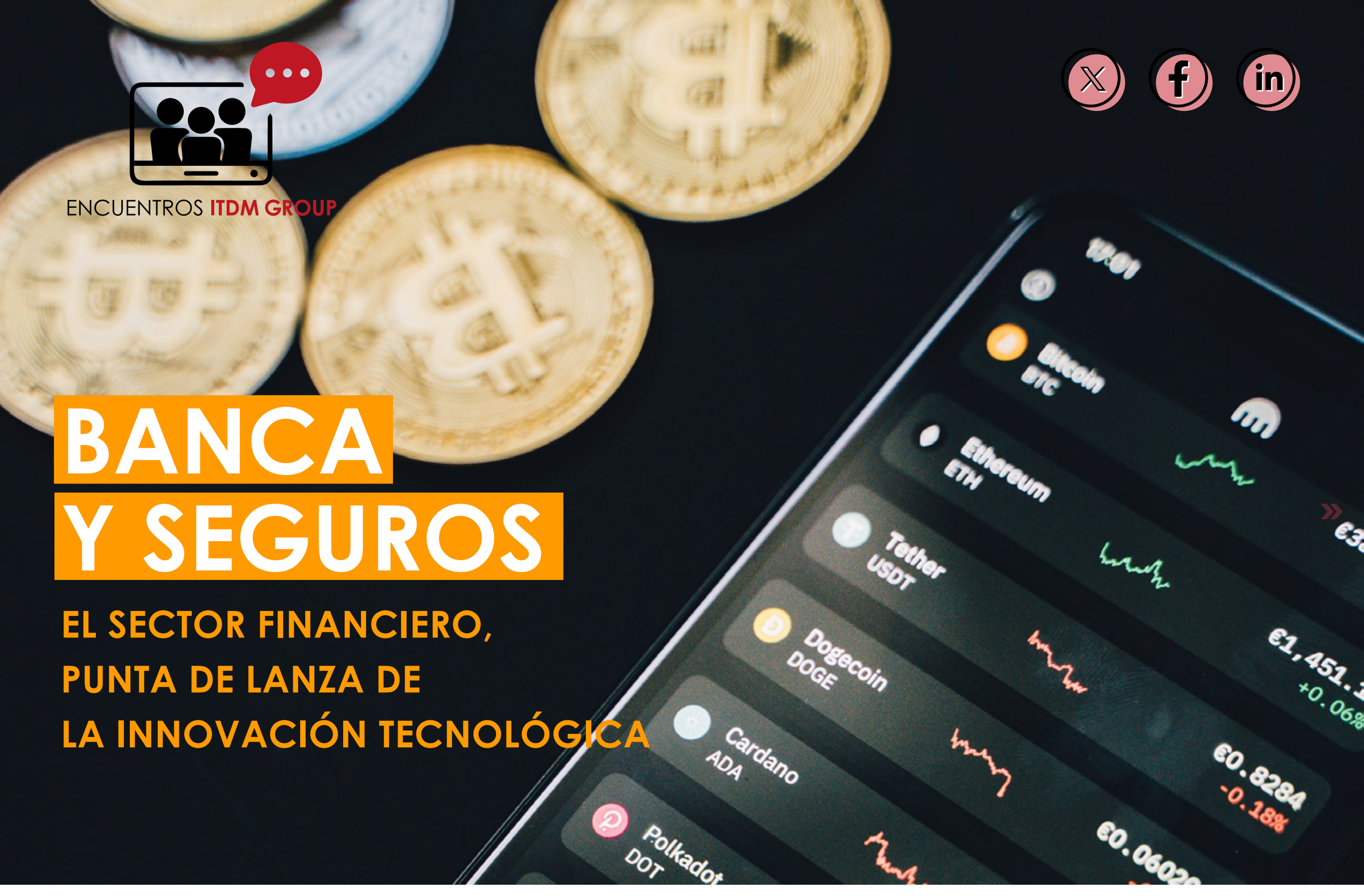
ENCUENTROS ITDM GROUP

BANCA Y SEGUROS

EL SECTOR FINANCIERO, PUNTA DE LANZA DE LA INNOVACIÓN TECNOLÓGICA



ORGANIZA

PATROCINADORES GOLD

PATROCINADORES SILVER

SUMARIO

ENCUENTROS ITDM GROUP

TRANSFORMACIÓN DE LA INDUSTRIA FINANCIERA

ENTREVISTAS

Miguel Jaureguízar, IEA

"Debemos seguir mejorando la seguridad y confiabilidad ante el aumento de ciberataques"

Gorka Briones, Deloitte

"Los pagos inmediatos son la mayor revolución en el sector de los medios de pago"

Daniel Rodríguez, Redtrust

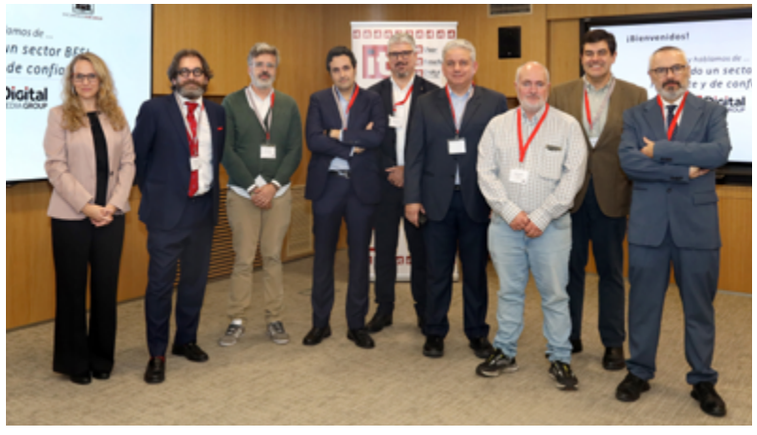
"El sector financiero es el primero en detectar las nuevas amenazas"

Alberto Pimpinela, Nationale-Nederlanden

"Orientamos la tecnología a tres pilares fundamentales: los datos, la conexión con terceros y el frontend"

MESA REDONDA

PRIORIDADES DE TRANSFORMACIÓN DE UN SECTOR FINANCIERO EN CONTINUA EVOLUCIÓN



GENERANDO UN SECTOR BFSI RESILIENTE Y DE CONFIANZA

EL SECTOR FINANCIERO, PUNTA DE LANZA DE LA INNOVACIÓN TECNOLÓGICA

PATROCINADORES GOLD

axians · bFY · fastly · Flexxible · veeam

PATROCINADORES SILVER

Bitdefender BUILT FOR RESILIENCE · redtrust · MicroStrategy · VERTIV. Architects of Continuity ™

#ENCUENTROSITDMGROUP

TRANSFORMACIÓN DE LA INDUSTRIA FINANCIERA

El sector de Banca, Finanzas y Seguros está experimentando una gran evolución digital, adoptando tecnologías que permiten brindar productos mejor enfocados a clientes cada vez más afines a lo digital. Esto está redefiniendo la forma de operar de las entidades, así como la infraestructura que sostiene todos sus servicios, que se mueve hacia la nube y se apoya en las últimas innovaciones para continuar a la vanguardia en un mercado altamente competitivo.

El progreso digital de la sociedad está impactando de lleno en el sector de Banca, Finanzas y Seguros (BFSI), que en la última década ha llevado a cabo una profunda transformación impulsada por la tecnología. A su vez, la llegada de nuevos medios de pago digitales y la expansión del comercio electrónico han dejado espacio para que surjan las Fintech, financieras nativas digitales que proporcionan servicios totalmente virtuales, y que están logrando una gran aceptación entre los consumidores españoles. Desde entonces, las entidades tradicionales se han volcado en desarrollar sus propias versiones o adquirir compañías especializadas para llevar sus productos financieros más allá de su ámbito tradicional.

Aunque esta industria es una de las más avanzadas en la digitalización, la diversificación de servicios y medios de pago, y la llegada de tecnologías de analítica avanzada e inteligencia artificial viene acompañada de numerosos cambios a nivel de infraestructura, operaciones, talento y cultura corporativa. Ante esto, las empresas están introduciendo grandes cambios para adaptarse a la nueva realidad, migrando aplicaciones y servicios a la nube, ampliando sus capacidades de análisis de datos y acompañando esto de las necesarias mejoras en gobernanza y ciberseguridad para cumplir con las regulaciones actuales y futuras.

ENCUENTROS ITDM GROUP >> Analizamos la evolución digital que está experimentando la industria de banca y finanzas, las nuevas tendencias y tecnologías que están surgiendo en torno a la financiación y los nuevos medios de pago, y los desafíos que enfrentan las entidades para seguir el ritmo de digitalización de la sociedad y los negocios en España.

NUEVAS VÍAS DE NEGOCIO

El concepto de Open Banking recibió un gran impulso tras el lanzamiento en 2015 de la Directiva de Servicios de Pago revisada (PSD2), que permitía a las entidades europeas compartir datos con terceras partes para ampliar el alcance de los productos bancarios. Según un informe de Capgemini sobre las finanzas integradas, la llegada de la banca abierta habilitó un nuevo modelo de negocio que "separa estructuralmente las operaciones bancarias de la interfaz con el cliente, haciendo que las finanzas sean invisibles y contextuales para los usuarios finales". Inicialmente, los bancos tradicionales actuaban desde el backend, dando soporte a las terceras partes que ofrecían los servicios financieros al cliente final. Pero esto ha ido cambiando a medida que los bancos han lanzado sus propios servicios finales, convirtiéndose en los propietarios de estas finanzas integradas.

Esto continuará evolucionando hacia el concepto de Open Finance, que permitirá llevar los productos financieros más allá, y los expertos anticipan que los ingresos de los bancos derivados de las finanzas integradas podrían pasar de los 22 billones de dólares registrados en 2020 a casi 558 billones para 2030. Esto da una medida de la importancia que tienen estos nuevos modelos de negocio para las entidades tradicionales, lo que seguirá impulsando la innovación y la exploración de nuevas fórmulas de finanzas abiertas en los próximos años.

MOVIMIENTO HACIA LA NUBE

Para adoptar nuevos modelos de negocio los bancos, financieras y

aseguradoras han ido desarrollando sus propios servicios digitales basados únicamente en plataformas online. Esto pasa por migrar sus aplicaciones y servicios a la nube, manteniendo on-premise solo los activos más críticos o que requieren un mayor control por cuestiones de seguridad o cumplimiento normativo. Para muchos expertos el futuro está adoptar servicios cloud bajo modalidades SaaS y, a medida que mejoren las redes de fibra y móviles se logrará reducir la latencia a niveles competitivos para una industria donde el tiempo es, literalmente, dinero.

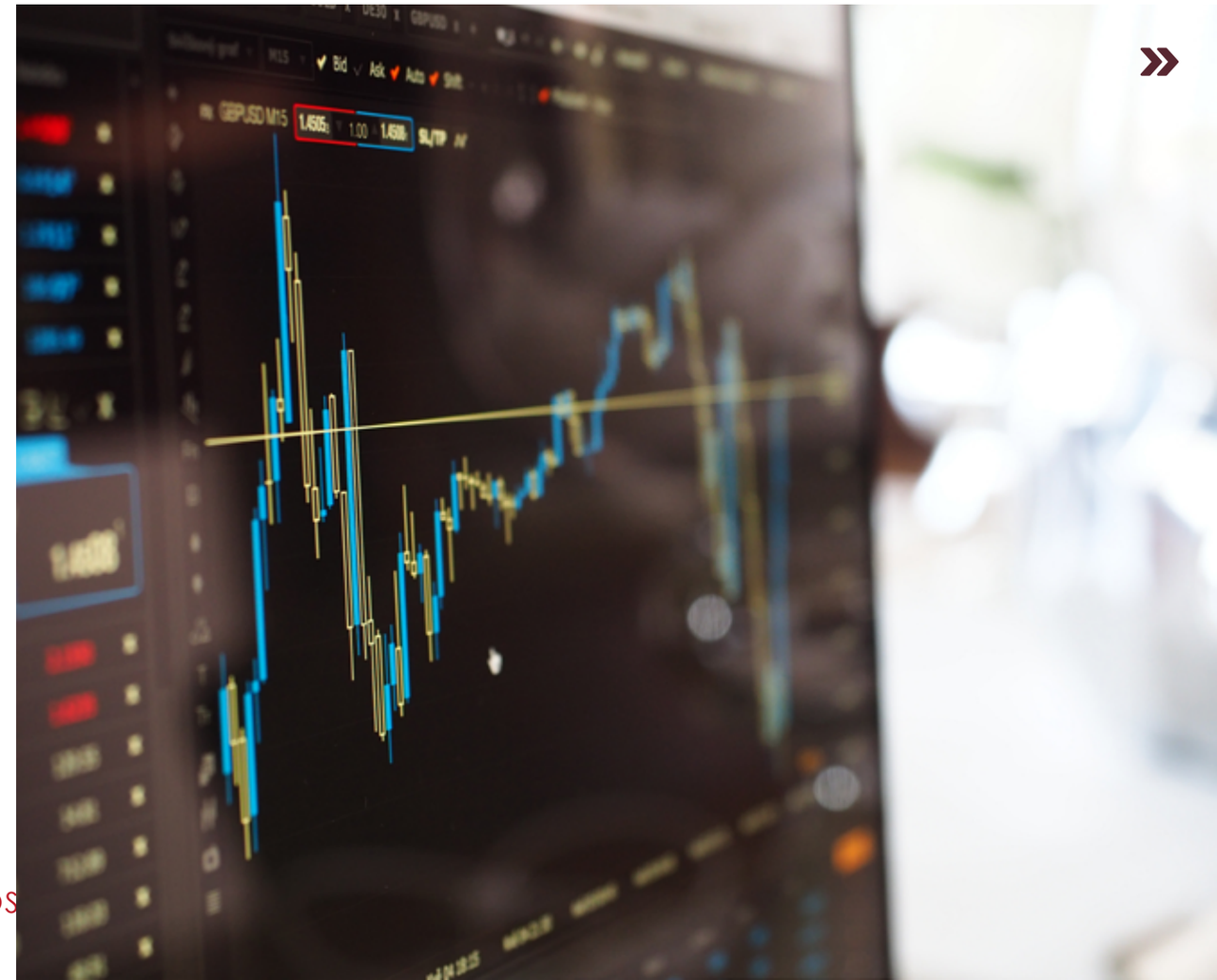
La adopción de la nube y otros factores como el paulatino cierre de sucursales bancarias está redefiniendo la arquitectura de TI en la industria. La necesidad de contar con grandes centros de datos y entornos Edge ligados a las oficinas está declinando a medida que se opta por infraestructuras gestionadas por terceros. Y, aunque el legacy continúa siendo importante para ciertas áreas, se buscan formas de sustituir estas infraestructuras obsoletas, o simplemente demasiado rígidas, por opciones más versátiles y flexibles, basadas en cloud. Esto afianzará aún más la fuerte relación que ya tienen los bancos, financieras y aseguradoras con los proveedores hiperescalares y los de colocation.

MÁS REQUISITOS DE SEGURIDAD

La industria de banca y fianzas siempre ha sido una de las más avanzadas en ciberseguridad, dado lo crítico de la información y los activos que manejan, pero la transformación que está experimentando acentúa aún más la necesidad de estar a la vanguardia en seguridad informática. Para ello se apoyan en socios tecnológicos que proporcionan herramientas para mejorar la visibilidad, aportando no solo datos, sino capacidades de inteligencia artificial que ayudan a prevenir amenazas. Y tecnologías pensadas para recuperar los sistemas lo más rápido posible tras sufrir un incidente de seguridad, garantizando que la amenaza no se reproducirá al restablecer los servicios.

En el ámbito de la infraestructura la seguridad, disponibilidad y confiabilidad también son factores críticos y los bancos buscan proveedores de centros de datos y servicios cloud que garanticen los más altos estándares de resiliencia y protección. Esto implica no solo contar con la mejor tecnología, sino también con estrategias de recuperación eficaces. Y esto plantea ciertos desafíos al relacionarlo con los objetivos de sostenibilidad medioambiental que ya forman parte de las estrategias ESG de la industria. Por ello, los proveedores están desarrollando ofertas que tratan de equilibrar ambas necesidades, recurriendo a tecnologías como la IA para identificar formas de mejorar la eficiencia sin mermar las capacidades que exigen los clientes.

> **EL CONCEPTO DE OPEN FINANCE PERMITIRÁ LLEVAR LOS PRODUCTOS FINANCIEROS MÁS ALLÁ DE LOS LÍMITES DE LA BANCA ABIERTA**



LA TRANSFORMACIÓN DEL SECTOR FINANCIERO ACENTÚA AÚN MÁS LA NECESIDAD DE ESTAR A LA VANGUARDIA EN SEGURIDAD INFORMÁTICA

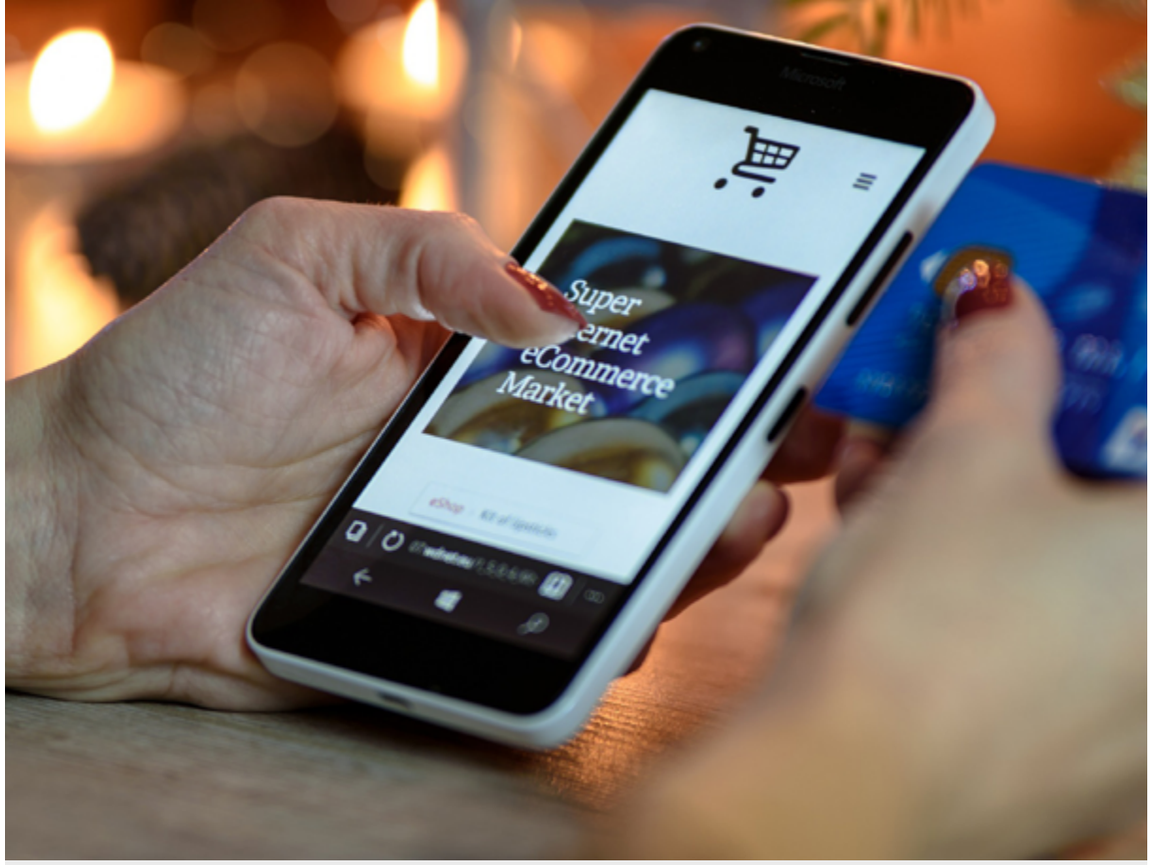
INNOVACIÓN IMPULSADA POR IA

De todas las tecnologías que utiliza la industria BFSI la más disruptiva es la inteligencia artificial, especialmente tras la popularización de los modelos de IA generativa. En un reciente artículo publicado por Gartner, Alexander Bant, vicepresidente de la práctica financiera de la consultora, explica que hay varios factores que impulsan la adopción de IA generativa entre los directivos financieros. En su artículo comenta que una inteligencia artificial generativa entrenada con datos financieros puede habilitar diferentes casos de uso innovadores, entre los que destaca cinco que pueden interesar a los CFO.

El primero es la revisión de contratos y documentos, detectando errores y términos específicos de forma automática, permitiendo hacer consultas y obtener las respuestas en lenguaje natural, así como categorizar y resumir documentos. También está la creación de borradores de informes financieros y de gestión, la interpretación de políticas financieras para proporcionar recomendaciones, la asistencia a la codificación y traducción de lenguajes antiguos, como COBOL, a lenguajes más modernos. Finalmente, Bant señala que la IA generativa puede proporcionar mejores explicaciones de las variaciones de forecast y presupuesto para los equipos de Planificación y Análisis Financiero (FP&A), aportando conclusiones más sintetizadas para presentar ante los ejecutivos y la junta directiva. ■

MÁS INFO +

» La banca española sumará 6 millones de clientes digitales en 5 años



LA IA REDUCIRÁ EL COSTE DE LA VERIFICACIÓN DE IDENTIDAD PARA LOS BANCOS

Según una investigación publicada por Juniper Research, entre 2023 y 2028 la IA podría reducir en un 30% el tiempo dedicado a las operaciones de verificación de identidad, reduciendo los costes asociados y el riesgo relacionado con el fraude por identidad sintética. Los expertos señalan que los ingresos por onboarding digital aumentarán mucho en este tiempo, gracias a la adopción generalizada de la verificación digital en la banca, pero el gasto total de las entidades también crecerá sustancialmente, pasando de 7.400 millones de dólares en 2023 a 9.900 millones en 2028.

axians

cisco Partner

Nuestra web
axians.es

En Axians no solo hablamos de innovación,

La vivimos

- Customer experiencie
- Estrategia data-driven
- Partner experiencie

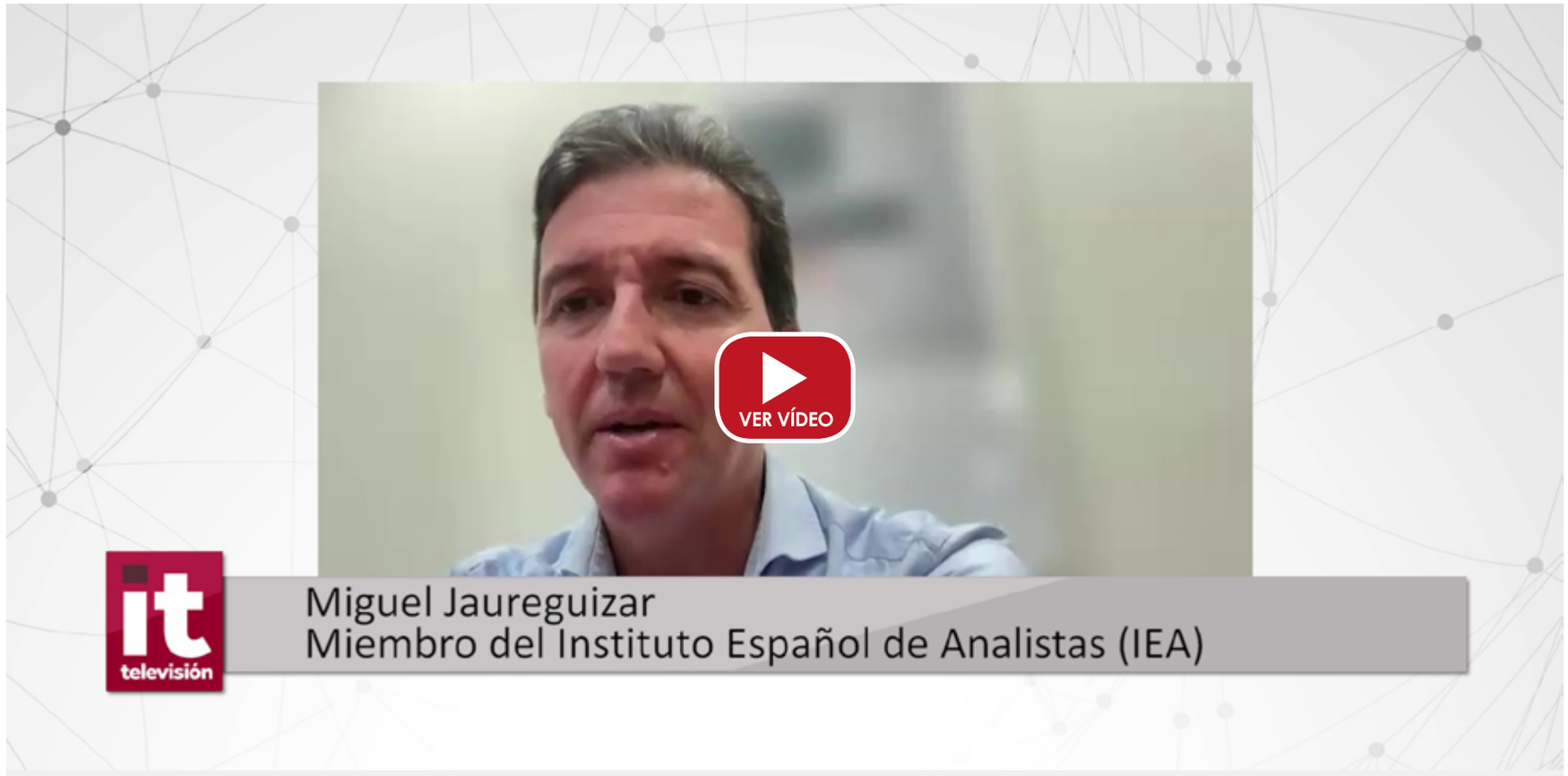
Convertimos tus ambiciones en resultados

VINCI ENERGIES

MIGUEL JAUREGUÍZAR, MIEMBRO DEL INSTITUTO ESPAÑOL DE ANALISTAS (IEA)

“Debemos seguir mejorando la seguridad y confiabilidad ante el aumento de ciberataques”

Comenzamos este encuentro ITDM Group con una entrevista a Miguel Jaureguízar, del Instituto Español de Analistas (IEA), quien nos explica cómo ha evolucionado el panorama de la ciberseguridad en el sector financiero. En la última década se ha triplicado el número de ciberataques y los servicios financieros son uno de los blancos predilectos de los ciberdelincuentes. Miguel Jaureguízar comentaba que en este tiempo el sector ha modernizado mucho sus servicios para volverse “más electrónicos, mucho más ágiles, más accesibles, pero también más en formato plataformas”. Y afirmó que en esta evolución la ciberseguridad siempre se ha puesto por delante, ya que se trata de proteger un activo tan importante como el dinero.



ENTREVISTA >> Miguel Jaureguízar explica cómo responde el sector financiero al aumento de ciberamenazas para proteger a las entidades y a sus clientes.

TENDENCIAS EN SEGURIDAD FINANCIERA

En opinión de Miguel Jaureguízar, las decisiones tecnológicas sobre la seguridad en el sector financiero están guiadas por la necesidad de proporcionar una mayor protección, "incluso si es a costa de un pequeño deterioro de la experiencia de usuario". El objetivo es seguir mejorando la seguridad y confiabilidad ante el aumento de ciberataques, de phishing, de accesos no autorizados a las cuentas y los activos de los clientes y, en sus palabras, también para cumplir con normativas como PSD2 o DORA (Digital Operational Resilience Act).

Explicaba que estos requisitos están condicionando las decisiones de compra en el sector tecnológico, ya que PSD2 ha obligado a construir sistemas de autenticación fuerte, y DORA a "a revisar una y otra vez todos y cada uno de nuestros procesos y asegurarse de que todos los puntos que forman el proceso están securizados, tanto a nivel global como a nivel individual".

> "SE NECESITA UN MAYOR NIVEL DE CONCIENCIACIÓN Y DE EDUCACIÓN CIUDADANA PARA AYUDAR A MINIMIZAR LOS RIESGOS"

MIGUEL JAUREGUÍZAR,
Miembro del **Instituto Español de Analistas (IEA)**

PRINCIPALES AMENAZAS

Nuestro entrevistado identifica dos grandes categorías de ciberamenazas para el sector financiero, que son los ataques a los sistemas de las organizaciones y los que se realizan a través de los clientes. En el primer grupo destacó los de denegación de servicio, el phishing o el spare pshishing, y en el segundo también están los intentos de suplantación de identidad a través del phishing, con el objetivo de consultar información y realizar operaciones. En su opinión, el sector financiero está bien preparado para hacer frente a estos peligros, ya que se han implementado numerosas medidas para prevenirlos y combatirlos. Aunque señaló que necesitan "un mayor nivel de concienciación y de educación ciudadana" para ayudar a minimizar los riesgos, algo que intentan a través de campañas destinadas a la población y los clientes. Por ejemplo, recalcando que no se les pedirán contraseñas ni códigos en comunicaciones que no hayan iniciado ellos, y que no se debe responder a estos intentos.

RETOS PARA EL FUTURO

Para Miguel Jaureguízar, los principales retos que enfrenta el sector en lo que se refiere a la seguridad cibernética son cuatro, comenzando por la formación de todos aquellos que trabajan en las entidades financieras. El segundo es la formación a los clientes, para que "entiendan cuál es el origen de determinadas prácticas de ciberdelincuencia, como el phishing". En tercer lugar, están los costes que conlleva la incorporación de nuevas tecnologías de seguridad a las entidades y, por último, trabajar conjuntamente en estándares, "poder intercambiar prácticas, tener determinadas bases de datos y elementos comunes para que el desarrollo sea sectorial, y no exclusivamente de las entidades individuales".

De cara al futuro, para seguir mejorando la seguridad de los entornos financieros, abogaba por avanzar en la implementación de DORA y en esa concienciación de la ciudadanía, ya que opina que "esta lucha global tiene que involucrar a otros participantes, a los proveedores de telefonía, a las grandes plataformas y marketplaces de comercio electrónico", "porque son puertas de entrada a través de las que muchas veces los clientes sufren este fraude". Además, recalcó que "necesitamos también que no sea un trabajo sectorial exclusivo, sino una colaboración transectorial", involucrando principalmente a los grandes proveedores de comercio electrónico. ■

MÁS INFO +

» Encuentro ITDM Group Banca

La ciberdelincuencia en España representa el 15,6% de los hechos delictivos*.

No dejes que los ciberdelincuentes acaben con tu negocio.

b-fy

TU BIOMETRÍA SOLO CONTIGO

b-fy.com

b-fy.com

*** Informe sobre la Criminalidad en España 2021.**

PRIORIDADES DE TRANSFORMACIÓN DE UN SECTOR FINANCIERO EN CONTINUA EVOLUCIÓN

El mercado financiero está viviendo en los últimos años una completa transformación por la combinación de fuerzas ya establecidas con nuevos actores, las fluctuaciones bursátiles y la digitalización de sus procesos, productos y clientes. Todas estas líneas obligan al negocio financiero a no frenar su innovación, apoyándose en tecnología. Para analizar estas estrategias de transformación, se celebró un Encuentro de la Comunidad IT con la participación de Abanca, Asisa, Banco Mediolanum, Bestinver, Evo Banco, Mapfre, Nationale-Nederlanden, OpenFinance, Santander Global Tech y Seguros RGA, y la colaboración de Flexxible, Fastly y Veeam Software.

MESA REDONDA >> Conclusiones del Encuentro sobre prioridades de transformación del sector financiero en el que participaron Abanca, Asisa, Banco Mediolanum, Bestinver, Evo Banco, Mapfre, Nationale-Nederlanden, OpenFinance, Santander Global Tech y Seguros RGA, con la colaboración de Flexxible, Fastly y Veeam Software.

> ASEGURARSE DE MANTENER TODAS LAS TECNOLOGÍAS IMPLANTADAS EN UN FUTURO ES EL GRAN CABALLO DE BATALLA DE TI

CARLOS GONZÁLEZ,
IT Governance Architecture and Process Director de **Abanca**

> ESTÁ BIEN PONER EL FOCO EN LO NUEVO, PERO DETRÁS DE TODO TIENE QUE ESTAR SIEMPRE LA EFICIENCIA

JOSÉ CARLOS OROZCO,
Director de Tecnología de **Asisa**

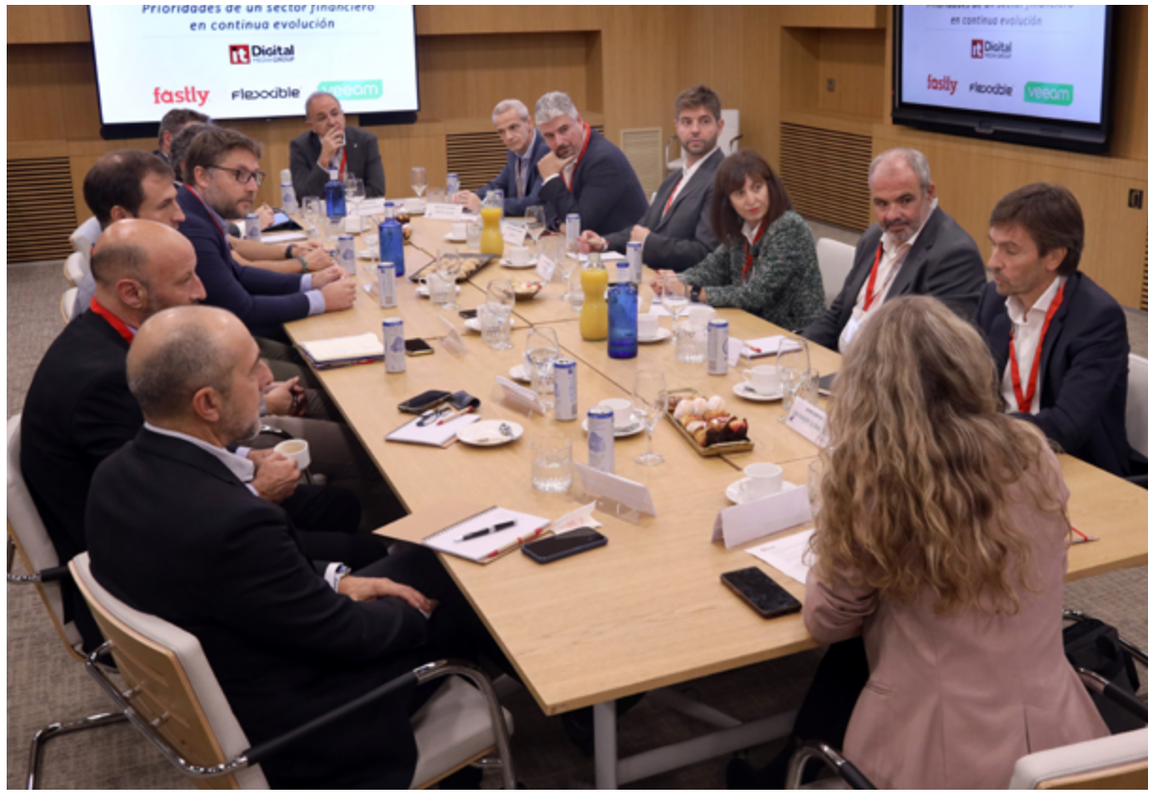
Clica en la imagen para ver la galería

La digitalización de los servicios y productos financieros supone una gran oportunidad para el crecimiento del negocio. Por ello, las organizaciones que conforman el sector BFSI (banca, servicios financieros y seguros) tienen como prioridad seguir desarrollando su oferta digital al tiempo que aplican tecnologías a tareas propias del negocio para la gestión de recursos humanos, la optimización de procesos e infraestructuras y la gestión de la información. Igualmente deben prestar atención al cumplimiento de normativas y a la gestión del talento digital. Así pues, se presentan numerosos vectores de innovación para las organizaciones de este mercado tanto en el front office como en el back office.

“Nosotros hemos ido incorporando otros bancos e integrándolos, pero ahora nos estamos transformando de forma completa: procesos, personas y tecnologías”, explicó Javier Cortijo, IT Transformation Director de Santander Global Tech; “para ello tenemos que estar pendientes de las tecnologías que ayudan al cambio y aportan valor al negocio. Además, la combinación de tecnologías disruptivas aporta motores tales como la eficiencia, la reducción de costes o ese componente de valor. Y no podemos olvidar que somos un sector muy regulado y nuestras soluciones son básicas para el cumplimiento”.

Clica en la imagen para ver la galería

En este sentido, Carlos González, IT Governance Architecture and Process Director de Abanca, señaló que “las decisiones de compra giran en torno a tres puntos: un crecimiento inorgánico, lo que motiva las compras y las condiciona por los procesos de integración; el continuo cambio de la tecnología y la com-



Clica en la imagen para ver la galería

plejidad de encontrar determinados perfiles; y la migración de tecnología legacy, aunque esto no es algo que se pueda hacer de forma acelerada. Con todo, la principal prioridad es dar servicio al negocio".

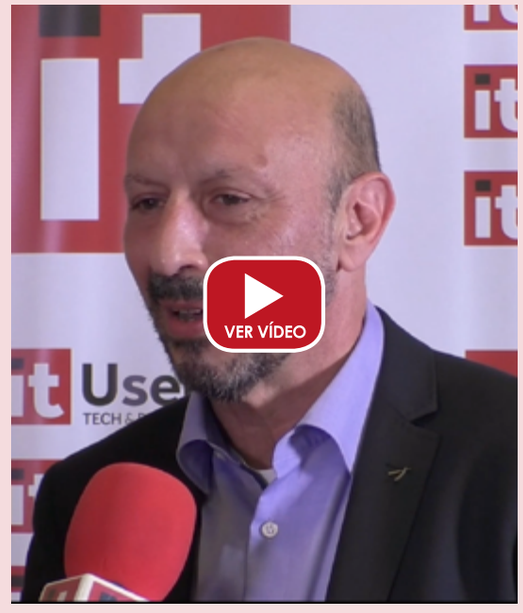
Juan Carlos Server, Director de Operaciones de Banco Mediolanum, explicó que "la tecnología es un aliado esencial en nuestras funciones de asesoramiento financiero. Por eso, nuestras ratios de digitalización son muy elevados, y nuestras prioridades pasan por mejorar la experiencia del cliente y ayudarle a que tomen la mejor decisión. Queremos que esos usuarios no encuentren diferencias entre nuestras apps y las que ellos usan habi-

RESPONDIENDO A LOS RETOS DEL SECTOR

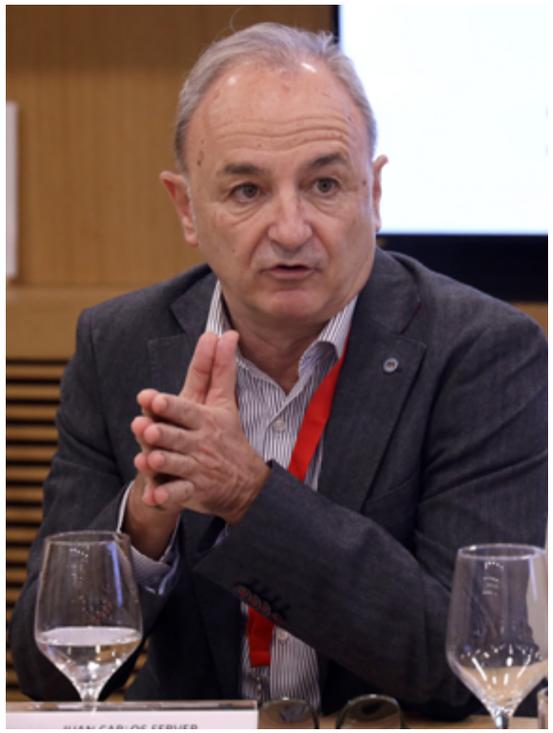
MANUEL DE DIOS, SALES SPECIALIST DIRECTOR DE FLEXXIBLE

"Evitamos la fricción del usuario con la tecnología"

Manuel de Dios, Sales Specialist Director de Flexxible, multinacional española de software, especializada en soluciones para el trabajo digital, comentaba que, al hilo de las opiniones mostradas en el debate, "para todas las organizaciones sigue siendo muy relevante el aspecto humano", un área de la ecuación tecnológica que cubre Flexxible, "evitando la fricción del usuario con la tecnología, y ayudando a los departamentos de TI, tanto a gestionar esa relación con el usuario como a eliminar una gran cantidad de procesos, ofreciendo una observabilidad de 360 grados



de la plataforma de dispositivos de sus usuarios, para consumo de toda la organización, y no solo del propio departamento de tecnología".



> ANTES DE IR A CLOUD, HAY QUE APIFICAR. EN TODO CASO, HAY QUE TENER CLARA LA HOJA DE RUTA Y CONTAR CON LOS EQUIPOS NECESARIOS

JUAN CARLOS SERVER,
Director de Operaciones de
Banco Mediolanum

> HAY QUE ADOPTAR LA IA PARA QUE LA COMPETENCIA NO NOS DEJE ATRÁS, Y DEBE CALAR LA ORGANIZACIÓN DE ARRIBA ABAJO

BEGOÑA MORENO,
Head of IT de **Bestinver**

Clica en la imagen para ver la galería

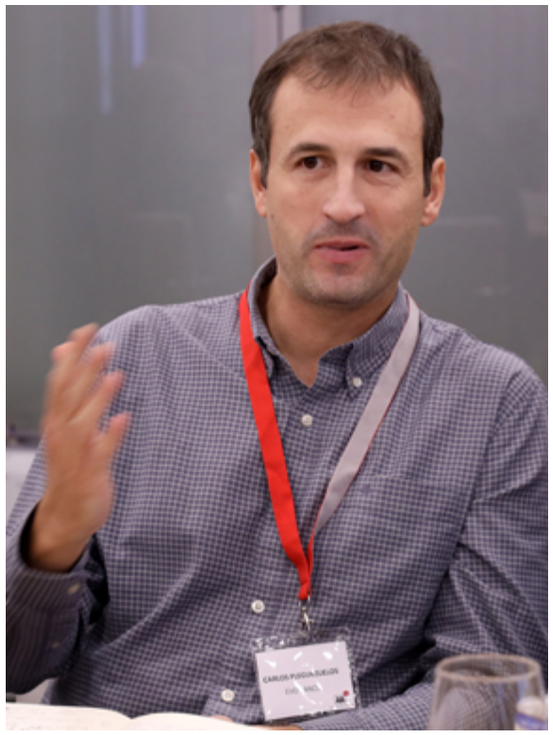
tualmente en su día a día, pero, eso sí, con una seguridad superior".

Begoña Moreno, Head of IT de Bestinver, apuntó que "el gran reto es un negocio en continuo cambio y el hype alrededor de la tecnología. Pero el verdadero desafío es hacerlo manteniendo la seguridad, los costes, la protección de datos y el talento, porque no se pueden cubrir muchas posiciones abiertas en capacidades y tecnologías punteras. La IA avanza muy rápido, pero hay que concienciar a negocio para que el proceso de adopción sea el adecuado. No se trata de integrarla, sino de hacerlo de forma coherente y de la forma en que la necesite la organización".

¿ES POSIBLE DEJAR ATRÁS EL LEGACY Y CONVERTIRSE EN ORGANIZACIONES ÁGILES?

No hay que olvidar que las entidades financieras, por ser pioneras en digitalización, cuentan con un gran bagaje tecnológico, con frecuencia no tan moderno como se espera y que sigue estando operativo. "El legacy es nuestro gran reto, ser capaces de apificarlo. Nuestra tecnología debe ir orientada a que el negocio venda, y ahí el talento es fundamental. Responder a las necesidades que impone la Customer Experience es otro reto, así como la usabilidad de los desarrollos. Nosotros apostamos por la filosofía Agile, e integrar negocio y TI es importante, pero no podemos olvidar los requerimientos normativos en todos los desarrollos", agregó Alberto Pimpinela, Head of Front Office de Nationale-Nederlanden, a la conversación.

Carlos Pleguezuelos, Director de Tecnología de Evo Banco, recordó que "TI tiene demasiadas cosas sobre la mesa donde poner el



> PARA EL REGULADOR BANCARIO LO IMPORTANTE TIENE QUE SER EL CONTROL Y EL GOBIERNO, NO DÓNDE SE IMPLEMENTE LA TECNOLOGÍA

CARLOS PLEGUEZUELOS,
Director de Tecnología de
Evo Banco

foco. Hemos pasado por muchas etapas y la motivación la marca la escala de recursos disponibles y lo que necesitamos hacer con esos recursos. Nuestro motor es maximizar los recursos apoyándonos en terceros y siendo muy prácticos en nuestras soluciones. No podemos iniciar un proyecto que no acabe en producción, y así ha sido desde 2016. Por suerte, no tenemos legacy y aplicamos tres principios: cloud first, nada on-premise; app first, con todo desarrollado vía API; y

Clica en la imagen para ver la galería

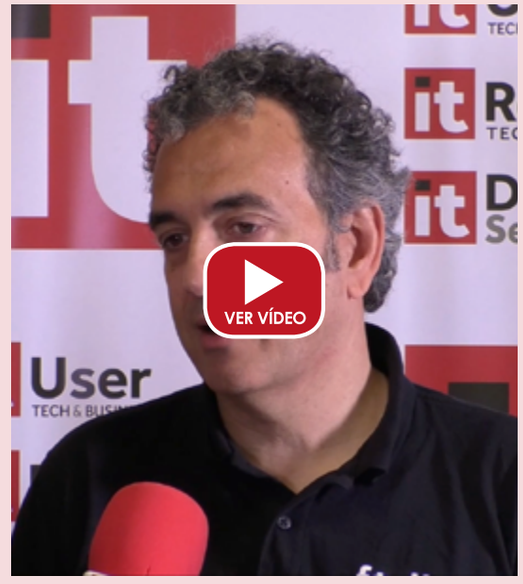
aaS first, apostando por el modelo como servicio porque no podemos abarcar todo internamente desde TI. En base a esto, seleccionamos las tecnologías. Por ejemplo, controlamos los costes en la nube con un proyecto de FinOps que nos alerta de cualquier incremento del

RESPONDIENDO A LOS RETOS DEL SECTOR

DANIEL HOWE, SENIOR SALES ENGINEER DE FASTLY

"Eliminamos la denegación de servicio y mejoramos la latencia que deben soportar los aplicativos financieros"

Daniel Howe, Senior Sales Engineer de Fastly, proveedor de plataformas edge cloud, explicaba que "todas las empresas del sector están adaptando sus estructuras, y creemos que podemos ayudarles desde el punto de vista de la securización y la capacidad de protección de la continuidad de negocio, eliminando cuestiones como la denegación de servicio y mejorando la latencia que debe soportar todos sus aplicativos, porque son conscientes de que tienen que evolucionar a lo que está marcando el mercado, donde más del 50% del tráfico se consume por API y apps móviles.



En resumen, en unos servicios cada vez más consumidos por dispositivos móviles, podemos ayudarles mucho en la seguridad".

> APARTE DE CRITERIOS DE TI, SEGURIDAD Y REGULACIÓN, LO MÁS IMPORTANTE ES BUSCARLE SENTIDO TECNOLÓGICO Y DE NEGOCIO PARA LA COMPAÑÍA

JESÚS PABLO GUTIÉRREZ,
Director de Tecnología/
Arquitectura de **Mapfre**

> NUESTRA TECNOLOGÍA DEBE IR ORIENTADA A QUE EL NEGOCIO VENDA, Y AHÍ EL TALENTO ES FUNDAMENTAL

ALBERTO PIMPINELA,
Head of Front Office de
Nationale-Nederlanden

Clica en la imagen para ver la galería

gasto en cualquier servicio. Aunque ser una entidad más pequeña nos facilita la labor". Asimismo, para Juan José Peña, Head of Business Management de OpenFinance, resaltó "el papel de los equipos para la transformación del negocio y el cumplimiento. Reducir los tamaños de los proyectos facilita mucho las cosas y se reducen los tiempos de entrega, lo que redunda en una mejor integración y comunicación entre equipos. Cloud es clave porque permite crecer más rápido y ser más eficiente. La tecnología debe ser la palanca para el negocio".

ASEGURAR EL SERVICIO, UN ELEMENTO BÁSICO DE LA ESTRATEGIA

A la hora de integrar nuevas tecnologías en estas organizaciones hay que tener en cuenta diferentes aspectos. "TI tiene mucha presión por integrar las nuevas tecnologías, incluso sin saber para qué, en algunos casos. La IA va a ser disruptiva, pero no necesariamente tenemos que usarla para el negocio, sino que puede ser más efectiva para buscar la eficiencia. En todo caso, lo primero que hay que hacer es buscar casos de uso. No podemos olvidar, no obstante, que el área de Seguros va un paso o dos por detrás del negocio bancario en su transformación, pero, aun así, el gobierno de todo lo que se va integrando recae en TI, aunque sea algo que haya generado negocio", destacó Carlos Castellano, Director de Sistemas de Información de Seguros RGA.

Por su parte, Jesús Pablo Gutiérrez, Director de Tecnología/Arquitectura de Mapfre, señaló que

> LA IA PUEDE AYUDARNOS EN NUESTROS PROCESOS FACILITANDO LA LABOR DE LOS GESTORES PROFESIONALES

JUAN JOSÉ PEÑA,
Head of Business Management de **OpenFinance**

"aparte de los criterios de TI, seguridad y regulación, lo más importante es buscarle sentido tecnológico y de negocio para la compañía. Hay tecnologías emergentes que pueden interesarnos, pero no poner el foco. El valor real explota con la convergencia de tecnologías, aunque cada una, por su parte, aporte su propio valor. Con todo, cada día es más difusa la frontera entre TI y negocio, y cuando empiezas a trabajar juntos, te das cuenta de que no sirve trabajar por separado. En todo caso, negocio debe apoyarse en tecnología, porque TI tiene una gran visión de la responsabilidad que hay veces que no se ve desde negocio".

Y en este sentido, José Carlos Orozco, Director de Tecnología de Asisa, recordaba que "asegurar el

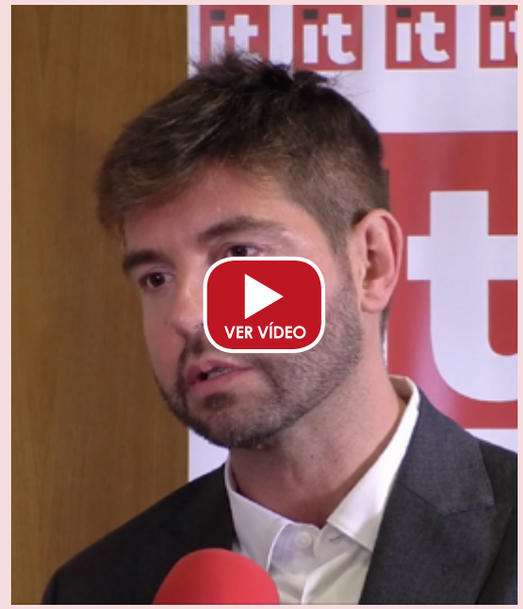
Clica en la imagen para ver la galería

RESPONDIENDO A LOS RETOS DEL SECTOR

LUIGI SEMENTE, REGIONAL ALLIANCE SALES MANAGER ITALIA E IBERIA DE VEEAM SOFTWARE

"Garantizamos la disponibilidad de los datos cumpliendo las normativas vigentes"

Luigi Semente, Regional Alliance Sales Manager Italia e Iberia de Veeam Software, suministrador de soluciones de protección de datos y recuperación ante ransomware, señalaba que "la llegada de DORA va a ser un cambio muy relevante para el sector, y nosotros les ayudamos garantizando la disponibilidad de los datos, y, en el caso específico de esta área del negocio, les permitimos cumplir con la normativa vigente. Les proporcionamos todos los procedimientos para garantizar la disponibilidad del dato y la continuidad del negocio, y lo hacemos de una forma moderna y segura, cuidando del legacy pero sin perder de vista el futuro, y con la adecuada protección sencilla y eficiente".



> CLOUD REDEFINE NUESTRA FORMA DE TRABAJAR Y ES UN PILAR FUNDAMENTAL DE LA ESTRATEGIA TECNOLÓGICA

JAVIER CORTIJO,
IT Transformation Director de
Santander Global Tech

> LA APUESTA NO ES SOLO CLOUD, SINO LOS MODELOS SAAS, LO QUE PERMITE PAGAR POR LO QUE USAMOS Y OLVIDARNOS DEL RESTO

CARLOS CASTELLANO,
Director de Sistemas de
Información de **Seguros RGA**

servicio se ha convertido en una commodity. Está bien poner el foco en lo nuevo, pero detrás de todo esto tiene que estar siempre la eficiencia". Orozco introdujo también la cuestión de la regulación, "que nos tiene en jaque por la seguridad y la privacidad de los datos. En el viaje a la nube, hemos encontrado, además, una normativa muy restrictiva referida a dónde tienes estos datos. Con todo, hay que ponerla en valor. No deberíamos verla como una complejidad, sino saber poner sobre la mesa el valor del cumplimiento". Y es que el sector financiero es uno de los más regulados y las normativas tienen un claro impacto en la aplicación de la tecnología, la gestión de los proveedores y la ubicación de la información. ■

Clica en la imagen para ver la galería

Clica en la imagen para ver la galería

MÁS INFO +

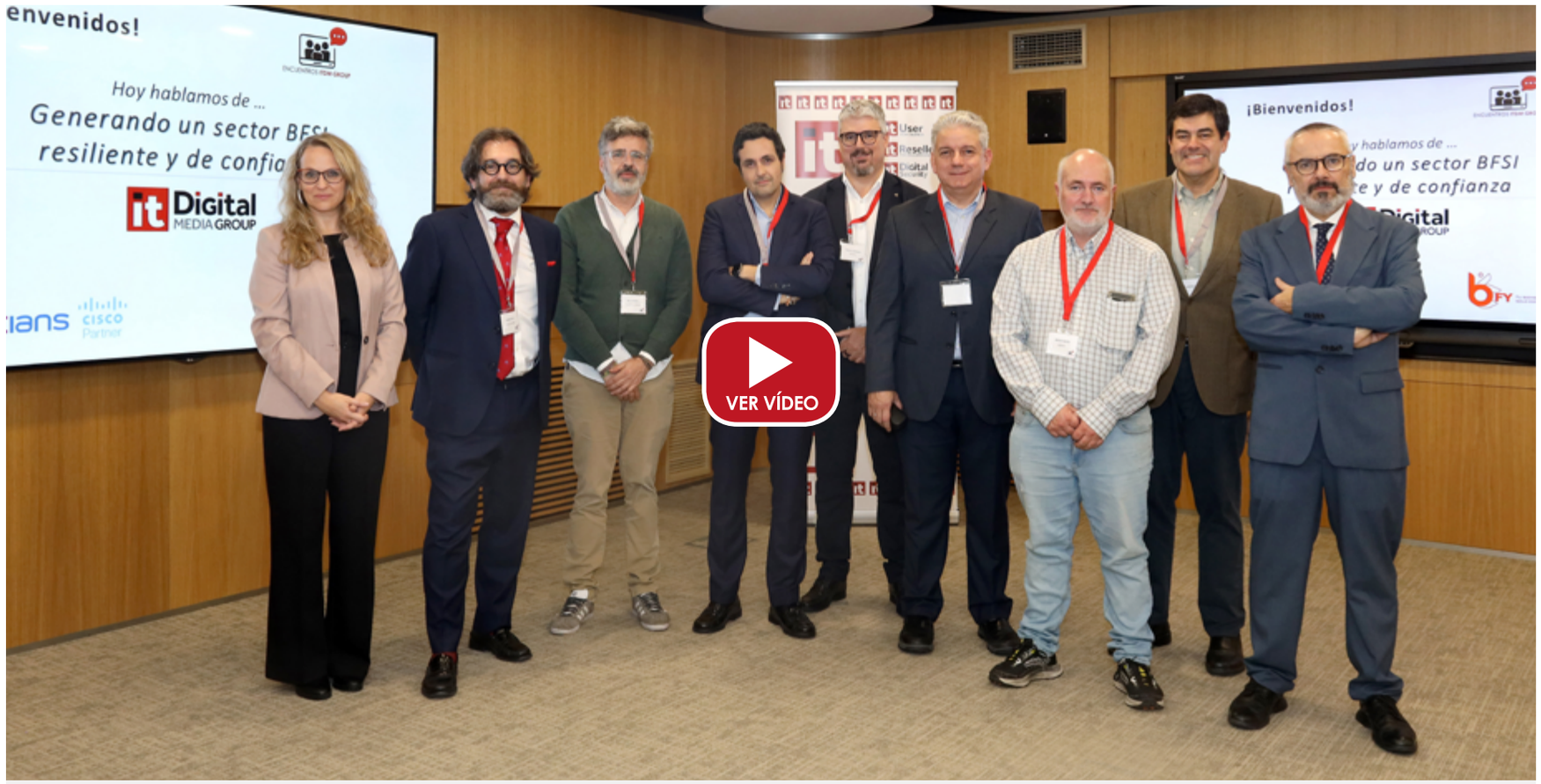
» Prioridades de transformación de un sector financiero en continua evolución

COMPARTIR EN REDES SOCIALES

GENERANDO UN SECTOR BFSI RESILIENTE Y DE CONFIANZA

El denominado sector BFSI, compuesto por compañías con actividades bancarias, servicios financieros y seguros, es uno de los más digitalizados de la economía española. Sin embargo, esta transformación genera una necesidad de avanzar hacia un nivel de resiliencia y confianza que proteja tanto la operativa del negocio como los datos de los clientes. Con Abanca, Arcano Partners, Banco Caminos, Banco Cooperativo Español, Nationale-Nederlanden y Singular Bank, y la colaboración de Axians, partner de Cisco, y B-FY, analizamos en este Encuentro IT User Tech & Business las necesidades de las empresas financieras para la generación de una operativa segura y continua.

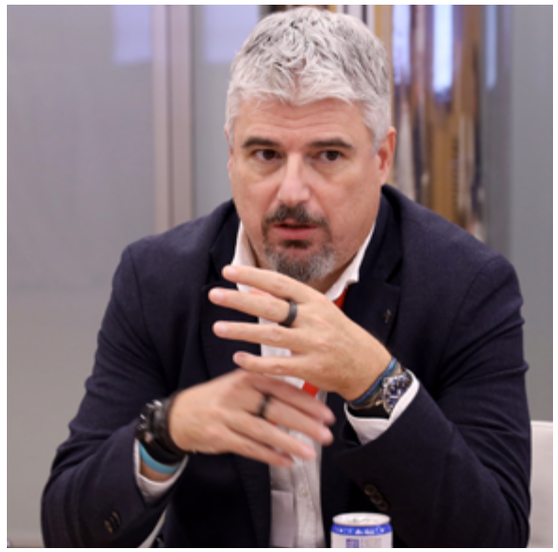
Los servicios financieros se han convertido en el tercer vector más atacado en Europa, Oriente Próximo y África (EMEA). En lo que llevamos de 2023, han sufrido un aumento del 119% de



MESA REDONDA >> Analizamos las estrategias para desarrollar un sector financiero resiliente y de confianza de la mano de Abanca, Arcano Partners, Banco Caminos, Banco Cooperativo Español, Nationale-Nederlanden y Singular Bank, con el apoyo de Axians, partner de Cisco, y B-FY.

> PUEDES TENER INFRAESTRUCTURAS IMPENETRABLES, PERO LO QUE NECESITAS PROTEGER SON LOS DATOS PARA PODER RECUPERARLOS EN CASO DE QUE SEA NECESARIO

CARLOS GONZÁLEZ,
IT Governance, Architecture and Process Director de **Abanca**



Clica en la imagen para ver la galería

> LOS ÓRGANOS DE GOBIERNO DEBEN SER LOS QUE, EN ÚLTIMA INSTANCIA, SIEMPRE ACEPTEN LOS RIESGOS Y, SI ES NECESARIO, SE IDENTIFIQUEN NUEVAS INICIATIVAS DE CIBERSEGURIDAD, DENTRO DE LA ESTRATEGIA DE LA COMPAÑÍA, QUE AYUDEN A SU MITIGACIÓN

FERNANDO SANZ DE GALDEANO,
Chief Information Security Officer de **Arcano Partners**

Clica en la imagen para ver la galería

ofensivas respecto a 2022, según recientes estudios. La rápida expansión de los canales de ventas y servicios digitales hace que las empresas BFSI persigan la continuidad de su negocio de manera continua. Disponer de infraestructuras de datos globales, reducir la latencia o mantenerse a salvo en caso de ciberataque son garantía de disponibilidad del negocio de forma ininterrumpida. ¿Cómo lograrlo? Los ingredientes de la estrategia son varios.

Para Carlos González, IT Governance Architecture and Process Director de Abanca, el principal elemento en una estrategia de resiliencia es "el dato. Puedes tener infraestructuras impenetrables, pero lo que necesitas proteger son los datos para poder recuperarlos en caso de que sea necesario. Pero estos proyectos son complicados por el entorno y por los costes, que pueden ser elevados. Por eso, lo que estamos haciendo es abordar el proyecto por fases, primero la infraestructura y después los productos y servicios, priorizando los más esenciales para la operativa diaria del negocio. Con todo, hay que ir un paso más allá de lo que supone un backup de los datos".

En este sentido, Roberto Veronesse, IT Security Delivery de la aseguradora Nationale-Nederlanden, señaló que "no solo hay que tener en cuenta las tecnologías, sino también las personas, que deben estar preparadas para un ataque, porque no se trata de si te van a atacar, sino de cómo estás de preparado cuando ocurra. Hay que implementar programas de concienciación de los usuarios, porque es el eslabón más débil de la cadena. Así que, en nuestro caso, prestamos mucha atención a preparar a los compañeros para que sepan responder a las amenazas y afrontar cualquier eventualidad".

Coincidió con él Miguel Ángel Hernández, Responsable de Riesgos Tecnológicos de Banco Cooperativo Español: “los planes de concienciación son fundamentales. Necesitas implicar a la dirección, y el marco regulativo nos ha ayudado mucho con esto. Tres de cada cuatro interacciones son telemáticas, con lo que en los datos está el dinero, y eso es lo que debemos proteger, con planes de contingencia probados y con una constante concienciación de los usuarios”.

En palabras de Pablo Blanco, Gerente de Riesgo Operacional de Banco Caminos, “la tecnología es la punta del iceberg. Están los procesos, las personas, los proveedores, la inteligencia… si no tenemos más controles que los tecnológicos, estamos ante un problema. La tecnología ayuda, pero hay que ir más allá, porque el usuario no siempre es consciente de los riesgos a los que está expuesto y hay que incidir en ello”.

INVOLUCRAR A TODA LA ORGANIZACIÓN

Y es que la seguridad de una organización, más si cabe por el riesgo que de su actividad en el sector financiero, debe implicar al conjunto de la empresa. “Además de los riesgos de ciberseguridad y continuidad que se originan en el ámbito puramente tecnológico, es necesario incluir aquellos que generan las personas y los proveedores. Toda la organización y las terceras partes deben tener su gestión del riesgo específica y conocer y colaborar estrechamente con las áreas técnicas, indicó Fernando Sanz de Galdeano, Chief Information Security Officer de Arcano Partners. “Hay vectores de ataque comunes a todas las empresas de nuestro sector, pero hay otros más específicos según cada tipología de servicio. Por eso, la seguridad debe estar presente en todas las fases de adquisición o desarrollo de nuevos servicios y procesos, tanto de negocio como tecnológicos, así como monitorizar aquellos ya existentes. Casi siempre negocio va un paso por delante y es complicado garantizar que la ciberseguridad esté incluida en todas las fases de una iniciativa, porque hay que primar la rapidez y el despliegue para generar ventajas competitivas, pero si no se garantiza la seguridad desde una potencial idea, hasta su despliegue, seguro que, a largo plazo, supone un problema. La normativa DORA nos ayuda en estas labores, dado que “obliga” a disponer de un gobierno de la seguridad y ejecutar una serie de procesos de gestión y aceptación del riesgo, y por

RESPONDIENDO A LOS RETOS DEL SECTOR

JAVIER PRIETO, ARQUITECTO DE CIBERSEGURIDAD DE AXIANS

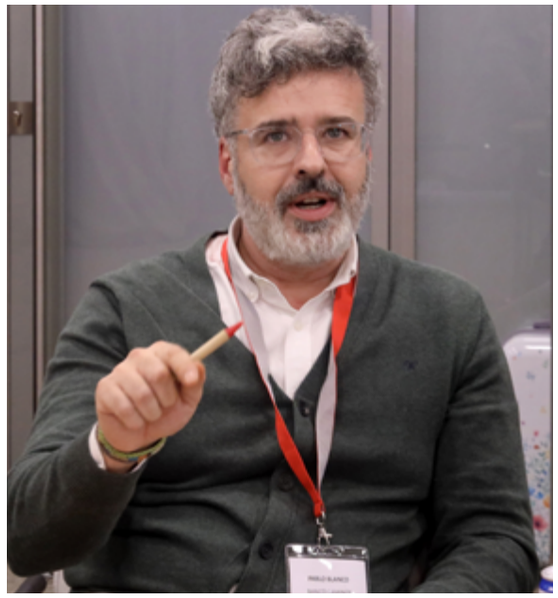
“En la gestión de la resiliencia es donde podemos aportar nuestro valor”

Javier Prieto, Arquitecto de Ciberseguridad de Axians, proveedor de servicios digitales, partner de Cisco, apuntaba que “el riesgo es la principal preocupación de las empresas financieras. En Axians, como proveedor de servicios, podemos ayudarles en la resiliencia y en el problema de la falta de talento en ciberseguridad”.

Como todas estas organizaciones saben, “el riesgo no puede estar cubierto al cien por cien, por lo que, cuando entran en una organización, es cuando es necesaria la resiliencia y los servicios asociados a ella para dar respuesta a un incidente lo más rápidamente posible. Por eso es esencial para un proveedor contar con las herramientas precisas. Desde Axians confiamos en la tecnología de Cisco para ofrecer una serie de servicios que permitan a las organizaciones levantar el negocio lo antes posible ante un incidente”.

“LA TECNOLOGÍA AYUDA, PERO HAY QUE IR MÁS ALLÁ; EL USUARIO NO SIEMPRE ES CONSCIENTE DE LOS RIESGOS Y HAY QUE INCIDIR EN ELLO”

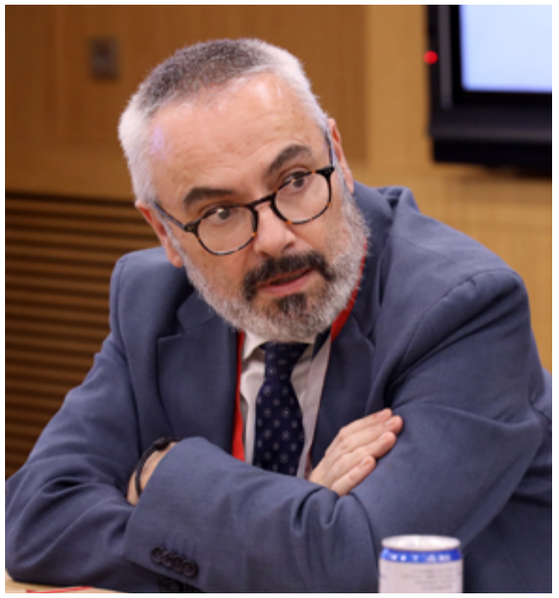
PABLO BLANCO,
Gerente de Riesgo Operacional de **Banco Caminos**



Clica en la imagen para ver la galería

“DEBEMOS PROTEGER LOS DATOS CON PLANES DE CONTINGENCIA PROBADOS Y CON LA CONSTANTE CONCIENCIACIÓN DE LOS USUARIOS QUE SEA NECESARIA”

MIGUEL ÁNGEL HERNÁNDEZ,
Responsable de Riesgos Tecnológicos de **Banco Cooperativo Español**



Clica en la imagen para ver la galería

tanto, nos faculta a los departamentos técnicos a ejecutar análisis previos a cualquier despliegue”.

Y en esta misma línea se posicionó Damián Ruiz, Chief Information Security Officer de Singular Bank. “Hay que tener en cuenta la tecnología, los procesos y las personas. DORA afecta principalmente a los procesos y eso genera mucho ruido, pero no podemos olvidar a las personas y su concienciación. Por eso estamos trabajando en un plan de respuesta a incidentes con simulación de escenarios de crisis y ataques para poder valorar la realidad y nuestra capacidad de reacción. Es una buena opción para reforzar la resiliencia de la entidad, con datos reales de la respuesta ante incidentes”, dijo.

EL VALOR DE LAS NORMATIVAS

La Ley de Resiliencia Operacional Digital (DORA, por sus siglas en inglés) es un reglamento de la Unión Europea que entró en vigor el 16 de enero de 2023 y se aplicará a partir del 17 de enero de 2025. Su objetivo es reforzar la seguridad informática de entidades financieras como bancos, compañías de seguros y empresas de inversión y garantizar que el sector financiero en Europa pueda mantenerse resiliente en caso de una interrupción operativa grave.

Sobre la aplicación de esta normativa, Fernando Sanz de Galdeano (Arcano Partners) señaló que “debemos analizar los nuevos riesgos de nuevas tecnologías y, por eso, DORA es de gran ayuda, porque nos permite establecer a nivel compañía procesos de gestión, monitorización y, en caso de que un riesgo sea superior al aceptable, escalarlo para su toma de decisión. Los órganos de gobierno de las compañías deben ser los que en última instancia siempre acepten los riesgos, aunque no siempre se haga a la velocidad que necesita negocio y las áreas técnicas sigamos teniendo la fama de bloqueantes y, si es necesario, se identifiquen nuevas iniciativas de ciberseguridad, dentro de

la estrategia de la compañía, que ayuden a su mitigación".

Carlos González (Abanca) apuntó que "combinar el cumplimiento de las normativas y avanzar con el negocio no es sencillo. Algunas normativas afectan a nivel tecnológico, otras a nivel de riesgos... pero siempre aportan elementos nuevos para analizar los posibles riesgos, como es el caso de la gestión sobre terceros de DORA, que no es realmente un problema de complejidad, sino de volumen de proveedores".

Para Damián Ruiz (Singular Bank), "sería recomendable que las normativas pusieran un foco superior en los procesos que realmente tengan un riesgo y DORA va a permitir priorizar los procesos a securizar, porque no todos afectan de la misma manera".

Y es que el control de los proveedores es uno de los puntos establecidos por DORA, si bien detectar el origen del problema no exime a las organizaciones de la responsabilidad, sobre todo en lo referente al impacto reputacional. Además, esto ayuda a los departamentos de seguridad a incrementar sus presupuestos.

IT, NEGOCIO Y SEGURIDAD

Que TI y negocio tienen que estar próximos es una afirmación cada vez más interiorizada en las organizaciones, pero ¿qué sucede con la seguridad?

En el caso de Abanca, comentó Carlos González que "seguridad no depende de TI, y eso incrementa la fricción entre seguridad, tecnología y negocio. Hay que analizar cómo puede afectar a cualquier proyecto a la compañía, y debe hacerse desde el principio, aunque es algo que no ha calado lo suficiente. Hay que seguir trabajando también en la concienciación de los usuarios, porque las tecnologías y las amenazas cambian y, con ellas, los riesgos. No podemos orillar la seguridad como tampoco lo podemos hacer con la calidad. Seguridad debe participar en las decisiones de negocio, pero sin convertirse en un stopper".

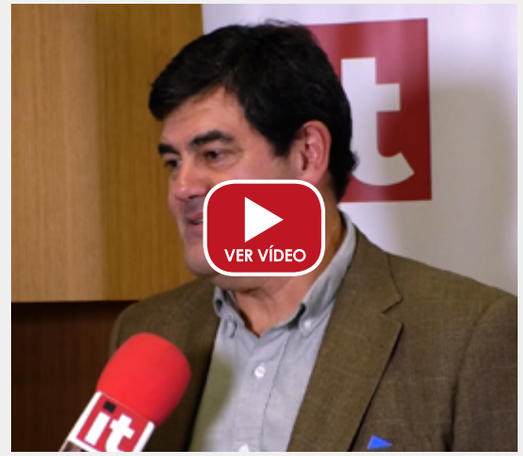
Para Pablo Blanco (Banco Caminos), "en muchos casos, negocio va por delante de la seguridad, y ésta se entera cuando ya son hechos consumados. Por eso es importante estar presentes desde el principio, aunque no podemos olvidar que los procesos y negocio priman, porque tanto en los más tradicionales como en los bancos más digitales, lo que más importa es mantener el negocio".

En este sentido, Miguel Ángel Hernández (Banco Cooperativo Español)

RESPONDIENDO A LOS RETOS DEL SECTOR

RODRIGO JIMÉNEZ, MANAGING DIRECTOR DE B-FY

"El dato es esencial para el sector financiero, y nosotros protegemos el acceso al mismo"

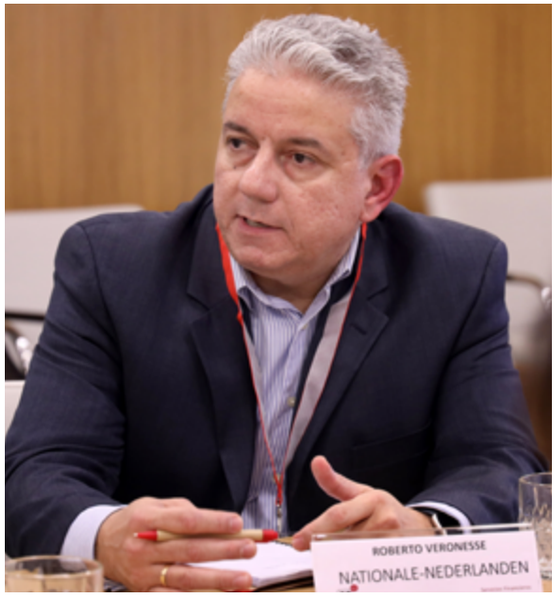


Rodrigo Jiménez, Managing Director de B-FY, compañía que ofrece tecnología de Identificación como Servicio, señaló que "estas compañías han demostrado tener un gran foco sobre la ciberresiliencia, las personas, los procesos, los datos y el propio negocio. El dato es crítico para ellos, y son organizaciones muy volcadas en el servicio al cliente".

Desde nuestra posición "podemos ayudarles a asegurarse de que la persona que quiere acceder a un servicio es quien dice ser. En la seguridad perimetral colaboramos con ellos con nuestra tecnología de Identificación como Servicio, que puede incorporarse en sus herramientas de servicio a los clientes, de tal forma que se eliminan las contraseñas para clientes y usuarios internos, lo que redunda en que la entidad no pueda sufrir un ataque para robar identidades. Además, si emplean tecnología de biometría centralizada, pueden sufrir el mismo problema si alguien roba esos patrones biométricos. Con B-FY se solucionan estos problemas porque la identificación se realiza en el propio dispositivo del usuario".

> NO SOLO HAY QUE TENER EN CUENTA LAS TECNOLOGÍAS, SINO TAMBIÉN LAS PERSONAS, QUE DEBEN ESTAR PREPARADAS PARA RESPONDER A UN ATAQUE

ROBERTO VERONESSE,
IT Security Delivery de
Nationale-Nederlanden



Clica en la imagen para ver la galería

> SE HA HECHO UN GRAN ESFUERZO CON LOS PRESUPUESTOS, PERO HAY QUE TRABAJAR MUCHO EN DEFENDERLOS BIEN ANTE LA ORGANIZACIÓN

DAMIÁN RUIZ,
Chief Information Security Officer en **Singular Bank**

Clica en la imagen para ver la galería

apostillaba que “somos bancos y nuestro principal objetivo es dar servicio al cliente, seguro, por supuesto, pero ininterrumpido”.

Un ejemplo de implicación lo aportaba Roberto Veronesse (Nationale-Nederlanden): “analizamos con compras los niveles de seguridad desde el principio del proyecto. Trabajamos con filosofía Agile, pero seguridad siempre está pendiente de los proyectos desde su arranque, aunque al alcanzar una versión operacional volvamos a analizar las vulnerabilidades”.

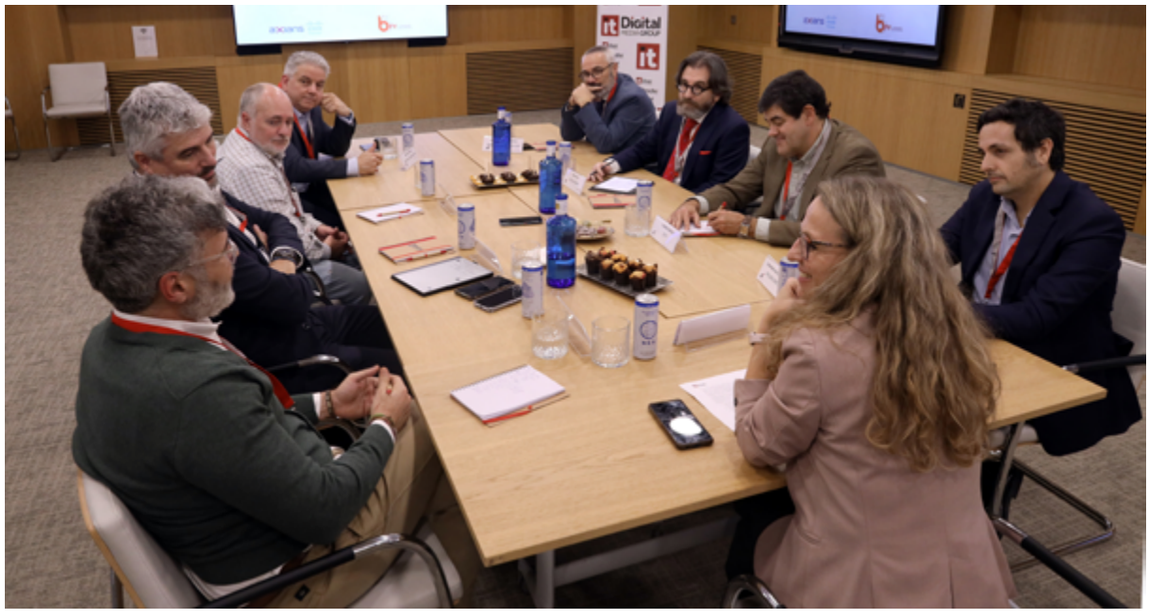
En opinión de Damián Ruiz (Singular Bank) para mejorar esa integración “hay que establecer tres capas de seguridad: tecnología, definición de controles y gestión de riesgos. Esto facilita la labor de todos los implicados. Nosotros analizamos los riesgos de todos los proyectos y, en muchos casos, de forma preventiva”.

UN PRESUPUESTO INCREMENTAL PARA SEGURIDAD

Que la continuidad del servicio en el sector financiero sea fundamental para el funcionamiento de todo el sistema ha generado una mayor atención a los presupuestos invertidos en su seguridad. Así lo recalcó Carlos González (Abanca), para quien “el negocio de los bancos es la confianza, y eso eleva los presupuestos, aunque estos han crecido más por el negocio que por la operativa de seguridad”.

Sin embargo, Pablo Blanco (Banco Caminos) apuntó que “el volumen y la complejidad de los ciberataques, junto con el entorno tecnológico dinámico, nos obliga a que haya que graduar los presupuestos según las necesidades de cada momento, adoptando la eficiencia y competitividad como pilares fundamentales”. Y es que, efectivamente, como reconocía Miguel Ángel Hernández (Banco Cooperativo Español), “hemos sido considerados un gasto durante muchos años, si bien ahora la percepción está cambiando”.

“Se ha hecho un gran esfuerzo con los presupuestos, pero hay que trabajar mucho en defenderlos bien ante la organización”, añadió Damián Ruiz (Singular Bank), “aunque también ha mejorado mucho nuestra capacidad para hablar con los consejos de administración”. “Es muy difícil y no siempre real, calcular el impacto y el coste de un potencial ciberataque, pero a veces es necesario para elevar el tono cuando se habla de presupuestos”, comentó Fernando Sanz de Galdeano (Arcano Partners), mientras que Damián Ruiz (Singular Bank) agregó que “el ROI de la ciberseguridad hay que cuantificarlo y ponerlo sobre la mesa a la hora de definir los presupuestos”.



EL PROBLEMA DE LA FALTA DE TALENTO

Sobre la mesa se puso también la cuestión de la continuidad y gestión del talento para garantizar la propia continuidad del servicio financiero. “En ciberseguridad la falta de talento no es tan problemática como en TI, pero también existe”, reconoció Carlos González (Abanca). De hecho, como apuntó Miguel Ángel Hernández (Banco Cooperativo Español), “el Banco de España estima que se van a necesitar 25.000 perfiles de seguridad y no se encuentran profesionales para cubrirlos. Y eso sin contar con la tasa de reemplazo necesaria”.

“Lo sufrimos a nivel interno cuando se publica una posición”, añadió Fernando Sanz de Galdeano (Arcano Partners), “y también en nuestros proveedores, lo que nos puede provocar un problema incluso en la provisión de un servicio. No sé si realmente es un problema de formación o capacitación, pero el problema de retención de talento es evidente, incluso en los proveedores y esto debe tratarse como un riesgo más”.

En cuanto a posibles soluciones, desde Banco Cooperativo Español, Miguel Ángel Hernández señaló que “como en España hay pocas universidades que tengan grados para cubrir este gap, hay que fomentar la colaboración entre el ámbito educativo y la empresa para paliar el problema”.

Clica en la imagen para ver la galería

De acuerdo se mostró Damián Ruiz (Singular Bank) sobre un problema que reside en “el perfil social y económico de los nuevos profesionales, en centros formativos que no cubren realmente las necesidades existentes, en la poca oferta universitaria, y en el coste de contar con los profesionales adecuados” en un momento en el que la competencia es muy fuerte.

Asimismo, apostillaba Carlos González (Abanca), “aunque la ratio de profesionales de TI y ciberseguridad es diferente, el volumen de profesionales tampoco es suficiente. Vemos, además, un gap brutal en la búsqueda de tecnólogos que se ocupen del compliance, sin olvidar que cada vez hay más apartados de la tecnología que no se reducen a ceros y unos. Es un reto adaptar los perfiles a las nuevas necesidades más allá de la tecnología. Vamos a necesitar nuevas skills para atender estas demandas y va a ser un reto adaptar a los profesionales a los nuevos requisitos, cuando necesitas una formación que no se ofrece en los centros educativos”. ■

MÁS INFO +

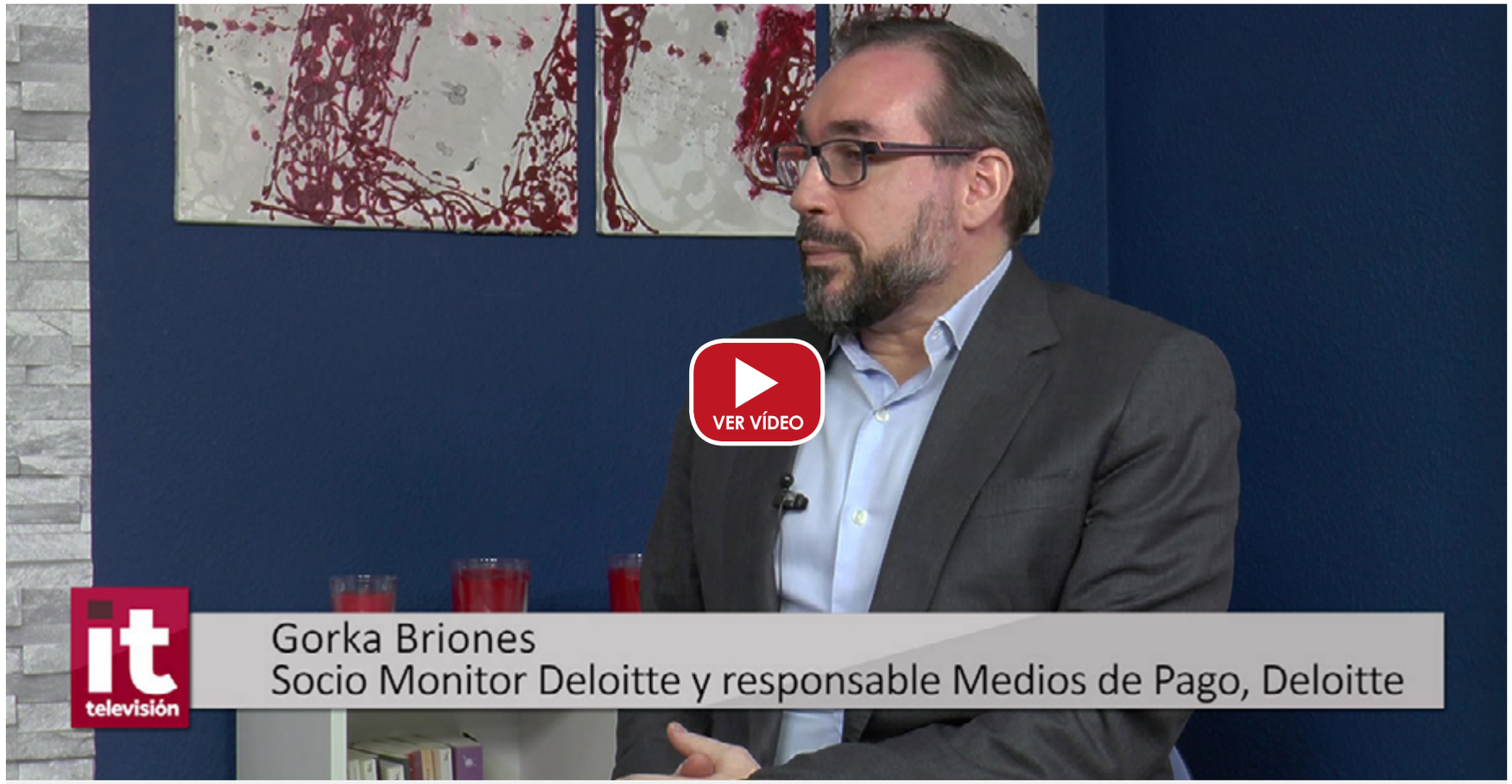
» Generando un sector BFSI resiliente y de confianza

COMPARTIR EN REDES SOCIALES

GORKA BRIONES, SOCIO DE MONITOR DELOITTE Y RESPONSABLE DE MEDIOS DE PAGO EN DELOITTE

“Los pagos inmediatos son la mayor revolución en el sector de los medios de pago”

En la segunda entrevista de este Encuentro ITDM Group: Banca y Seguros, punta de lanza de la innovación tecnológica, hablamos con Gorka Briones, Socio de Monitor Deloitte y responsable de Medios de Pago en Deloitte, quien nos habla sobre la digitalización de los servicios financieros. Comenzando por el ámbito de los pagos, que ha experimentado diversas fases de disrupción con la introducción de tecnologías que han habilitado nuevas formas de pagar para los consumidores, y que en el futuro seguirán cambiando a medida que avance la transformación digital.



ENTREVISTA >> Gorka Briones nos habla sobre la evolución del sector de banca y seguros con la llegada de nuevos medios de pago y con el Open Finance.

PRESENTE Y FUTURO DE LOS PAGOS

Gorka Briones explicaba que los medios de pago tradicionales se han digitalizado y se ha pasado de usar tarjetas físicas a tener un token

en los smartphones, que sustituye a este medio tradicional de emisión de pagos. Esto ha permitido pagar con los dispositivos móviles en comercios físicos a través de aplicaciones que también permiten pagar en plataformas de comercio electrónico. Comentaba que "lo que menos está digitalizando por ahora es la parte del efectivo, por su propia naturaleza".

Por otro lado, señalaba que los pagos inmediatos constituyen "la mayor revolución que hemos tenido en el sector de los medios de pago en los últimos años". Hace diez años teníamos tres fórmulas: "efectivo, para las transacciones entre personas o de bajo importe"; transferencias o adeudos, para los pagos domiciliados recurrentes; y tarjetas para pagos en tiendas. A esto se han sumado los pagos inmediatos, que permiten transferir dinero entre personas al momento, una tecnología que, para Gorka Briones, "se va a desplegar para que podamos hacer pagos tanto en el comercio electrónico como en los puntos de venta físicos". Pero apunta que el reto está en que estos pagos sean interoperables, para que se puedan utilizar entre entidades de diferentes países.

EVOLUCIÓN DEL DINERO EN EFECTIVO

A diferencia de lo que han expresado ciertas voces del sector, y de ciertas iniciativas para incentivar que no se use el dinero en efectivo, Gorka Briones opina que este no va a desaparecer, al menos a medio plazo. Decía que "tenemos una resistencia como sociedad a dejar el efectivo porque tiene un componente de confidencialidad, de anonimato, que la gente de alguna forma demanda". Esto es especialmente importante en la población de más edad, pero las generaciones que han asumido la digitalización tienden a usar menos la moneda corriente y, en el futuro, cuando esta sea 100% nativa digital, se podría llegar a un escenario diferente.

Por otro lado, comentaba que el Euro digital, o las Divisas Digitales de los Bancos Centrales (CBDC), "surgen precisamente como respuesta a esto", proporcionando un dinero electrónico emitido directamente por el Banco Central que sustituiría al efectivo. Señalaba que esto constituirá un quinto esquema de pago que, de alguna forma sustituiría a todos los anteriores. Esto podría complicar más la forma de pagar y cobrar ya que, si se despliegan sistemas redundantes, el sistema podría ser ineficiente.

> "OPEN FINANCE PERMITIRÁ QUE TERCEROS ACCEDAN A TODA LA INFORMACIÓN FINANCIERA PARA OFRECER SERVICIOS"
>
> **GORKA BRIONES,** Socio de Monitor Deloitte y responsable de Medios de Pago en **Deloitte**

OPEN FINANCE

Como explica Gorka Briones, la forma en que se están adoptando los principios del Open Banking en Europa consiste en "abrir las infraestructuras bancarias para que terceros nos puedan ofrecer servicios", a través de la directiva PSD2. Explicaba que "se destinó fundamentalmente a que los terceros, las fintechs, pudieran ofrecer servicios a los ciudadanos, eminentemente de pagos, operando contra las cuentas bancarias", para lo que era necesario que estos servicios pudiesen acceder a información como el saldo de las cuentas. Opina que esta forma de entender el Open Banking va a evolucionar para integrar otra información, como el saldo de la hipoteca, los fondos de inversión o los seguros de ahorro, dando forma al paradigma que se ha denominado Open Finance. Briones apuntó que "en la futura PSD3 y con la nueva directiva FIDA, que se está diseñando actualmente, se permitirá que terceros, de carácter tecnológico, "puedan acceder no solo a tu información de pagos, a tu información de cuenta corriente, sino a toda la información financiera". ■

MÁS INFO +

» Encuentro ITDM Group Banca

COMPARTIR EN REDES SOCIALES

FlexxClient

by Flexxible®

DANIEL RODRÍGUEZ, DIRECTOR GENERAL DE REDTRUST

“El sector financiero es el primero en detectar las nuevas amenazas”

La siguiente entrevista que forma parte del Encuentro ITDM Group: Banca y Seguros, punta de lanza de la innovación tecnológica, se centra en la ciberseguridad en el sector financiero. Para ello hablamos con Daniel Rodríguez, director general de Redtrust, quien nos explica cuáles son las principales amenazas cibernéticas que afectan a la industria y cómo se enfrentan a ellas las entidades para proteger sus activos y los de sus clientes. Además, nos explica qué retos tecnológicos y de talento están surgiendo el sector en relación a la ciberseguridad.

ENTREVISTA >> Daniel Rodríguez nos brinda su visión sobre la ciberseguridad en el sector financiero español y cómo enfocan sus servicios para esta industria.

TECNOLOGÍA PARA ENFRENTARSE A LAS AMENAZAS

Daniel Rodríguez señalaba que en la industria financiera hay dos velocidades en cuanto a la modernización tecnológica. Por un lado, en lo que

se refiere al negocio en sí, el sector "se mueve lentamente en cuanto a renovación tecnológica. En cambio, en ciberseguridad las empresas están siempre a la última, siempre buscando nuevas soluciones", y son los primeros en detectar las nuevas amenazas que surgen. Y destacó que precisamente por esto buena parte de sus clientes son bancos, siendo el segundo sector en el que actualmente tienen más clientes.

En cuanto a las ciberamenazas más importantes para el sector bancario y las finanzas destacó las denominadas amenazas avanzadas persistentes, como las APT. Como explicaba Daniel Rodríguez, para su compañía la más importante es el "robo de identidad, tanto por parte del empleado de la propia entidad bancaria, como del cliente". Por ello, las entidades financieras no pueden limitarse a la protección de sus propios sistemas, sino que necesitan proteger la identidad de sus clientes, adoptando medidas de identidad seguras, algo que aportan desde Redtrust.

ESTRATEGIAS DE CIBERSEGURIDAD

Para Daniel Rodríguez, es obvio que los empleados son el principal punto de entrada para acceder a las entidades financieras, y destacó el riesgo de la suplantación de identidad, tanto a nivel de empleado como de empresa, ya que alguien podría firmar algo en nombre de dicha empresa. Concretamente, las entidades españolas hace años que están obligadas a tener su certificado digital para identificarse frente a las Administraciones Públicas, pero se trataba de un único certificado, lo que elevaba el riesgo de suplantación de esa identidad.

> "NUESTRA PROPUESTA PARA 2024 SE BASA EN LA GESTIÓN DE IDENTIDAD DIGITAL BASADA EN EL CERTIFICADO DIGITAL"
>
> **DANIEL RODRÍGUEZ,**
> Director general de **Redtrust**

En cuanto a sus estrategias de ciberseguridad, Rodríguez considera que los directivos españoles del sector "están bastante concienciados, cada vez más", y destacó que "ya no tenemos que ir a explicarles cuál es nuestra idea de gestión de la identidad digital, sino que vienen ellos a nosotros, ya directamente con la idea preconcebida". Por ello, y gracias a que el ecosistema de ciberseguridad en España es muy bueno, opina que el sector aventaja al de otros países de nuestro entorno.

NOVEDADES PARA 2024

La propuesta de Redtrust para el año que viene en materia de ciberseguridad se centra en la "gestión de identidad digital basada en el certificado digital, tanto para la empresa como para el propio empleado". En palabras de Daniel Rodríguez, esta consiste en crear una serie de políticas con las que poder permitir o denegar el uso de ese certificado digital, y en hacerlo con transparencia para "no ir en detrimento de la usabilidad". Destacaba que normalmente usabilidad y seguridad chocan entre sí, pero ellos siempre intentan facilitar las cosas tanto a los administradores de sistemas como a los propios usuarios. Tratan de que "el administrador tenga una visibilidad total de lo que está sucediendo y qué se está haciendo con los certificados digitales de su empresa", y "que el usuario final tenga la seguridad y la tranquilidad de que no pueda extraviarse ese certificado por un error suyo".

También destacó su intención de seguir expandiéndose internacionalmente y que "hay diferentes casos de uso para otros mercados, como pueden ser otros más centrados en la firma digital, en la firma electrónica. No tanto en la autenticación con la identidad digital, sino en la firma con PDF, firma macro o firma de código", casos en los que se está planteando un enfoque similar al que había en España hace unos años. ■

MÁS INFO +

» Encuentro ITDM Group Banca

COMPARTIR EN REDES SOCIALES

We Keep Your
Business Running

veeam

Radical Resilience Starts Here

Data Security Data Recovery Data Freedom

LEARN MORE

EL SECTOR FINANCIERO, PUNTA DE LANZA DE LA INNOVACIÓN TECNOLÓGICA

El sector de la banca y los seguros está llevando a cabo una profunda transformación impulsada por la tecnología, tanto a nivel interno como de cara a sus clientes, que demandan nuevas fórmulas financieras que se integren mejor en un estilo de vida cada vez más vinculado a lo digital.

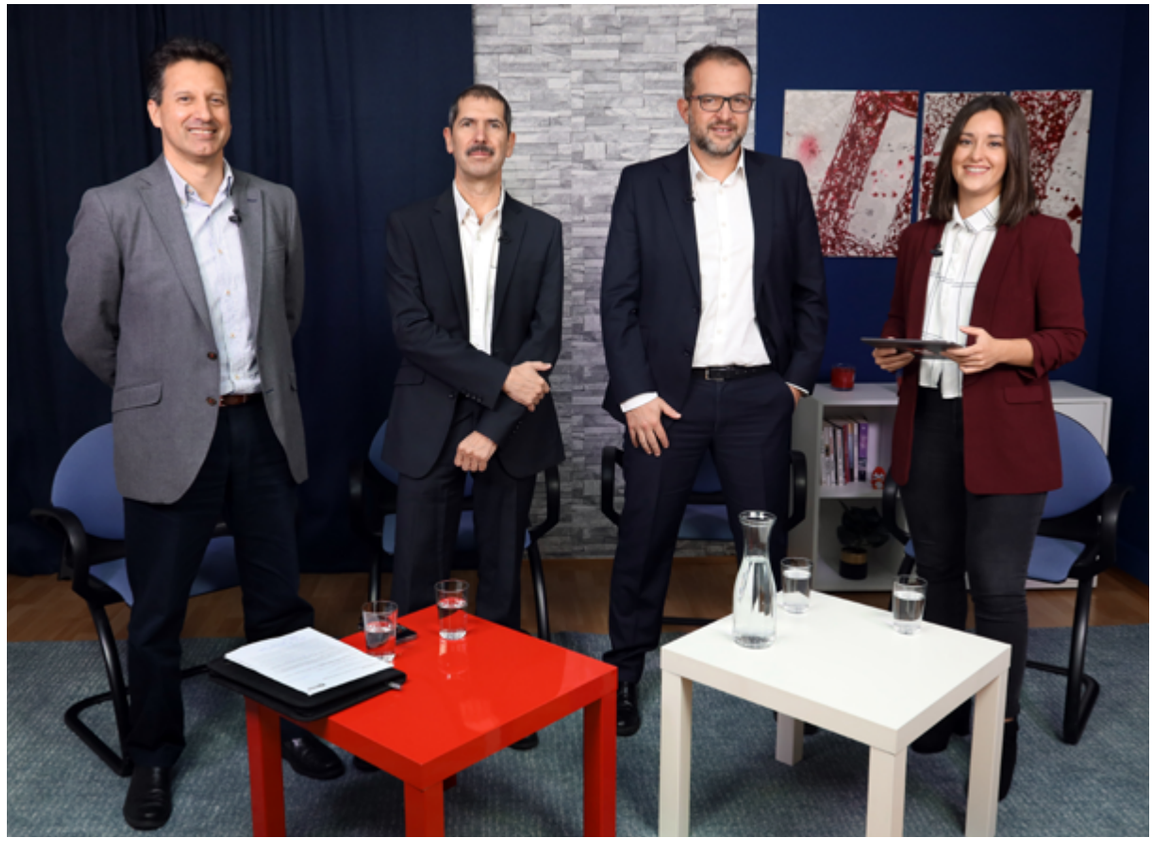
Para conocer en profundidad qué supone esta modernización para la industria financiera y qué retos están surgiendo en torno a las nuevas tecnologías y servicios bancarios

MESA REDONDA >> Debatimos con representantes de importantes firmas de ciberseguridad, servicios e infraestructura sobre la transformación digital del sector de banca y seguros. Nos desvelan las claves de la rápida evolución que está experimentando esta industria a raíz de las nuevas tecnologías y estrategias comerciales, que plantean nuevas vías de negocio, pero también muchos desafíos.

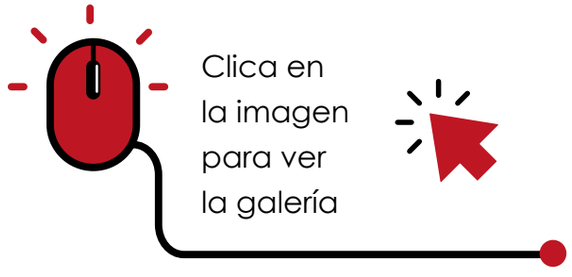
hablamos con Raúl Benito, Territory Account Manager de Bitdefender; Jaime Rubio, director de Servicios Profesionales de MicroStrategy; y José Alfonso Gil, Service Sales director Southern Europe de Vertiv.

MODERNIZACIÓN DE INFRAESTRUCTURA Y SERVICIOS

Para seguir avanzando al ritmo que marcan las nuevas tendencias y tecnologías el sector financiero lleva años modernizando su infraestructura para impulsar la innovación en sus procesos de negocio y en el trato con sus clientes. Desde el punto de vista de la propia infraestructura, José Alfonso Gil, de Vertiv, apuntaba que el sistema bancario está inmerso en la misma evolución digital que está experimentando la sociedad. Concretamente, los bancos "están yendo más hacia el cloud híbrido, siempre intentando cumplir con todas las necesidades de seguridad" lo que, en su opinión, "está llevando a una atracción muy importante de hiperescalares y proveedores de colocation, que dan servicios a los bancos, grandes clientes suyos". Añadía que, al mismo tiempo, están surgiendo "nuevas aplicaciones y formas de relacionarse con el cliente, y nuevas empresas que ya son totalmente virtuales".



Por su parte, Jaime Rubio, de MicroStrategy, destacaba dos grandes movimientos a nivel de infraestructura en los bancos. Por un lado, la migración a la nube de sus aplicaciones, salvo algunas de naturaleza muy crítica que por el momento se están manteniendo en entornos on-premise. El segundo tendría más que ver con el negocio bancario, que se está volviendo "cada vez más abierto e



internacional, y donde ha cambiado mucho la forma de relacionarse con sus clientes". Señala que, mientras que "antes era un trato muy directo con el agente bancario o el director de la sucursal, ahora es un trato desde el ciberespacio". Y en este contexto el uso de datos y analítica está ganando peso a la hora de establecer y modificar las estrategias comerciales.

Para Raúl Benito, de Bitdefender, "el sector bancario es el estandarte de la transformación digital", en parte porque las entidades siempre tratan de adelantarse a los cambios tecnológicos que van surgiendo para no perder competitividad. Considera que esta transformación se ha visto en las sucursales, pero también en todos sus procesos internos, con la automatización de las operaciones, la trazabilidad y la interconexión entre diferentes países. Coincidía con Jaime Rubio en que, ante la disminución del trato personal con el cliente, la analítica de datos se ha vuelto esencial para comprender sus necesidades y desarrollar productos a medida. También destacó como la digitalización ha impulsado el cierre de sucursales en los últimos años, y alabó cómo "los bancos están mucho más globalizados, la cantidad de servicios que han puesto en el mercado es increíble y lo han hecho sin que nos diésemos cuenta".

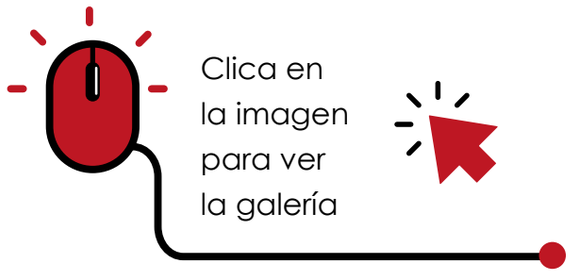
José Alfonso Gil añadía que, con el progreso digital, y aprovechando

los datos que reciben, los bancos han empezado a ofrecer servicios más allá de los financieros, y opinaba que “probablemente van a seguir aumentando todos esos servicios, esas ventas que hacen a través de aplicaciones o en la misma oficina”. Jaime Rubio añadía que “esto afecta a muchos otros, porque todo ese negocio mixto tiene que ver con comunicaciones y operaciones entre diferentes entidades, y la seguridad ahí es fundamental”. Para Raúl Benito, “ha cambiado un poco el paradigma de la seguridad”, y cosas que antes no eran viables desde el punto de vista de la ciberseguridad ahora sí son securizables. En su opinión, “la labor del CISO dentro del comité de dirección ha cambiado radicalmente y ahora la seguridad se está viendo más como un facilitador”, por lo que aporta al negocio “y porque el usuario también lo busca”.

EL PAPEL DEL CENTRO DE DATOS Y EL EDGE

Para soportar toda esta nueva generación de servicios las entidades se apoyan cada vez más en la nube, trasladando gran parte de la infraestructura a los proveedores de colocation e hiperescalares. Aunque

> “EL SECTOR BANCARIO ES QUIEN ESTÁ DIRIGIENDO HACIA DÓNDE VA LA INDUSTRIA”
>
> **RAÚL BENITO,**
> Territory Account Manager de **Bitdefender**



el Edge todavía tiene un papel importante, en opinión de José Alfonso Gil, que considera el perímetro como “parte de una misma cadena de CPD conectados”. Señalaba que “la parte de hyperscale está dando servicios a los bancos, pero el Edge es una parte natural del sistema bancario”, vital para tener parte de las aplicaciones en las oficinas y reducir la latencia.

Jaime Rubio indicaba que los bancos “llevan tiempo repensando el rol de las

oficinas para intentar dar más servicio que el que ya tienes a través de la aplicación de Internet”, y José Alfonso Gil añadió que las entidades necesitan “centros de datos totalmente fiables, con una infraestructura capaz de asegurar el funcionamiento 99,999 y, por supuesto, con un sistema de mantenimiento”. Destacaba la necesidad de poder recuperar los servicios de manera inmediata, ya sea en una oficina o en un gran CPD, pero en este sentido hay dos modalidades. Están los bancos que poseen y mantienen su propia infraestructura, y los que recurren a proveedores de colocación e hiperescalares, que también tienen “esos equipos perfectamente mantenidos y esperando a solucionar cualquier problema que surja”.

MÁS RESILIENCIA PARA GARANTIZAR LOS SERVICIOS

Como comentaba Raúl Benito, los equipos de ciberseguridad o el propio CISO no nacen para evitar que algo pase, sino para reducir el riesgo y saber cómo actual y recuperarse lo antes posible tras sufrir un incidente. Por ello, decía, “se está invirtiendo mucho más en analítica de datos, inteligencia artificial, monitorización, toda esa visión de lo que está pasando, para ver cómo recuperarse tras un incidente”. Comentaba que, al igual que en infraestructura se intenta reducir el tiempo de recuperación ante caídas eléctricas y otros incidentes, en ciberseguridad la clave es volver a funcionar lo antes posible tras un ataque, y que “todos los servicios estén funcionando y no corras el riesgo de que esa amenaza se vuelva a replicar”, algo que en el sector bancario implica una disponibilidad de más de 99,999.

Opinaba que la velocidad es un factor clave en un sector que con la digitalización debe ofrecer servicios

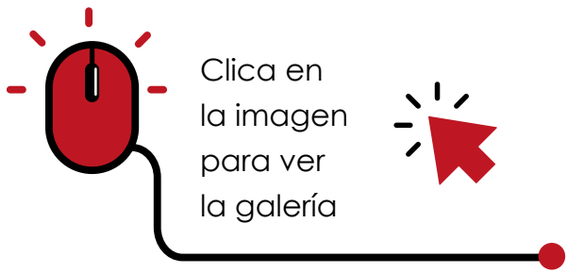
al microsegundo y “permitir que los clientes puedan pasar de un banco a otro, de una pasarela de pago a otra, en cuestión de segundos”. La gran competencia que está surgiendo con las finanzas digitales está impulsando la innovación y la digitalización del sector bancario, y considera que “el sector bancario es quien está dirigiendo hacia dónde va la industria o a qué necesidades tenemos que responder para garantizar la continuidad del negocio”. Lo mismo opinaba José Alfonso Gil, que destacaba la dependencia entre el sector bancario y el de telecomunicaciones, al que demanda la capacidad, velocidad y confiabilidad necesaria para que nada falle.

APORTACIÓN DE LA INDUSTRIA TECNOLÓGICA

Cada uno de los participantes de esta mesa redonda aporta desde sus respectivas compañías diferentes soluciones enfocadas a la industria de la banca y los seguros. En el caso de Bitdefender, Raúl Benito comenta que cuentan con servicios de monitorización de alerta 24/7 para cualquier empresa del sector bancario. Explicaba cómo “los sistemas EDR, MDR, de monitorización, de detección y de respuesta, que tenían un

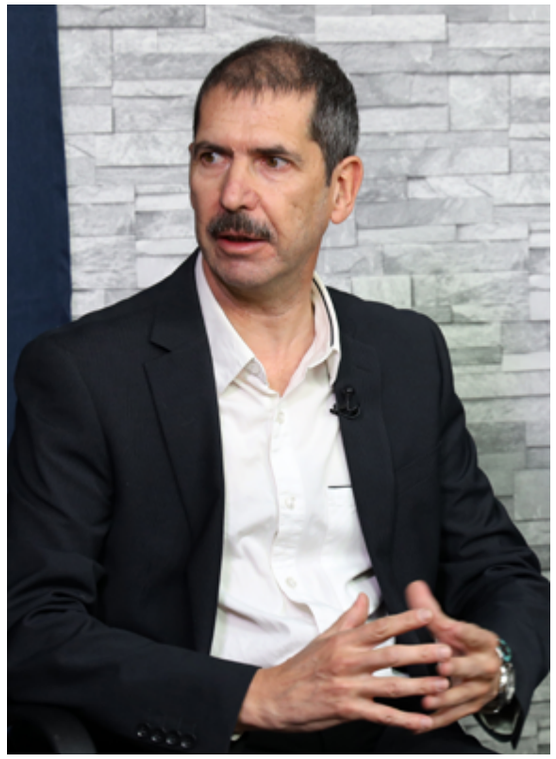
> “LOS BANCOS VAN A TENER PARTE DE NEGOCIO PROPIO Y PARTE DE SERVICIOS FINANCIEROS A TRAVÉS DE TERCEROS”

JAIME RUBIO,
Director de Servicios Profesionales de **MicroStrategy**



precio fuera de mercado para cualquier otra empresa”, se han vuelto más accesibles. Atribuye esto a la digitalización y a la gran competitividad en el sector de la ciberseguridad, y desde su compañía se centran en aportar a los clientes la tranquilidad de que su negocio esta seguro.

Jaime Rubio decía que las entidades bancarias siguen necesitando el reporting tradicional, la cuenta de resultados, los saldos de la sucursal, el seguimiento de objetivos para la red comercial, etcétera. Pero, por otro lado, son conscientes de que necesitan explorar nuevas tendencias como la analítica avanzada basada en el big data, y por ello llevan tiempo trabajando en ciencia de datos. A esto se ha sumado la irrupción de la inteligencia artificial, y todos quieren trabajar con ella. MicroStrategy proporciona todas las herramientas que tienen que ver con la analítica de datos, “desde el aprovisionamiento de datos a la explotación”, a la que es-



tán incorporando capacidades de IA. Esto supone un reto, ya que hay que aprender a usar una nueva tecnología y porque los modelos de IA no están en la entidad, sino en proveedores externos. Destacó un caso de uso que ya tienen las entidades bancarias, que es la capacidad de que sus analistas de negocio hagan analítica de datos corporativos impulsada por IA, aprovechando el reconocimiento de lenguaje natural.

Desde Vertiv, como explicaba José Alfonso Gil, se centran en la infraestructura que soporta los servicios digitales desde el centro de datos, proporcionando la energía necesaria para que los sistemas funcionen, y el enfriamiento que requieren los equipos, a través de “un producto fiable, preparado para específicamente para los centros de datos, desarrollado para centros de datos, tanto en UPS como en aire acondicionado, sistema eléctrico del CPD, etcétera”. A esto se suma un servicio de mantenimiento con “técnicos perfectamente preparados, que se están formando de manera continua”. Además, proporcionan sistemas de monitorización como parte de ese mantenimiento y servicios de auditoría de centros de datos para “buscar mejoras en la

climatización y el sistema eléctrico, reducir los costes de la energía buscando mayor eficiencia y, por tanto, ayudando a los clientes a cumplir con sus objetivos ESG".

CAMBIO IMPULSADO POR DATOS

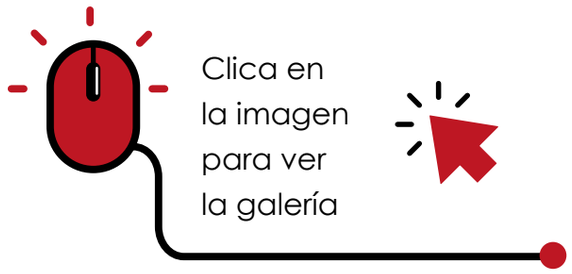
El dato se ha convertido en un activo para empresas de todos los sectores, pero en el bancario es todavía más importante, así como garantizar su seguridad para velar por su veracidad y coherencia, de forma que sirva para impulsar la toma de decisiones. Raúl Benito ponía como ejemplo que "la inteligencia artificial toma decisiones en función de los datos que están obteniendo, y si tenemos una mala adecuación de esos datos, o una transformación de los datos, tenemos un grave problema". De igual forma opinaba el representante de Microstrategy, para quien la cultura data-driven materializa la idea de que en la banca no se pueden tomar decisiones basadas en la intuición, sino en datos fiables y contrastados. Y, en su opinión, especialmente en el sector financiero, "el tema de la confidencialidad, la privacidad de datos y la seguridad es primordial".

José Alfonso Gil añadía que la importancia de los datos se extiende

a todas las áreas, incluyendo la de infraestructura, que más trabajan en Vertiv. En este contexto, opina que las máquinas van a estar cada vez más sensorizadas, y que "vamos a pasar en algún momento de un mantenimiento preventivo a sistemas que van a ser mucho más predictivos". Comentaba que "cada vez vamos a sacar más información de las máquinas, a intentar estar más dentro del cliente en ese sentido y traernos más información a nuestras propias inteligencias artificiales para analizar esos datos" que sirven para lanzar avisos que permitirán un mantenimiento constante y menos reactivo.

> "EL MÓVIL Y LAS ENTIDADES BANCARIAS CADA VEZ VAN A ESTAR MÁS UNIDOS"

JOSÉ ALFONSO GIL,
Service Sales Director Southern Europe de **Vertiv**



TENDENCIAS DEL SECTOR FINANCIERO

La digitalización viene acompañada de numerosos cambios para las entidades, y José Alfonso Gil apuntaba que los clientes jóvenes demandan otro modelo de banca, más ligado a ecosistemas digitales que a sucursales físicas. Opina que a medida que se sucedan los cambios generacionales, cabe la posibilidad de llegar a un escenario en el que no haya oficinas. Incluso "puede ocurrir que todo esté centralizado en grandes centros de datos, que la ciberseguridad solamente tenga que estar en los centros de datos", así como la inteligencia artificial y los datos que manejan los bancos. Pero la tendencia que ve más cercana es que "el móvil y las entidades bancarias cada vez van a estar más unidos", y que probablemente los grandes marketplaces sigan ampliando los servicios financieros para los consumidores. Además, cree que, a medida que desaparezcan las oficinas, lo mismo podría suceder con el Edge en el sector bancario, aunque desde Vertiv seguirán teniendo un papel en este sector, ya que siempre va a haber infraestructura, y considera que son "una parte vital de todo ese conglomerado" que conforman las entidades, los centros de datos y los sistemas de comunicaciones.

Desde MicroStrategy, Jaime Rubio percibe que "los bancos van a tener parte de negocio propio y parte de servicios financieros a través de terceros, algo que ya existe". Pone como ejemplo que ahora se puede

pedir un préstamo a una financiera directamente en un concesionario al comprar un coche, y esto se trasladará a entornos como los marketplaces, donde en el futuro podría contratarse un préstamo o un seguro. La aportación que pueden hacer desde su compañía tiene que ver con que “cualquier proceso de negocio arrastra hoy en día una generación de datos para optimización, mejora, análisis de riesgos…” Y tratan de dar respuesta a la necesidad de los bancos de que el dato sea más inteligente, para lo que siempre han contado con un extractor de cuentas, cuenta de resultados, saldo de oficina, que ahora aporta más inteligencia con predicción de precios, análisis de riesgos, todo desde “una plataforma corporativa que por debajo lleva una capa semántica que refleja el negocio”.

Por último, Raúl Benito opinaba que “el sector financiero va a evolucionar de forma radical”, y en un futuro las entidades o agentes actuales se habrán transformado en otros. Comentaba que el Edge ya no estará en la calle en oficinas que probablemente desaparecerán, sino integrado en el marketplace online, y que muchas entidades continuarán haciendo cosas nuevas, al igual que los grandes marketplaces de consumo se están inundando de servicios financieros. Desde Bitdefender aportan la confianza en que los servicios financieros son seguros, proporcionando la capacidad de ciberseguridad que requieren los procesos que hay detrás de esos servicios, logrando que “el cliente final se sienta cómodo al utilizar las herramientas en cualquier lugar”. ■

Clica en la imagen para ver la galería

MÁS INFO +

» El sector financiero, punta de la lanza de la innovación tecnológica

COMPARTIR EN REDES SOCIALES

redtrust
a KEYFACTOR company

IDENTIDAD DIGITAL SEGURA
EN BANCA Y ASEGURADORAS

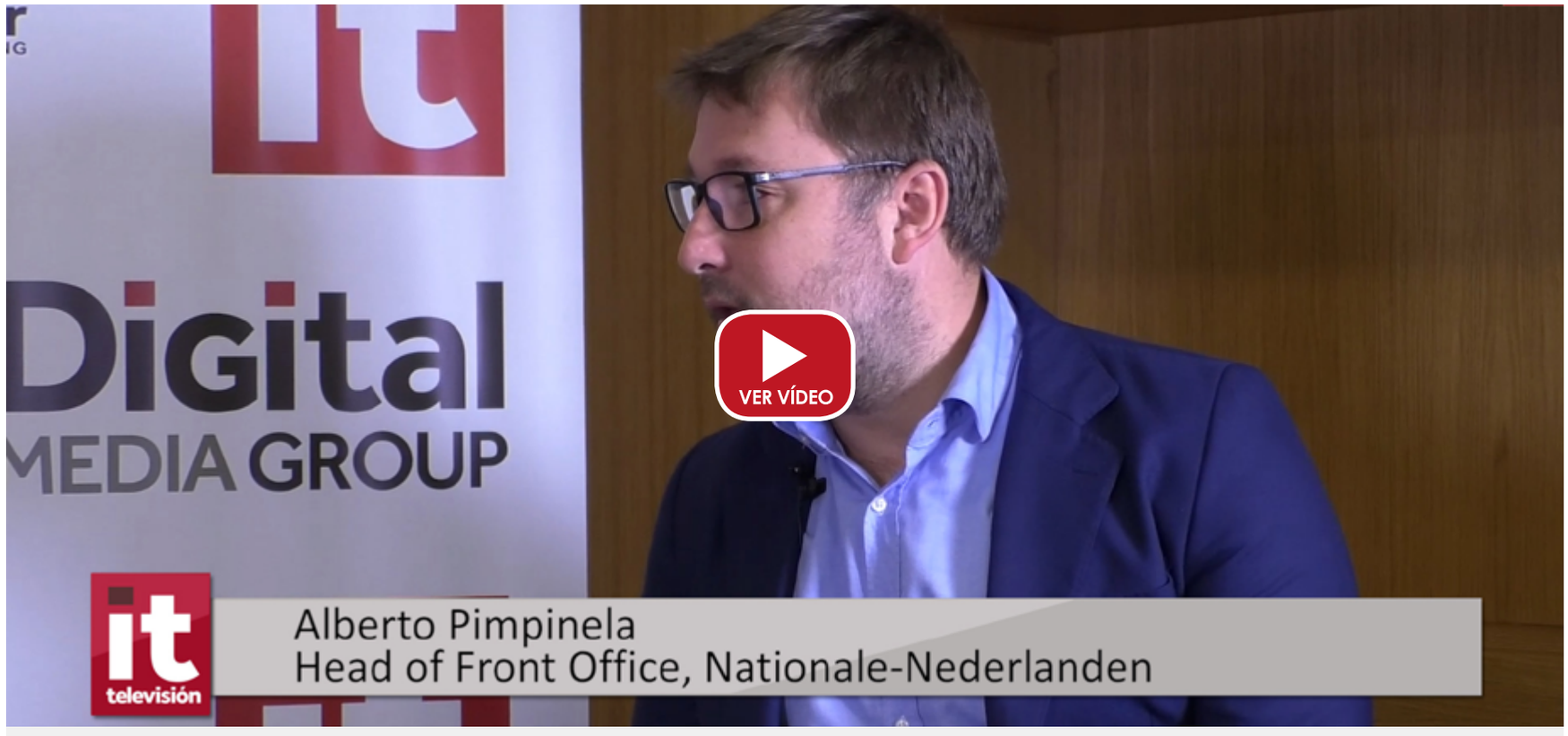
Gestión centralizada y control de los certificados digitales

- Custodia en **servidor seguro**
- **Movilidad total** de los certificados
- Gestión de **permisos de uso**
- Creación de **alertas de caducidad**
- **Trazabilidad** de acciones y usuarios

ALBERTO PIMPINELA, HEAD OF FRONT OFFICE, NATIONALE-NEDERLANDEN

“Orientamos la tecnología a tres pilares fundamentales: los datos, la conexión con terceros y el frontend”

Cerramos el Encuentro ITDM Group: Banca y Seguros, punta de lanza de la innovación tecnológica, con una entrevista a Alberto Pimpinela, Head of Front Office, Nationale-Nederlanden, una entidad bancaria con cerca de 850.000 clientes en España que ofrece muchos servicios en el ámbito digital. Comienza explicando que en 2014 se gestó el embrión de lo que actualmente es su proceso de venta, y fueron de las primeras empresas de banca y seguros en las que sus agentes comerciales vendían todos sus productos íntegros a través de un tablet.



ENTREVISTA >> Alberto Pimpinela, de Nationale-Nederlanden, nos explica cómo han abordado la transformación digital a lo largo de la última década.

TRANSFORMACIÓN INTERNA

Alberto Pimpinela comentaba que a lo largo de la última década la

compañía ha continuado su transformación en diversos ámbitos. Por ejemplo, en Madrid “empezamos a trabajar con herramientas digitales en la gestión de postventa, con un CRM que ya llevaba muchos años instaurado, pero seguía evolucionando a este proceso de venta digital”. En 2017 comenzaron a “aplicar metodología ágil para trabajar en los equipos de desarrollo, para llevar productos a producción”, mezclando en los mismos equipos negocio, test, desarrollo, etcétera. Y en 2019 lanzaron la primera prueba de concepto de su aplicación móvil para clientes, que el año que viene sufrirá una importante actualización que considera disruptiva.

Otras grandes transformaciones son su viaje a cloud, que comenzó en 2017-2018, y su inversión en ciberseguridad, con un equipo dedicado que se constituyó en 2017 y ha ido creciendo. Además, Alberto Pimpinela señalaba que han seguido adoptando tecnologías digitales y se encuentran en pleno proceso de migración de su CRM, con el que consideran que tendrán un valor diferenciador frente a otras compañías. Y que han ido desarrollando departamentos cada vez más específicos,

> “LA GOBERNANZA DE LA NUBE Y LA ADOPCIÓN DE SAAS SON FUNDAMENTALES PARA LA ESTABILIDAD Y EL CONTROL DEL GASTO”
>
> **ALBERTO PIMPINELA,** Head of Front Office, **Nationale-Nederlanden**

con talento especializado en cada área de tecnología, como frontend, backend, cloud, infraestructura y seguridad, entre otros.

TECNOLOGÍAS CLAVE PARA EL NEGOCIO

Para Alberto Pimpinela, lo principal son las tecnologías orientadas a tres pilares fundamentales. El primero tiene que ver con los datos, con cómo utilizarlos para la creación de productos. El segundo es lo que denominaba “third party connectivity”, con una capa de apificación que les permite conectarse con terceros para generar servicios. Por último, está la capa frontal, que están empezando a modernizar para proporcionar a sus equipos de ventas tecnologías fáciles de usar para ellos y también para el cliente “para salir un poco de estándares antiguos, visores antiguos”.

Todo esto se apoya en una infraestructura basada en gran medida en la nube pública, salvo algunos servicios on-premise, como su sistema de gestión de póliza, que debe estar en local. Por ello, considera que la gobernanza de la nube y la adopción de servicios SaaS son fundamentales para mejorar la estabilidad y el control del gasto.

RETOS PARA EL SECTOR

Uno de los principales desafíos para Nationale-Nederlanden es cumplir con las regulaciones vigentes y futuras, algo que, como explica Alberto Pimpinela, “afecta puramente a la tecnología, proveedores, modelos de servicio…” y también a los modelos de negocio, ya que “el sector asegurador es un sector muy regulado por varios organismos”. Esto implica cambios frecuentes en los procesos de venta, postventa, información de datos y otras áreas, y la tecnología y los proveedores deben cubrir nuevas necesidades, como en la identificación o la seguridad del dato.

Otro gran reto proviene de la necesidad de aplicar innovación para responder a los constantes cambios tecnológicos, y en su compañía deben establecer guidelines que guíen la toma de decisiones sobre tecnología para poder comprometerse con ellas y seguir avanzando en el camino correcto. También considera un desafío la adaptación de la cultura en la organización, no solo de los trabajadores de TI, sino del resto de departamentos, para fomentar la aceptación de los cambios tecnológicos. Esto también tiene que ver con el reto del talento digital, algo que en Nationale-Nederlanden abordan invirtiendo en la capacitación de su personal a nivel interno. ■

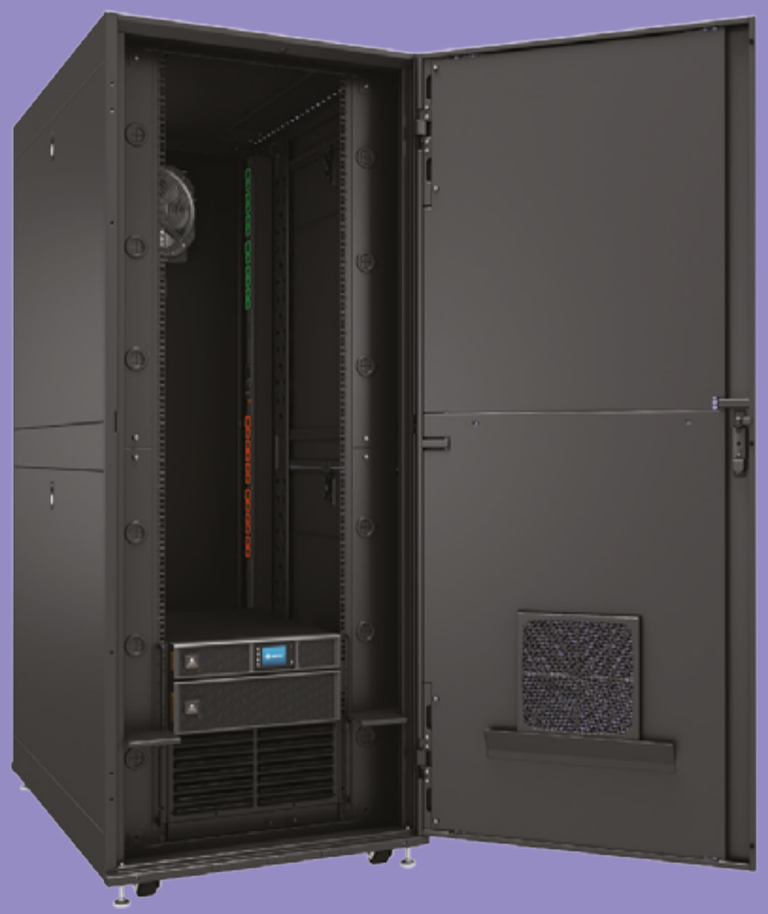
MÁS INFO +

» Encuentro ITDM Group Banca

COMPARTIR EN REDES SOCIALES

VERTIV™

¿Poco espacio TI?



Piensa en pequeño.

Descubre **Vertiv™ VRC-S**, un microcentro de datos todo en uno preparado para el Edge. Diseñado para una rápida y fácil instalación, este rack de TI totalmente ensamblado en fábrica viene equipado con SAI, refrigeración y distribución eléctrica inteligente.

- **SAI Vertiv™ Liebert® GXT5** con certificado Energy Star 2.0
- **PDU en rack Vertiv™ Geist™** para una distribución y monitorización inteligentes
- Unidad de refrigeración para rack **Vertiv™ VRC**
- 3 años de garantía para el sistema completo*

Vertiv.com/VRC-S-ITU

Available on the App Store

GET IT ON Google Play

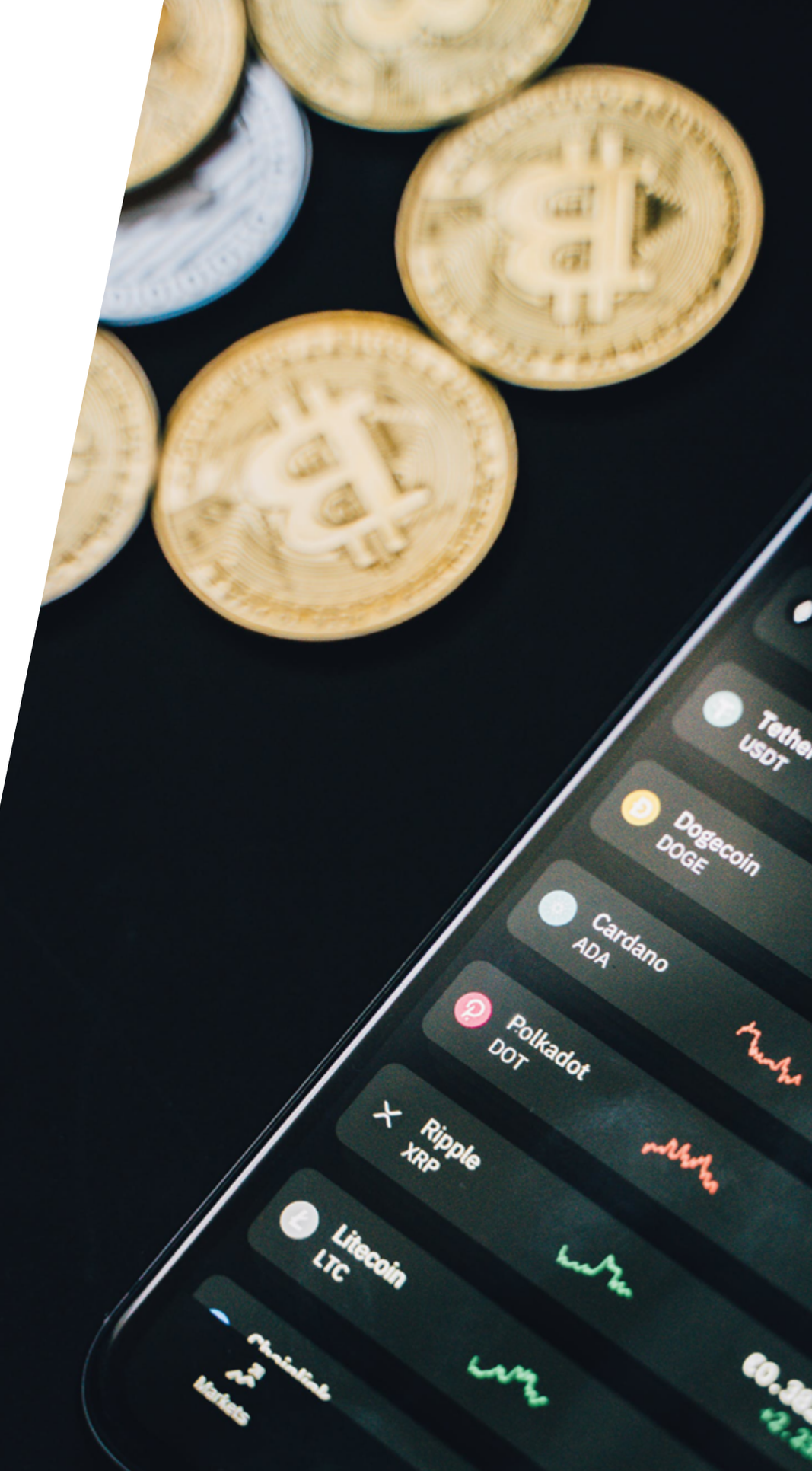
Con nuestra app **Vertiv™ XR** de realidad aumentada, puedes explorar esta solución desde cualquier lugar.

*El periodo de garantía empieza en el momento de la entrega, de acuerdo a los términos de garantía Vertiv. Garantía solo disponible mediante el registro del equipo.

BANCA Y SEGUROS.

EL SECTOR FINANCIERO, PUNTA DE LANZA DE LA INNOVACIÓN TECNOLÓGICA

¡VER AHORA!



it Digital MAGAZINE

ENCUENTROS ITDM GROUP