ESPECIAL

"Ojo al dato"

DE Tecnología & Sentido Común

ESPECIAL
AGOSTO
2023

ESPECIAL "Ojo al dato" 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

Ricard Martínez

Profesor en el Departamento de Derecho Constitucional, Ciencia Política y de la Administración y Director de la Cátedra de Privacidad y Transformación Digital. Doctor en Derecho por la Universitat de València. Miembro de la mesa de expertos en datos e Inteligencia Artificial de la Consejería de Innovación y Universidades de la Generalitat Valenciana. Miembro del grupo de expertos para la elaboración de una Carta de Derechos Digitales de la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital. Ha sido Presidente de la Asociación Profesional Española de la Privacidad y responsable del Área de Estudios de la Agencia Española de Protección de Datos.

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

Twitter: https://twitter.com/ricardmm

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

índice

DE CONTENIDOS

https://tecnologiaysentidocomun.com

índice

#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

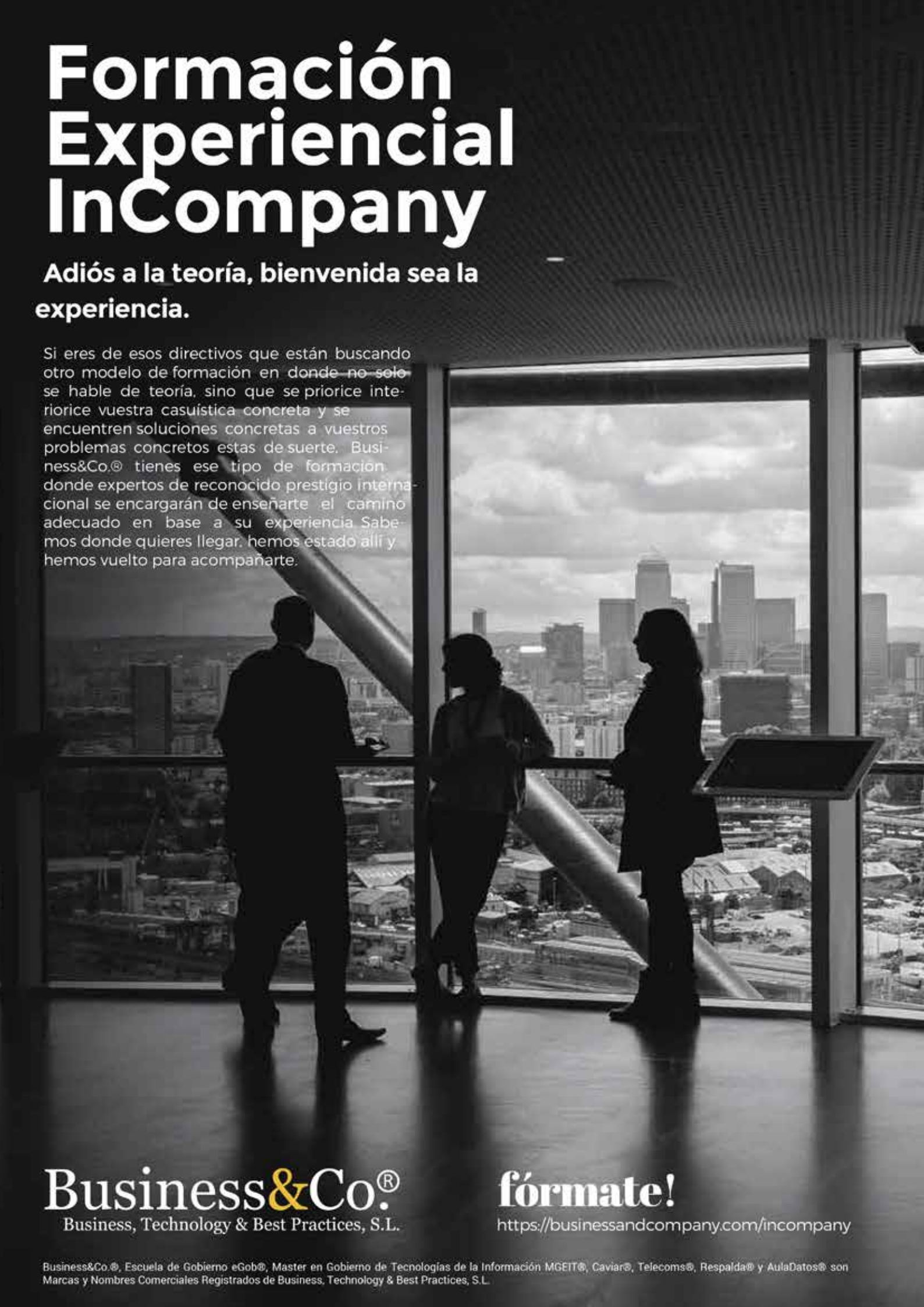
VI Premios ESET Periodismo y Divulgación: Tecnología y Sentido Común Premiada en la Categoría Blogs por el Articulo de Ricard Martínez "Seguridad en el Smartphone".
Los Premios ESET apuestan por la educación y la concienciación de la sociedad en materia de ciberseguridad, y los medios de comunicación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

Protección de datos personales y Administración Pública: un largo camino por recorrer: la formación

La Administración Pública en España ha sido tratada con particular benevolencia por parte de la legislación en protección de datos. En esencia, y sin perjuicio de las especificidades en materia policial, el marco de las obligaciones que se le imponen es el mismo que al sector privado con escasas obligaciones adicionales, pero no así el modo de sustanciar la responsabilidad administrativa ante eventuales infracciones administrativas. En efecto, y expresado en términos coloquiales: no se pagan multas, se declara la infracción y en casos excepcionales se ha suspendido el funcionamiento de un "fichero" o tratamiento hasta que se remedian los problemas que presenta. La tesis dominante se sustentó sobre la idea de que sancionar a la Administración constituye una mera transferencia de fondos y, además, perjudica esencialmente al contribuyente al detraer fondos del presupuesto público.

Sin perjuicio de que no se haya estudiado científicamente la presencia de una relación de causa a efecto lo cierto es que el enfoque del riesgo regulador puede haber influido en los procesos de toma de decisiones. El mapa que cualquier experto en la materia presentaría incluiría en esta bitácora la formación, la escasez de personal en términos de delegados de protección de datos y su equipo de soporte, un inadecuado posicionamiento de los delegados y su no inserción inadecuada en la planificación estratégica de la entidad.

A diferencia de lo que sucede en materia de prevención de riesgos laborales no existe una política de formación universal del personal en protección de datos. Basta con ojear la oferta formativa en Institutos de Administración Pública, o en servicios especializados vinculados al personal estatutario en salud, al personal de instituciones educativas y en servicios de formación de municipios, diputaciones o universidades públicas. En muy pocos casos se ha emprendido una labor de formación básica, general u obligatoria. Se oferta un volumen limitado de cursos/año de carácter voluntario.

El efecto de estas políticas públicas es demoledor. En primer lugar, en función del volumen de la plantilla se necesitarían varios centenares de años para formar al personal activo en un determinado momento. Por ejemplo, ¿Cómo esperan formarse miles de sanitarios cuando se oferten cursos para 200 personas al año?

CONTINÚA EN PRÓXIMA PÁGINA

Además, la voluntariedad provoca disfuncionalidades muy graves. Si la asistencia al curso es voluntaria es perfectamente posible que en una determinada unidad administrativa los puestos con menor responsabilidad y capacidad de decisión posean un mayor conocimiento. Y ello, conduce a la melancolía en el menor de los casos y al conflicto en el peor. ¿Cómo va el personal auxiliar a cuestionar decisiones de la dirección técnica que infringen la normativa? Así que, aunque el ejemplo sea peregrino, "si se te ordena que registres a los asistentes de la jornada en una cuenta de Google Drive creada al efecto como jornadaX@gmail.com, tú lo haces y no me vengas con lo del encargado del tratamiento".

Por otra parte, el diseño en la formación tiende a ser particularmente ineficiente desde el punto de vista de los contenidos. En este sentido, en más de una ocasión se produce una gradación de una mera exposición de las obligaciones de seguridad a sesudos cursos teóricos en los que analizar la legislación aplicable. Y ello sin atender a las necesidades reales de las organizaciones. Por experiencia e intuición cabe apostar a que la formación a la dirección política ni se contempla y cuándo esta sucede se limita de nuevo a los aspectos básicos de la seguridad. Del mismo modo, no se forma operativamente a los cuadros técnicos. Y el desarrollo de formación estratégica orientada a los servicios de tecnologías de la información y las comunicaciones no siempre se tiene en cuenta. Allí donde ha calado con mayor intensidad la formación contempla al menos el conocimiento de los procesos internos de cumplimiento normativo.

Evidentemente, se ha dibujado aquí el peor de los escenarios posibles. Si las y los lectores de este artículo se sienten reflejados en él tienen un serio problema. Porque el resultado que producen es sobradamente conocido. Vds. viven en una Administración en la que la dirección política no se sentirá concernida por esta materia. En ella, la persona delegada de protección de datos será percibida con hostilidad por los cuadros directivos de alto nivel y carecerá de un marco de coordinación y soporte en los cuadros técnicos. Por otra parte, las pocas personas concienciadas generarán conflicto cada vez que constaten una infracción o, en el menor de los casos, la mera dación de cuentas de lo que hallen o la necesidad de obtener soporte ante el incumplimiento sistemático de cualquier tipo de procesos desbordarán la oficina del DPD con decenas de consultas y solicitudes de informe.

La formación, el compromiso y el empoderamiento constituyen el pilar sobre el que se sostiene el cambio cultural en cualquier organización. Por eso sorprende enormemente que no se haya impuesto por Ley el deber de formar al personal y la ausencia de tal formación sea expresamente considerada una infracción. Afortunadamente, las Directrices 4/2019 del Comité Europeo de Protección de Datos, de 20 de octubre de 2020, relativas al artículo 25, Protección de datos desde el diseño y por defecto, (Versión 2.0) nos ofrecen un criterio claro cuando señalan que Una medida técnica u organizativa o una g a r a n t í a puede ser cualquier cosa desde la aplicación de soluciones técnicas avanzadas hasta la formación básica del personal».

Así pues, no cabe duda de que aquellas administraciones que no hayan previsto una formación básica de todo el personal que participen en los tratamientos incurrirían potencialmente en la infracción tipificada por el artículo 73.d de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales consistente en

La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para aplicar de forma efectiva los principios de protección de datos desde el diseño, así como la no integración de las garantías necesarias en el tratamiento, en los términos exigidos por el artículo 25 del Reglamento (UE) 2016/679 (…)

La carencia de formación es territorio abonado para la violación del derecho fundamental a la protección de datos y parece que vamos con unos 30 años de retraso.

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

Protección de datos personales y Administración Pública, un largo camino por recorrer: el modelo de gestión.

Como se señaló en el número anterior, la carencia de una adecuada estrategia de formación se erige en obstáculo para el adecuado cumplimiento de la Administración en materia de protección de datos. Esta situación podría agravarse cuando no se cuenta con un modelo de gestión de la privacidad. De hecho, es la ausencia de un modelo de *compliance* sea probablemente origen y consecuencia de esta carencia.

En la mayor parte de entidades públicas se atribuye la función de fiscalización del cumplimiento normativo a unidades del más diverso signo. Con carácter general, dicha tarea puede atribuirse a la inspección de servicios, en algunas entidades aparecen las denominadas unidades de control interno, o, en cualquier caso, existen órganos de intervención generalmente dedicados al control contable y presupuestario. Por su parte, el delegado de protección de datos, pieza clave para la garantía del cumplimiento normativo, se suele situar bajo la esfera de competencia de alguno de los órganos que integran el Gobierno de las respectivas administraciones. Los podemos encontrar con la categoría de dirección o subdirección general bajo la dependencia de un ministerio o una consejería en las comunidades autónomas, como jefaturas de servicio bajo de la dependencia de la presidencia de las corporaciones locales, insertos en unidades de tecnologías de la información y las comunicaciones, o en la esfera de las secretarías generales de las universidades públicas.

Sin perjuicio de que dediquemos otro artículo al encaje funcional, nos centraremos aquí en las condiciones que usualmente definen la estrategia de cumplimiento normativo en el marco de las administraciones. En esta materia deberían adoptarse buenas prácticas fácilmente deducibles de las distintas guías publicadas por la Agencia Española de Protección de Datos y las autoridades autonómicas. Particularmente deberían tenerse en cuenta tanto las metodologías de análisis de riesgos, como las de protección de datos desde el diseño y por defecto.

Sin embargo, resulta relevante subrayar primero algunas de las carencias que hemos podido constatar a lo largo de nuestra experiencia. La primera de ellas, se refiere a la asignación de recursos humanos. El anteproyecto de ley de lo que después sería la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, señalaba expresamente la necesidad de que la implantación de la figura del delegado de protección de datos fuese a coste cero.

Aunque esta referencia desapareció en la versión definitiva de la ley, su filosofía ha inspirado la práctica administrativa. Por lo general, el equipo humano del que disponen los delegados de protección de datos suele ser particularmente limitado. Si a ello unimos la carencia de formación de los técnicos de gestión, que deberían ser otra palanca natural para la aplicación de los criterios de cumplimiento normativo, resulta sencillo concluir que la primera carencia reside en la falta de capacidad para la gestión de los objetivos mínimos de cumplimiento normativo en organizaciones de altísima complejidad.

Por otra parte, se corre el riesgo de desplegar un modelo de cumplimiento de carácter puramente epidérmico. Este consiste en convertir en "tratamientos" las antiguas declaraciones de ficheros ante la AEPD, y la declaración gestión y gestión de ulteriores tratamientos en el rellenado de una tabla de Excel o Word que posteriormente se publica en el registro de actividades de tratamiento del portal de transparencia que corresponda. En otros casos, en lugar de disponer de recursos adecuados, se externaliza el cumplimiento normativo en proveedores privados, aplicando como criterio esencial para la contratación el del menor coste ofertado. En uno u otro modelo, cualquier mínimo requerimiento de cumplimiento normativo resultará imposible de alcanzar.

CONTINÚA EN PRÓXIMA PÁGINA

En nuestra opinión, las organizaciones públicas deberían de disponer de procedimientos funcionales al propio ciclo de vida del dato. Desde este punto de vista, es la autodeclaración interna de una necesidad de tratamiento la que debería orientar el punto de inicio de un adecuado modelo de gestión. Ningún tratamiento debería alcanzar la autorización del responsable correspondiente, ni integrarse en un registro de actividad del tratamiento, sin haber sido sometido a los procedimientos de análisis de riesgos que derivan claramente de los artículos 24,32 y 35 del RGPD y de un proceso de diseño funcional a los requerimientos de su artículo. Todos estos procesos deben relacionarse adecuadamente con los principios de protección de datos del artículo 5 del RGPD.

Paralelamente, no se deberían descuidar ni los procesos de gestión de la externalización mediante contratación de proveedores privados que traten datos personales, ni de la gestión de la seguridad en todas sus dimensiones, y particularmente de los incidentes graves de seguridad, y por último cuidar la presencia pública de la institución a través de espacios de Internet y medios sociales. Por último, en una lista que no pretende ser exhaustiva, resultan imprescindibles los servicios de consulta y atención a los usuarios internos y a las personas interesadas, teniendo en cuenta que el deber de transparencia y la gestión de los derechos de acceso, rectificación, supresión, portabilidad, limitación u oposición al tratamiento, poseen singularidades que las hacen merecedoras de especial atención.

De uno u otro modo, el conjunto de procesos dirigidos al cumplimiento normativo en protección debe ser diseñado funcionalmente atendiendo a las características y necesidades de la entidad pública de la que se trate, debe documentarse adecuadamente y debe someterse a un procedimiento constante de análisis y de retroalimentación en cuanto a su calidad y eficiencia.

Nada distinto de lo que atañe a la gestión ordinaria de cualquier proceso en el seno de la Administración.

La ausencia de procesos de gestión en materia de protección de datos, la carencia de un plan, pone de manifiesto la importancia que cada organización pública conceda a esta materia como elemento estratégico, o meramente accesorio en las decisiones de gobierno de la entidad. En el segundo caso, el desgobierno del cumplimiento normativo en protección de datos augura con total seguridad la existencia de carencias significativas en la calidad de la información que va a manejar la institución y a buen seguro en el medio plazo generará inconvenientes graves para cualquier proceso de digitalización.

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®
admisio
https://e

Protección de datos y Administración Pública, un largo camino por recorrer: el liderazgo.

En los dos últimos artículos de esta sección se ha dedicado una cierta atención a considerar el conjunto de aspectos que inciden de modo significativo en el cumplimiento normativo del Reglamento General de Protección de Datos y la legislación española en la materia por parte de la Administración Pública. En esta tercera, y última entrega, trataremos de considerar lo que nuestro juicio constituye el elemento determinante para la existencia de una falta de incentivos al cumplimiento.

Existen dos factores que en nuestra opinión inciden de manera determinante: una regulación de la responsabilidad particularmente laxa junto a una carencia de compromiso por parte de quienes desde la política o desde el desempeño de altos cargos no realizan los debidos esfuerzos para asegurar una labor de impulso que, como se demostrará, resulta crucial. En primer lugar, si algo ha caracterizado al modelo español de protección de datos, desde la interpretación que la Agencia Española de Protección de Datos hizo de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal LORTAD), y cristalizó posteriormente en Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), no es otra que la ausencia de responsabilidad pecuniaria de las administraciones públicas españolas. La teoría que sustentaba esta decisión de naturaleza política con enorme trascendencia jurídica no era otra que el hecho de considerar que cuando se impone una sanción económica a una administración pública se trasladan el importe de la multa desde el presupuesto de la sancionada hacia la Administración General del Estado. Ello, en opinión de la autoridad de protección de datos, resulta además lesivo para la ciudadanía, al detraer del presupuesto de la sancionada, cantidades significativas necesarias para el despliegue de políticas públicas.

Podremos estar de acuerdo con esta tesis mantenida. Lo cierto es que su resultado no fue otro que la inacción de las administraciones. Por si fuera poco, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) reguló esta materia desde una doble aproximación.

En primer lugar, ha consistido en un cambio de tiempos verbales en el artículo seis 77.3 que parece apuntar a la necesidad de apertura de oficio de expedientes disciplinarios a los funcionarios responsables de las infracciones a la legislación de protección de datos ya que la autoridad de protección de datos **propondrá** también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. A día de hoy casi nunca ha encontrado esos indicios. Por otra parte, se contempla la pena de boletín oficial cuando las infracciones sean imputables a autoridades y directivos, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no hubieran sido debidamente atendidos.

CONTINÚA EN PRÓXIMA PÁGINA

Lo que sin embargo resulta sorprendente es la extensión del régimen de responsabilidad a todas y cada una de las entidades del sector público, definidas en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. Esto significa en la práctica, la existencia de una amplia panoplia de instituciones, y particularmente las fundaciones del sector público, eximidas de cualquier responsabilidad económica o pecuniaria, con independencia de la gravedad de la infracción que se hubiera podido cometer.

Por otra parte, y recordando el primer artículo de esta serie relacionado con la formación, lo cierto es que los procesos de formación y concienciación en rara ocasión alcanzan a quienes ocupan el liderazgo político o administrativo en los distintos organismos del sector público. Al inicio de la legislatura en los municipios o tras la toma de posesión y la renovación del equipo ministerial o de una consejería autonómica no esperen encontrar una nota de prensa que diga que el alto responsable político y su equipo directivo se han reunido con la persona delegada de protección de datos para recibir un curso de formación, comprender cuáles sean sus obligaciones y asumir un compromiso con la garantía del derecho a la vida privada de la ciudadanía. Y así, multitud de altos cargos a los que se atribuye la función de responsable en el correspondiente reglamento orgánico y de funcionamiento, o en el registro de actividades de tratamiento, carecen de formación, capacidad, competencia e incluso criterio político en esta materia.

La consecuencia es trágica si no tuviera la vez algo de cómico. La carencia de compromiso político y directivo convierte a la tarea de las personas delegadas de protección de datos de la Administración en un asunto de interés residual, cuando no en un engorro del que conviene deshacerse a la mayor velocidad posible. A las DPD no les queda otro expediente que oficiar al correspondiente responsable indicándoles su posición de independencia, recordándole y subrayando su responsabilidad y, en no pocas ocasiones, haciendo uso de la facultad y obligación que les impone el artículo 36.4 de la LOPDGDD de notificar las infracciones de las que se tuviera conocimiento.

No es este, por tanto, el mejor ecosistema para garantizar el cumplimiento de la normativa de protección de datos por parte de la Administración. Y esta es sin duda una muy mala noticia para nuestra sociedad. La Administración en todas sus áreas se halla inmersa en un proceso de transformación digital literalmente incompatible con esta carencia. Y no sólo esto, enfrentamos una evolución del Ordenamiento jurídico de carácter revolucionario. La Unión Europea está potenciando un ecosistema de datos al servicio de la comunidad en el cual el papel de las administraciones es determinante. Tras la reforma de la Directiva Open Data, la Data Governance Act impulsa la creación de entidades del sector público capaces de poner a disposición de la sociedad grandes volúmenes de datos que hasta ahora no pueden ser liberados por razones relacionadas con la identificabilidad de las personas, o con la tutela de otros derechos como los derechos a la propia intelectual y los secretos industriales y comerciales.

Una Administración que ha dejado de lado el derecho fundamental a la protección de datos, que no se encuentra en disposición de desplegar análisis de impacto riguroso, o de certificarse en el Esquema Nacional de Seguridad difícilmente podrá proveer condiciones que aseguren la generación de repositorios seguros, controlados y trazables para la explotación de la información del sector público. Esta carencia, esta falta de atención a un elemento cualitativo crucial no sólo afecta a la calidad y confiabilidad de los datos, sino que impide materialmente su reutilización. Esta ausencia de compromiso tendrá consecuencias particularmente graves para nuestra economía y competitividad. La creación de los espacios europeos de datos y la regulación de la inteligencia artificial deberían entenderse como un aldabonazo que obliga a convertir el cumplimiento normativo en protección de datos y la adopción de decisiones estratégicas en materia de seguridad y de ética de la inteligencia artificial en una tarea prioritaria para la administración española. Ganarán los derechos fundamentales, ganará la competitividad de la investigación y la innovación en nuestra economía, y ganará nuestra sociedad. Aunque no existan multas.

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

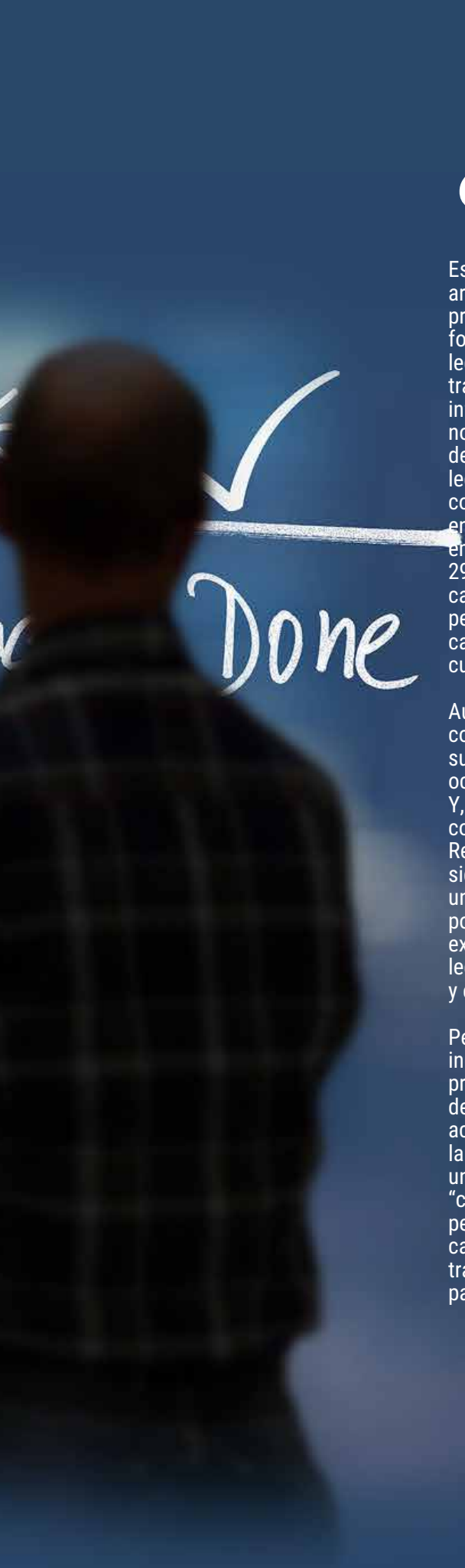
- **SEPTIEMBRE 2022 (Formato Martes y Jueves Tardes)**
  Martes 20, jueves 22, martes 27 y jueves 29
- **OCTUBRE 2022 (Formato Viernes Tardes y Sábados Mañanas)**
  Viernes 21, sabado 22, viernes 28 y sábado 29
- **FEBRERO 2023 (Formato Viernes Tardes y Sábados Mañanas)**
  Viernes 3, sabado 4, viernes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

eGob

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


Stories
ToDo
In Progress
Testin

¿Es legal...?



Esta es sin duda una de las preguntas, y uno de los modos de titular artículos y posts, que más zozobra me causa en el mundo del derecho a la protección de datos. Este tipo de afirmación suele venir acompañada de la formulación de alguna cuestión relacionada con las condiciones de legitimidad o legitimación para tratar datos personales. Usualmente se trata de un asunto de carácter básico, de la mera reproducción de algún informe o resolución de alguna autoridad de protección de datos, cuando no sencillamente de una mistificación. Lo preocupante en esta materia no deriva tanto de un ejercicio de análisis, por lo demás perfectamente legítimo, cuanto de expresar un modo de entender la garantía las condiciones de tratamiento de datos de carácter personal. Se trata de un enfoque reactivo y me atrevería a decir que en ocasiones resignado. Y, sin embargo, en mi experiencia profesional, desde la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal hasta nuestros días este ha sido un interrogante permanente en cualquier proceso de formación. Y también en aquellos casos en los que se han ejercido funciones de consultoría y soporte al cumplimiento normativo en protección de datos.

Aunque en principio pueda parecer una manifestación positiva de compromiso con la aplicación de la legalidad vigente, lo cierto es que suele responder a otro tipo de intereses. En una parte significativa de las ocasiones quien formula la pregunta ya se encuentra tratando los datos. Y, de hecho, no es en absoluto inusual que las cuestiones relativas al conjunto de procesos que es necesario implementar de acuerdo con el Reglamento General de Protección de Datos se hayan descuidado significativamente. En el mejor de los casos, la consulta se acompaña con un modelo de consentimiento informado. La lista de ejemplos, que se podrían narrar en este artículo desbordaría con toda seguridad la extensión completa de Tecnología y Sentido Común. Así que permita al lector, que reproduzcamos ni uno sólo por una cuestión obvia de síntesis y eficiencia en la compartición de nuestras ideas.

Personalmente, y en primer lugar, la dichosa pregunta me genera incomodidad porque no es la cuestión correcta. En realidad, el primer proceso a la hora de decidir si se tratan datos de carácter personal, debería ser tan sencillo como el planteamiento de un juicio de oportunidad acompañado por una estructura organizativa clara y definida en cuanto a la atribución de funciones. Y es que “cualquiera” no puede preguntar en una organización si es legal tratar datos personales del mismo modo que “cualquiera” no se puede dedicar a la selección y contratación de personal. Porque, cuando eso sucede, no significa otra cosa que todos y cada uno de los integrantes de la entidad se sienten con plena libertad de tratar datos personales sin tener capacidad de decisión o competencia para ello y sin necesidad de sujetarse a proceso alguno.

CONTINÚA EN PRÓXIMA PÁGINA

En segundo lugar, este tipo de interrogantes suele ser un síntoma de que la organización ha perdido por completo el control de sus procesos de gestión en este ámbito. De hecho, existen un conjunto de cuestiones que deberían avanzarse en el tiempo al juicio de legalidad en materia de protección de datos. La lista sería larga, pero compartir alguna de ellas aportará luz a la propuesta. En el caso de que la consulta fuera formalizada por una persona con competencia para tomar decisiones en relación con la gestión de datos personales en la organización, la siguiente cuestión se referiría a un juicio de oportunidad. No basta con la voluntad de tratar datos personales, es necesario que se asignen un conjunto de recursos organizativos técnicos y presupuestarios sin los cuales el tratamiento no es viable. De hecho, en la mayor parte de las ocasiones el usuario, generalmente desinformado, preguntará respecto de un tratamiento que con toda probabilidad ya existe en el registro de actividades y cuenta con recursos asignados para su despliegue.

En caso contrario, es decir, cuando la cuestión no puede resolverse mediante la asignación de un perfil de usuario a un sistema de información preexistente, cabe preguntarse si el tratamiento propuesto se alinea y es funcional con los objetivos de negocio. Porque, en no pocas ocasiones, la propuesta responde a una mera ocurrencia. Incluso en el caso de que tratar datos fuese coherente y valioso desde el punto de vista de los objetivos de negocio sigue siendo necesario determinar si se contará con los recursos necesarios para el desarrollo del mismo. Unas veces será necesaria la adquisición de software, de hardware, o la contratación de servicios de terceros. En otras, el tratamiento deberá desarrollarse con recursos propios, lo cual incluye analistas, desarrolladores, capacidad de procesado y almacenamiento, la constitución de un equipo interdisciplinar y la definición de los requerimientos de seguridad y resiliencia de los sistemas de información.

En consecuencia, si la organización no se encuentra en condiciones de garantizar todos estos aspectos económicos, funcionales y organizativos carece de sentido realizar cualquier otra pregunta. Y cuando en su labor, el delegado de protección de datos alienta este tipo de consultas está causando perjuicios y costes innecesarios al responsable del tratamiento. Nunca las

indicaciones organizativas internas, ni tampoco cualquier guía o recomendación de las autoridades de protección de datos, puede prestar soporte a este tipo de conductas. Lo que primariamente define a un responsable es su capacidad de tomar decisiones, del mismo modo que un encargado del tratamiento debe definir con precisión su cartera de servicios y/o identificar las necesidades de las entidades que lo contratan.

Así que recuerden, ¡se lo ruego!, en la próxima ocasión en la que nos encontremos no me pregunten si es legal tratar datos. No me usen como ariete para imponer en su entidad un tratamiento que nadie pidió, que nadie solicitó y que, seguramente, nadie conocía. Se lo prometo, no les responderé. Diríjanse a su soporte en protección de datos exclusivamente cuando satisfechos todos los requerimientos organizativos internos para la toma de decisión se cuente con el aval de las personas con autoridad en la organización y con los recursos necesarios, no sólo para realizar el tratamiento, sino para ser capaces de cumplir con las obligaciones jurídicas que de él se deriven.

Mientras tanto, por favor absténganse de tratar datos, no nos hagan perder el tiempo y sobre todo no generen costes y deficiencias que además comportan un riesgo regulatorio que puede salir muy caro a su entidad en términos económicos y reputacionales.

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

Es el equipo....

Desde la llegada de la informática de usuario, es decir, desde el momento en el que en las organizaciones se pudo prescindir de procedimientos de programación complejos, han existido serias disfunciones a la hora de definir las condiciones para el tratamiento de datos de carácter personal. Usualmente el cumplimiento normativo en esta materia, tanto desde el punto de vista de la seguridad, como desde el punto de vista de legal de la legalidad se producía tradicionalmente ex post facto. Alguien había decidido que era conveniente tratar datos y cuando el proceso era particularmente sencillo y podía desplegarse mediante el recurso a la ofimática convencional: se trataban los datos. Posteriormente se regularizaba el tratamiento cuando se descubría su existencia, tras un proceso de formación, de una auditoría, o en el peor de los casos con motivo de un procedimiento sancionador.

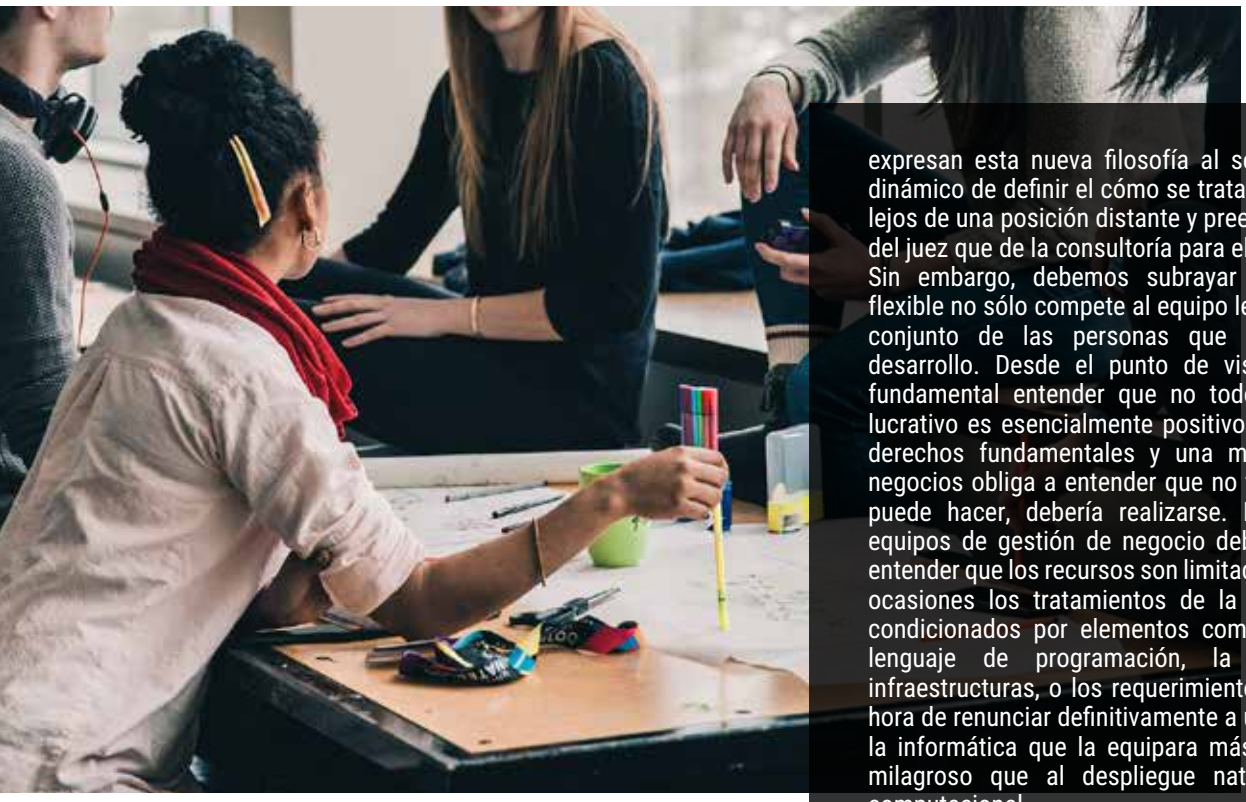
Existía otra metodología que trataba de incorporar un rudimentario pero incompleto modelo de gestión. Se trataba de aquellos supuestos en los que la necesidad de procesar datos adquiría una dimensión compleja que no estaba al alcance del personal que había decidido llevarlo a cabo. Usualmente se vinculaba a necesidades de gestión o actividades de marketing. En tales casos, los responsables acudían a aquellas unidades de negocio con capacidad para diseñar el sistema de información, o bien procedían a la contratación externa de empresas o de personas individuales con estas capacidades de desarrollo. De nuevo el conocimiento se encontraba parcialmente distribuido y no tenía porque necesariamente alcanzar ni a los responsables de la seguridad ni aquellos a los que se encomienda el cumplimiento normativo en materia de protección de datos. En aquellos casos en los que el proceso se completaba adecuadamente, no era en absoluto inusual que la última notificación se destinarse a las unidades que tienen encomendado el cumplimiento normativo.

Obviamente no resultaba en absoluto extraño que se detectasen en significativos incumplimientos o barreras que hacían materialmente imposible el desarrollo de la actividad tal y como se había planificado desde sus inicios.

La consecuencia directa de este estado de cosas no era otra que la existencia de una cierta anarquía en los sistemas de información, tanto desde el punto de vista de la gestión y organización de la empresa como desde el punto de vista de las medidas de seguridad. Y esto comportaba consecuencias generalmente indeseables. La primera de ellas, fruto del caos organizativo, no era otra que el despliegue de esfuerzos paralelos y redundantes, con la consiguiente pérdida de eficiencia en la administración de la información y de calidad de la misma. La segunda, la multiplicación de los incidentes de seguridad. La tercera, y obviamente la más indeseable, incurrir infracciones que en no pocas ocasiones eran objeto de investigación por las autoridades de protección de datos. Sin en el año 2023 la descripción de nuestro pasado sigue siendo actualidad en su organización tiene usted un serio problema. En nuestros tiempos, desde la más pequeña de las empresas al más complejo de los entornos el trabajo multidisciplinar, el trabajo en equipo resulta un requisito esencial.

En el primer caso, puede que usted piense que carece de necesitar soporte alguno, habida cuenta de que sus datos se encuentran en un servicio en la nube y todo el software que utiliza ha sido licenciado por un tercero experto en su área de negocio. Y, sin embargo, en los ordenadores de su pequeña empresa sigue existiendo ofimática. Sus colaboradores pueden seguir utilizando entornos no autorizados para el almacenamiento de información, y en el peor de los casos pueden estarse utilizando los datos, contraviniendo los principios más elementales de la seguridad o de la finalidad para la que se recogieron desde un punto de vista jurídico.

CONTINÚA EN PRÓXIMA PÁGINA



En los centros más complejos, la aplicación de los principios de protección de datos desde el diseño y por defecto impone ineludiblemente la generación de equipos multidisciplinares que iteran conjuntamente. Como hemos señalado reiteradamente en los artículos publicados en esta sección, la decisión de tratar un dato no es primariamente jurídica, sino organizativa y comporta la atribución de los recursos necesarios para un adecuado diseño e implementación del sistema de información del que se trate. Tomada esta decisión, resulta ineludible construir un equipo de trabajo que integre a aquellas personas que desde la perspectiva del negocio conocen las necesidades del tratamiento con aquellas que cuenten con la capacidad de soportar el diseño e implementación del sistema, junto con la adopción de las medidas de seguridad necesarias en todos los niveles.

Se trata de un trabajo dinámico y altamente creativo que comporta una necesaria flexibilidad del conjunto del equipo. Hemos dedicado muchas líneas en esta publicación a señalar el ineludible cambio de actitud de los equipos jurídicos que deben entender su función de servicio y adoptar nuevas metodologías que suponen cambios significativos en los patrones de conducta usuales. Palabras como “compliance” o “legaltech”

expresan esta nueva filosofía al servicio de un modo dinámico de definir el cómo se tratarán los datos, y muy lejos de una posición distante y preeminente más propia del juez que de la consultoría para el desarrollo.
Sin embargo, debemos subrayar que este enfoque flexible no sólo compete al equipo legal, sino también al conjunto de las personas que se integran en el desarrollo. Desde el punto de vista de negocio, es fundamental entender que no todo fin beneficioso o lucrativo es esencialmente positivo. La garantía de los derechos fundamentales y una mínima ética de los negocios obliga a entender que no todo aquello que se puede hacer, debería realizarse. Por otra parte, los equipos de gestión de negocio deben ser capaces de entender que los recursos son limitados y que en muchas ocasiones los tratamientos de la información vienen condicionados por elementos como la naturaleza del lenguaje de programación, la disponibilidad de infraestructuras, o los requerimientos de seguridad. Es hora de renunciar definitivamente a un entendimiento de la informática que la equipara más a la magia y a lo milagroso que al despliegue natural de la ciencia computacional.

Por su parte, los equipos de tecnología de la información deben pertrecharse de un conocimiento jurídico y ético básico que les capacite para entender cuáles son los límites que no deberían poder ser traspasados. Y, en este enfoque basado en metodologías de protección de datos desde el diseño y por defecto deben interiorizar que, en la medida en que su código definirá las condiciones de cumplimiento, una parte que sus tareas es materialmente normativa. Por otro lado, deben ponerse en el lugar del cliente y del usuario de los sistemas de información. En más de una ocasión, el problema de seguridad o de cumplimiento normativo deriva más de un programador que decidió hacer las cosas de acuerdo con su enfoque de conocimiento altamente especializado. Y el resultado no es otro que programar un sistema de información utilizado por personas que carecen de sus altas capacidades en esta materia y que, por tanto, cuanto más complejo es el entorno mayor riesgo de incumplimiento existirá.

Alcanzar la virtud comporta siempre esfuerzo, sacrificio y dedicación. Pero, y debo insistir, si en 2023 estas lecciones no han sido aprendidas su organización tiene un serio problema

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

El equipo directivo un riesgo para la seguridad

Primero fue Hillary Clinton, a la que afectó significativamente en campaña electoral el haber enviado mensajes institucionales a través de cuentas de Gmail. Después Donald Trump que creó una oficina paralela en una instalación puramente privada y no devolvió la documentación de inteligencia al final de su mandato. Y ahora, parece que, debido a la senectud, el presidente de los Estados Unidos tampoco recuerda haber sacado documentos de un entorno seguro y haberlos olvidado en determinados despachos durante su vicepresidencia. El único elemento diferencial que probablemente presentan estas noticias con la realidad española consiste en que, en Estados Unidos, cuando estos hechos son conocidos la fiscalía inicia actuaciones que podrían acabar en un procedimiento en el que se exija responsabilidad penal al político o al directivo.

Pero la cuestión de fondo es la misma y obliga a formular una pregunta particularmente incómoda: ¿es que quien ocupa la posición de consejero/a delegado/a, una concejalía, una alcaldía, una consejería o presidencia autonómica, o la presidencia del Gobierno, no son usuarios de sistemas de información?; ¿poseen estas personas algún derecho que se nos escape al resto de la humanidad a manejar la información a su libre albedrío y sin garantías de seguridad? La respuesta es absolutamente obvia. Bajo cualquier punto de vista jurídico, material, organizativo, o técnico, no sólo son usuarios de un sistema de información, sino que son puntos particularmente críticos desde el punto de vista de las amenazas y de las vulnerabilidades.

Y, sin embargo, no es demasiado aventurado afirmar que con carácter bastante usual en nuestras administraciones, y quien sabe hasta qué punto en el sector privado, al jefe no se le obliga a ir a un curso de formación en materia de privacidad, seguridad y confidencialidad. Apostaría, -aunque juro que nada me apetecería más que perder lo apostado-, que las personas delegadas de protección de datos, y responsables de seguridad en muy pocos casos podrán exhibir en nuestro país un documento firmado en el que un alto responsable en la gestión o en la política de las organizaciones haya asumido que conoce, respeta y aplica las obligaciones de seguridad que emanan del Reglamento General de Protección de Datos, del Esquema Nacional de Seguridad y, permítanme decirlo con crudeza, del más elemental sentido común.

CONTINÚA EN PRÓXIMA PÁGINA

Por ello, porque tal vez sería conveniente no tener razón, hay que reivindicar el papel que, en protección de datos y seguridad debe atribuirse a la formación. El estado óptimo sería aquel en que tras el nombramiento y toma de posesión el alto responsable asiste a un acto formativo destinado a inculcar los principios básicos de actuación de la organización desde distintas perspectivas. No estoy proponiendo que estos responsables vayan a clase, no consiste nuestra apuesta en convertir la seguridad en una pesada carga que reste operatividad y dedicación a estas personas. Se trata de encontrar un modelo de formación enfocado a la particular posición de estos directivos. Y a nuestro juicio, existen varios componentes esenciales.

En primer lugar, vaya por delante, que nada más ineficiente que diseñar cursos de derecho para estos perfiles. Y desde luego, esta recomendación no se debe a cuestionar su capacidad de atención y aprendizaje. Sencillamente, salvo en puestos muy concretos, no es su rol en la organización tener un conocimiento profundo del marco jurídico. El primer componente esencial consiste en proporcionar al directivo o a la directiva una visión estratégica que ponga en valor como los componentes de seguridad y protección de datos resultan esenciales para el funcionamiento ordinario de su organización, constituyen un pilar crucial para la transformación digital, y estarán siempre presentes en cualquier proceso de innovación, cambio, o emprendimiento. Se trata por tanto de poner en su justo contexto en términos de valor cuantitativo y cualitativo estos dos elementos cruciales para garantizar la seguridad de la información. En segundo lugar, estos las personas con responsabilidades de dirección deberían recibir exactamente la misma formación e información que cualquier usuario de los sistemas de información a los que se encuentren vinculados.

Existe un tercer componente que ha sido puesto de manifiesto por los ejemplos de los políticos norteamericanos a los que hacíamos alusión. Si en los dos primeros pilares la interacción y el diálogo con los usuarios es fundamental, en el tercero que voy a proponer resulta ineludible. A diferencia de los colaboradores o trabajadores de una organización que cumple con sus tareas en el horario establecido y a los que la legislación reconoce el derecho a la desconexión digital, el personal de alta dirección suele mantener una dedicación intensa a la organización. Por otra parte, ello implica que no sea inusual ni la dedicación hasta altas horas de la noche o durante el fin de semana en condiciones de teletrabajo.
Ello comporta necesariamente una movilidad que no suele afectar a otros puestos. Por ello, resulta esencial conocer cuáles son las condiciones en las que se desempeñará la tarea, cuáles son los hábitos de estas personas, para trata de dibujar o de diseñar un traje a medida. Ciertamente es más sencillo afirmar o comunicar las obligaciones relativas al deber de manejar los sistemas de información desde el entorno de trabajo sin complicarse la vida. Pero lo cierto es que la gestión de los puestos de alta dirección por su propia naturaleza es complicada y requiere de un esfuerzo de adaptación. Por supuesto, no estamos proponiendo aquí que, como en el caso del presidente Trump o de Hillary Clinton, uno pueda hacer cosas que no debería hacer. Lo que se propone es adaptar nuestra estrategia en materia de seguridad a condiciones razonables para el desempeño de tareas de la alta dirección, que a su vez se puedan producir en condiciones de garantía suficiente.

Es evidente, que con una estrategia centrada y eficiente en materia de alta dirección no sólo evitaremos el riesgo para la reputación de la compañía o la administración sino que aseguraremos la protección de activos muchas veces vitales para el futuro de las organizaciones.

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

Cuidado con el WhatsApp...

En los últimos meses, la Agencia Española de Protección de Datos ha sorprendido a la comunidad de expertos dictando dos resoluciones contradictorias en materia de uso de WhatsApp en el marco de las relaciones laborales. En la primera de ellas, la más extensa y documentada, la autoridad de protección de datos considera que infringe el reglamento general de protección de datos la imposición de la obligación de utilizar esta mensajería en el contexto de un sistema de doble validación para el acceso a una base de datos. Se trataba, en este caso de una policía local que había implementado un software de gestión para el desempeño de sus funciones y que siguiendo las directrices del CCN proponía una autenticación en dos pasos para el cumplimiento y ejecución del Esquema Nacional de Seguridad. El primero de ellos se basaba en una metodología tradicional, esto es un usuario y una contraseña (algo que se sabe), mientras que el segundo partía de la existencia de algo que se tiene, esto es un terminal móvil al que se puede enviar un código pin generado para el inicio de sesión de modo que se singularice y asegure la identidad de del usuario que accede al sistema.

En el segundo caso, el uso era más simple. Se había informado al trabajador con carácter previo del uso de WhatsApp para comunicarse con el mismo. Sorprendentemente, a diferencia de lo decidido en el primer caso, al que ahora nos referiremos, la AEPD consideró que el uso era procedente. Volviendo al primer supuesto, la AEPD es particularmente contundente en unas conclusiones que desarrolla de modo particularmente prolijo a lo largo de su resolución. En esencia, puede concluirse que la autoridad española considera que el número telefónico, y podríamos decir que, por extensión, el smartphone particular, se integran en la esfera de vida privada que la normativa protege al trabajador. Por tanto, usar este número en un espacio de comunicación presenta severos problemas desde el punto de vista de la legitimación para el tratamiento. En esencia, no es viable basar estos tratamientos en el consentimiento del trabajador en la medida en la que, como bien señalaron las Directrices sobre el consentimiento del Comité Europeo de Protección de Datos, es prácticamente imposible asegurar la existencia de una libre manifestación de voluntad en la esfera de las relaciones laborales. Sin embargo, en la segunda de las resoluciones, la autoridad no ve inconveniente alguno en este uso.

Con independencia del criterio adoptado por el regulador, creo que es conveniente desarrollar un profundo análisis de riesgos a la hora de decidir el uso de un servicio de mensajería privada como canal de comunicación con nuestros empleados y colaboradores. Debemos tener en cuenta antes de tomar una decisión de esta naturaleza una serie de cuestiones que a nuestro juicio, resultan relevantes, incluso más allá de la garantía del derecho fundamental a la protección de datos. Aunque sin duda, podríamos comenzar por este ámbito, esto es, por la atribución legal de una serie de derechos aquellas personas que despliegan una relación laboral, y me atrevería a decir también que de prestación de servicios con nuestras organizaciones. La Constitución Española reconoce en su artículo 18 un conjunto de derechos que pueden ser vulnerados consciente o inconscientemente por el uso de estos medios. Así, en nuestro Estatuto de los Trabajadores se garantiza el derecho a la esfera privada y a la dignidad de la persona del trabajador. Más allá de la protección de datos, la utilización de servicios de mensajería puede repercutir sobre los derechos del artículo 18.1 de la Constitución, singularmente sobre la intimidad personal y familiar, el honor, y quien sabe si en circunstancias excepcionales, el derecho a la inviolabilidad del domicilio.

Señalamos estos riesgos en la medida en la que un terminal telefónico como en reiteradas ocasiones ha expresado nuestro Tribunal Constitucional, es un espacio de privacidad sobre el que descansan todos estos derechos. En estas mensajerías, salvo que el trabajador limite o bloquee el acceso a su perfil y/o a sus estados estaría revelando, aspectos muy personales o de otros familiares en las fotos de su perfil o su estado emocional en un momento determinado. Ninguna de estas informaciones debería ser accesible jamás para el empleador ni para ningún tercero en el ámbito laboral. De

modo, que se estaría cargando sobre el trabajador no sólo el deber de soportar el uso de este tipo de medios en un terminal de su propiedad, sino que además se le impondría la tensión emocional de estar permanentemente controlando cual sea la configuración de esa concreta mensajería. Y jamás podría evitar el riesgo de que tras una actualización del software esta información personal fuera compartida. Y con ello, un riesgo de infracción del ordenamiento jurídico por parte de la empresa.

Por otra parte, las video-llamadas con estas con estos medios que no hayan sido debidamente reguladas y estandarizadas podrían suponer un visionado del interior de un domicilio. Si bien no consideramos este escenario una violación o una ruptura del derecho a la inviolabilidad de la morada, no deja de resultar ciertamente impactante desde el punto de vista de la protección de la vida privada de las personas. Decían los juristas norteamericanos, que resulta difícil definir qué cosa sea la privacidad, pero también que un juez la reconoce en cuanto se la encuentra de cara. Sirva esta expresión para subrayar que, aunque la AEPD haya parecido avalar el uso de estas mensajerías, nada impide a un juez de lo social, o de lo civil, reconocer la existencia de una afectación a los derechos del artículo 18.1 CE, con las consabidas consecuencias para la empresa.

CONTINÚA EN PRÓXIMA PÁGINA

No debemos olvidar aquí que existe una repercusión ulterior. Si la empresa no es capaz de dimensionar adecuadamente el uso de estos canales puede incurrir en riesgos adicionales. El primero de ellos, consistiría en la infracción del deber de garantizar el derecho a la desconexión digital del trabajador.

Por mucho que se quiera, incluso aunque la entidad haya prohibido la consulta del canal fuera de horas de trabajo, lo cierto es que cualquier mensajito que entre, cualquier y ruidito que el trabajador escuche lo pondrá en alerta, le alterará emocionalmente, le hará pensar en una potencial urgencia y seguramente determinará una lectura del mensaje y quien sabe si una respuesta. Y día a día, cada una de esas acciones, irá dejando una prueba indeleble que sustentará sin ningún género de dudas, la correspondiente demanda por los daños causados por infracción del deber de garantizar la dignidad del trabajador y su espacio de vida privada y de conciliación familiar fuera de las horas de trabajo. Además, estos canales lejos de ser exclusivamente un entorno profesional son muy proclives al ejercicio con partición de opiniones, bromas, chistes, chascarrillos que en no pocas ocasiones definen situaciones embarazosas que afectan gravemente a la reputación empresarial cuando alcanzan los medios de comunicación. Otro riesgo que desde luego se debería considerar.

Un segundo bloque de riesgos es el que deriva de la propia naturaleza de este tipo de herramientas. Noa retrotraen de nuevo al viejo debate sobre el Bring Your Own Device (BYOD) y presentan muy diversas aristas. En primer lugar, cuando la mensajería opera con el número privado del trabajador supone la posibilidad de compartir información estratégica de la empresa en un terminal privado respecto del cual nadie garantiza que resulte accesible en el entorno familiar. Es un smartphone que se usa 24 horas al día siete días a la semana en cualquier esfera de la vida privada del trabajador y, por tanto, susceptible de riesgos como las pérdidas o el acceso accidental por terceros no autorizados. Es decir, un canal por el cual circula información estratégica de la compañía, a veces, archivos y documentos, estarían circulando por entornos altamente lábiles, escasamente controlados, y susceptibles de pérdidas significativas de información. Por otra parte, en relación con una cuestión que acabamos de señalar, se trata de un entorno que permite revelar información a terceros sin dejar prueba. Un canal abierto a que información significativa que pueda afectar a la reputación empresarial llegue a los medios de comunicación o a la competencia. Por otra parte, la definición de reglas de uso precisas resulta particularmente relevante. Hemos conocido por los medios de comunicación como a través de estas mensajerías se han podido estar compartiendo comentarios relativos a las capacidades de niños en entornos escolares, fotografías de pacientes, o informaciones confidenciales en el marco de la gestión policial cuando no directamente apelando a la rebelión contra el Estado constitucional.

Aunque la AEPD no entre absoluto en su resolución, no es infrecuente en el contexto de la PYME española que se utilicen como recurso mensajerías privadas en sus versiones libres de pago, esto es, sin ninguna de las garantías, ni compromisos que el Reglamento General de Protección de Datos impone al proveedor. Cuando se dan estas circunstancias, esto es, el empleo de un medio propio del trabajador, el uso de una de un servicio no contratado, y la carencia de unas mínimas reglas de conducta y seguridad estamos en condiciones de de afirmar que en lugar de invertir en un medio de comunicación empresarial de algún modo estamos diseñando y programando una bomba de relojería. En consecuencia, parece evidente que la única solución funcional para alcanzar resultados suficientes en la comunicación interpersonal a través de terminales móviles con los empleados debería basarse en el empleo de los terminales proporcionados por la compañía, con software específicamente licenciado y seguro, y con unas reglas claras de uso, así como con una definición precisa de las obligaciones de seguridad.

Es posible, que la autoridad de protección de datos haya exonerado a una pequeña compañía de responsabilidad para dar instrucciones a sus mensajeros a través de WhatsApp. Les rogaría que no confundan la anécdota con la categoría, que

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

Canales de denuncias internas: protección de datos desde el diseño y por defecto

La Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción plantea un plazo de tres meses a contar desde el 21 de febrero de 2023 para la implementación de canales de denuncias internas. Este es un reto significativo para las organizaciones públicas y privadas que sin duda va a contribuir a la mejora de las condiciones de gobernanza y a la reputación de nuestro sector público y privado. Se trata de la transposición de una directiva europea, que busca garantizar condiciones de gestión de las organizaciones que prevengan cualquier atisbo de la corrupción o mala praxis, que en el pasado demostraron ser capaces de poner en jaque nuestras democracias e incluso de generar amenazas sistémicas para nuestra economía. Precisamente por ello los retos que deben afrontar quienes diseñan estos canales son particularmente relevantes. En este artículo nos referiremos a algunos de ellos.

UN SISTEMA DIFERENCIADO

La regulación ordena disponer de un sistema de información claramente diferenciado, con una atribución de responsabilidades muy precisas. Debe ser capaz de incorporar denuncias o notificaciones, tanto escritas como orales en un entorno bajo la responsabilidad del órgano de gobierno, que debe garantizar la completa indemnidad, tanto de las personas que presentan una comunicación, como de las que resulten mencionadas en la misma. Ello implica sin duda una un conjunto de decisiones de naturaleza organizativa de un lado, pero también desde un punto de vista tecnológico. Por ello, un buen diseño será aquel que conociendo las condiciones internas de la organización y el modo más eficiente de gestionar la información dote de singularidad específica al recurso como sistema claramente independiente desde el punto de vista de su conformación tecnológica. Deberá asegurarse que las personas a cargo de su gestión asumen de modo adecuado su responsabilidad, con un perfil de funciones claramente establecido y un conjunto de garantías de acción muy precisas, entre las que la trazabilidad en el uso podría ser crucial.

EL ENCARGADO DEL TRATAMIENTO

Del mismo modo que ha sucedido en prevención de riesgos laborales, es posible acudir a entidades externas para el desarrollo de esta actividad. Aquí debemos ser particularmente exigentes. El artículo 28 del RGPD obliga a ser diligentes en la elección del encargado del tratamiento. Este debe ofrecer las suficientes garantías en relación con el cumplimiento normativo. A mi juicio, no bastará con una oferta de garantías enmarcadas en relación con el cumplimiento del artículo 28. Siempre se ha defendido una aproximación a la interpretación de la normativa de protección de datos con un enfoque de 360°. Desde una interpretación sistemática del ordenamiento jurídico los proveedores de servicios en este ámbito deben incorporar el conjunto de garantías de protección de la información y de los informantes que define la nueva Ley. Deberían rechazarse las ofertas de servicios sin garantías adecuadas y que no incluyan en la definición de su servicio opciones un compromiso claro de certificación o auditoría regular y externa de sus sistemas de información.

EL ANONIMATO

Puesto que se permite tomar la decisión de permitir la presentación de información de forma anónima o bien a través de sistemas de seudonimización, debemos tener en cuenta la particular exigencia que ambos elementos implican. El anonimato, desde el punto de vista de la concepción del RGPD y de las autoridades de protección de datos, se caracteriza por su irreversibilidad y el responsable del tratamiento debe asegurar la exclusión de cualquier riesgo de reidentificación por singularización, inferencia o vinculación. Es más, no basta con ello debe tener en cuenta el estado del arte y las previsiones del avance futuro de la tecnología. En este caso no se trata de anonimizar datos personales, sino de garantizar en origen que dichos estos no existirán. Esto posee una cierta trascendencia ya que por ejemplo en el acceso a sistemas de información online, las cookies, la trazabilidad de IP o de dirección MAC puede ser determinante a la hora de establecer la identidad de un sujeto. En particular, cuando la denuncia se formule desde un terminal vinculado al sistema de información de la entidad. Pero no basta, en ocasiones la información incorpora referencias que ineludiblemente pueden permitir identificar a la persona denunciante. Por ello los gestores del sistema, deben revisar la información escrita u oral a la búsqueda de posibles elementos que permitieran eventualmente identificar a la persona denunciante.

Por otra parte, se plantea la seudonimización como modelo de gestión a las denuncias de las denuncias presentadas por personas que se identifican. En este sentido, la norma hace referencia a la atribución de un código de identificación a cada expediente. En cualquier caso, si la seudonimización debe operar como una barrera que permita establecer un vínculo entre el contenido de la información y la persona que la facilitado, todas nuestras observaciones en relación con el anonimato y el modelo de gestión son pertinentes y relevantes y deberían aplicarse.

CONTINÚA EN PRÓXIMA PÁGINA

TRANSPARENCIA

El principio de trasparencia psee aquí un valor fundamental y va más allá del mero cumplimiento del RGPD. El Comité Europeo de Protección de Datos ha subrayado que para una adecuada la perfecta comprensión de las condiciones e implicaciones del tratamiento no basta con cumplir de modo formal los artículos 12 y 13 del RGPD. Es necesario ofrecer una información suficiente que permita a la persona interesada entender las condiciones específicas del tratamiento, las implicaciones de éste y las consecuencias que eventualmente podrían derivarse para sus derechos. A nuestro juicio, ello implica un esfuerzo adicional, incluyendo una sección que de modo muy gráfico ofrezca la persona denunciante una comprensión clara de las condiciones en las que será tratada su información. Particularmente, en aquellos casos, en el que el canal de denuncia, no siendo completamente anónimo, prevea la posible cesión de los datos, a requerimiento de la autoridad judicial en los términos que establece la propia ley. Finalmente, un elemento relevante desde el punto de vista de la transparencia consiste en mantener informado no sólo la plantilla sino la representación sindical a través de los órganos que existan.

EXCEPCIONES A LOS DERECHOS

Como es lógico la protección de la investigación ha obligado legislador a establecer excepciones a los derechos. Estas son particularmente robustas, la que se refiere al derecho de oposición al tratamiento, cuya denegación prácticamente se presume y por ello es conveniente dotar de trazabilidad estos procesos. La aplicación del principio de responsabilidad proactiva obliga a documentar de modo muy preciso el alcance de las limitaciones a los derechos y de las garantías para evitar accesos o transferencias ilícitos o abusivos. Es fundamental establecer de modo muy preciso, las finalidades y categorías de datos que se van a tratar, el alcance de las limitaciones que se establezcan, las garantías que se implementan los plazos de conservación, los riesgos para los derechos y libertades y las condiciones bajo las cuales establecen excepciones a los derechos.

MINIMIZACIÓN DE DATOS, CONSERVACIÓN Y BLOQUEO DE LOS DATOS

Desde el punto de vista de la gestión ordinaria de los datos es importante ser capaz de establecer cuáles van a ser los datos estrictamente necesarios para promover la investigación de las conductas denunciadas. Ello implica una especial diligencia a la hora de definir qué datos merecen la pena ser conservados y cuáles no y afecta de modo particularmente relevante a la cualificación de los gestores del sistema de información. El principio de minimización, de ser aplicado por personas que carezcan de la formación adecuada podría acabar eliminando informaciones muy relevantes o, por el contrario, la conservación de datos excesivos podría generar no sólo ruido informativo sino riesgos adicionales como por ejemplo la potencial reidentificación de la persona denunciante.

Por otra parte, la supresión o bloqueo de la información resulta particularmente complicada en esta norma ya que se trata de una obligación de contenido cualitativo. Debemos definir “el tiempo imprescindible” para decidir sobre la procedencia de iniciar una investigación con un límite de tres meses. Otro criterio de supresión tiene que ver con la veracidad o no de la información. Cuando esta no sea veraz deberá procederse su inmediata supresión, salvo que se pudiera constatar la presencia de un ilícito penal y por el tiempo necesario para el trámite del procedimiento judicial. No obstante, cabe disponer de un plazo de conservación, no sólo por razones de tramitación sino también cuando se tenga por finalidad verificar el funcionamiento del sistema

Estas breves pinceladas demuestran que la gestión de canales de denuncias internas plantea retos estratégicos desde el diseño que no pueden ser obviarse en la medida en la que el funcionamiento adecuado de los mismos es altamente dependiente no sólo del cumplimiento de la normativa de protección de datos, sino de un entendimiento funcional de los valores que aporta la protección de datos desde el diseño y por defecto.

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.

A propósito de las prisas para la Inteligencia Artificial

Dos acontecimientos han sacudido el horizonte de la protección de datos personales en los últimos meses. En primer lugar, la investigación norteamericana a Tik-Tok, siguiente affaire en la linea de sucesión del asunto Huawei y la carta abierta solicitando la suspensión del desarrollo de la inteligencia artificial durante un periodo de seis meses. Uno y otro acontecimiento guardan un nexo común. Deberíamos preguntarnos qué grado de cumplimiento normativo y ético hace confiable una tecnología.

En el primer caso, se realiza una inferencia lógica, aunque no necesariamente demostrada o demostrable: si existe un riesgo de cualquier naturaleza en la provisión de un servicio de la sociedad de la información este debe ser auditado o analizado. En un mercado global los riesgos no sólo derivan del diseño y funcionamiento de las tecnologías de la información también es necesario valorar el riesgo geopolítico. Seamos sinceros, ¿almacenaría Vd. sus datos en una nube físicamente ubicada en un país política o socialmente inestable? La respuesta, por obvia, no merece ser escrita.

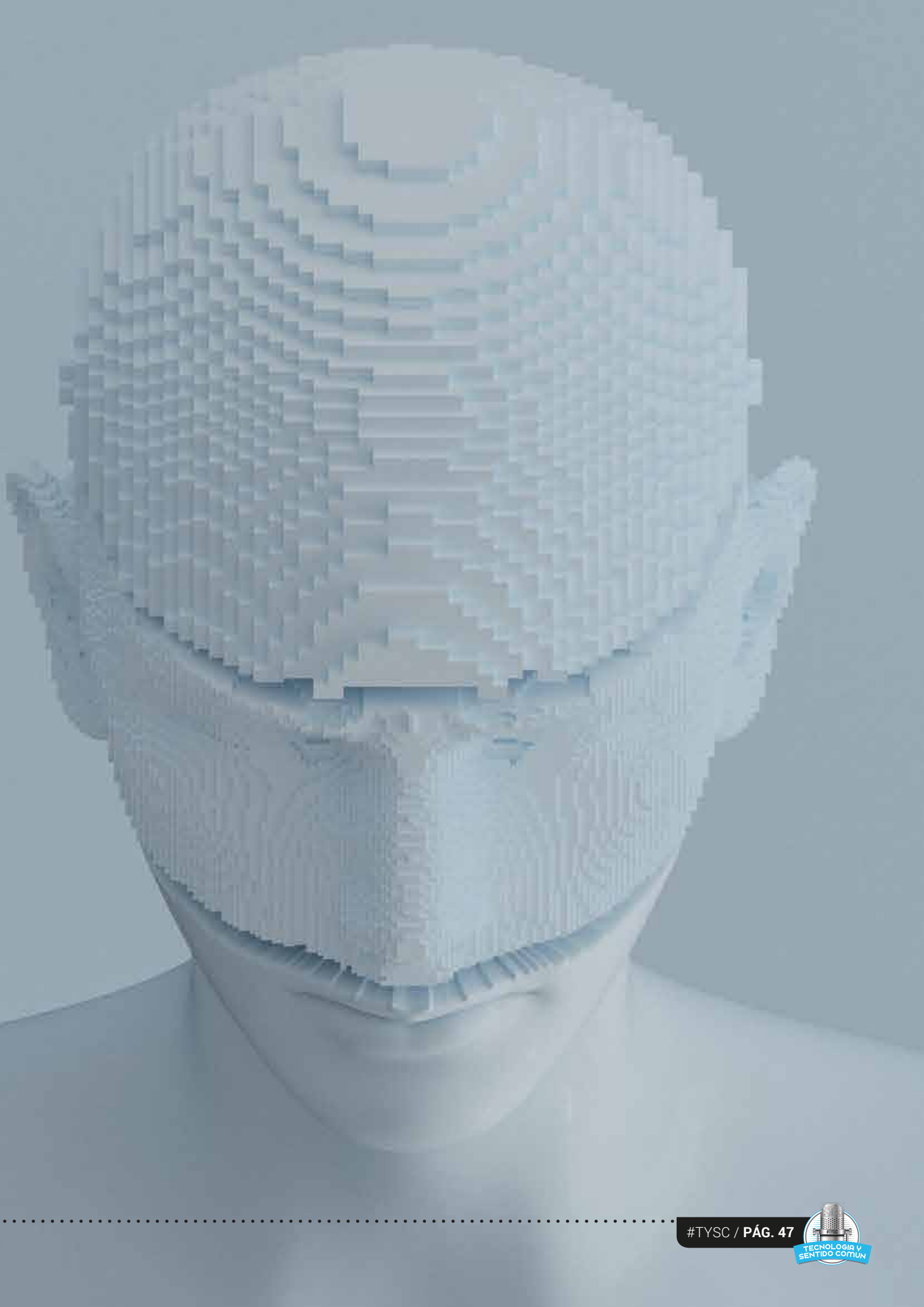
Los hechos demuestran la existencia de otro tipo de inestabilidad: el riesgo geopolítico. Los expertos en seguridad vienen advirtiendo desde hace años sobre los escenarios de riesgo asociados a las estrategias de ciberguerra. Y en este ámbito los hechos demuestran que no sólo hay que pensar en infraestructuras críticas. Ciertamente sui una compañía se posiciona en un mercado estratégico, como el de la provisión de tecnologías de red o el de infraestructuras críticas para los sistemas de salud debería estar sujeta a controles muy estrictos. También las nacionales, le patriotismo no tiene porque generar automáticamente confianza.

Por otra parte, el asunto Pegasus demostró sobradamente las vulnerabilidades de un smartphone. Y es evidente, que la aplicación más anodina del mundo, la más banal, la más infantil puede ser una puerta de entrada. Es más, los hechos muestran que las personas que pueden ser un objetivo en la infraestructura estratégica de defensa de un Estado se cuentan por miles. Si además el aplicativo, por si mismo puede ser un vehículo idóneo para la desinformación y la manipulación social todas las alertas deben estar encendidas.

En uno u otro caso, la comparecencia parlamentaria y la investigación pública pueden parecer una exageración, afectan a la reputación de las empresas y hacen crecer la desconfianza social. Por ello, este tipo de acción debería reservarse para casos muy claros y bajo condiciones muy precisas. Lo cual no impide que se tratase incluso de controles rutinarios. Por otra parte, lo que el sentido común indica es que la monitorización del riesgo es sistemática y sostenida en el tiempo. Y aunque el riesgo no lo genere la compañía o el producto, sino la legislación del país de origen o las malas prácticas de terceros, ello no excluye en absoluto una permanente atención.

El otro gran asunto en todos los medios de comunicación fue la alerta roja lanzada mediante carta abierta sobre los riesgos que la inteligencia artificial plantea para el futuro de la humanidad. No es algo con lo que se pueda o deba bromear, pero lo cierto es que la llegada de una IA de propósito general, amplias capacidades y autonomía decisional plena, está por llegar. Mientras esto ocurre la apertura de GPT4 ha maravillado y aterrado a partes iguales a la sociedad, a los expertos y a los políticos. Para un lego, los resultados que ofrece la máquina se acercan a la magia. Pero en realidad lo único que muestra es su capacidad para generar textos con un lenguaje coherente. De hecho,

CONTINÚA EN PRÓXIMA PÁGINA



mientras se escriben estas líneas se aprecia un cambio estratégico dirigido a no permitir ciertos usos como la realización de currículums o biografías sin aportación directa de datos. E incluso así, cuando se le propone leer una CV real desde un enlace el sistema decide que "el enlace proporcionado pertenece a Rafael Martínez Tomás, quien es profesor titular de Matemáticas en la Universidad de Valencia en España".

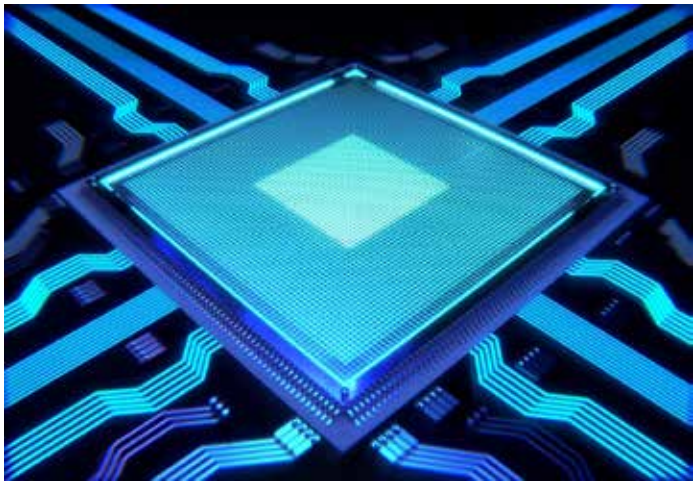
Al margen de anécdotas GPT4 demuestra muy interesantes habilidades en la traducción de textos, en la generación de notas de prensa, en la redacción de contratos básicos o en el desarrollo de trabajos académicos. Aparte de mostrar una coherencia significativa cuando se decide "hablar con él". Y tal vez esta, sea la cuestión que despierte nuestra inquietud al percibir que nos encontramos en esa delicada frontera en que podríamos no saber si nos relacionamos con una persona o una máquina o no distinguir imágenes falsas de reales.

La respuesta en este segundo caso ha sido particularmente controvertida. De un lado, se solicita una moratoria en el desarrollo tecnológico. De otro, se afirma por no pocas voces que plantearse esta idea ralentiza la investigación, nos limita y únicamente favorece el diseño de la geopolítica y la economía China. Al margen de este debate, pueden obtenerse e inferirse ciertas lecciones comunes a uno y otro caso:

1.-La gestión del riesgo reputacional es muy relevante. Cualquier estrategia empresarial o del sector público dependiente de o basada en la inteligencia artificial debe integrar políticas de cumplimiento normativo y ético y generar la confianza de la sociedad.

2.-Las empresas, y los emprendedores deberían aprender que no todo vale, y deberían invertir en madurar su conocimiento experto en materia legal y ética.

3.-Las autoridades independientes no dejarán de hacer su papel es más lo intensificarán. Ello implica que crece el riesgo regulador en ámbitos como la protección de datos, la competencia, la propiedad intelectual e industrial y en el futuro en el desempeño de las futuras agencias de IA. En mi opinión, han perdido en los últimos años oportunidades cruciales para nuestros derechos, nuestra sociedad y nuestra economía. Por muy brillante que sea, la aproximación Top Down no es ninguna buena idea.



Pongamos un ejemplo altamente esclarecedor. Los documentos generados por la Agencia Española de Protección de Datos sobre Inteligencia Artificial, tanto desde las recomendaciones de diseño como sobre criterios de auditoría, son sencillamente excelentes. Sin embargo, son sectorialmente percibidos como un estándar de imposible cumplimiento. Y ello se debe a dos razones esenciales. La primera, el hecho de que desde fuera no se haya percibido como un documento colaborativo, abierto a los sectores. La segunda, deriva de lo obvio. Ante la falta de recursos, la labor pedagógica, la que enseña el qué, el porqué y el cómo hacer las cosas no existe y, por tanto, el documento cae en el vacío en un ecosistema de PYMEs que no pueden digerir este nivel de complejidad.

4.-El legislador es lento y vive inmerso en una burbuja de garantías. Y esto sería excelente si eliminamos precisamente la "burbuja", la barrera invisible que exige ir más allá y entender la realidad. Basta con leer la Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el Espacio Europeo de Datos Sanitarios para apreciar que quien la escribió no ha construido jamás un repositorio de datos de salud. Porque si lo hubiera hecho sabría que las personas delegadas de protección de datos en toda la Unión Europea los vetan habida cuenta de que el Comité Europeo de Protección de Datos desde 2014 les ha comunicado que la anonimización irreversible es sencillamente inviable.

5.-O empezamos de modo urgente a diseñar un modelo tan garantista como viable para nuestra transformación digital o perderemos una carrera que merece la pena ganar.
La Inteligencia Artificial, así con mayúsculas, promete a la vez utopía y distopía, pero como cualquier creación humana depende de nuestras decisiones. Tomemos las correctas.

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

Una legislatura que comienza

Honestidad obliga, y por ello debemos confesar que este artículo se escribe en el mes de abril, para ser exactos un sábado día 15 de abril, cuando la campaña electoral todavía no ha empezado y cuando con carácter general se desconocen las previsiones y estrategias políticas que van a seguir nuestros ayuntamientos y comunidades autónomas después de la toma de posesión y la constitución de gobiernos y corporaciones tras las elecciones de finales de mayo. Esto nos permite pronunciarnos libremente, y manifestar nuestra opinión, sin ningún tipo de apriorismo o condicionamiento.

Nos jugamos mucho en la legislatura que comienza. Usualmente solemos poner el foco y centrar nuestra atención en las grandes cuestiones de política general y estatal. No hay ninguna duda que los planes estratégicos del Gobierno central en materia de transformación digital e inteligencia artificial poseen una enorme relevancia. Sin embargo, es en el territorio de lo autonómico y local donde se ejecutan la mayor parte de políticas públicas que repercuten de modo sustancial en la vida de todas las personas. Nos referimos a la sanidad, la educación, las políticas de bienestar y también a un conjunto de actuaciones de la Administración dirigidas a fomentar la investigación, la innovación, la transferencia de resultados y la iniciativa empresarial. Por otra parte, es en el territorio de lo local, donde nacen las jóvenes iniciativas empresariales que se vertebran en torno a incubadoras, polos de investigación universitaria, y ecosistemas específicos de innovación y emprendimiento de carácter privado o mediante los incentivos que promueve o que provee la administración pública.

Por eso resulta esencial asegurar que las agendas de nuestras administraciones autonómicas y locales, han incorporado de modo definitivo y profundo la transformación digital. Sin ánimo de ser agoreros, no podemos olvidar la experiencia y la historia reciente de nuestras instituciones. A nadie se le escapa que las sucesivas capas de transformación digital de la Administración se saldaron al menos en el corto plazo con sonoros fracasos.

Estoy refiriendo con esto a la sucesiva legislación que trató de crear una administración electrónica al servicio de la ciudadanía. La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos nunca se llegó a aplicar plenamente, y su sucesora la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, estuvo salpimentada de constantes ampliaciones de plazos para conseguir la completa implantación digital. Y mientras escribimos estas líneas, siguen conociéndose significativos problemas a la hora de ser eficientes, accesibles y usables para la administración. Lo cual tiene una

CONTINÚA EN LA PRÓXIMA PÁGINA

particular incidencia en las políticas públicas propias del Estado social que no acaban de alcanzar al 100% de sus destinatarios, personas precisamente caracterizadas por ser las primeras víctimas de la brecha digital.

Por otra parte, se percibe una Administración cuyos recursos físicos, el hardware y las personas, afrontan una etapa de envejecimiento cargada de ineficiencias. Baste con situar algunos ejemplos. Nunca conseguimos diseñar sistemas de gestión administrativa compartidos en entornos de Cloud-Público. Existen tantas administraciones electrónicas como comunidades autónomas y diputaciones, tantos sistemas de gestión de la información sanitaria como comunidades autónomas e incluso dentro de ellas con especialidades no interoperables por sectores primarios u hospitalarios, e incluso puede afirmarse que se han diseñado tantas sedes electrónicas y modelos de gestión como universidades públicas hay en el país. Ello implica, cuando la Administración dispone de recursos informáticos propios un escenario de inversión en hardware en el que las necesidades y las capacidades presupuestarias son asimétricas cuando no inversamente proporcionales. Y, por último, de la mano de la funcionarización ni sólo no es extraño que se produzcan situaciones de clara y manifiesta resistencia al cambio por parte de las plantillas, es que además su renovación y rejuvenecimiento son harto difíciles ya que resulta imposible competir con los salarios y condiciones del sector privado a la hora de innovar en los perfiles y particularmente en aquellos que tienen que ver con la analítica de los datos.

Finalmente, salvo en raras excepciones, no hemos sido capaces de superar el escenario definido para el open data por la primera directiva dictada en la materia. En estos momentos y con la excepción del impulso del Gobierno estatal en la SEDI y la Oficina del Dato, la idea de disponer de espacios de datos y de los servicios de intermediación previstos por la Data Governance Act se presenta como una mera entelequia.

Por eso resulta esencial abordar la legislatura que comienza con una estrategia centrada en la transformación digital y, ¡cómo no! en el dato. Ser capaces de disponer de una infraestructura generadora de datos de alta calidad susceptibles de ser adecuadamente reutilizados se antoja como un elemento fundamental para impulsar la prosperidad en nuestros respectivos territorios. Es un aspecto que han entendido muy bien algunos espacios de datos en España, y singularmente los que tienen que ver con la compartición o la reutilización de datos en los sectores industriales y en el marco del turismo. Pero no basta con ellos, es necesario, es necesario impulsar las políticas públicas ordenadas a la construcción de repositorios de datos que dotados de una adecuada gobernanza y condiciones de

CONTINÚA EN PRÓXIMA PÁGINA

cumplimiento normativo. Estos espacios o repositorios deberían ser capaces de desarrollar una explotación inteligente de los datos, tanto para las funciones propias de la Administración como para el impulso de la investigación, la innovación y el emprendimiento. Por otra parte, no podemos olvidar que gran parte de los resultados que deriven de la explotación de la información disponible por la Administración deberían redundar en beneficio de la propia institución, contribuyendo a alcanzar los objetivos de desarrollo sostenible, a mejorar las condiciones de vida de las ciudades y de la población que en ellas habita, y a promover políticas públicas para el territorio más eficientes cuando están basadas en datos de alta calidad.

No es lugar este, ni por supuesto tenemos ni la competencia, ni la capacidad, para decirle a cada administración como debería hacer sus deberes. Nos basta con constatar la necesidad de implementar de modo urgente políticas públicas transparentes y proactivas que permitan impulsar, de modo definitivo la transformación digital del país y desarrollar el ecosistema adecuado para el pleno desarrollo de las tecnologías disruptivas que cambiarán nuestra visión, nuestro modo de ser, y probablemente nuestro modelo económico.

No está solo

Mas de 20 años acompañando a la Alta Dirección.

La Misión de Business&Co.® consiste en ayudar a las Organizaciones a conseguir sus Objetivos de Negocio aplicando Buenas Prácticas con la ayuda de la Tecnología.

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

más información en:
https://businessandcompany.com

A propósito del nuevo petróleo, sus costes y las estrategias de inversión

Desde los inicios de Internet se ha comparado la información con los bienes más preciados o con valores de cambio como el petróleo o el oro. Seguramente debamos en gran medida los pioneros trabajos de Castells, -La era de información: economía, sociedad y cultura (1996)-, una de las primeras aproximaciones a un fenómeno cuya complejidad no ha hecho sino crecer con cada capa de disrupción. De alguna manera, la Ley de Moore integraba en su seno algo más que la pura física y economía de los procesadores. En los albores de la informática la perfección del código, su síntesis y agilidad convertían a los programadores en artesanos u orfebres. Hoy nadamos en una cierta abundancia que ha permitido el despliegue de aplicaciones de desarrollo o ensamblaje rápido multiplicando exponencialmente, por ejemplo, el ecosistema de aplicaciones móviles.

Década tras década hemos asistido a una vorágine de innovación basada en la informática como plataforma y en los datos como materia prima. Si la World Wide Web abrió las puertas de internet al conjunto de la sociedad y particularmente al comercio, la blogsfera y las redes sociales ensayaron nuevas formas de socialización y servicios que escalaron rápidamente tras la llegada del smartphone. Y ello, sin citar todos y cada uno de los usos que en el plano industrial están cambiando nuestro mundo gracias a la monitorización del internet de los objetos, o las capacidades de cálculo que nos han permitido la generación de nuevos materiales o la miniaturización a escalas inimaginables.

Cada una de estas etapas ha planteado retos jurídicos, éticos, económicos, sociales… Hoy hemos identificado con precisión uno de ellos: la inteligencia artificial. Y, venimos abordando la cuestión con los mismos mecanismos con los que afrontamos cada una de las disrupciones anteriores. De un lado, los procesos de innovación se aceleran constantemente y algunos de sus resultados alcanzan la madurez tecnológica en el contexto adecuado que les permite una rápida penetración en el mercado. En algunos casos estas tecnologías presentan riesgos apreciables o plantean serios interrogantes sobre sus repercusiones. Cuando esto sucede saltan las alarmas y se reacciona frente a lo que de algún modo podría percibirse como una amenaza.

En la práctica, se han interiorizado un conjunto de principios que probablemente influyen en este estado de cosas. En primer lugar, en no pocos casos la investigación y el desarrollo se encauzan desde los objetivos y los resultados sin considerar el proceso de gestación y el gobierno del riesgo. Va ser el mercado, la realidad, la que definirá los aspectos positivos o negativos de aquello que se ha diseñado. Este es un fenómeno particularmente visible o comprobable en las redes sociales y la analítica de datos. No debería existir ninguna duda en que las cookies,los fingerprints y, finalmente, los algoritmos de customización, fueron diseños ordenados a maximizar los recursos de los terminales, facilitar el acceso a la información y servirla con rapidez. Sin embargo, muy pronto se apreciaron sus virtudes para la manipulación emocional de los usuarios y el control social. Se diseñaron plataformas y servicios sin tener en cuenta los riesgos.

En cuanto los efectos dañosos se producen únicamente quedan tres caminos. Verificar si se trata de una conducta constitutiva de delito,

CONTINÚA EN PRÓXIMA PÁGINA

determinar si procede la exigencia de daños conforme a las leyes civiles o regular. Ello sin perjuicio de que la reprobación social y el daño reputacional puedan repercutir gravemente sobre los intereses y resultados de una compañía.

La aceleración constante, parece que superior al ritmo de la Ley de Moore, nos sitúa en la encrucijada de poner en valor no sólo los datos sino de diseñar un modelo de generación de innovación basada en datos y de gestión de procesos. Al cumplimiento normativo en el uso de los datos personales y no personales, le sucede lo mismo que a los profesionales que trabajamos en ello: somos necesarios, pero se nos soporta o tolera, somos indispensables un recurso primario, pero se nos ningunea y desprecia. El cumplimiento en nuestra cultura, y los que lo sirven, no son valorados de modo suficiente y adecuado.

Pero, a diferencia de la revolución industrial o del petróleo, la regulación no va a esperar más de medio siglo, ante la ausencia de efectos apreciables. En la sociedad de la información los riesgos, y con ellos los daños, se producen prácticamente a la misma escala de velocidad que su implantación. Ciertamente, la inocencia regulatoria pudo conceder cierta moratoria que acabó con el Reglamento General de Protección de Datos. Hoy, no tengan la menor duda con la consolidación de un régimen sancionador muy elevado es cuestión de tiempo que los jueces comiencen a entender y valorar también “cuánto vale la información” y se produzca la correspondiente escalada en las cantidades que incorporen las condenas civiles. Por otra parte, el daño reputacional puede hacer descender dramáticamente el volumen de clientes o la credibilidad bursátil.

Esta es sin duda la cara más difícil del enfoque europeo. Los datos serán oro o petróleo, pero la garantía de los derechos fundamentales se integra en una escala de valores difícilmente monetizable. Así que conviene comenzar a percibir la definición de procesos de cumplimiento ético y normativo desde el diseño como una inversión estratégica y a situar a quienes lo sirven en una posición adecuada porque producen valor. Y este discurso vale para la última de las PYMEs, porque ¿quién les debería ayudar a escoger el proveedor adecuado cuando surja un mercado de analítica de datos? ¿Cómo podrán escoger un servicio de chatbot confiable? ¿Se encuentran sus datos preparados para ser curados, enriquecidos y cruzados con los espacios de datos o son inadecuados, ilícitos y generadores de sesgos?

Nos guste o no, el Reglamento General de Protección de Datos, Data Governance Act, las futuras Data Act y/o el Reglamento de Inteligencia Artificial, así como las metodologías de análisis de riesgos y ética de la IA van a llegar y se asentarán definiendo un esquema complejo que deberá conocer, aplicar y usar como palanca reputacional y competitiva. Vd. puede seguir relegando a los profesionales y al cumplimiento al desagradable papel de invitado incómodo que tiene que estar en la fiesta, pero al que se relega en un rincón, o entender que los tiempos están cambiando.

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

www.abogadoamigo.com

NUEVOS MASTERS

eGob®

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