad de negocio. Errores y carencias habituales.

Dijo Murphy: "Si algo puede salir mal, saldrá mal".
Añado aquello de "Todo objeto inanimado, por definición, es hostil".

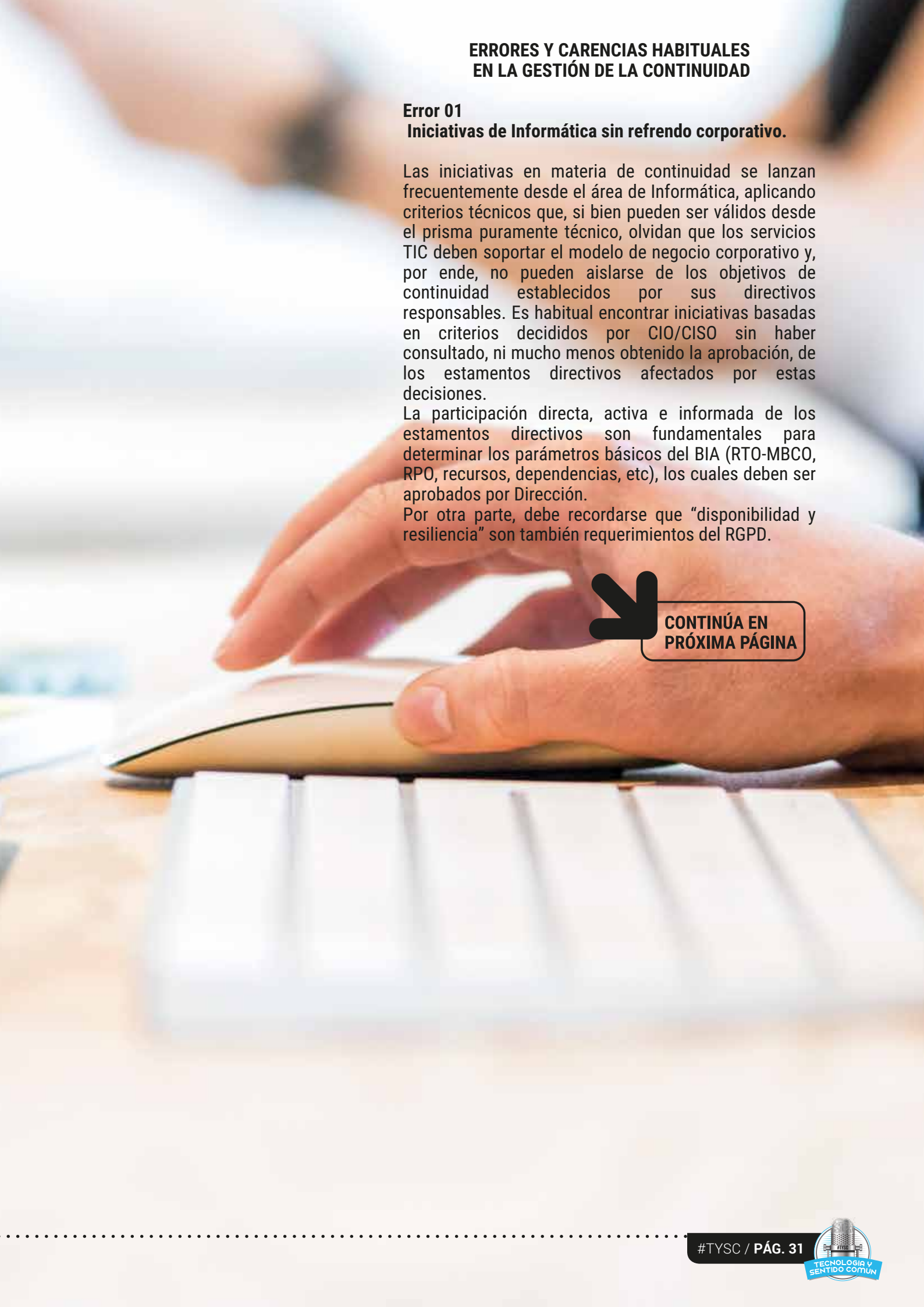
CONTEXTO

No era consciente de mi dependencia de los servicios TIC hasta que los perdí.

Los servicios TIC constituyen una base en cualquier organización para el desarrollo de sus actividades, y su pérdida puede comprometer seriamente el modelo de negocio corporativo. Las organizaciones deben adoptar, adaptar y aplicar medidas de Gestión de la Continuidad para tratar los eventos disruptivos sobre sus servicios TIC y, por ende, sobre sus actividades, siendo su enfoque como sistema de gestión el medio ideal para conseguir sus objetivos, dentro de un SGSI global.

Sistema de gestión de la continuidad de negocio (sgcn)–referenciales.

La construcción de un SGCN dispone de normas referenciales, en este caso la familia cuya matriz es la norma certificable ISO 22301:2019-Security and resilience – Business continuity management systems – Requirements, acompañada de un amplio conjunto de normas complementarias que desarrollan puntos de la norma matriz y, por tanto, facilitan su implementación, destacando entre ellas ISO/TS 22317:2021-Security and resilience – Business continuity management systems – Guidelines for business impact analysis, y también UNE-EN ISO 22313:2020 - Seguridad y resiliencia. Sistemas de gestión de la continuidad del negocio. Directrices para la utilización de la norma ISO 22301.



ERRORES Y CARENCIAS HABITUALES EN LA GESTIÓN DE LA CONTINUIDAD

Error 01
Iniciativas de Informática sin refrendo corporativo.

Las iniciativas en materia de continuidad se lanzan frecuentemente desde el área de Informática, aplicando criterios técnicos que, si bien pueden ser válidos desde el prisma puramente técnico, olvidan que los servicios TIC deben soportar el modelo de negocio corporativo y, por ende, no pueden aislarse de los objetivos de continuidad establecidos por sus directivos responsables. Es habitual encontrar iniciativas basadas en criterios decididos por CIO/CISO sin haber consultado, ni mucho menos obtenido la aprobación, de los estamentos directivos afectados por estas decisiones.
La participación directa, activa e informada de los estamentos directivos son fundamentales para determinar los parámetros básicos del BIA (RTO-MBCO, RPO, recursos, dependencias, etc), los cuales deben ser aprobados por Dirección.
Por otra parte, debe recordarse que “disponibilidad y resiliencia” son también requerimientos del RGPD.

CONTINÚA EN PRÓXIMA PÁGINA

Error 02
BIA, Planes de continuidad y procedimientos no documentados adecuadamente.

Es habitual encontrar BIA, planes de continuidad y procedimientos no documentados o con una documentación que, nuevamente, sólo contempla aspectos técnicos, dejando sin cubrir actuaciones sobre aspectos jurídicos, contractuales, reputacionales, comerciales, comunicaciones, recursos humanos y materiales internos y externos, infraestructuras y financieros, resultando en planes incompletos que sólo serían efectivos ante disrupciones técnicas sin trascendencia en los aspectos mencionados anteriormente.
En la elaboración del BIA, planes y procedimientos deben participar todas las áreas corporativas bajo un prisma de integración de roles y responsabilidades en las actuaciones a desarrollar y, en todos los casos, bajo una directriz formal de Dirección obligando a todos los actores a cumplir con lo requerido en cada escenario. La documentación debe mantenerse permanentemente actualizada, protegida y disponible.
Otra carencia habitual es la falta de una detallada, actualizada y documentada apreciación de riesgos, actividad nuclear para el proceso.

ERROR 03
Pruebas incompletas de los planes y procedimientos de continuidad.

Las pruebas de los planes y procedimientos de continuidad pueden ser complejas, costosas e incluso peligrosas si no se tienen en cuenta sus riesgos inherentes, pero lo que resulta inasumible es no realizar pruebas que permitan verificar que, en caso de ocurrencia de un evento disruptivo real, los planes y procedimientos aportan capacidades reales de recuperación alineadas con RTO-MBCO y RPO.
El diseño de las pruebas debe realizarse para cada uno de los planes de continuidad diseñados, contemplando todas las actividades contenidas en el mismo y especificando las métricas que permitan determinar su grado de cumplimiento respecto a los objetivos marcados. Las pruebas deben incluir los procedimientos a seguir con su versión vigente.
Por supuesto, debe realizarse una evaluación de riesgos de la propia prueba y tomar las medidas pertinentes para mitigarlos a niveles asumibles.
Cada prueba realizada debe registrar los valores obtenidos para sus métricas y obtener indicadores de cumplimiento respecto a los objetivos marcados. Las pruebas que no alcancen el cumplimiento de los objetivos deben ser analizadas inmediatamente para determinar las causas y adaptar los planes convenientemente, pudiendo ser necesario reconsiderar RTO-MBCO y/o RPO por parte de Dirección.
Uno de los errores más habituales en las pruebas de los planes de continuidad consiste en trabajar con "hipótesis única favorable", es decir, suponer que todos los recursos previstos van a estar disponibles. Esta hipótesis puede cumplirse en las pruebas, pero es necesario desarrollar supuestos menos favorables (y más realistas) donde recursos técnicos, humanos e infraestructuras no estén disponibles en porcentajes determinados.
Un medio de prueba cada vez más utilizado consiste en el desarrollo de ejercicios de simulación (tabletop excercises), donde pueden simularse numerosos escenarios y evaluar el desempeño, principalmente de los recursos humanos, en los planes y procedimientos de continuidad.

ERROR 04
Me voy a la nube pero no verifico lo que contrato.

Los proveedores de servicios en la nube, al menos los más relevantes, suelen disponer de certificación sobre ISO 22301:2019, pero esta certificación no garantiza en absoluto que cualquier servicio que se contrate con ellos quede automáticamente englobado dentro del contexto de "alta disponibilidad" que conlleva la certificación. De hecho, todos ellos ofrecen opciones (pagando) que aportan la mencionada "alta disponibilidad" a los servicios básicos que ofrecen como punto de partida. Por tanto, siendo altamente recomendable utilizar servicios en la nube con certificación ISO 22301:2019 (y certificación ENS si sois Administración Pública) deben estudiarse detalladamente las opciones a contratar para que los planes de continuidad queden efectivamente reflejados en ese contrato.

CONCLUSIONES

La "necesidad de continuidad" está muy clara, pero su materialización no tiene, en un alto porcentaje de organizaciones, un enfoque adecuado para conseguir unos objetivos que ni siquiera están definidos ni aprobados por Dirección en la mayoría de los casos, resultando en "sorpresas" perfectamente alineadas, eso sí, con las Leyes de Murphy.

MGEIT® MPPM®

eGob®

OpenPM² (PjM) + ISO 21502
Project Management
Gestión de Proyectos

CERTIFICATE EN PROYECTOS

La Gestión de Proyectos es la vía natural con la que implementar cambios en las organizaciones. Por encima de la ejecución de actividades una adecuada Gestión de Proyectos permite tener bajo control y garantizar aspectos tan importantes como plazos, costes, riesgos y beneficios ofreciendo información confiable a quien la necesita.

NIVELES DE CERTIFICACIÓN

Nivel de Certificación Board*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de la materia, su entorno y ámbito de aplicación, sus roles y responsabilidades que les permita participar en las inicativas.

Nivel de Certificación Executive*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de las Buenas Prácticas, Metodologías y Bases de Conocimiento aplicables con el fin de dirigir o participar en equipos de implementación.

Nivel de Certificación Leader*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de las normas y Estándares ISO aplicables con el fin de dirigir o participar en equipos de implementación.

Nivel de Certificación Skilled*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de la elaboracion de documentos, informes, planes, herramientas y/o artefactos que les permitan la aplicación práctica de los conocimientos.

*Niveles de Certificación pertenecientes a los Esquemas de la Entidad de Certificacion Business&Co.® y alineados con la Norma UNE-EN ISO/IEC 17024:2012 Evaluación de la Conformidad. Requisitos Generales para los Organismos que realizan Certificación de Personas. Más información: https://businessandcompany.com/certificacion-de-personas

MISION

Nuestra misión consiste en instituir una nueva clase directiva capaz de liderar con éxito las oportunidades que nos brinda la era digital.

FORMACIÓN BUSINESS CLASS

- Formación experiencial y participativa en remoto y en directo para una mayor comodidad del alumno.
- Cursos de cuatro sesiones en formato tardes de martes y jueves o formato viernes tardes y sábados mañanas.
- Máximo doce alumnos por convocatoria para una mayor interacción y compartición de experiencias y anécdotas.
- Cursos de Doble Certificación convalidables por asignaturas de los Masters MasterGEIT® y/o MasterPPM®.

CONVOCATORIAS 2022/23

- **SEPTIEMBRE 2022 (Formato Viernes Tardes y Sábados Mañanas)**
  Viernes 16, sabado 17, viernes 23 y sábado 24
- **OCTUBRE 2022 (Formato Martes y Jueves Tardes)**
  Martes 18, jueves 20, martes 25 y jueves 27
- **NOVIEMBRE 2022 (Formato Viernes Tardes y Sábados Mañanas)**
  Viernes 18, sabado 19, viernes 25 y sábado 26

eGob®

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

Seguridad específica para la privacidad. Norma ISO/IEC 27701:2019.

Las normas de seguridad son generalistas, pero algunos sectores y temáticas disponen de normas específicas diseñadas para contemplar su ecosistema concreto. Este es el caso de la norma ISO/IEC 27701:2019, contemplando el amplio universo y casuística asociada a "la privacidad". En adelante, omitiré los sufijos "2013" para ISO/IEC 27001-27002 y "2019" para ISO/IEC 27701.

ACLARACIONES SOBRE LA RELACIÓN ENTRE ISO/IEC 27001 e ISO/IEC 27701

Certificabilidad

He detectado en numerosas ocasiones cierta confusión al relacionar estas normas, dado que, siguiendo la regla de "certificabilidad" de ISO/IEC, las acabadas en "01" son certificables, pero ISO/IEC 27701 se presenta como "complementaria" de ISO/IEC 27001 desde su propio título: "*Técnicas de seguridad. Extensión de las normas ISO/IEC 27001 e ISO/IEC 27002 para la gestión de privacidad de la información. Requisitos y directrices. (ISO/IEC 27701:2019)*".

Ambas normas **son certificables**, pero con una condición. Para obtener la certificación sobre ISO/IEC 27701 una entidad debe poseer una certificación vigente sobre ISO/IEC 27001 o abordar ambas certificaciones simultáneamente. Por tanto, no es posible obtener una certificación aislada para ISO/IEC 27701. A la fecha de redacción del presente artículo, enero de 2023, no está disponible una versión de ISO/IEC 27701 alineada con las ediciones de 2022 de ISO/IEC 27001 e ISO/IEC 27002, siendo aplicables las versiones de 2013 ante la existencia de un periodo transitorio establecido entre las normas de 2013 y las de 2022.

Ámbito objetivo

Tal como indica su propio título, la norma ISO/IEC 27701 contiene los requisitos para construir y evolucionar un "Sistema de Gestión de la Privacidad de la Información", si bien suele utilizarse el acrónimo en inglés PIMS – Privacy Information Management System), cuya definición, contenida en el punto 3.2 de la norma es: *Sistema de gestión de seguridad de la información que enfoca la protección de la privacidad como potencialmente afectada por el tratamiento de datos personales*".

CUESTIONES TERMINOLÓGICAS IMPORTANTES

La norma ISO/IEC 27701 menciona el acrónimo PII - del inglés *Personally Identifiable Information* - y plenamente compatible con la definición de "datos personales" contenida en el artículo 4 del Reglamento (UE) 2016/679 (RGPD en adelante): «*datos personales»: toda información sobre una persona física identificada o identificable*.

A su vez, en la Unión Europea, el Supervisor Europeo de Protección de Datos introduce el acrónimo PIMS como "*Personal Information Management System*" – "*Sistema de Gestión de la Información Personal*", pero, en cualquier caso, el alineamiento persiste con el ámbito objetivo de la norma ISO/IEC 27701.

Es conveniente aclarar estas cuestiones terminológicas dado que, aunque estamos tratando sobre los mismos conceptos, no podemos olvidar que la norma no está orientada únicamente al cumplimiento del RGPD sino a todas las normativas sobre protección de la privacidad que puedan existir globalmente.

CONTINÚA EN PRÓXIMA PÁGINA

DIMENSIONES DE SEGURIDAD

Dentro del ámbito de la "seguridad de la información" encontramos tres dimensiones principales: **confidencialidad, integridad y disponibilidad**.

Tradicionalmente (incorrectamente, en mi opinión) , la privacidad estaba vinculada con la confidencialidad, pero el RGPD deja muy claras sus dimensiones en el artículo 32 – *Seguridad del tratamiento*- donde requiere "*la capacidad de garantizar la* ***confidencialidad, integridad, disponibilidad y resiliencia*** *permanentes de los sistemas y servicios de tratamiento*".

Queda explícito el alineamiento entre RGPD y SGSI-SGPI, máxime cuando la propia UE define la privacidad como "*empoderar a las personas físicas pata tomar sus propias decisiones sobre quién puede tratar sus datos y con qué finalidades*".

APORTACIONES DE LA NORMA ISO/IEC 27701

¿Qué aporta la norma ISO/IEC 27701 a la norma ISO/IEC 27001?

Las aportaciones de la norma ISO/IEC 27701 son, en mi opinión, muy significativas dentro del modelo adoptar-adaptar-aplicar.
La adopción de medidas de seguridad para la protección de datos personales es una obligación legal, por lo que "adoptar" no tiene discusión.
El valor añadido viene por la adaptación+complementación de unas medidas de seguridad generalistas a la casuística concreta de la protección de datos personales, incluyendo cuestiones tan importantes como un mapeo específico para el cumplimiento del RGPD (Anexo D de la norma), un capítulo específico para responsables de tratamiento (cap 7) y otro para encargados de tratamiento (cap 8). Asimismo, contiene extensiones concretas para ISO/IEC 27001 (cláusulas 4 y 6) e ISO/IEC 27002 (todas las cláusulas salvo la 17), con unas ampliaciones relevantes en sus guías de implementación.

¿Qué aporta la norma ISO/IEC 27701 al cumplimiento del RGPD?

Esta norma contiene previsiones para la realización de Evaluaciones de Impacto sobre Protección de Datos (EIPD), plenamente alienadas con lo requerido en el RGPD, así como previsiones sobre acuerdos de corresponsable de tratamiento, contratos de encargado de tratamiento, ejercicio de derechos, privacidad por diseño y por defecto y un etc obligado por las limitaciones de espacio en el artículo.

En relación con el RGPD, la norma ISO/IEC 27701 aporta a las organizaciones un marco de referencia relevante para el cumplimiento de las obligaciones legales emanadas de la legislación en materia de protección de datos personales, con alto valor añadido para aquellas afectadas por el RGPD y/o normativas similares vigentes en otros entornos geográficos.

¿Qué aporta la norma ISO/IEC 27701 a las organizaciones?

Esta norma, al ser certificable, aporta a las organizaciones certificadas la acreditación de un Sistema de Gestión de la **Seguridad y la Privacidad**, pilar importante para sustentar evidencias de cumplimiento de los marcos normativos sobre protección de datos personales y, por ende, con alto valor en el mercado. Como ejemplo, compañías como Microsoft o Google han obtenido este certificado para sus plataformas representativas.

CONCLUSIONES

Las cuestiones sobre seguridad relacionadas con la privacidad son fundamentales al ser también fundamental el derecho a la privacidad de las personas físicas, cuya protección es un requerimiento de todos los marcos normativos sobre la materia y cuyo incumplimiento conlleva sanciones altamente impactantes, no solo a nivel económico sino también reputacional. En este contexto, la disponibilidad de una norma específica sobre seguridad orientada a la privacidad y, en el caso de la UE, mapeando medidas con el RGPD, aporta un alto valor en sí misma, y su certificabilidad añade una vía de acreditación interna y externa para una organización.

MGEIT® MPPM®

eGob®

OpenPM² (PgM) + ISO 21503
Programme Management
Gestión de Programas

CERTIFICATE EN PROGRAMAS

La Gestión de Programas de Proyectos es responsable de que los resultados de los proyectos se conviertan en beneficios, mientras que los Proyectos finalizan con la entrega de sus resultados, los Programas quedan aportando valor al negocio más allá de la vida de cada proyecto. Si quieres de verdad lograr beneficios certificate en Gestión de Programas.

NIVELES DE CERTIFICACIÓN

Nivel de Certificación Board*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de la materia, su entorno y ámbito de aplicación, sus roles y responsabilidades que les permita participar en las inicativas.

Nivel de Certificación Executive*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de las Buenas Prácticas, Metodologías y Bases de Conocimiento aplicables con el fin de dirigir o participar en equipos de implementación.

Nivel de Certificación Leader*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de las normas y Estándares ISO aplicables con el fin de dirigir o participar en equipos de implementación.

Nivel de Certificación Skilled*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de la elaboracion de documentos, informes, planes, herramientas y/o artefactos que les permitan la aplicación práctica de los conocimientos.

*Niveles de Certificación pertenecientes a los Esquemas de la Entidad de Certificacion Business&Co.® y alineados con la Norma UNE-EN ISO/IEC 17024:2012 Evaluación de la Conformidad. Requisitos Generales para los Organismos que realizan Certificación de Personas. Más información: https://businessandcompany.com/certificacion-de-personas

MISION

Nuestra misión consiste en instituir una nueva clase directiva capaz de liderar con éxito las oportunidades que nos brinda la era digital.

FORMACIÓN BUSINESS CLASS

- Formación experiencial y participativa en remoto y en directo para una mayor comodidad del alumno.
- Cursos de cuatro sesiones de 5 horas en formato tardes de martes y jueves o formato viernes tardes y sábados mañanas.
- Máximo doce alumnos por convocatoria para una mayor interacción y compartición de experiencias y anécdotas.
- Cursos de Doble Certificación convalidables por asignaturas de los Masters MasterGEIT® y/o MasterPPM®.

CONVOCATORIAS 2022/23

- **NOVIEMBRE 2022 (Formato Martes y Jueves Tardes)**
  Martes 15, jueves 17, martes 22 y jueves 24
- **ENERO 2023 (Formato Viernes Tardes y Sábados Mañanas)**
  Viernes 20, sabado 21, viernes 27 y sábado 28

eGob

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

ISO 27001-27002:2022 vs ENS 2022. Mismo fondo, diferentes formas.

Las normas ISO/IEC 27001:2022 e ISO/IEC 27002:2022 (ISO 27001 o ISO 27002 en adelante) y el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS en adelante) tienen objetivos comunes, pero su implementación y certificación difieren en aspectos sustanciales.

FONDO COMÚN

Sistema de Gestión de la Seguridad de la Información (SGSI) certificable.

Tanto ISO 27001 como ENS construyen, mantienen y evolucionan un SGSI, por lo que sus objetivos y resultados son comunes. Su enfoque orientado al análisis y gestión de los riesgos TI es común para ambas y sus esquemas de certificación, con sus particularidades, mantienen también unas actividades muy similares.

Medidas de seguridad

En cuanto a las medidas de seguridad, en el caso del ENS especificadas en su Anexo II y en el caso de ISO 27001 recogidas en la norma ISO 27002, comparten criterios y guías de implementación dado que tratan los mismos campos de aplicación.

DIVERGENCIAS

Obligatoriedad.

La norma ISO 27001 no tiene carácter obligatorio para el cumplimiento normativo. Su implementación y certificación viene determinado por la conciencia en materia de seguridad TI de una organización – En España, en numerosas ocasiones, conciencia "sobrevenida" tras un evento TI disruptivo – o bien por requerimientos de interlocutores de negocio que exigen seguridad TI en su cadena de suministros.

En cambio, el cumplimiento del ENS y su acreditación es obligatorio para todo el sector público y para el sector privado que preste servicios y/o venda productos al sector público donde puedan estar implicadas cuestiones relacionadas con la seguridad y también cuando existan tratamientos de datos personales.

Esta última cuestión amplía el escenario de aplicabilidad del ENS, dado que, en la Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD en adelante) se menciona el ENS en su Disposición adicional primera, al señalar el ENS como marco de referencia para las medidas de seguridad que deben implementarse cuando existen tratamientos de datos personales en el sector público y en el sector privado suministrador de productos y servicios implicados en dichos tratamientos.

CONTINÚA EN PRÓXIMA PÁGINA

Por si faltaba algún refrendo, el *artículo 3 del ENS - Sistemas de información que traten datos personales* - incide nuevamente en esta vinculación con RGPD – LOPDGDD.

La obligatoriedad queda plasmada explícitamente en el articulo 2.3 del ENS, cuando exige:

"*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*"

Por otra parte, las medidas de seguridad aplicables del ENS son obligatorias, si bien se admiten exclusiones y medidas compensatorias debidamente justificadas, mientras que las medidas contenidas en la norma ISO 27002 son opcionales y así lo refleja su forma verbal condicional "should" (debería) en su texto. Es decir, las medidas incluidas en la norma ISO 27002 constituyen una ayuda muy útil para el SGSI, pero pueden ser tenidas en cuenta o no en su construcción, mantenimiento y evolución.

Niveles y categorías

Una de las diferencias notorias entre ENS e ISO 27001 es la existencia en el ENS de niveles (ALTO, MEDIO, BAJO) por dimensión de seguridad (confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad), basados en un análisis de impacto sobre los servicios e informaciones corporativos causados por posibles eventos, y la categorización (BÁSICA, MEDIA; ALTA) de sistemas de información en el ENS, todo ello asociado a las medidas concretas a implementar, dependientes de la categoría del sistema, de los niveles por dimensión y del resultado de la apreciación de riesgos desarrollada.

Estos conceptos (nivel, categoría) no existen en ISO 27002, donde el catálogo de medidas es único (sin niveles) y la implementación de sus medidas depende fundamentalmente de los resultados de la apreciación de riesgos desarrollada.

Convalidaciones

Una pregunta recurrente, sobre todo en el sector privado, donde las certificaciones sobre ISO 27001 son más habituales, se centra en la convalidación entre las certificaciones actuales sobre ISO 27001 y las que se requieren sobre el ENS.
La respuesta del CCN ha sido un rotundo NO, y tiene sus razones, algunas de las cuales pueden derivarse de los puntos anteriores. Existe una guía - *CCN-STIC 825 - Esquema Nacional de Seguridad - Certificaciones 27001* – que expone una vía de transición entre ambas certificaciones, pero podemos considerarla obsoleta dado que data del año 2013 y tanto ENS como ISO 27001 e ISO 27002 disponen de versiones actualizadas en el año 2022, todas ellas con diferencias respecto a su versión anterior.

En este sentido, sigo viendo todavía algunos pliegos de la Administración Pública que siguen exigiendo certificación sobre ISO 27001, algunas veces adicionalmente a la del ENS y otras sin mencionar al ENS. Estos pliegos podrían ser impugnables por las entidades licitantes, dado que la certificación obligatoria es la del ENS, a menos que algún requerimiento externo (p.e. proveniente de otro país, UE, etc.) lo exija, y siempre adicionalmente a la del ENS.

¿Por qué se creó el ENS teniendo ya unas normas de seguridad TI maduras y universalmente aceptadas como "buenas prácticas", la familia ISO 27001, adoptadas como norma nacional por otros países (p.e. Perú, Chile) evitando mantener dos certificaciones para un SGSI? Una de las razones esgrimidas se centra en el criterio de disponer de marcos normativos no dependientes de organizaciones externas como ISO/IEC.

Conclusiones

Es necesaria una vía de transición entre ISO 27001 y ENS para minimizar el esfuerzo necesario en conseguir ambas certificaciones. Las entidades del sector privado no suelen reconocerse entre sí las certificaciones sobre el ENS y siguen manteniendo como referencial ISO 27001, situación que, actualmente, conlleva en el sector privado esta necesidad de doble certificación y redundancia para la misma organización.

MGEIT® MPPM®

eGob®

COSO + ISO 37000
Corporate Governance
Buen Gobierno Corporativo

CERTIFICATE EN
BUEN GOBIERNO

El Buen Gobierno significa que la toma de decisiones dentro de la organización se basa en el espíritu, la cultura, las normas, las prácticas, los comportamientos, las estructuras y los procesos de la organización. El Buen Gobierno crea y mantiene una organización con un propósito claro que ofrece valor a largo plazo.

NIVELES DE CERTIFICACIÓN

Nivel de Certificación Board*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de la materia, su entorno y ámbito de aplicación, sus roles y responsabilidades que les permita participar en las inicativas.

Nivel de Certificación Executive*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de las Buenas Prácticas, Metodologías y Bases de Conocimiento aplicables con el fin de dirigir o participar en equipos de implementación.

Nivel de Certificación Leader*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de las normas y Estándares ISO aplicables con el fin de dirigir o participar en equipos de implementación.

Nivel de Certificación Skilled*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de la elaboracion de documentos, informes, planes, herramientas y/o artefactos que les permitan la aplicación práctica de los conocimientos.

*Niveles de Certificación pertenecientes a los Esquemas de la Entidad de Certificacion Business&Co.® y alineados con la Norma UNE-EN ISO/IEC 17024:2012 Evaluación de la Conformidad. Requisitos Generales para los Organismos que realizan Certificación de Personas. Más información: https://businessandcompany.com/certificacion-de-personas

MISION

Nuestra misión consiste en instituir una nueva clase directiva capaz de liderar con éxito las oportunidades que nos brinda la era digital.

FORMACIÓN BUSINESS CLASS

- Formación experiencial y participativa en remoto y en directo para una mayor comodidad del alumno.
- Cursos de cuatro sesiones de 5 horas en formato tardes de martes y jueves o formato viernes tardes y sábados mañanas.
- Máximo doce alumnos por convocatoria para una mayor interacción y compartición de experiencias y anécdotas.
- Cursos de Doble Certificación convalidables por asignaturas de los Masters MasterGEIT® y/o MasterPPM®.

CONVOCATORIAS 2022/23

- **JUNIO 2023 (Formato Martes y Jueves Tardes)**
  Martes 20, jueves 12, martes 27 y jueves 29
- **JULIO 2023 (Formato Viernes Tardes y Sábados Mañanas)**
  Viernes 21, sabado 22, viernes 28 y sábado 29

eGob®

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

Fuentes de conocimiento y criterio

Los marcos normativos, normas y estándares contienen requerimientos y guías de implementación para los Sistemas de Gestión de Seguridad de la Información (SGSI), pero no llegan a un alto nivel de detalle. En este artículo exponemos fuentes de conocimiento y criterio relevantes para materializar el SGSI.

DI LO QUE HACES + HAZ LO QUE DICES + DEMUÉSTRALO

Simplificando el proceso de implementación del SGSI, podemos establecer una fase documental (políticas, normativas, procedimientos, instrucciones técnicas) que constituyen el concepto **"di lo que haces"**, una fase de implementación de las medidas multidisciplinares que aporta el concepto **"haz lo que dices"** (obviamente alineada con "di lo que haces") y una fase de obtención de evidencias (registros, métricas, indicadores) que aporta el concepto **"demuestra que haces lo que dices"**. Podemos añadir una cuarta fase, asociada al requerimiento de mejora continua que toda norma certificable contiene, denominada **"mejora todo lo anterior y dime cómo lo vas a hacer"**.

¿HASTA DÓNDE LLEGAN LAS NORMAS?

Prisma documental
Desde el prisma documental no se plantea un problema significativo dado que todas las normas y marcos normativos disponen de un catálogo de documentos nucleares obligatorios y descripción de su contenido mínimo, así como directrices para su aprobación, mantenimiento y divulgación.

Prisma organizativo
Desde el prisma organizativo también se dispone de requerimientos y criterios para definir una estructura organizativa alrededor del SGSI, siendo especialmente relevante en este sentido el Esquema Nacional de Seguridad (Real Decreto 311/2022 de 3 de mayo), marco normativo que especifica una estructura concreta con sus funciones y competencias (órgano competente, responsable de servicio, responsable de la información, responsable de seguridad y responsable de sistema) y posibles comités.

La norma ISO/IEC 27001:2022 no contiene especificaciones con este nivel de detalle, asignando a la "alta dirección" (top management) la tarea de asignar roles, responsabilidades y competencias relevantes para la seguridad de la información, dejando altos grados de libertad para definir la estructura organizativa.

Prisma técnico

El problema relacionado con posibles carencias de fuentes de información y criterio sobre **"cómo hacerlo"** se suscita, principalmente, en la implementación de las medidas técnicas.

INFORMACIÓN Y CRITERIO SOBRE "CÓMO HACERLO"

Documentación y soporte de fabricantes

Todos los fabricantes de componentes securizables disponen de documentación respecto de la securización de los mismos, y es una fuente prioritaria dado que asumen una alta responsabilización ("accountability") y potencial indemnización ("liability") ante incidentes achacables a problemas de seguridad, pero también por carencia de información sobre su securización que pudiera inhibir la activación de las medidas disponibles.

En este sentido, es muy recomendable (obligatorio en el ENS para categoría MEDIA y ALTA) la contratación de los denominados en el ENS "componentes certificados", concepto que engloba los componentes 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* y también los productos certificados bajo *Common Criteria*, ya que, dentro del proceso de certificación, se evalúa también la disponibilidad y calidad de la documentación aportada con el componente.

CONTINÚA EN PRÓXIMA PÁGINA

Guías CCN STIC
El Centro Criptológico Nacional ha desarrollado (y sigue desarrollando) un amplísimo conjunto de guías de seguridad y "buenas prácticas" que abarcan todo el ciclo de vida de construcción del SGSI, así como unas magníficas guías de bastionado y securización de componentes hardware y software habitualmente utilizados. Estas guías son particularmente útiles por su calidad, ejemplos y escenarios, incluyendo algunas de ellas scripts que materializan acciones concretas, si bien estos scripts deben siempre probarse en un entorno de pruebas y, en su caso, adaptarlos a cada arquitectura particular. Pueden accederse en: https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic.html

Adicionalmente, el CCN dispone de muy diversas plataformas de automatización de la seguridad de la información, su gestión, monitorización y auditoría.

NIST-National Institute of Standards and Technology
Esta entidad mantiene y evoluciona una ingente cantidad de documentación, estructurada en bloques: **FIPS** - *Federal Information Processing Standards: Security standards*, **SP** - *NIST Special Publications, dividida a su vez en: SP 800 - Computer security*, **SP 1800** - *Cybersecurity practice guides* y **SP 500** - Information technology (relevant documents), **NISTIR**- *NIST Internal or Interagency Reports y* **CWSP** - *NIST Cybersecurity White Papers*.

A la fecha, NIST dispone de un catálogo de 783 publicaciones, ofreciendo un gran caudal de información y criterios de implementación en materia de seguridad de la información, e incluyendo también documentos sobre securización de las plataformas habitualmente utilizadas. Puede accederse a través de: https://csrc.nist.gov/publications

INCIBE
El Instituto Nacional de Ciberseguridad de España (INCIBE) dispone de numerosa documentación en materia de ciberseguridad, si bien su enfoque y grado de detalle difiere de las fuentes anteriores. Disponibles en https://www.incibe.es/

ENISA
ENISA (Agencia de la Unión Europea para la Ciberseguridad) dispone a la fecha de un catálogo de 398 publicaciones, con un contenido diverso en la materia, aportando conocimiento y criterio unificado para el conjunto de la Unión Europea y, con ello, homogeneizando taxonomías y criterios. Estas publicaciones, en cualquier caso, no contienen detalles técnicos que permitan desarrollar instrucciones técnicas. Accesibles en: https://www.enisa.europa.eu/about-enisa/about/es

OWASP
The Open Worldwide Application Security Project® (OWASP) aporta directrices de alto valor añadido para la securización del desarrollo de software, muy especialmente aplicaciones web. Su "top ten" recoge las mayores amenazas para estos desarrollos y propone soluciones para mitigar sus riesgos asociados. Accesibles en; https://owasp.org/www-project-top-ten/

CLOUD SECURITY ALLIANCE
Organización dedicada a la securización de los servicios cloud. Dispone de un amplio catálogo de publicaciones sobre este particular, accesibles en:

https://cloudsecurityalliance.org/research/guidance/

CONCLUSIONES
Las fuentes enumeradas en este artículo son aquellas que considero más relevantes, pero esta enumeración no es exhaustiva ni completa por motivos de espacio.
El volumen de información sobre "cómo hacer" en materia de seguridad / ciberseguridad es ingente y, por supuesto, existen numerosas entradas sobre un mismo tema, por lo que cada entidad que aborde la implementación de un SGSI debería evaluar y seleccionar la/s fuente/s que mejor se adapten a su proceso particular y a la norma concreta que desea certificar.

Stakeholders.news

Cada tercer domingo de mes disfruta de la Revista Stakeholders.news
Revista Mensual de los Profesionales en Dirección y Gestión de Porfolios, Programas y Proyectos, Cambio Organizacional y Transformación Digital.

Integración entre el ENS y RGPD-LOPDGDD.

El RGPD y la LOPDGDD requieren una serie de actividades similares a las que se deben realizar en la implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI en adelante) pero, en la práctica, no es habitual su integración.

ESCENARIO NORMATIVO

Los requerimientos en materia de seguridad de la información están especificados en el RGPD, principalmente, en su ***Artículo 32 – Seguridad del tratamiento:***

Teniendo en cuenta el **estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento**, así como riesgos de probabilidad y gravedad variables para los **derechos y libertades** de las personas físicas, el responsable y el encargado del tratamiento aplicarán **medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo**, que en su caso incluya, entre otros: …..

Este texto del RGPD podría ser perfectamente asimilable a una declaración de objetivos de un SGSI cuyo alcance estuviera delimitado por los tratamientos de datos personales de una organización. Ahora bien, el RGPD y la LOPDGDD no contienen internamente un conjunto de medidas concretas aplicables, aspecto que sí contempla el Esquema Nacional de Seguridad (ENS) en su anexo II, compartiendo RGPD-LOPDGDD y ENS las dimensiones básicas de seguridad (confidencialidad, integridad, disponibilidad-resiliencia).

Para este artículo voy a centrarme en el ENS dado que la LOPDGDD (Disposición adicional primera) sí menciona este marco normativo de forma explícita como referente en cuanto a las medidas de seguridad a aplicar, tanto en el sector público (AAPP en adelante) como en las entidades del sector privado que proveen productos y servicios al sector público en los que existen tratamientos de datos personales.

A su vez el ENS, en su *Artículo 3 - Sistemas de información que traten datos personales* hace una mención explícita al necesario cumplimiento de lo dispuesto en el RGPD y LOPDGDD, realizando los pertinentes análisis de riesgos y, en su caso, las evaluaciones de impacto sobre protección de datos, **determinando la prioridad de las medidas resultantes de estas actividades sobre las que hubieran sido determinadas en las valoraciones propias del ENS**.

CONTINÚA EN PRÓXIMA PÁGINA


1ST EUGENE
2ND ELOFF
3RD MATTHEW
4TH DAVID
5TH JOSH
6TH PATRICK
7TH STEPHEN
8TH CATALAN
9TH KEVIN

ESCENARIO OPERATIVO EN LAS AAPP

El escenario real de los servicios e informaciones ofrecidos por las AAPP, muy especialmente las entidades locales (EELL en adelante) refleja la mayor concentración de tratamientos de datos personales que puede encontrarse en una organización, incluyendo datos clasificables como de máxima sensibilidad en áreas como Servicios Sociales o Policía Local.
En todos los casos dichos tratamientos están basados en el uso de "medios electrónicos" que menciona el ENS en su Artículo 1 - Objeto y, por ende, la intersección entre los ámbitos subjetivos y objetivos de RGPD-LOPDGDD y ENS queda claramente definida y debería resultar en una integración plena. Debería …….

LA REALIDAD

La realidad es muy diferente a la necesidad de integración derivada de los puntos anteriores, ya que lo habitual es encontrar proyectos de cumplimiento del ENS no solo separados de los de cumplimiento de RGPD–LOPDGDD (asumible aunque no deseable) sino también desintegrados (este es el verdadero y habitual problema). Ejemplos:

•Registro de Actividades de Tratamiento (RGPD) no sincronizado con el catálogo de servicios e informaciones del ENS que tratan datos personales, cuando ambos documentos podrían estar integrados incluyendo la información requerida por cada uno de estos marcos. En consecuencia, encontramos denominaciones, descripciones y valoraciones diferentes para las mismas informaciones en el mismo organismo, así como inconsistencias, incoherencias y redundancias, derivando en una especie de "fabada de datos" de difícil digestión y asimilación.

•Análisis de riesgos no sincronizados. En el caso de RGPD – LOPDGDD la AEPD ha publicado guías muy útiles para su análisis de riesgos y, en su caso, evaluaciones de impacto, como: https://www.aepd.es/es/documento/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf, así como herramientas específicas para su automatización, pero no ha tenido en cuenta la existencia del ENS como referencia para las medidas de seguridad aplicables y que derivarán, tras su aplicación, en el riesgo residual para los tratamientos. Por su parte, el cumplimiento del ENS requiere un análisis de riesgos (medida op.pl.1) que debería integrar los riesgos derivados de los tratamientos de datos personales. En este punto quiero destacar que diversas plataformas disponibles en el mercado sí ofrecen esta integración, entre ellas PILAR, gratuita para las AAPP, obteniendo con ello un proceso integral de análisis y gestión riesgos de índole jurídica, organizativa y técnica, plenamente utilizable para acreditar el cumplimiento integrado de RGPD-LOPDGDD y ENS.

•Brechas de seguridad que afectan a datos personales. Encontramos numerosos casos de falta de coordinación entre los roles Responsable de Seguridad (RSEG, ENS) y Delegado de Protección de Datos (DPD, RGPD). Es necesario reforzar la formación de quienes ejercen como DPD para que tengan en cuenta que las brechas de seguridad pueden tener su causa raíz en incidentes de seguridad que deben ser comunicados también al CCN y no solo a la AEPD, coordinándose adecuadamente con quien ejerce como RSEG. A la inversa, quienes ejercen como RSEG deben ser formados para coordinarse con el rol DPD y evaluar conjuntamente las brechas para determinar las acciones a tomar y las comunicaciones (AEPD, CCN, ambos) a realizar.

•Guías sectoriales del CCN (p.e. Entidades Locales) con valoraciones muy discutibles sobre datos personales de máxima sensibilidad tratados en determinados servicios municipales, al aplicar criterios del Anexo I del ENS difícilmente defendibles ante una evaluación de impacto sobre protección de datos, cuyos resultados, en base al Artículo 3 del ENS, son los que realmente valdrán para determinar las medidas a aplicar.

CONCLUSIONES

Es necesaria una iniciativa de **integración entre los proyectos de cumplimiento de RGPD-LOPDGDD y ENS**, una guía conjunta AEPD-CCN facilitadora de actuaciones tendentes a la optimización del cumplimiento de todos estos marcos de forma integral e integrada, dado que ofrece poca discusión esta necesidad en contraste con la realidad actual. Un buen indicador de la consecución de este objetivo podría ser la disminución del número de veces que escuchamos aquello de "**¿ENS? Eso es un tema de Informática"** incluso por parte de empresas consultoras de cierto renombre.

12 MESES GRATIS

NUEVO PROGRAMA DE DIGITALIZACIÓN DISPONIBLE

Programa ITSM

Implementa uno de los ITSM más completos de todo el mercado europeo a un coste 0€ (paquete básico)

¿Por qué elegir ITSM de Efecte?

1. Contamos con más de 20 años de experiencia.
2. Plataforma low-code, fácil de usar y muy gráfica.
3. Efecte es el único proveedor que ofrece 12 meses de uso GRATIS.
4. Ofrecemos ayuda experta gratuita y a medida, antes, durante y después de la implementación.

El proceso de selección de empresas ya está abierto y las plazas son limitadas. ¡DATE PRISA!

MÁS INFORMACIÓN

efecte

www.efecte.es

Certificación ENS de productos, servicios y aplicaciones.

La certificación de productos y servicios bajo el Esquema Nacional de Seguridad (Real Decreto 311/2022, ENS en adelante) genera, en el caso de las aplicaciones informáticas, unas casuísticas particulares y, en algunos casos, problemáticas.

SEGURIDAD ACREDITABL

La medición de la seguridad de la información y los servicios es fundamental para que cualquier organización, pública o privada, obtenga una "expectativa de seguridad" para sus sistemas de información. Ahora bien, esa medición debe seguir unos criterios que permitan establecer comparaciones y adoptar decisiones basadas en parámetros y valores significativos para el escenario donde se van a implementar.

En este sentido, la disponibilidad de marcos de certificación, nacionales y globales, aporta un alto valor añadido para los procesos de selección, máxime cuando en el ENS de 2022 el requerimiento de adquisición de "componentes certificados" ha sido extendido a los sistemas de categoría MEDIA cuando, en el ENS de 2010, era un requerimiento para sistemas de categoría ALTA.

CATÁLOGO DE COMPONENTES CERTIFICADOS

EL marco de referencia para la consulta de los componentes certificados es *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). Este catálogo incluye dos niveles de certificación:

1.Productos cualificados. Productos y servicios que cumplen los requisitos de seguridad exigidos para el manejo de información sensible en el ENS, en cualquiera de sus categorías (ALTA, MEDIA y BÁSICA).

2.Productos aprobados. Productos que se consideran adecuados para el manejo de información clasificada.

FIEBRE CERTIFICADORA

Este requerimiento del ENS deriva en una auténtica avalancha de procesos de certificación dado que, en la práctica, estar o no estar en el catálogo de componentes certificados puede suponer la inclusión o exclusión de los procesos de licitación pública teniendo en cuenta que un porcentaje mayoritario de sistemas de información en el sector público adquieren la categoría MEDIA.

¿LOS PRODUCTOS CERTIFICADOS EN EL CPSTIC SON "MEJORES" QUE LOS NO CERTIFICADOS?

La obtención de la certificación y la inclusión de productos y servicios en el CPSTIC no implica en absoluto superioridad tecnológica ni de otro tipo sobre los que no están en el CPSTIC, tampoco certifica la calidad del fabricante ni del proveedor del servicio, sólo se centra en las prestaciones en materia de seguridad del producto o servicio en sí mismo.

De hecho, es posible justificar el empleo de productos no incluidos en el CPSTIC siempre y cuando se acredite su necesidad y unas prestaciones de seguridad suficientes. Esta es una situación habitual en arquitecturas de seguridad donde se aplicaron los criterios del ENS de 2010, cuando no era obligatorio en categoría MEDIA implementar productos incluidos en el CPSTIC, y cuya sustitución puede suponer problemas no solo económicos sino también operativos.

APLICACIONES INFORMÁTICAS – UN CASO PARTICULAR

Las aplicaciones informáticas no están en el CPSTIC, catálogo reservado a "productos y servicios de seguridad". Sin embargo, las aplicaciones forman el núcleo que materializa los servicios corporativos para usuarios y ciudadanos, aportando las

CONTINÚA EN PRÓXIMA PÁGINA

interfaces y funcionalidades de gestión para cada una de las áreas competenciales del organismo público. En este contexto, la certificación de la seguridad de las aplicaciones adquiere una importancia fundamental que, sin embargo, a la fecha, no encuentra un reflejo en un esquema de certificación específico.
El esquema de certificación actual del ENS certifica "sistemas de información". La definición contenida en el *Anexo IV – Glosario* del ENS es, en mi opinión, desafortunada e incompleta, así como poco aplicable a las certificaciones de "productos software" que ofrezcan garantías a los organismos contratantes sobre las prestaciones de seguridad que aportan.

Como ejemplo, el alcance certificado de la aplicación con mayor implantación en la AAPP es:

Los sistemas de información que soportan los servicios de Gestiona, ubicados en Centros de Datos externalizados en España.

Es decir, al certificar sistemas de información que soportan el producto, **y no el propio producto software**, no se obtiene garantía alguna de que dicho producto aporte las prestaciones de seguridad necesarias en base a la categorización del sistema de información donde se integra. Por otra parte, en la certificación actual se auditan las medidas del ENS, las cuales incluyen previsiones en materia de seguridad pero no incluyen la "calidad del software" (ISO 25000) ni el "proceso de desarrollo de software" (ISO 33000), referenciales que deberían ser exigibles (total o parcialmente) para productos software de cuya calidad y prestaciones dependen, **literalmente**, los servicios de la AAPP.

SOMBRAS DE LA CERTIFICACIÓN ENS PARA APLICACIONES

Adicionalmente a las insuficiencias del modelo actual de certificación para aplicaciones informáticas, encontramos alcances certificados cuyo contenido es de tal nivel de ambigüedad que, en la práctica, no aportan información sobre el producto. Ejemplos:

El Sistema de información que da soporte a los procesos de desarrollo y comercialización de software ….

Los sistemas de información que dan soporte a la actividad de negocio: comercialización, consultoría e implantación, BPO, formación, soporte a usuarios y mantenimiento de software de gestión ……..

Teniendo en cuenta que las empresas titulares ofrecen sus **productos concretos** a la AAPP, a la vista de estos alcances ¿qué garantía ofrece la "comercialización de software" sobre las prestaciones de seguridad de dichas aplicaciones **concretas**? ¿Es admisible este alcance en un proceso de licitación de aplicaciones informáticas? ¿Por qué se admiten estos alcances por parte de las entidades certificadoras y supervisoras del proceso de certificación? ¿Alguien imagina que en el CPSTIC la descripción del producto certificado fuera "sistema de información que soporta el desarrollo y la comercialización de cortafuegos"?
En el siguiente ejemplo la empresa certificada es mucho más clara en su alcance:

"Sistema de Información de la marca TAO propiedad de T-Systems ITC Iberia SAU, para ser implantado en ....."

Pero sigue "sufriendo" la necesidad de incluir "sistema de información" como unidad de certificación del actual esquema.

CONCLUSIONES

El esquema de certificación de productos y servicios necesita incluir un esquema específico para las aplicaciones informáticas como ya existe para otros grupos de productos incluidos en el CPSTIC.

Problemática de los Roles y responsabilidades del ENS en las entidades locales

Para finalizar la temporada actual vamos a exponer los problemas relacionados con las estructuras organizativas requeridas por el Esquema Nacional de Seguridad (Real Decreto 311/2022, ENS en adelante), ya que contemplan una serie de roles que, en la Administración Local, son complicados de implementar por la endémica escasez de recursos.

¿QUÉ REQUIERE EL ENS?

Nivel Gobierno.
•Responsable del Servicio. Determinará los requisitos de seguridad de los servicios prestados.
•Responsable de la Información. Determinará los requisitos de seguridad de la información tratada.
Roles asignados a personas, comités u órganos colegiados. Habitualmente asociados a jefaturas de unidades administrativas dado que, en teoría, son quienes conocen con mayor profundidad las características concretas de un servicio y de la información que trata, muy especialmente los requerimientos legales que les afectan y los datos que gestionan, lo que supone una ayuda relevante para las valoraciones correspondientes. En la práctica, estas personas necesitan una formación y soporte adecuado para que su conocimiento especializado se transforme en criterio aplicable en el ENS. Es admisible que estos roles sean asumidos por un Comité de Seguridad de la Información adecuadamente configurado, manteniendo siempre una participación fluida por parte de las personas responsables de las unidades administrativas.

Nivel Supervisión.
•Responsable de Seguridad. Determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisará la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones.

Este rol es fundamental pero no fácil de identificar en un Ayuntamiento, ya que, idealmente, debería tener un conocimiento global de las unidades administrativas para interactuar adecuadamente con sus responsables pero también unos conocimientos técnicos globales que le permitan interactuar con el Responsable del Sistema y su equipo técnico. En la práctica, puede nombrarse un Responsable de

Seguridad y Responsables de Seguridad Delegados (p.e. por especialidades), así como constituir un Comité al respecto.
Las empresas adjudicatarias de servicios externalizados deben nombrar un Responsable de Seguridad con las potestades suficientes para determinar las decisiones en materia de seguridad que sean necesarias en su organización.

Nivel Operación.
•Responsable del Sistema. Por sí o a través de recursos propios o contratados, se encargará de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo, pudiendo delegar en administradores u operadores bajo su responsabilidad.
Este rol requiere de perfiles informáticos con los conocimientos y experiencia necesarios para la implementación, control, mantenimiento y evolución de la seguridad de los sistemas informáticos.

El ENS requiere que el Responsable de Seguridad y el Responsable del Sistema sean independientes y sin relación jerárquica entre ellos, algo que choca frontalmente con la realidad de los Ayuntamientos pequeños e incluso medianos, donde los recursos disponibles no permiten estos planteamientos, por lo que se deben documentar las medidas compensatorias correspondientes para contemplar en la mayor medida posible esta independencia.

PROBLEMA CRÓNICO = ESCASEZ DE RECURSOS
Siempre he defendido el ENS como una gran iniciativa teórica pero con poco realismo para llevarlo a la práctica en diferentes aspectos, muy especialmente cuando se trata de recursos humanos dado que, dentro de la histórica escasez de recursos en general, la escasa (o nula) disponibilidad de personas capacitadas para absorber las tareas que el ENS requiere supone un inhibidor de primer orden para una

CONTINÚA EN PRÓXIMA PÁGINA

efectiva implantación y certificación en organismos cuyo volumen de personal es inversamente proporcional al volumen de servicios. Es decir, los Ayuntamientos.
Las diferencias con otros organismos están claras. Un ministerio o consejería gestiona temas determinados y bastante acotados (p.e. bienestar social, educación, sanidad, ordenación territorial, etc) mientras que un Ayuntamiento concentra la mayoría de estos temas dentro de sus competencias o por delegación de otros organismos competentes. Sólo es necesario acudir a los artículos 25 y 26 de la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local (LBRL en adelante) para comprender el volumen de servicios que deben prestar los Ayuntamientos, las dificultades inherentes para disponer del personal adecuado y, en determinadas épocas (como la actual), los problemas presupuestarios y restricciones legales para ampliar su plantilla.
En este contexto, la aparición de nuevos requerimientos supone una sobrecarga adicional sobre un personal ya sobrecargado y difícilmente ampliable, máxime cuando la asunción de los roles del ENS requiere, a su vez, formación específica sobre el propio ENS y su praxis para personas que, muy probablemente, no conocen este marco normativo.
Quiero destacar que, por otra parte, en los Ayuntamientos puede observarse un aumento significativo en la securización de sus plataformas informáticas, así como una conciencia clara de la "necesidad de la seguridad", pero esas iniciativas vienen habitualmente generadas desde los departamentos de Informática y carecen de la visión del principio básico del ENS denominado "Seguridad como un proceso integral".

SOLUCIÓN = RACIONALIDAD

El ENS ha nacido asumiendo unas disponibilidades de recursos que no tienen un reflejo real en la inmensa mayoría de entidades locales de España, ni siquiera con el soporte de organismos supramunicipales que, a su vez, adolecen de las mismas carencias que los Ayuntamientos en cuanto a la escasez de recursos.
La intervención e implicación de la FEMP es relevante, aportando guías útiles para facilitar el cumplimiento y la certificabilidad del ENS, pero siguen sin resolver los aspectos organizativos de base.
Por otra parte, iniciativas como µCeENS facilitan la certificabilidad para los sistemas de categoría BÁSICA y es una magnífica plataforma de inicio, pero tampoco resuelve la indisponibilidad de recursos en los roles requeridos.
En mi opinión, y teniendo en cuenta que la inmensa mayoría de Ayuntamientos de España tienen volúmenes de población muy reducidos, servicios muy reglados y una endémica escasez de recursos, debería plantearse un perfil de cumplimiento donde se adapten los requerimientos organizativos a las capacidades reales.

FIN DE TEMPORADA

Con esta edición de julio de 2023 finaliza la temporada actual. Espero que esta sección haya resultado interesante, nos veremos de nuevo en la próxima temporada.

MGEIT®

eGob®

COBIT® 2019 + ISO 38500
IT Governance
Gobierno TI

CERTIFÍCATE EN
GOBIERNO DE TI

Gobierno de Información y Tecnología EGIT es un nivel de madurez sobre la Gestión de las Tecnologías de la Información ITSM que consigue Alinear la Tecnología al Negocio y no viceversa. Puede haber Gestión sin Gobierno, pero jamás habrá Gobierno sin Gestión. Y tú ¿Gobiernas o solo Gestionas la Información y la Tecnología?

NIVELES DE CERTIFICACIÓN

Nivel de Certificación Board*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de la materia, su entorno y ámbito de aplicación, sus roles y responsabilidades que les permita participar en las inicativas.

Nivel de Certificación Executive*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de las Buenas Prácticas, Metodologías y Bases de Conocimiento aplicables con el fin de dirigir o participar en equipos de implementación.

Nivel de Certificación Leader*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de las normas y Estándares ISO aplicables con el fin de dirigir o participar en equipos de implementación.

Nivel de Certificación Skilled*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de la elaboracion de documentos, informes, planes, herramientas y/o artefactos que les permitan la aplicación práctica de los conocimientos.

*Niveles de Certificación pertenecientes a los Esquemas de la Entidad de Certificacion Business&Co.® y alineados con la Norma UNE-EN ISO/IEC 17024:2012 Evaluación de la Conformidad. Requisitos Generales para los Organismos que realizan Certificación de Personas. Más información: https://businessandcompany.com/certificacion-de-personas

MISION

Nuestra misión consiste en instituir una nueva clase directiva capaz de liderar con éxito las oportunidades que nos brinda la era digital.

FORMACIÓN BUSINESS CLASS

- Formación experiencial y participativa en remoto y en directo para una mayor comodidad del alumno.
- Cursos de cuatro sesiones de 5 horas en formato tardes de martes y jueves o formato viernes tardes y sábados mañanas.
- Máximo doce alumnos por convocatoria para una mayor interacción y compartición de experiencias y anécdotas.
- Curso de Doble Certificación del Master de Gobierno y Gestión de Información y Tecnología MasterGEIT®

CONVOCATORIAS 2022/23

- **ABRIL 2023 (Formato Martes y Jueves Tardes)**
  Martes 4, jueves 6, martes 11 y jueves 13
- **MAYO 2023 (Formato Viernes Tardes y Sábados Mañanas)**
  Viernes 5, sabado 6, viernes 12 y sábado 13

eGob®

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

Lanzamiento del Service Management Institute SMI®

El miércoles 26 de abril tuvo lugar el lanzamiento del Service Management Institute SMI®, la comunidad global de profesionales en la Dirección y Gestión de Servicios, Comprometidos con la Innovación, las Buenas Prácticas y la Mejora Continua.

Este acto fue la escenificación de la transformación de la Asociación sin Ánimo de Lucro itSMF España, asociación profesional que desde el año 2004 ha atendido las necesidades de la Gestión de Servicios de Tecnología (ITSM), y que a partir de 2023 se renueva para atender los servicios de una forma global en todas las áreas de la empresa.

Con el lanzamiento del Service Management Institute SMI® nace la nueva Certificación Profesional en el Ámbito de la Dirección de Servicios, que tiene como objetivo acreditar a los mejores profesionales en dirección de servicios a nivel internacional. Por tanto, es una acreditación global que no depende de sectores o países, sino que es aplicable a cualquier empresa y sector.

El presidente del Consejo Asesor del Service Management Institute SMI®, Marlon Molina, fue el encargado de dar la bienvenida al acto de lanzamiento, que calificó como "un momento histórico", ya que "casi 20 años después pasamos a atender la dirección y la gestión de todos los servicios en un mundo 'As a Service'".

"El sector público y el sector privado, todos están viviendo una gran transformación. Hasta el año 2030 vamos a movernos de los productos a un mundo 'As a service', un mundo absolutamente lleno de servicios que, además, interactúan unos con otros. Hace 20 años que ya existe la profesión de gestión de servicios y hoy ha nacido oficialmente la Asociación de Director de Servicios. Tenemos una gran oportunidad porque todo está por crear, pero desde nace desde la experiencia", resaltó Molina.

CONTINÚA EN PRÓXIMA PÁGINA

Acto seguido, el presidente del Service Management Institute SMI®, Javier Peris, apuntó que la presentación es "el renacimiento" de itSMF España, que a partir de ahora aplicará su conocimiento en dirección servicios no únicamente a IT, sino a todos los departamentos: "La asociación lleva 20 años en los que ha ido aprendiendo, los servicios han ido cambiando, las tecnologías han ido apareciendo, hemos vivido nuevos enfoques y tecnologías, y de alguna manera cada vez más vamos a un mundo más 'As a Service' donde no solo se requieren gestión de servicios sino verdaderos Directores de Servicios" .

Por tanto, "si lo que la ciudadanía necesita es percibir los servicios, también deberíamos de acreditar a verdaderos directores de servicios que los ofrezcan con el valor que se espera", recalcó el presidente de Service Management Institute SMI®. De esta forma, nace esta comunidad global que tiene como objetivo certificar a aquellos profesionales que cuentan con las habilidades necesarias para no solo gestionar sino tambien dirigir servicios.

En este punto, Javier Peris destacó que a pesar de que "estamos impactados por una cantidad de servicios tremenda, hasta la fecha se le había dado demasiada importancia al proyecto". "Los proyectos son necesarios, pero tienen una fecha de inicio y de fin conocida, mientras que los servicios son lo que perdura, se disfruta y el usuario de verdad percibe. Es fácil encontrar disciplinas, metodologías y profesionales formados y certificados como directores de proyectos, pero hasta hoy no era fácil encontrar profesionales en dirección de servicios. Gracias al Service Management Institute ya es posible, podemos encontrar la alta dirección formada adecuadamente como Directores de Servicios", añadió.

CONTINÚA EN PRÓXIMA PÁGINA

Durante el acto, el presidente del Colegio Oficial de Ingeniería Informática de la Comunitat Valenciana (COIICV), Alejandro Blasco, se congratuló de que la asociación escogiera la Semana Informática como el espacio idóneo para presentarse de forma oficial y consideró "muy oportuno el momento de nacimiento de Service Management Institute SMI®", que representa a un colectivo que tiene mucho que ver con la parte IT, pero que va más allá.

A continuación, tuvo lugar un acto simbólico sobre el escenario de Las Naves, con una fotografía de familia de representantes de los cuatro sectores 'padrinos' de Service Management Institute SMI®: Manuel Serrat, Vicepresidente de la Asociación de Técnicos Informáticos de la Administración Local ATIAL; a Carlos Pampliega, Vicepresidente del Capítulo de Madrid del Project Management Institute PMI Madrid; Cayetano Hernández, Presidente de la Federación de Asociaciones de Informática de la Salud FAIS, y Alejandro Blasco, presidente del Colegio Oficial de Ingeniería Informática de la Comunidad Valenciana COIICV.

Tras la fotografía, la presidenta del Consejo Académico del Service Management Institute SMI®, Esperanza Marcos, presentó la Base de Conocimiento de la Asociación, el Service Management Body of Knowledge SMBoK®, quien afirmó que "estamos en un mundo absolutamente de servicios". La globalización, el aumento de la esperanza de vida o la transformación digital son algunos de los factores que, según Esperanza Marcos, han provocado que, cada vez más, las economías se basen en servicios.

En su ponencia, la presidenta del Consejo Académico del Service Management Institute SMI® explicó que, a pesar de estar en un mundo de servicios, las organizaciones trabajan como en una época industrial y los profesionales siguen formándose de esta manera. Por este motivo, señaló, es el momento de empezar a formar a profesionales para un mundo de servicios y para organizaciones de servicios.

"Nos faltan certificaciones de profesionales en dirección de servicios. El Service Management Institute SMI® es una iniciativa muy pertinente en este momento y estamos trabajando en la elaboración de un cuerpo de conocimientos que defina qué conocimientos debe tener un director de servicios", resaltó.

A su juicio, el director de servicios es como el director de orquesta: "No tiene que saber tocar perfectamente el piano o ser un experto violinista, pero necesita saber cómo suena cada instrumento y saber en qué momento y con qué intensidad les tiene que dar la entrada".

CONTINÚA EN PRÓXIMA PÁGINA

Tras la intervención de Esperanza Marcos, fue el turno del Vocal y miembro de la Junta Directiva del Service Management Institute SMI®, Marcos Navarro Alcaraz, quien expuso los detalles de la Certificación Service Management Profesional SMP® y su Proceso de Grandfathering que permite por Méritos Propios obtener la Certificación. Marcos Navarro detalló que, con la creación del Service Management Institute SMI®, se extiende la vinculación anterior de itSMF únicamente con la tecnología, para pasar a acreditar y reconocer además de certificar a profesionales de todos los sectores y ámbitos.
"Queremos que los servicios no solo se gestionen sino se dirijan cada vez mejor, esa dirección va a requerir mejores profesionales y que se puedan identificar más fácilmente. Generando esta certificación lo que queremos es que se puedan identificar de la misma forma que cuando las empresas buscan profesionales en la dirección de proyectos", explicó.
Marcos Navarro subrayó que se trata de una certificación global, que no depende de sectores, países o tecnologías, por lo que es aplicable a cualquier empresa: "Nuestro objetivo primordial con la certificación es que, mirando a una sala, sepamos quienes tienen el pin del Service Management Profesional SMP® del Service Management Institute SMI®. Queremos que sea un distintivo de calidad de los profesionales". Así, el objetivo del Service Management Institute SMI® es generar una certificación que sea reconocida por la industria y que permita evaluar a buenos profesionales en la dirección de los servicios, mediante experiencia, conocimientos y un examen de evaluación.

Por último, Marlon Molina Presidente del Consejo Asesor del Service Management Institute SMI® presentó y moderó la mesa redonda titulada 'La Dirección y Gestión de Servicios en la Administración Pública y la Alta Dirección' con la participación de Inmaculada Sánchez Ramos, de Madrid Digitaliza; Ana Bastida, del Instituto Municipal de Informática del Ayuntamiento de Barcelona; y Ana María Pont, de la Oficina de Proyectos Europeos del Ayuntamiento de Valencia. En dicha mesa, las ponentes abordaron la necesidad de extender la cultura de los servicios a las administraciones públicas, del reto que supone para éstas el mundo 'As a Service' o de la importancia de la figura del director de servicios.

En su intervención, Inmaculada Sánchez insistió en la importancia de "generar ecosistemas de relación y confianza mutua en las administraciones públicas, porque las realidades hoy en día son sofisticadas y son servicios continuos, y no proyectos que empiezan y acaban". "Toda la vida hemos ofrecido servicios, pero el mundo 'As a Service' supone movernos en procesos dinámicos y flexibles, antes éramos muy lineales y ahora estamos en un mundo totalmente dinámico", dijo.

Para Inmaculada Sánchez, las administraciones públicas han de adaptarse al mundo actual y "aprender a pensar fuera de la caja", de forma que se ponga al ciudadano en el centro. También insistió en la necesidad de crear consejos asesores para que se generen espacios de colaboración público-privada.

CONTINÚA EN PRÓXIMA PÁGINA


Institute

Por su parte, Ana Bastida recalcó la importancia de "impulsar servicios y proyectos transversales porque los ciudadanos necesitan que tengamos una visión holística de los mismos y que cuando les ofrezcamos un servicio, lo hagamos de manera transversal".

Sobre el nacimiento de Service Management Institute SMI®, Bastida lo calificó como "una oportunidad" para trasladar el concepto de gestión y de dirección de servicios no al ámbito de IT, sino al ámbito municipal y de todas las administraciones públicas. "Espero y deseo que esta iniciativa ayude a las administraciones públicas a posicionarse como administraciones 'As a Service', que es lo que esperan los ciudadanos: tener una administración líquida en consonancia con lo que es la sociedad actual", aseguró.

Respecto a este cambio hacia el mundo 'As a Service' en las administraciones, Ana Pont consideró que es "un camino que todavía no hemos explorado y que puede ser parte de la solución a este estado de bienestar en el que vivimos y que queremos fortalecer". Para ello, resaltó que "el proceso de transformación en las administraciones públicas debe partir desde arriba: desde la visión política hacia abajo".

En este sentido, Ana Pont señaló que "es un reto y una obligación" transformar cómo funcionamos en las administraciones y extender la cultura del proyecto a la dirección de servicios. "Es más necesario que nunca el Service Management Institute SMI® sobre todo para las administraciones y los empleados públicos. El mundo gira cada vez más 'As a Service' y los ciudadanos requieren que las administraciones, como prestadoras de servicios, lo hagamos cada vez mejor, con un coste más eficiente y que el ciudadano realmente se sienta satisfecho con lo que hacemos", concluyó.

Un evento el Lanzamiento del Service Management Institute SMI® que concluyó con un vino español, cóctel y exhibición de corte y degustación de Jamón ibérico a cargo de un maestro cortador que permitió el Networking y el intercambio de experiencias, anécdotas y conocimientos entre distinguidos profesionales tanto del sector público como el privado llegados tanto de distintos puntos de la geografía española como de países donde el Service Management Institute SMI® empieza a tener presencia.

ABOGADOAMIGO

Bufete Experto en
Nuevas Tecnologías

NUEVOS MASTERS

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