ESPECIAL

"Ojo al dato"

DE Tecnología & Sentido Común

AGOSTO
2021

ESPECIAL "Ojo al dato" DE Tecnología & Sentido Común

EQUIPO DIRECTO:
Javier Peris - Piloto
Manuel D. Serrat - Copiloto
Alberto Rodríguez - Equipo Directo
Juan Carlos Muria - Equipo Directo

MICRO-ESPACIOS
Marlon Molina - Es Tendencia
Ricard Martínez - Ojo Al Dato
Catalina Valencia - Ecosistema Emprendedor
Víctor Almonacid - La Nueva Administración
Shirley Villacorta - América Próxima
Fernando Ley - Geo Energía

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

GABINETE JURÍDICO
Jesús López Peláz

ATENCIÓN AL LECTOR
tecnologiaysentidocomun@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://businessandcompany.com
soluciones@businessandcompany.com

RICARD MARTÍNEZ 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

PREPARA A TU ORGANIZACIÓN PARA RETOS FUTUROS CON ITIL® 4

Los avances tecnológicos han transformado la forma en la que adquirimos e interactuamos con bienes y servicios; creando nuevos comportamientos, expectativas y experiencias.
Pero ¿estás preparado para esos retos?

El mundialmente reconocido ITIL 4, es el método de gestión de servicios que proporciona, a organizaciones y profesionales, un modelo operativo digital / de TI de extremo a extremo para la entrega y operación de productos y servicios habilitados por tecnología y permite a los equipos de TI continuar desempeñando un papel crucial en una estrategia de negocios más amplia.

¿Quieres conocer más?

AXELOS.com/ITIL4-futuro
(Página en inglés)

ESPECIAL AGOSTO 2021

índice

DE CONTENIDOS

https://tecnologiaysentidocomun.com

Índice de Contenidos

¡ic

#TYSC

Que significa ser un delegado de protección de datos

Uno nunca sabe cuándo la iluminación sale a su encuentro, pero sobre todo debe entender que la oportunidad de aprender nuevas lecciones se encuentra en todas partes. Algo así sucedió en la Jornada de la Asociación Profesional Española de Privacidad sobre recursos humanos y privacidad, en la que la única persona no experta en protección de datos nos ofreció una lección impagable.

La regulación del derecho fundamental a la protección de datos desde su génesis se ha caracterizado por su enorme fuerza de atracción. Ello se debe a la confluencia de factores diversos. El primero de ellos, y nada desdeñable, es el de una configuración extremadamente sencilla y comprensible. Se trata de un derecho al control de nuestros datos personales cuando son objeto de tratamiento. Tan sencillo como el mecanismo del botijo, o eso tendemos a creer: existe un tratamiento aplíquese la ley.

El segundo, deriva de la propia naturaleza de su objeto: el tratamiento de información personal. En el contexto primero de internet, después de las redes, y hoy de la transformación digital, prácticamente no existe una actividad pública o privada que no requiera del tratamiento de datos personales. Ello, convierte a esta materia en una suerte de eje sobre el que pivota un volumen significativo de los retos estratégicos para la gestión de las organizaciones. En tercer lugar, el llamado enforcement, el carácter tremendamente disuasorio del régimen sancionador opera de modo determinante en los procesos de toma de decisiones. Un último elemento, quizás resultado de la suma de los anteriores, consiste en la adopción por los profesionales y expertos de un enfoque que a través del prisma del derecho a la protección de datos tamiza nuestra visión de la realidad.

Desde el punto de vista humano, pueden añadirse ingredientes adicionales al cóctel para hacerlo explosivo. De una parte, no es infrecuente que los expertos en protección de datos nos erijamos en adalides de la defensa no ya de este derecho, sino de los derechos fundamentales de la humanidad entera. Y lo hacemos desde una visión alterada de la realidad en la que nada importa más que el supremo valor de proteger la privacidad. Cuándo, además, y como es el caso de quien escribe, nos proyectamos cual estrellona en el firmamento profesional, podemos destrozar reputaciones, negocios y expectativas con una sola opinión.

Por otra parte, la formación de los delegados de protección de datos adolece en muchas ocasiones de un cierto monismo en los contenidos que promueve futuros profesionales con una visión de túnel, carentes de visión periférica, incapaces de ir más allá del Reglamento General de Protección de Datos y de la Ley Orgánica de Protección de Datos Personales. La consecuencia de ello no es otra que un enfoque profesional maniqueo, en blanco y negro, cuya proyección sobre una realidad multicolor puede llegar a resultar gravemente dañosa. En esta aproximación, lo que importa es determinar si algo "es legal". Y bajo este paraguas disfrutamos de la gratificante experiencia de salvaguardar derechos cada día. Y, sin embargo, en muchas ocasiones nada hay más pernicioso y lesivo para los derechos que este tipo de ópticas.

CONTINÚA EN PRÓXIMA PÁGINA

En la sesión de APEP, mientras los expertos en privacidad andábamos perdidos y felices en nuestro mundo de unicornios, el ponente experto en recursos humanos nos bajó a la tierra. Porque a las organizaciones, no les sirve saber si algo es legal o no cuando se trata de gestionar un proceso en una situación de urgencia. Sencillamente en marzo tuvo que diseñar y ejecutar el traslado de 9000 puestos de trabajo a su casa. Y hoy, necesita saber cómo conciliar la garantía de los derechos de su equipo con la preservación de su salud, y con asegurar un ambiente laboral en el que el llamado virus SARS-COVID-2 no campe a sus anchas provocando la enfermedad. Y responder a estas preguntas, requiere de un enfoque bastante ajeno al modo en que una gran parte de los profesionales, incluidos los de las autoridades de protección de datos, enfocamos la cuestión.

En un proceso ordenado de protección de datos desde el diseño y por defecto, debemos ineludiblemente partir de los hechos, y nunca de nuestros prejuicios sobre ellos. Y no sólo esto, debemos ser capaces de comprender cuales son las necesidades, objetivos y fines que persigue la organización.

Nuestra tarea consiste en determinar si disponemos de herramientas jurídicas y técnicas adecuadas para el logro de tales objetivos garantizando no ya la protección de datos, sino el conjunto de los derechos fundamentales. Y en estos azarosos días nos enfrentamos de modo recurrente con situaciones inéditas que comportan nuevos requerimientos. Afrontar el reto que ello supone exige un conocimiento profundo de las necesidades de la organización. A la vez, se requiere una visión holística del Ordenamiento y una suerte de pensamiento lateral. Ni el RGPD ni la nueva LOPD lo regulan todo. Las condiciones de legitimación para tratar datos personales de los artículos. 6, 9 y 10 encuentran fundamento en muchos casos en la legislación nacional y en la fijación de criterios por las autoridades de protección de datos. Y no sólo esto, como ocurre en los llamados experimentos mentales de los físicos, debemos ser capaces de construir y dibujar una mapa mental que contemple caminos y posibilidades muy diversas.

En este esfuerzo el profesional nunca debe traspasar ciertos límites. Nunca podremos tolerar que se infrinja la Ley, pero nuestro deber ineludible se orienta a la búsqueda de soluciones viables, adecuadas y proporcionales. Y para ese empeño, se requiere de una metodología abierta a la interacción con los distintos roles y personas en la organización. Una mente abierta y dispuesta a evitar las trampas que nos pone la plana estructura del derecho fundamental a la protección de datos. Y ello exige no sólo, un conocimiento profundo del marco jurídico aplicable, de las políticas de la organización, de las condiciones materiales del tratamiento y los requerimientos de diseño y seguridad.
Estos tiempos difíciles, nos guste o no, nos ofrecen un regalo, nos regalan la oportunidad de dar lo mejor de nosotros al servicio de la comunidad, nos retan a innovar, a mejorar las cosas. Y tal vez para lograrlo baste con escuchar sin prejuicios y trabajar en y con el equipo.

¿Comprometernos con la privacidad?

Aunque se presuma de haber dispuesto de las más rigurosas normas sobre protección de datos, España ha sido un país de privacidad epidérmica. Hace unos años el cumplimento de la archiconocida LOPD seguía lo que podríamos definir como sistema del archivador. Se trataba de un modelo en cuatro fases

1ª Un avezado consultor organizaba una charla formativa para un determinado sector empresarial. Si era muy avezado el "plan conferencia" incorporaba dos sub-planes:

a.-Traer a algún funcionario de la Agencia Española de Protección de Datos a hacer el primo y servir de anzuelo. Sé de qué hablo, yo fui ese primo en no pocas ocasiones.

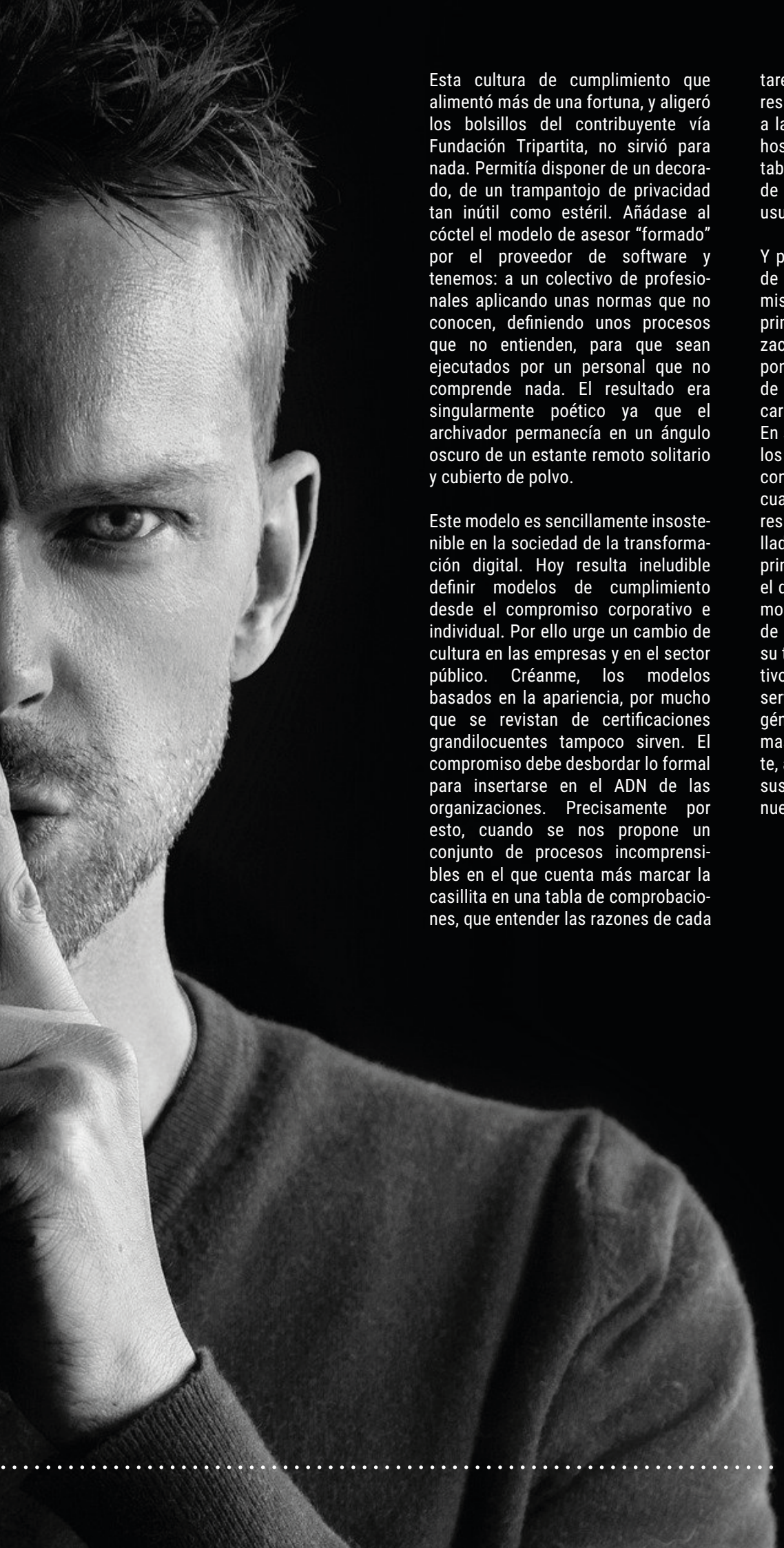
b.-Conseguir que el colegio profesional, la asociación empresarial, o la cámara local hiciera de prescriptor.

2ª Se disponía de una metodología copy-paste. Ya se sabe, vista una PYME, vistas todas.

El procedimiento esencialmente debía incluir: una inscripción de ficheros, -siempre la misma-, un documento de seguridad, -generalmente copiado de los templates de la Agencia de Protección de Datos de la Comunidad de Madrid-, una política de privacidad, y, con suerte, un modelo de contrato de encargado del tratamiento.

3ª Se rellenaban los huecos, -a veces incluso se tenía un software para ello-, y después, "a imprimir y al archivador".

4ª En caso de extrema diligencia el consultor visitaba a la empresa regularmente para inventarse algunas incidencias, y con suerte, para realizar una auditoría bienal.



Esta cultura de cumplimiento que alimentó más de una fortuna, y aligeró los bolsillos del contribuyente vía Fundación Tripartita, no sirvió para nada. Permitía disponer de un decorado, de un trampantojo de privacidad tan inútil como estéril. Añádase al cóctel el modelo de asesor "formado" por el proveedor de software y tenemos: a un colectivo de profesionales aplicando unas normas que no conocen, definiendo unos procesos que no entienden, para que sean ejecutados por un personal que no comprende nada. El resultado era singularmente poético ya que el archivador permanecía en un ángulo oscuro de un estante remoto solitario y cubierto de polvo.

Este modelo es sencillamente insostenible en la sociedad de la transformación digital. Hoy resulta ineludible definir modelos de cumplimiento desde el compromiso corporativo e individual. Por ello urge un cambio de cultura en las empresas y en el sector público. Créanme, los modelos basados en la apariencia, por mucho que se revistan de certificaciones grandilocuentes tampoco sirven. El compromiso debe desbordar lo formal para insertarse en el ADN de las organizaciones. Precisamente por esto, cuando se nos propone un conjunto de procesos incomprensibles en el que cuenta más marcar la casillita en una tabla de comprobaciones, que entender las razones de cada tarea, se abona el terreno de la resistencia al cambio. Se convierte así a la normativa sobre privacidad en un hostil enemigo, en una carga insoportable para el negocio, para los equipos de dirección, y para cada uno de los usuarios.

Y para evitar este riesgo necesitamos de algo de incalculable valor: compromiso. Este valor debe permear en primer lugar la dirección de las organizaciones. Deben realizar el esfuerzo de poner en valor y entender el significado de la protección de datos, de identificar el valor que aporta a su actividad. En segundo lugar, es crucial identificar los distintos planos de formación y concienciación. No es lo mismo un cuadro directivo, un técnico con una responsabilidad definida, un desarrollador o el conjunto de los usuarios. El principio de protección de datos desde el diseño y por defecto se proyecta de modos muy diversos sobre cada uno de ellos, y en momentos distintos de su tarea. Pero, si este esfuerzo formativo no existe, nuestros productos y servicios presentarán taras desde su génesis y presentarán serios problemas de viabilidad jurídica y, obviamente, asumirán graves riesgos materiales susceptibles de afectar gravemente a nuestra reputación.

CONTINÚA EN PRÓXIMA PÁGINA

Debemos apostar por la privacidad en momentos muy difíciles en los que los recursos de las organizaciones se orientan a la supervivencia. Esto, nos conduce a un escenario contraintuitivo en el que la privacidad se percibe como un gasto superfluo, o al menos secundario. Sin embargo, vivimos un momento histórico en el que resulta esencial para la transformación digital del negocio, el teletrabajo, o sencillamente para lograr un grado de virtualización que permita seguir operando y ofreciendo servicio y/o producto incluso en casos de confinamiento, abriendo además una ventana a la internacionalización.

Ello implica dedicar esfuerzos muy significativos dirigidos a poner en valor el Reglamento General de Protección de Datos y su normativa nacional. Para lograrlo la estrategia no puede consistir en la tradicional entrega de una lista interminable de obligaciones como anexo al contrato, o en los procesos de acogida e incorporación. Implica apelar a la privacidad como un valor subjetivo y ciudadano que nos mejora y enriquece como personas e incluirlo entre los valores de la propia organización.

Para nosotros, para los profesionales, el compromiso con la privacidad implica entender el imperativo ético y emocional que existe detrás de la tarea del delegado de protección de datos y del experto en seguridad y conciliarla con los objetivos que persigue la organización. Ser servidores y no servirnos, ser promotores y no stoppers. Se trata de proporcionar a la entidad, a los clientes y a los administrados un marco de cumplimiento cuyo centro pivota alrededor de la garantía de los derechos fundamentales ofreciendo un espacio seguro y confiable en el que desplegar la actividad. Significa haber entendido que el manejo de información personal de calidad asegura, a su vez, un sustrato de datos cuyo análisis y uso contribuye a tomar buenas decisiones. Por el contrario, una mala praxis multiplica exponencialmente los riesgos que se asocian al sesgo, y a la discriminación. Comporta finalmente, poner al ser humano y el respeto de su dignidad en el centro de nuestro diseño.

más información en:
https://javierperis.com/bpm

Y tú ¿Transformas o Trastornas tu Organización?

Aprende a:

- ✓ Modelar
- ✓ Mejorar
- ✓ Automatizar Procesos de Negocio

Curso Oficial de Certificación en
Gestión de Procesos de Negocio
ISO/IEC 19510
BPM Professional

Si quieres Aprender, Certificarte, Practicar y recibir posteriormente Ayuda para Liderar con Éxito la Transformación Digital en tu Departamento, Startup, Empresa o Administración, no te quede la menor duda de que este es tu Curso y esta es tu Certificación.

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

Derechos digitales: un reto para la organización

La presentación en consulta pública de la Carta de Derechos Digitales enmarca de modo significativo el impacto que debería tener para muchas organizaciones la transformación digital. Hasta el 20 de diciembre podemos contribuir a la consulta aportando nuestra opinión, nuestras ideas nuestra capacidad de innovar. Sin embargo, el documento posee en sí mismo una trascendencia práctica indudable.

El documento admite lecturas muy diversas. De entre ellas proponemos a nuestros lectores una introspectiva y actual. Lejos de concebir el documento como un esfuerzo prospectivo, o de esperar que un día inspire la regulación, deberíamos verificar cuantas lecciones aprendidas podemos extraer del mismo. ¿Incorpora la carta algún valor añadido? ¿Aporta lecciones que pueda aplicar? ¿Me ofrece algún espacio de innovación?

La primera lección que proporciona el texto procede de su pasado. El documento se inserta sin ningún género de dudas en la tradición constitucional europea. Y ello implica una determinada concepción de una sociedad regida desde el Derecho y enfocada a la garantía de los derechos fundamentales. En la Unión Europea la innovación y el desarrollo deben armonizarse con la norma. Y aunque en ocasiones, no sin cierta razón, se acuse al continente de un reglamentarismo excesivo, en el marco de la garantía de los derechos y la ética en la investigación científica, la innovación y la transferencia tecnológica los hechos demuestran que la garantía jurídica es esencial.

En este sentido, por razones de sistemática la Carta recoge lo previamente avanzado en las normas sobre protección de datos, administración electrónica, neutralidad en internet y garantía de los derechos digitales. Se trata de normas pioneras que han abierto el camino, aunque algunas de ellas pendientes de ejecución. Sin embargo, en este artículo quisiera centrar el enfoque en un conjunto de ideas, principios y valores que vertebran y permean la Carta y poseen una naturaleza inspiradora para el futuro de nuestras organizaciones.

El primero, antes apuntado, se centra en la idea del diseño basado en el cumpli- miento normativo. El llamado "compliance" debe insertarse en nuestro modo de concebir la transformación digital. Y debe hacerse con una mirada abierta ya que la ausencia de una ley específica no implica la carencia de criterios normativos aplicables. A título de ejemplo, la no discriminación, la garantía de la vida privada, la no manipulación de la voluntad, la protección de nuestra libertad ideológica, o la protección de la juventud y la infancia son derechos, valores y bienes constitucionales que deben ser aplicados. Y lo mismo sucede con las normativas sectoriales. ¿Acaso podemos innovar en el mundo de las Apps y los wearables en salud sin conocer y aplicar la legislación sanitaria, la relati- va a los dispositivos médicos o los seguros? No se puede innovar y después cumplir, hay que innovar desde el cumplimiento normativo.

La segunda lección aprendida se centra en el valor sustancial de la formación. Ésta es abordada por la Carta desde cualquiera de sus dimensiones: formación reglada, formación continuada y para el empleo, formación de formadores, formación a los mayores, formación online... y de tan variadas referencias deriva una conclusión certera: la transformación digital de nuestras organizaciones será muy dependiente de las capacidades y conocimiento del país. No se trata tan solo de proveer los puestos de trabajo que, en materia de ciencia de datos, computación, ética o derecho, ya sabemos que van a resultar necesarios. Se trata de entender que la automatización de procesos va a implicar nuevas interacciones persona-máquina en la mayoría de perfiles laborales y profesionales. Y sobre todo de comprender que este es un esfuerzo colectivo en el que no podemos dejar atrás a nuestra población. Y que resulta además estratégico incluso desde un punto de vista egoísta: ¿Podremos crecer si no hemos sido capaces de asegurar la adquisición de competencias de nuestros equipos? ¿Podremos mejorar si no apostamos por generar nuevo talento desde la formación?

Una tercera y última lección aprendida, se refiere al diseño centrado en el ser humano. Este enfoque se plantea desde una visión humanista tanto en el plano ético como en el jurídico cuyo alcance es muy profundo. Significa poner en valor a las personas: profesionales, empleados, colaboradores, clientes... Implica ir más allá del mero economicismo y apostar por una humanización de nuestra actividad que redundará no sólo en la calidad de nuestra tarea sino también en la percepción social sobre nuestra organización.

CONTINÚA EN PRÓXIMA PÁGINA

Supone recordar que el respeto a la persona, las políticas de accesibilidad, la salvaguarda de los valores éticos del negocio, o la sostenibilidad ambiental son valores irrenunciables en la transformación digital.

La propuesta de Carta de Derechos Digitales ofrece muchas lecturas. Aborda cuestiones muy variadas de la administración electrónica a la inteligencia artificial, de la biónica a la neurociencia.

Su mayor valor probablemente resida en el esfuerzo colectivo de poner sobre la mesa de modo sistemático los valores en juego en el mundo que estamos transformando. Vivimos tiempos milenaristas, todas las pestes lo son, en los que todos nuestros valores se ponen en juego. Lejos de frenar nuestro impulso, la grave crisis sanitaria y económica que padecemos será superada con aquello que nos hace humanos: esfuerzo, tesón, solidaridad de grupo, análisis racional, investigación, imaginación y creación.

Ante nuestros ojos se abre un abismo, nuestro ojo no percibe la transparente pasarela de cristal que lo atraviesa, pero la encontraremos y la cruzaremos. Y, cuando lo hagamos, ¿con qué valores cambiaremos el mundo?

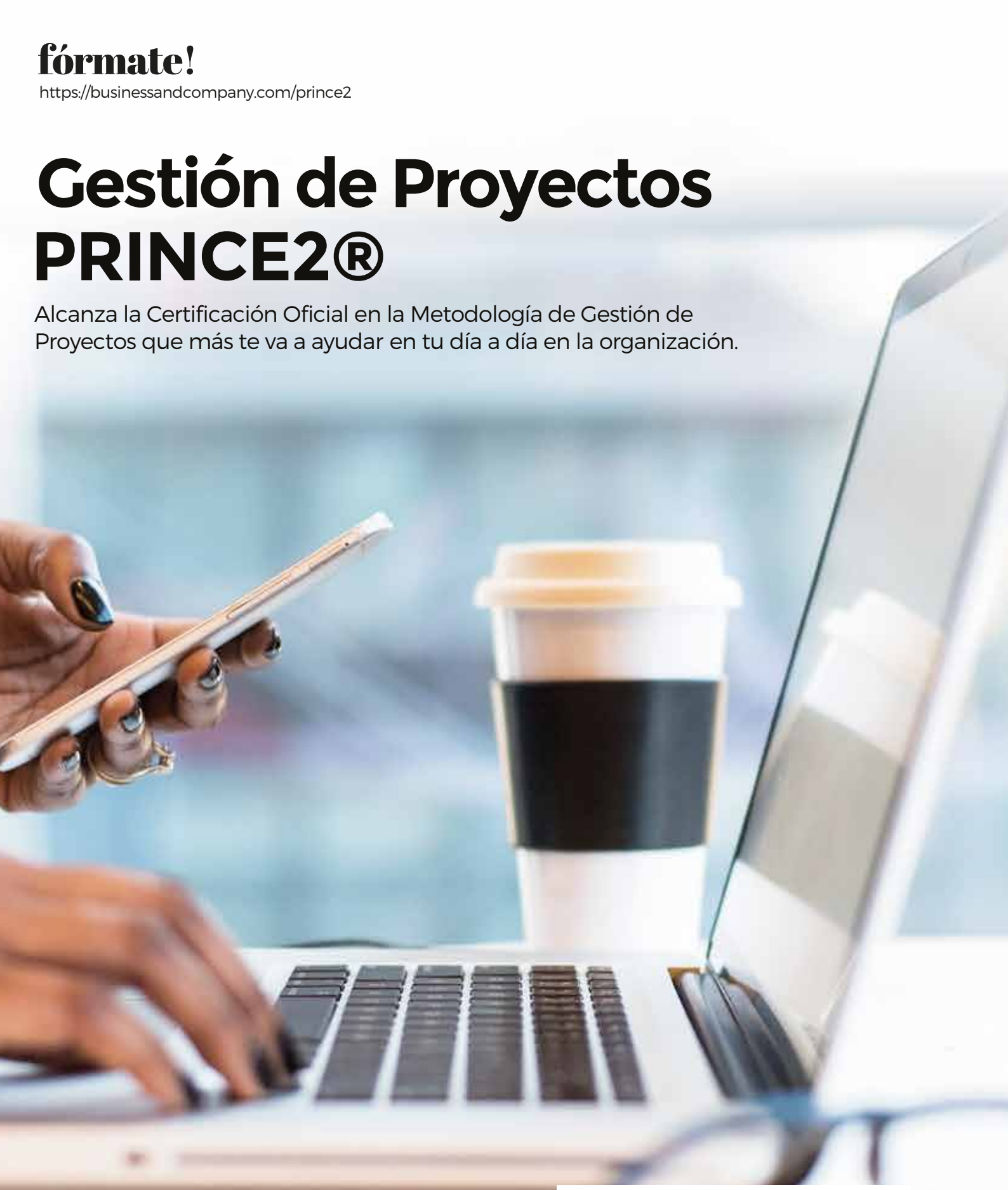
La Carta nos propone hacer la ruta desde la tradición democrática de los derechos con la vista puesta en la innovación. Pero no deberíamos esperar a que la Carta adquiera normatividad, deberíamos empezar a trabajar desde hoy, a aportar, a construir juntos.

fórmate!

https://businessandcompany.com/prince2

Gestión de Proyectos PRINCE2®

Alcanza la Certificación Oficial en la Metodología de Gestión de Proyectos que más te va a ayudar en tu día a día en la organización.



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

PRINCE2®
ACCREDITED TRAINING ORGANIZATION
PeopleCert ON BEHALF OF AXELOS

L'anno che verrà.

El inolvidable Lucio Dalla nos regaló una extraordinaria canción para tiempos de crisis que recomiendo disfrutar a nuestros lectores.

En un mundo oscuro de soledad y pobreza el bueno de Dalla escribe a un amigo prometiendo un año nuevo inolvidable. En la televisión auguran un año con tres navidades, de fiesta diaria y primavera permanente. Un tiempo de milagros, amor y creatividad.

Parece que 2021 podría ser un annus mirabilis. Paso a paso el circulo normativo se cierra, lenta pero inexorablemente. De un lado, el Reglamento General de Protección de Datos es una norma "rodada". De otro, la Unión ha definido las reglas para evitar las barreras al uso de datos no personales, y ha dispuesto las condiciones de para un nuevo modelo de reutilización de los datos del sector público. Y no acaban aquí las novedades, mal que bien la ePrivacy Regulation sigue su andadura, el Parlamento Europeo afronta la Inteligencia Artificial, se trabaja en el Espacio Europeo de Salud y la propuesta de Digital Governance Act cierra el círculo que sienta las bases para el despegue de una economía basada en datos.

En España el Gobierno impulsa una Carta de Derechos Digitales, el Plan España Digital 2025 y la Estrategia nacional de Inteligencia Artificial. En el futuro que nos anuncian la transformación digital debería cambiar el país. Es evidente, incluso para un lego en materia económica como el que esto escribe, que nuestro futuro ya no transitará los viejos caminos. El sol seguirá aquí, pero la historia nos impele a dejar de ser un país de ladrillo y camareros. De hecho, si algo ha demostrado la crisis pandémica es el carácter crucial de las tecnologías de la información para la gestión del territorio y la gestión inteligente de servicios.

En este sentido, nuestra industria señera debería estar profundamente concernida por un modelo de transformación digital que va mucho más allá de la reserva electrónica y alcanza a todas las dimensiones del negocio con la finalidad no sólo de servir experiencias a sus clientes sino de proporcionar una relación basada en la confianza y la seguridad.

Pero, sobre todo, tanto el Plan España Digital 2025 como la Estrategia Nacional de Inteligencia Artificial nos ofrecen un futuro distinto de transformación, innovación y cambio de modelo. Esta nueva sociedad y economía requieren de un uso masivo de datos de toda naturaleza y nos enfrenta a al menos tres retos estratégicos. El primero de ellos se refiere a la calidad y disponibilidad de los datos. No basta con manejar "muchos datos". Es necesario garantizar su calidad y confiabilidad, así como lo que se ha definido como curación de los datos. Es decir, resultará indispensable disponer de un modelo de gestión de los datos a lo largo de todo su ciclo de vida que asegure la utilidad de su explotación, compartición y reutilización.

Un segundo requisito deriva de la seguridad. La seguridad no sólo ofrece una barrera protectora frente a eventos dañosos. Constituye un elemento necesario e imprescindible a través de los valores que persigue, -confidencialidad, integridad, disponibilidad y resiliencia-, para ofrecer una capa de confianza en los conjuntos de datos y de procedimientos trazables en relación con su acceso y uso.

El tercer y fundamental requisito se refiere a la ética y el cumplimiento normativo. La transformación digital que se avecina debería tener un rostro humano. Debería fijar como guía la aspiración al bien común, a una sociedad inclusiva y centrada en el ser humano que proscriba toda forma de discriminación, que apueste por la sostenibilidad, y elimine las brechas digitales.

CONTINÚA EN PRÓXIMA PÁGINA




Curiosamente, nuestra vieja y odiada protección de datos define una parte de las rutas que nos permitirán alcanzar tales objetivos. El Reglamento General de Protección de Datos define un conjunto de procesos idóneos para proporcionar seguridad, confianza y gobernanza.

La regulación no agota la totalidad de las estrategias y rutas a seguir, pero se erige en una guía determinante para las duras jornadas que se avecinan. La protección de datos desde el diseño y por defecto, el análisis de riesgos y la evaluación de impacto relativa a la protección de datos centrados en la garantía de los derechos fundamentales, así como toda la experiencia adquirida en seguridad, ofrecen una cultura que debería permear el conjunto de nuestras organizaciones.

Alcanzar los objetivos de la transformación digital requerirá un esfuerzo significativo para todos los sectores y entidades. No importa su tamaño, no importa su naturaleza ni el sector de actividad. La gestión digital de las cosechas es un hecho, la conectividad y presencia en internet del pequeño comercio un requerimiento de supervivencia, la gestión de lo público basada en datos un reto ineludible. La generación, compartición y reutilización de los datos al servicio del bien común garantizando la seguridad y los derechos fundamentales de las personas una exigencia imperativa.

Deberíamos entender que nuestras prometidas tres navidades parten de la transformación digital y requieren de planificación, esfuerzo y tesón. Querido lector, no sé cuáles serán sus deseos para este 2021 que comienza. Yo seguiré el consejo de mi querido y admirado Lucio Dalla porque «L'anno che sta arrivando tra un anno passerà. Io mi sto preparando, è questa la novità».

fórmate!

https://businessandcompany.com/msp

Managing Successful Programmes MSP®

Curso de Gestión de Programas de Proyectos MSP® Fundamentos

MSP®

ACCREDITED TRAINING ORGANIZATION

PeopleCert ON BEHALF OF AXELOS

Business&Co.®

Business, Technology & Best Practices, S.L.


MacBook Air

28 DE ENERO

Aviso para navegantes

Desde 2006 cada 28 de enero celebramos el Día Europeo de la Protección de Datos. Y cada celebración ha sido acompañada por hitos relevantes. No hay duda que en el ámbito de la Unión Europea se ha construido un sólido modelo de garantía de este derecho fundamental. Desde 2016 el Reglamento General de Protección de Datos ha aportado los elementos estructurales básicos para la construcción de un edificio de garantía en el que el propio Reglamento dispone que el tratamiento de los datos se ordene al bien común.

El esfuerzo normativo europeo se enmarca en una estrategia de enorme calado a la que hacíamos referencia en el artículo del numero anterior. La Unión despliega una estrategia digital que abarca de modo global los usos de los datos e integra la Inteligencia Artificial. Este modo de entender los datos personales, y con ello la garantía de la privacidad, no se aviene bien con posiciones reduccionistas, con lo que en un tiempo definimos en nuestro sector como "talibanes de la protección de datos".

Por otra parte, nuestra sociedad de vez en cuando parece despertar y ser consciente de la importancia de un adecuado tratamiento de los datos para la garantía de nuestra libertad. Todavía no se trata de la toma de conciencia que algunos vaticinamos al precio de ser tachados de ilusos. Podría decirse, tomando prestado un aforismo de la cultura jurídica anglosajona, que la sociedad no sabe definir qué cosa sea la privacidad pero la reconoce al primer conflicto. Y así, un sencillo cambio de una política de privacidad ha supuesto un abandono de 25 millones de usuarios de una conocida aplicación en sólo 72 horas. Puede que la ciudadanía no distinga entre intimidad, protección de datos y secreto de las comunicaciones. Pero la pérdida de confianza deriva sin duda de ese modo de conocer las cosas, aunque no se sea consciente de ellas, aunque resulten indefinibles.

En años recientes la privacidad se ha convertido en una cuestión de moda que convierte a unos en héroes en la defensa de los derechos civiles y al resto, a los profesionales que navegan en las procelosas aguas del día a día, en verdaderos villanos al servicio del Gran Hermano o del Leviatán. Para sus taumaturgos nada es tan valioso, nada es tan precioso. En graves tiempos de pandemia luchamos contra un virus posmoderno y líquido con el invento de Antonio Meucci patentado Graham Bell porque no supimos encontrar una interpretación garante del Ordenamiento que facilitase aplicar tecnologías ágiles, disponibles y eficientes. Sobre su conciencia caiga cada una de las intolerables muertes que la carencia de trazabilidad eficiente ha causado y causará.

Navegar la privacidad como profesional, como poder público, como empresa o desde la política y la legislación es una actividad de alto riesgo. No hay patrón que haya pilotado antes barcos en esta tormenta perfecta. Nada vende hoy tanto como un escándalo de privacidad, nada es tan jurídicamente vinculante como una nota de prensa, nada pone tanto en riesgo la reputación empresarial como un desliz en protección de datos.

CONTINÚA EN PRÓXIMA PÁGINA

Y el 28 de enero se impone una profunda reflexión que exige un delicado equilibrio. Desde siempre se postuló un enfoque de la privacidad ordenado, garante de los derechos y funcional al contexto. Desgraciadamente, las posiciones intermedias son las más sufridas cuando el debate público se despliega en tonos de blanco y negro. Hay que aproximarse a los tiempos con el pulso del mejor de los cirujanos, con la sabiduría de los ancianos, con un grado de precisión imposible. Nos jugamos mucho en el envite.

Es un momento delicado para nuestra economía en el que se decide el futuro. Nuestras empresas necesitan digitalizarse a una enorme velocidad. El comercio de proximidad también será electrónico. Las PYME ya no pueden ser empresas ancladas en un mundo físico. El placer de lo artesano, la cercanía del tendero debe combinarse con la agilidad de una mensajería privada integrada en el móvil y con la gestión inteligente de todos nuestros recursos.

La Administración ya no resiste más. La gestión masiva de las ayudas sociales en pandemia ha mostrado las costuras de lo público. Nuestro emperador no está desnudo, anda vestido de harapos. Una burocracia tan insufrible como innecesaria retrasa meses lo que un algoritmo básico resolvería en minutos. De ahí la decidida apuesta de los Gobiernos por la transformación digital. El propio arte de gobernar exige sin duda de una gobernanza de los datos.

La salud, la investigación, el futuro de nuestra sociedad requiere sin duda de un manejo masivo de datos personales o no. Y este tratamiento está siendo ordenado por una ley general, el RGPD, de una significativa factura técnico-jurídica. Y va ser completado por un ecosistema funcionalmente orientado al progreso, al bien común y a la garantía de los derechos fundamentales.

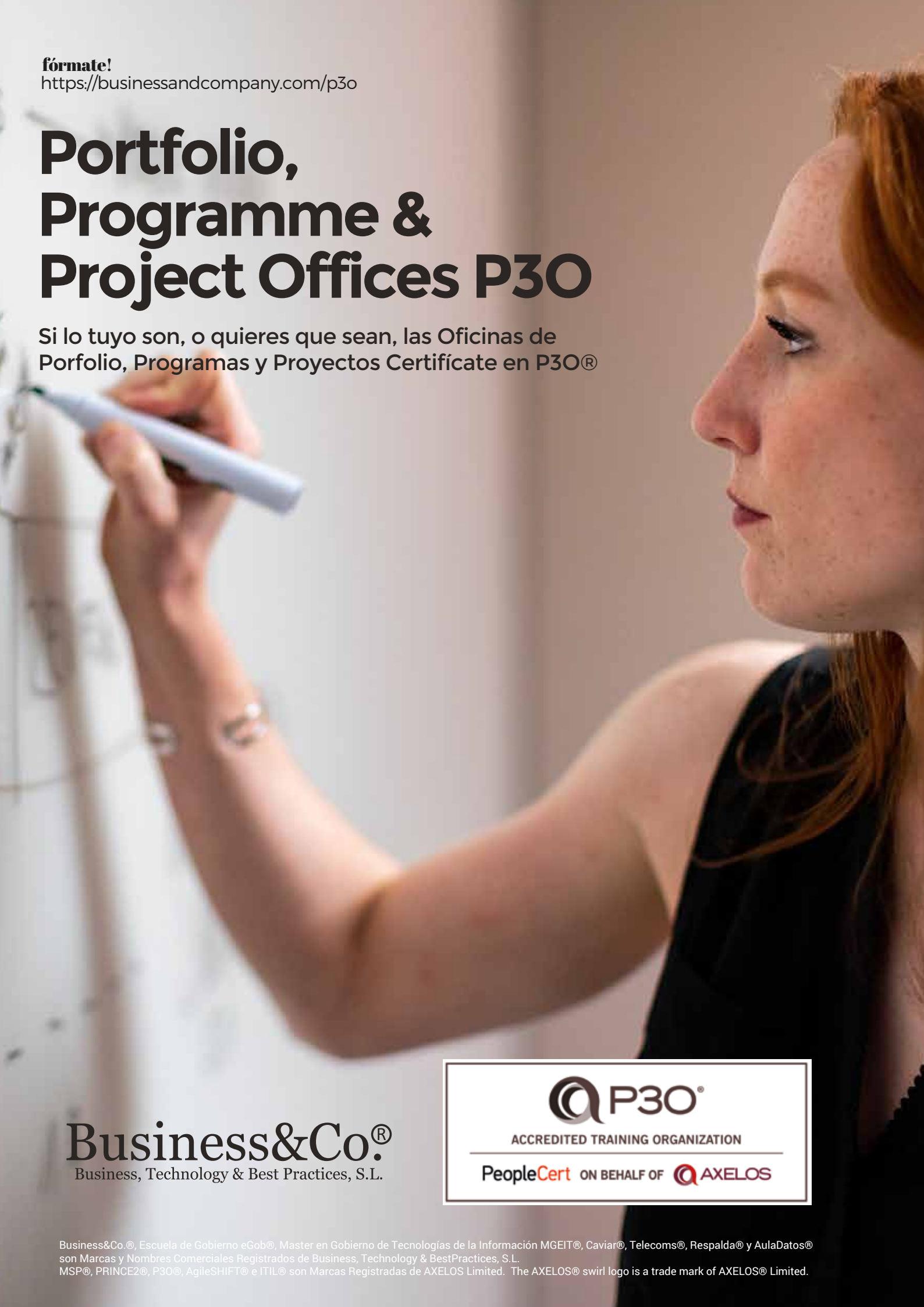
El 28 de enero de 2021 nos sitúa ante el abismo de la elección. El debate público o, para ser más precisos, el debate publicado es liderado por el discurso que demoniza al Estado, a las empresas y a la tecnología.

Este ambiente frena la iniciativa, lamina cualquier innovación. Debemos plantearnos hasta qué punto sea necesario un planteamiento ponderado. Por supuesto implacable con quienes abusen de nuestros derechos y cercenen nuestras libertades, pero a la vez capaz de ofrecer una vía adecuada de progreso para el bien común. Nos jugamos todo en el envite.

fórmate!
https://businessandcompany.com/p3o

Portfolio, Programme & Project Offices P3O

Si lo tuyo son, o quieres que sean, las Oficinas de Porfolio, Programas y Proyectos Certifícate en P3O®



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

P3O®
ACCREDITED TRAINING ORGANIZATION
PeopleCert ON BEHALF OF AXELOS

Colaboración público-privada en la investigación en salud: el reto de los datalakes gobernados

La reciente concesión del premio de proactividad y buenas prácticas de la Agencia Española de Protección de Datos de datos a la Fundación 29 por el proyecto por el Proyecto 'Healthdata29: Guía legal y repositorio para fomentar la compartición de datos de salud'. pone de manifiesto valores que debemos considerar para una adecuada estrategia de futuro de la transformación digital en nuestro país.

Este proyecto es fruto de la ambición en su dimensión más positiva. Se trata de un conjunto de aspiraciones convergentes cuyo resultado se pone al servicio del bien común. En primer lugar, resultaba evidente desde el punto de vista de Fundación 29 la necesidad de apostar por la generación de ecosistemas para la investigación con datos en salud. Desde este punto de vista, no puede afirmarse que en nuestro país existan grandes data-lakes o entornos de open data en el ámbito de la salud que ofrezcan un contexto de acceso masivo a los datos. La regla general consiste en un modelo de gestión tradicional de la información de los pacientes centrado en la vieja mecánica que inspiró en su día los ensayos clínicos.

Se trata de procesos altamente dependientes de la iniciativa investigadora del personal médico de un concreto hospital, generalmente centradas en un área de investigación muy específica y con objetivos particularmente limitados. Esto, en absoluto significa que una parte de la excelencia investigadora en salud en nuestro país, no haya descubierto ya la importancia que la investigación masiva con datos tanto para estudios retrospectivos, como para estudios prospectivos y predictivos. Tanto para los usos primarios como para los usos secundarios. E incluso, que derive en un nuevo modo de entender los ensayos clínicos. Allí donde este aprendizaje se ha consolidado, comienzan a descollar proyectos significativamente interesantes que sitúan a nuestro país en la vanguardia de la investigación en salud en ámbitos como la gestión hospitalaria de pacientes y máquinas, los estudios de comorbilidad, de imagen médica, o de interacción ambiental con la salud, entre otros muchos.

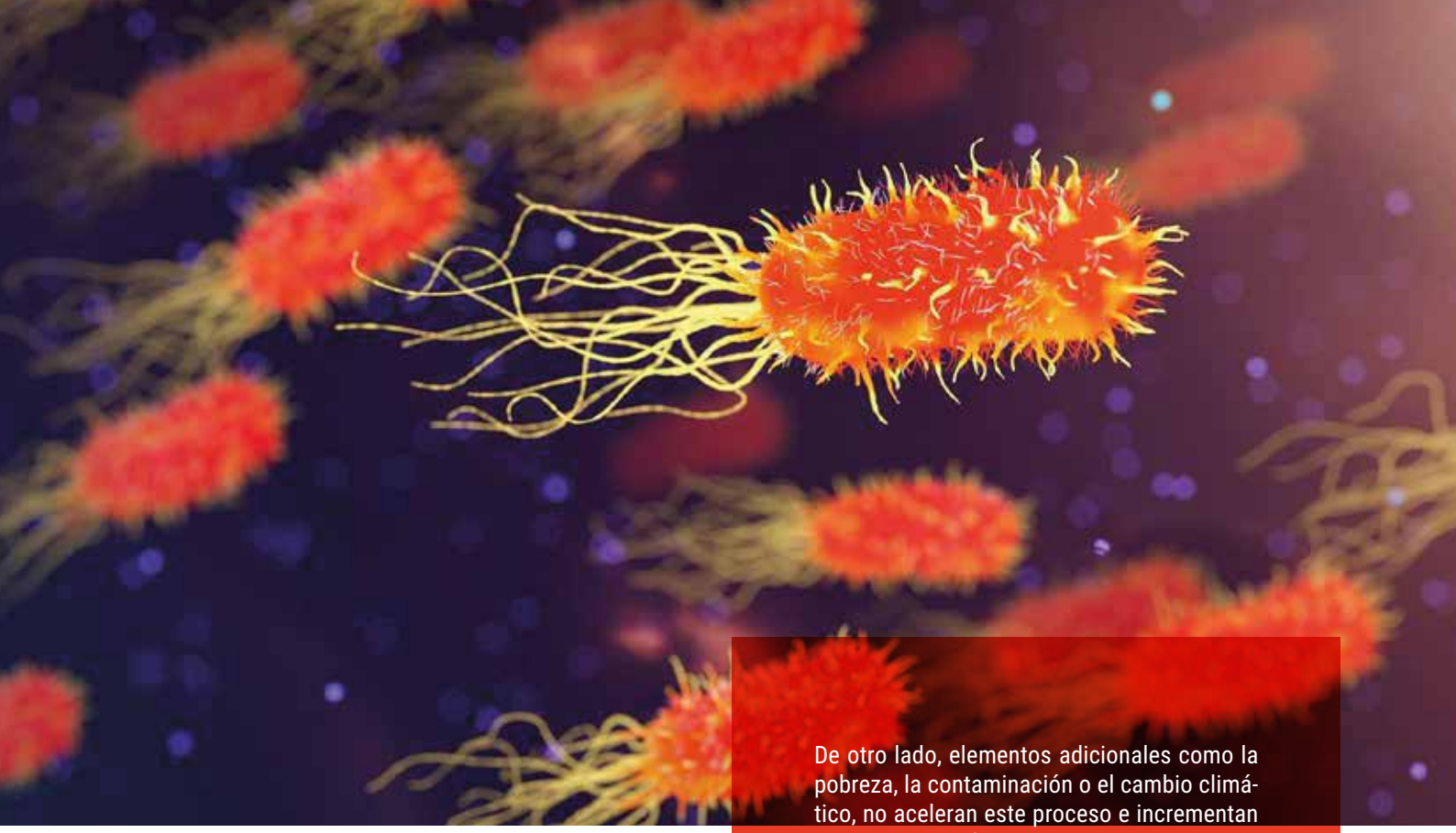
Sin embargo, este modelo atomizado, sigue configurando a los investigadores de excelencia como una suerte de islas, de guías que nos marcan el camino, pero sin alcanzar a ofrecer soluciones integrales. Y no sólo esto, el interés en el estudio con datos de salud va mucho más allá de las profesiones médicas, de la farmacología o de la investigación biológica o biotecnoló- gica básica. Existe un amplio grupo de profesionales en el mundo de la ingeniería en todas sus dimensiones, -la industrial, la informática, las telecomunicaciones pasando por la imagen o el sonido-, para la economía, o para ámbitos muy directamente relacionados como las dinámicas de gestión poblacional, y aquellas necesarias para el mantenimiento del estado del bienestar. Y a día de hoy las interacciones entre estas distintas áreas de conocimiento, y las posibilidades de fertilización cruzada que de ello derivarían, se encuentran particularmente limitadas por cuestiones que van mucho más allá de la infraestructura y de la cultura heredada en materia de investigación en salud. Alcanzan también al modo en que tradicionalmente se ha venido interpretando y aplicando la norma.

Y esta es la segunda de las ambiciones que pone sobre la mesa el proyecto. Es de justicia recordar que en nuestro país las posturas respecto del uso de datos de salud en materia de investigación habían sido tradicionalmente hiperrestrictivas. En este sentido, el uso de los datos para investigaciones concretas, la prohibición de su uso para finalidades distintas, y una interpretación absolutamente defensiva de la normativa de protección de datos por el regulador y por los equipos jurídicos en los sistemas de salud, definía un escenario caracterizado por una burocracia imposible, por la existencia de barreras procedimentales e interpretaciones normativas que abonaban al fracaso prácticamente cualquier escenario de investigación masiva con datos en salud. Esta situación, fue remediada por el Reglamento General de Protección de Datos que pone en valor el interés público existente en el uso de los datos con fines de investigación en salud y su relevancia para bien común.

En esta materia, aunque queda mucho camino por recorrer, puede afirmarse la presencia de una aproximación matizada por las cautelas de las autorida- des de protección de datos. Durante la crisis de COVID19 las autoridades han afirmado con rotundidad y a cada ocasión que el Reglamento General de Protección de Datos es una herramienta útil para promover la investigación en salud y al mismo tiempo garantizar los derechos de los pacientes y ello, tanto desde el punto de vista más urgente, esto es el epidemiológico y asistencial, como desde el punto de vista de la investigación básica y aplicada ordenada al futuro. Sin embargo, estas afirmaciones, generalmente no han venido acompañadas de documentos que permitieran a la comunidad aprender el modo de hacer las cosas.

Y este fue el segundo gran objetivo del proyecto. ¿Tendríamos la capacidad de diseñar un modelo básico de interpretación de la norma que resultase funcional al objetivo de generar entornos de data Lake con datos de salud susceptibles de ser utilizados con fines de investigación? La respuesta era sin duda afirmativa. Y ahí la Cátedra de privacidad y Transformación Digital Microsoft-Universitat de Valencia a partir de la experiencia previa adquirida con en la colaboración en proyectos de investigación del Instituto de Investigación Sanitaria INCLIVA, singularmente BigMedilytics, y el análisis del ecosistema de investigación del Instituto de Investigación Sanitaria, el IIS La Fe, y proyectos como Chaimeleon, ha podido ensayar un enfoque basado en la idea de favorecer ecosistemas de *open data* controlado.

CONTINÚA EN PRÓXIMA PÁGINA



Gracias a las oportunidades que ofrece la disposición adicional decimoséptima sobre tratamientos de datos de salud de la Ley Orgánica de Protección de Datos Personales es posible construir un modelo caracterizado por una gobernanza adecuada de los datos y por una separación funcional clara entre el repositorio y los investigadores que asegura la inaccesibilidad física y lógica de los datos y las posibilidades de aplicar analítica mediante un proceso intermediado en el que la Fundación como tercero de confianza ofrece las garantías tecnológicas y jurídicas adecuadas para asegurar estos tratamientos. Sólo faltaba una guinda, un equipo que trasladase la investigación básica de la Cátedra a un modelo adecuado a las condiciones de la Fundación con una guía práctica con principios sólidos de actuación. Y a ello se dedicó el equipo de Garrigues Asociados.

Varias son las lecciones aprendidas de esta experiencia. La primera es de naturaleza ética. La investigación en salud es un elemento estratégico y crucial para el futuro de nuestras sociedades. La pandemia solo ha puesto de manifiesto algo que podíamos probar. En un mundo que se ha empequeñecido, en un mundo completamente globalizado, la incidencia de cualquier enfermedad puede afectar de modo rápido al conjunto de sistemas de salud.

De otro lado, elementos adicionales como la pobreza, la contaminación o el cambio climático, no aceleran este proceso e incrementan de modo significativo las necesidades de nuestros sistemas. Ello exige un cambio radical en nuestra óptica, como ciudadanos nos obliga entender la importancia de aportar nuestros datos para la investigación, como sociedad nos obliga a definir cuál sea el alcance del principio del bien común en el uso de los datos de salud y de otros datasets con fines de investigación.

La segunda lección aprendida, implica entender que, con las herramientas normativas a nuestra disposición, con un alto grado de innovación jurídica y con una aproximación basada Oen la protección de datos desde el diseño y el conocimiento de la realidad material, pueden alcanzarse soluciones altamente funcionales para conseguir los objetivos de la investigación en salud.

La última de ellas, y no menos valiosa, consiste en comprender que la colaboración público-privada, la transferencia de conocimiento desde el mundo universitario a la economía, la empresa y la Administración, constituyen un pilar estratégico para el crecimiento y la transformación digital de nuestro país. Ya sólo falta, que se incorporen a esta dinámica las autoridades de protección de datos. Conceder un premio, no deja de ser un primer paso significativo, aunque no suficiente.

Privacidad, ¿amarla o temerla?

A partir de la aprobación de la muy conocida Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal el bloque en nuestro país el miedo a la sanción fue siempre un significativo argumento de venta. La metodología es bien conocida en el sector de la pequeña y mediana empresa.

Las empresas que ofrecían consultoría en materia de protección de datos utilizaban con frecuencia el temor a la imposición de una severa multa, ya sea como primer argumento, ya sea como argumento definitivo. Para ello bastaba, con invocar algún caso que hubiera aceptado a una empresa de similares características a la tipología de aquella en la que se estaba desarrollando el llamado marketing de puerta fría.

Ciertamente, se trata de una estrategia de marketing que con generosidad puede calificarse de poco elegante, aunque no resultase estrictamente ilegal. Desgraciadamente "el argumento del palo" era el único que restaba a los consultores a falta de un compromiso serio de nuestras empresas con la garantía del derecho fundamental a la protección de datos. Y menos mal, porque el de la "zanahoria" adquirió tintes surrealistas. Con el tiempo el cumplimiento "despegó" con la llamada LOPD Coste cero consistente en una utilización claramente fraudulenta de los fondos de formación para encubrir lo que en realidad era soporte al cumpli- miento normativo. Y no fu este el peor de los escenarios. En ocasiones, un comercial amenazaba con abrir una inspección utilizando nombres parecidos al de la Agencia Española de Protección de Datos, e incluso utilizando de modo simulan- do su imagen corporativa, mientras otro remataba la faena consiguiendo el contrato. Se trata sin duda de un episodio más de esa absurda y surrealista escopeta nacional en la que parecemos vivir inmersos. El resultado es bien conocido una estrategia de cumplimiento epidérmico y sin alma de la normativa.

Sin embargo, a lo largo del tiempo y sin desfallecer muchas personas tratamos de poner en valor, de "amar" la privacidad. Tratamos de trasladar a la sociedad un mensaje claro. El compromiso con la garantía de los derechos fundamentales de los clientes, de los asociados, o de los administrados, comportaba sin duda beneficios significativos. No sólo se trataba de la conciencia del deber cumplido. Mucho más allá de esto, el desarrollo de procesos de implantación y cumplimiento de la legislación sobre protección de datos suponía una ingeniería de procesos que permitía una reorganización significativa de los sistemas de información, una mejora cualitativa de la seguridad de los mismos, y en definitiva un incremento en la calidad de los datos y en la eficiencia en su manejo.

Ahora que el Reglamento General de Protección de Datos alcanza una adecuada velocidad de crucero el viejo debate vuelve aparecer con fuerza. En primer lugar, porque el tan criticado modelo de "enforcement" español se ha consolidado como una clara apuesta de la Unión Europea. Las lecciones aprendidas de la Ley Orgánica 15/1999 mostraban que un régimen sancionador significativo, pero económicamente asumible con los presupuestos ordinarios de las grandes compañías no incentiva un mejor cumplimiento normativo. En la práctica lo que sucede es que la compañía provisiona en cada ejercicio el riesgo normativo, considerando una dotación económica de recursos para hacer frente a una suerte de impuesto anual adicional. Basta con verlas memorias de la Agencia Española de Protección de Datos en el período 2007-2016 para constatar cómo determinados sectores venían asumiendo un volumen de sanciones prácticamente similar año a año. Y ello sin que se redujese la litigiosidad o el número de infracciones y sanciones detectadas e impuestas. La conclusión es obvia: incluso con el gravoso modelo español, resultaba rentable incumplir.

Tal vez por ello, el legislador europeo ha importado al Reglamento General de Protección de Datos procedimientos sancionadores propios del Derecho de la competencia. Para ello decidió establecer un modelo de graduación de la sanción que puede permitir un significativo grado de proporcionalidad. El regulador puede escoger el imponer multas con una cantidad fija de hasta 20 millones de euros, o bien calcularlas sobre un porcentaje significativo de los ingresos globales brutos de una compañía. Ello le permite modular una política sancionadora que evita el riesgo de cerrar una pequeña o mediana empresa y al mismo tiempo imponer sanciones a grandes compañías cuyo monto total opera de modo particularmente disuasorio.

Y efectivamente a ello se han puesto todas las autoridades de protección de datos. España, lo hecho con contención y discreción. Sin embargo, en este último trimestre hemos venido conociendo sanciones de cinco a seis millones de euros. Ciertamente muy lejos de las cantidades que imponen otras autoridades de protec- ción de datos. Por ejemplo, el Information Commissioner británico ha impuesto sanciones de importe superior a veinte millones de euros y se otean en el horizonte de los reguladores europeos multas centenarias en millones. En cualquier caso, el mensaje es muy claro, ha pasado suficiente tiempo desde la plena entrada en vigor del Reglamento como para que las organizaciones hayan alcanzado un grado de madurez adecuado y cumplan la normativa con el debido rigor.

CONTINÚA EN PRÓXIMA PÁGINA

Sin embargo, es de nuevo el momento de plantearse cuál es la mejor opción si amar o temer la privacidad.

Creo que deberíamos mantener el enamoramiento. Las metodologías que propone el Reglamento General de Protección de Datos constituyen sin duda una bitácora idónea para navegar la transformación digital con un diseño centrado en el ser humano. Desde un punto de vista ético, no todo puede valer para monetizar. Desde un punto de vista material el RGPD diseña un conjunto de procesos de extraordinaria utilidad para adaptar los tratamientos a condiciones idóneas de cumplimiento normativo. Ocioso resultaría recordar, como ya se señaló con anterioridad, los beneficios que de ellos derivan.

Sin embargo, este modo de amar la privaci- dad debe ser incentivado también por los reguladores. En la vida, no solemos desear aquello que se nos impone. Tendemos a rechazar aquellas personas, aquellas organizaciones, y aquellos procedimientos que de modo vertical se imponen a sus destinatarios sin ningún espacio para el diálogo, para el aprendizaje compartido, y para el desarrollo común. Sería hipócrita compadecer a aquellos que incumplen la ley. Pero no sólo sería menos, tratar de convertir el territorio del derecho fundamental a la protección de datos en una nueva batalla maniquea entre buenos y malos. Es el momento de considerar cuáles van a ser las estrategias que en el futuro nos permitan alcanzar un alto nivel de cumplimiento normativo garantizando los objetivos que exige superar la grave crisis que nos aqueja.

Cuando cese la pandemia las lecciones aprendidas de una transformación digital acelerada, el despliegue de todas nuestras capacidades de analítica de datos en la investigación y en la gestación de políticas públicas, e incluso las propias metodologías que nos han llevado alcanzar en un tiempo récord la vacuna, demostrarán hasta qué punto el futuro depende de una transformación que garantice los derechos fundamentales. Necesitaremos tratar un volumen ingente de datos, y deberemos ordenar sus usos a la garantía de las libertades, al crecimiento de la economía, a la aceleración de la digitalización de todos los sectores. En definitiva, al bien común. Y en este proceso amar la privacidad producirá siempre mejores resultados que temerla.

fórmate!
https://businessandcompany.com/cobit

Tu vida puede depender de la tecnología

COBIT® 2019 Marco de Gobierno y Gestión de la Tecnología

La Implementación de un Marco de Gobierno y Gestión de Tecnologías de la Información permite conocer la salud global de los Sistemas de Información de los que depende los procesos habituales de una organización, sin un adecuado Marco de Gobierno y Gestión se podrá trabajar la seguridad, privacidad y otros aspectos de manera disociada tampoco se podrá garantizar que se estén teniendo en cuenta todos los factores necesarios para una adecuada operación. COBIT® aporta confianza.

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

Violaciones de seguridad

En los últimos tiempos, es raro el mes e incluso la semana, en la que se publica información sobre alguna violación masiva de la seguridad de compañías o administraciones. Alguna de las multas récord impuestas por autoridades de protección de datos deriva precisamente de una gestión inadecuada de las obligaciones que en esta materia impone el Reglamento General de Protección de Datos. Corremos el riesgo tanto de magnificar como de relativizar una cuestión particularmente trascendente.

La seguridad constituye una necesidad y una obligación inherente a la gestión de activos valiosos. Con independencia de que incluyan datos personales, los sistemas de información deben ofrecer una seguridad adecuada, robusta, bien dimensionada, que proporcione resiliencia. Es un hecho conocido que la regulación de la protección de datos impulsó de modo significativo la adopción de medidas de seguridad en todos los ámbitos.

Sin embargo, esta virtud envuelve bajo su manto un terrible pecado. Es necesario preguntarse cuantas organizaciones conciben la seguridad como una obligación impuesta. Porque este es un modo erróneo de abordarla que conduce a una concepción formal y a una implementación epidérmica que no permea la cultura corporativa.

A finales de los años 90 la reforma del llamado paquete de directivas “telecom” introdujo una novedad: la notificación de violaciones de seguridad. No bastaba ya con diseñar una estrategia de seguridad capaz de gestionar incidentes, ahora correspondía evaluar bajo qué condiciones un incidente debería ser notificado a una autoridad de protección de datos, y en último extremo a las personas afectadas. Este procedimiento se incorporó al Reglamento General de Protección de Datos que define como elemento determinante la constatación de un riesgo para los derechos y las libertades, en cuyo caso debe notificarse la brecha a la autoridad, o un alto riesgo que determinará el deber de comunicarla al interesado sin dilación indebida.

El valor que subyace al marco normativo pone en el centro de su diseño la protección de las personas. Ello tiene profundas consecuencias jurídicas, pero también éticas. De una parte, obliga a un esfuerzo de empatía que modula la valoración de un impacto en nuestra seguridad. La seguridad se proyecta aquí, más allá de la gestión de un incidente, como un instrumento de garantía de los derechos de las personas, como una barrera cuya violación pone en riesgo a seres humanos.

Sin seguridad no existe ni una garantía de privacidad ni una protección adecuada de la información. Y una vez que ésta es accedida, alterada, manipulada, o robada, la naturaleza instrumental de la misma se proyecta sobre distintas esferas de nuestra vida. Y no se trata exclusivamente de considerar aquellos impactos que de modo objetivo nos ponen en riesgo. Es, obvio que, si roban nuestros usuarios y contraseñas, acceden a datos de identificación y números de cuentas bancarias, corremos el riesgo de se suplante nuestra identidad. Si entran en nuestra casa, se pasean por ella, husmean en nuestros armarios y se marchan sin romper o robar nada puede que nos sintamos aliviados, pero no por ello menos violados o vulnerables. Y esto es lo que debería suceder cuando se entra en nuestra cuenta en cualquier entorno digital: aunque no se lleven nada, han accedido a nuestra casa digital, nos han mirado sin autorización. Incluso en tales casos la intrusión nunca puede ser calificada como banal habida cuenta de las posibilidades que ofrece la analítica de datos.

CONTINÚA EN PRÓXIMA PÁGINA

El sentido de la regulación de las violaciones de seguridad es bastante evidente y busca comprometer activamente a responsables y encargados del tratamiento. Se trata de generar una cultura de compromiso con un diseño centrado en el ser humano y en la garantía de sus derechos. Este compromiso implica una mirada analítica y profunda que verifique las condiciones en las que una brecha de seguridad puede proyectarse sobre la vida de las personas en todas sus dimensiones. Este compromiso se refuerza con un deber de transparencia que busca satisfacer al menos dos objetivos.

En primer lugar, implica una supervisión administrativa. Cuando la brecha alcance un determinado nivel de criticidad es obligatorio someterse al criterio del regulador. Es decir, no basta con activar nuestro plan de contingencia o respuesta, resulta necesario que una autoridad independiente revise que nuestro diseño de la seguridad y su ejecución respondía a criterios de adecuación, diligencia y profesionalidad. En esencia, se trata de demostrar que fuimos una víctima y no un descuidado agente que facilitó la brecha desde la negligencia. Con ello se ofrece un incentivo particularmente contundente a las organizaciones ya que su seguridad será siempre verificable por una autoridad con poderes de inspección y sanción.

En segundo lugar, la notificación de una violación de seguridad implica un compromiso colectivo. En esencia, se alinea con políticas de coordinación pública y privada bien conocidas que han ido creciendo desde la Directiva NIS. Es indispensable compartir con los organismos competentes en materia de seguridad nuestros incidentes. De esta socialización dependen la capacidad global del sistema para monitorizar el estado de la seguridad, detectar precozmente nuevas amenazas y definir políticas preventivas y reactivas. El Reglamento General de Protección de Datos da un salto adelante incluyendo en la ecuación la supervisión del regulador y la necesidad de comunicar a las personas en situaciones de alto riesgo.

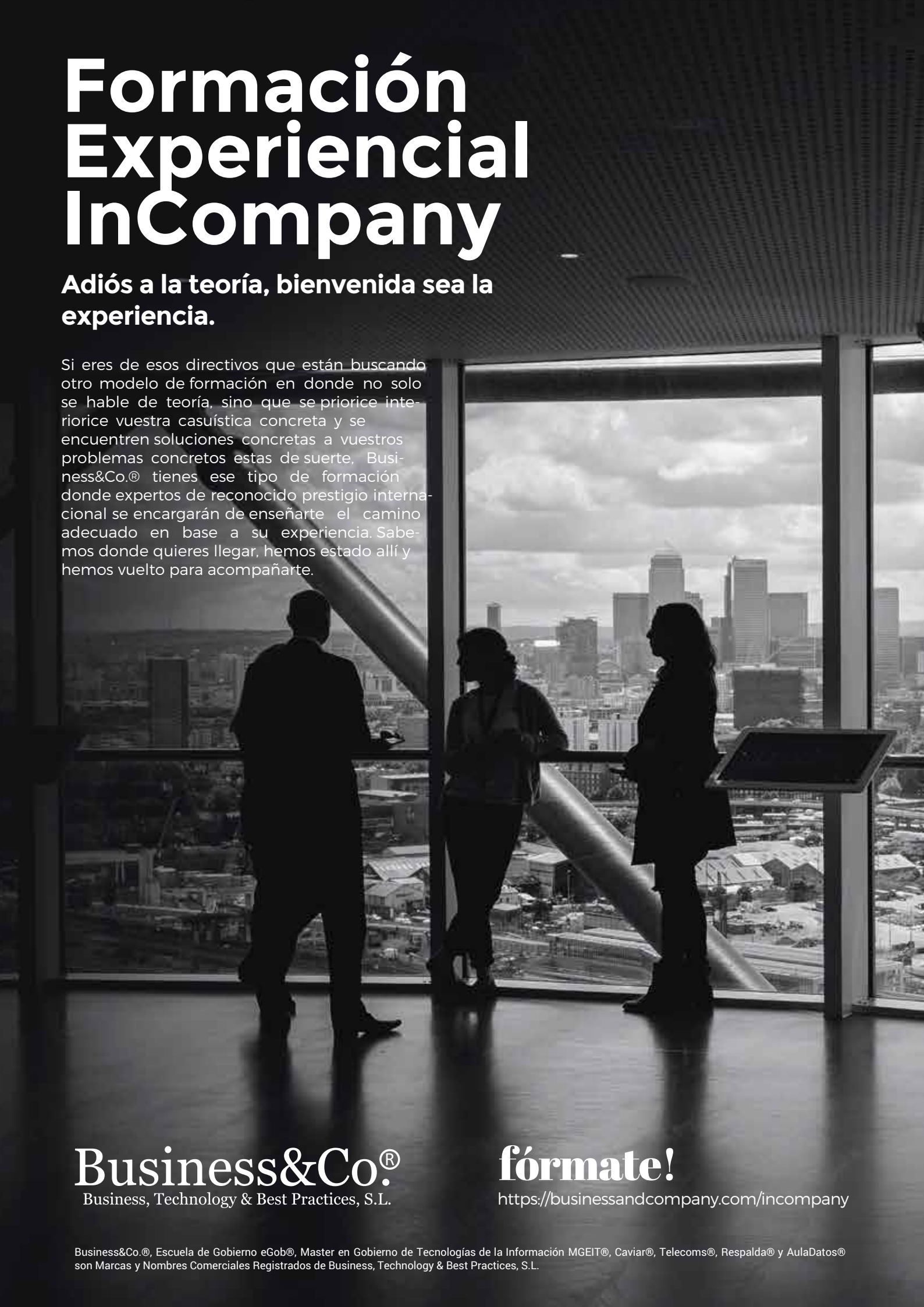
Ninguna de estas previsiones puede ser menospreciada en una economía que monetiza la privacidad, y tampoco en el contexto de la transformación digital de un sector público que necesita pasar a un modelo de decisiones basadas en la evidencia, en el dato. La ciudadanía, los usuarios no deben ser en absoluto ajenos al problema. Las aplicaciones móviles, las redes sociales, los servicios gratuitos de la sociedad de la información no son ni un regalo ni una donación. Y las administraciones no nos ofrecen servicios basados en la beneficencia sino en los derechos que nos concede nuestro modelo de estado del bienestar. La seguridad no sólo es una obligación para responsables y encargados del tratamiento, es un derecho para los usuarios.

Magnificar una violación de seguridad y estigmatizar a quienes las notifican es un grave error de juicio de muchos medios. Relativizarlas, restarles importancia, y banalizarlas constituye una grave afectación de nuestros derechos, una manifiesta desconsideración del ser humano, y una posición éticamente inadmisible.

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 formación 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

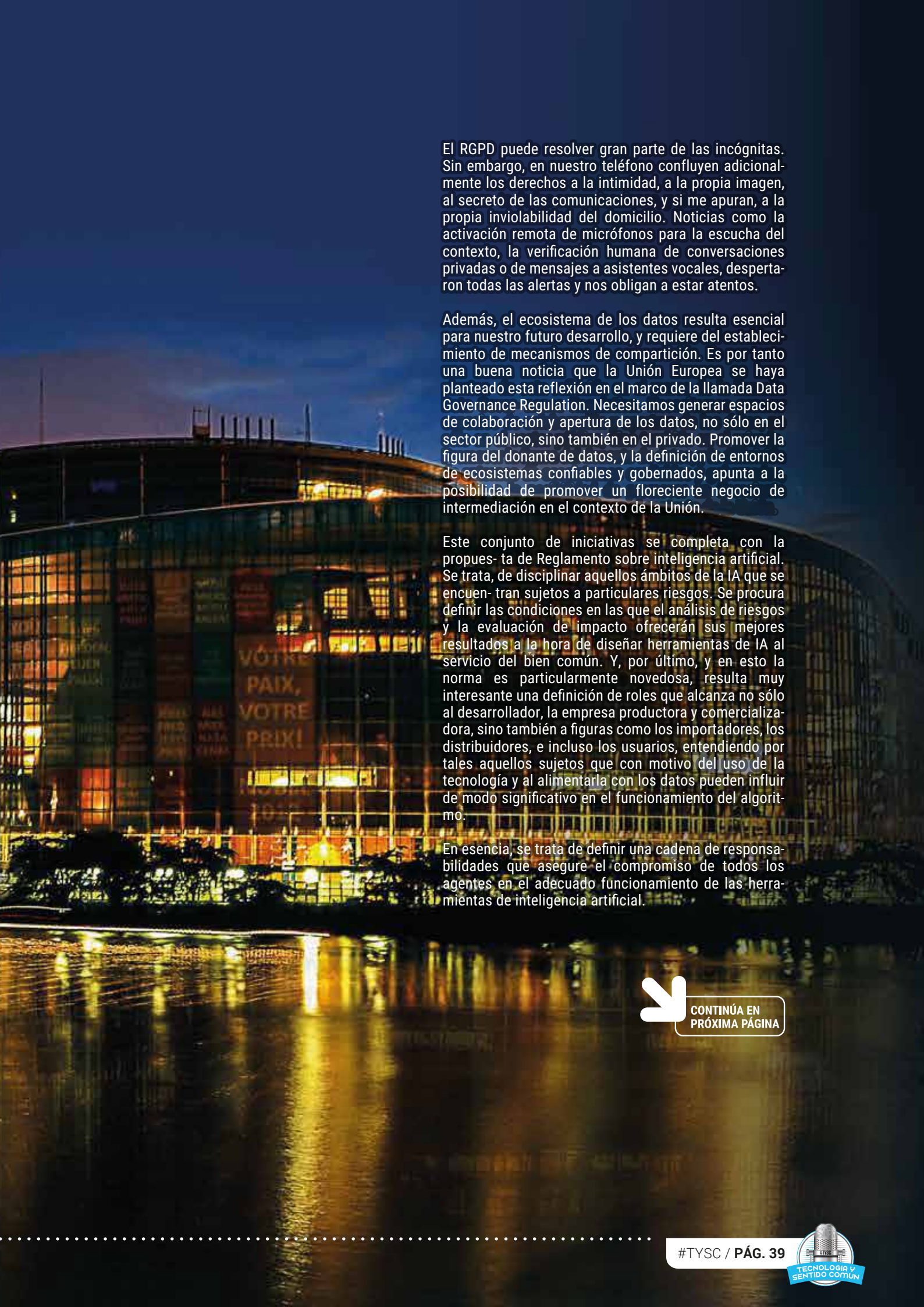
Eppur si muove

La entrada en vigor del reglamento General de Protección de datos el 25 de mayo de 2018 parecía haber cerrado un ciclo enormemente productivo en la producción normativa de la Unión Europea. El Reglamento venía a resolver un viejo problema de dispersión normativa. En la práctica, la Directiva 95/46/CE había sido transpuesta desde la cultura y los intereses propios de cada país. Generó un batiburrillo de disposiciones, no sólo contradictorias entre sí, sino también profundamente alejadas desde el punto de vista de su concepción del enforcement. El resultado práctico de este fracaso no fue otro que favorecer el dumping normativo y multiplicar los costes de las entidades que operaban en distintos territorios de la Unión.

El RGPD contiene más de 50 remisiones a la legislación nacional en sectores específicos. Además empiezan a entreverse entre las costuras de la norma algunos rotos que conviene parchear. También se necesita de la adopción de decisiones estratégicas en ámbitos tan sensibles para nuestro futuro como el espacio europeo de salud y la investigación. El pasaporte COVID, o la infinita discusión en relación con las medidas adoptadas para el uso de información personal en la lucha contra la pandemia, han sido claro y mani- fiesto ejemplo de las carencias estructurales que todavía plantea el Derecho de la Unión.

Así pues, contamos con el RGPD, con la Directiva que regula el tratamiento de datos en el ámbito de la investigación judicial y policial penal, -en fase de trasposición- y con leyes nacionales de adaptación o de adecuación del RGPD al ordenamiento nacional. Pero se trata de un ecosistema que no para de crecer. Se podría afirmar que está condenado a un crecimiento relativa- mente constante y mantenido. El Convenio 108/1981 marcó el Big Bang en un sector del Ordenamiento en permanente estado inflacionario. A las citadas normas se han unido en el último par de años el Reglamento que regula el uso de datos no personales y la Directiva Open Data. En estas dos últimas normas, se hace una leve llamada al RGPD, en la medida en que los datos generados en tales contextos pudieran tener la naturaleza de datos personales, pudieran encontrarse inextricablemente unidos a ellos, o pudie- ran cruzarse y convertirse en datos personales.

Por otra parte, el ámbito de las telecomunicaciones debe completarse con la e-Privacy Regulation. Existen muchos interrogantes sin resolver en el ámbito de la prestación de servicios equivalentes al servicio de telecomunicaciones, y con el crecimiento exponencial del universo *smartphone*. Necesitamos seguridad jurídica y procedimientos claros de actuación.



El RGPD puede resolver gran parte de las incógnitas. Sin embargo, en nuestro teléfono confluyen adicionalmente los derechos a la intimidad, a la propia imagen, al secreto de las comunicaciones, y si me apuran, a la propia inviolabilidad del domicilio. Noticias como la activación remota de micrófonos para la escucha del contexto, la verificación humana de conversaciones privadas o de mensajes a asistentes vocales, despertaron todas las alertas y nos obligan a estar atentos.

Además, el ecosistema de los datos resulta esencial para nuestro futuro desarrollo, y requiere del establecimiento de mecanismos de compartición. Es por tanto una buena noticia que la Unión Europea se haya planteado esta reflexión en el marco de la llamada Data Governance Regulation. Necesitamos generar espacios de colaboración y apertura de los datos, no sólo en el sector público, sino también en el privado. Promover la figura del donante de datos, y la definición de entornos de ecosistemas confiables y gobernados, apunta a la posibilidad de promover un floreciente negocio de intermediación en el contexto de la Unión.

Este conjunto de iniciativas se completa con la propues- ta de Reglamento sobre inteligencia artificial. Se trata, de disciplinar aquellos ámbitos de la IA que se encuen- tran sujetos a particulares riesgos. Se procura definir las condiciones en las que el análisis de riesgos y la evaluación de impacto ofrecerán sus mejores resultados a la hora de diseñar herramientas de IA al servicio del bien común. Y, por último, y en esto la norma es particularmente novedosa, resulta muy interesante una definición de roles que alcanza no sólo al desarrollador, la empresa productora y comercializadora, sino también a figuras como los importadores, los distribuidores, e incluso los usuarios, entendiendo por tales aquellos sujetos que con motivo del uso de la tecnología y al alimentarla con los datos pueden influir de modo significativo en el funcionamiento del algoritmo.

En esencia, se trata de definir una cadena de responsabilidades que asegure el compromiso de todos los agentes en el adecuado funcionamiento de las herramientas de inteligencia artificial.

CONTINÚA EN PRÓXIMA PÁGINA

En todas y cada una de las regulaciones a las que nos hemos referido, y en todas las áreas de negocio a las que directa o indirectamente hemos aludido, existe un sustrato común: el dato. Éste, puede ser un dato de carácter personal, seudonimizado, anominimizado, o sencillamente un dato no personal. En todos y cada uno de estos casos, información valiosa de cuya calidad y certeza depende significativamente el buen funcionamiento de los sistemas de información y herramientas de analítica de IA que pueden tener un impacto profundo en nuestro futuro.

A todos ellos deberíamos aplicar sin duda las lecciones aprendidas a lo largo de 30 años de experiencia regulatoria en materia de protección de datos. Debemos tener en cuenta que la licitud y lealtad en el tratamiento, la transparencia, la integridad y la confidencialidad, en resumen, la responsabilidad proactiva, deben servir como como valores que inspiren nuestro modelo de gestión.

Es posible que el crecimiento constante del marco regulador pueda generar una cierta zozobra. Pero deberíamos empezar por el principio. Disponer de un adecuado marco de cumplimiento, de un modelo de gobernanza en el tratamiento de los datos personales será el sustrato que nos permitirá no sólo cumplir con el escenario normativo que se avecina, sino tener la capacidad de adoptar decisiones altamente productivas para nuestra organización. La analítica de datos, la inteligencia artificial, ya no son productos exclusivos de la investigación básica universitaria, un privilegio sólo a disposición de las grandes compañías multinacionales. Cada día, crecen las estrategias de inteligencia artificial en los países y en las administraciones públicas, y se desarrollan *hubs* dirigidos a proveer de servicios de esta naturaleza a la pequeña y mediana empresa. Es un reto, para el que todos debemos estar preparados, y deberíamos comenzar por por asegurarnos de disponer de unos datos de calidad, legítimamente obtenidos, y altamente confiables.

fórmate!
https://businessandcompany.com/itil

El Sistema de Valor del Servicio de ITIL®4

...o todavía andas pensando en el ciclo de vida del Servicio.

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

ITIL®
ACCREDITED TRAINING ORGANIZATION
PeopleCert ON BEHALF OF AXELOS

Un horizonte de esperanza

A lo largo de los últimos meses hemos venido compartiendo con nuestros lectores y lectoras luces y sombras en la protección de datos personales.

Nuestros artículos han sido siempre dirigidos valores muy concretos: tratar de responder a cuestiones relevantes en la materia, proporcionar lecciones aprendidas, y, por encima de todo, encontrar un marco de referencia que permita conseguir los objetivos de las organizaciones cuando tratan datos de modo que concilien con la garantía de los derechos fundamentales de los clientes o administrados.

En el último artículo de esta temporada es conveniente abordar cuáles deberían ser los objetivos en materia de protección de datos en un contexto más amplio. Es momento de volver a preguntarse hacía dónde caminamos y en que debería consistir nuestro enfoque como país en el contexto de las estrategias de la Unión Europea.

Como es sobradamente conocido se está produciendo una aceleración en el desarrollo del marco normativo de la protección de datos. España, aunque con retraso, ha traspuesto finalmente la Directiva 2016/680. Mientras, la Unión Europea produce nuevas piezas regulatorias que siguen alimentando el ecosistema regulador del tratamiento de datos de carácter personal y no personal.

A la ya longeva Propuesta *ePrivacy* que tratará de disciplinar el ámbito de las telecomunicaciones, se han sumado al menos tres iniciativas adicionales relevantes. La primera de ellas, es la Data Governance Regulation. Un reglamento, cuyo objetivo primordial consiste en promover el uso de los datos para el bien común. Se trata de dar un salto más allá de los principios que rigen la reutilización de la información del sector público, promoviendo el nacimiento de un modelo de explotación de datos orientado a la producción de innovación y conocimiento que sea capaz de explotar datos personales, tanto de origen público como privado.

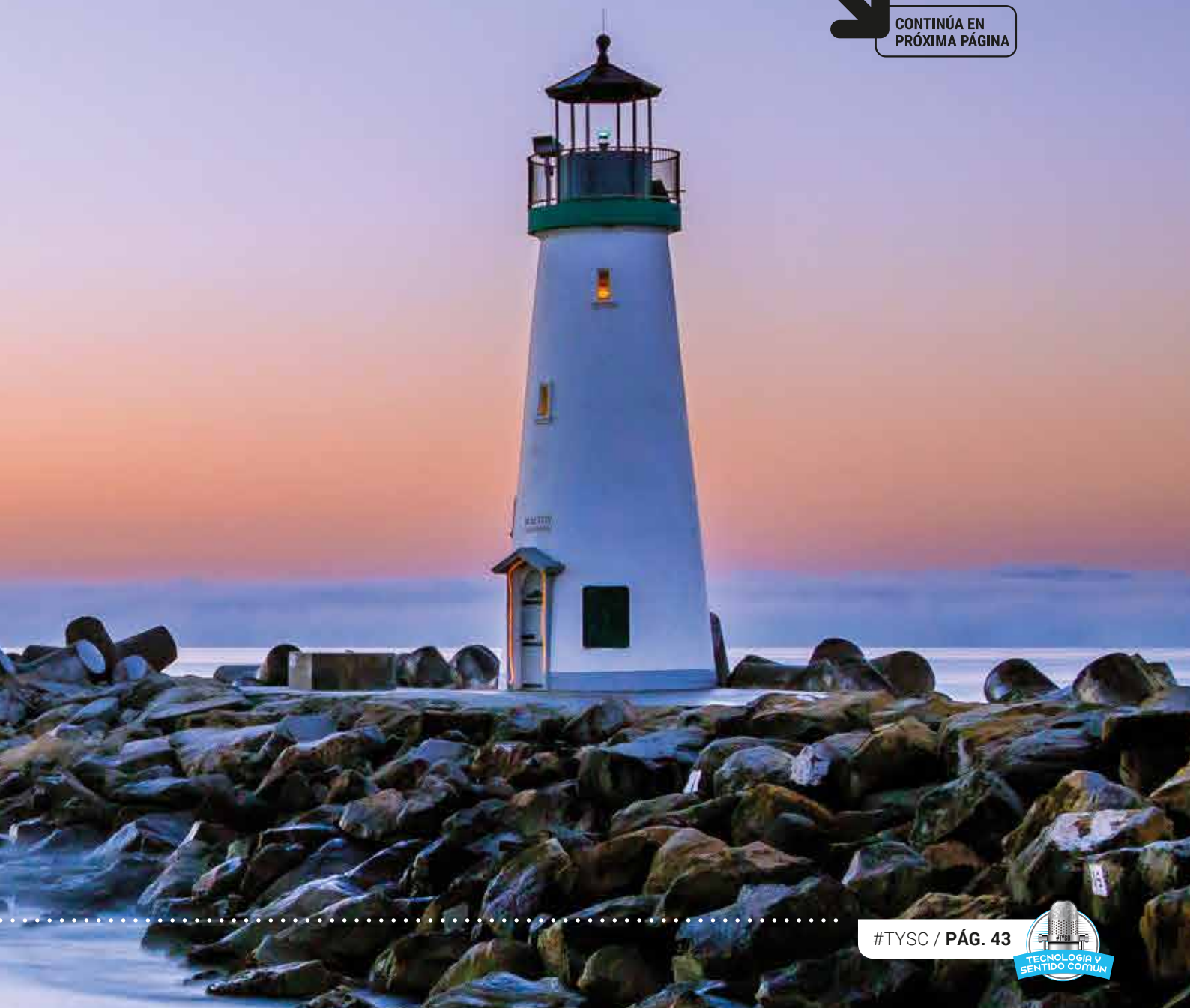
Posee particular relevancia tanto el estímulo de las donaciones de datos como la generación de un entorno favorable a la aparición de entidades de intermediación que faciliten el uso de los datos, garantizando el pleno respeto al RGPD.

De otro lado, el llamado *Digital Services Act package* podrá contribuir a la definición del nuevo marco para los servicios de la sociedad de la información o servicios digitales. Territorio en el que sin duda deberá asegurarse la garantía de las condiciones adecuadas del tratamiento conforme al RGPD como instrumento necesario para el funcionamiento adecuado de los negocios. La última recién llegada es la Propuesta de Reglamento sobre normas armonizadas en materia de inteligencia artificial. Una propuesta que define escenarios de confiabilidad en la inteligencia artificial desde un enfoque centrado en el riesgo, en la garantía de los derechos fundamentales de la persona, y en los debidos controles y responsabilidades asociados a la supervisión humana. La Propuesta traslada al ámbito del Derecho los resultados del Grupo de Expertos de Alto nivel en Inteligencia Artificial de la Comisión Europea. Es muy conveniente tener en cuenta la filosofía que inspira todos y cada uno de estos hitos regulatorios. Se trata de proporcionar un marco ordenado para el desarrollo de las tecnologías de la información que facilite y discipline el avance tecnológico acomodándolo a los requerimientos del Derecho y de la filosofía de garantías que inspira la Unión Europea.

Por otra parte, este escenario convive con un intenso crecimiento del volumen de sanciones que se imponen en protección de datos en el conjunto de la Unión Europea. Si bien España no ha alcanzado el nivel de las decenas de millón de euros, es cierto que comienzan a imponerse sanciones millonarias. Esto debe suponer un toque de atención, pero no sólo para responsables y encargados del tratamiento. Desde el punto de vista de los reguladores debe ponderarse con particular cuidado el ejercicio del derecho sancionador en este ámbito. El marco sancionador de la Unión Europea debe operar con una doble finalidad disuasoria y de remedio. Se trata de conseguir que en el desarrollo de la tecnología se garanticen los derechos y, en caso de infracción, que se obtengan las debidas lecciones aprendidas para mejorar las condiciones de los tratamientos. Por otra parte, las autoridades deben acompañar este proceso con el estímulo de la adopción de códigos de conducta, certificaciones, y en todo caso promoviendo guías de cumplimiento normativo abiertas a la participación sectorial que definan objetivos "alcanzables" para un cumplimiento de calidad. Si las autoridades dan la espalda a los sectores público y privado, si se enrocan en un modelo de ejercicio funcional centrado en la fijación de criterios desde arriba y sin un conocimiento adecuado de la realidad, no sólo no se garantizan los derechos fundamentales, sino que se impondrán barreras insalvables al desarrollo de la tecnología en el contexto de la Unión Europea.

En este sentido, cada una de las administraciones, cada una de las empresas en este país se juega mucho ante la necesidad de definir un modelo de recuperación económica fuertemente centrado en la innovación y el emprendimiento. Cuando lleguen los fondos *Next Generation* esperamos que operen como un trampolín que cambie nuestro modo de concebir la economía y el progreso. No reivindicamos con ello la desaparición de sectores tradicionales y que seguirán produciendo un alto rendimiento a nuestra economía. Estos sectores, como el turismo, están particularmente necesitados de una transformación digital que genere modelos competitivos de alta calidad e intensidad.

CONTINÚA EN PRÓXIMA PÁGINA



El turismo comprometido con los valores de nuestro país no puede ser un turismo de charanga y organillo, debe ser acompañado de herramientas altamente cualificadas en términos tecnológicos que proporcionen al cliente, servicios de valor añadido que hoy por hoy ni siquiera imaginamos.

Pero no sólo se trata de transformar sectores tradicionales, sino de innovar y emprender. Nuestras universidades generan talento más que suficiente para el que no encontramos nichos de mercado adecuados. La evolución de sectores como el del de la prestación de servicios de salud, la economía y el marketing o el desarrollo de producto cuentan con los más variados profesionales egresados en nuestras universidades. De las ingenierías al derecho, de las ciencias humanas a la sociales, aparecen especializaciones enfocadas a las tecnologías de la información y futuros egresados con altos conocimientos en ciencia de datos o inteligencia artificial, por citar algunos ejemplos.

Pero para su crecimiento, este talento necesita de un ecosistema favorable. De un entorno que definitivamente permita una adecuada reutilización de los datos del sector público al servicio del bien común. Y en un contexto en el que las condiciones de cumplimiento normativo no se perciban como una rémora insalvable, como un coste inasumible, sino como una inversión. Y necesitamos que el sector privado aprenda a compartir datos y a vincularlos a *hubs* de analítica de datos al servicio del conjunto de la sociedad.

Parece, que sabemos lo que queremos. El Estado cuenta con una estrategia de inteligencia artificial, y un plan de transformación digital a medio plazo a corto plazo, el plan 2025. Las comunidades autónomas están desarrollando estrategias equivalentes a la estatal.

Los fondos europeos, pueden ser la plataforma de inversión desde la que construir nuestro futuro. La protección de datos, debe acompañar estos procesos, ofreciendo respuestas viables, señalando el camino al servicio de los objetivos del país. Lo diremos una y 1000 veces, la protección de datos nos ofrece una respuesta a la pregunta sobre cómo hacer las cosas. Y esa respuesta debe ser funcional con un único límite que no puede ser jamás traspasado: protegemos datos, protegemos a las personas.

#BestPractices #BetterProfessionals

Cursos oficiales de Certificación

septiembre

GOBIERNO I&T

COBIT® 2019 FUNDAMENTOS

PRIMERA SESIÓN:
Viernes 3 de Septiembre de 2021 de 16:00 a 21:00 horas

SEGUNDA SESIÓN:
Sábado 4 de Septiembre de 2021 de 09:00 a 14:00 horas

TERCERA SESIÓN:
Viernes 10 de Septiembre de 2021 de 16:00 a 21:00 horas

CUARTA SESIÓN:
Sábado 11 de Septiembre de 2021 de 09:00 a 14:00 horas

GESTIÓN DE SERVICIOS

ITIL® 4 FUNDAMENTOS

PRIMERA SESIÓN:
Martes 7 de Septiembre de 2021 de 16:00 a 21:00 horas

SEGUNDA SESIÓN:
Jueves 9 de Septiembre de 2021 de 16:00 a 21:00 horas

TERCERA SESIÓN:
Martes 14 de Septiembre de 2021 de 16:00 a 21:00 horas

CUARTA SESIÓN
Jueves 16 de Septiembre de 2021 de 16:00 a 21:00 horas

GESTIÓN POR PROCESOS

BPM PROFESIONAL ISO/IEC 19510

PRIMERA SESIÓN:
Viernes 17 de Septiembre de 2021 de 16:00 a 21:00 horas

SEGUNDA SESIÓN:
Sábado 18 de Septiembre de 2021 de 09:00 a 14:00 horas

TERCERA SESIÓN:
Viernes 24 de Septiembre de 2021 de 16:00 a 21:00 horas

CUARTA SESIÓN
Sábado 25 de Septiembre de 2021 de 09:00 a 14:00 horas

GESTIÓN DE SERVICIOS

ITIL® 4 STRATEGIST: DIRECT, PLAN & IMPROVE

PRIMERA SESIÓN:
Martes 21 de Septiembre de 2021 de 16:00 a 21:00 horas

SEGUNDA SESIÓN:
Jueves 23 de Septiembre de 2021 de 16:00 a 21:00 horas

TERCERA SESIÓN:
Martes 28 de Septiembre de 2021 de 16:00 a 21:00 horas

CUARTA SESIÓN
Jueves 30 de Septiembre de 2021 de 16:00 a 21:00 horas

octubre

GESTIÓN DE SERVICIOS

ITIL® 4 FUNDAMENTOS

PRIMERA SESIÓN:
Viernes 1 de Octubre de 2021 de 16:00 a 21:00 horas

SEGUNDA SESIÓN:
Sábado 2 de Octubre de 2021 de 09:00 a 14:00 horas

TERCERA SESIÓN:
Viernes 8 de Octubre de 2021 de 16:00 a 21:00 horas

CUARTA SESIÓN
Sábado 9 de Octubre de 2021 de 09:00 a 14:00 horas

GOBIERNO I&T

COBIT® 2019 FUNDAMENTOS + ISO 38500 PROFESIONAL

PRIMERA SESIÓN:
Martes 5 de Octubre de 2021 de 16:00 a 21:00 horas

SEGUNDA SESIÓN:
Jueves 7 de Octubre de 2021 de 16:00 a 21:00 horas

TERCERA SESIÓN:
Martes 12 de Octubre de 2021 de 16:00 a 21:00 horas

CUARTA SESIÓN:
ISO/IEC 38500 a elegir por el Alumno.

GESTIÓN DE PROYECTOS

PRINCE2® FUNDAMENTOS

PRIMERA SESIÓN:
Viernes 15 de Octubre de 2021 de 16:00 a 21:00 horas

SEGUNDA SESIÓN:
Sábado 16 de Octubre de 2021 de 09:00 a 14:00 horas

TERCERA SESIÓN:
Viernes 22 de Octubre de 2021 de 16:00 a 21:00 horas

CUARTA SESIÓN:
Sábado 23 de Octubre de 2021 de 09:00 a 14:00 horas

GESTIÓN OFICINAS DE PROYECTOS

P3O® FUNDAMENTOS

PRIMERA SESIÓN:
Martes 19 de Octubre de 2021 de 16:00 a 21:00 horas

SEGUNDA SESIÓN:
Jueves 21 de Octubre de 2021 de 16:00 a 21:00 horas

TERCERA SESIÓN:
Martes 26 de Octubre de 2021 de 16:00 a 21:00 horas

CUARTA SESIÓN:
Jueves 28 de Octubre de 2021 de 16:00 a 21:00 horas

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

Más información en
https://javierperis.com/formacion-oficial/