CSO ESPAÑA

IDG COMMUNICATIONS

Seguridad, gobernanza y accesibilidad del dato en la sociedad digital

Marga Verdú/ Imagen: Sergi Salas

La llegada del Reglamento General de Protección de Datos (GDPR, de sus siglas inglesas) ha supuesto un trampolín hacia la innovación.

Con la finalidad de profundizar sobre estos conceptos, *CSO España*, en colaboración con Accenture e Informática, ha organizado recientemente una mesa de debate que ha tratado sobre la importancia de proteger el dato de manera responsable, y de cómo ha evolucionado la información hasta convertirse en un activo monetizable para cada vez más organizaciones.

Contando con directivos procedentes de grandes organizaciones de diversos ámbitos económicos como *retail*, banca, farmacia o salud pública entre otros sectores, buena parte del debate ha contado con numerosas referencias al impacto de la entrada en vigor del Reglamento General de Protección de Datos (GDPR, de sus siglas inglesas), una normativa que ha supuesto un gran cambio en la forma en que se concibe la protección de datos a lo largo y ancho de la Unión Europea. La llegada de dicha normativa también, se ha transformado, según los expertos, en un trampolín hacia la innovación. Actuando de moderadora, Maria José Marzal, directora de *CSO España*, planteaba un escenario del dato que se ha modificado considerablemente con la llegada del GDPR, en el que las compañías se enfrentan al reto de automatizar los procesos de la información: descubrimiento, etiquetado y clasificación de los datos en su mapa de sistemas (ingesta y almacenamiento), para luego poder gobernar y securizar los datos en entornos estructurados y no estructurados.

Para, Xabier Mitxelena, managing director Iberia cybersecurity de Accenture Security apeló a la importancia de la llegada del GDPR, ya que está ayudando a entender que la seguridad no es un coste sino un elemento competitivo. “También hemos de contemplar la seguridad como una inversión lejos de representar un coste, ya que las compañías están inmersas en la transformación digital y, por tanto, entra a formar parte del formato de negocio. También nos

María José Marzal, directora de *CSO España*.

Jaume Soler, responsable de data privacy & data security lead for Iberia de Accenture Security.

> “Disponer de capacidades para el descubrimiento, clasificación, etiquetado y autodestrucción del dato va a ser básico”

hemos dado cuenta de que la seguridad es un ejercicio de responsabilidad”, señaló el directivo.

Por su parte, Gloria Saavedra, directora sector retail, utilities, travel & pharma de Informatica, puntualizó que la tecnología forma parte de la ayuda de que disponen las empresas para afrontar estos retos, necesidades y preocupaciones. “Como parte de esa transformación digital, la tecnología que esté respaldada por socios que la conocen y que, además, sus creadores sean sabedores de las necesidades que abordan actualmente los negocios, pueden evolucionar y hacer que esas preocupaciones y retos sean más llevaderos, con la finalidad de que cada organización consiga alcanzar ese control de la información y de esos datos que tanto nos preocupan”.

Consciente de la importancia de proteger el dato y de cómo se almacena la información en nuestros sistemas, Rubén Garrido, CIO de Electrodomèstics Candelsa, abogó por mantener unos niveles de securización del entorno, situando al dato en el eje estratégico de la organización. “Ya que el dato que se encuentre

> “Cuando los datos crecen de manera exponencial aparecen nuevas regulaciones para intentar salvaguardar nuestra propia seguridad como ciudadanos”

María José Pérez, directora de soluciones de seguridad del dato Iberia de Informatica.

“Aparecen nuevas regulaciones enfocadas al tratamiento y las garantías que se han de dar al dato en protección”

Para Jaume Soler, responsable de data privacy & data security lead for Iberia de Accenture Security, la economía, que estaba basada en modelos de producción ha dado paso a otros modelos de negocio que basan su operativa en la centralización del dato y en cómo pueden extraer valor económico del mismo”, señala Soler, al tiempo que justifica la llegada de normativas en torno al dato. “Derivado de este afán de monetización del dato aparece una serie de retos que van focalizados a nivel normativo, como puede ser el GDPR, del que ahora parece que empezamos a respirar un poco después de que los reguladores hayan establecido muchos requisitos tanto de securización como de control del dato. “No obstante, este experto señala que ahora empiezan a aparecer nuevas regulaciones que también van enfocadas al tratamiento y las garantías que se han de dar al dato en aspectos relativos a su protección, en el momento de recopilar de dato, así como en toda la vida útil del dato y en su proceso en el momento de securizarlo”.

“Desde Accenture Seccurity hemos identificado cuatro grandes retos que deberían estar abordándose de manera inminente: las tareas de descubrimiento, etiquetado y clasificación y destrucción del dato no representan medidas nuevas, pero si queremos llevar una buena gobernanza del dato para sanear la organización y para ser más óptimos en el establecimiento de modelos de monetización del dato, debemos mantener un orden dentro de la casa”. Jaume soler asegura que tener capacidades para el descubrimiento, la clasificación, el etiquetado y la destrucción del dato va a ser básico, “un proceso que ha de evitar que el procedimiento final no recaiga sobre el usuario, sino forzando de alguna manera dentro de la organización para que realice la transformación de la manera más automatizada posible”. Para Soler este circuito que ha de realizar todo dato necesita seguridad.

Jaume Soler, responsable de data privacy & data security lead for Iberia de Accenture Security.

en este nuevo entorno digital es más crítico que nunca, se hace imprescindible dotarlo de las medidas necesarias para evitar cualquier mal uso o pérdida de información. Para nosotros, toda la implementación de GDPR así como de otras normativas ha modificado enormemente los planes de inversión de la empresa, dado que tenemos muy claro que el dato es un bien que ha de ser protegido y almacenado en nuestros sistemas de información”.

Javier Montoya, director de seguridad de Aigües de Barcelona, afirmó que si bien es cierto que el concepto de GDPR ha cambiado alineándose con el concep-

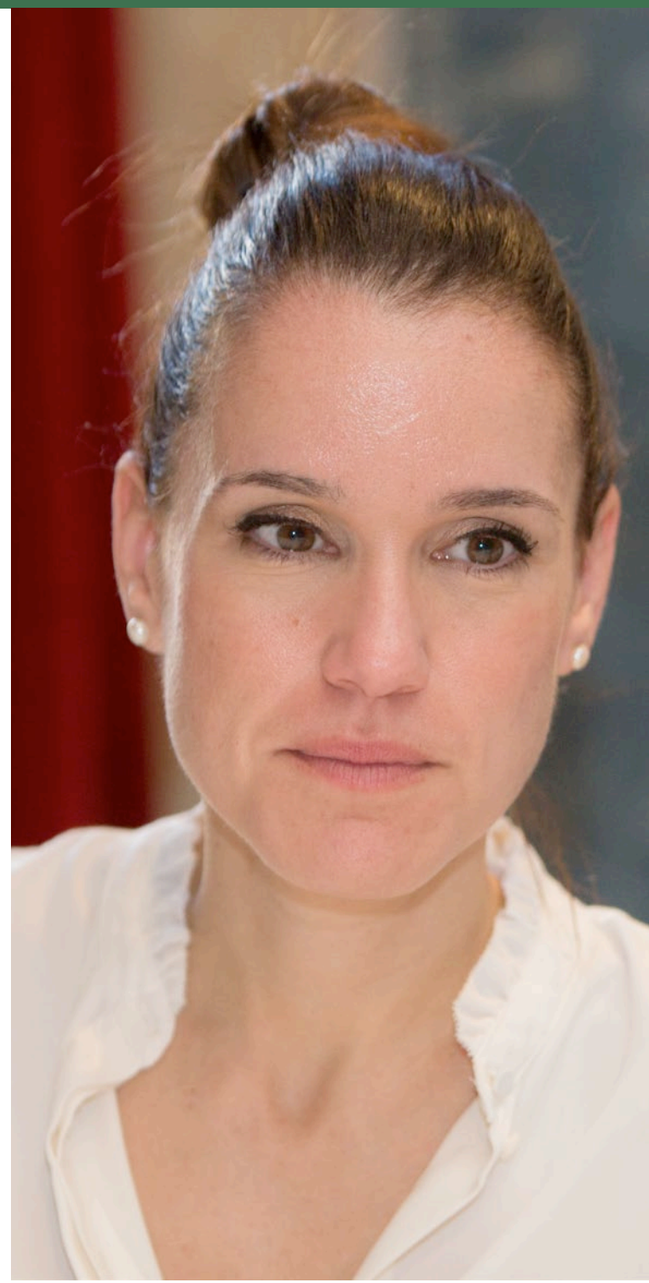
Javier Montoya, director de seguridad de Aigües de Barcelona.

> “La aparición de GDPR ha sido un acierto, ha puesto al sector en su sitio”

to relacionado con los análisis de riesgo, “creo que ha sido un acierto su aparición, pero ha abierto la caja de los truenos en el sentido que antes se tomaba la lista de los ficheros automatizados y se cubría. A día de hoy, había quedado mucha cosa en un segundo plano y, la salida del reglamento, que surgió antes que la ley, nos puso las pilas a todos”. Para Montoya, el GDPR emerge como un nuevo compañero dispone de un enfoque jurídico y sobre el que ha de arrojarse luz para saber cómo funciona, “ya que alguien que se acerque desde fuera a los sistemas tiene siempre ese escalón de incremento y una visión diferente. Los que hemos trabajado en sistemas o en seguridad previamente durante muchos años ya damos por sabido o por asumidas un montón de cosas, para que llegue alguien de fuera ajeno y nos diga cómo han de funcionar las cosas”. Para el director de seguridad de Aigües de Barcelona, la norrmativa europea en torno al dato ha cambiado el concepto del análisis de riesgos, “si bien llegado este punto emerge la necesidad de un enfoque más jurídico que ofrezca las claves de cómo funciona”, aseguró.

Efectuando un repaso de las responsabilidades que recaen sobre el organismo que dirige, Josué Sallent Ribes, director de la Fundació TIC Salut Social, del Instituto Catalán de la Salud, Centro de Competencia Tecnológica, afirmó que: “Somos

> “Antes, cuando se iniciaba un proyecto, nadie se preocupaba de la protección de los datos personales”



Carmen López, coordinadora de seguridad de la información de B Braun Medical.

Lluis Esteban, CDO de Caixabank.

> "GDPR ofrece transparencia a todos los clientes"

el DPO (Delegado de Protección de Datos, de sus siglas inglesas) de todo en el sistema de salud, actuando como entidad pública que es Catsalut y disponiendo en un segundo nivel de 176 proveedores diferentes". Este responsable explica que algunas compañías son propiedad de la Generalitat al 100%, mientras que otras son gestionadas por ayuntamientos así como por Cruz Roja. "Los datos fluyen entre estas 176 entidades, y tenemos centralizado algún repositorio como puede ser el historial clínico, e imágenes digitales junto con toda una serie de información. Cada uno de los proveedores tiene sus propios sistemas de información, por consiguiente, eso no significa que tengamos un DPD, sino que estamos montando un ecosistema de DPO". Asimismo, Sallent, explicó que la fundación gestiona 36 hospitales y, este año va a acabar con unos 500 incidentes la mayoría de los cuales son reclamaciones no atendidas a los ciudadanos y, en otros muchos casos, les llegan reclamaciones que pertenecen a otros ámbitos como el social. "Dentro de la Generalitat, cada departamento ha montado su DPD y mantenemos una coordinación estableciendo reuniones mensuales para analizar la problemática. Hay negocios en los cuales todavía no se han estrenado con ningún caso, mientras que en el día a día de nuestra entidad estamos desbordados".

Incidiendo en la complejidad que rodea el nuevo entorno digital en torno al dato,

> "La seguridad, lejos de representar un coste, debe ser contemplada como una inversión"

Xabier Mitxelena, managing director Iberia Cybersecurity de Accenture.

“El mercado de la información se caracteriza a su vez por la gran proliferación que está teniendo el dato”

Centrándose en la problemática que plantea el incremento del riesgo del dato en el momento actual, María José Pérez, directora de soluciones de seguridad del dato Iberia de Informatica, alude a las brechas de seguridad y las amenazas constantes procedentes de los nuevos *hackers* y sus intervenciones maliciosas en los sistemas. “Otro gran obstáculo que plantea el intento de mantener nuestro feudo protegido reside en la incipiente aparición de nuevas regulaciones y leyes que nos hacen cumplir continuamente en favor de la protección de esa información. El incumplimiento de tales normativas conlleva importantes sanciones económicas además de una pérdida de la credibilidad de la empresa”.

María José Pérez, directora de soluciones de seguridad del dato Iberia de Informatica.

Desde la perspectiva de la directora de soluciones de seguridad del dato de Informatica, el mercado de la información se caracteriza a su vez por la gran proliferación que está teniendo el dato, ya que estamos viendo cómo a través de nuevos dispositivos el volumen de datos se dispara, así como la tipología de datos en distintos dispositivos. “El uso de los datos coincidiendo con la gran proliferación de los mismos nos hace tener que identificar información sensible casi en tiempo real. Ya no nos sirve esa foto estática de aplicar un Excel para que registre la información contenida en la base de datos. Esta acción ya no nos sirve porque el gran volumen de información hace inmanejable todo el sistema”, declara Pérez.

Carmen López, information security coordinator de B Braun Medical, explicó que el control del mismo en el pasado era un procedimiento relativamente sencillo. “Se nos ha complicado bastante la gestión porque su tratamiento y protección son tareas mucho más subjetivas en un entorno más complejo y diverso”. Esta directiva afirma que en un sector como el farmacéutico que está entrando de lleno en la digitalización y en entornos mucho más abiertos y colaborativos con instituciones sanitarias y administraciones públicas, “cada vez que nos planeamos un análisis nos resulta mucho más complicado. Lo positivo que se desprende de la publicidad que se dio al GDPR a nivel doméstico ha impactado muy bien también en el sector empresarial. Lo cual significa que, si el ciudadano es más consciente de los derechos que tiene, aunque luego no los ejerza, ayuda mucho en la concienciación en su puesto de trabajo, y eso a las organizaciones también nos ayuda porque siempre tenemos personas dentro de los departamentos que son mucho más sensibles a nivel individual con sus datos personales y nos hacen de dinamizadores dentro de la propia organización”. Con respecto a la LPD y el GDPR,

Gloria Saavedra, directora de sector retail, utilities, travel y pharma de Informatica.

> "Los negocios han de evolucionar para alcanzar el control de la información, que tanto nos preocupa"

Carmen López dijo haber notado que en los departamentos se producen muchas más consultas cuando se inicia un proyecto, lo cual antes no pasaba. "Anteriormente, cuando se iniciaba un proyecto, nadie se preocupaba de la protección de los datos personales, ni tampoco de la protección del dato, de manera que ahora se nos complica mucho la gestión. Pero el lado positivo es que tenemos muchos más aliados en este sentido".

En cuanto a las nuevas maneras de protección al dato Evaristo Ruiz, CTO de Deutsche Bank, aseveró que securizar datos es una actividad que su organización viene haciendo desde hace bastante tiempo. "No obstante, lo que sí nos ha cambiado notablemente, al menos en el sector financiero, han sido los procedimientos que utilizamos a la hora de comunicar los datos de que disponemos a la autoridad, en nuestro caso, al Banco de España, ya sean de clientes o bien datos empresariales". Ruiz indica que han de redactar tantos informes que necesitan disponer de mecanismos que aporten coherencia interna los datos, saber qué es lo que se reporta y hacerlo correctamente. "Estos procedimientos han llevado a Deutsche Bank a un replanteamiento de los procesos que realizaba con los sistemas de información que

> "En el sector financiero han cambiado los procedimientos de comunicación de los datos que disponemos"

Evaristo Ruiz, CTO de Deutsche Bank.

Rubén Garrido, CIO de Electrodomestics Candelsa.

> "Es imprescindible dotar al dato de las medidas necesarias para evitar cualquier mal uso o pérdida de información"

tenía, teniendo en cuenta que debían mantener un nivel de coherencia interna, buscando la información que solicitan, lo cual ha supuesto un gran reto, según expresó. "Por un lado, estos datos tenían que facilitarse a las entidades reguladoras, como ha sido tradicional hacerlo con el Banco de España, pero también ha surgido como novedad que lo hagan otros miembros. Tenemos la directiva de los sistemas de pago que, de alguna forma, nos obliga a comunicar información económica sobre clientes en condiciones muy determinadas, siempre bajo la autorización del cliente". Para Evaristo Ruiz, esta situación compromete a las entidades financieras de cara a los clientes a la hora de utilizar y compartir hasta donde se pueda y, sobre todo, su securización".

Para Marc Paus, CISO de Fira de Barcelona, la concienciación de mantener salvaguardado el elemento privado está ayudando a empresas como Fira de Barcelona, que dispone de infinidad de aplicaciones, a que la gente empiece a requerir medidas de protección de los datos en la puesta en marcha de proyectos relacionados con la recopilación de datos biométricos. "Tenemos muchas pruebas piloto para detectar si en un *stand* de un salón determinado acuden visitantes, de quienes se detecta su es-

> "Estamos percibiendo un notable crecimiento de los presupuestos de seguridad"

Marc Paus, CISO de Fira de Barcelona.

Josué Sallent Ribes, director de la Fundación TIC Salut Social del Instituto Catalán de Salud.

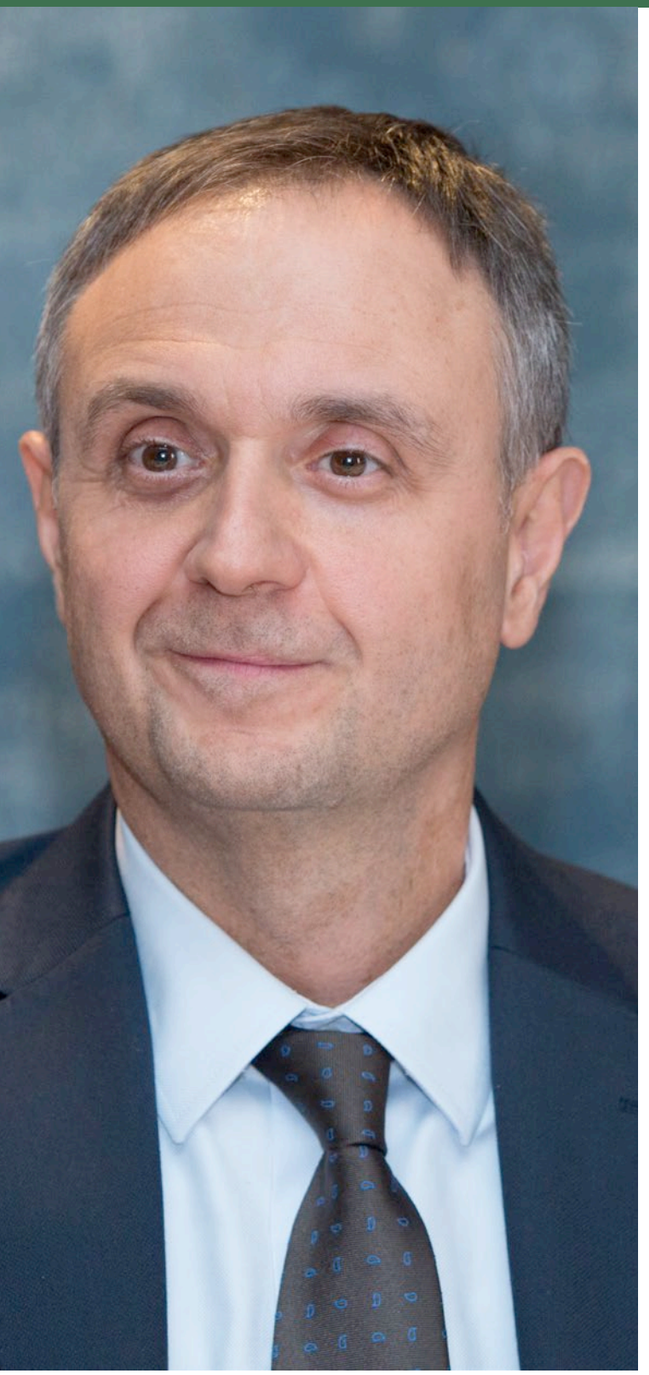
> "Cada departamento de la Generalitat tiene su propio delegado de protección de datos"

tado de humor al visitar el *stand*... todos estos datos suponen información muy sensible que hemos de proteger". Paus explica que algunos grandes eventos tanto internos como externos, como el Mobile World Congresss, también requieren de la presencia de elementos de internet de las cosas con la finalidad de monetizar el dato. "Los requerimientos que plantean las circunstancias regulatorias y de protección del dato representan un gran reto para nosotros. No obstante, empezamos a notar, tanto BPO como yo mismo, que nos empiezan a preguntar los departamentos acerca de la salvaguarda de información sensible, y también estamos percibiendo por parte de dirección general un notable incremento en los presupuestos de seguridad".

Con respecto a la labor relacionada con la protección de los datos, Lluís Esteban, Chief Data Officer de CaixaBank, afirmó que es una función que desde siempre se ha atribuido a los bancos, dado que el mantenimiento de la confidencialidad y la seguridad de la información representa la máxima instancia a efectos de responsabilidad. "Por lo tanto, estos factores constituyen el ADN de las organizaciones financieras. Estamos adaptados a la LOPD (Ley Orgánica de Protección de Datos) quienes mantienen unos controles muy estrictos, mientras que GDPR lo que ofrece a todos los clientes es un efecto de transparencia, algo de lo que hasta ahora el cliente no era tan cons-

> "Utilizamos el dato para aportar valor a los clientes"

Marc Planas, CIO de La Sirena Alimentación Congelada



David Ortiz, CIO de Mecalux.

> "La concienciación sobre la importancia del dato no ha hecho más que empezar"

ciente, mientras que ahora puede decidir lo que se puede hacer o no con sus datos, y también cómo se utilizan los datos y para qué". Esteban señala haber experimentado un gran cambio en la compañía en torno a los analistas y gestores de los datos, quienes preguntan qué tratamientos pueden aplicar y bajo qué condiciones. "Ahora solicitan información relativa al tipo de negocio que se quiere hacer y para qué se pueden utilizan los datos. Para nosotros todo el sistema informacional es *core*, y creo que la protección y el gobierno del dato es un paradigma que tiene que ver con la revolución de la información que plantea *big data* y todo lo que ha surgido alrededor que hace necesaria la aplicación de normativas de protección de los datos como el GDPR".

Desde una visión que mantiene al dato como elemento fundamental para el desarrollo de un negocio y el mantenimiento de la fidelización de los clientes, Marc Planas, CIO de La Sirena Alimentación Congelada, señaló que "para una empresa de *retail* como la nuestra, hacer un uso correcto del dato es fundamental para aportar valor. Por fortuna, no disponemos de datos que sean de estricta confidencialidad, ni tampoco tenemos que reportar a entidades reguladoras. En cualquier caso, no tenemos ningún interés en compartir el dato con terceros, sino que los queremos para aportar valor a nuestros clientes". Planas explica que el mundo del *retail* es muy competido,

> "Hemos adoptado los máximos estándares de todas las normativas del mundo"

Víctor Funes, director of digital health de Roche Diagnostics.

"un mundo en el que el dato resulta fundamental en nuestro sector. Disponemos de muchas referencias de congelados y, si pretendemos diferenciarnos de un supermercado generalista, tenemos que hacer uso de la información, comunicar nuestros productos a nuestros clientes, y ofrecerles la posibilidad que nos comenten cómo les podemos ayudar a la hora de elegir, por ejemplo, un salmón determinado de nuestras 20 referencias de catálogo. Este experto señala que ello les brinda la posibilidad "no solo de recomendar las ofertas o las promociones, que es en lo que todos pensamos cuando una firma como la nuestra bombardea a los clientes, sino que también les ofrecemos consejos y novedades. Para Marc Planas, la estrategia y casi la supervivencia en muchos casos, salvo si se trata de grandes *retailers*, pasa por cómo hacemos uso de los datos. Asimismo, Marc Planas señala como fundamental todo lo relativo a la seguridad del dato, con la finalidad de ser estrictos en el cumplimiento de todos los requisitos legales.

Por su parte, David Ortiz, CIO de Mecalux, apeló a la evolución del dato como elemento de gran importancia para las organizaciones. "No hace muchos años atrás,

el dato no tenía tanta transcendencia, de hecho el dato tiene sentido cuando lo podemos transformar desde las empresas en información para tomar decisiones, para fidelizar a nuestros clientes y para sacarle valor económico. Ortiz afirma que, a nivel global, la concienciación en la importancia del dato se ha visto incrementada en un proceso que no ha hecho más que empezar. "En su día, cuando arrancó el RGPD, contratamos para el departamento de IT a un abogado especialista para llevar los temas relacionados con la contratación en el mundo tecnológico, pero también para que se ocupase de todo lo relacionado con la protección de los datos. Cuando la concienciación de la organización pudo asumir a nivel legal esta responsabilidad, esta persona pasó a formar parte del departamento legal con dos activos muy importantes: el conocimiento legal de las normativas, pero resulta fundamental conocer la compañía y también los sistemas de información que maneja. Creo que no puede haber una cosa sin la otra, ya que en el caso concreto de Mecalux estos temas se llevan de una manera totalmente colaborativa entre el departamento legal e IT, y vamos de la mano porque por separado no podríamos

conseguirlo. “Otro aspecto interesante de la llegada del GDPR es que a nivel de presidencia de la empresa también se habla de estos temas, ya que damos servicio a nuestros clientes en sus instalaciones automáticas de almacenes de monitorización y seguimiento, lo cual requiere un plus de seguridad que garantice que los datos del cliente no van a salir fuera”.

Víctor Funes, director of digital health de Roche Diagnostics, hizo mención al gran volumen de datos que maneja la entidad por su especialización en el entorno de la salud, con lo cual plantea dos visiones a tener en cuenta en torno al dato: “la primera es la interna, la de los empleados de la propia compañía; y la segunda es esa visión externa de cuando somos *partners* o proveemos servicios al mercado, ¿qué situación debemos abordar para acercarnos de la manera correcta?”, se cuestionó Funes. El director of digital health de Roche Diagnostics de Roche señala que el cumplimiento de GDPR así como de las normativas de Estados Unidos y China han obligado a

Roche a adoptar los máximos estándares de todas las normativas de todos el mundo, lo cual hace que el nivel de exigencia sea muy alto. “En nuestra compañía se ha empezado a hablar del dato personal, y también de la importancia del dato dentro del contexto de nuestro negocio en general. En este sentido, acabamos de certificar en la 27000 1 y en el esquema nacional de seguridad, donde se trata no solamente el dato personal sino también la clasificación de los diferentes tipos de información. Todo ello con un nivel de exigencia muy alto, porque es complicado aislarnos del resto del mundo, y tenemos que empezar a hablar de cómo interactuamos con los ciudadanos”. Desde la perspectiva de Funes, los datos relativos a la salud de las personas no son del hospital ni del médico, sino que pertenecen al paciente. “Junto con ello, Víctor Funes apela a tener en cuenta cómo utilizamos estos datos para entrenar a sistemas de inteligencia artificial y que luego redunden en un beneficio para la salud, en un contexto que todavía no ha sido creado con el propósito de generar un nuevo modelo de servicio. **CSO**