ENCUENTROS **ITDM GROUP**

VENTAJAS Y RETOS DE LA NUEVA ERA DEL DATO

©freepik

ORGANIZA

PATROCINADORES GOLD

PATROCINADORES SILVER

VENTAJAS Y RETOS DE LA NUEVA ERA DEL DATO

El dato es el nuevo oro en la era del conocimiento, ya que permite a las empresas mejorar su forma de trabajar, comprender mejor a sus clientes y diferenciarse de la competencia. Muchas organizaciones están tratando de sacar más provecho a la información que manejan, llevando a cabo una transformación hacia modelos operativos y de negocio impulsados por datos, un camino lleno de oportunidades, pero también de nuevos retos.

El progreso digital está introduciendo muchos cambios en las organizaciones, y uno de los más significativos es el creciente volumen de datos que proviene de sus operaciones y de las interacciones con sus clientes y con toda su cadena de valor. Tradicionalmente, esta información se ha recopilado y utilizado de forma separada en cada área del negocio, acumulando infinidad de datos estructurados y no estructurados en diferentes silos, sin una estrategia u objetivo común. Pero la necesidad de adaptarse a las cambiantes condiciones del mercado está obligando a las empresas a replantear el modelo de aprovechamiento del dato.

Ahora, muchas organizaciones comprenden que los datos son un activo de gran valor que puede explotarse para optimizar sus operaciones, comprender mejor al cliente e impulsar la toma de decisiones a todos los niveles. Lograr esto va más allá de cambiar la forma de recopilar y analizar los datos, ya que supone un cambio disruptivo en la forma de trabajar y hacer negocios, adoptando un modelo data-driven. Las empresas españolas están invirtiendo en procesos de transformación de datos y las más avanzadas están mejorando su eficiencia y su competitividad. Pero en este camino se han encontrado con numerosos desafíos relacionados con el cambio de la cultura empresarial, la gestión de datos, la adopción de nuevas tecnologías y la seguridad de la información.

ENCUENTROS ITDM GROUP >> Analizamos cómo las empresas están aprovechando cada vez más el dato para impulsar la transformación de su negocio hacia un modelo data-driven, las oportunidades y retos que surgen en esta transición y qué tecnologías ayudarán a explotar y proteger mejor los activos de datos.

TRANSFORMACIÓN DATA-DRIVEN

Convertirse en una empresa impulsada por datos implica llevar a cabo una profunda transformación que se apoya en varios pilares. Por un lado, se debe cambiar el modelo de gestión de datos, abarcando su recopilación, almacenamiento, clasificación y análisis para determinar su naturaleza y su criticidad para el negocio. En este sentido, las organizaciones más evolucionadas han buscado una unificación del dato, rompiendo paulatinamente los silos tradicionales y los que se pueden generar en nuevos entornos de TI como la nube o los despliegues IoT. El objetivo es crear una única verdad en lo que se refiere al dato para que todos trabajen con la misma información y puedan aportar conocimiento valioso al resto de la organización, de una forma dinámica y transparente. Esto permite crear un modelo de toma de decisiones basado en datos que llega desde la parte operativa a la de negocio.

Cada sector y cada empresa tienen su propia idiosincrasia y avanza hacia la digitalización a un ritmo diferente y por distintos caminos, por lo que no existe un modelo único para todas las empresas. Por ello, los expertos recomiendan llevar a cabo una exhaustiva planificación de esa estrategia data-driven, y para muchas organizaciones es necesario contar con socios tecnológicos que puedan aportar conocimiento y experiencia, y que se impliquen en el proyecto desde el diseño.

Esto se complica mucho en redes empresariales ampliamente distribuidas y de alcance internacional, donde los datos están repartidos entre centros de datos on-premise, cloud y de terceros en diferentes regiones. Estas arquitecturas añaden

gran complejidad y puntos débiles en materia de gobernanza y seguridad, y es vital que todos los implicados trabajen bajo un mismo paraguas para evitar riesgos. En esto tiene un papel clave la figura del responsable de datos, que debe conocer a fondo las necesidades tecnológicas de la organización sin perder de vista los objetivos del negocio.

NUEVOS ROLES EN LA GESTIÓN DE DATOS

La figura del responsable de datos, análisis o inteligencia artificial surgió en la primera década de este siglo en ciertos sectores como la banca, y se ha ido extendiendo a otras industrias a medida que ha avanzado la digitalización y han evolucionado tecnologías transformadoras como la IA. El cargo de Chief Data Officer (CDO) está cada vez más extendido, pero en los últimos años sus funciones han ido ampliándose, dando lugar a nuevas denominaciones como el Chief Data and Analytics Officer (CDAO) o el Chief Digital & Artificial Intelligence Officer (CDAIO).

> **CONVERTIRSE EN UNA EMPRESA DATA-DRIVEN IMPLICA LLEVAR A CABO UNA PROFUNDA TRANSFORMACIÓN**

Estos roles tienen gran importancia en la transformación hacia modelos de negocio impulsados por datos, y están cambiando su enfoque original, centrado en el control de la información y del riesgo, por uno más vinculado a los resultados comerciales. Su posición como responsables de datos y tecnologías asociadas hace que tengan un mayor peso en la toma de decisiones de compra de tecnología, pero no siempre cuentan con el respaldo de la dirección. En un artículo publicado recientemente por Harvard Busines Review, Randy Bean, experto de la consultora Wavestone, explica que los líderes de datos necesitan redirigir su estrategia tradicional, centrada en la tecnología y la infraestructura, hacia los resultados comerciales, considerando casos de uso con potencial de éxito. Esto impulsa la confianza de la dirección en las inversiones en datos, análisis e IA, y ayuda a revalidar su apuesta por la tecnología relacionada.

CALIDAD DE LOS DATOS

De nada sirve diseñar una estrategia data-driven para transformar el modelo de negocio si los datos en que se apoya no son los adecuados. Gran parte de la información que manejan las empresas no tiene un valor significativo, y lo principal para los responsables de datos es identificar los datos útiles y garantizar su calidad para que la toma de decisiones se base en información verídica, precisa y aprovechable. El primer paso para asegurarse de que la información es de calidad debería ser clasificar los datos y comprender lo que representan, para después aplicar técnicas de analítica que extraigan de ellos el conocimiento realmente útil.

Jason Medd, director analista de la consultora Gartner, comenta en un artículo que los problemas de calidad de los datos pueden tener un alto coste, pero afirma que “no son difíciles de solucionar y no se requiere mucho tiempo”. En su opinión, es vital que los líderes de datos (CDO, CDAO, etc.) cuenten con buenos programas Data Quality para evitar complicaciones y no perder oportunidades. Sus investigaciones revelan que “para 2024, el 50% de las organizaciones adoptarán soluciones modernas de DQ para respaldar mejor sus iniciativas comerciales digitales”.

En Gartner aconsejan a los CDAO centrarse en los datos que influyen en los resultados comerciales, comprendiendo los KPI clave de rendimiento y los indicadores de riesgo (KPR), que construyan un caso comercial y busquen un lenguaje común para establecer estándares de calidad de datos. Una vez establecidas las bases, se debería aplicar responsabilidad sobre la calidad de los datos, estableciendo administradores de datos provenientes de las unidades comerciales y del equipo de datos y análisis. A continuación, Gartner recomienda mejorar la calidad de los datos creando perfiles de datos sujetos a monitorización y mejora constante, y hacer una transición a un modelo de gobierno basado en la confianza en los datos.

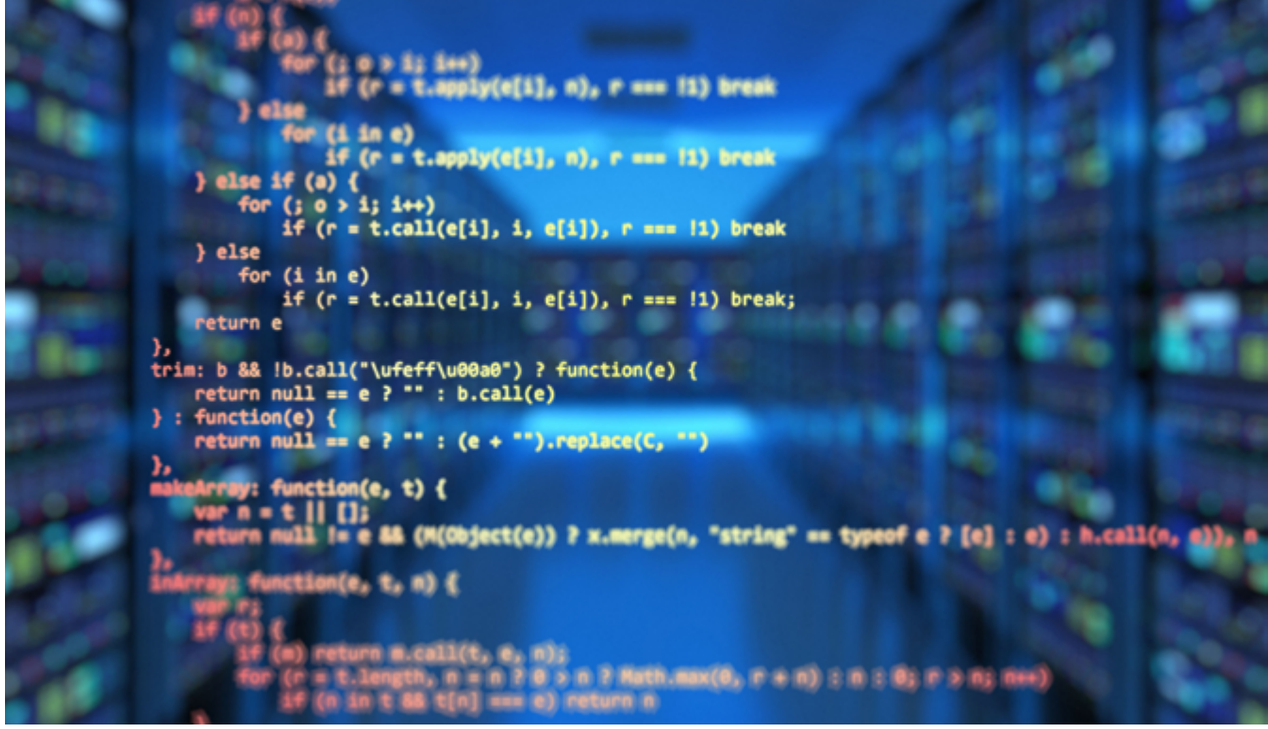
La última categoría de acciones a llevar a cabo es la integración de la calidad de los datos en la cultura corporativa. Para ello aconsejan emplear tecnología para reducir el trabajo manual relacionado con los datos y mejorar el rendimiento en el trabajo con información. Esto requiere que los CDAO dediquen más esfuerzos en la alfabetización de datos en toda la empresa e incentiven la colaboración y el intercambio de conocimiento.

GOBERNANZA Y SEGURIDAD EN LA ERA DE LA IA

Uno de los principales retos en el camino hacia modelos data-driven es diseñar una estrategia de gobernanza de datos capaz de impulsar esta transformación y garantizar el cumplimiento normativo, ahora y en el futuro. La ley marca el camino a seguir en lo que se refiere al almacenamiento, la gobernanza y la seguridad de los datos, pero no basta solo con cumplir con la regulación. Es necesario mantenerse al día constantemente a nivel legal, pero también tratar de ir un paso por delante para que la organización pueda adaptarse a los futuros cambios con el suficiente dinamismo.

Cuando se añade la inteligencia artificial a la ecuación, y especialmente la IA generativa, todo se complica y es vital diseñar una estrategia de datos e IA que permita seguir explorando las posibilidades de esta tecnología en el futuro. Esto implica garantizar el cumplimiento con las regulaciones de privacidad y seguridad de los datos, propiedad intelectual y otros factores vinculados a los datos.

En opinión de Avivah Litan, vicepresidenta analista en Gartner, “Las organizaciones deben actuar ahora para formular una estrategia en toda



la empresa para la gestión de la confianza, el riesgo y la seguridad de la IA (AI TRiSM)”. Aunque explica que, por el momento, “no hay en el mercado herramientas que ofrezcan a los usuarios garantías de privacidad sistemáticas” o un filtrado efectivo “de errores, alucinaciones, materiales protegidos por derechos de autor o información confidencial”. Por ello, dice que los desarrolladores de IA deberían trabajar con los legisladores para “establecer políticas y prácticas para la supervisión y la gestión de riesgos de la IA generativa”.

En este Encuentro ITDM Group, titulado “Ventajas y retos de la nueva era del dato”, analizamos todas estas cuestiones con representantes de empresas de diversos sectores, incluyendo a importantes proveedores de tecnología. Lo hacemos a través de dos mesas redondas temáticas y tres entrevistas con expertos en datos, inteligencia artificial, business intelligence y ciberseguridad, que nos hablan de su experiencia y de las oportunidades y retos que acompañan a esa transformación hacia modelos operativos y de negocio impulsados por datos. ■

MÁS INFO +

» Encuentro ITDM Group

» Acciones para mejorar en Data Quality

COMPARTIR EN REDES SOCIALES

making science

THE DIGITAL ACCELERATION COMPANY™

« FROM DATA CHAOS » TO AI CLARITY

USA, UK, Spain, Ireland, France, Italy, Portugal,
Germany, Sweden, Denmark, Mexico, Colombia.

www.makingscience.es

JAVIER ECHÁNIZ, SOCIO Y RESPONSABLE DE DATA E INTELIGENCIA ARTIFICIAL, DELOITTE

“Gran parte de los beneficios y riesgos de la IA generativa están todavía por explorar”

En la primera entrevista enmarcada en este Encuentro ITDM Group hablamos con Javier Echániz, socio y responsable de Data e Inteligencia Artificial en Deloitte. Nos explica cómo está impactando la inteligencia artificial en la forma de trabajar de las empresas con la información y qué riesgos plantea el uso de la IA generativa. Opina que las organizaciones pueden encontrar muchos beneficios en sus procesos gracias a la automatización y la IA generativa. También considera que este tipo de IA puede transformar el engagement de los clientes y de los empleados, y habilitar la hiper-personalización, generando “contenido mucho más adaptado a las características de las personas, desde un punto de vista de vídeo, de voz, de texto, etcétera”.

Echániz cree que estamos en un momento de gran disrupción, como

ENTREVISTA >> Javier Echániz nos habla del potencial y los riesgos del uso de IA generativa y de las últimas tendencias en cumplimiento y gobierno del dato.

cuando surgieron los smartphones, "donde también existe la posibilidad de crear diferentes aplicaciones relacionadas con innovación, con nuevos ámbitos para las compañías, nuevas fuentes de ingresos o de innovación", como aplicando la IA generativa al desarrollo de productos tecnológicos, industriales y a la generación de documentación relacionada.

RIESGOS ASOCIADOS A LA IA

En Deloitte destacan los riesgos relacionados con la propiedad intelectual ya que, aunque muchas plataformas de IA generativa están cediendo los derechos sobre el contenido, "empieza a haber controversia con algunas plataformas de generación de vídeo o de foto". Por otro lado, Echániz muestra preocupación por otros temas, como "la trazabilidad de los datos de la información, dónde reside, y cómo se van a utilizar estos datos que ponemos a disposición de estas plataformas". Otro problema proviene de que la IA generativa está diseñada para satisfacer las preguntas que se le plantean, y esto no siempre se hace con veracidad, generando el denominado "riesgo de alucinación". Por último, está el modelo de costes que se aplique, y cómo integrar este tipo de herramientas en el ecosistema de las compañías.

En opinión de Echániz, las organizaciones están tratando de establecer su propio marco ético, intentando situarse por encima de lo que previsiblemente marcarán las futuras leyes, ya que necesitan demostrar que son confiables en todo lo que se refiere al uso del dato y la inteligencia artificial. Considera que "en todo este proceso de automatización, de generación del engagement, etcétera, tiene que haber un proceso de transparencia: en qué se está utilizando, cómo se está supervisando, cómo se está controlando el uso de la inteligencia artificial dentro de las compañías".

TENDENCIAS EN TORNO AL DATO

El cumplimiento normativo, la gobernanza de datos y los riesgos asociados a las nuevas tecnologías como la IA generan preocupación, y en Deloitte cuentan con grupos especializados que están monitorizando y colaborando con organismos públicos para ver cómo se pueden implantar estas tecnologías. Echániz reconoce que en Europa se ha dado un gran paso adelante con las últimas directivas aprobadas, mientras en Estados Unidos van más rezagados, aunque moviéndose en la dirección correcta. Por su parte, las empresas están trabajando en el modelo de tratamiento de los datos, la privacidad y el propósito del uso de inteligencia artificial. En sectores como el financiero también surgen preocupaciones sobre la trazabilidad de los datos y la explicabilidad de los procesos y lo modelos de IA.

> "ES FUNDAMENTAL INCREMENTAR LA COLABORACIÓN ENTRE EMPRESAS Y UNIVERSIDADES PARA GENERAR MÁS TALENTO"
>
> **JAVIER ECHÁNIZ,** socio y responsable de Data e Inteligencia Artificial en **Deloitte**

Al mismo tiempo, muchas compañías están teniendo problemas derivados de la escasez de talento, ya que las universidades no están logrando generar el suficiente volumen de profesionales con carreras STEM. Esto supone un freno para la implantación de nuevas tecnologías como la IA, y Echániz considera fundamental la colaboración de las empresas y los centros de enseñanza superior para ser capaces de generar cada vez más talento en disciplinas como matemáticas o ingeniería.

Destaca que el teletrabajo "está proporcionando también la posibilidad a profesionales españoles de poder trabajar para empresas internacionales y eso eleva todavía más el listón para poder atraer y desarrollar el talento en nuestro país". Opina que no basta con contratar a nuevos profesionales, sino que también es fundamental llevar a cabo un plan de reskilling para todos los perfiles de la compañía, para lo que se necesita el apoyo de la alta dirección y la adaptación de los modelos organizativos. ■

MÁS INFO +

» Encuentro ITDM Datos

» Deloitte

COMPARTIR EN REDES SOCIALES

HYPERINTELLIGENCE®

Las respuestas
le encontrarán

MicroStrategy®
Intelligence Everywhere

ESTRATEGIAS PARA UNA EMPRESA POTENCIADA POR LOS DATOS

Aprovechar los datos para reforzar la toma de decisiones, agilizar la respuesta al mercado, mejorar los procesos internos, optimizar la cadena de suministro y los canales de atención a los clientes, y maximizar los objetivos del negocio, son algunas de las características que definen a las organizaciones data-driven.

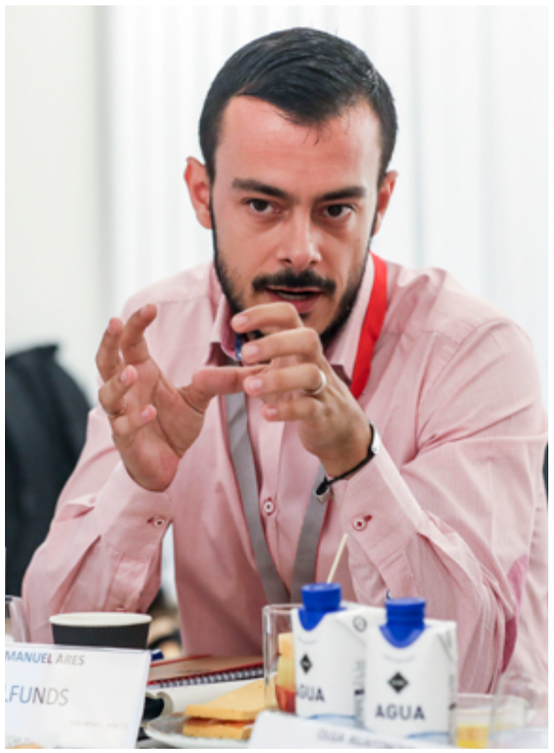
¿Cómo gestionan las compañías las estrategias de datos en su proceso para convertirse en entidades data-driven? **Aedas Homes, AllFunds, Atlético de Madrid, Axpo Iberia, Banco Caminos, Beam Suntory, Eptisa, Logista, Nationale Nederlanden España, Singularu y Venca**, aportaron su visión en un Encuentro de la Comunidad IT que, apoyado por **Making Science y MicroStrategyCo**, forma parte del programa "Ventajas y retos de la nueva era del dato".

En el análisis de la situación de las estrategias de datos en las organizaciones participantes, uno de los primeros pasos y retos que se plantean es la **integración de datos**. Ángel Rodríguez Chicote, Head of Data de Singularu, comercializadora de joyas

MESA REDONDA >> En este Encuentro de la Comunidad IT conversamos sobre cómo potenciar una organización data-driven de la mano de Aedas Homes, AllFunds, Atlético de Madrid, Axpo Iberia, Banco Caminos, Beam Suntory, Eptisa, Logista, Nationale-Nederlanden España, Singularu y Venca. La cita contó con la colaboración de Making Science y MicroStrategy.

> LOS DATOS NO SIEMPRE SON IGUALES PARA TODOS LOS DEPARTAMENTOS; ES NECESARIO TENER EN CUENTA TODAS LAS VISIONES

JORGE VALERO ELÍAS,
Director de Aplicaciones y Data de **Aedas Homes**



> HAY QUE ELIMINAR LAS BARRERAS PARA EXPLOTAR LOS DATOS, ACABANDO CON LOS MUROS ENTRE IT Y NEGOCIO

JUAN MANUEL ARES SANTIBÁÑEZ,
Head of Data de **AllFunds**

con más de 180 proveedores locales, destacó que el hecho de trabajar con "muchas terceras partes dificulta la integración de los datos. En ocasiones, diferentes fuentes proporcionan distintos datos, de ahí la importancia de contar con un adecuado gobierno del dato. Necesitaríamos una gran cantidad de recursos. Así que estamos consolidando las fuentes en Google Cloud y tomamos todas las decisiones en virtud de estos datos. Aun así, todavía nos queda camino por recorrer".

En términos similares se pronunció Juan Manuel Ares Santibáñez, Head of Data de AllFunds, firma que desarrolla soluciones digitales para la cadena de valor de la distribución de fondos financieros, si bien también se refirió a los datos procedentes del cliente interno: "antes, cada división tenía sus propios datos, pero ahora esta información afecta realmente a toda la compañía. Es esencial consolidar el dato para poder explotarlo. Además, como los

diferentes proveedores proporcionan los datos de distinta manera, es imprescindible normalizarlo para poder obtener valor de la información. En ese punto estamos nosotros. Hay que eliminar las barreras para explotar los datos, acabando con los muros entre TI y negocio, un paso que es fundamental para todas las empresas".

Desde Axpo Iberia, productora de energía, su CIO Ángel Matía Huélamo detallaba su experiencia en ese pro-

> SE DEBE DEFINIR LO QUE ES ESTRATÉGICO Y PRIORIZAR EN FUNCIÓN DEL RESULTADO, LA NECESIDAD Y LOS OBJETIVOS REALES

ÍÑIGO LÓPEZ PÉREZ,
Head or Data & Analytics de **Atlético de Madrid**

> PERMITIMOS A LOS USUARIOS DEFINIR SUS PROPIOS MODELOS, PORQUE NO QUEREMOS QUE DEJEN DE ACCEDER A LOS DATOS SI VEN LA TECNOLOGÍA COMO UNA BARRERA

ÁNGEL MATÍA HUÉLAMO,
CIO de **Axpo Iberia**

Clica en la imagen para ver la galería

pósito de consolidación: “nosotros intentamos normalizar los datos de nuestras 5 compañías, pero cada una tiene diferentes necesidades. El primer intento fue poner en marcha un proyecto muy ambicioso, y fallamos. Ahora estamos consolidando y enseñando a los usuarios a obtener valor de los datos, con lo que está funcionando mucho mejor, porque aportamos valor de forma rápida, lo que motiva cada día más a los usuarios. Este enfoque más minimalista está funcionando mucho mejor. La metodología está bien, pero lo mejor es trabajar con un modelo incremental. Nosotros hemos centralizado todo, pero sin consolidar un modelo de datos, y en eso TI puede ayudarnos”.

Clica en la imagen para ver la galería

En un proyecto similar se encuentran en Eptisa, multinacional de ingeniería y consultoría. “Estamos inmersos en un proyecto de consolidación de datos. De hecho, tenemos algunos datos normalizados, pero no centralizados. Tenemos que seguir avanzando en esta línea, porque tenemos diferentes fuentes y no siempre coinciden”, explicó su CIO, Carlos Merino.

También las fusiones entre empresas obligan a integrar datos. Es el caso de Beam Suntory, comercializadora de bebidas espirituosas con marcas en España como Larios, Brugal, DYC y Centenario. Según Olga Agafonova, BI & Data Manager para EMEA & SA de la compañía, “nosotros tenemos muchas fuentes de datos, y la consolidación es compleja. Estamos trabajando en crear un

> EL USUARIO DEBE APRENDER A USAR EL DATO Y TIENE QUE SER RESPONSABLE DE SU APROVECHAMIENTO

ÁLVARO EGEA ALONSO,
Director Corporativo de Tecnología e Innovación de **Banco Caminos**

> TI POSEE EL DATO, PERO EL RESPONSABLE DE SU DESARROLLO DEBE SER NEGOCIO. POR ESO HAY QUE ASEGURAR LA CALIDAD DEL DATO Y CONTAR CON UN RESPONSABLE DE NEGOCIO EN CADA PROYECTO

OLGA AGAFONOVA,
BI & Data Manager para EMEA & SA de **Beam Suntory**

Clica en la imagen para ver la galería

data hub entre divisiones y países para ver cómo podemos explotarlos. La integración de la compañía en España, tras la compra de Maxxium, ha sido compleja, y ponemos ahora mucho foco en los datos para dejar atrás una orientación más antigua".

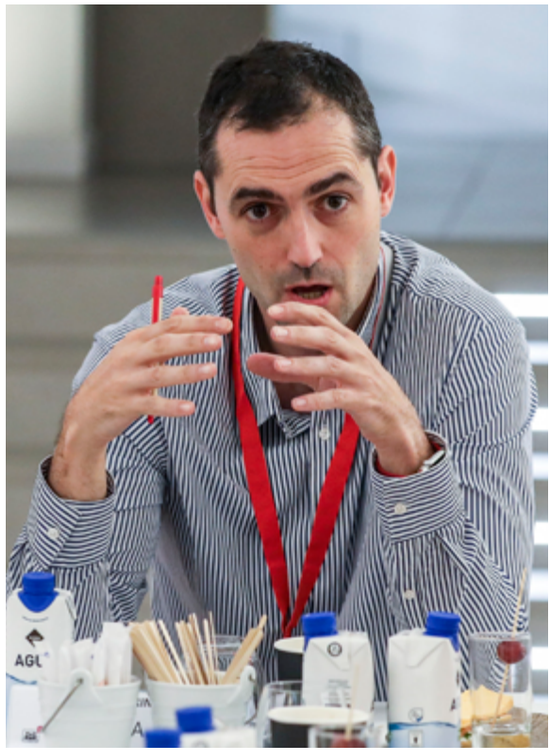
EJES PARA AMPLIFICAR EL VALOR DEL DATO

Además, de la integración, también se necesitan otros elementos para diseñar esas estrategias data-driven. David Sanz Bascuas, Head of Corporate Business Intelligence de Logista, uno de los mayores operadores logísticos del sur de Europa, especializado en la distribución a canales de proximidad, opinó que "antes las empresas optaban por adquirir hardware, pero alguien se dio cuenta de que el valor

Clica en la imagen para ver la galería

estaba en los datos, que es necesario que estén consolidados y organizados. Para esto se precisan roles específicos, como el **CDO**, porque si no, es muy complicado. El elemento diferenciador actual es que la estrategia parta del comité de dirección. En nuestro caso, estamos en un proceso de digitalización bastante profundo y vemos en el dato tanto valor que, incluso, hemos creado una división para comercializarlo. Todavía no estamos en ese punto en todos los aspectos de la estrategia, pero sí hemos alcanzado un nivel suficiente para monetizarlo".

Fernando Fracchia, BI and Data Science Manager de Venca, firma con más de 30 años de experiencia en la venta de moda, textil y hogar a través de catálogo e Internet, añadió nuevos



> ES ESENCIAL AVANZAR EN LOS PROCESOS DE CONSOLIDACIÓN Y UNIFICACIÓN DE DATOS

CARLOS MERINO DÍAZ,
CIO de **Eptisa**

> LAS EMPRESAS EMPIEZAN POR PROCESOS INTERNOS Y, A ÚLTIMA HORA, INTEGRAN A LOS USUARIOS Y LOS CUADROS DE MANDO. PERO ¿NO SERÍA MÁS INTERESANTE HACERLO A LA INVERSA, EMPEZANDO POR LAS NECESIDADES DE LOS CLIENTES?

DAVID SANZ BASCUAS,
Head of Corporate Business Intelligence de **Logista**

ingredientes al exponer su caso: “tras dos años de trabajo en la normalización del dato, ya somos digitales casi al 100%. Hemos pasado de la venta por catálogo al e-commerce y la digitalización. Para ello, establecimos un roadmap preciso con todos los detalles para avanzar en la **gobernanza del dato** y crear plataformas de democratización del dato, con el objetivo de ponerlo a disposición del cliente, que es el último paso. Ahora estamos incrementando el nivel de análisis para amplificar el valor del dato. No es un proceso sencillo, hay que ir paso a paso, adaptando la tecnología a lo que necesitamos y no al revés, y definiendo cuál es la mejor solución y el proveedor adecuado”.

Álvaro Egea Alonso, Director Corporativo de Tecnología e Innovación de Banco Caminos, especialistas en banca privada y personal, insistió en el concepto de cultura. “Teníamos el dato muy desperdigado y con una organización muy anárquica. Es imprescindible contar con una adecuada **cultura del dato**. El usuario debe aprender a usarlo y debe ser responsable de su aprovechamiento. Hasta hace cuatro años teníamos muchos informes manuales, que provocaban que los usuarios no pudieran poner el foco en los clientes. Además, cuando se tiene la obligación de controlar el dato, debe existir el compromiso de la organización, que debe favorecer el uso de la información de forma ordenada. No se trata solo de definir un data owner, sino de profundizar en su uso para obtener valor. De hecho, la lupa con la que se

> ES CLAVE FORMAR A LAS PERSONAS DESDE EL PRINCIPIO. EN NUESTRO CASO LO HICIMOS ASÍ Y HA SIDO TODO UN ÉXITO

DAVID VAQUERO LÓPEZ,
Chief Technology Officer de
Nationale-Nederlanden España

> CONTAR CON DIFERENTES FUENTES DE DATOS EXIGE UN ADECUADO GOBIERNO DEL DATO

ÁNGEL RODRÍGUEZ CHICOTE,
Head of Data de **Singularu**

Clica en la imagen para ver la galería

mira el dato es la que define las actualizaciones y eso solo puede hacerlo el usuario que controla el dato. Con todo, nosotros hemos consolidado los datos apoyándonos en casos de uso, pero hay que trabajar en el dato que el negocio necesita, porque es lo que acelera los proyectos".

Íñigo López Pérez, Head or Data & Analytics de Atlético de Madrid, tercer club de fútbol de España por valor de mercado, resaltó que su compañía tiene muchas líneas de negocio y muchos datos a integrar. "Hace años hicimos una transformación integrando diferentes herramientas, y ahora estamos precisando una estrategia del dato, definiendo casos de uso alineados con el negocio. Nos hemos encontrado barreras, pero la principal es asegurar la **calidad de los datos** históricos y consolidar y unificar las

Clica en la imagen para ver la galería

estructuras y el gobierno del dato, con una información correctamente definida. Después de eliminar estas barreras, definimos los casos de uso".

CUANDO EL DATO ES NEGOCIO

Desde Nationale-Nederlanden España, entidad que ofrece servicios de ahorro, inversión y seguros, David Vaquero López, su Chief Technology Officer, añadió a estas barreras expuestas por sus contertulios que "el problema es la falta de un gobierno del dato y un glosario de negocio. Nosotros tenemos ya tecnologías del dato y tenemos gran variedad de informes estandarizados. Hemos apostado por un modelo de consolidación, pero ir en esa línea aplicando un modelo de big-bang puede ser un fracaso, de modo que es conveniente moverse dirigidos por **casos de uso**, escalando las posibilidades de los

RESPONDIENDO A LOS RETOS DEL SECTOR

PAULA GÓMEZ, MAKING SCIENCE

"Tenemos soluciones orientadas a la activación del dato"

"Las empresas deberían estar centradas en los datos, pero la realidad no es así. Estamos dando pasos en la buena dirección, pero todavía hay empresas un tanto bloqueadas por la gran cantidad de datos que tienen que manejar", indicó Paula Gómez, Data & Adtech Director de Making Science, consultora de tecnología y marketing digital especialista en e-commerce y transformación digital. En su opinión, es "básico definir los casos de uso de la estrategia de datos antes de diseñar el resto de los elementos. En nuestro caso, ofrecemos un servicio 360, ayudando con todos los elementos necesarios, desde el desarrollo del marketing para obtener información hasta el uso de la tecnología con el foco en el dato. Contamos con soluciones muy orientadas a la activación del dato, que es un elemento esencial para alcanzar los objetivos marcados".

ANA LACUNA, MICROSTRATEGY

"Ofrecemos una plataforma para llevar la información donde se necesita"

"La necesidad de hacer llegar los datos a los usuarios de negocio, que son los que aprovechan los proyectos, no siempre es posible, porque el dato puede estar muy disperso. Por eso es necesaria una capa de normalización antes de dar los pasos para poder explotarlo", apuntó Ana Lacuna, Responsable de Cuentas en MicroStrategy, proveedor de software de analítica empresarial.

"Hay que buscar siempre el ROI necesario para la organización y la elección de casos de uso para cada entidad. Nosotros proporcionamos una plataforma analítica, que puede instalarse tanto en cloud como on-premise, y que permite a las empresas llevar la información más necesaria a las personas adecuadas de la forma más natural. Contamos con una capa semántica que garantiza el gobierno del dato y su calidad. Además, integra funcionalidades de IA para que los usuarios puedan diseñar sus propios cuadros de mando", expuso.

> LA CALIDAD DE LA INFORMACIÓN SE VE AFECTADA POR LA VELOCIDAD DE OBTENCIÓN, QUE ES MAYOR QUE LA CAPACIDAD DE VALIDACIÓN

FERNANDO FRACCHIA,
BI and Data Science Manager de **Venca**

Clica en la imagen para ver la galería

datos y cumpliendo los requisitos legales. En nuestra línea estratégica, es fundamental tenerlo en cuenta antes de ofrecer datos a los usuarios para su consumo, o, incluso, ofrecérselos a terceros. En cualquier caso, resulta imprescindible velar por el adecuado modelado, pero debe ser negocio el que lidere este consumo de la información".

Y es que una de las claves de la conversación se centró en el papel que los datos han adquirido para el negocio y cómo éste se relaciona con los datos. Desde la promotora inmobiliaria Aedas Homes, Jorge Valero, Director de aplicaciones y data, señaló que "nuestra estrategia se basa en ver los datos como un activo para el negocio para dotar de eficiencia a la organización. No ponemos en marcha ningún proyecto sin medir el ROI. Estos proyectos los decide negocio con nuestro apoyo, y deben contar siempre con unos KPI aprobados por la dirección. Por otra parte, contamos con datos de terceros y estamos industrializando su uso, pero no buscamos datos porque sí, si no para mejorar el ROI de cualquier proyecto. Con todo, la lección aprendida ha sido olvidarnos de la tecnología y poner el dato como el interruptor de todo. No se trata de mi dato o el dato de la organización. La información es de toda la compañía, no de cada departamento". ■

Clica en la imagen para ver la galería

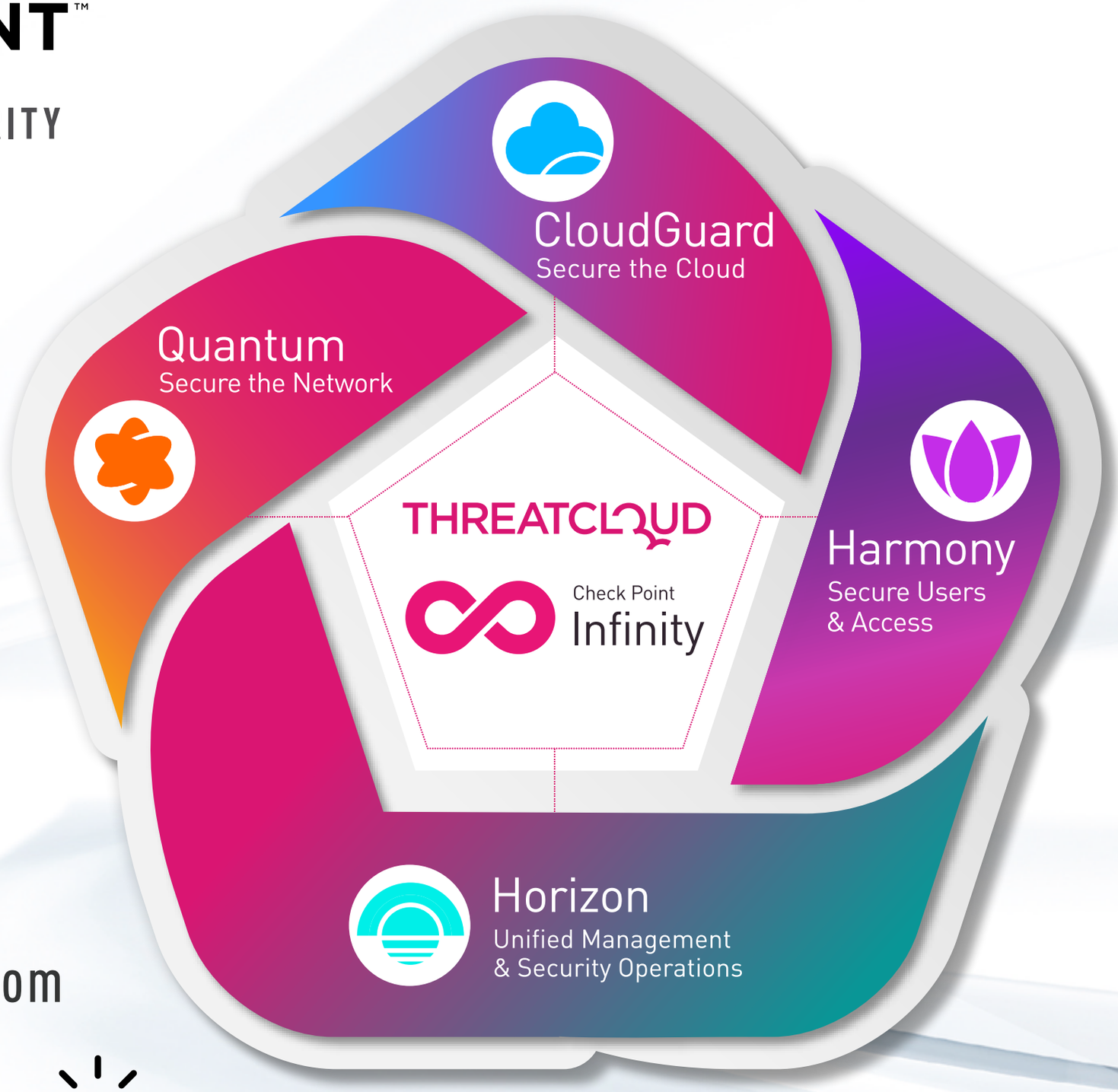
MÁS INFO +

» Estrategias para una empresa potenciada por los datos

COMPARTIR EN REDES SOCIALES

CHECK POINT™

YOU DESERVE THE BEST SECURITY



MÁS INFORMACIÓN:

www.checkpoint.com/es

info_iberia@checkpoint.com

DAVID SANZ, HEAD OF CORPORATE BUSINESS INTELLIGENCE, LOGISTA

“Para nosotros el dato se ha convertido en un activo crítico empresarial”

Como parte del Encuentro ITDM Group: “Ventajas y retos de la nueva era del dato” entrevistamos a David Sanz, head of Corporate Business Intelligence en Logista, uno de los principales operadores logísticos del sur de Europa. Sanz nos explica que su compañía “está muy centralizada en el canal del Estanco, en el de tiendas de proximidad y en el servicio de venta farmacéutica”, distribuyendo productos muy diversos. Se han enfocado en la sensorización de todos los elementos, generando una ingente cantidad de datos del transporte y de sus almacenes. Sanz comenta que el volumen de información crece constantemente, lo que los lleva a seguir modernizándose, aplicando la robotización y la automatización, y a convertirse en una empresa impulsada por los datos.

ENTREVISTA >> David Sanz nos explica cómo abordan en Logista el aprovechamiento del dato para impulsar su estrategia empresarial y su negocio.

EL VALOR DEL DATO PARA LA LOGÍSTICA

Como explica David Sanz, el dato permite tomar decisiones críticas "no solo en el ámbito puramente operativo, sino en generar líneas de negocio vinculadas al dato, donde podemos explotarlo, ponerlo a disposición de nuestros clientes e, incluso, monetizar la información que somos capaces de generar". El uso del dato es vital para la cadena de distribución y, para ello, "todo eso tiene que estar correctamente monitorizado para garantizar que los contratos que tenemos con nuestros clientes se cumplen" Y asegura que, para Logista, "el dato se ha convertido en un activo crítico empresarial que tenemos que potenciar, garantizar su calidad, defender y proteger".

Sanz explica que su proceso de modernización y su estrategia de datos no se basan en un enfoque tecnológico, sino que "el negocio tiene que ser elemento tractor que nos haga tomar dinámicas hacia el dato que sean innovadoras". Por ello, se basan en casos de negocio, entendiendo las necesidades y la estrategia global del negocio, que "tiene que ir entroncada perfectamente con nuestra estrategia del dato". Sanz señala que están dirigiéndose hacia escenarios cloud y que el gran volumen de datos que manejan los obliga a externalizar para poder escalar a medida que lo requiere el negocio, apostando por "estructuras mucho más ágiles, dinámicas y escalables".

TRANSFORMACIÓN CULTURAL Y TECNOLÓGICA

Para David Sanz, "hay dos elementos críticos que se tienen muy poco en cuenta, que son las propias personas y el gobierno del dato". Por un lado, es necesario que las personas usen la información, confíen en ella y sepan cuál pueden utilizar. Aquí entra en juego la cultura empresarial, pero también poner en marcha una buena práctica de gobierno del dato, buscando estandarizar y homogeneizar la información para que "todos hablen un lenguaje similar y todo el mundo sepa dónde puede acudir a consultar la información". Esta evolución se basa en tres elementos: construir una arquitectura escalable y flexible, con un proceso de gestión del cambio adecuado, y todo bajo un paraguas de gobernanza adecuado, lo que requerirá en el futuro contar con la figura del CDO (Chief Data Officer).

La tecnología es clave en esta modernización y en Logista están apostando cada vez más por escenarios de la nube, teniendo en consideración las limitaciones que pueden imponer los proveedores a nivel de servicio y software. Con el rápido ritmo de desarrollo digital, no quieren atarse a una única solución o a un único stack tecnológico, ya que podrían perder oportunidades. Por ello, Sanz comenta que intentan seguir esa filosofía del agnosticismo de la tecnología, buscando soluciones que no les obliguen a depender de un tercero.

RECOMENDACIONES SOBRE GESTIÓN DE DATOS

Como empresa avanzada en la digitalización y el aprovechamiento de la información, desde Logista recomiendan a las empresas una serie de buenas prácticas para la gestión de activos de datos. Sanz las resume en tres puntos: pensar en el negocio, buscando soluciones que resuelvan un problema de negocio; pensar en las personas, desarrollando procesos de gestión del cambio adecuados; y, por último, poner en práctica modelos de gobierno del dato para garantizar la calidad y fiabilidad de la información. Considera que estos puntos son fundamentales para lograr el éxito al desarrollar una estrategia del dato en la organización. ■

> "EL NEGOCIO DEBE SER ELEMENTO TRACTOR PARA TOMAR DINÁMICAS HACIA EL DATO QUE SEAN INNOVADORAS"

DAVID SANZ,
head of Corporate Business Intelligence en **Logista**

MÁS INFO +

» Encuentro ITDM Datos

» Logista

COMPARTIR EN REDES SOCIALES

Crayon

Nuevo informe de SAPIO Research

El estado de la optimización de costes TI en 2023

Una nueva investigación global sobre la optimización de costes TI revela que la complicada situación económica actual ha afectado al gasto en TI, ¿Por qué tantas empresas tienen dificultades para controlarlo y en qué áreas buscan reducir costes?

El informe, realizado por la compañía de investigación SAPIO Research, recoge las opiniones de más de 2.000 responsables de TI de 17 países de todo el mundo. El estudio destaca que la optimización de costes TI es el mayor reto que afrontan estos profesionales, y que el 54% está planteándose incrementar el control a la hora de llevar a cabo nuevas inversiones debido a la situación económica.

El 47 % de los responsables de TI afirma que la optimización de costes es su mayor preocupación.

El 95% de los encuestados cree que su presupuesto de TI no está totalmente optimizado.

El 54% está valorando incrementar el control a la hora de llevar a cabo nuevas inversiones debido a la situación económica.

Obtener el informe

SAPIO RESEARCH

CIBERSERGURIDAD Y GOBERNANZA: ¿CÓMO PROTEGER LA NUEVA ERA DEL DATO?

En la tercera mesa redonda de nuestro Encuentro ITDM Group debatimos sobre los desafíos que enfrentan las organizaciones en torno a la protección del dato. Para ello contamos con la presencia de Víctor Molina, Security Engineering Team Leader en Check Point España; José Manuel Bernal, director de servicios en Crayon Spain; Ramón Rodríguez, Data Center Solution Architect Expert en Schneider España y Sergio Martínez, Iberia regional manager en SonicWall. Estos expertos analizan la complejidad que introducen las nuevas regulaciones y el aumento de las amenazas por la digitalización, la expansión de las redes empresariales y la llegada de nuevas tecnologías transformadoras, como la inteligencia artificial.

MESA REDONDA >> La última mesa de debate de este Encuentro ITDM Group gira en torno a los problemas que enfrentan las organizaciones en materia de ciberseguridad y protección del dato. En este espacio contamos con la presencia de expertos en la materia pertenecientes a Check Point, Crayon, Schneider Electric y SonicWall.

NUEVO CONTEXTO PARA LAS ORGANIZACIONES

La digitalización está generando ingentes cantidades de datos que permiten a las empresas conocer mejor a sus socios y clientes, una información que debe ser protegida y que se ve sometida a regulaciones. Como explicaba Víctor Molina, “hay que asegurar que se cumplen las normativas”, pero también saber “por qué se recogen estos datos, dónde y durante cuánto tiempo se almacenan, y cómo se puede acceder a ellos”. Comentaba que “es importantísimo asegurar que tenemos los niveles de seguridad adecuados para proteger estos datos y que se debe contar con “un plan de respuesta, de recuperación, en caso de que tengamos algún incidente”.

José Manuel Bernal, de Crayon, coincidió en que cada vez se generan más datos y señaló que el problema más habitual es saber “cuántos datos tengo, dónde y cómo los tengo”. Considera fundamental la clasificación de los datos como un paso previo a la aplicación de medidas de ciberseguridad ya que, “dependiendo del tipo de datos, estas serán de una manera o de otra”. Además, planteó la cuestión de que los datos generan otros datos, lo que complica cuestiones como la propiedad intelectual.

Para Ramón Rodríguez la clasificación sobre la criticidad y la naturaleza de los datos es fundamental como paso previo y, después, “se debe cumplir con estas normativas y con nuestros propios criterios de criticidad del dato para establecer qué topología y qué solución híbrida es la idónea para cada empresa, en función de la naturaleza de estos datos”. También destacó que “estamos en un momento de explosión del dato, que no va a hacer más que seguir creciendo, lo cual nos va a exigir más flexibilidad”, y que probablemente los costes de gestión de los datos variarán más en el futuro.

Sergio Martínez opinaba que lo primero a tener en cuenta es el contexto normativo, que marca el camino a seguir, y que no basta con cumplir la normativa sin más, ya que hay que tener mucho cuidado con otros factores, como las credenciales de acceso. Destacó que en SonicWall están viendo un gran aumento de ataques de ransomware y del modelo de doble estafa, bloqueando el acceso a la información y amenazando con publicar datos sensibles robados por los hackers o los APT. Su último informe Cyber Threat Report muestra cómo los criminales están utilizando una sutileza sin precedentes en sus ataques, dirigiéndose a los datos y las credenciales.

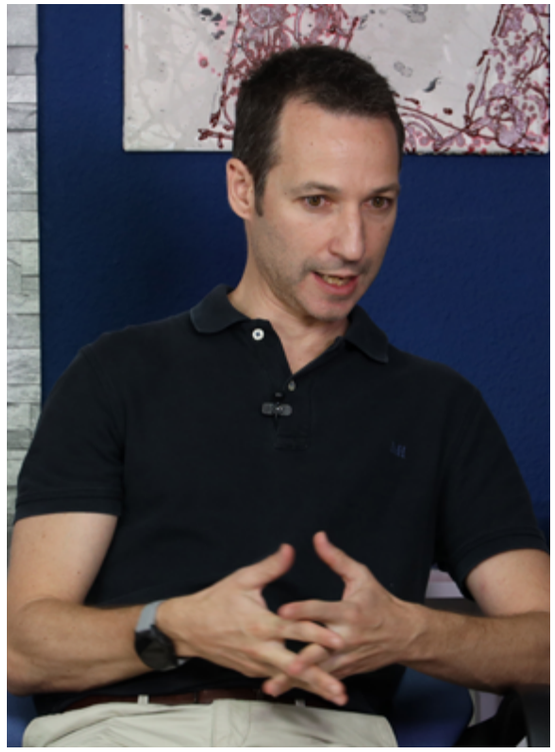
CONOCER EL DATO PARA SABER CÓMO PROTEGERLO

En opinión de Víctor Molina, se pueden hacer muchas cosas, pero lo principal es sentar unas bases que comienzan por la configuración de seguridad, tanto en los datacenter propios como en la nube. Destacó que constantemente se encuentran problemas de configuración y datos expuestos que deberían estar protegidos, incluyendo credenciales de acceso no cifradas, y remarcó la importancia del cifrado de datos en reposo para evitar las peores consecuencias de esa doble extorsión.

El representante de Crayon coincidía con que hay que empezar por determinar la naturaleza de los datos para poder aplicar las políticas de protección adecuadas, y después desplegarlas y mantenerlas. Bernal opinaba que

"tenemos que ir un paso por delante y buscar mecanismos que nos permitan evolucionar", porque todo avanza muy deprisa, y esto implica una mayor concienciación. Lo mismo opinaba Ramón Rodríguez, quien lanzó el mensaje de que las brechas de ciberseguridad van a ocurrir. Por ello, recomendó "elaborar una estrategia que nos permita minimizar esas brechas y, sobre todo, protocolos de actuación cuando ocurre algo". Comentaba que la cultura dentro de las empresas es un factor importante, que se debe apostar por la capacitación, algo que en Schneider hacen mediante planes de formación sobre ciberseguridad.

Desde SonicWall hacían énfasis en que más del 70% de los incidentes de ciberseguridad, como el robo de credenciales, se originan en el correo electrónico. Sergio Martínez dijo que "al final va a haber un problema de seguridad y hay que poder detectarlo y reaccionar de forma rápida para minimizar el impacto". En su opinión, esto pasa por establecer una defensa por capas y sensorización de todo lo que sucede en la red, la infraestructura, las aplicaciones y la nube, "porque algunas APT dejan rastros siempre en algún sitio y tenemos que ser capaces de detectarlo". También



aconsejó contar con más visibilidad y control sobre los datos de telemetría y "tener capacidad para detectar ataques de corte desconocido", que pueden provenir malware habitual ofuscado, todo ello "con un TCO adecuado, que se pueda pagar".

> "ES IMPORTANTÍSIMO ASEGURAR LOS NIVELES DE SEGURIDAD ADECUADOS PARA PROTEGER LOS DATOS"

VÍCTOR MOLINA,
Security Engineering Team Leader en **Check Point España**

AUMENTO DEL RIESGO POR LA DISTRIBUCIÓN DEL DATO

El cambio hacia modelos de trabajo híbridos está incrementando el riesgo de seguridad para las organizaciones y, como comentaba Víctor Molina, "los datos ya no están en un silo superlocalizado, sino que están muy distribuidos entre la nube pública y privada, los datacenter on-premise e, incluso, en varios datacenter". Los propios usuarios tienen datos, contraseñas y otra información sensible en sus equipos, y no todos son corporativos, incrementando el riesgo en los accesos remotos. Por ello, recomienda verificar la identidad de los usuarios y ser muy estrictos al aplicar estrategias de confianza cero.

José Manuel Bernal fue más allá, apostando firmemente por el plataformado en los equipos, implementando "una serie de características, certificados, etcétera, de tal manera que cuando te conectas lo primero que haces es verificar que tu equipo cumple con las políticas de seguridad de la compañía", y asegurarse de que "es parte de la compañía". Otras medidas que aplican en su propia empresa son el bloqueo de los puertos USB, las limitaciones estrictas de acceso en la propia intranet y la securización de la información en tránsito.

Desde el punto de vista de Schneider Electric, apuestan por plataformas securizadas desde el origen, por diseño, con protocolos de encriptación, doble identificación y otras medidas para reducir al mínimo posible la superficie de exposición. Y Ramón Rodríguez dijo que hay que extender esta protección a la seguridad física, ya que "el acceso físico a los servidores a través de personal interno puede generar una brecha muy importante y todavía

más difícil de detectar". Para ello, destacó el uso de herramientas de monitorización, que permitan saber qué persona está accediendo a qué equipo físico y para qué.

Para Sergio Martínez, de SonicWall, la mayor preocupación para el 91% de los CIO, CISO, etc. es que les cifren los datos con ransomware y, dado que el 70% o más del tráfico de internet está cifrado, es muy difícil analizarlo para detectar posibles amenazas. Finalmente, destacó el gran crecimiento del malware sobre IoT, aprovechando que muchos de estos dispositivos conectados no están categorizados y no cumplen con las normativas, lo que los convierte en ideales como punto de acceso.

DISOLUCIÓN DEL PERÍMETRO

Una de las ideas desarrollados en este debate es que el concepto de perímetro está obsoleto, diluido. En Crayon consideran que se deben "implementar políticas que ayuden a saber lo que está ocurriendo en todas las partes de la red". Víctor Molina ve en SIEM la solución ideal para este contexto, pero destacó que "cuando lo instalas, lo que recibes son millones de mensajes, tanto

falsos positivos como cosas serias. Luego, el trabajo está en definir qué puntos hay que medir, si es Azure, si es AWS, si es mi data center, los endpoint, etc., y montar controles, pero controles filtrados", que establezcan claramente qué es un ataque y qué no.

> "TENEMOS QUE IR UN PASO POR DELANTE Y BUSCAR MECANISMOS QUE NOS PERMITAN EVOLUCIONAR"

JOSÉ MANUEL BERNAL,
director de servicios
en **Crayon** Spain

José Manuel Bernal comentaba que las empresas no tienen que ser expertos en ciberseguridad, sino apoyarse en partners como Crayon, que se consideran "expertos en eliminar la complejidad". Con el asesoramiento que pueden aportar expertos externos se puede solicitar a la dirección los recursos necesarios para el nivel de seguridad adecuado. Y, según Víctor Molina, hay que prestar atención a los pequeños silos que van saliendo, como los que está generando la incorporación de dispositivos IoT, sobre los que no hay un control tan preciso como en otros equipos de la red.

AUMENTO DE DATOS Y SOSTENIBILIDAD

Más allá de la ciberseguridad, el aumento de datos genera otros desafíos para las organizaciones, como el aumento del coste de la energía, lo que en ocasiones choca con los objetivos de sostenibilidad. En este sentido, Ramón Fernández, de Schneider Electric, explicaba que "este tema está impactando muchísimo en el sector, hasta el punto de que las grandes empresas de colocation y los gigantes de Internet se preocupan mucho por esto, e incluso están cambiando sus modelos de negocio" y tomando medidas de emergencia. Conciben la eficiencia en base a tres pilares, comenzando por la parte IT, cada vez más densificada.

En segundo lugar, está la infraestructura, donde para reducir el consumo energético hay que trabajar en sistemas de enfriamiento más eficientes, igualmente basándose en la monitorización. Finalmente, está el apartado de la electricidad, donde hay que controlar con precisión lo que se consume y buscar formas de reducir el gasto innecesario. Por ejemplo, aprovechando el conocimiento que aporta la nueva generación de Data Center Infrastructure Management

(DCIM 3.0), que monitoriza lo que sucede en todos los centros de datos, ayudando a mejorar de la eficiencia.

RIESGOS DE LA INTELIGENCIA ARTIFICIAL

Los riesgos de ciberseguridad aumentan y, como comentaba Sergio Martínez, en la primera mitad de 2023 el volumen de ataques se ha reducido en un 20%, pero no su letalidad. Explicaba que "los ataques son cada vez más grandes, más bien preparados y las APT están haciendo un daño difícilmente mesurable". Afirma que el malware también sigue muy activo, con casi medio millón de versiones publicadas, pero ofuscadas, desconocidas. Mientras tanto, las vulnerabilidades han aumentado un 30%, dejando infinidad de agujeros por los que los delincuentes pueden colarse.

En este contexto, las nuevas herramientas de inteligencia artificial generativa se están utilizando tanto por los defensores como por los atacantes. Víctor Molina explicaba que "la democratización de las herramientas de ataques a lo mejor ahora tiene un poco más de peligro", ya que permite a los atacantes, por ejemplo, crear correos de phishing mejor escritos, más engañosos. Decía que "ahora la tecnología que podría identificar estas amenazas de forma automática a lo mejor ya no las identifica". Esto podría mejorar un poco la calidad general de los ataques, pero señalaba que también se están usando tecnologías basadas en IA para protegerse mejor.

> "HAY QUE EXTENDER LA PROTECCIÓN DEL DATO A LA SEGURIDAD FÍSICA"

RAMÓN RODRÍGUEZ,
Data Center Solution Architect Expert en **Schneider Electric** España

PROTECCIÓN DE DATOS EN 2023

Nuestro debate finalizó con una serie de recomendaciones de estos expertos para mejorar la protección y la gestión de datos en lo que resta de año. Comenzó Sergio Martínez, diciendo que lo fundamental es, primero, "saber lo que tienes que proteger para luego saber cómo tienes que protegerlo. Por lo menos, entender lo que tienes". A partir de eso, "construir una defensa por capas, desde el módulo central hasta el endpoint, pasando por aprobación de correo electrónico y teniendo un sistema de visibilidad y control, y tener capacidad para detectar lo desconocido y proteger el acceso remoto".

En opinión de Ramón Rodríguez, "todo parte de la seguridad de que algo te va a ocurrir en el mundo en el que estamos cada vez más complejo, con una infraestructura híbrida, con dispositivos IoT". Después, recomendaba tomar las medidas oportunas y considera que "es clave rodearse de un ecosistema de empresas que nos den soporte, ya no solo de la parte IT, sino en la parte de infraestructuras", con "software de ciberseguridad, empresas expertas en el despliegue, empresas que hacen seguimiento del perímetro expuesto, empresas externas que buscan brechas de ciberseguridad para taparlas antes de que las descubra un tercero". Todo ello sin dejar de lado la seguridad física, para fortalecer la seguridad de los ecosistemas IT y OT.

En Crayon destacaron la próxima creación de un Security Operations Center, que servirá para aprovechar las herramientas que el cliente ha comprado y, si no lo ha hecho, invitarle a comprarlas y encargarse ellos de la gestión. Destacó la importancia de rodearse de socios expertos en ciberseguridad que ayuden a lidiar con las nuevas amenazas que vayan surgiendo, incluyendo

> ES FUNDAMENTAL CONOCER LO QUE NECESITAS PROTEGER PARA SABER CÓMO DEBES PROTEGERLO

SERGIO MARTÍNEZ,
Iberia regional manager en
SonicWall

Clica en la imagen para ver la galería

las relacionadas con la inteligencia artificial generativa. También puso en valor las ventajas de los datos virtuales, por ejemplo, en data lakes virtualizados, que considera “más gestionables, más fácilmente securizables, con un menor consumo energético y generación de CO2, y más fáciles de montar”.

Por último, Víctor Molina destacó que no se deben dejar puertas de entrada abiertas, como las relacionadas con la nube, el correo electrónico, los dispositivos IoT o los móviles, que “siempre están en lo último de la lista por cubrir y todo el mundo los utiliza para manejar datos confidenciales de la empresa”. En segundo lugar, aconsejaba ir hacia una filosofía de confianza cero, teniendo en cuenta el riesgo de exfiltración de datos desde el interior, “porque ha habido bastantes casos de insider

Clica en la imagen para ver la galería

todos los años y va a seguir habiéndolos”. Finalmente, recomendó tener en cuenta la seguridad desde el diseño y vigilar la configuración de los sistemas, ya que muchos problemas provienen de diseños y configuraciones inseguras. ■

MÁS INFO +

» ¿Cómo proteger la nueva era del dato?

COMPARTIR EN REDES SOCIALES

ACTUALIZACIÓN SEMESTRAL EN:
SONICWALL.COM/THREATREPORT

2023

INFORME DE CIBERAMENAZAS DE SONICWALL

EL CAMBIANTE PANORAMA
DEL CIBERCRIMEN

SONICWALL®

sonicwall.com | @SonicwallSpain

ENRIQUE SERRANO APARICIO, EXPERTO EN SEGURIDAD INFORMÁTICA

“Hay que dar por hecho que en algún momento te van a hackear”

La tercera y última entrevista que forma parte de este Encuentro ITDM Group se centra en las amenazas para la seguridad y la privacidad de los datos que enfrentan las organizaciones. Para ilustrarnos sobre esta problemática hablamos con Enrique Serrano Aparicio, uno de los principales expertos en seguridad informática de España. Comienza dándonos las claves sobre cómo proteger los datos, que van más allá de cumplir estrictamente con las medidas establecidas por la ley de protección de datos europea. Serrano hace hincapié en la importancia de cifrar la información que se almacena o se transmite y de usar software específico de protección de datos.

Además, explica que no solo se debe tener en cuenta la protección de datos a nivel legal, sino que se

ENTREVISTA >> Enrique Serrano nos habla sobre la importancia de proteger los datos y la privacidad frente a las amenazas cibernéticas modernas.

deberían “incluir herramientas o metodologías que permitan luego auditar, trazar qué ha ocurrido, ir un pasito más allá”.

AUMENTAN LAS AMENAZAS

La ciberseguridad se ha vuelto crucial para las organizaciones ante amenazas tan graves como el ransomware, que permite a los delincuentes secuestrar los datos, o el phishing, que es un método común para hacerse con credenciales de acceso. Serrano destaca cómo ahora los delincuentes pueden usar un doble método de extorsión, impidiendo el acceso a los datos y amenazando con publicar información sensible o con borrarla. Considera que el humano es el punto débil de las organizaciones en cuanto a ciberseguridad, y que de nada sirve invertir en ello si no se forma a los trabajadores en buenas prácticas.

A pesar de ello, el phishing es cada vez más sofisticado y difícil de detectar. Además, Enrique Serrano comenta que se están viendo en España campañas de phishing e intentos de extorsión en los que el correo incluye la propia contraseña del usuario, lo que genera más temor e incita a la reacción. Estas credenciales provienen muchas veces de una fuga de datos de grandes empresas que llegan a la dark web, y se usan para incitar a las víctimas de phishing a pagar.

IRRUPCIÓN DE LA IA EN CIBERSEGURIDAD

En opinión de Enrique serrano, “los humanos somos la primera vía donde más hay que enfocarse”, y las empresas deben dar por hecho que en algún momento las van a hackear. Cree que la IA tendrá un papel cada vez más relevante en la ciberseguridad, ya que “si nosotros tenemos acceso a la IA, los ciberdelincuentes también”. Ya es posible crear un ransomware mediante inteligencia artificial en 10 minutos o menos, así como elaborar en muy poco tiempo campañas de phishing personalizadas por idioma y ubicación, entre otras muchas cosas.

Serrano dice que “hay que cambiar el chip y hay que dar por hecho que la IA ya está siendo involucrada en ciberataques” y, por ello, “estamos prácticamente obligados a usarla en ciberdefensa”. Sobre las leyes de inteligencia artificial, opina que regular esta tecnología hasta el extremo es un error, “como poner vallas al campo”, y que lo ideal es aprender a convivir con esta tecnología, porque ha llegado para quedarse.

> “VA A SER OBLIGATORIO USAR LA INTELIGENCIA ARTIFICIAL PARA LA DEFENSA”
>
> **ENRIQUE SERRANO APARICIO,** experto en seguridad informática

RECOMENDACIONES DE SEGURIDAD

Como señala Serrano, la ciberseguridad es una obligación para organizaciones de todos los tamaños, y aunque se trate de una empresa pequeña, y “ya sabemos que un hackeo es inevitable, que la seguridad al 100% no existe, al menos tu empresa debe esforzarse al máximo para no ser hackeado”. Pone en valor las herramientas que ayudan a cumplir con la ley de protección de datos, que también permiten saber qué ha ocurrido en cada momento con los datos y los accesos. Las hay más o menos caras, y Serrano dice que “poco a poco y proporcionalmente al tamaño de empresa o el activo, hay que invertir en esto, porque el dato es el valor que buscan los cibercriminales”.

Además, hay que tener en cuenta que muchas veces los delincuentes infiltran malware que permanece a la espera del momento adecuado para actuar, pudiendo replicarse en las copias de seguridad. Por ello, hay que esforzarse en la parte de detección y prevención, para evitar ataques de ransomware latentes y posibles fugas de datos que pongan en riesgo información vital para el negocio, desde datos de negocio o de clientes a propiedad intelectual. ■

MÁS INFO +

» Encuentro ITDM Datos

COMPARTIR EN REDES SOCIALES

VENTAJAS Y RETOS DE

LA NUEVA ERA DEL DATO

¡VER AHORA!

©freepik

it Digital MAGAZINE

ENCUENTROS ITDM GROUP