

El dato, la empresa y su negocio

El triángulo perfecto

Guarda esta revista en tu equipo y ábrela con Adobe Acrobat Reader para aprovechar al máximo sus opciones de interactividad



**Director**

Pablo García Reales

pablo.garcia@itdmgroup.es**Redacción y colaboradores**

Hilda Gómez, Arantxa Herranz, Reyes Alonso, Ricardo Gómez, Belén Juárez, Eva Herrero

Diseño revistas digitales**Producción audiovisual****Fotografía**

Favorit Comunicación, Alberto Varet, Ania Lewandowska

**Director General**

Juan Ramón Melara

juanramon.melara@itdmgroup.es**Director de Contenidos**

Miguel Ángel Gómez

miguelangel.gomez@itdmgroup.es**Directora IT Televisión y Lead Gen**

Arancha Asenjo

arancha.asenjo@itdmgroup.es**Directora División Web**

Bárbara Madariaga

barbara.madariaga@itdmgroup.es**Director de Operaciones**

Ángel Porras

angel.porras@itdmgroup.es

Clara del Rey, 36 1º A · 28002 Madrid · Tel. 91 601 52 92

Cinco años de éxitos



Se acaban de cumplir cinco años del nacimiento de IT Digital Media Group, y deseo aprovechar esta tribuna, el editorial de IT User, buque insignia de este grupo, para homenajear una onomástica de este relieve. Una de las funciones de mi anterior proyecto profesional, centrado en la comunicación y las relaciones públicas, radicaba en no perder de vista los movimientos de los medios de comunicación y de sus plantillas, movimientos generalmente desalentadores ya que la sangría que la crisis económica estaba causando en este maltruchado sector parecía no tener fin. Por ello, cuando ocasionalmente emergía un nuevo proyecto editorial, todos los profesionales de la comunicación afilábamos ávidos el colmillo con un doble objetivo: por un lado, enterarnos de quiénes eran los valientes que, con la que estaba cayendo, le habían echado el coraje de embarcarse en tamaña aventura; y, a continuación, a más o menos tardar, tratar de

contactarles para venderles nuestras cuitas. La sorpresa, hace justo un lustro, me sobrevino cuando llegaba a mis oídos el nacimiento de IT Digital Media Group, del ambicioso proyecto que traía consigo y, sobre todo, del equipo que estaba detrás de ello y que reunía a algunos de los mejores profesionales de este sector. El tiempo ha dado la razón a su bravura, a su ideario y a su tesón, y nadie en esta industria, mal que le pese en algunos casos, puede negar que se ha asentado como una de las opciones editoriales tecnológicas con más presente y futuro de nuestro país.

Y, es cierto, me sonreí en aquel momento pensando: "Cómo me gustaría unirme algún día a ellos". Pues bien, justo hace dos años me subí a este barco, que no deja de soñar, de crear y de innovar, como estamos demostrando más que nunca en estos momentos tan complicados. ¡Ahora a por la década! ■

Pablo García Reales



NO SOLO



TENDENCIAS



Factores que
ralentizan la
Transformación
Digital



¿Cómo aprovechar
los datos
desestructurados en
la revolución digital?

ANUNCIANTES

[HPE](#)
[VERTIV](#)
[IFS](#)
[EKON](#)
[GOFACING](#)
[STORMSHIELD](#)
[IT WHITEPAPERS](#)
[FUNDACIÓN ADELIAS](#)
[IMPRESIÓN DIGITAL](#)
[TECNOLOGÍA Y EMPRESA](#)
[IT DIGITAL SECURITY](#)
[YES MANAGEMENT](#)
[IT RESELLER](#)

ACTUALIDAD



Las claves para
emplear una estrategia
de ciberseguridad
inteligente en el
escenario digital



Europa reducirá
sus inversiones
en TIC en 2020
a causa del COVID-19



La Comisión Europea
se fija objetivos a
corto plazo para dar
forma al futuro digital



Micro Focus muestra
a las empresas cómo
ser más competitivas
en Universe 2020

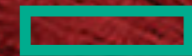


NetApp elige
Barcelona para
instaurar su Digital
Sales Hub para EMEA

MESA REDONDA IT



Tendencias en torno a
la Industria 4.0, a debate



**Hewlett Packard
Enterprise**

¿QUIERES DOMAR AL MONSTRUO DE LA TI?

Webinars de soluciones de TI para pequeñas y medianas empresas.

¡Descúbrelos todos!



IDC SECURITY CONFERENCE

Las claves para emplear una estrategia de ciberseguridad inteligente en el escenario digital

IDC Security Conference, que tuvo lugar el pasado 3 de marzo en Barcelona, puso el énfasis en que las nuevas estrategias de ciberseguridad deben adaptarse al escenario digital multicloud y a las nuevas amenazas que aprovechan la globalización y la movilidad para llegar hasta el dato.

El dato se erige como epicentro del negocio y del interés para el cibercrimen. Esta es la principal conclusión del evento IDC Security Conference, que tuvo lugar el pasado 3 de marzo en Barcelona. La firma analista habló en todo momento de un dato que se mueve libremente por el espacio multicloud y por el universo de dispositivos que las organizaciones utilizan en su día a día. El empleo de la ciberinteligencia será decisivo para evolucionar cualquier estrategia de ciberseguridad al plano proactivo necesario para contener el riesgo y orquestar eficientemente el escenario global al que nos enfrentamos. IDC considera que construir plataformas de ciberseguridad para



desplegar y/o consumir servicios de ciberseguridad inteligente gestionados se convierte en una necesidad para cualquier organización que desee integrar sus estrategias de transformación digital en un marco de seguridad y confianza.

Durante el evento también se ha mostrado al público asistente cómo la ciberinteligencia debe aportar una capa adicional a la estrategia de ciberseguridad, y qué políticas de integración y gestión de plataformas de ciberseguridad debemos adoptar para poder nutrir a las organizaciones de los servicios gestionados

de ciberseguridad adecuados para generar la confianza segura del espacio digital.

MERCADO EN CRECIMIENTO

La inversión en ciberseguridad en España supondrá, según IDC Research, 1.381 millones de euros este año, lo que va a representar un incremento del 6% con respecto a 2019 y un crecimiento interanual del 5,8% en el periodo que abarca de 2019 a 2022. “Todas las industrias van a crecer. Existe una gran pre-

PATROCINADORES

IDC Security Conference contó en Barcelona con los siguientes patrocinadores: Akamai, Anubisnetworks, BT, ContecNow, Forescout, IThinkUPC, OneTrust Privacy, Palo Alto y Softeng, así como IT User como Media Partner.

ocupación por la gestión del riesgo, la influencia de la regulación está ganando enteros, así como la seguridad y la confianza desde el diseño y por defecto, ya que la experiencia del usuario es la prioridad”, explica José Antonio Cano.

Según compartió la firma analista durante el evento, los servicios de seguridad gestionados acaparán el 27% del total, mientras que los servicios de integración representarán un 25%.



Propuesta de visibilidad de Forescout

María García Iñáñez, Regional Sales Manager de Forescout Technologies Iberia, observa tres tendencias claras en la actualidad en torno al mundo de la ciberseguridad: el aumento de dispositivos sobre todo en IoT, que se conectan a Internet y en torno a los cuales brotan numerosas vulnerabilidades; la migración a la nube y la virtualización de redes; y la convergencia de los mundos IT y OT. Para resolver estas problemáticas el fabricante proporciona una plataforma de visibilidad y control de todos los entornos y tipos de tecnologías que antes destacaba para afrontar este tipo de amenazas con más garantías.



ASÍ FUE #IDCCIBERSEGURIDAD BARCELONA 2020

Por primera vez, el software de identidad digital y confianza aparece en el ranking con un 4%, lo que desvela la tendencia al alza de la confianza digital que ya empieza a despuntar como prioridad entre los CISOs de nuestro país.

Ya para 2021 el 50% de los analistas de los centros de operaciones de seguridad (SOC) elevará su productividad gracias a la inteligencia artificial y el aprendizaje automático. Y lo más significativo radica en que el 35% de los clientes de servicios de seguridad gestionados serán atendidos por proveedores especializados en la nube, debido al incremento en las cargas de trabajo en modo cloud que se esperan para los próximos dos años.

DESAFÍOS DEL CISO

De cara a este año IDC Research España considera que tres serán los desafíos a los que ten-



drá que enfrentarse el CISO: la excelencia en la seguridad operacional, la gestión del riesgo para generar impacto comercial y una confianza digital que permita la transformación digital.

“Como consecuencia, el CISO debe ir más allá del conocimiento y experiencia técnica para involucrarse directamente en el negocio”, aclara José Antonio Cano.

Como apunta la consultora, los CISOs del futuro no lo van a tener fácil pues deberán erigirse como gestores del riesgo, manejadores de crisis, habilitadores de confianza, comunicadores y profesionales con habilidades en la parcela de negocio. Según IDC, 2022 será el punto de corte para que los CISOs se establezcan como líderes empresariales capacitados para proporcionar confianza digital a todo su entorno. ■

El tándem BT-Akamai

Akamai y BT constituyen un tándem estratégico en materia de ciberseguridad. Como explica Francisco Arnau, Regional Director de Akamai Technologies España, actualmente el escenario es muy complejo, debido al volumen y la sofisticación de los ataques a las organizaciones. Estas amenazas giran en torno a tres tendencias: por un lado, la avalancha de dispositivos, cada día más ingente entre las organizaciones, para lo que Akamai recomienda confianza cero; por otro lado, entornos complejos multi-cloud, que exigen soluciones de seguridad que sean capaces de escalar y soportar los ataques que se están produciendo actualmente; y, por último, securizar los entornos DevOps, es decir, la seguridad tiene que aparecer desde el primer momento del ciclo de vida del software. BT suma a esta visión la necesidad de que la ciberseguridad se considere no solo desde el CISO y su departamento, sino que aplique a toda la organización, de manera proactiva y por diseño. David López Rojo, Responsable de Consultoría e Integración de Seguridad de BT España, entiende que la seguridad se tiene que afrontar desde el extremo hasta la nube, alejando las amenazas lo más posible, y aplicándola tanto a entornos SaaS como IaaS a través de servicios gestionados, apoyados en tecnologías de garantías.



LA ORQUESTACIÓN DE TECNOLOGÍAS DE SEGURIDAD, SEGÚN AGBAR

Sergi Carmona, CISO de AGBAR (Aguas de Barcelona), subrayó durante el evento que los ataques ahora son más sofisticados y se dirigen a capturar el dato y a chantajear a las empresas. “La seguridad no puede parar el negocio sino ser un propulsor, y por ello siempre nos estamos adentrando en nuevas tecnologías, relacionadas con IT, OT, etc.”, apunta el directivo. “La tecnología está evolucionando de manera brutal y la seguridad debe progresar en línea con ella”. Como la seguridad tradicional se ha basado en incorporar múltiples capas tecnológicas, hoy día Agbar está trabajando en orquestar y automatizar todas las tecnologías de seguridad que ha ido adquiriendo, y poner el foco en las amenazas directas y graves.

NEGOCIO Y TECNOLOGÍA, CLAVE PARA GBFOODS

La compañía de alimentación GBfoods contaba con numerosas plataformas de seguridad y se vio obligada a reducir el número porque no era capaz de entrelazar la información entre ellas. “Nuestro reto estriba en tratar de llevar todo lo que viene de negocio hacia las plataformas actuales buscando la simplificación al máximo con plataformas

de seguridad y optimizar su día a día”, ha esgrimido en el evento **Julián Pastor, IT Risk & Security CISO de GBfoods**.

LA IMPORTANCIA DEL ZERO TRUST PARA SABIS

Sabis es la filial tecnológica de **Grupo Banco Sabadell**. Su **CISO, Eduardo González**, destaca como principal tendencia para este año el fenómeno del Zero Trust, con variables relacionadas con la protección del dato pero también con todo lo que tiene que ver con micro-servicios o la protección entre proveedores, donde se ha de aplicar la confianza cero. “También estamos observando en este entorno la aplicación de la inteligencia artificial en entornos de automatización, como soluciones tipo SOAR, aunque todavía no están lo suficientemente maduras como para confiar plenamente en ellas, pero prometen”, apunta el directivo.

EL RETO DE EDREAMS ODIGEO

eDreams **ODIGEO** es una plataforma de e-commerce con dos décadas de trayectoria que hace dos años decidió mover sus cargas de trabajo a la nube. En este contexto **Josep Mangas, Head of IT Security and QA** de la compañía, reconoce que “el proveedor tradicional de seguridad está un poco perdido en


lo que tiene que ver con la securización del cloud. El fabricante tiene el reto de traslucir qué puede aportar en el ámbito de la seguridad y que los grandes hiperescaladores como Google o Azure no estén proporcionando ya”. Entre los principales propósitos de eDreams ODIGEO se encuentra conseguir profesionales que no solo estén versados en ciberseguridad sino también en la casuística del negocio.

SECURIZACIÓN DEL IOT, SEGÚN FLUIDRA


Fluidra es una empresa especializada en desarrollar componentes para piscinas, principalmente piscinas conectadas. Esta realidad le empuja a trabajar intensamente en el área IoT, lo que le está obligando a securizar los múltiples dispositivos relacionados y cumplir con las exigentes políticas de privacidad. Como apunta **Angel Uruñuela, Global IT Security Director & CISO de Fluidra**, “el mercado y los fabricantes de seguridad nos están empujando en ocasiones a construir la casa por el tejado y a tratar de incluir tecnologías que no siempre necesitamos. Los servicios gestionados, SOCs y soluciones SIEM ofrecen muchas ventajas, pero muchas organizaciones no tenemos todavía el nivel de madurez suficiente para sacarles partido”.

A continuación, puedes ver más entrevistas de IDC Security Conference




 **“Es muy importante que la seguridad se extienda a lo largo de toda la empresa” (Akamai, BT)**



 **“Hay una evolución hacia una mayor conciencia sobre ciberseguridad” (Softeng)**



 **“La gran amenaza para una empresa es la falta de concienciación de las personas” (IThinkUPC)**



 **“Necesitamos una plataforma heterogénea que te permita una visibilidad de toda la red” (ForeScout)**

¿Te gusta este reportaje?

Compártelo en redes



Concienciación: principal apuesta de Softeng

Según Carlos Colell, CEO de Softeng, “a pesar del complejo panorama tecnológico que abre la puerta a un torrente más amplio de amenazas, también percibimos una mayor concienciación entre las organizaciones sobre esta realidad”. “Las empresas –asegura– nos llaman para decirnos que se quieren desentender de toda la problemática de la seguridad, pero nosotros les comentamos que también deben involucrarse en su protección, a pesar de que les podamos dotar de servicios y herramientas muy sofisticados”. Para poder proteger la complejidad actual de las organizaciones, Softeng establece una serie de recomendaciones: primero, trabajar en la concienciación y la confianza digital; por otro lado, eliminar todas las contraseñas, y, mientras se consigue, gestionar mejor sus identidades; en tercer lugar, ascender más rápido a la nube de manera ordenada y protegida; y, por último, apostar por estrategias de confianza cero.

La amenaza de las personas, según IThink UPC


José Luis Montero, Cybersecurity Business Manager de IThink UPC, considera que las amenazas provienen de las personas, y aunque existe más concienciación parece que “todavía tienen que suceder ciertas situaciones desagradables para que las empresas se den cuenta de la problemática de la ciberseguridad”, subraya el directivo. Otros de los

retos a los que apunta Montero pasan por una notable falta de talento, es decir, escasez de profesionales en este campo; el gran volumen de incidentes a gestionar, lo que supone que las organizaciones no sean capaces de resolver con eficacia y agilidad la atención a estas alertas; antes los incidentes solo se producían sobre entidades bancarias,

pero hoy día las amenazas también recaen sobre los sectores de infraestructuras críticas; la amenaza sobre la pyme, que no suele operar de manera proactiva; los ataques relacionados con la conectividad, la movilidad y el IoT son fatales, y más si se combinan; la amenaza sobre los servicios en cloud; y los problemas de privacidad en torno al big data.

MÁS INFORMACIÓN

 [Estos son los retos de las empresas en ciberseguridad](#)

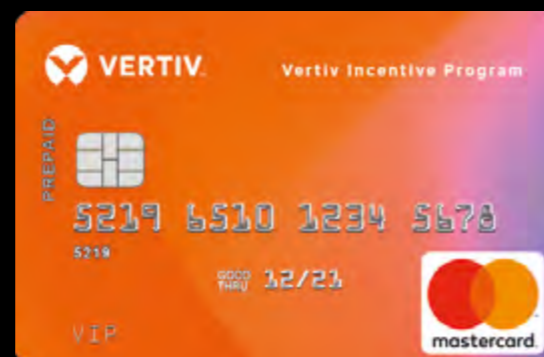
 [Diez pautas de ciberprotección para los hospitales y centros sanitarios](#)



I want it all... I want it now.

Tanto si eres director de orquesta o solista, Vertiv ofrece una amplia gama de soluciones disponibles inmediatamente para tus necesidades de infraestructura de TI. El rack Vertiv™ VR, la consola en serie Avocent® ACS 800, las PDU para rack Vertiv™ Geist™ y Vertiv™ Liebert® GXT5 Vertiv™ no son solo potentes equipos, sino que están diseñados para trabajar juntos en perfecta armonía.

Sigue disfrutando de la experiencia en [vertiv.com/vertivrocks_ES](https://www.vertiv.com/vertivrocks_ES) para ver toda la orquesta en detalle.



Recompensas que suenan muy afinadas.

Los resellers de Vertiv ahora ganan dinero con cada venta. Regístrate gratis.

Sin compra mínima. Sencillo. **VENDE. GANA. REPITE.**

Visita [vertiv.com/partner_ES](https://www.vertiv.com/partner_ES) para obtener más información.

Europa reducirá sus **inversiones TIC** en 2020 a causa del Covid-19

A medida que los países de Europa aceleran sus protocolos de contención para detener la propagación del virus sus economías comienzan a sentir los efectos, lo que está teniendo un impacto en industrias como la tecnológica. Así, los planes de gasto en TIC de los países de la Unión están siendo revisados a la baja, y los expertos prevén que en 2020 las inversiones crecerán menos de lo previsto.

Anteriormente, las previsiones de gasto en Tecnologías de la Información y las Comunicaciones dentro de la Unión europea indicaban que este año se invertiría un 2,8% más que en 2019. Ahora, a la luz de la paralización de la economía en los países de la región, a causa de las medidas contra el coronavirus, los expertos de IDC han revisado estas previsiones a la baja, y afirman que el crecimiento interanual de las inversiones en TIC sería de tan solo un 1,4%.

Esto ya se ha ido viendo en los primeros meses del año en diferentes países asiáticos, especialmente en China, y ahora Europa comenzará a sentir los efectos de las estrictas medidas de contención. Los consumidores y las empresas están dejando de invertir en TIC para minimizar los riesgos de contagio y para evitar inversiones

precipitadas, que después podrían resultar poco rentables. Como consecuencia, los expertos prevén una desaceleración importante en el gasto tecnológico a lo largo de, al menos, la primera mitad de 2020, reduciendo a la mitad las cifras previstas para este año.

Como ha señalado en su último comunicado Thomas Meyer, de IDC Europa, "los vendedores y compradores de tecnología europea se están adaptando rápidamente a la interrupción y las condiciones de mercado extremadamente rápidas. En un escenario tan fluido, todavía es temprano para evaluar completamente el panorama general del impacto europeo de las TIC". Ante esta situación,





dijo que "IDC recomienda que todos los líderes tecnológicos recalibren sus estrategias. En casos de uso como la atención al paciente, así como la experiencia y proximidad de clientes, ciudadanos, estudiantes o empleados, esperamos ver una adopción acelerada de soluciones digitales".

A su vez, Philip Carter, analista jefe de IDC Europe, comentó que "para ayudar a los proveedores y compradores de tecnología con su planificación de inversiones comerciales y tecnológicas a corto plazo, [en IDC] hemos desarrollado dos escenarios para Europa: uno probable en el que el alcance del coronavirus está ampliamente contenido en las próximas semanas, y uno pesimista, que considera un efecto dominó menos controlado a escala global".

Sus previsiones menos alarmistas son las que reducen el crecimiento del gasto al 1,4% para este año, pero todavía no se descarta que la situación pueda empeorar, algo que solo se podrá ir determinando con exactitud a medida que se desarrolle la epidemia y se vea la efectividad de las medidas de contención y

de estímulo de la economía. Para dijo Giorgio Nebuloni, de IDC Europa, "al tener una visión histórica amplia del gasto europeo en TIC en la última década, el impacto de la crisis COVID-19 aún no ha alcanzado los niveles de la crisis financiera 2007-2008. Sin embargo, representa la primera fuerte desaceleración en el crecimiento del gasto desde la crisis de la deuda europea en 2013-2014".

Así, por ahora se prevé que los mercados de hardware se verán bastante afectados por el

virus, ya que las empresas y los consumidores se sienten más inclinados a reducir su gasto en equipos. En cuanto a los servicios TI, se prevé que las empresas pospondrán las decisiones de compra para más adelante, y ralentizarán la ejecución de los proyectos que ya tienen en marcha. Mientras tanto, se prevé un impacto menos profundo en los mercados de software y telecomunicaciones, algunos segmentos se verán seriamente afectados, pero otros podrían experimentar un crecimiento inusitado, como es el caso de las soluciones de trabajo remoto, comunicaciones unificadas y colaboración, que son las herramientas que están permitiendo a muchas empresas seguir operando a pesar de las restricciones de movimiento que afectan a sus trabajadores.

Para Carla La Croce, analista de investigación sénior de IDC Europe, "los factores que pesan sobre la inversión van desde una disminución en la demanda de los clientes hasta la ruptura de las cadenas de suministro. Sin embargo, hay áreas en las que crecerá el gasto. Existen soluciones específicas y casos de uso, como videoconferencias, suministro inteligente, chatbots y plataformas de aprendizaje electrónico, entre otros, que destacan cómo la tecnología puede ayudar a las empresas y las sociedades a enfrentar (y con suerte superar) estos nuevos desafíos".

En cuanto al escenario más pesimista, los expertos de IDC quieren proporcionar una visión anticipada de hasta dónde podría afectar la cri-



Los expertos de IDC quieren proporcionar una visión anticipada de hasta dónde podría afectar la crisis actual al gasto tecnológico dentro de la UE, y su apreciación actual es que el crecimiento podría reducirse a un mero 0,2% este año

sis actual al gasto tecnológico dentro de la Comunidad Europea. Su apreciación actual es que el crecimiento podría reducirse a un mero 0,2% este año, y anticipan que el software podría ser la categoría más afectada por la crisis. Esto se debería a ciertos factores ajenos al sector de las TIC, como podría ser el cambio en el precio del petróleo, la caída del valor de las divisas de referencia o las dificultades de los gobiernos para pagar la deuda, así como a posibles mayores retrasos en diferentes cadenas de suministro y a la importante destrucción de empleo que se está dando en países como España, donde se están anunciando multitud de Expedientes de Regulación Temporal de Empleo (ERTE).

LA PANDEMIA IMPULSA EL MERCADO EMPRESARIAL DE PORTÁTILES PARA TELETRABAJO

En lo que se refiere a la pandemia global del coronavirus, no todo es negativo, y los expertos en tecnología afirman que las limitaciones sanitarias proporcionan una oportunidad para avanzar en la transformación digital, aunque

sea por obligación. Por ejemplo, en cuanto al trabajo en movilidad, ya que una de las mejores formas de que las empresas limiten los riesgos y logren mantener las operaciones en funcionamiento es que sus empleados puedan trabajar desde casa.

Para ello es vital que la empresa garantice las condiciones de rendimiento y seguridad en el trabajo remoto, por lo que muchas organizaciones están incrementando la adquisición de ordenadores portátiles de categoría empresarial. Esto está contribuyendo a mejorar las cifras en el mercado de portátiles, que según los expertos podría lograr unas cifras anuales relativamente estables. Estas perspectivas son bastante positivas, al menos si se comparan con las previsiones pesimistas de otros mercados tecnológicos, que probablemente perderán mucho valor durante la mayor parte del año.

Concretamente, se espera que las ventas de portátiles empresariales crezcan en las economías más desarrolladas y digitalizadas, como son Norteamérica, Europa y ciertas regiones de Asia. Ejemplos de ello se están viendo en



grandes empresas tecnológicas, como Microsoft, Apple, Google, Facebook, Amazon y otras muchas, que han instado a sus empleados a trabajar desde casa para evitar el contagio. En Europa se está dando una situación similar, y en países como España o Italia, donde se están tomando medidas altamente restrictivas, es muy probable que el mercado de portátiles empresariales vea un repunte, gracias al trabajo en remoto.

Según comentan los expertos, por ahora, los principales fabricantes de portátiles todavía no han reportado un incremento de los pedidos de sus clientes empresariales en sus canales europeos. Pero se prevé que esta situación cambie a la luz de los recientes acontecimientos, ya que las restricciones de movimiento de la población obligarán a muchas empresas a habilitar capacidades de teletrabajo. ■

MÁS INFORMACIÓN

 [Gartner: preparados para afrontar la crisis del coronavirus](#)

 [IDC: Impacto del coronavirus en el gasto TI](#)

La Comisión Europea se fija objetivos a corto plazo para dar forma al futuro digital

La digitalización es clave para la Comisión Europea. Aparte de hacer balance de lo conseguido en los ámbitos prioritarios en sus primeros 100 días de mandato, se ha fijado como objetivos avanzar en el futuro digital de Europa y ha avanzado que, a finales de año, estará lista la norma sobre servicios digitales, y que habrá nuevas normas de inteligencia artificial, identidad digital y ciberseguridad de las infraestructuras.

En su valoración de los primeros 100 días tras la creación de la nueva Comisión, la presidenta Ursula von der Leyen ha destacado los esfuerzos realizados en los asuntos prioritarios que van a marcar la agenda europea durante este mandato. Así, ha sostenido que “nuestros cien primeros días se han dedicado a la doble transición a la que se enfrenta Europa. Se trata de hacer de la lucha contra el cambio climático una oportunidad de crecimiento y empleo, de aprovechar las ventajas de la tecnología y de ponerla al servicio de los ciudadanos, sin olvidar el refuerzo de la influencia geopolítica de la UE”.

En lo que respecta a Transformación Digital, la Comisión va a impulsar la configuración del “futuro digital”, y esto abarca todo, “desde la ciberseguridad a la educación digital y desde las plataformas hasta la supercomputación”.

En este ámbito, se ha fijado un enfoque común para garantizar la seguridad de las redes 5G y se





va a trabajar para desarrollar una “Inteligencia Artificial de vanguardia y fiable en la UE”, con propuestas previstas para finales de este año.

También a finales de año, estará lista la norma sobre servicios digitales que, según la Comisión, aportará “responsabilidades más claras y normas modernizadas para las plataformas online”.

Dentro de los próximos pasos también se encuentran una regulación común sobre la identidad digital online para las personas y las empresas, y nuevas normas sobre la ciberseguridad de las infraestructuras y los servicios esenciales.

LA ESTRATEGIA DIGITAL EUROPEA SE BASARÁ EN LOS DATOS Y LA INTELIGENCIA ARTIFICIAL

Los datos y la Inteligencia Artificial serán dos de las principales claves del futuro digital europea, según los detalles que acaba de dar la Comisión Europea sobre las ideas y medidas “para una transformación digital que redunde en benefi-

cio de todos y refleje lo mejor de Europa”. El plan presentado contiene las que, a juicio de la Comisión, son los ejes para conseguir una sociedad europea impulsada por soluciones digitales que sitúan en el lugar preferente a las personas, abre nuevas oportunidades para las empresas y da impulso al desarrollo de una tecnología fiable. Y en él son fundamentales dos estrategias: la de datos y la de desarrollo de la inteligencia artificial.

El proyecto es ambicioso ya que, como explicó la presidenta de la Comisión Europea, Ursula von der Leyen, “abarca todo, desde la ciberseguridad a las infraestructuras críticas, de la educación digital a las capacidades, de la democracia a los medios de comunicación. Quiero que la Europa digital refleje lo mejor de Europa: que sea abierta, justa, diversa, democrática y con confianza en sí misma”.

En la base del plan digital figuran tres objetivos para los próximos cinco años: una tecnología

Primeros pasos

A lo largo de este año la Comisión presentará una norma de servicios digitales y un plan de acción europeo para la democracia, propondrá una revisión del Reglamento eIDAS y reforzará la ciberseguridad mediante la creación de una unidad informática conjunta.

También será importante seguir construyendo alianzas con socios internacionales para impulsar un modelo europeo de digitalización.

Entre los primeros pasos se ha abierto a consulta el Libro Blanco sobre la Inteligencia Artificial, para cuya elaboración se ha abierto a la consulta pública hasta el 19 de mayo de 2020. La Comisión también está recabando observaciones acerca de su estrategia de datos. En función de estos dos trabajos, tomará nuevas medidas de apoyo al desarrollo de una IA fiable y de la economía de los datos.



LIBRO BLANCO SOBRE INTELIGENCIA ARTIFICIAL

La IA se está desarrollando rápido. Cambiará nuestras vidas, pues mejorará la atención sanitaria (por ejemplo, incrementando la precisión de los diagnósticos y permitiendo una mejor prevención de las enfermedades), aumentará la eficiencia de la agricultura, contribuirá a la mitigación del cambio climático y a la correspondiente adaptación, mejorará la eficiencia de los sistemas de producción a través de un mantenimiento predictivo, aumentará la seguridad de los europeos y nos aportará otros muchos cambios que de momento solo podemos intuir.





que redunde en beneficio de las personas; una economía justa y competitiva; y una sociedad abierta, democrática y sostenible. Para llegar a ellos, es fundamental liderar los ámbitos de la Inteligencia Artificial y la economía de los datos.

Sobre el primer tema, la Comisión cree que Europa posee todo lo necesario para convertirse en un líder mundial en sistemas de Inteligencia Artificial (IA) que puedan usarse y aplicarse de forma segura, y aquí habla de que “contamos con excelentes centros de investigación,

sistemas digitales seguros y una posición sólida en robótica, así como unos sectores manufactureros y de servicios competitivos, que abarcan desde la automoción a la energía, pasando por la asistencia sanitaria o la agricultura”.

Así, en el Libro Blanco que acaba de presentar, propone un marco para una Inteligencia Artificial fiable, basado en la excelencia y la confianza, en el que, a través de la asociación con los sectores público y privado, se movilicen recursos a lo largo de toda la cadena de



valor y se creen los incentivos apropiados para acelerar la implantación de la IA, también entre las pequeñas y medianas empresas.

Para que esto se plasme en hechos, será también necesario colaborar con los Estados miembros y la comunidad investigadora, con el fin de atraer y retener el talento.

Además, será clave crear confianza en torno a la tecnología por lo que “son necesarias normas claras, que aborden los sistemas de IA con un elevado nivel de riesgo sin suponer una excesiva carga para los que entrañan unos riesgos menores”, ha asegurado la Comisión.

LOS DATOS

El objetivo de la estrategia europea de datos es asegurar que la UE se convierte en un modelo de sociedad empoderada por los datos y en un líder de esa sociedad. Con ese fin, busca crear un auténtico espacio europeo de datos, un mercado único de datos, para desbloquear los datos no utilizados, permitiendo que fluyan libremente por toda la Unión Europea y entre sectores, en beneficio de las empresas, los investigadores y las administraciones públicas. Los ciudadanos, las empresas y las organizaciones deben estar habilitados para tomar mejores decisiones con base en el conocimiento que aporten los datos no personales. Los datos deben estar disponibles para todos, ya se trate de entidades públicas o privadas, de empresas emergentes o de grandes empresas.

Para avanzar ello, la Comisión propondrá, en primer lugar, la creación del marco regulador correcto en materia de gestión de los datos, del acceso a ellos y de su reutilización entre

¿Te gusta este reportaje?

Compártelo en redes



empresas, entre administraciones y entre empresas y administraciones. En segundo lugar, pretende apoyar el desarrollo de los sistemas tecnológicos y la siguiente generación de infraestructuras que permitan aprovechar las oportunidades que ofrece la economía de los datos. "Contribuirá a las inversiones en proyectos europeos de gran impacto sobre espacios de datos europeos e infraestructuras en la nube fiables y eficientes desde el punto de vista energético", asegura.

Finalmente, pondrá en marcha medidas sectoriales específicas, para construir espacios europeos de datos, por ejemplo en relación con la fabricación industrial, el pacto verde, la movilidad o la salud. ■

MÁS INFORMACIÓN

- [Estrategia industrial para una Europa ecológica, digital y competitiva a escala mundial](#)
- [Estrategias de la UE en relación con los datos y la Inteligencia Artificial](#)
- [Configurar el futuro digital de Europa: preguntas y respuestas](#)
- [Dando forma al futuro digital de Europa, por Ursula von der Leyen](#)
- [Libro Blanco sobre Inteligencia Artificial](#)
- [Una estrategia europea para los datos](#)

UNA ESTRATEGIA EUROPEA PARA LOS DATOS

En los últimos años, las tecnologías digitales han transformado la economía y la sociedad, afectando a todos los sectores de actividad y a la vida cotidiana de todos los europeos. Los datos están en el centro de esta transformación y hay más por venir. La innovación impulsada por los datos aportará enormes beneficios a los ciudadanos, por ejemplo, mediante la mejora de la medicina personalizada, la nueva movilidad y su contribución al Pacto Verde Europeo.



A close-up photograph of a dog's face, likely a bulldog, with its mouth open and tongue out. The dog has white fur with brown patches around its eyes and on its ears. The background is a plain, light color.

NO DEJE QUE SU

SOFTWARE LE INTIMIDE

¿Su proveedor de software le presiona para actualizar de versión?
¿Le dan opción de hacerlo en la nube, on premise o SaaS?

Los clientes merecen decidir.
Dirija su negocio a su manera.

#forthechallengers | ifs.com

IFS



LA COMPAÑÍA DECIDIÓ CELEBRAR UNIVERSE 2020 DE MANERA VIRTUAL

Micro Focus muestra a las empresas cómo ser más competitivas en Universe 2020

Micro Focus Virtual Universe es el principal evento que lleva a cabo la compañía con el fin de potenciar la transformación digital de todos sus clientes. Este año, la compañía decidió que se celebrase de manera virtual de tal forma que todo el mundo pudo seguir todas las sesiones desde casa y de manera gratuita.

La crisis sanitaria que ha provocado el coronavirus a nivel mundial ha hecho que sean múltiples los eventos que se iban a celebrar en marzo que se han cancelado. Éste no ha sido el caso de Universe 2020, un evento que se iba a celebrar en La Haya (Holanda) y que Micro Focus decidió que fuera virtual.

Eso sí, el objetivo de Micro Focus Universe continuó siendo el mismo: ayudar a las empresas a seguir siendo competitivas en el mercado. Durante las tres jornadas se habló de cómo las empresas deben permanecer a la vanguardia de la tecnología mientras controlan los presupuestos, aprovechan los datos y garantizan la seguridad.

Además, los asistentes tuvieron acceso al mismo contenido de calidad proporcionado por ejecutivos de Micro Focus, expertos en productos, socios y clientes. Incluso tuvieron la oportunidad de reuniones 1: 1 y demostraciones de



productos, todo adaptado a sus necesidades comerciales y objetivos de desarrollo profesional.

INAUGURACIÓN VIRTUAL

Stephen Murdoch, CEO de Micro Focus, fue el encargado de inaugurar Micro Focus Virtual Universe 2020, destacando que en el mundo actual las reglas de los negocios, las expectativas sobre las instituciones del sector público y las definiciones de éxito están cambiando.

“El ritmo del cambio solo está haciendo una cosa: se está acelerando”, destacó el directivo. “Esa aceleración está impulsada por los avances tecnológicos y los cambios en la forma en que pensamos sobre los procesos impulsados por la digitalización, un aumento increíble en las expectativas de los clientes y el aumento creciente de modelos de negocio disruptivos y fundamentalmente nuevos de formas de hacer negocios”.

En su opinión, cada empresa, “incluidos nosotros”, está analizando “cómo encontramos un equilibrio entre la gestión de nuestro negocio hoy y la transformación de lo que creemos que debe ser en el futuro. La realidad es que tenemos que encontrar y capturar nuevas fuentes de ingresos, además de nuestra infraestructura comercial existente, los procesos comerciales y nuestras estructuras organizacionales. Necesitamos evolucionar, pero tenemos que construir sobre lo que tenemos”.



Según Murdoch, se trata de encontrar este equilibrio entre “innovar a gran velocidad, pero hacerlo con un perfil de costos y riesgos, lo cual es apropiado para la empresa”.

Murdoch añadió que la infraestructura de TI ha sufrido una cantidad de cambio “increíble” durante nuestras vidas con una explosión de innovación, pero también una gran complejidad. “La realidad es que hoy en día la mayoría de nuestros clientes viven en un entorno de modelo multigeneracional, multiproceso y de desarrollo”, dijo.

Además, Murdoch explicó por qué fallan algunas transformaciones digitales: porque no están conectada a la estrategia comercial. “En Micro Focus tratamos de adoptar un enfoque mucho más disciplinado y pragmático sobre la forma en que se brinda la Transformación digital. Y eso comienza con la evaluación”.

SESIONES VIRTUALES

Durante las tres jornadas que duró Micro Focus Virtual Universe 2020, diversos responsables de la compañía mostraron cómo la firma está en



Genefa Murphy
Chief Marketing Officer
Micro Focus



Accede a la versión on-demand de Micro Focus Virtual Universe



Stephen Murdoch, CEO de Micro Focus

“una posición única” para ayudar a las empresas a innovar, con menos riesgo, en la carrera hacia la transformación digital.

Las sesiones estuvieron divididas en cinco temáticas alineadas con las principales tendencias que están impactando a clientes y partners.

Cada una de estas temáticas incluía sesiones dirigidas por los clientes, talleres en profundidad, demostraciones de productos y conocimientos sobre las mejores prácticas.

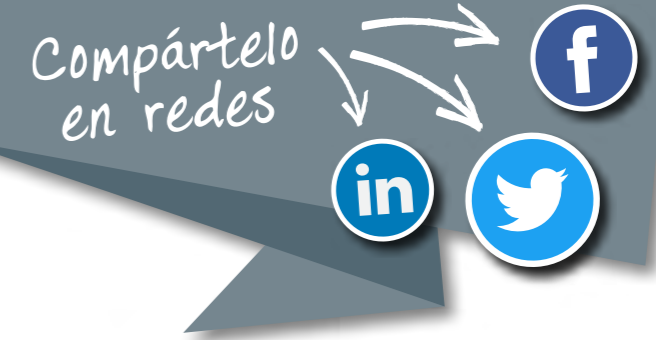
Por eso, Micro Focus Virtual Universe 2020 estuvo dirigido a todos los roles de una empresa, desde ejecutivos de negocios hasta usuarios técnicos (y todos los demás).

Algunos de los principales responsables de Micro Focus así como otros expertos de reconocido prestigio de la industria compartieron su visión sobre la transformación digital y lo que significa para las empresas.

Los asistentes también pudieron conocer de primera mano las historias de algunos clientes que están llevando a cabo con éxito esta transformación digital de la mano de las soluciones de Micro Focus.

Las sesiones de Micro Focus Virtual Universe 2020 también están bajo demanda, de tal forma que aquellos que tuvieron que elegir entre una u otra sesión, o no pudieron conectarse,

¿Te gusta este reportaje?



pueden conocer la propuesta de Micro Focus para ayudar a las empresas a innovar más rápido con menos riesgo en la carrera hacia la Transformación Digital. ■

MÁS INFORMACIÓN

-  [Consulta todas las presentaciones de Micro Focus Virtual Universe](#)
-  [Cómo impulsar la Transformación Digital de tu empresa](#)
-  [Descubre el poder de la Transformación Digital](#)



PRINCIPALES TENDENCIAS EN LA SEGURIDAD DE LAS APLICACIONES 2019

La seguridad de las aplicaciones recibe cada vez más atención. Esencialmente se trata de prevenir ataques que puedan explotar fallos en cualquier software que utilice una organización. Existen cientos de herramientas disponibles para asegurar las aplicaciones, incluso algunas especializadas en aplicaciones móviles, en aplicaciones basadas en red, incluso firewalls diseñados específicamente para las aplicaciones web.



Tú concéntrate en ser especial. Nuestro cloud ERP se encarga del resto

Con Ekon puedes estar seguro de que el valor de tu empresa fluye de forma ágil y eficiente hacia tus clientes mientras dedicas tu tiempo a trabajar en lo que hace especial a tu negocio.



Primer Cloud ERP desarrollado en España



Más de 4.000 empresas confían en nosotros



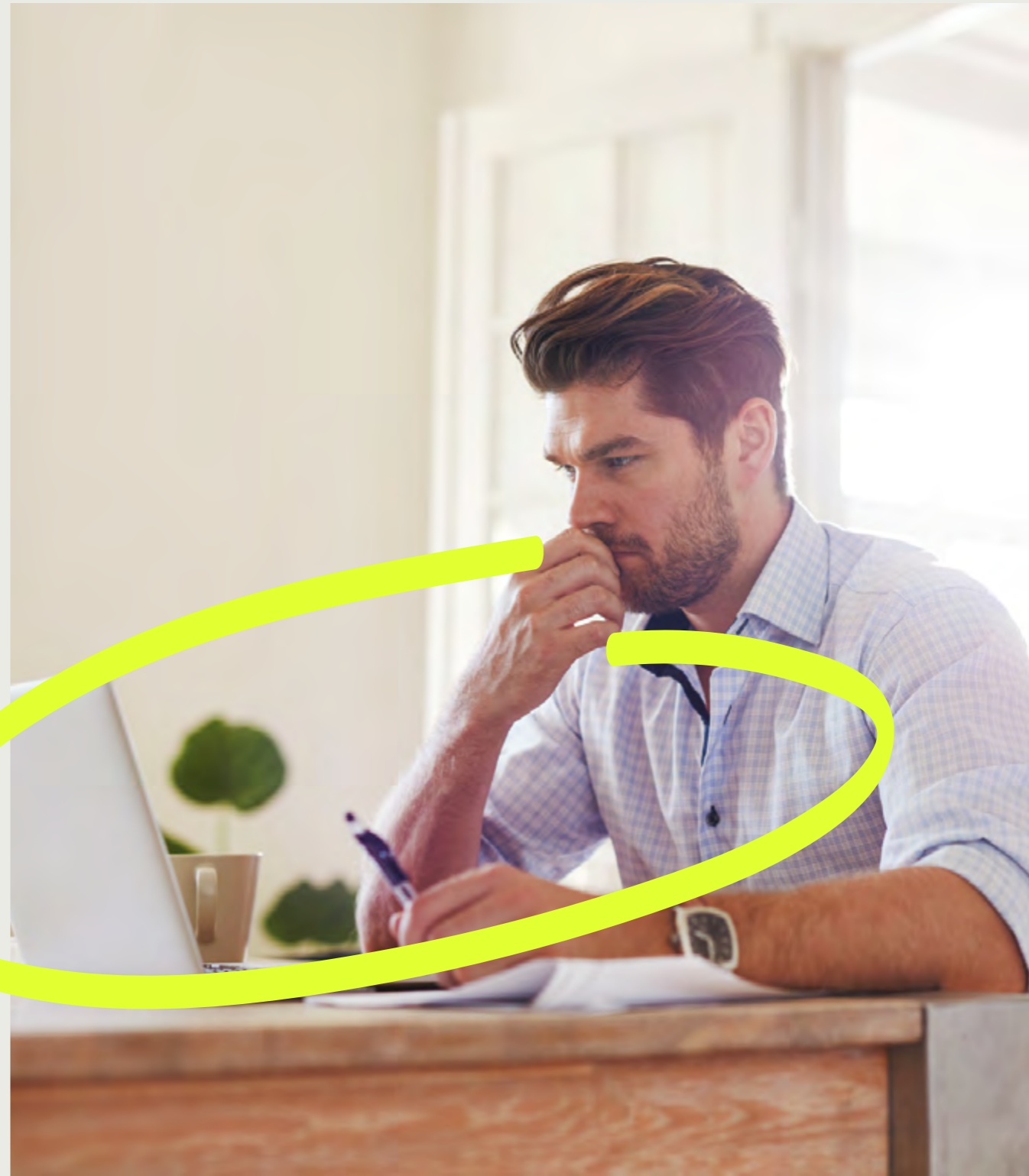
50 años de experiencia tecnológica

ekon

Software para la nueva generación de negocios



ekon.es



NetApp elige Barcelona para ubicar su Digital Sales Hub para EMEA

NetApp acaba de abrir un nuevo Digital Sales Hub en Barcelona desde el que se dará soporte a la región EMEA. Ésta “es una gran oportunidad para NetApp España que se consolida como foco de innovación y talento”, destaca la firma. **Bárbara Madariaga**. Barcelona

Barcelona ha sido la ciudad elegida por NetApp para crear su Digital Sales Hub (DSH) con el que dará soporte a todos sus equipos comerciales en la región EMEA. Esta decisión es una muestra más de “los 28 años de innovación” de NetApp, tal y como destacó Ignacio Villalgordo, director general de NetApp España, quien explicó cuáles han sido los pilares que ha llevado a la firma a “liderar el mundo de la cloud híbrida” y que se resumen en su estrategia Data Fabric y en la confianza de clientes de la talla de Dreamworks, BBVA o Ducati.

Este nuevo proyecto nace con el principal objetivo de gestionar de forma óptima las oportunidades de negocio de los equipos de venta digital, especialmente ahora que NetApp cuenta con una “gran oferta de soluciones cloud y sólidos acuerdos con partners hiperescalares como Amazon Web Services, Google Cloud y Microsoft Azure, alianzas estratégicas que impulsan la innovación en la nube”.



De izquierda a derecha Michael Donaldson, CTO y CIO del Ayuntamiento de Barcelona; Jordi Puigneró, consejero de Políticas Digitales y Administración Pública del Gobierno de Cataluña; Ignacio Villalgordo, director general de NetApp España; y Lori Harmon, vicepresidenta mundial Virtual Sales de NetApp.



Otro objetivo de NetApp con su nuevo DSH, que estará situado en el corazón de Barcelona, es que éste sea “un referente” para la región al reunir a profesionales de diferentes países que ofrecerán “un trato personalizado a nuevos clientes y asegurarán los máximos niveles de excelencia y satisfacción”. Los recursos del nuevo Hub también podrán destinarse al seguimiento de campañas de marketing o ventas, la detección de potenciales clientes y oportunidades en cualquier segmento de mercado, colaborando con todo el ecosistema de partners de NetApp. “Queremos reunir al mejor talento para dar respuesta a las necesidades de las organizaciones que se encuentran bajo una gran

presión para modernizar sus infraestructuras y migrar a la nube”. Barcelona es “la mejor ciudad para instalar este Hub”, afirmó Lori Harmon, vicepresidenta mundial Virtual Sales de NetApp. “La combinación de nuestra apuesta por el modelo de negocio digital, nuestras soluciones en la nube y la emoción de vivir en Barcelona, nos permitirá experimentar una rápida evolución y crecimiento de nuestro negocio en la región”.

APOYO INSTITUCIONAL

Jordi Puigneró, consejero de Políticas Digitales y Administración Pública del Gobierno de Cataluña, aprovechó la ocasión para agradecer a NetApp su apuesta por Barcelona. “Trabaja-

mos para tener un ecosistema de talento” que permita que Cataluña sea “uno de los Hub digitales más importantes del mundo”.

Por su parte, Michael Donaldson, CTO y CIO del Ayuntamiento de Barcelona, resaltó los puntos fuertes de la Ciudad Condal para convertirse en un referente. “El ecosistema que hay en Barcelona es fuerte y se sabe reponer a acontecimientos como la cancelación del Mobile World Congress”. Donaldson, además, destacó que Barcelona es “una ciudad donde la diversidad” es la tónica dominante, lo que permite “que las empresas crezcan. Para nosotros es importante atraer y retener el talento” de tal forma que se impulse “la transformación digital para lograr ser más competitiva”.



Este nuevo proyecto nace con el principal objetivo de gestionar de forma óptima las oportunidades de negocio de los equipos de venta digital

20 AÑOS EN ESPAÑA

Esta inauguración coincide con la celebración de los 20 años de NetApp en España. La firma estadounidense abrió su primera oficina en España en Madrid en el año 2000, dentro de su estrategia de consolidarse en aquellos países europeos que tuviesen un tejido empresarial sólido y necesitase la tecnología de almacenamiento para gestionar sus datos de forma eficiente y rentable. Desde entonces, ha ampliado presencia con distintas oficinas repartidas en España y, a medida que se desarrollaba, su equipo cre-



cía para, apoyándose en una red de alianzas y socios de canal, dar soporte a los clientes.

Durante estos 20 años, dice la compañía que ha sido testigo de la evolución y transformación de las estrategias tecnológicas en las organizaciones, convirtiéndose además en una pieza fundamental para ayudarles en sus objetivos de negocio en un momento en el que el dato "es la piedra angular de cualquier organización española para conseguir una mayor ventaja competitiva, ya que es el nuevo petróleo del siglo XXI", asegura.


Para Ignacio Villalgordo, "no solo nos hemos enfocado en mantener el ritmo que marca el panorama actual del sector tecnológico, sino que, además, hemos dado un paso más allá creando y brindando soluciones para sacar la mayor rentabilidad a la gestión de los datos con nuestra estrategia Data Fabric".

El directivo califica estas dos décadas como "excepcionales" y dice que la empresa espera "otros 20 años con la misma ilusión y entusiasmo contando con el apoyo incondicional de nuestros empleados, clientes y partners". ■

MÁS INFORMACIÓN

 [20 años de NetApp en España](#)

 [Cuál es la oferta de NetApp](#)

 [Entrevista a Ignacio Villalgordo, director general e NetApp España](#)



IT TRENDS 2020, EL AÑO DE LA CONSOLIDACIÓN DIGITAL

2020 se presenta como el año de consolidación para muchas de las estrategias de digitalización puestas en marcha por las organizaciones. Esta nueva edición del Informe IT Trends muestra la realidad digital de la empresa y sus planes de inversión y despliegue tecnológico en 2020. Según esta encuesta, seguridad y cloud serán las principales áreas de inversión en TI durante 2020. La primera es una preocupación que las empresas manifiestan a todos los ámbitos, y que justifica las previsiones de continuo crecimiento para el mercado de la seguridad en los próximos años.



goTotal+

Unificando el teletrabajo:
tus herramientas Cloud + goFacing



 goFacing

 Únete a goTotal+

Factores que ralentizan la Transformación Digital

Las organizaciones están decididas a completar el proceso de Transformación Digital, pero hay diferentes factores que les están obligando a ralentizar sus expectativas. Entre ellos está la falta de recursos y de habilidades digitales entre los trabajadores, pero también se enfrentan a la resistencia de ciertos socios y a una cultura empresarial anticuada, que dificulta el cambio.

Estas son las principales conclusiones de una investigación recientemente publicada por Cloud Industry Forum (CIF) y el grupo BT, en la que identifican diferentes factores que están ralentizando el avance de la Transformación Digital en las organizaciones. Este estudio se basa en una encuesta realizada a 40 responsables de la toma de decisiones de TI y de decisiones empresariales dentro de empresas de Reino Unido con más de 1.000 trabajadores.

Casi todas estas organizaciones tienen planes de Transformación Digital basados en la nube, e identificó una serie de obstáculos clave para lograr sus objetivos. La investigación muestra que el 98% de las organizaciones tiene una estrategia moderadamente clara, aunque

un gran porcentaje de ellas está enfrentándose a varias barreras. La principal es la falta de recursos humanos, como ha señalado el 41% de los entrevistados, y a continuación está la falta de habilidades internas (40%) y el presupuesto limitado (38%). Finalmente, el 25% de los entrevistados afirma que no creen tener el apoyo que necesitan de sus socios. Todo ello está impidiendo que sus estrategias de DX se desarrollen a la velocidad deseada.

Por otra parte, este estudio señala que las organizaciones están optando por una arquitectura de TI en la que se combinan sus propios centros de datos (37%) con espacio privado en instalaciones de terceros (28%) y con la nube (33,5%), que se ha convertido en

una tendencia al alza. La media indica que el 35% de las cargas de trabajo organizativas están ubicadas en la nube pública, pero un notable 60% de las cargas de trabajo totales se basan en la nube, mientras que un 38% todavía se almacenan en las propias instalaciones.

Según esta investigación, un 33% de las empresas tienen una estrategia de Transformación Digital completamente desarrollada, y otro 44% se encuentra en camino de hacerlo. Se espera que en los próximos dos años se complete este proceso, pero se trata solo de implantar la estrategia de DX, y no implica que se complete del todo. En este camino destaca el avance de los proyectos de Inteligencia Artificial, que son la principal prioridad para el 58% las empresas. Las siguientes prioridades de la lista son digitalizar la administración de la infraestructura (53%), mejorar las redes (47%) y llevar a cabo la migración a la nube (41%).

En opinión de David Simpkins, gerente general de servicios gestionados y de nube pública de BT, “la Transformación Digital es ahora común, pero está claro que muchas empresas se enfrentan a desafíos importantes para encontrar las habilidades especializadas y los recursos adecuados para crear y administrar la infraestructura híbrida adecuada para su negocio digital”. Explicó que, “si bien la nube pública es atractiva y de rápido crecimiento, la nube priva-



¿Te avisamos del próximo IT User?

da sigue siendo la opción correcta para muchas organizaciones que tienen requisitos de rendimiento de aplicaciones rigurosos, aplicaciones heredadas que no son adecuadas para la nube pública o que operan en un entorno altamente regulado”.

Teniendo esto en cuenta, señaló que “la gestión de la nube híbrida puede ser compleja, pero con una explosión en el tráfico de datos, el aumento de las expectativas de los clientes, la aparición de nuevos competidores y la intensificación de las presiones de costos, las empresas no pueden correr el riesgo de retrasos en su transformación empresarial”.

Por su parte, Alex Hilton, CEO de CIF, dijo de la Transformación Digital que “las empresas son plenamente conscientes de su importancia, y cada vez más lo ven como parte integral del buen funcionamiento del negocio. El siguiente paso crucial para los proveedores de la nube es tomar nota de lo que buscan las organizaciones en términos de experiencia y soporte en la nube, y garantizar que se cumplan estas demandas”.

LAS ORGANIZACIONES PRIORIZAN LA MODERNIZACIÓN DE SUS TECNOLOGÍAS

En una época de rápidos cambios como es la era digital las tecnologías anticuadas restan agilidad y competitividad a las organizaciones, y sus responsables no pueden permitírselo. Por ello, como muestran los últimos estudios

sobre la tecnología en las empresas, los líderes de TI están dando prioridad a la modernización de sus sistemas y aplicaciones. Y uno de los aspectos más importantes que destacan los expertos es que las organizaciones están apoyándose en SaaS para proporcionar capacidades informáticas a los trabajadores, lo que les permite disponer de tecnologías de nueva



Clica en la imagen para ver la imagen más grande

generación mientras llevan a cabo su propia modernización de TI.

Según una investigación realizada en el Reino Unido, el 40% de los profesionales de TI del país reconoce que este año llevará a cabo la modernización de sus aplicaciones. Mientras tanto, el 28% están llevando a cabo proyectos de desarrollo de aplicaciones web de nueva generación, y un notable 58% están embarcados en proyectos de gestión de API. Han seguido este camino para romper la peligrosa dinámica que incluso durante el año pasado constató Gartner, según la cual el 90% de las aplicaciones en uso eran antiguas y no estaban recibiendo la inversión necesaria para ser modernizadas.

En un contexto en el que tres cuartas partes de los responsables de TI reconocen que su organización se encuentra en la etapa inicial o intermedia de la Transformación Digital, seguir utilizando tecnologías anticuadas supone un freno y un riesgo excesivos. Por ello, este año

¿Te gusta este reportaje?

Compártelo en redes



el 32% de los líderes de TI ha incluido la modernización de aplicaciones como parte de su estrategia de Transformación Digital. Otra de las estrategias clave que entran en las prioridades de las organizaciones es la automatización de procesos comerciales, que está siendo llevada a cabo por más de la mitad de las empresas.

Otra de las tendencias que destacan los expertos responsables de este estudio es que en 2020 casi la mitad de los profesionales de TI tienen intención de aumentar el uso de las infraestructuras en la nube para apoyar sus iniciativas de Transformación Digital. Como resultado, un 38% de los responsables van a incrementar el presupuesto destinado a la nube, con el fin de poder ubicar más aplicaciones en

las plataformas de infraestructura cloud. Así, las máquinas virtuales en la nube sustituirán a los servidores físicos y a las máquinas virtuales ubicadas en servidores físicos.

Todas estas tendencias muestran que los líderes de TI lo están enfocándose acertadamente en la modernización, tratando de dejar atrás las tecnologías obsoletas para seguir siendo competitivos. Esto dará más fuerza al mercado de servicios en la nube, pero también impulsará la implementación interna de tecnologías de nueva generación, necesarias para dar vida a las aplicaciones empresariales más críticas, con nuevas capacidades como la Inteligencia Artificial. ■

MÁS INFORMACIÓN

 [Cloud Industry Forum](#)

 [El rol cambiante del departamento TI](#)



EL ROL CAMBIANTE DEL DEPARTAMENTO TI

Han pasado muchos años desde que las organizaciones comenzaron a adoptar la transformación digital, y esta apertura a la evolución y a las nuevas formas de trabajo es ahora fundamental para mantener la ventaja competitiva en cualquier industria. Estos viajes digitales pueden haber comenzado hace mucho tiempo, pero están lejos de haber terminado: la rápida evolución de los retos empresariales significa que la innovación y la agilidad constantes son el camino a seguir.





STORMSHIELD

La opción europea en ciberseguridad

El partner de confianza
para

securizar sus

**infraestructuras
operacionales
y sensibles**

www.stormshield.com



¿Cómo aprovechar **datos** **desestructurados** en la **revolución digital**?

Resulta imposible entender el ecosistema digital de las empresas sin tener en cuenta las nuevas fuentes de datos no estructurados, como las que contienen los correos electrónicos, las imágenes o los documentos digitales. Pero la necesidad de capturar la información que éstas encierran está planteando serios problemas para la gestión de los datos. Y ante el creciente volumen de información digital que les llega de fuentes cada vez más diversas, las organizaciones están buscando soluciones que hagan más fácil y productivo el trabajo.

Las fuentes de datos tradicionales contienen información, pero muchas veces la más importante o valiosa se encuentra en los archivos considerados como no estructurados. Por ejemplo, las fotografías, los emails, los documentos de texto y los ficheros de audio o vídeo. Obtener información de estas fuentes es complicado, ya que se requieren tecnologías





capaces de determinar la naturaleza específica de estos archivos y de extraer la información que contienen. Además, es vital que los datos resultantes sean analizados en cierta forma para poder contextualizarlos y categorizarlos, de forma que puedan añadirse a los sistemas.

Esto se ha convertido en una especialidad en sí misma, pero las organizaciones no cuentan con personal capacitado para gestionar este tipo de información, lo que les impide extraer un valor que de otra forma quizá no podrían obtener. Según la versión de 2020 del estudio Rise of the Data Economy, publicado recientemente por la empresa Igneus, el 70% de las organizaciones considera extremadamente difícil gestionar los datos no estructurados.

Esto genera una importante preocupación a los líderes de datos, ya que estas fuentes se están convirtiendo en vitales para las organizaciones, y no poder identificarlas, gestionarlas y extraer la información valiosa que contienen supone un problema creciente. Las empresas que más están avanzando en la digitalización, especialmente aquellas que ya han reorientado sus modelos de negocio para aprovechar el valor del dato, comienzan a percibir este problema, y a enfrentarse a los retos que genera el trabajo con datos no estructurados.

DESAFÍOS EN LA GESTIÓN DE DATOS NO ESTRUCTURADOS

Una de las dificultades más importantes que enfrentan las organizaciones digitalizadas es

que las principales fuentes de datos no estructurados son máquinas que funcionan constantemente. Debido a ello generan datos “en bruto” de forma permanente, a una escala de petabytes, tan rápido que resultan difíciles de asimilar por las infraestructuras tecnológicas que tienen las organizaciones.

Otro de los problemas es que estos archivos no se pueden incluir en ningún sistema tradicional de organización o clasificación que permita contextualizar los datos que contienen, por lo que no se pueden introducir en bases de datos tal cual. Primero se debe extraer la información que contienen y, después, categorizarla para que pueda entrar a formar parte del sistema de datos. Además, según el estudio, estos archivos se encuentran casi siempre en sistemas NAS locales, lo que dificulta aún más su gestión.

A estos dos retos se suma la creciente complejidad de las infraestructuras empresariales, que actualmente incluyen multitud de fuentes de datos internas y externas, donde ya no hay

La encuesta de Igneus indica que el 60% de las organizaciones se ven obligadas a administrar más de 1.000 millones de archivos de forma constante



una única nube, sino varias. Esto hace que sea más difícil mover los archivos entre las distintas plataformas locales y cloud, lo que reduce, igualmente, la visibilidad de los millones de archivos que manejan las organizaciones, y más aún la gestión de los datos no estructurados que estos contienen.

Los estudios más optimistas sobre el asunto indican que aproximadamente un tercio de los datos que tienen las organizaciones carece de valor, pero se ven incapaces de eliminarlos. Esto se debe, según los expertos, a una combinación de la dificultad para mover estos datos y la falta de visibilidad de los mismos. Una invisibilidad que complica el proceso de archivado y respaldo de la información, lo cual redundará en un grave problema, especialmente en lo que se refiere al creciente volumen de datos en la nube, y más particularmente en el porcentaje proveniente de archivos desestructurados.

CRECIMIENTO EXPONENCIAL DE LOS DATOS

La encuesta de Igneus indica que el 60% de las organizaciones se ven obligadas a administrar más de 1.000 millones de archivos de forma constante. De ellas, el 10% que más archivos gestiona supera la barrera de los 150.000 millones, con una capacidad total de, al menos, 83 Petabytes de datos. Y estas cifras no paran de crecer, haciendo que la ingente cantidad de información a administrar por las organizaciones se vuelva inmanejable con las técnicas tradicionales.

Más capacidad de movimiento para los datos

La segunda etapa que enfrentan las organizaciones para la gestión de datos no estructurados, tras aumentar la visibilidad, es mejorar la capacidad que tienen para mover la información entre las diferentes plataformas en las que se alojan. Como señalan los responsables de este estudio, las soluciones tradicionales fallan de nuevo cuando deben trabajar con grandes cantidades de datos, especialmente al pasar la barrera de los mil millones de archivos, que fácilmente alcanza la escala de petabytes.

Como en el caso anterior, de cara al movimiento de los datos se recomienda a las organizaciones que escojan una solución de gestión de datos rápida, eficiente y rentable, en la que deben considerar tres aspectos fundamentales:

* GRANDES VOLÚMENES DE ARCHIVOS: el reto más impor-

tante para las soluciones de gestión de datos no estructurados es que puedan ocuparse de la gran avalancha de información que reciben las organizaciones en la era digital. En este sentido, lo principal es que se garantice la capacidad de mover grandes volúmenes de archivos, a una escala de Petabytes o superior, entre las diferentes plataformas de la organización. Y para ello es vital que sea capaz de aprovechar al máximo el ancho de banda de la red, así como contar con capacidad para escalar horizontalmente con eficiencia para manejar las cargas de transferencia más elevadas.

* ADMINISTRACIÓN EFICIENTE DE LA RED: aprovechar las capacidades de la red no consiste sólo en poder hacer grandes transferencias de datos entre las diversas fuentes disponibles, sino en hacerlo de la forma más eficiente

posible. Para ello, es vital que la solución de gestión de datos sea capaz de monitorizar la red y de modificar su desempeño en tiempo real, para que la experiencia del usuario no se vea afectada.

* EXPERIENCIA EN LA NUBE: las organizaciones están moviendo buena parte de sus datos a la nube a la vez que incrementan su capacidad en la TI local, ya que el coste en ambos entornos está reduciéndose. Pero esto no implica que sea fácil mover la información y los archivos entre estos entornos, especialmente cuando se trata de datos no estructurados. Por ello, es preferible escoger una solución que cuente con ciertas capacidades de inteligencia en lo que se refiere al trabajo en la nube, lo que permitirá reducir los costes de las transferencias de datos desde y hacia la TI local.



Los ejemplos de crecimiento explosivo son claros en industrias como la de la salud, donde se están empleando sistemas de secuenciación de ADN e imágenes de diagnóstico digitales, generando archivos no estructurados que contienen enormes cantidades de datos. Para comprenderlos y utilizarlos en los tratamientos médicos y en la lucha contra enfermedades se está recurriendo cada vez más a sistemas como la inteligencia artificial, la visión por ordenador y el aprendizaje automático, que parecen ser las únicas tecnologías capaces de manejar tal cantidad de información.

Otra industria en la que se prevé un crecimiento explosivo de los datos no estructurados, y en la que se alcanzará la escala de Exabytes con sor-

prendente facilidad, será la de los vehículos autónomos. De hecho, lo que se considera como su versión preliminar, la industria de vehículos conectados, ya está experimentando un aumento enorme de los datos generados por los coches, tanto de imágenes como de posicionamiento y servicios asociados a la conducción.

MEJORANDO LA VISIBILIDAD DE LOS DATOS

Todos estos desafíos ponen en jaque a las organizaciones a la hora de administrar las nuevas fuentes de datos no estructurados, ya que la falta de visibilidad les impide trabajar con la información en sus diferentes ubicaciones de forma precisa y fiable. Y los líderes de datos echan en falta acuerdos de nivel de servicio adaptados a sus necesidades actuales y futuras en cuanto a los datos, que actualmente quedan desprotegidos.

Esto está suponiendo un freno para las estrategias de digitalización de muchas organizaciones, que no logran aprovechar bien las posibilidades de la nube para reducir el volumen de su TI local. Por ello, las organizaciones están buscando la forma de recuperar el control de la situación, para lo que los expertos recomiendan trabajar en dos principales líneas de acción.

El primer frente de batalla para optimizar el trabajo con datos no estructurados es mejorar la visibilidad de esta información, ya que los responsables de TI necesitan contar con datos fiables para la toma de decisiones y para la propia administración de los archivos. Esto les permite determinar con más precisión el lugar adecuado para todos los datos, ya sea en un nivel primario, secundario o en el almacenamiento en frío, y también saber cuáles pueden ser eliminados sin riesgos.

El primer frente de batalla para optimizar el trabajo con datos no estructurados es mejorar la visibilidad de esta información, ya que los responsables de TI necesitan contar con datos fiables para la toma de decisiones y para la propia administración de los archivos



Esto es algo imposible de lograr con las herramientas tradicionales, que tardan demasiado tiempo en proporcionar información fiable sobre el estado del almacenamiento. Además, no son capaces de determinar la naturaleza de los datos con la precisión que se requiere para el trabajo con archivos desestructurados. Por ello, según afirman los analistas de Igneus en su informe, las organizaciones deben optar por soluciones que les proporcionen una buena visibilidad teniendo en cuenta estos tres factores fundamentales:

❖ **Escala:** el problema de muchas herramientas de administración de datos convencionales es su incapacidad para funcionar al rendimiento adecuado cuando la escala se incrementa hasta la barrera de los mil millones de archivos. Porque la cantidad de archivos no estructurados que manejan las organizaciones va a superar esta cifra, si no lo hace ya, y es necesario acelerar al máximo el análisis de esta información. Por ello, es necesario contar con un sistema capaz

de realizar el trabajo en horas o días, en vez de en semanas o meses, como ocurre actualmente.




❖ **Alcance:** otro de los terrenos donde las herramientas de gestión de datos convencionales fallan es en su capacidad para trabajar en entornos altamente diversificados. Y este es precisamente el contexto en el que se mueven las empresas en la era digital, ya que sus datos provienen de múltiples fuentes y se encuentran repartidos entre diferentes sistemas de archivos locales, en la nube, en el borde y en las aplicaciones finales. Por este motivo, es vital que las organizaciones escojan una herramienta de gestión capaz de moverse ágilmente en todos estos entornos, proporcionando una buena visibilidad independientemente de la ubicación.

❖ **As-a-Service:** las organizaciones ya tienen suficientes cargas tecnológicas que aumentan la complejidad y el gasto de capital, por lo que añadir a la lista un sistema propio para la gestión de archivos puede generar demasiada complejidad a la TI local. Por ello, y especialmente para



las empresas de menor volumen y recursos, los expertos recomiendan buscar soluciones entregadas como servicio que se puedan integrar en el ecosistema de TI existente aportando la visibilidad que se necesita. ■

MÁS INFORMACIÓN

-  [El auge de la economía de datos](#)
-  [Gestión de datos para la empresa inteligente](#)
-  [Convierte los datos en oportunidades de negocio con una plataforma de datos inteligente](#)

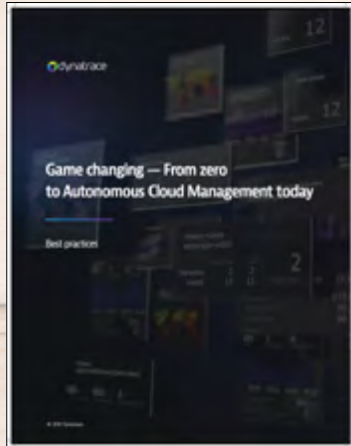


EL AUGE DE LA ECONOMÍA DE DATOS

Según The Economist, los datos han superado al petróleo como la economía más valiosa del mundo. Unos datos que van a cambiar nuestro mundo para siempre. Podemos, de hecho, decir que estamos viviendo el surgimiento de la “economía de datos”. Pero no son iguales los datos generados por las personas que los creados por instrumentos de investigación, simulación de diseño, sensores e imágenes y otros tipos de máquinas que acumulan petabytes y exabytes rutinariamente por las empresas de economía de datos.



La documentación TIC, a un solo clic



Cambio de juego: cómo lograr una gestión autónoma de la nube

En el mundo digital actual casi todas las empresas son compañías de software, y la mayoría de las organizaciones buscan formas innovadoras de crear nuevos productos o identificar modernas maneras de operar para ser más competitivos. Dynatrace es una firma que vio el cambio digital desde el principio y pasó de entregar software a través de un modelo tradicional on premise, al innovador modelo híbrido-SaaS.

Caso de uso:

Codere ahorra un 27% de su gasto en Azure con Cloud Economics de Crayon

La compañía energética CenterPoint Energy está aprovechando la innovación, incluyendo cosas como contadores y redes inteligentes, para mejorar la calidad de sus servicios de energía. Sin embargo, los sistemas IoT y las transacciones complejas con los clientes generan cantidades enormes de datos, parte central de su estrategia, operaciones e, incluso, identidad.



Transformación a la seguridad Zero Trust

La noción de un perímetro de red, en el que todo el que está fuera de la zona de control de la empresa es malicioso y todo el que se encuentra dentro es honesto y bienintencionado, no es algo en lo que se pueda confiar en el panorama empresarial actual. La amplia adopción de aplicaciones SaaS, la migración a arquitecturas basadas en la nube, un número creciente de usuarios remotos y un flujo cada vez mayor de dispositivos BYOD han convertido la seguridad perimetral en irrelevante.

Cómo el análisis de datos incrementa el valor del negocio y aporta ventajas competitivas

Todas las empresas se encuentran inmersas en procesos de transformación digital, y la red es un elemento fundamental para el éxito. Las organizaciones modernas exigen agilidad y conectividad ininterrumpida, y la red es hoy día el facilitador de cualquier iniciativa digital donde el análisis de datos se ha convertido en un componente absolutamente crítico. Este documento expone cómo las organizaciones que incorporan análisis de datos en su actividad consiguen mejores resultados; con ejemplos prácticos de los sectores de educación, retail, entretenimiento y sanidad.



En un momento en que el ánimo puede estar un poco decaído por la situación general que estamos viviendo, desde la Fundación Adalias quieren enviarnos un mensaje positivo, un mensaje de esperanza y optimismo.

Siempre sale el sol

En casi trece años hemos ayudado a más de 15.000 menores. Entre ellos:

- ❖ Bebés huérfanos, cuidarles y protegerles mientras encuentran una familia.

- ❖ Miles de menores enfermos y bebés neonatos, que se han beneficiado de: instrumental sanitario, incubadoras, respiradores... que Fundación Adalias ha proporcionado al hospital Hassani

- ❖ Cientos de menores de familias pobres en colegios de Madrid, que se han beneficiado con becas, ordenadores, material escolar...

- ❖ Hemos proporcionado los medios y promocionado la educación para que muchos menores que sus familias no les pueden proporcionar una educación puedan acceder a ella. Buscando siempre normalizar la igualdad entre los niños y niñas en el colegio Wikxan. Además de ayudar a muchas mujeres adultas a que aprendan a leer y escribir.

- ❖ Cientos de menores procedentes de familias pobres o de pobreza extrema a los que Fundación Adalias ha ayudado salvándoles la vida.



¿Quieres colaborar?

Puedes hacer tus aportaciones en la cuenta ES27 2100 6274 3202 0003 5801 o, si lo prefieres, tienes otras opciones en este enlace



❖ Menores que presentaban diferentes patologías, entre las que destacaban el notable número de cardiopatías congénitas. Han sido operados en Hospitales de Madrid y Barcelona. Hoy por hoy, el 99,9% de estos casos se encuentran en perfecto estado y tienen una vida normal porque han tenido una segunda oportunidad.

Es una gran satisfacción saber que estos peques están bien, y disfrutando de esa segunda oportunidad. Alguna vez sus madres nos envían fotos de cómo crecen, de cómo pueden celebrar un nuevo cumpleaños, de cómo van al colegio. Esa es nuestra mayor recompensa ¡Verles vivir!

Estos niños y niñas son un ejemplo de superación y frente a las adversidades y la situación que estamos viviendo toda la humanidad. Queremos que estos testimonios sean un ejemplo de positividad, de resiliencia, de esa esperanza a la que nos tenemos que agarrar porque siempre sale el sol.

Es momento de ser solidarios, responsables, de ayudarnos los unos a los otros porque las enfermedades no entienden de edad ni de posición social. ■



MÁS INFORMACIÓN



Fundación Adelias



¿Te gusta este reportaje?

Compártelo en redes



Fundación Adelias

La Fundación Adelias nace de la mano de empresarios, ejecutivos de multinacionales y jueces que piensan, profundamente, que un mundo mejor es posible. Dedicamos tiempo, fondos, talento e ilusión para trabajar por niños y adolescentes en

dos ámbitos fundamentales: educación y salud. Movidos por un compromiso con la sociedad, con la población más vulnerable, los niños, trabajamos construyendo hospitales, casas cuna, escuelas, impulsando el progreso y el desarrollo. Mo-

vemos especialistas de un lado a otro del continente y formamos a los hombres del futuro para cambiar la realidad de las comunidades para las que trabajamos. El foco es España en materia educativa y Marruecos en el ámbito de la salud.

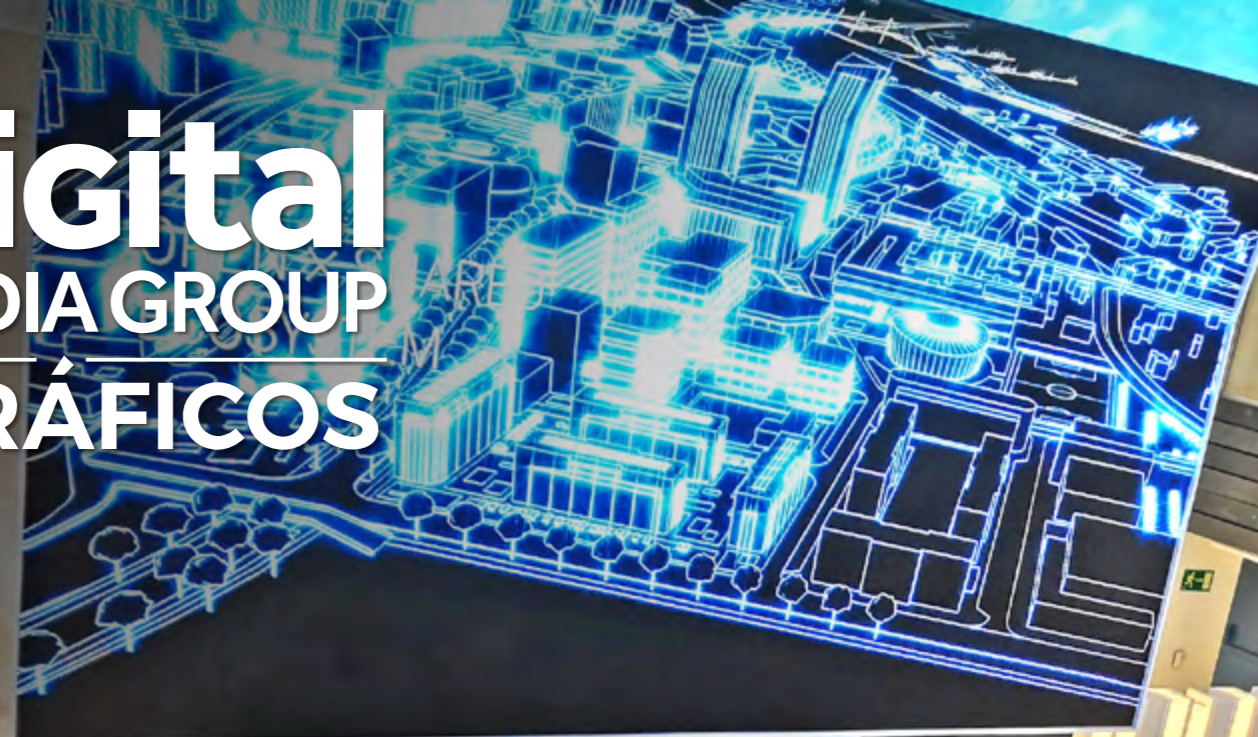
*"Si me caí,
es porque estaba
caminando.
Y caminar vale
la pena aunque
te caigas"*

Eduardo Galeano



Digital
MEDIA GROUP

MONOGRÁFICOS



**HACIA LA DIGITALIZACIÓN INTELIGENTE
DE LAS ORGANIZACIONES**

LA AGENDA DIGITAL IMPULSA EL GASTO TECNOLÓGICO

PRIORIDADES EN LA AGENDA DEL CIO



EL FUTURO DE LA SOCIEDAD Y DE LA DE ECONOMÍA ES DIGITAL. 2020 ABRE UNA NUEVA DÉCADA EN LA QUE LAS EMPRESAS E INSTITUCIONES VAN A LLEGAR A ESTADOS MÁS AVANZADOS DE MADUREZ DIGITAL, QUE TIENEN EN LA TECNOLOGÍA EL GRAN HABILITADOR. LOS CIO TOMAN LA PALABRA PARA CONDUCIR EL VIAJE DIGITAL DE SUS ORGANIZACIONES PRIORIZANDO LAS INVERSIONES EN LAS TECNOLOGÍAS QUE IMPULSAN LA ECONOMÍA DE LOS DATOS.

La evolución tecnológica experimentada en las dos últimas décadas ha dado como resultado un mundo hiperconectado, que ha sido detonante de otros cambios en la forma en la que nos comunicamos y consumimos, desde un punto de vista individual, y en la manera en la que operan, trabajan y se relacionan las empresas con sus ecosistemas. La revolución digital lo impregna todo y es imparable.

Todavía no sabemos exactamente cómo afectará el fenómeno del Coronavirus a nuestra industria, pero el último pronóstico de la firma de análisis IDC pasaba porque el gasto mundial en tecnología y comunicaciones en 2020 se elevará a 4,3 billones de dólares (3,9 billones de euros), lo que supone un crecimiento del 3,6% con respecto a 2019. De esta cantidad, 2,7 billones de dólares (2,4 si hablamos en euros) corresponderán al mercado corporativo, es decir, será lo que gasten las empresas en TI, y en servicios empresariales y de telecomunicaciones, mientras que el resto procederá del sector consumo.

Como explican sus expertos, la mayoría de las organizaciones están acelerando sus procesos de transformación digital, invirtiendo en tecnologías para evolucionar su forma de trabajar, y en construir una oferta de productos y servicios más digitales.

La última edición del Gartner IT Symposium/Xpo, de Barcelona, también dejaba hace unas semanas estimaciones positivas sobre la inversión en TI para la región de EMEA, donde retornará por fin al crecimiento en 2020 tras tres años de descensos. Las predicciones de la consultora apuntan a que se gastarán 798.246 millones de dólares (en torno a 739.500 millones de euros).

Se trata de una tendencia mundial y tiene su reflejo en nuestro país. El gasto tecnológico,

RESULTAN CRÍTICAS LAS SOLUCIONES QUE CONTRIBUYEN A IMPULSAR UNA ECONOMÍA DE LOS DATOS, POR LO QUE TIENEN MUCHO SENTIDO LAS INVERSIONES EN ALMACENAMIENTO, BIG DATA Y ANALÍTICA AVANZADA, INTERNET DE LAS COSAS, INTELIGENCIA ARTIFICIAL, COMUNICACIONES 5G A LA CABEZA, Y PLATAFORMAS QUE, CONVERTIDAS EN NÚCLEO DIGITAL, PERMITEN OPERAR MODELOS DE NEGOCIO INNOVADORES BASADOS EN EL DATO

de acuerdo con las Predicciones 2020 de IDC Research España, se elevará este año a 49.300 millones de euros, lo que representa una expectativa de crecimiento algo superior al 1% si se compara con los 48.800 millones de 2019. Un ciclo alcista que se mantendrá en los próximos años, con un ritmo de crecimiento medio agregado del 2,2% entre 2020 y 2022. En esa fecha la cifra será de 51.600 millones.

PRIORIDADES DEL CIO EN ESPAÑA

Seis de cada diez empresas españolas están desarrollando, o ya lo ha hecho, mientras que el porcentaje de las que no han iniciado su proceso de digitalización se ha reducido en 14 puntos hasta el 9%.

Es una evolución estratégica que en muchos casos viene impulsada por la alta dirección. Al respecto, el informe Perspectivas España, que elaboran KPMG y la Confederación Española de Organizaciones Empresariales (CEOE) confirma que los empresarios y ejecutivos asientan como sus prioridades la transformación

digital (55%) y, en línea con ello, les preocupa la mejora de los procesos (56%) y la necesidad de desarrollar nuevos productos y servicios (39%).

El director de tecnología o CIO, en sus siglas inglesas, es consciente de estos imperativos en su rol de orquestador de un modelo de TI flexible y escalable que permita aprovechar las oportunidades de la digitalización. Dicho de otro modo: tiene que encontrar la forma de armonizar y combinar las arquitecturas, sistemas y tecnologías que hacen posible y aceleran la evolución a modelos digitales.

En este punto, los análisis del mercado coinciden en que las tecnologías transformadoras que van a permitir llegar a un estado avanzado de madurez digital son aquellas que ayudan a aprovechar la explosión del dato, a automatizar procesos, a mejorar la experiencia del cliente, del empleado y todo el ecosistema con el que se relaciona la organización, además de acelerar el despliegue de productos y servicios digitales.

Sobra decir que son críticas las soluciones que contribuyen a impulsar una economía de los datos, por lo que tienen mucho sentido las inversiones en almacenamiento, big data y analítica avanzada, Internet de las Cosas, inteligencia artificial, comunicaciones 5G a la cabeza, y plataformas que, convertidas en núcleo digital, permiten operar modelos de negocio innovadores basados en el dato, en las que cloud puede ser muy relevante.

Según los datos de IDC Research España, el año que viene el 60% de los CIOs implementará un modelo de negocio de TI y una cultura que cambiará el enfoque de los proyectos de TI a productos orientados digitalmente. Y un porcentaje muy similar ya está priorizando las inversiones en plataformas de transformación digital.

Claramente éste es el camino, donde la estrella que guía el proceso es la inteligencia artificial, aplicada a la mejora de procesos y, cómo no, al apoyo en la toma de decisiones. Esta tecnología es ya una prioridad para cuatro de cada diez directores de tecnología. En sus previsiones, el brazo español de IDC dice también que, para 2022, el 75% de las empresas incorporarán la automatización inteligente en la tecnología y el desarrollo de procesos, apuesta que llevará a este segmento de mercado a mover 650 millones de euros en España en 2022.

De cumplirse este pronóstico, habrá crecido un 32,3% respecto a 2019, y un 35,6% en el acumulado entre 2020 y 2022, también ayudado por la adopción de esta tecnología para ofrecer una experiencia de cliente totalmente personalizada.

HACIA ORGANIZACIONES IMPULSADAS POR LOS DATOS

Precisamente la inteligencia artificial es clave para poder aprovechar la economía de los datos, definidos como el nuevo “petróleo” para

evidenciar que es el principal activo corporativo y motor de la sociedad del conocimiento.

La mitad del gasto tecnológico que realicen las empresas europeas este año estará asociado a este concepto, dado que el 80% de sus ingresos van a proceder de la venta de productos y servicios basados en este activo, según los expertos de IDC en Europa.

Por tanto, los CIO están teniendo en cuenta también en sus partidas presupuestarias las necesidades de sus compañías en capacidad de procesamiento, sistemas de al-



macenamiento que optimicen el centro de datos y el rendimiento de las aplicaciones críticas, big data y soluciones analíticas, etc.

Estas áreas tienen también un gran potencial de crecimiento. Según los expertos de ResearchAndMarkets, el mercado de centros de datos crecerá en todo el mundo a un ritmo anual del 2%, lo que impulsará el aumento de las ventas de servidores, sistemas de networking y arrays de almacenamiento híbrido y all-flash, que sustituyan a los discos tradicionales HDD y que soporten los despliegues de proyectos de big data e inteligencia artificial. Los ratios de evolución de las soluciones de la tecnología de Big Data y Analytics también son prometedores, ya que se situarán por encima del 13% hasta 2022, lo que dejará la cifra en 274.300 millones de dólares (253.070 billones de euros), según IDC. En España, la inversión en Big Data y soluciones de Analítica será de 5.960 millones de euros en ese mismo periodo.

PREPARARSE PARA 5G

En este puzzle tecnológico debe incluirse también 5G o la quinta generación de tecnologías de telefonía móvil, que será una palanca de crecimiento y un componente tecnológico esencial en los procesos de digitalización durante esta década.

El pronóstico de firmas, como Strategy Analytics, incide en que esta tecnología ten-

drá un gran impacto en la productividad, la movilidad y la rentabilidad empresarial, a través de nuevos casos de uso en sectores como turismo, movilidad, transporte y logística, seguridad ciudadana, 'smart cities' industria, telemedicina, etc. Éstos se ven favorecidos por el avance en términos de ancho de banda y latencia que trae consigo, puesto que estamos hablando de servicios inalámbricos de banda ancha a velocidades Gigabit (hasta 100 veces superiores) que reducen sustancialmente los tiempos de descarga, mientras que la latencia se acercará a cero, lo que mejora la capacidad de carga y las transferencias de datos y todo tipo de contenidos.

2019 fue un año importante para el despegue de 5G gracias al avance de las operadoras en el despliegue de las redes. También están llegando al mercado productos Wi-Fi 6, necesarios para construir redes fiables y, a lo largo de 2020, aterrizarán más dispositivos compatibles con esta tecnología. Por tanto, las empresas deben tener ya en el punto de mira las posibles aplicaciones para su negocio con objeto de extraer una notable ventaja competitiva. Y no es algo que dejar para mañana porque, aunque es complicado hablar de cifras, el World Economic Forum en su último informe estima que el impacto de 5G en la economía mundial podría llegar a superar los 13,2 billones de dólares (12,1 billones de euros) en 2035. ■



EN PRO DE LA TRANSFORMACIÓN DIGITAL

La transformación digital está en la hoja de ruta de las organizaciones que, además, aceleran el paso para mejorar la operativa y los procesos de todas sus áreas de negocio. En la economía del dato y de las empresas inteligentes, esto se traduce en inversiones en infraestructuras, plataformas, tecnologías y soluciones que les permiten responder a los desafíos actuales de agilidad, flexibilidad, productividad o escalabilidad, que definen los modelos digitales.

EL COMPROMISO DE HUAWEI POR LA ECONOMÍA Y LA SOCIEDAD ESPAÑOLA



TONY JIN YONG

CEO DE HUAWEI IBERIA

A lo largo de los últimos años, Huawei se ha posicionado a nivel mundial como proveedor líder de soluciones de Tecnologías de la Información y Comunicación (TIC), infraestructuras y dispositivos inteligentes. Nuestras importantes inversiones en I+D, área en la cual están dedicados más del 40% de nuestros 194.000 empleados, nos han permitido posicionarnos como motor impulsor de la transformación digital a nivel mundial.

Este posicionamiento nos ha permitido llevar nuestro negocio a más de 170 países, y dar servicio a más de tres mil millones de personas. Sin embargo, España es un mercado especial para nosotros. A lo largo de

nuestros 19 años de historia en el país hemos establecido un importante vínculo con la sociedad española. Tenemos un significativo compromiso con la economía digital española, la cual impulsamos a través del desarrollo de tres unidades de negocio: Operadores -trabajamos con los principales operadores nacionales-, Empresas -trabajamos con más de 17 clientes que forman parte del IBEX35-, y Consumo.

En concreto, la Unidad de Negocio de Huawei Empresas ha contribuido al desarrollo de las sociedades digitales inteligentes en España. En el último año fuimos parte del desarrollo de varios proyectos de escuelas conectadas, salud e investigación, así como de Smartcities, en ciudades como [Barcelona](#), [Rivas](#), o [Villarreal](#).

Sin embargo, este compromiso va más allá de nuestro negocio y la contribución al desarrollo económico. La voluntad de Huawei de contribuir con España, y los españoles, ha sido una apuesta constante y sostenida en el tiempo. Hemos mostrado nues-

tro apoyo al Gobierno de España, contribuyendo con las Instituciones nacionales, como ha sido recientemente durante la crisis sanitaria causada por el Coronavirus (COVID-19), para la cual hemos donado material sanitario y tecnológico. Huawei seguirá contribuyendo en aquellos ámbitos en los que nuestro expertise tecnológico y apuesta social aporte a la economía digital y a la sociedad española, en su conjunto.

Así, uno de los pilares fundamentales de Huawei en España es el impulso de iniciativas de Responsabilidad Social Corporativa. Recientemente ha finalizado la segunda edición del [Smartbus](#), un proyecto que promueve el uso seguro y responsable de las nuevas tecnologías entre los niños y adolescentes. Esta edición recorrió 45 ciudades de 13 comunidades autónomas, visitando 81 colegios y formando a más de 25.000 personas. La iniciativa nació de forma pionera en el año 2012 con la organización de encuentros didácticos impartidos a más de 12.000

escolares en España. En aquel momento, la interacción con los jóvenes permitió comprender multitud de comportamientos y hábitos de los menores en relación al uso de las nuevas tecnologías.

En el ámbito cultural, el año pasado firmamos un acuerdo de patrocinio con el Teatro Real para apoyar el desarrollo de la cultura española. Este acuerdo también habilitará futuras posibilidades de colaboración entre ambas organizaciones para llevar a cabo el proceso de digitalización del Teatro Real. El desarrollo tecnológico de Huawei, así como su apuesta por la innovación, lo posiciona como un socio estratégico en la transformación digital de España.

España es un país de gran relevancia para Huawei. Llevamos 19 años operando y contribuyendo al desarrollo de la sociedad digital española y tenemos el férreo compromiso de seguir aportando la máxima innovación, nuestro conocimiento y experiencia para lograr la completa transformación digital de España. ■

“SOMOS UN IMPULSOR CLAVE DE LA TRANSFORMACIÓN DIGITAL DE LAS EMPRESAS PÚBLICAS Y PRIVADAS DEL PAÍS”

MARS CHEN, DIRECTOR GENERAL EN HUAWEI ENTERPRISE BUSINESS GROUP SPAIN

El negocio de Empresas de Huawei en España está plenamente consolidado en el mercado español como socio estratégico de las organizaciones que abordan su transformación digital. Crece año tras año a doble dígito, cuenta con un sólido ecosistema de canal y tiene la confianza de las empresas españolas. A lo largo de esta entrevista, su principal responsable en el país, Mars Chen, profundiza en su estrategia, la evolución y las fortalezas de la unidad.

¿Cuál es la trayectoria de Huawei Empresas en España?

Huawei Empresas arrancó en España en 2011 y en menos de diez años, ha experimentado una transformación impresionante. Comenzamos con un equipo muy pequeño que ya cuenta con 100 personas y hemos ido aumentando nuestra presencia territorial. La fórmula para conseguir ratios de crecimiento superior al doble de facturación año tras año ha sido apostar



por el valor, basándonos en un portfolio diferencial y en escuchar las necesidades del cliente, pero siempre apoyándonos en nuestro canal. Disponemos de un ecosistema cada vez más maduro. Contamos con más de 200 partners y hemos hecho un gran esfuerzo para maximizar su beneficio y acelerar la habilitación y la formación de los equipos, que se refleja en los más de 600 ingenieros certificados en las áreas de preventa y/o postventa en diversas tecnologías, que ya aseguran la mayor calidad de servicio a nuestros clientes.

Todo esto, unido al alto nivel de satisfacción postventa, nos ha permitido ganarnos la confianza de más de 17 clientes que forman parte del IBEX35, tener la máxima presencia en proyectos claves de Administración Pública, como el despliegue de tecnología Wi-fi en escuelas y el Ministerio del Interior, así como múltiples iniciativas universidades, gobiernos regionales y otros organismos públicos.

Seguiremos esforzándonos cada día, ya que aún tenemos mucho que demostrar y, por eso, mantendremos nuestra constante inversión en pruebas de concepto, formación o marketing. Acciones como nuestro gran evento anual, el "Huawei Enterprise Day", impensable hace nueve años, reúne cada edición a más de mil asistentes y es un buen reflejo de nuestro avance.

EN 2019, LA UNIDAD DE NEGOCIO DE HUAWAI EMPRESAS DE HUAWAI ESPAÑA MANTUVO UNA POSICIÓN ASENTADA EN EL MERCADO ESPAÑOL, CON UN CRECIMIENTO EN INGRESOS DEL 15%. ASÍ, 2019 FUE EL SEXTO AÑO CONSECUTIVO DE CRECIMIENTO DOBLE DÍGITO DE ESTA ÁREA DE NEGOCIO EN ESPAÑA

¿Cuál es la diferencia de las tres áreas de negocio de la compañía?

Se trata de tres áreas de negocio con focos completamente diferenciados. En el área de Negocio de Infraestructura de Redes de Telecomunicaciones, trabajamos con los grandes operadores del mercado español para desplegar todos los equipamientos y servicios necesarios para construcción de redes de telecomunicaciones.

En el área de Empresas hemos alcanzado una sólida posición en el mercado a través del desarrollo de un fuerte ecosistema de canal y de la apertura de nuevas oficinas en Galicia, País Vasco, Andalucía y la Comunidad Valenciana. Nos hemos convertido en un impulsor clave de la transformación digital de las empresas públicas y privadas del país, gracias a nuestro amplio catálogo de soluciones verticales. En este sentido, Huawei se ha convertido en proveedor de soluciones TIC, clave en los sectores financiero, industrial, transporte y energético. Contamos con 3 mayoristas y 200 partners en el mercado español. Y por último, la Unidad de Negocio

de Consumo, que es la que se encarga del lanzamiento y comercialización de los dispositivos más innovadores.

Desde su perspectiva, ¿cuáles son los principales puntos fuertes de Huawei Empresas?

Huawei está presente en proyectos de la Administración Pública entre los que se encuentran iniciativas de escuelas conectadas, de Inteligencia Artificial (AI, por sus siglas en inglés), de salud e investigación, así como de Smart Cities, área en la que hemos puesto en marcha diferentes proyectos en ciudades como Barcelona, Rivas o Villarreal.

El pasado año presentamos novedades como la solución de Smartcity HiCity, basada en la plataforma digital Horizon, que optimiza la integración de una variedad de nuevas tecnologías y datos TIC para agilizar los procesos de servicio, los datos compartidos y la transferencia de flujos de información, reduciendo el umbral para el uso de nuevas tecnologías y facilitando su integración.

Contamos con 23 centros de investigación en Europa y programas de investigación jun-

to a 140 universidades europeas, centrados en el desarrollo de la tecnología inalámbrica, tecnología óptica y computación en la nube. A través de esto, Huawei está ayudando a las industrias europeas a fortalecer su competencia en estas áreas.

Entre los proyectos destacados del pasado año, se encuentran también la solución de red Campus, que permite la implementación y gestión de servicios de red basados en la nube. En comparación con las soluciones convencionales de la industria, red Campus ofrece una eficiencia operativa y una experiencia de usuario mejorado, y un impulso a la digitalización de las empresas, gracias al acceso a una red inalámbrica que integra acceso Wi-Fi e IoT.

En este sentido, hace unos meses anunciamos el desarrollo de un proyecto pionero de Wi-Fi 6 que explorará casos de uso de Realidad Aumentada en la Universidad de Mondragón. En esta iniciativa se realizarán una serie de pruebas de verificación con el objetivo de explotar la aplicación y el valor de la tecnología Wi-Fi 6 en diferentes escenarios de educación universitaria, así como de promover conjuntamente el desarrollo de la industria de Wi-Fi, con el apoyo del integrador de soluciones TI LKS.

Otros productos y soluciones innovadores que nos posicionan como líderes en el sector son el desarrollo del primer Wi-Fi 6 AP

comercial del mundo, OceanStor Dorado –el almacenamiento All Flash más rápido e inteligente del mundo–, la plataforma informática de Inteligencia Artificial Atlas y la solución LampSite 5G, entre otras.

¿Cuál es la situación actual de Huawei Enterprise Business Group?

En 2019, la Unidad de Negocio de Huawei Empresas de Huawei España mantuvo una posición asentada en el mercado español, con un crecimiento en ingresos del 15%. Así, 2019 fue el sexto año consecutivo de crecimiento a doble dígito de esta área de negocio en España, lo que nos ha consolidado como un impulsor clave de la transformación digital de las empresas públicas y privadas del país. Actualmente cooperamos tanto con el sector público como con el privado, con más de 200 partners españoles y contratos en los principales sectores de la economía española, como el Financiero, el de la Energía, el de Transporte o la Administración Pública.

Todo ello ha sido posible gracias a un catálogo amplio, confiable y competitivo, que incorpora soluciones para las empresas en España, incluyendo el desarrollo de redes empresariales, de acceso y transmisión ópticos, soluciones en la nube y de software, redes inalámbricas, sistemas de colaboración y administración, e Internet de las Cosas.



¿Podemos esperar alguna novedad este año en su estrategia tecnológica o de negocio?

En el área de Negocio de Huawei Empresas mantenemos nuestro compromiso por construir plataformas digitales integradas, innovadoras y abiertas para nuestros clientes. Estas permiten a gobiernos y empresas innovar con mayor agilidad y eficiencia, pasando a la tecnología digital y haciendo que las operaciones diarias sean más inteligentes.

Asimismo, la compañía continúa innovando en dominios avanzados que incluyen Cloud Computing, IoT, Inteligencia Artificial y Big Data, a medida que los nuevos desarrollos en las TIC aceleran la transformación digital

de las industrias, los productos y soluciones innovadores de Huawei –Data Centers, campus empresarial, Intent-Driving Networks, almacenamiento All-Flash, los sistemas troncales de banda ancha (eLTE, por sus siglas en inglés) y soluciones de comunicaciones empresariales– se adaptan a los sectores verticales clave para la compañía: Gobierno, Energía, Transporte, Finanzas e Industria.

Al mismo tiempo, seguimos potenciando la construcción de un ecosistema para apoyar la transformación digital. En este sentido, mediante la creación de plataformas TIC abiertas, OpenLabs y plataformas para marketing, capacitación y servicios globales, la compañía está atrayendo cada vez a más

DURANTE LOS 9 AÑOS DE PRESENCIA DE HUAWEI EMPRESAS EN ESPAÑA HEMOS CONSEGUIDO GANARNOS LA CONFIANZA DE MÁS DE 17 COMPAÑÍAS QUE FORMAN PARTE DEL IBEX-35, Y TENER LA MÁXIMA PRESENCIA EN PROYECTOS CLAVES DE LA ADMINISTRACIÓN PÚBLICA, COMO EL DESPLIEGUE DE TECNOLOGÍA WI-FI EN ESCUELAS Y EL MINISTERIO DEL INTERIOR

socios, permitiendo la innovación conjunta y construyendo un ecosistema alrededor de servicios al cliente.

¿Por qué Huawei está apostando tan fuerte por áreas como 5G y IA?

Si bien diferentes industrias están obteniendo nuevas utilidades de la primera ronda de aplicaciones industriales 5G como banda ancha móvil mejorada, entretenimiento y

fabricación, aún no se puede decir con certeza qué tipo de aplicaciones se verán en el futuro, pero el 5G va a beneficiar a numerosos sectores verticales, desde proveedores de infraestructuras y operadores, hasta pequeños desarrolladores y pymes. Y, en este contexto, el compromiso de Huawei sigue siendo proveer de la mejor tecnología a todas y cada una de las industrias.

También apostamos firmemente por la IA porque creemos que puede ampliar los límites de lo humanamente posible. En este sentido, uno de nuestros proyectos más importantes con esta tecnología es la creación de StorySign, la primera plataforma de alfabetización del mundo para niños sordos. Aprender a leer puede resultar difícil para cualquier niño, pero, para aquellos que padecen una discapacidad auditiva grave o profunda, puede suponer un desafío infinitamente mayor. Con esta aplicación móvil gratuita, podemos ayudar a acercar la lectura a 32 millones de niños sordos de todo el mundo y a adentrarlos en un universo lleno de fantasía, curiosidad y creatividad. ■



HACIA LA DIGITALIZACIÓN INTELIGENTE DE LAS ORGANIZACIONES



Mars Chen, Managing Director en Huawei Enterprise Business Spain

Víctor Jiménez, Chief Engineer en Huawei Enterprise Business Spain

José Concepción, Senior Director Sales Storage en Huawei Enterprise Business Spain

Carlos Piqueras, Sales Manager Health en Huawei Enterprise Business Spain

Miguel Angel Leal, Carrier Enterprise Business & Channel Director en Huawei Enterprise Business Spain

LA DIRECCIÓN DE HUAWEI ENTERPRISE BUSINESS SPAIN EXPONE LA ESTRATEGIA DE LA COMPAÑÍA



Miguel Angel Leal, Carrier Enterprise Business & Channel Director en Huawei Enterprise Business Spain



Carlos Piqueras, Sales Manager Health en Huawei Enterprise Business Spain



Víctor Jiménez, Chief Engineer en Huawei Enterprise Business Spain



José Concepción, Senior Director Sales Storage en Huawei Enterprise Business Spain

TECNOLOGÍAS PARA CONSTRUIR ORGANIZACIONES CONECTADAS E INTELIGENTES

EN APENAS UNA DÉCADA DESDE SU CREACIÓN, LA UNIDAD DE NEGOCIO DE EMPRESAS DE HUAWEI ESPAÑA SE HA POSICIONADO COMO REFERENTE DEL MERCADO, CON UN AMPLIO CATÁLOGO DE SOLUCIONES QUE PERMITEN ABORDAR CON GARANTÍAS LA EVOLUCIÓN A MODELOS DIGITALES QUE ESTÁN LLEVANDO A CABO LA MAYOR PARTE DE LAS ORGANIZACIONES DEL MUNDO.

Huawei ha sido capaz de conformar un gran abanico de soluciones que dan respuesta a los retos empresariales de hoy, pero que también les ayuda a estar preparados para el futuro, por lo que su tecnología es el motor de muchos proyectos transformadores en todos los sectores de actividad: Industria, Banca, Seguros, Transporte, Energía, Administración Pública, etc.

La oferta de esta unidad se compone de productos extremo a extremo, fiables y flexibles para centros de datos, conectividad y red, almacenamiento, plataformas y sistemas, basados en inteligencia artificial, que impulsan proyectos de Big Data y Analítica, Internet de las Cosas, etc.

En este reportaje repasaremos algunas de sus soluciones insignia y casos de éxito de empresas, que acreditan las ventajas competitivas que les han aportado estas tecnologías.



HIDC, LA SOLUCIÓN DE DATA CENTER INTELIGENTE

Los data centers son una infraestructura esencial en la economía digital. Lo han sido siempre, pero hoy, con los datos convertidos en el principal activo de las compañías, cobran un papel crítico. Las empresas tienen que disponer de los recursos que les permitan hacer frente a la ingente cantidad de datos que se generan y, no solo se trata de capturarlos, sino también de poder explotarlos. Ésta es una realidad que va a ir más, ya que se calcula que, en 2025, se genera

rá a nivel mundial un volumen de datos de 180 ZB (zetabytes), frente a los 33 que se creaban hace solo dos años.

La solución Huawei Intelligent Data Center (HiDC) cubre todo el ciclo de vida del centro de datos, desde la construcción hasta la operación y el mantenimiento. Además, contribuye a acelerar la transformación digital al ofrecer una arquitectura flexible e incluir innovaciones que dotan al centro de datos de inteligencia, eficiencia y lo hacen más ecológico.

■ NATIONAL HEALTH SERVICE (NHS)

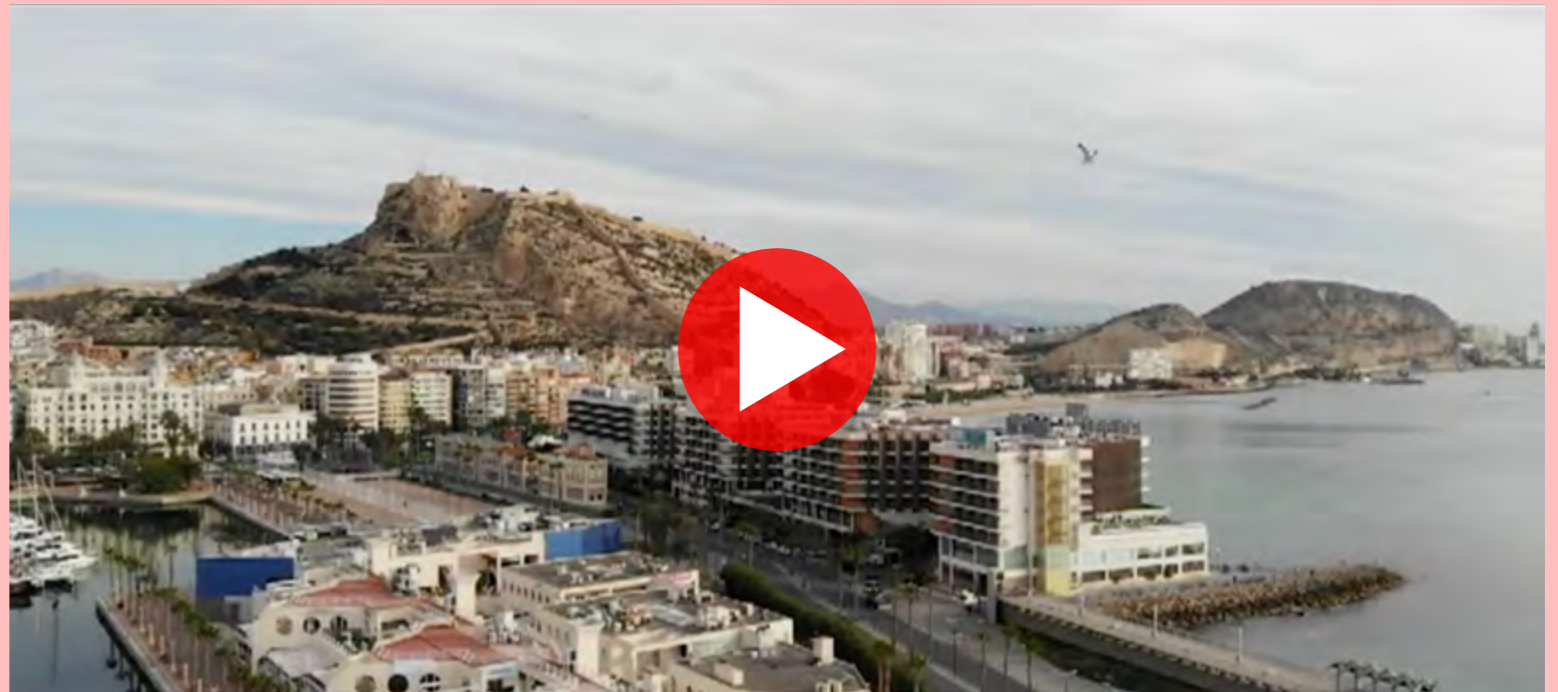
El sistema sanitario de Reino Unido ha construido un centro de datos en nube privada extremo a extremo con la solución de Huawei.



CASOS DE ÉXITO

■ DIPUTACIÓN DE ALICANTE

El organismo provincial ha confiado en Huawei para implantar redes de Data Center y de campus unificadas, que emplean arquitectura SDN (red definida por software) y un Agile Controller para conseguir una gestión de extremo a extremo y automatización de la configuración. En este vídeo sus portavoces explican las mejoras obtenidas en términos de estabilidad, seguridad, gestión simplificada, etc., logradas con este proyecto que persigue la mejora y el rápido despliegue de los servicios públicos.



Caso de éxito: Diputación de Alicante

CAMPUS, SOLUCIÓN DE RED INALÁMBRICA PARA ENTORNOS CONECTADOS

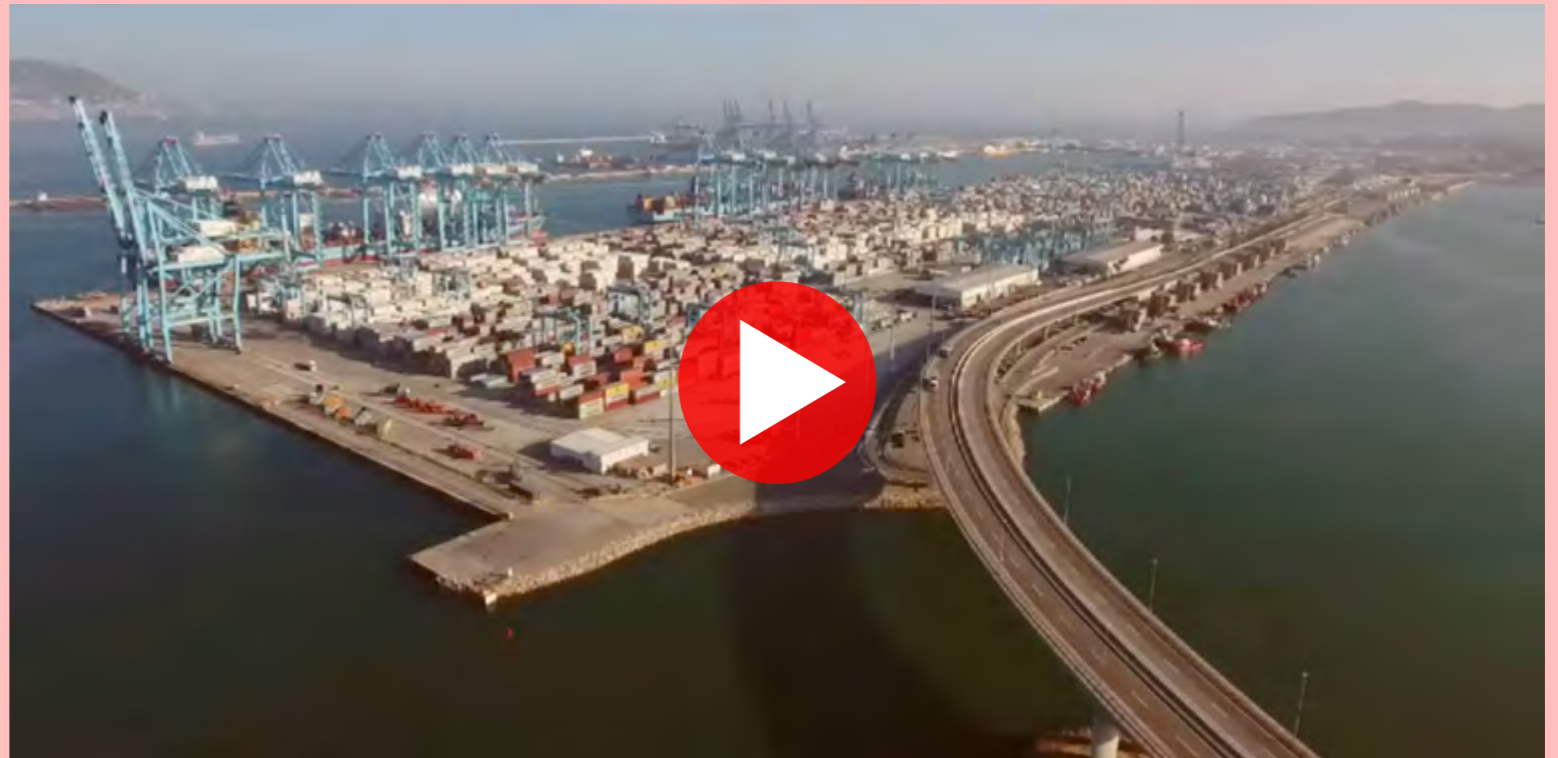
La solución de red Campus supone un nuevo paradigma de servicio de red que permite la implementación y gestión de servicios de red basados en cloud. Este producto mejora la eficiencia operativa y la experiencia del usuario, además de facilitar la rápida implementación de múltiples servicios en una sola red. Por ejemplo, pueden converger múltiples redes para producir conexiones totalmente inalámbricas entre personas, cosas y entornos, y también destaca por la seguridad, el acceso sencillo, la gestión de la eficiencia energética, así como por la automatización de la operación y mantenimiento.

Desde el punto de vista tecnológico, emplea la plataforma digital Horizon y nuevas tecnologías como Inteligencia Artificial, Big Data y Cloud, para rediseñar los sistemas de servicios de los campus. La solución utiliza Wi-Fi 6 (AirEngine), switches (CloudEngine), acceso completamente óptico (Huawei OptiXaccess y Huawei OptiXstar), así como otros productos de vanguardia para ofrecer redes para entornos inteligentes, fáciles de usar y con un elevado ancho de banda.

CASO DE ÉXITO

■ PUERTO DE ALGECIRAS

El Puerto de Algeciras es por volumen de carga el primero en España y el cuarto a nivel europeo. Ha implementado un sistema de comunicación radio que es clave en su estrategia de incluir la innovación como un proceso clave de negocio. Cuenta en este vídeo su experiencia con la tecnología y su estrategia para seguir siendo líder en su sector, basándose en la excelencia de servicios,



Caso de éxito: Puerto de Algeciras

OCEANSTOR,

ALMACENAMIENTO ALL-FLASH RÁPIDO E INTELIGENTE PARA ENTORNOS CRÍTICOS

Las empresas necesitan infraestructuras que den soporte a sus necesidades de manejar grandes cantidades de datos y les permitan extraer conclusiones con la máxima rapidez. El almacenamiento All-Flash ofrece los niveles de rendimiento, fiabilidad, escalabilidad, flexibilidad y costes controlados para gestionar entornos críticos de negocio, y Huawei ha hecho una decidida apuesta por esta tecnología a través de su gama OceanStor.

El sistema insignia de la serie es el modelo Dorado V3, apropiado para bases de datos, infraestructura de escritorio virtual (VDI, en sus siglas inglesas) y uso compartido de archivos.

OceanStor Dorado V3 ofrece una latencia de 0,3 milisegundos, lo que triplica el rendimiento de las aplicaciones, y una disponibilidad del 99,9999%, lo que es posible porque utiliza tres tipos de procesadores inteligentes e incorpora la arquitectura NVMe y algoritmos inteligentes FlashLink para conseguir un uso inteligente de los discos SSD, en los que se almacenan los datos.

Además, proporciona una escalabilidad de hasta 16 controladores y admite

7.000.565 de IOPS SPC-1, y es compatible con funciones completas SAN y NAS. También integra la tecnología de deduplicación y compresión en línea líder de la industria, que logra una tasa de reducción de datos de hasta 5:1 y un 75% de ahorro en OPEX.

CASOS DE ÉXITO

■ BINERO GROUP

Un importante Data Center sueco reduce su impacto ambiental

■ SCSTI

La plataforma nacional de almacenamiento del SCSTI consolida 100 sistemas TI



AIRENGINE, LA REFERENCIA MUNDIAL EN TECNOLOGÍA WI-FI 6

Huawei está a la vanguardia en el desarrollo de Wi-Fi 6 de uso comercial en el mundo, con AirEngine. La compañía implantó la primera red Wi-Fi 6 empresarial en Shanghái en 2018, y su tecnología está implantada en países como India, Sudáfrica, Suiza, Bélgica y España.

Esta familia de productos, compuesta por controladores, antenas 5G y puntos de acceso (PA, en sus siglas inglesas), permiten construir redes Wi-Fi 6 sin brechas de cobertura, ofrecer servicios sin tiempo de espera y evitar cualquier pérdida de paquetes durante la itinerancia. Multiplica por cuatro el ancho de banda de la red y la cantidad de usuarios que se pueden conectar a ella de forma simultánea.

Al permitir una notable reducción de latencia de la red y una ampliación del abanico de tecnologías y aplicaciones que se ven beneficiadas por el aumento de rendimiento que aportan, como la realidad virtual o la aumentada, hace que estas soluciones aceleren la transformación digital.

Son fáciles de desplegar en oficinas, aulas, aeropuertos, establecimientos de retail, ciudades inteligentes, entornos de fabricación, etc.

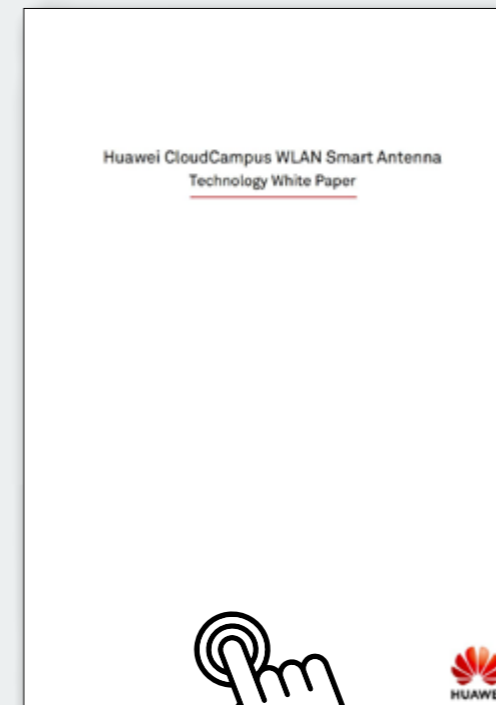
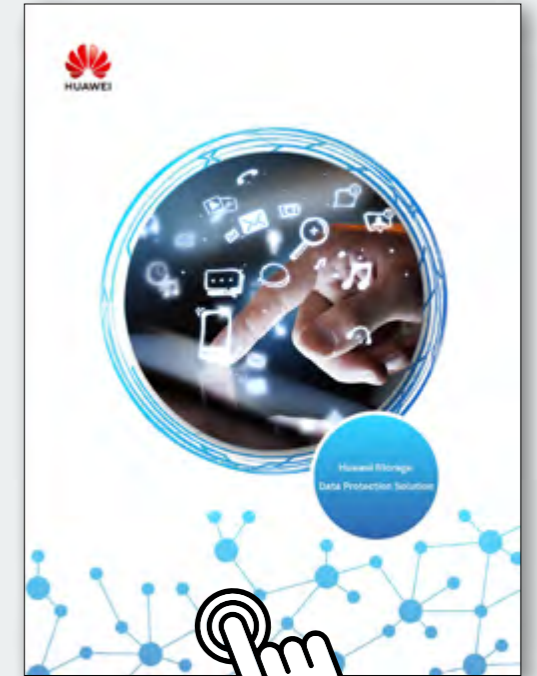
CASO DE ÉXITO

■ UNIVERSIDAD DE MONDRAGÓN

La institución educativa vasca ha conseguido con la tecnología Wi-Fi 6 de Huawei un acceso Wi-Fi fiable y estable a una amplia variedad de aplicaciones, mejorando la experiencia de usuario que ofrece a sus estudiantes.



LA PROPUESTA DE HUAWEI A TRAVÉS DE WHITEPAPERS



SI TE HA GUSTADO ESTA REVISTA, COMPÁRTELA





huawei.com/es

Huawei contribuye al desarrollo de la **economía digital** española

18 años apostando por la formación y el talento en nuevas tecnologías





Ciberseguridad en entornos financieros, el reto que no cesa

Patrocinadores:





El sector financiero ante el reto digital, el cliente en el centro de todo

Como una rueda que no deja de girar, el sistema financiero lleva inmerso en una transformación digital sistémica desde hace más de medio siglo. Tanto es así que este desarrollo tecnológico ha favorecido la mecanización de distintas tareas de soporte a la actividad financiera, como la dispensación automática de

efectivo, pero, también, ha marcado el movimiento hacia un negocio basado en el conocimiento y en el análisis de la información donde el cliente es el núcleo del negocio.

Así, y a lo largo de todos estos años, se han dado pasos de gigante en innovación con el desarrollo de soluciones tecnológicas destinadas

a la informatización de los sistemas de gestión (mainframes), el almacenamiento de la información, comunicaciones corporativas, ofimática y servicios web, auspiciados, estos últimos, por ese gran descubrimiento que ha sido Internet. Pero también, como decíamos, y por el deseo de evolucionar desde un sistema estático y me-

ramente transaccional, basado en la operación, hacia otro más inteligente asentado en el conocimiento del cliente y en su relación con la entidad, se ha apostado fuerte por tecnologías que permitan optimizar el servicio y la calidad ofrecida a los usuarios. En este punto, tecnologías como Big Data y Analytics, Inteligencia Artificial, Machine Learning, Blockchain o Biometría se han integrado a la perfección en las entrañas tecnológicas de los sistemas financieros, adaptándose por entero a las nuevas demandas y promoviendo una eficiencia operativa sin precedentes de

para a mantener un concepto "Open Banking" y de omnicanalidad permanente.

LIDERANDO LA TRANSFORMACIÓN DIGITAL

En este punto, y con la innovación tecnológica por bandera, el sistema financiero actual contempla una [estructura heterogénea](#) en la que convergen instituciones financieras monetarias (entidades de crédito, establecimientos financieros de crédito, entidades de pago electrónico u organismos de autoridad bancaria como el Banco Central Europeo o el Banco de España) junto a otros inter-

mediarios no financieros (Sociedades de Valores, Fondos de Capital Riesgo, Fondos de Titulación...), auxiliares financieros y empresas de seguros. Todas ellas, conviven a su vez con otras entidades que, como en el caso de las Fintech y, posteriormente, las BigTech, Neobancos y empresas de telecomunicaciones (Telecos) utilizan la tecnología para ofertar servicios financieros diferenciadores y que durante los últimos años han experimentado un auténtico boom, propiciado por una oferta disruptiva pero también por unas exigencias regulatorias mucho más livianas.

Por todo ello, el sector financiero necesita seguir avanzando como un gran bloque unido y cohesionado, y que, además, cumpliendo con los principios básicos de la protección al consumidor, estabilidad financiera e integridad del mercado, adaptar su modelo de negocio a una nueva realidad. Para ello, esta entente requiere de un entorno competitivo adecuado que le permita progresar hacia un hábitat flexible, donde se favorezca la innovación, y se limiten prácticas como la intermediación financiera no bancaria (shadow banking), que pueden suponer una amenaza potencial para la estabilidad financiera a largo plazo.

EL FARRAGOSO MUNDO DE LAS NORMATIVAS

Tras la crisis financiera global que comenzó en 2007, se produjo una revisión de los estándares regulatorios globales del sector financiero para que las entidades adoptasen una serie de políticas y estrategias para mejorar su resistencia a los

La nube se ha instaurado como una tendencia en alza en el sector financiero. Sin embargo, para mantener seguros los datos confidenciales la salvaguarda de esta información se convierte en un reto



Desde hace tiempo los ciberataques más exitosos están siendo ejecutados por redes criminales altamente profesionales

riesgos que pudiesen surgir en el ejercicio de su actividad. Dichas medidas, que fueron lideradas por el G20 y el Consejo de Estabilidad Financiera (FSB), se centran principalmente en tres aspectos básicos: solvencia (Basilea III), supervisión (MUS) y contabilidad (IFRS9).

Adicionalmente, el sector financiero tiene que lidiar también con otras leyes que marcan requisitos de liquidez y de capital más altos, como TLAC (a nivel global) y MREL (a escala europea); pruebas de resistencia internas como parte de sus procesos de gestión de riesgos, incluyendo los procesos de adecuación de capital y de liquidez (ICAAP e ILAAP) y otras relacionadas con la conducta, en materia de protección de los inversores y los clientes, como MIFID II y PRIIP.

En lo que respecta a la protección de datos, una de las [prioridades](#) que la Unión Europea se ha marcado en su haber, el Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés) o la regulación europea sobre servicios de pagos electrónicos PSD2, han su-



puesto un antes y un después para un sector en el que la explotación de los datos se ha convertido en uno de sus principales activos. En este sentido, y desde la perspectiva de que la información personal y financiera de los clientes bancarios no pertenece a las entidades financieras ni a terceros, sino que es propiedad de los usuarios, estas organizaciones han tenido que avanzar en múltiples aspectos para adecuarse a una regulación estricta que sanciona cualquier brecha de seguridad.

UNA AMENAZA REAL: LOS DATOS EXPUESTOS

Llegados a este punto, no hay duda de que los datos de los usuarios son un activo de un valor incalculable.

Sin embargo, y por el alcance que representan, la actividad cibernética maliciosa supone una amenaza continuada para el sector financiero

que, en los últimos años, se ha convertido en un ansiado objetivo para los ciberdelincuentes. Tanto es así, que los incidentes de seguridad, tanto online como offline, han aumentado en número y sofisticación, y no solo por parte de ciberdelincuentes o grupos hacktivistas, sino también por parte de los Estados, según el Informe [Ciberamenazas y Tendencias 2019](#) de CCN-CERT.

A este respecto, se estima que, a nivel mundial, en 2021, el crimen cibernético tendrá un coste para las organizaciones de más de 6.000 millones de dólares anuales, frente a los 3.000 millones de dólares que supuso en 2015, según [el Informe Oficial Anual sobre Ciberdelincuencia de 2020](#) de Cybersecurity Ventures. Dicha cantidad incluye el daño y la destrucción de datos; el dinero sustraído; la pérdida de productividad; el robo de propiedad intelectual, de datos personales y de información financiera; la interrupción del curso

normal de los negocios después de un ataque o el daño a la reputación de la marca, entre otros.

Y es que, a pesar de que desde hace años las entidades financieras han incrementado sus inversiones en seguridad, inyectando de media entre el 11% (bancos) y el 10% (entidades no bancarias) de sus presupuestos, según un estudio de [Deloitte](#), la realidad evidencia que los ciberataques, sobre todo los destinados al robo o alteración de datos personales, se han incrementado.

Así, en los últimos años, el mundo de las finanzas ha quedado particularmente expuesto ante ataques dirigidos, DDoS y ransomware. Asimismo, se ha observado un fuerte aumento en el número

de usuarios infectados por troyanos bancarios (Emotet), malware móvil (open banking), phishing dirigido, ingeniería social, ataques 'watering hole' y de puertas traseras que han permitido a los delincuentes cibernéticos infiltrarse en los sistemas de información con total confidencialidad. Los ataques XSS (Cross Site Scripting) como SQL Injection que explotan las vulnerabilidades en los navegadores o servidores web, también representan una amenaza importante.

Además, en el caso de las instituciones bancarias, los cibercriminales han seguido desplegando técnicas tradicionales como la manipulación física de los cajeros automáticos (ATM), el robo de

datos de tarjetas de pago y cuentas bancarias en línea, y la clonación de tarjetas de crédito.

Ante tal proliferación de ataques, muchas empresas han movido ficha, recurriendo a soluciones perimetrales, como firewalls tradicionales para intentar frenar esta escalada de ataques. Sin embargo, ha quedado demostrado que este tipo de tecnologías, por sí mismas, no son suficientes para plantar cara a las nuevas técnicas de ataque, que requieren otra aproximación muy diferente.

Adicionalmente, la escasez de habilidades que golpea a un sector necesitado de profesionales especializados ha resultado ser también un gran desafío para los equipos de seguridad TI de las

La solución pasa por un enfoque multicapa

Desde hace tiempo, los hackers han puesto su diana en las personas, más allá de las infraestructuras. Es una simple cuestión práctica: ¿para qué perder tiempo y recursos atacando redes corporativas o endpoints si es mucho más rápido y sencillo doblegar la naturaleza humana?

A raíz de esta realidad, el mercado financiero se ha puesto manos a la obra para cerrar las brechas de vulnerabilidad y responder a las nuevas amenazas de

manera sistemática. Ser capaces de utilizar un enfoque integral de la ciberseguridad, comenzando por la identificación de los riesgos y las respuestas, se plantea como una forma de potenciar el rendimiento de estas organizaciones. Ya no basta con desplegar modelos tradicionales de seguridad estáticos basados en la detección, lo inteligente es evitar que estas amenazas afecten a los sistemas mediante técnicas de protección multicapa y proactivas. Por tanto, se hace

necesario aumentar el nivel de seguridad informática mediante una combinación de tecnología fiable (prevención de amenazas en tiempo real) inteligencia compartida y protecciones avanzadas en toda la infraestructura corporativa.

De igual modo, la nube se ha instaurado como una tendencia en alza en el sector financiero, dadas sus grandes ventajas, que la convierten en una plataforma idónea para migrar determinados procesos y ayudar a las instituciones

financieras a gestionar grandes cantidades de datos de forma rentable. Sin embargo, para mantener seguros los datos confidenciales y la salvaguarda de esta información se convierte en un reto, así como la necesidad de obtener visibilidad y control sobre miles de servicios cloud, sobre todo según las diversas regulaciones tienden a endurecer las condiciones y a exigir de las entidades mayor transparencia y niveles más altos de protección del consumidor.

empresas financieras. La buena noticia es que ya son muchos los que están trabajando en una mejor cultura en seguridad y, por supuesto, en una mayor inversión en educación, necesaria para formar a los empleados, la primera línea de defensa de cualquier corporación.

CUIDANDO LA TECNOLOGÍA, PERO TAMBIÉN EL COMPONENTE HUMANO

Las amenazas del mundo digital están en constante evolución, por lo que el entorno de seguridad corporativo debe avanzar en idéntica línea, o anticiparse, utilizando una serie de tecnologías que puedan asegurar una protección proactiva frente a estos peligros. En este sentido, los riesgos deben quedar dimensionados para tratar todas las áreas, desde la tecnológica hasta la humana.

A nivel de infraestructura tecnológica una defensa integrada, con las mejores soluciones de su clase, irá encaminada a proteger tanto el correo electrónico (spam, phishing, malware...) como la navegación web (filtrado URL, sandboxing, Ga-

En los últimos años, el mundo de las finanzas ha quedado particularmente expuesto ante ataques dirigidos, DDoS y ransomware

taway Web Seguro...) la nube (CASB, o tecnologías basadas en el nuevo concepto SASE), la red (firewalls, UTMs), o las estaciones de trabajo y los servidores, con tecnología EDR y EPP.

Otra técnica que ha demostrado su capacidad y ha permitido responder a las amenazas con mayor confianza y velocidad es la Inteligencia Artificial, y son cada vez más las empresas que recurren a ella para proteger sus infraestructuras. Sobre esta evolución, un [estudio de Capgemini](#) alude a que el 63% de las organizaciones desplegará IA en 2020 para mejorar la ciberseguridad, siendo su aplicación más popular la seguridad de la red. Adicionalmente, y además

de para proteger la red, las compañías, incluidas las entidades financieras, utilizan la IA para otros fines, como asegurar sus datos, salvar sus endpoints y desarrollar una mejor gestión de la identidad y el acceso, sin olvidar, su idoneidad para identificar y entender las intenciones del phishing y de los correos electrónicos fraudulentos.

Sin embargo, y al igual que ocurre con el Machine Learning, utilizado para monitorizar la actividad de cualquier ordenador a fin de detectar y bloquear automáticamente los procesos sospechosos antes de que ocurran, o el Deep Learning, empleado para realizar predicciones a partir del



conocimiento, estas tecnologías se han convertido en objeto de deseo para los cibercriminales más avezados. Desde hace tiempo, los ciberataques más exitosos están siendo ejecutados por redes criminales altamente profesionales que aprovechan estas tecnologías para explotar vulnerabilidades como el comportamiento de los usuarios o las brechas de seguridad, y así obtener acceso a sistemas y datos empresariales.

La biometría también se está convirtiendo en un gran aliado para la ciberseguridad. De hecho, las técnicas de autenticación biométrica como las huellas dactilares, el iris y la voz son extremadamente útiles para el reconocimiento de personas basada en rasgos de conducta o físicos.

Para proteger la información, además del uso de técnicas de análisis, aprendizaje e inteligencia de amenazas, contar con herramientas criptográficas que por medio del cifrado de los datos ayuden a garantizar la confidencialidad e integridad de la información financiera, será de gran ayuda. De hecho, estas tecnologías resultarán cruciales para cumplir con los requerimientos de seguridad en los entornos financieros y asegurar el cumplimiento, tanto a nivel normativo como de negocio. Por ello, la implantación de comandos criptográficos y de Tarjetas EMV, o la actualización de las Claves de los ATM's y el uso de la firma digital permitirán luchar contra amenazas como el phishing en el ámbito financiero. Por supuesto, tampoco

¿Te gusta este reportaje?

Compártelo en redes






hay que olvidar la tecnología de Blockchain, que emplea mecanismos criptográficos de seguridad para acceder, firmar y cifrar las transacciones, los bloques y su encadenado.

Por último, no hay que olvidar el componente humano que, como ha quedado verificado a lo largo de los años, es el eslabón más débil de la cadena y la principal causa de infracciones de datos. Y es aquí donde las compañías deben revisar sus protocolos de actuación y, por supuesto, nunca dar nada por sentado. Ninguna fuerza laboral, ni siquiera la más joven, lleva aparejada una conciencia innata de las amenazas a la ciberseguridad. ■



MÁS INFORMACIÓN

-  [Las API son ahora el objetivo de los ciberataques contra entidades financieras](#)
-  [El 41% de las familias de malware observadas en 2019 eran nuevas](#)
-  [Se disparan los ataques DDoS inteligentes centrados en la capa de aplicación](#)

**THE ART OF
CYBERSECURITY**



Presentamos el arte de proteger su nube híbrida

Cuando los entornos físicos, virtuales, cloud y de contenedores están protegidos de una manera sencilla y automatizada, la ciberseguridad puede ser una obra de arte.

Conozca cómo en www.theartofcybersecurity.com

Amenazas desconocidas detectadas
y detenidas en el tiempo por Trend Micro.
Creado con datos reales por el artista Brendan Dawes



EVA CRISTINA CAÑETE BONILLA, CISO DE UNICAJA BANCO

“Los modelos de seguridad tradicionales ya no tienen el efecto deseado”

En plena transformación digital, en un momento en que los usuarios demandamos un acceso a los servicios en todo momento y lugar, los bancos y los servicios financieros se han convertido en uno de los objetivos preferidos de los ciberdelincuentes. De los retos y amenazas a las que se enfrentan preguntamos a Eva Cristina Cañete Bonilla, CISO de Unicaja Banco.

La banca, los servicios financieros, son ahora digitales, móviles y cada vez más centrados en los clientes. A nivel de seguridad, ¿qué retos cree que está afrontando el sector financiero?

Sin duda alguna la Transformación Digital, el uso masivo de dispositivos móviles, el IoT o el Big data son retos importantes para la protección de nuestra información. Desde hace algún tiempo se nos viene demandando acceder a ella en cualquier momento y desde cualquier lugar.

Y no solo empleados o proveedores, también los clientes quieren relacionarse con su banco de este modo, provocando un alto impacto en la forma de protegernos. Por todo ello, los modelos de seguridad tradicionales ya no tienen el efecto deseado. Se hace imprescindible adaptarlos a la nueva forma de ser empresa.

Esto no va solo de un cambio en la estrategia de seguridad sino de un cambio en los departamentos de seguridad, que ahora más que nunca tienen que ser ágiles, flexibles y resilientes.



Cómo hacer frente a los nuevos modelos omnicanal donde se transfieren más datos entre sistemas que nunca.

La omnicanalidad habla de fronteras, o mejor dicho habla de su desaparición. Las empresas tenemos que estar preparadas para que consuman nuestros servicios desde cualquier lugar y en cualquier momento. El intercambio de información es incesante e imparable. Esto adquiere especial relevancia si pensamos que la mayoría estamos adoptando modelos de trabajo colaborativo, amparados en la Transformación Digital.

Lo que nos lleva a basar nuestra estrategia de seguridad en la protección del dato, con independencia de donde esté, quién y cómo lo consume.

Las amenazas internas en el sector financiero no solo proceden de los empleados o la cadena de distribución, sino de miles de clientes, ¿cómo se aborda este reto?

Las entidades llevamos formando y concienciando a nuestros empleados, ya que es la forma de prevenir que sean víctimas de engaños que puedan acabar provocando incidentes de segu-

ridad. Se trata de crear cultura de seguridad corporativa que redunde también en una mejora en la concienciación de los clientes, los cuales son objetivos de los planes de seguridad, formación y concienciación. Realizar consejos sencillos de seguridad, comunicados a través de los diferentes canales de interacción con los clientes, es el mejor modo de combatir este tipo de amenazas.

Las técnicas de múltiple factor de autenticación que garantizan que la persona adecuada accede a la cuenta correcta, ¿son imprescindibles en estos entornos? ¿se está haciendo uso de la biometría?

Aunque el uso de técnicas de múltiple factor de autenticación no está generalizado, es una tendencia al alza y en mi opinión, imprescindible. En especial cuando se consumen servicios en Internet, como pueden ser servicios de almacenamiento de información, espacios de trabajo colaborativo, etc.

Por otro lado, las entidades financieras estamos preparadas para ofrecer biometría como segundo factor de autenticación en el consu-

“La aparición de normativas en materia de seguridad supone una palanca para los departamentos de seguridad de las empresas”



mo de servicios bancarios. Observamos que esta adopción va al ritmo en el que los clientes poseen dispositivos móviles con estas capacidades, como no podría ser de otro modo. Con el tiempo, y gracias al uso de este tipo de móviles, acabará imponiéndose como mecanismo de autenticación.

¿Qué impacto han tenido normativas como GDPR, PCI DSS o PSD2?

En general, la aparición de normativas en materia de seguridad supone una palanca para los departamentos de seguridad de las empresas que le ayudan a visualizar su función, al tiempo que suponen un consumo en tiempo

y recursos muy importante. Y este impacto no se puede medir solo en términos de adecuación. Hay que contabilizar el impacto que tiene mantener esos cumplimientos. Por ello, hay que buscar sinergias y elementos comunes entre las normativas que nos apliquen minimizando los esfuerzos individualizados.

El uso de los marcos de controles de seguridad o framework que analizan la seguridad desde distintas perspectivas (legal, organizativa y técnica) y capacidades o dominios (gobierno, seguridad, vigilancia y resiliencia) facilitan la adecuación a diferentes normativas. Nos permiten aunar esfuerzos y aprovechar los requisitos comunes y no comunes de todas ellas. ■

¿Te gusta este reportaje?


Compártelo en redes



 **MÁS INFORMACIÓN**

 [Unicaja Banco](#)

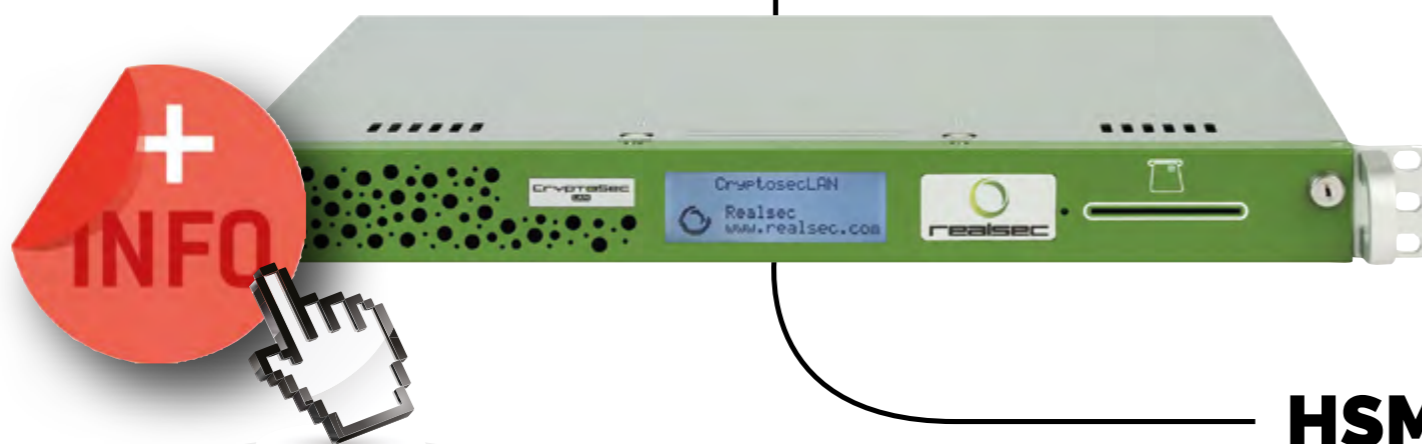
 [Unicaja Banco refuerza sus medidas de prevención](#)

 [Medidas a adoptar por la banca móvil para garantizar la seguridad de las transacciones](#)



CIFRADO HARDWARE EN EL ÁMBITO FINANCIERO

CRYPTOsec LAN



HSM con el mayor rendimiento transaccional del mercado

- Incluidos todos los algoritmos de cifrado simétricos y asimétricos **(sin costes adicionales ocultos).**
- Autenticación de doble factor para cumplimiento PSD2 e integración con soluciones de Blockchain.
- Certificación FIPS 140-2 level 3 del NIST y la Certificación PCI PTS HSM v2.0. del PCI Security Standards Council.



realsec

La clave para proteger su negocio



www.realsec.com

JOSÉ DE LA CRUZ, DIRECTOR TÉCNICO, TREND MICRO IBERIA

“En la adopción de las correctas medidas de seguridad el sector financiero progresa adecuadamente”

Las instituciones financieras asumen un papel aún más activo en la creciente convergencia de la tecnología de la información (TI) y la tecnología operativa (OT). La necesidad de dar servicio a los clientes las 24 horas, los 7 días de la semana, ha llevado a la industria a adaptarse, especialmente con la adopción de dispositivos inteligentes conectados. Sobre los retos de seguridad que afrontan los servicios financieros o cómo impactan las regulaciones hablamos con José de la Cruz, Director técnico de Trend Micro.

La banca, los servicios financieros, son ahora digitales, móviles y cada vez más centrados en los clientes. A nivel de seguridad, ¿qué retos cree que está afrontando el sector financiero?

Aprecio 2 retos. Desde el punto de vista de infraestructura: el banco tiene que garantizar que

su infraestructura es segura y resistente ante ataques de robos de información, denegación de servicio, suplantación de identidad, etc. Desde el punto de vista del usuario: el banco tiene que intentar garantizar que el usuario no sea víctima de ningún tipo de estafa que esté suplantando la identidad del banco.



¿Cuán maduro es el sector financiero respecto a la adopción de las adecuadas medidas de seguridad?

Progresada adecuadamente. No estamos en el escenario ideal, pero se aprecia una fuerte inversión en ciberseguridad la cual se incrementa de manera progresiva y constante año tras año.

¿Cree que se está educando a empleados y clientes para adoptar de manera segura los nuevos entornos bancarios financieros?

Si, la concienciación es uno de los puntos clave. Como apuntaba anteriormente, el banco es indirectamente responsable de que sus usuarios sean capaces de discernir una estafa de una comunicación legítima por parte del banco.

Esto se consigue con campañas de concienciación y con una estrategia de comunicación

¿Quieres saber más?

Puedes ampliar la información de la propuesta de Trend Micro para proteger los entornos financieros en este enlace



muy clara (ej.: el banco nunca se va a dirigir por correo electrónico al usuario para pedirle datos).

Por otra parte, al igual que cualquier otra compañía que maneje datos sensibles, la concienciación, formación y evaluación continua al empleado es fundamental para conseguir

que éste represente la primera barrera de protección.

¿Qué impacto tiene el cumplimiento regulatorio de normativas como PSD2 en este mercado?

Un impacto positivo y, a mi entender, asumible por bancos y usuarios. Cuestiones como la doble autenticación son una realidad desde hace tiempo en servicios de correo o a nivel empresarial. Incluso los propios bancos las utilizaban para autenticar operaciones sensibles (ej.: Transferencia). Ahora simplemente se volverán generalizadas.

Es una normativa que va a ayudar a mejorar la seguridad y a reducir drásticamente ataques basados en robos de credenciales.

¿Qué puntos cree que tendría que mejorar el sector financiero?

Creo que debe continuar en la línea actual y quizás ser más flexible y ágil a la hora de implementar mecanismos de protección. ■

¿Cuál es la propuesta de Trend Micro?

La propuesta de Trend Micro radica en cubrir todos los vectores de ataque con una tecnología que permita colaboración (no sólo con productos del mismo fabricante) y que proporcione visibilidad y control al banco.

Adicionalmente, ponemos foco en la protección de vulnerabilidades las cuales continúan representando un foco de ataque crítico y que deben ser cubiertas tanto en sistemas soportados como en aquellos que

ya están fuera de soporte por parte del fabricante (ej.: Windows 2000, 2003 y 2008). Esto se consigue implementando la tecnología de parchado virtual tanto en el endpoint como en servidores y/o la red.



MÁS INFORMACIÓN



[Bancos bajo ataque: Tácticas y técnicas utilizadas para apuntar a organizaciones financieras](#)



[Caso de éxito: Bulgarian American Credit Bank](#)

JESÚS RODRÍGUEZ, CEO DE REALSEC

“Uno de los más importantes retos a los que se enfrenta la Banca europea es dar cumplimiento al marco normativo PSD2”

Caminamos hacia la consolidación de una sociedad y economía digitales, en la que la Banca, Entidades financieras y empresas de Medios de Pago han tenido que adaptar sus procesos de negocio hacia un entorno cada vez más digital. Sobre los retos de seguridad que afrontan los servicios financieros o cómo impactan las regulaciones hablamos con Jesus Rodríguez, CEO de Realsec.

La banca, los servicios financieros, son ahora digitales, móviles y cada vez más centrados en los clientes. A nivel de seguridad, ¿qué retos cree que está afrontando el sector financiero?

Efectivamente, en este momento estamos asistiendo a importantes cambios en la Banca, la mayoría determinados por procesos de transformación digital. Entre estos, destacamos la aparición de las empresas financieras tecnológicas o Fintechs, que apoyándose en tecnología digital están ofreciendo una amplia variedad de

servicios innovadores para el consumidor a un menor coste. Por lo que respecta a los retos, en mi opinión, uno de los más importantes retos al que se enfrenta la Banca europea, en este momento, es dar cumplimiento al marco normativo PSD2. En España, el cumplimiento de este nuevo marco normativo deberá hacerse efectivo, tal como ha establecido el Banco de España, a finales del presente año.

La Banca tiene además otros importantes retos a los que hacer frente, tales como la extracción de un mayor valor a sus datos, la lucha contra el



fraude o los ciberataques, cada vez más sofisticados, a los que se enfrenta cada día.

¿Cuán maduro es el sector financiero respecto a la adopción de las adecuadas medidas de seguridad?

La banca española siempre ha estado comprometida con la seguridad y, en muchos casos, ha sido pionera en la definición de las políticas y procedimientos y medidas de seguridad necesarias para evitar los riesgos inherentes a su operativa de negocio. En mi opinión, cuenta con un

¿Cuál es la propuesta de Realsec?

Realsec, como empresa desarrolladora de sistemas de cifrado basados en hardware (HSM), dispone de varias soluciones para proteger la operativa bancaria y de los Medios de Pago.

Una de nuestras soluciones más implantadas en la Banca de múltiples países es nuestro HSM financiero y para pagos "Cryptosec-BANKING". Se trata de un HSM que incorpora funciones y comandos criptográficos complejos, definidos para la Banca Universal por el Consorcio PCI (VISA y MASTERCARD) y que han sido desarrollados utilizando algoritmos de cifrado simétrico y asimétrico estándar. Estos comandos, protegen las transacciones bancarias y proporcionan un entorno seguro en el ámbito de los medios de pago.

Entre las funcionalidades de Cryptosec-BANKING se encuentran: la generación, validación y verificación de los códigos PIN de las Tarjetas de crédito y débito, competencia como centro autorizador de tarjetas, funciones de autenticación, generación de mensajes, tokenización, etc.

Realsec, dispone de otras soluciones basadas en hardware criptográfico para reforzar los sistemas de autenticación robusta (SCA), gestionar y proteger de forma centralizada las claves y los certificados, cifrar datos y archivos o fortalecer las nuevas plataformas de Blockchain.

alto conocimiento, en materia de seguridad lógica y digital, así como con la capacidad suficiente para poder adoptar e implantar cualquier tipo de medida, venga o no determinada por las diversas normativas a las que está sujeta.

¿Cree que se está educando a empleados y clientes para adoptar de manera segura los nuevos entornos bancarios financieros?


Más que educar considero que la Banca está informando a sus clientes usuarios para que adopten determinadas medidas que eviten los posibles riesgos de fraude o ciberdelitos cuando éstos operan con la Banca digital.

¿Qué impacto tiene el cumplimiento regulatorio de normativas como PSD2 en este mercado?

En el caso de la normativa europea PSD2, su cumplimiento tiene un elevado coste para la Banca por cuanto está obligada a desarrollar las APIS necesarias que permitan poner a disposición de terceros los datos de sus clientes. Además, las entidades financieras están obligadas a implantar soluciones de autenticación robusta (SCA) que utilizan claves que deberían de ser generadas y custodiadas en dispositivos criptográficos. Hasta ahora, muchas de las entidades financieras han optado por salvar la situación mediante el envío de un mensaje SMS a sus clientes, con una clave de autenticación de un solo uso, pero su elevado coste por cada transacción les llevará sin duda a implantar soluciones tecnológicas de autenticación

¿Quieres saber más?

Puedes ampliar la información de la propuesta de **Realsec** para proteger los entornos financieros en este enlace



ción más eficientes y menos costosas.

¿Qué puntos cree que tendría que mejorar el sector financiero?

En materia de seguridad todo es siempre mejorable, pero podemos decir que el sector financiero, en general, está preocupado por el alto incremento del malware, cada día más sofisticado y dirigido hacia la banca móvil, así como por el incremento del phishing sobre los dispositivos móviles.

La Banca tendría que mejorar sus sistemas de autenticación implantando soluciones más robustas de doble o triple factor para lograr así una mayor protección de los sistemas de pago en la Banca Móvil; al mismo tiempo que mejora los sistemas de protección de los datos, las claves y los certificados y avanza en la usabilidad de la tecnología Blockchain para determinados procesos de negocio. ■

MÁS INFORMACIÓN

[Hardware para la encriptación de datos](#)

[Caso de éxito: Diebold](#)

MIGUEL ÁNGEL ROJO, CEO DE BOTECH

“El principal reto del sector financiero continúa siendo la protección de datos sensibles”



Cada día se realizan ingentes cantidades de operaciones financieras a través de internet, no sólo compras, sino pagos de facturas y todo tipo de transacciones bancarias. Todas estas operaciones crean una gran cantidad de datos confidenciales que se deben proteger. Sobre los retos de seguridad que afrontan los servicios financieros o cómo impactan las regulaciones hablamos con Miguel Ángel Rojo, CEO de BOTECH.

La banca, los servicios financieros, son ahora digitales, móviles y cada vez más centrados en los clientes. A nivel de seguridad, ¿qué retos cree que está afrontando el sector financiero?

El sector financiero lleva muchos años situado en el punto de mira de los ciberdelincuentes y es uno de los principales focos de ciberataques. Esto no es algo nuevo y el sector, que es muy consciente de ello, se está regulando constantemente. El principal reto del sector financiero continúa siendo la protección de datos sensibles, tanto de manera interna como externa. Por eso, cada día el estándar PCI-DSS es requerido

por más empresas ya que, si se procesa, guarda o transmite datos de tarjetas, se debe cumplir con el estándar.

La normativa PCI ha tenido un fuerte impacto en este mercado, ¿qué viene a regular y a quiénes? ¿cómo impacta en los pagos móviles?

Hemos trasladado nuestra tarjeta física a un entorno digital, que convive con muchas aplicaciones que tenemos descargadas en nuestro dispositivo. Es fundamental que todas esas aplicaciones estén desarrolladas con el estándar PA-QSA, Payment Application Qualified Security Assessor (PA-QSA), dentro de las normas de PCI Council.

Además está la variante de firma en dispositivos con tabletas o Smartphones; dentro del estándar PCI hay una norma para este tipo de aplicaciones que es PCI Pin On Glass, lo que demuestra que es un estándar vivo. Es fácil imaginar que en muy poco tiempo todas nuestras tarjetas estén incluidas en nuestro dispositivo móvil y tenemos que tener la misma seguridad que tenemos ahora en el pago con tarjeta física.

Es muy importante que seamos conscientes de que no importa tu sector de actividad, si tu organización procesa, guarda o transmite datos de tarjetas debe cumplir con el estándar PCI DSS. Para cumplir con este estándar, es necesario definir

¿Cuál es la propuesta de BOTECH?

Desde BOTECH, junto a nuestro partner 1st Secure IT, impulsamos el cumplimiento de la normativa PCI DSS. Nuestra propuesta ofrece la posibilidad de conseguir esta certificación con una metodología muy sencilla. Proponemos, en primer lugar, realizar un curso inicial de capacitación con el objetivo de abordar temas sobre conceptos generales, puntos clave para el cumplimiento y concienciar dentro de la organización. En segundo lugar, llevar a cabo un asesoramiento experto para el alcance del PCI DSS, para lo cual se realizan entrevistas, se recopila información y se revisa la documentación necesaria para identificar de manera clara los procesos, activos y proveedores involucrados que determinarán el alcance de PCI DSS. En tercer lugar, realizamos un GAP Analysis gratuito para nuevos clientes con el fin de analizar todos los procesos de seguridad existentes y determinar el nivel de cumplimiento de la organización. Y, en último lugar, se realiza una fase de revisión final donde se determina el estado de cumplimiento de PCI DSS y la posterior preparación del informe ROC (Report on Compliance) y AOC (Attestation of Compliance).

También es muy importante recordar que, aunque la normativa PCI DSS debe completarse anualmente, al igual que la auditoría, se recomienda obtener reportes aprobados de forma trimestral.

con el comité de dirección una persona responsable dentro de la empresa. PCI DSS no es, ni mucho menos, una normativa imposible de cumplir, pero sí es necesario apoyo experto para lograr la implementación de forma eficiente.

La normativa PCI DSS consta de seis categorías, 12 requisitos, alrededor de 200 controles y 250 procedimientos de prueba con el fin de garantizar la confidencialidad de los datos de la tarjeta de pago.

Estos son los requisitos fundamentales que es necesario cumplir:

- ❖ Construir y mantener una red segura.
- ❖ Proteger los datos de los titulares de las tarjetas cifrando la transmisión de datos e información confidencial de los titulares.
- ❖ Establecer un programa de gestión de vulnerabilidades.
- ❖ Crear medidas sólidas de control de acceso.
- ❖ Monitorizar y testar regularmente las redes y mantener una política de seguridad de la información actualizada.

Se habla de PCI DSS, y también de PCI 3DS, PCI PIN, PCI ISA... ¿Qué les diferencia?

Todas estas normativas buscan garantizar la protección de datos y la seguridad en las transacciones económicas. Por ejemplo, PCI ISA (Internal Security Assessor) permite evaluar y validar el cumplimiento de PCI DSS a través de la realización de autoevaluaciones internas. El objetivo de la normativa PCI PIN es garantizar la gestión se-

¿Quieres saber más?

Puedes ampliar la información de la propuesta de **BOTECH** para proteger los entornos financieros en este enlace



gura, el procesamiento y la transmisión del número PIN en las transacciones económicas. PCI 3DS crea un marco de trabajo transversal que permite la implementación en forma masiva de este protocolo de seguridad en entornos de e-commerce y m-commerce o comercio móvil.

¿Cuál es el nivel de adopción de esta normativa en España?

Según un reporte sobre seguridad en medios de pago de la firma Verizon, 2019 Payment Security Report, 15 años después de la puesta en vigor del PCI DSS, el número de empresas que logran mantener el cumplimiento al 100% de los 12 requisitos de la normativa se redujo del 52.5 % registrado en 2018 a un mínimo de 36.7% en todo el mundo, un dato muy significativo y preocupante. ■

MÁS INFORMACIÓN

 [El cumplimiento PCI cae por primera vez en seis años](#)

 [BOTECH Academy](#)

LUIS SUÁREZ, PRESALES MANAGER DE KASPERSKY IBERIA

“El mercado financiero es uno de los más conscientes de la importancia de adoptar medidas de seguridad”

Los incidentes de ciberseguridad que afectan al mundo financiero no solo provocan pérdidas económicas a las entidades y a sus clientes, sino que también implican pérdida de datos, daños en la reputación corporativa, filtraciones de información confidencial, etc. Sobre los retos de seguridad que afrontan los servicios financieros o cómo impactan las regulaciones hablamos con Pedro García Villacañas, Director preventa de Kaspersky Iberia.

La banca, los servicios financieros, son ahora digitales, móviles y cada vez más centrados en los clientes. A nivel de seguridad, ¿qué retos cree que está afrontando el sector financiero?

Entre los retos a afrontar se encuentran los ataques de phishing financiero, que crecieron un 9,5% en el último trimestre de 2019.

Además, durante el pasado año los ciberdelincuentes aplicaron un nuevo método: el robo

mediante la manipulación directa de las aplicaciones bancarias utilizando los servicios de accesibilidad de las aplicaciones.

Los troyanos bancarios, que crecieron un 61% en 2019, y el malware para cajeros también son retos a los que la banca debe hacer frente.

¿Cuán maduro es el sector financiero respecto a la adopción de las adecuadas medidas de seguridad?



El mercado financiero es uno de los más conscientes de la importancia de adoptar medidas de seguridad para su negocio y clientes. De hecho, el impulso de medidas de seguridad como la biometría, la autenticación multifactor o la basada en el comportamiento, viene dado en buena parte por su adopción por el sector financiero. Eso no impide, sin embargo, que los ciberdelincuentes sigan buscando vectores de ataque para superarlos.

¿Cree que se está educando a empleados y clientes para adoptar de manera segura los nuevos entornos bancarios financieros?

La formación de empleados y clientes es uno de los puntos más importantes cuando hablamos de ciberseguridad. Los empleados sue-

len ser considerados el eslabón más débil de la cadena por lo que es importante poner a su disposición una formación continua sobre las políticas, las amenazas actuales y cómo enfrentarse a estas amenazas. Debería prestarse especial atención a la ingeniería social, que sigue siendo el vector de ataque más común y exitoso.

¿Cuál es la propuesta de Kaspersky ?

Kaspersky dispone de distintas soluciones para elevar los niveles de seguridad a través de la predicción, prevención, detección y respuesta al cibercrimen. Entre ellas:

- ❖ **KASPERSKY ENDPOINT SECURITY FOR BUSINESS.** Protección adaptativa para amenazas dirigidas a los endpoints.

- ❖ **THREAT MANAGEMENT AND DEFENSE.** Protección avanzada basada en inteligencia de amenazas.

- ❖ **IOT & EMBEDDED SECURITY.** Protección de los sistemas IoT y dispositivos integrados, reduciendo al máximo los riesgos en estos dispositivos.

- ❖ **KASPERSKY ANTI TARGETED ATTACK PLATFORM.** Una solución de seguridad unificada contra ataques dirigidos.

- ❖ **KASPERSKY ENDPOINT DETECTION AND RESPONSE.** Prevención de las interrupciones de la actividad al eliminar los riesgos de las amenazas avanzadas.

¿Qué impacto tiene el cumplimiento regulatorio de normativas como PSD2 en este mercado?


El cumplimiento de dichas normativas suele obligar a la adopción de nuevas tecnologías. Debemos entender que la inclusión de nuevas tecnologías suele ir de la mano con nuevos vectores de ataque, y es muy probable que los atacantes recurran a nuevos esquemas fraudulentos para abusar de estos nuevos mecanismos.

¿Qué puntos cree que tendría que mejorar el sector financiero?

La interconexión de los sistemas y el uso de los dispositivos móviles se encuentra muy extendido tanto para el acceso remoto como para compartir datos. Esta digitalización expone cada vez más a las organizaciones financieras a ataques tanto genéricos como dirigidos.

Por eso, además de todas las medidas que las entidades tengan en marcha, es recomendable prestar atención a los nuevos vectores de ataque que se podrían desarrollar en los próximos meses:

¿Quieres saber más?

Puedes ampliar la información de la propuesta de **Kaspersky** para proteger los entornos financieros en este enlace 

- ❖ **Ataques a Fintech.** Las apps de inversión son cada vez más populares entre los usuarios de todo el mundo, pero no todas estas aplicaciones utilizan las mejores prácticas de seguridad.

- ❖ **Nuevos troyanos para banca móvil.**

- ❖ **Acceso de pago a la infraestructura bancaria y ataques ransomware a bancos.** Los expertos de Kaspersky esperan un aumento de la actividad de los grupos especializados en la venta de accesos a la red de bancos de las regiones de África y Asia, así como de Europa del Este.

- ❖ **Magecarting 3.0:** más grupos de ciberdelincuentes se centrarán en los sistemas de procesamiento de pago online. En los últimos años, el llamado JS-skimming (el método de robo de datos de tarjetas de las tiendas online) ha ganado popularidad entre los atacantes. ■



MÁS INFORMACIÓN



[Caso de éxito: Alfa Bank](#)



[Machine Learning in Cybersecurity](#)

NURIA ANDRÉS, TERRITORY ACCOUNT MANAGER SPAIN&PORTUGAL DE FORCEPOINT

“Los clientes seguimos siendo la gran asignatura pendiente”

Los bancos siempre han estado a la vanguardia de la ciberseguridad empresarial. Sus enormes reservas de efectivo y datos de consumidores los han convertido en un objetivo principal para los ciberdelincuentes, y la amenaza de pérdidas financieras, consecuencias regulatorias y daños a la reputación los ha impulsado a innovar y acelerar el campo de la ciberseguridad. Sobre los retos de seguridad que afronta o cómo impactan las regulaciones hablamos con Nuria Andrés, Territory Account Manager Spain&Portugal de Forcepoint

La banca, los servicios financieros, son ahora digitales, móviles y cada vez más centrados en los clientes. A nivel de seguridad, ¿qué retos cree que está afrontando el sector financiero?

Está claro, que desde el punto de vista económico el gran reto del sector financiero es la solvencia, pero desde el punto de vista de la seguridad, sin lugar a dudas, es la protección del dato, datos de clientes o activos financieros. ¿Y por qué? Porque pueden provocar pérdidas económicas millonarias por filtraciones de información confidencial de clientes, pero

también pueden suponer una enorme pérdida reputacional, y está demostrado que la pérdida reputacional que sufren los bancos, por incidentes o brechas de seguridad, es mucho más grave que en compañías de otros sectores. Suele decirse que, “el dinero es miedoso”. También es un sector especialmente sensible a ataques de phishing o ransomware, pero contra sus clientes.

¿Cuán maduro es el sector financiero respecto a la adopción de las adecuadas medidas de seguridad?



Probablemente, el sector financiero sea uno de los sectores más regulados. Están sujetos a múltiples normativas, GDPR, MiFID II o PSD2, y eso ha ayudado a desplegar diferentes soluciones de seguridad, pero también procesos y procedimientos. Por eso, si comparamos al sector financiero frente a otros sectores, quizás sea el “alumno aventajado”.

¿Cree que se está educando a empleados y clientes para adoptar de manera segura los nuevos entornos bancarios financieros?

En banca y también en otros muchos sectores, se está “educando y concienciando” a los empleados, por ejemplo, simulando campañas de phishing,

que sigue siendo uno de los principales vectores de ataque, e impartiendo cursos con nociones, al menos, básicas de ciberseguridad, para aquellos empleados que hayan “caído en la trampa”.

Sin embargo, los clientes seguimos siendo la “gran asignatura pendiente”. En mi opinión, no sólo es una responsabilidad del sector bancario concienciar a sus clientes, nociones de ciberseguridad deberían impartirse desde la escuela, ya que vivimos en un mundo, enteramente digital, y debería estar en nuestro ADN saber que no tenemos que proporcionar nunca a nadie, nuestro usuario y nuestra password de acceso a la banca online. Nuestro banco, nunca nos la pedirá.

¿Qué impacto tiene el cumplimiento regulatorio de normativas como PSD2 en este mercado?

La implementación de la directiva PSD2 supuso un reto, desde el punto de vista tecnológico para los bancos, y sobre todo en el lado del cliente. La Banca tradicionalmente se había centrado en proteger “el host”, quiero decir, sus servidores, su propia infraestructura, sus Data Center ON-Premise, y ahora, el cliente cobra un especial protagonismo.

¿Qué puntos cree que tendría que mejorar el sector financiero?

La Banca evolucionó de políticas de seguridad centradas en la infraestructura, hacia políticas de seguridad centradas en la protección dato. Pero, sin lugar a dudas, el siguiente reto es entender

¿Quieres saber más?

Puedes ampliar la información de la propuesta de Forcepoint para proteger los entornos financieros en este enlace



que el nuevo perímetro es el propio usuario. Y en banca tenemos muchos y muy variados tipos de usuarios, desde directores de oficina, traders, operadores en un contact center, que realmente trabajan para un tercero, o por supuesto, los clientes.

Por tanto, poder analizar el comportamiento de los usuarios, y poder aplicar políticas de seguridad dinámicas, en base al comportamiento de los usuarios y la criticidad del dato, es la evolución de las políticas de seguridad, que pueden permitir la detección del fraude. ■



MÁS INFORMACIÓN



[Protección de los datos en reposo, en movimiento y en uso en entornos híbridos](#)



[Análisis de comportamiento](#)

¿Cuál es la propuesta de Forcepoint ?

La visión de la ciberseguridad de Forcepoint, tiene dos pilares, la protección del dato, allá donde esté, y el análisis del comportamiento de los usuarios. Y precisamente, datos y usuarios son clave en la protección del sector bancario.

Muchos pueden estar pensando en que, para proteger el dato, tenemos que desplegar soluciones de DLP. Sin embargo, nosotros ya no hablamos de DLP, sino de “Protección Dinámica del Dato” (DDP, Dynamic Data Protección). Es decir, analizamos el comportamiento de los usuarios y en base al riesgo de los mismos, podemos aplicar distintas políticas de seguridad de manera automatizada, y dependiendo del tipo de dato que estemos considerando.

Además, creemos firmemente en que el nuevo perímetro es el propio usuario, somos fieles seguidores de SASE. De tal modo que nuestras soluciones más tradicionales, NGFW, Proxy o Correo, las podemos desplegar tanto ON-PRE-MISE, puras CLOUD o HÍBRIDAS, precisamente, para ayudar a nuestros clientes, y en especial al sector bancario, en su viaje al CLOUD, y su proceso de transformación digital.

¿Necesitas cumplir con el estándar PCI DSS?

Si tu organización transmite, procesa o almacena datos de tarjetas de pago debes cumplir PCI DSS.



Garantiza la protección de datos y la seguridad



Minimiza el fraude y evita cuantiosas sanciones



Transmite confianza y seguridad



Implementa buenas prácticas de seguridad



“Los bancos tienen que luchar, por un lado, para que sus sistemas sean seguros, y por otro para que sus usuarios no caigan en estafas”

JOSÉ DE LA CRUZ, DIRECTOR TÉCNICO, TREND MICRO IBERIA

La seguridad ha sido una de las principales preocupaciones del sector financiero. Sin embargo, tanto los bancos y aseguradoras como sus clientes siguen siendo objetivos prioritarios de los ciberdelincuentes. Dice José de la Cruz, director técnico de Trend Micro, que hasta hace poco eran dos los tipos de ataque más habituales: los dirigidos, que tenían un trabajo previo de adquisición de información e inteligencia sobre el objetivo; y los genéricos, en los que se lanza una campaña de spam y se va infectando en masa. “Ahora no. Ahora lo que se está produciendo es una mezcla de los dos”, dice José de la Cruz.

Explica el directivo que la tendencia es lanzar un ataque genérico con Emoted y una mezcla de TrickBot y cuando se consigue infectar a la víctima se publica la infección en el mercado negro. Cuando aparece algún interesado se le venden los accesos e incluso las herramientas “y utilizando otro ransomware distinto, que es Ryuk, se cifra la información y se reclama el



```
...},c.prototype.  
and('[data-toggle="tab"]'  
removeClass("in"):b.removeClass(  
ia-expanded",...)}var g=d.  
length&&h?g.one("bsTransitionEnd",f)  
onstructor=...conflict=fl  
.data-api",...["tab"],e)  
each(function(...this),e=d  
) {this.opt... {},c.DEF  
"click.bs.affix.data-api",a.  
tion());c.VERSION="3.3  
rollTop(),f=thi
```

pago. Es decir, hay dos o tres actores involucrados en un ataque”, dice José de la Cruz.

Los bancos no sólo tienen que lidiar con la amenaza de los ciberdelincuentes, sino también con miles de usuarios, que a menudo no toman precauciones y además esperan una experiencia impecable. Dice José de la Cruz que los usuarios son muy exigentes y que una entidad financiera no se puede permitir, bajo ningún concepto, un problema de seguridad porque afecta a su línea de flotación, que es la reputación, “sobre todo si eres un banco online”. Pero también hay que tener en cuenta la protección desde dentro del propio banco, y menciona que un banco jamás envía un correo electrónico, un banco jamás le va a pedir al usuario que ponga al descubierto las credenciales, “de forma que hay que aplicar el sentido común. Y son los bancos quienes más tienen que luchar, por un lado, para que sus sistemas sean seguros, y por otro para que sus usuarios no caigan en estafas”.

Sobre las normativas a las que están sujeto el mercado financiero, dice José de la Cruz que su impacto es grande, “aunque solo sea por las sanciones”, pero que algunas, como PCI DSS ya están bastante rodadas y otras, como GDPR, se están empezando a tomar en serio.

Destaca el directivo de Trend Micro como tecnología imprescindible para el mercado financiero la gestión de vulnerabilidades, “algo en lo que siempre insisto pero que creo que es

importante”, sobre todo ahora que ha finalizado el soporte de Windows 7 y otros sistemas operativos más antiguos en los que se siguen detectando vulnerabilidades que los ciberdelincuentes van a explotar.

Respecto a la propuesta de Trend Micro para proteger los entornos financieros, extensible por supuesto al resto de mercados, explica José de la Cruz que este año la compañía está poniendo foco en tres áreas: la nube, los sectores industriales y protección del correo electrónico.

La seguridad de la nube se articula en torno a Cloud One, que incluye tanto la parte de protección tradicional del servidor desde el punto de vista de parcheado virtual, de antimalware, gestión de contenedores, protección de la aplicación e incluso protección en los entornos de almacenamiento de nube pública como Amazon S3, Azure Block o Google Storage.

En la parte de Cloud Security Posture Management “tenemos una solución específicamente diseñada para analizar el cumplimiento normativo”, explica José de la Cruz, añadiendo que se ha integrado toda la parte de IPS dentro de la nube, “porque yo puedo tener una infraestructura IPS y un firewall maravilloso dentro de mi casa, pero cuando me voy a la nube pierdo esa capa y nosotros hemos desarrollado una solución con Tipping Point, nuestro IPS tradicional, que se puede implementar en soluciones Amazon exactamente igual que los aplicamos onpremise”. ■



“Los bancos no sólo tienen que lidiar con la amenaza de los ciberdelincuentes, sino también con miles de usuarios”



MÁS INFORMACIÓN



[Trend Micro Cloud One](#)



[Trend Micro Hybrid Cloud Security](#)

“El sector financiero en general está preocupado por el alto incremento del malware”

JESÚS RODRÍGUEZ, CEO DE REALSEC

Uno de los sectores en los que Realsec tiene mucha presencia es el de la banca. ¿Cómo habéis visto su evolución en los últimos años?

La Banca ha sufrido importantes cambios en estos últimos cinco años. Lo asegura Jesús Rodríguez, CEO de Realsec, una empresa tecnológica europea, con presencia internacional, que desarrolla soluciones de Cifrado y Firma digital para los sectores de Banca, Fintech y Medios de Pago, Gobierno, Defensa y Sector Empresarial. Asegura Jesús Rodríguez que se ha pasado de una Banca tradicional, cuyos usuarios-clientes operaban con sus Bancos de manera presencial a través de las sucursales bancarias, o haciendo uso de sus tarjetas de crédito-debito, tarjetas contacless y de la Banca electrónica; a una Banca en la que se hace uso de nuevos canales, como es la Banca Móvil o los sistemas Wallet.

“En este momento, estamos asistiendo al proceso de transformación digital que ha propiciado la aparición de las Fintechs, que, apoyándose en tecnología digital, ofrecen una amplia variedad de servicios innovadores para el consumidor a un menor coste”, añade El CEO de Realsec, asegurando que muchos bancos aún no están preparados para competir en este escenario.

Dar cumplimiento al nuevo marco normativo europeo es uno de los principales retos a los que se enfrenta la banca, dice Jesús Rodríguez. Este nuevo marco normativo europeo o PSD2, deberá de hacerse efectivo en España, tal y como ha establecido el Banco de España, a finales del presente año, e implica “la obligación de tener que compartir y poner a disposición de los nuevos actores financieros tecnológicos los datos de sus clientes. Lo que se llama “OPEN BANKING”.



Añade el CEO de Realsec que el cumplimiento de la normativa PSD2 tiene, además, un elevado coste para la banca porque “no solamente está obligada a desarrollar las APIS necesarias que permitan poner a disposición de terceros los datos de sus clientes; sino que además está obligada a implantar sistemas de autenticación robusta SCA (Strong Customer Authentication) para evitar el riesgo de suplantación de identidad en su operativa”.

Además, la Banca tiene además otros importantes retos a los que hacer frente, como la transformación digital, la extracción de un mayor valor a sus datos o la lucha contra el fraude y los ciberataques cada día más sofisticados.

Realsec cuenta con varias soluciones para proteger la operativa bancaria y de los Medios de Pago. Explica Jesús Rodríguez que una de las soluciones más vendidas e implantadas es Cryptosec-BANKING, un HSM financiero que incorpora todas las funciones y comandos criptográficos complejos, definidos por las normas ANXI x9 y por el Consorcio PCI (VISA y MASTERCARD) desarrollados mediante algoritmos de cifrado simétrico y asimétrico. “Estos comandos y funciones protegen las transacciones bancarias y proporcionan un entorno seguro en el ámbito de los medios de pago y la operativa bancaria en general”, dice el CEL de Realsec.

Entre las funcionalidades de Cryptosec-BANKING destaca la generación, validación y/o ve-

rificación de los códigos PIN de las Tarjetas de crédito o débito, las funciones para los centros autorizadores de tarjetas, la generación y custodia de claves de cifrado y autenticación, la generación mensajes, la tokenización etc.

Así mismo, Realsec cuenta con soluciones para automatizar los procesos de carga de las claves en los Cajeros y Terminales punto de venta. Sobre lo que hemos alcanzado acuerdos de integración de nuestros HSMs con terceros que tienen aplicaciones para la gestión de tarjetas, soluciones de SCA, Blockchain etc.

“En materia de seguridad podemos decir que el sector financiero en general está preocupado por el alto incremento del malware, cada día más sofisticado y dirigido hacia la banca móvil, así como por el incremento del phishing sobre los dispositivos móviles”, dice Jesús Rodríguez. Añade el directivo que la situación demanda la incorporación de herramientas y soluciones de seguridad más eficientes para la prevención y defensa contra ataques.

Añade que por lo que respecta a tecnología vinculada a Realsec como fabricante, la Banca está demandando, entre otras: soluciones para proteger sus sistemas de pago (especialmente para la Banca Móvil), para la gestión centralizada de claves y certificados, el cifrado de datos y archivos, sistemas de autenticación (SCA), HSMs para tecnología Blockchain etc. ■



“Dar cumplimiento al nuevo marco normativo PSD2 es uno de los principales retos a los que se enfrenta la banca”

MÁS INFORMACIÓN

 [Cryptosec-BANKING](#)

 [Soluciones de seguridad en banca](#)

“PCI DSS es una normativa que ayuda, que transmite confiabilidad”

MIGUEL ÁNGEL ROJO, CEO DE BOTECH FPI

Todas las empresas que procesan, transmiten o almacenan datos de tarjetas de pago deben cumplir con el estándar de seguridad PCI DSS para garantizar la protección de los datos del titular de la tarjeta y evitar el fraude. De esto hablamos con Miguel Ángel Rojo, CEO de BOTECH FPI, quien asegura que en el sector financiero se mueve mucho dinero y por tanto es muy atractivo para los ciberdelincuentes.

Explica Miguel Ángel Rojo que desde hace dos años la compañía se ha asociado con 1st SecureIT, una empresa que durante diez años ha desarrollado toda la parte de consultoría en entornos PCI en Estados Unidos y Latinoamérica, “y nosotros hemos ampliado esa cobertura a toda Europa”. Asegura el directivo que la normativa quiere dar al usuario final un marco de protección, garantizando que sus datos y los de su tarjeta van a viajar cifrados en cualquier tipo de operación.

“El principal reto es entender que es una normativa que ayuda, que transmite confiabi-



lidad”, asegura Miguel Ángel Rojo en relación a PCI DSS. Añade que una vez que entras en la rueda de la certificación PCI la tienes que estar cumplimentando año tras año, y que si bien en Europa hubo un alto grado de concienciación con la normativa en los años 2011-2012, “eso ya ha bajado bastante”. Asegura que donde más concienciación hay ahora mismo es en la región de Asia Pacífico y que en Latinoamérica es donde todavía “cuesta explicar a los negocios qué aporta la normativa, para qué sirve”. Respondiendo a alguna pregunta que le han hecho, dice Miguel Ángel Rojo que “nadie te va a multar por no cumplir con la normativa PCI DSS, pero seguramente es algo que te van a exigir las marcas de las tarjetas con las que trabajas [VISA, Mastercard, American Express...]”.

Explica el directivo de BOTECH FPI que la norma se ajusta a todo tipo de empresas que admitan la tarjeta como medio de pago, desde las que pasan ocho millones de tarjetas al año a las que pasan 87; “la normativa está adaptada a todos los tamaños de transaccionalidad”.

Sobre el proceso de implantación, asegura Miguel Ángel Rojo que “es un tema que tiene que estar liderado por la dirección”. Desde su compañía se ofrecen charlas de concienciación, se explican los beneficios, cuál debe ser el nivel de cumplimiento y se les ayuda en todo el proceso de implantación de PCI DSS. Entre las estrategias de BOTECH FPI está el empujar



La normativa PCI DSS es un estándar de seguridad que tiene como objetivo reducir el fraude relacionado con las tarjetas de crédito e incrementar la seguridad de los datos que intervienen en las transacciones online.

la normativa en el pequeño comercio para que den, hacia sus clientes, “una imagen de seguridad”, que es la que proporciona el sello de PCI Compliance. Entre las acciones que estas pequeñas empresas pueden hacer hay un formulario de autoevaluación que les permite saber cómo hacer frente a la normativa.

“Yo creo que estamos todos muy preocupados por los datos, porque no te llegue un cargo a tu cuenta bancaria, y creo que hace falta un proceso de concienciación. A veces hemos asumido que hacer procesos de calidad aportan mucho, y en este sentido yo creo que PCI aporta mucho a la industria del sector financiero”, concluye Miguel Ángel Rojo. ■



“El proceso de implantación de PCI DSS tiene que estar liderado por la dirección de las empresas”

MÁS INFORMACIÓN

 [BOTECH FPI - PCI DSS](#)

 [¿Necesitas cumplir con el estándar PCI DSS?](#)

“Los criminales saben que atacar al banco es mucho más difícil que atacar al usuario o la cadena de suministro”

LUIS SUÁREZ, PRESALES MANAGER DE KASPERSKY IBERIA

La banca, los servicios financieros, son ahora digitales, móviles y cada vez más centrados en los clientes. Las ciberamenazas en estos entornos se consideran algunas de las más peligrosas, ya que su impacto puede ocasionar pérdidas financieras directas para las víctimas. Dice Luis Suárez, Presales Manager de Kaspersky Iberia, que en estos entornos se está muy concienciado de la seguridad de sus activos; “han estado muy expuestos en sus activos físicos y al hacer el cambio hacia la digitalización de esos activos, esa madurez en la seguridad ha ido pareja”, dice el experto de seguridad.

Sobre los retos de seguridad a los que se enfrentan los servicios financieros, asegura Luis Suárez que la cadena de suministro es un tema que preocupa porque “los criminales son conscientes de que atacar al banco es mucho más difícil”. ¿Por qué soluciones están apostando para paliar este tipo de temas? “Yo hablaría de inteligencia de amenazas, del famoso Threat



Hunting, porque hay que abrazar la idea de que cualquier puede verse comprometido y de que a través de estos informes de inteligencia se pueden entender las técnicas, tácticas y procedimientos de cómo nos pueden atacar”.

No sólo es más fácil de atacar a la cadena de suministro, sino a los usuarios. Durante los últimos años los bancos han puesto un montón de servicios al alcance de los usuarios, colocando al usuario en el centro de todo; al usuario se le permite hacer casi cualquier operación sin tener que pasar por una oficina bancaria, y eso entraña unos riesgos de seguridad”, asegura Luis Suárez.

También hablamos con el Presales Manager de Kaspersky Iberia sobre fraude. Y es que uno de los productos de la compañía es [Kaspersky Fraud Prevention](#), disponible en dos versiones, “uno dedicado a la autenticación continua, que nos permite recoger una serie de telemetrías y eventos en torno a la situación del usuarios y del dispositivo”. Esto permitiría, por ejemplo, que si un usuario hace logging en los servicios de una entidad financiera de forma recurrente y periódica desde Barcelona, “y a los cinco minutos de cerrarse la sesión detecto un inicio de sesión en Corea, puedo tener una evidencia de que quizá esa transacción que se está produciendo tenga más indicios de fraude”, de forma que se puedan automatizar una serie de indicadores que puedan permitir tanto bloquear la transacción como mostrar una alerta al equipo de analistas de fraude. La solución también es

capaz de detectar el fraude cuando se hace uso de apps móviles.

La otra versión del producto está precisamente enfocado a los analistas de fraude, “para que tengan todas las herramientas y todas las métricas para que puedan analizar todos los casos de fraude”.

Explica Luis Suárez que Kaspersky Fraud Prevention “se está desarrollando teniendo muy en cuenta la normativa PSD2, que afecta a todo el mundo, pero especialmente a banca”. Añade que respecto a PSD2 hay algunas claves a destacar: por un lado lo que se busca es aunar la seguridad del usuario, y eso lleva a la inclusión de un segundo factor de autenticación; también se busca que eso no lastre la experiencia del usuario, y también que te otorgue una serie de herramientas para medir cómo estas consiguiendo estos objetivos “y Kaspersky Fraud prevention se está desarrollando con esta y otras muchas normativas en mente para poder cumplir con todas ellas”.

Además de Kaspersky Fraud Prevention, la compañía cuenta con otra serie de soluciones para proteger los entornos financieros. Menciona Luis Suárez otras opciones más orientadas a las amenazas, “tanto los servicios de inteligencia de Kaspersky, como soluciones que nos permitan sacar todo el jugo de esa inteligencia, para poder hacer un Threat Hunting efectivo, poder detectar los indicadores de compromiso y poder tener esa visibilidad, esa detección temprana antes de que se produzca la incidencia”. ■



“Al usuario se le permite hacer casi cualquier operación sin tener que pasar por una oficina bancaria, y eso entraña unos riesgos de seguridad”

MÁS INFORMACIÓN

 [Kaspersky Fraud Prevention](#)

 [Online Banking with Safe Money Technology](#)

“La seguridad tiene que ser conectada y automatizada”

NURIA ANDRÉS, TERRITORY ACCOUNT MANAGER SPAIN&PORTUGAL DE FORCEPOINT

Hace tiempo que Forcepoint apostó por una Human Centric Cybersecurity, y aseguró que las políticas de seguridad estáticas no son suficientes. Y eso mismo nos dice Nuria Andrés, Territory Account Manager Spain&Portugal de Forcepoint, a quien le preguntamos cómo se aplica la propuesta human-centric Cybersecurity de su compañía a los entornos financieros.

Nos cuenta que la estrategia tiene dos pilares: “El primero es la protección del dato, la protección de la información allá donde esté. Y el otro pilar es el análisis del comportamiento de los usuarios, porque existen muchos y muy diferentes tipos de usuarios y lo importante no es distinguir entre usuario externo e internos, sino entre usuarios maliciosos y legítimos”.

Uno de los grandes retos a los que ha tenido que hacer frente el mercado financiero, quizá más que otros por la tremenda regu-



“LA SEGURIDAD TIENE QUE SER CONECTADA Y AUTOMATIZADA” - Nuria Andrés, Territory Account Manager Spain&Portugal de Forcepoint

lación a la que está sujeto, es la adopción del cloud. Recuerda Nuria Andrés que el perímetro ya no existe; “en el sector financiero hemos protegido el perímetro con mucho ahínco. Sin embargo, hemos llevado los datos al cloud y el perímetro se ha diluido”, explica, añadiendo que el nuevo perímetro es la identidad de los usuario, “y dependiendo de esa identidad nosotros en tiempo real podemos provisionar desde el cloud diferentes soluciones de seguridad (firewall-as-a-service, DLP as a Service...)”.

Lo diferencial de Forcepoint, asegura Nuria Andrés, es el análisis del comportamiento de los usuarios mientras se monitorizan las conexiones online, lo que permite “pasar de políticas de seguridad estáticas a políticas de seguridad dinámicas”.

Otro de los retos a los que se enfrenta de manera especial el sector financiero es que debe tratar con diferentes tipos de usuarios. No sólo tiene que articular ciberdefensas en torno a sus empleados, y a la cadena de suministro, sino a miles de clientes que acceden a sus servicios, desde diferentes dispositivos, la mayoría de las veces sin las mínimas precauciones y exigiendo siempre la misma experiencia de usuario. Asegura Nuria Andrés que el cliente es la última barrera de defensa y que es muy importante educar y concienciar a los usuarios. Con Forcepoint

Insider Threat se analiza el comportamiento de los usuarios de forma que se pueda detectar una exfiltración de datos.

“It’s time for Human Centric Cybersecurity”, responde la directiva de Forcepoint al preguntarle por la propuesta de su compañía para proteger el sector financiero. Añade que además de tener en cuenta el factor humano, “la seguridad tiene que ser conectada y automatizada. Hemos invertido mucho en soluciones de seguridad y hemos montado auténticos silos, y es muy importante conectar y automatizar la seguridad; y eso con el amplio portfolio que tenemos en Forcepoint lo podemos hacer”.

Destaca Nuria Andres tres áreas en el portfolio de Forcepoint. Por un lado la parte de Dynamic User Protection, que hace referencia a todo el análisis del comportamiento de los usuarios; Dynamic Data Protection (DDP), que es todo lo relacionado a aplicar todo el análisis del comportamiento de los usuarios a la protección del dato; y la parte de Dynamic Edge Protection, que es la que aglutina las soluciones más tradicionales (proxy, seguridad para el correo electrónico, CASB...). “Tenemos soluciones tanto on premise, cloud, y también híbridas, para ayudar a nuestros clientes precisamente en esa transformación digital y en ese viaje al cloud”, concluye Nuria Andrés. ■



“Lo diferencial de Forcepoint es el análisis del comportamiento de los usuarios mientras se monitorizan las conexiones online”

MÁS INFORMACIÓN

 [Forcepoint Dynamic Data Protection \(DDP\)](#)

 [Forcepoint Converged Security Platform](#)



Incrementemente su ciberseguridad sin aumentar los recursos

Las tecnologías de ciberseguridad, con EDR en el núcleo, han sido aclamadas por el sector y por los clientes, y le permiten detectar y evitar ataques evasivos a gran velocidad, sin que su equipo tenga que realizar ningún esfuerzo adicional.



Kaspersky
Endpoint Security

kaspersky BRING ON
THE FUTURE

kaspersky.es



Dinero móvil: ¿cómo asegurar las aplicaciones bancarias?

Las aplicaciones de banca móvil que ayudan a los usuarios a comprobar los saldos de sus cuentas, transferir dinero o pagar facturas se están convirtiendo rápidamente en productos estándar de las instituciones financieras establecidas. Los bancos están añadiendo servicios y funciones más sofisticadas, permitiendo a los usuarios realizar transacciones más rápidas y eficientes. Y las opciones alternativas de pago online, como la app Venmo de PayPal o Cash de Square, también están ganando popularidad rápidamente. Muchos usuarios aprecian las transacciones rápidas e informales que ofrecen estas aplicaciones.

Pero a medida que estas aplicaciones ganan terreno en el panorama bancario, los ciberdelincuentes no se quedan atrás. Los atacantes pueden utilizar diferentes métodos para

poner en peligro a los usuarios de la banca móvil -desde aplicaciones falsas y de espionaje, hasta ataques a través de conexiones de red maliciosas y el abuso de credenciales de cuentas robadas- y ese no es el final. Los troyanos bancarios se han vuelto más avanzados y sofisticados en 2019. El malware Aunbis, por ejemplo, se ha actualizado continuamente desde que apareció por primera vez en 2018. En 2019, adoptó [sensores basados en movimiento](#) para eludir el análisis de sandbox y las superposiciones para robar información personal identificable. Este agosto también vimos que el [malware bancario Trickbot](#) lanzó una campaña que difundió correos electrónicos de spam con archivos adjuntos maliciosos. Más recientemente, se descubrieron apps falsificadas que impulsaban al [troyano Ginp](#), que roba

la información de acceso del usuario y de la tarjeta de crédito.

Dado que las apps financieras están todas tan estrechamente conectadas o directamente ligadas a las finanzas de un usuario, lo que las convierte en objetivos atractivos para los cibercriminales, la seguridad debería ser una prioridad máxima. A continuación ofrecemos consejos y directrices para asegurar las aplicaciones de banca móvil y añadir capas de defensa para ayudar a evitar las amenazas digitales.

APLICACIONES SEGURAS DE BANCA MÓVIL

- ❖ Descargar desde fuentes confiables y legítimas para minimizar la exposición a apps falsas.
- ❖ Actualizar lo antes posible: la versión más actual de una app tendrá correcciones para las últimas vulnerabilidades conocidas.

JOSÉ BATTAT,
director general
de Trend Micro Iberia



“Dado que las apps financieras están todas tan estrechamente conectadas o directamente ligadas a las finanzas de un usuario, la seguridad debería ser una prioridad máxima”

❖ Habilitar cualquier característica de seguridad incorporada en las apps de banca. Éstas pueden incluir tiempos de inactividad, que requieren que los usuarios vuelvan a iniciar sesión después de cada transacción o transcurrido un período de tiempo.

❖ Eliminar el correo basura y los mensajes con regularidad para reducir las posibilidades de hacer clic en un enlace malicioso, y no abrir ningún archivo adjunto en correos electrónicos no solicitados de remitentes desconocidos.

Establecer conexiones de red seguras

❖ No realizar operaciones bancarias mientras se esté conectado a redes Wi-Fi no seguras en lugares públicos; o bien, utilizar una VPN para cifrar las transacciones.

❖ En un navegador móvil, solo acceder a sitios web bancarios o financieros que utilicen direcciones https y muestren un icono de un candado, indicando que el sitio emplea comunicaciones cifradas.

❖ Cuando se utilicen apps bancarias en un lugar público, utilizarlas a través de 3G, 4G o LTE. Además, hay que desactivar el Wi-Fi y el Bluetooth para evitar el espionaje.

PROTEGER LAS CUENTAS FINANCIERAS ONLINE

★ Habilitar la autenticación de doble factor en todas las apps financieras e instalar apps de autenticación si están disponibles. Los códigos, que se requieren para iniciar la sesión, se suelen enviar por SMS o al autenticador registrado.

★ Deshabilitar la función de autocompletar en las apps financieras o en los inicios de sesión del navegador, y asegurarse de no almacenar las contraseñas en el navegador.

★ No responder a ningún texto o correo electrónico que solicite su PIN, número de cuenta o cualquier número de tarjeta de débito o crédito.

★ Utilizar una contraseña fuerte y única para cada aplicación financiera y asegurarse de cerrar la sesión después de las transacciones.

★ Supervisar las cuentas para poder detectar rápidamente cualquier actividad sospechosa.

HERRAMIENTAS PARA MEJORAR LA SEGURIDAD MÓVIL

Los fabricantes de aplicaciones móviles y las instituciones financieras generalmente res-

ponden a las amenazas y mejoran constantemente sus productos y servicios. Pero, aparte de la aplicación de parches y actualizaciones constantes, hay otras formas de mantener la seguridad de la banca móvil.

Trend Micro Mobile Security for Android e iOS proporciona un completo sistema de seguridad para endpoints de dispositivos móviles, incluida protección frente a las amenazas de seguridad del navegador, la web, los archivos y las apps. La protección Wi-Fi de Trend Micro para Android e iOS proporciona una VPN para hotspots Wi-Fi públicos mediante los servidores de nube seguros de Trend Micro, que cifra la conexión Wi-Fi y evita el secuestro mediante ataques de tipo "man-in-the-middle". Trend Micro HouseCall for Home Networks for Android e iOS (así como Windows y Mac) analiza todos los dispositivos de la red doméstica en busca de fugas de privacidad y otras infecciones de la red, ya que muchos dispositivos de la red doméstica tienen problemas de seguridad que los atacantes pueden utilizar para controlarlos a ellos o a la propia red. ■



Hardware Criptográfico para soluciones PSD2 y Aplicaciones Blockchain en el ámbito financiero

JESÚS RODRÍGUEZ CABRERO,
Fundador / Presidente
y CEO de REALSEC



Hoy nadie duda que la Banca Digital ya no es una opción y que el éxito de su desarrollo exige el cumplimiento, por parte de las entidades financieras, de las normativas de seguridad. Además de aportar múltiples beneficios, en términos de optimización y confianza, a los usuarios finales.

En el nuevo escenario financiero, donde conviven la banca tradicional, las Fintechs y otros modelos de Open Banking, tales como las transacciones efectuadas a través de plataformas como Amazon o Google, entre otras, la seguridad en los medios de pago, además de una necesidad es un requerimiento a cumplir.

Por lo tanto, las entidades financieras deben securizar sus transacciones financieras en línea a los estándares definidos por el consor-

cio PCI (VISA y Mastercard) y para ello, es de obligado cumplimiento la implementación de un hardware criptográfico, cuyo valor y credibilidad reside en que éste cuente con la certificación PCI HSM PTS v2.0 o superior, conforme al PCI Security Standards Council; o en ciertos casos, con la certificación FIPS 140-2 Level 3 por el NIST, según los requerimientos exigibles o recomendados en cada proceso de negocio.

CUMPLIMIENTO NORMATIVA DE PAGO PSD2

La entrada en vigor de la nueva Directiva Europea de Servicios de Pago PSD2, obliga a las entidades financieras a poner a disposición de terceros, actores en el ámbito financiero, los datos de sus clientes y a implantar soluciones de autenticación de doble factor (SCA), o au-

tenticación robusta (identificación y validación de la identidad), para evitar así los problemas de fraude derivados de la suplantación de identidad.

Dichas soluciones de autenticación robusta, utilizan claves que deberían de ser generadas y custodiadas en dispositivos criptográficos (HSMs) para dotar al proceso de autenticación de las máximas garantías de seguridad y confianza.

Muchas entidades financieras que no tienen implantadas soluciones de autenticación robusta, han optado por el envío de un mensaje SMS a sus clientes, con el uso de una clave de autenticación para validar las transacciones realizadas a través de medios digitales. Pero el elevado coste de los SMS por operación, les

“El objetivo de la normativa PSD2 no es otro que proteger, mediante una autenticación reforzada, de doble o triple factor, tanto al cliente como a la propia entidad”

predispone a implantar soluciones tecnológicas de autenticación robusta SCA más eficientes y seguras.

El objetivo de la normativa PSD2 no es otro que proteger, mediante una autenticación reforzada, de doble o triple factor, tanto al cliente como a la propia entidad, frente al riesgo de fraude por robo y suplantación de la identidad.

BLOCKCHAIN EN EL ÁMBITO FINANCIERO.

El auge experimentado por la tecnología Blockchain en el último año está poniendo su foco en diversos sectores, entre otros en el sector financiero, siendo cada vez mayor el número de entidades y organismos vinculados al sector financiero, que ya están trabajando en proyectos, en muchos casos piloto, con tecnología “open source” como es el caso de Corda o Hyperledger.

El dinero utilizado por la tecnología Blockchain son los tokens, objetos similares a las monedas, pero sin valor de curso legal negociable o fungible. Sin embargo, la tecnología de Blockchain va más allá de la propia gestión de activos (criptomonedas), y puede ser utilizada

en otros muchos procesos de negocio no solo en el ámbito financiero.

Tomando como punto de partida un “Smart Contract”, es posible registrar en bloque, de forma distribuida y compartida entre las diferentes partes, cualquier tipo de información o transacción con el consenso y aprobación de sus partícipes.

Dicho consenso, permite la eliminación de intermediarios, proporcionando confianza y solidez a la cadena de bloques, cuya inalterabilidad y robustez la proporciona el cifrado y conjunción de cada uno de los bloques, mediante el uso de una función criptográfica tipo resumen denominada “hash”.

Sin embargo, como ocurre con cualquier algoritmo o función criptográfica, un “hash” o función resumen puede realizarse por software, o bien haciendo uso de una plataforma de hardware criptográfico (HSM) para reforzar la seguridad, y así tener la certeza de que las claves privadas utilizadas en el proceso de la firma digital de las transacciones, no estén expuestas, y se encuentren almacenadas y custodiadas en un dispositivo seguro y aislado.



Si además el HSM cuenta con el nivel de certificación adecuado otorgado por un organismo de confianza, estaremos reforzando la seguridad de procesos y transacciones, garantizando la inalterabilidad de lo cifrado o firmado digitalmente.

Actualmente, existen en el mercado plataformas hardware y software para nodos de Blockchain, los cuales permiten la incorporación de aplicaciones de forma virtualizada, y que para reforzar la seguridad incorporan un HSM que realiza las funciones criptográficas necesarias, permitiendo hacer uso de un “hash” y de otros algoritmos de criptografía asimétrica, eje central de la firma digital, como es el caso del algoritmo de curvas elípticas (ECDSA).

En definitiva, el objetivo perseguido por las entidades financieras, en cuanto a la seguridad de las transacciones que hacen uso de la tecnología de Blockchain, es que la información replicada sea inmutable y que no pueda ser manipulada ni alterada. ■

PCI DSS, el nuevo reto de seguridad en los servicios de pago digitales

MIGUEL ÁNGEL ROJO,
CEO en BOTECH



La sociedad se encuentra inmersa en un proceso de mejora continua en materia de seguridad que no se puede detener ni un solo minuto, ya que el cibercrimen innova a velocidad de vértigo. Si procesas, guardas o transmites datos de tarjetas de pago, para garantizar un exhaustivo control de estos datos, es necesario cumplir con la certificación PCI-DSS. Este estándar de seguridad de referencia en la industria de las tarjetas de pago acredita que el tratamiento de la información confidencial que se maneja se ejecuta con el máximo nivel de protección y seguridad. Este modelo de seguridad, que otorga el PCI SSC (Payment Card Industry Security Standards Council), persigue, y consigue, reducir y evitar el fraude en este ámbito.

El método de pago más extendido entre los consumidores continúa siendo la tarjeta de

crédito y de débito. De hecho, según los últimos datos del Banco de España, las tarjetas de crédito alcanzaron su cifra récord el año pasado y el número de tarjetas de pago en circulación se situó en torno a los 85 millones. Una tendencia alcista que obliga a actualizar constantemente las normativas para regular su uso y velar por la seguridad en los servicios de pago. La normativa 'estrella' cuando se habla de tarjetas de pago es la denominada PCI DSS, una gran conocida por el sector financiero e imprescindible en cualquier negocio que opere con ellas, sin importar su tipo de actividad. Ya que, si una organización procesa, guarda o transmite datos de tarjetas debe cumplir con el estándar PCI DSS, porque si no corre el riesgo de perder su permiso para procesar tarjetas, puede enfrentarse a rigurosas auditorías e

incluso ser sancionada con el pago de cuantiosas multas. Una normativa que permite minimizar el fraude e implementar buenas prácticas de seguridad.

UNA NORMATIVA EXIGENTE QUE TRANSMITE CONFIANZA Y SEGURIDAD

Pero ¿qué es PCI DSS? Es una normativa que busca garantizar la protección de datos y la seguridad en las transacciones económicas. Cumplir con esta regulación es muy importante, no sólo para poder seguir con la actividad de un negocio, sino porque con ella también se transmite confianza y seguridad a los consumidores. La peculiaridad de esta normativa es que consta de seis categorías, 12 requisitos, alrededor de 200 controles y 250 procedimientos de prueba con el fin de garantizar la confidencialidad de

“La peculiaridad de la normativa PCI DSS es que consta de seis categorías, 12 requisitos, alrededor de 200 controles y 250 procedimientos de prueba”

los datos. Sin duda, una normativa muy exigente que necesita una persona responsable dentro de la compañía dedicada a ello.

Además, el principal reto del sector financiero continúa siendo la protección de datos sensibles, tanto de manera interna como externa. Por eso, el estándar PCI-DSS es cada vez más requerido por las empresas, sobre todo por temas relacionadas con el negocio, como son las grandes marcas Visa, Master Card o American Express (Amex).

Los requisitos fundamentales que es necesario cumplir para conseguir la certificación son varios. Por un lado, es necesario construir y mantener una red segura, a través de la instalación y mantenimiento de una configuración firewall para proteger los datos y evitar el uso de contraseñas o valores predeterminados suministrados por los proveedores. Por otro lado, se protegen los datos de los titulares de las tarjetas cifrando la transmisión de datos e información confidencial de los titulares a través de redes públicas abiertas. Además, se

debe establecer un programa de gestión de vulnerabilidades y crear medidas sólidas de control de acceso, limitando el acceso a la información únicamente a las empresas que lo necesiten, asignando una identificación única a cada persona con acceso al sistema y restringiendo el acceso físico a los datos solo a los propietarios de la tarjeta. Y, por último, se deben monitorizar y testar regularmente las redes y mantener una política de seguridad de la información siempre actualizada.

Aunque pueda parecer complicado, se puede cumplir con PCI DSS, no es imposible. Solo es necesario contar con un apoyo experto para lograr su implementación de forma eficiente. Desde BOTECH, compañía española especializada en ci-

¿Te gusta este reportaje?

Compártelo
en redes



berseguridad, junto a nuestro partner 1st Secure IT referente mundial en certificaciones PCI-DSS desde hace más de una década en EEUU y Latinoamérica, impulsamos el cumplimiento de la normativa para ayudar a nuestros clientes, para que puedan garantizar la protección de datos y la seguridad en las transacciones económicas online, minimizar el fraude y al mismo tiempo que evitar cuantiosas sanciones por el incumplimiento de PCI DSS. ■



El sector financiero, uno de los principales objetivos de los ataques dirigidos digitales

El atractivo del dinero convierte al sector de los servicios financieros en el objetivo principal de algunos de los cibercriminales más peligrosos. El hecho de que los sistemas estén interconectados, y que el uso de los dispositivos móviles se encuentre muy extendido tanto para el acceso remoto como para compartir datos convierte a las organizaciones financieras en foco de ataques tanto genéricos como dirigidos.

Además, resulta cada vez más evidente que, debido a los avances en las tecnologías fraudulentas, los cibercriminales están desviando su atención de los clientes «fáciles» y la están centrando en objetivos más difíciles, pero de los que pueden obtener mayores beneficios, como son los proveedores de servicios en sí mismos, es decir, las entidades financieras de todo tipo, tanto grandes bancos como empresas Fintech.

EL SECTOR FINANCIERO, UNO DE LOS MÁS PERJUDICADOS

Si nos fijamos en los datos sobre el coste de estos ataques, y de acuerdo con el último [informe de la consultora Accenture sobre el coste del cibercrimen](#), las entidades financieras aparecen como las más perjudicadas en comparación con el resto de sectores. Según dicho estudio, el coste medio anual del cibercrimen en el mundo financiero creció un 11% desde los 16,6 millones de dólares de 2017 a los 18,4 millones en 2018.

A esto hay que sumar que 2019 ha sido testigo de varios de los desarrollos más significativos en la industria del malware, algunos de los cuales ya anticiparon nuestros especialistas de investigación de Kaspersky. Entre ellos se cuenta el surgimiento de nuevos grupos de cibercriminales y

nuevas geografías en los ataques de grupos de ciberdelincuentes, que se centran en los datos para ayudar a eludir los sistemas antifraude en sus ataques, así como el incremento en el número de datos de comportamiento y biométricos a la venta en el mercado del cibercrimen.

PREVENIR, DETECTAR, RESPONDER Y PREDECIR

La ciberseguridad debe ser un proceso constante, que aborda las amenazas de forma integral. No se trata solo de prevenir los incidentes, sino también de predecir, detectar y responder de forma eficaz, flexible y fiable.

Los productos de seguridad basados en la prevención pueden ofrecer una protección muy eficaz frente a amenazas comunes, como el malware, los ataques de red y la filtración de

ALFONSO RAMÍREZ,
Director General
Kaspersky Iberia



“La ciberseguridad debe ser un proceso constante, que aborda las amenazas de forma integral”

datos. Pero incluso estas tecnologías no bastan por sí mismas para proteger a una empresa de ataques dirigidos o más sofisticados. Las tecnologías de seguridad convencionales basadas en la prevención pueden detectar ciertos incidentes, pero suelen fallar a la hora de determinar si los incidentes aislados forman parte de un ataque mucho más complejo y peligroso que podría estar causando graves daños a su empresa y que seguirá infringiéndolos a largo plazo. Dicho esto, las tecnologías basadas en la prevención a varios niveles siguen siendo un elemento fundamental de este nuevo enfoque proactivo para la protección contra ataques.

Cuanto antes se detecte un ataque, menores serán las pérdidas financieras y el tiempo de interrupción del negocio. De ahí la importancia de una adecuada tecnología de detección. Muchos ataques son complejos y compuestos, por lo que su detección exige un profundo conocimiento sobre cómo funcionan. Se necesitan tecnologías de detección capaces de acceder a los datos de inteligencia de amenazas en tiempo real, capaces de realizar análisis detallados de comportamientos

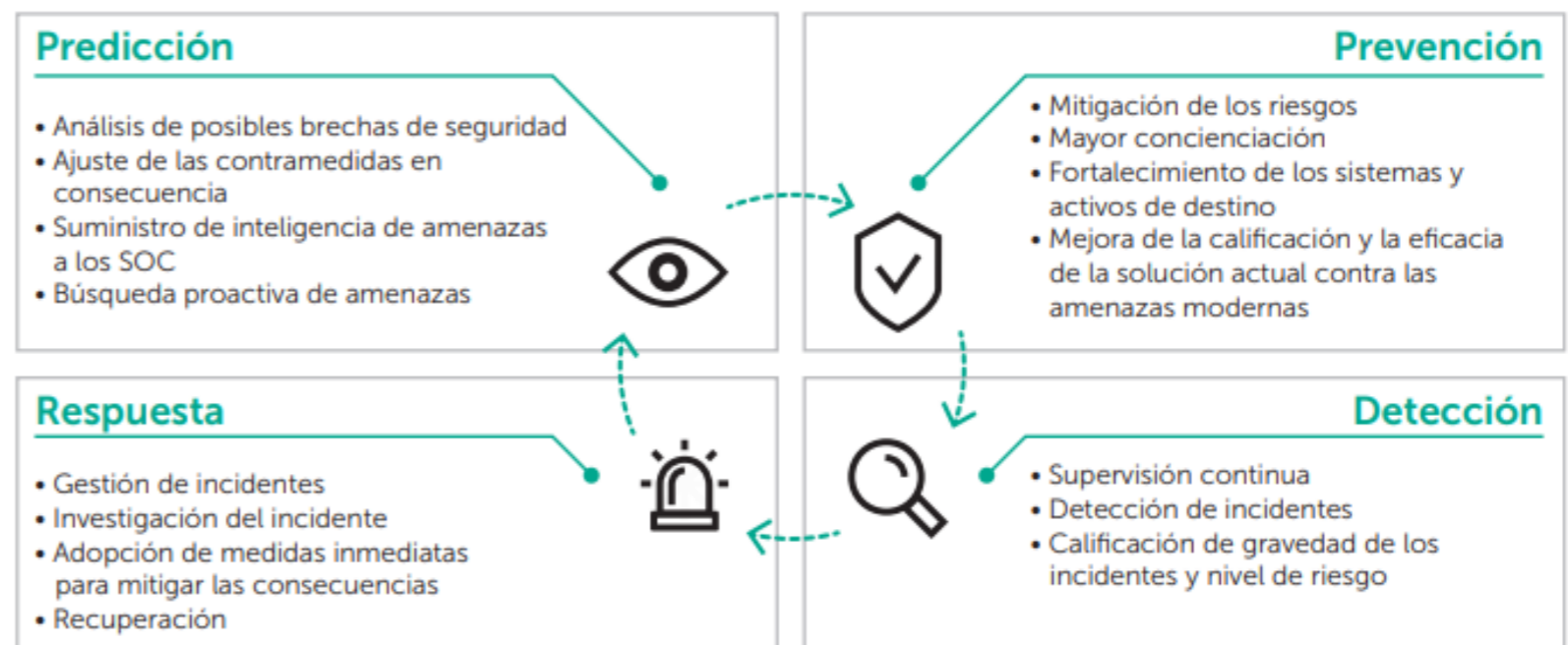
sospechosos que pueden estar ocurriendo en diferentes niveles de la red.

Como es lógico, de poco vale la detección de una amenaza si no estamos en condiciones de responder a ella de manera ágil. Después de detectar un ataque se requieren expertos de seguridad con habilidades y experiencia que ayuden a evaluar y rectificar el daño, que sean capaces de recuperar rápidamente sus operaciones, recibir información inteligente de la acción a llevar a cabo después del proceso de investigación de incidentes, y que además sea capaz de planificar acciones que impidan que el ataque vuelva a repetirse.

Por último, aunque no menos importante, y dado el panorama de amenazas en constante cambio, la predicción es un elemento clave en



toda estrategia de seguridad. Dicha estrategia debe evolucionar constantemente para hacer frente a los nuevos retos. La seguridad no es una “actividad puntual”, es un proceso constante que pasa por la evaluación continua de: las últimas amenazas y la eficacia de las medidas de seguridad para que una empresa pueda adaptarse a los nuevos riesgos y las exigencias cambiantes. ■



La revolución digital del sector financiero

NURIA ANDRÉS,
Territory Account Manager
Spain&Portugal de
Forcepoint



El sector financiero, además de ser uno de los sectores más regulados, desde el punto de vista de la seguridad, por la gran cantidad de normativas a las que está sujeto (GDPR, MiFID II, PSD2,...), está inmerso en la 4ª Revolución Industrial, la Revolución Digital. Y sin lugar a dudas, el gran reto de la transformación digital es también la Ciberseguridad.

Entre los principales retos a los que tiene que hacer frente este sector, encontramos “el viaje” al Cloud, pero también la gran cantidad y los distintos tipos de usuarios a los que hacer frente. Desde Traders, a directores de oficina, pasando por operadores en un call center externalizado o, por supuesto, nosotros, los clientes. Es por esto que, en este tipo de

entornos, es primordial discernir, donde está realmente la amenaza, porque no será solo externa, sino también puede ser interna, el llamado “insider threat”.

Es decir, en este entorno es clave proteger la información, allá donde esté, pero también saber discernir entre usuarios legítimos y usuarios maliciosos. Y precisamente, la visión de la ciberseguridad de Forcepoint tiene estos dos pilares: la protección de los datos, estén en Data Centers onpremise, o en el Cloud (0365, AWS, SFDC,..) y el análisis del comportamiento de los usuarios.

Esto también está totalmente alineado con el “viaje” al CLOUD. El perímetro que hemos conocido, hasta no hace demasiado tiempo,

ya no existe. Precisamente, en el sector financiero este perímetro se ha protegido con mucho ahínco. Hemos desplegado NGFWs de Front-End, de Back-End, hemos apostado por la microsegmentación dentro del Data Center, soluciones de Sandboxing....pero ya lo dice Gartner, “el futuro de la seguridad de Red, está en el Cloud”. Incluso han acuñado un nuevo termino, SASE (Secure Access Service Edge).

Es decir, el nuevo perímetro es el propio usuario, la identidad del usuario. Y en función de la identidad del usuario, se proporcionarán, desde el Cloud, en tiempo-real, políticas de seguridad de red (NGFWaaS, Threat PreventionaaS, ProxyaaS, DLPaaS, ..y tantos otros servicios de seguridad). Se monitorizarán continuamente

“Es hora de evolucionar las estrategias de seguridad centradas en la infraestructura, en aproximaciones centradas en el análisis del comportamiento de los usuarios”

las conexiones, e incluso, en Forcepoint, y esto es lo que nos hace diferentes, en base al comportamiento de los usuarios, en tiempo real, se podrán aplicar distintas políticas de seguridad. Es decir, proponemos migrar de políticas de seguridad estáticas, a políticas de seguridad dinámicas, en base al comportamiento de los usuarios.

Pero también es hora de apostar por la seguridad, conectada y automatizada. Tenemos que dejar de seguir montando silos de soluciones de seguridad, y poder desplegar políticas de seguridad desde el Endpoint al Cloud. Y el amplio portafolio de soluciones de seguridad de Forcepoint, también lo permite. De hecho, nuestras soluciones se pueden aglutinar en tres grandes bloques:



❖ **DUP-Dynamic User Protection (Protección dinámica de los usuarios):** Son soluciones que analizan el comportamiento de los usuarios. Por ejemplo, tenemos soluciones específicas para detectar Insiders Threats, que encajan muy bien en entornos de Trading.

❖ **DDP - Dynamic Data Protection (Protección dinámica del dato):** Aplicamos el análisis del comportamiento de los usuarios, a la protección del dato. Es lo que podríamos llamar Next-Generation DLP. De hecho, Gartner ya no habla de DLP, sino de “Data Lifecycle Protection”, la protección del ciclo de vida del dato.

❖ **DEP - Dynamic Edge Protection:** Aglutina las soluciones, quizás más tradicionales, como son nuestros NGFW, Proxy, Correo (sigue siendo uno de los principales vectores de ataque) o CASB, pero con el “matiz” SASE. Nuestras soluciones pueden ser On-Premise, CLOUD o Híbridas, para permitir precisamente ese viaje al CLOUD, y llevar a cabo la transformación digital que está llevando a cabo todo el sector financiero. ■





Human-Centric Cybersecurity

Los humanos son el nuevo perímetro

Forcepoint protege sus datos y usuarios dondequiera que estén

[Solicite una demo](#)

www.forcepoint.com/es



Protección del usuario



Protección del dato



Protección del edge

Transformación digital, ahora más que nunca





it TRENDS



it Digital MEDIA GROUP

Director General

Juan Ramón Melara

juanramon.melara@itdmgroup.es

Director de Contenidos

Miguel Ángel Gómez

miguelangel.gomez@itdmgroup.es

Directora IT Televisión y Lead Gen

Arancha Asenjo

arancha.asenjo@itdmgroup.es

Directora División Web

Bárbara Madariaga

barbara.madariaga@itdmgroup.es

Directora de IT Digital Security

Rosalía Arroyo

rosalia.arroyo@itdmgroup.es

Director de IT User e IT Reseller

Pablo García

pablo.garcia@itdmgroup.es

Director de Operaciones

Ángel Porras

angel.porras@itdmgroup.es

Redacción y colaboradores

Ricardo Gómez, Alberto Varet, Hilda Gómez, Arantxa Herranz, Reyes Alonso

Eva Herrero

Favorit Comunicación, Alberto Varet

Ania Lewandowska

Diseño revistas digitales

Producción audiovisual

Fotografía

Clara del Rey, 36 1º A · 28002 Madrid · Tel. 91 601 52 92

A marchas forzadas



A muchos les pilló por sorpresa, y a marchas forzadas se han visto obligados a enviar a sus empleados a casa ante las medidas de confinamiento por el COVID-19. Puede que los autónomos, los freelances, sean quienes menos problemas hayan tenido a la hora de seguir trabajando desde sus hogares como venían haciendo, pero quien más o quien menos se ha visto desbordado por la situación.

Son ya muchas las empresas las que contemplan el teletrabajo de sus empleados, pero no todas de una manera continua y más bien lo aplican en caso de necesidad o de forma esporádica. Las grandes organizaciones lo tienen incluido en sus planes de contingencia y serán las que menos problemas hayan sufrido al mover a sus trabajadores a casa, aunque, tal y como nos explicaron varios de los portavoces que participaron en el IT Webinar [Transformación Digital: casos prácticos](#), estos últimos días de marzo ayudaron a clientes a realizar sus despliegues de teletrabajo, porque no tenían la tecnología adecuada, precisamente como reza el título de este editorial: a marchas forzadas.

Los mayores problemas los están teniendo las pymes, los pequeños organismos y ayuntamientos, que faltos de previsión y concienciación de la transformación digital y el teletrabajo, han adoptado las medidas, literalmente, "como han podido". Equipos de empleados obsoletos, sin cámaras para hacer las

videoconferencias que ahora se imponen, faltos de memoria y lentos; servidores que no soportan las conexiones de los empleados; carencia de software y almacenamiento en la nube para seguir operando; y qué decir de la seguridad de las conexiones exteriores que se realizan a esos dispositivos informáticos corporativos desde terminales de los empleados, gran parte de ellos móviles y con aplicaciones de terceros descargadas y no siempre seguras, tal y como se puso de manifiesto en la sesión online [Movilidad e IoT, nueva frontera de la ciberseguridad](#), que también hemos celebrado este trimestre.

La digitalización del puesto de trabajo es una de las caras más visibles de la transformación digital. Ahora más que nunca se ha vuelto imprescindible. Por eso abordaremos las mejores prácticas para llevar a cabo este proceso de trabajo remoto en el webinar [Teletrabajo: productividad, flexibilidad y seguridad a pleno rendimiento](#). ¡No te lo pierdas! Para que nos pongamos a trabajar ya, y que un próximo (ojalá no) estado de alarma no nos haga ir de nuevo a marchas forzadas.

Espero que todos nuestros lectores se encuentren bien.

#JuntosSaldremos #elpresenteesdigitalyvirtual. ■

Arancha Asenjo
Directora de IT Televisión
y Lead Gen Programs

www.ittrends.es

DOCUMENTO EJECUTIVO

IT TRENDS 2020,
el año de la consolidación digital

ELABORADO POR **itRESEARCH**



Descarga este **documento ejecutivo** de **itRESEARCH**

Transformación digital en tiempos de coronavirus: cambia el rumbo de los proyectos

Las organizaciones no han dejado de lado sus planes de transformación digital, aunque su hoja de ruta se está viendo alterada por los efectos de la actual crisis sanitaria. A raíz de esta situación, las tendencias que han guiado la digitalización hasta finales del año pasado han perdido algo de fuerza, mientras que otras están progresando con más rapidez de lo previsto, ayudando a las empresas a capear el temporal.

A finales del año pasado los expertos en tecnología se mostraban bastante optimistas sobre el desarrollo de la transformación digital, ya que durante 2019 se produjeron importantes avances en las principales economías. Tecnologías como los servicios en la nube, la automatización, la inteligencia artificial, las nuevas tecnologías informáticas y de comunicaciones han progresado con rapidez, proporcionando herramientas útiles para las estrategias de digitalización. Esto ha dado alas a muchos proyectos que conducen a nuevos modelos productivos, de trabajo y de negocio que ahora se han topado con la barrera que supone la epidemia global del COVID-19.

La expansión del virus ha paralizado distintos sectores económicos, inicialmente en China y varios países orientales como Corea del Sur. Pero

ahora está sucediendo lo mismo en otras regiones clave para la economía global, como son Europa y Norteamérica, adquiriendo las dimensiones de una pandemia. Como consecuencia, todos los sectores económicos están reduciendo su actividad al mínimo, obligando a las empresas a enviar a los trabajadores a sus casas a la espera de que las restricciones de movimiento puedan relajarse y todo vaya volviendo a la normalidad.

Mientras tanto, y debido a la ralentización del impulso predicho en las tendencias a comienzos de año, las organizaciones están replanteándose su hoja de ruta en cuanto a la transformación digital. Esto no significa necesariamente que la digitalización vaya a frenarse de forma abrupta en 2020, sino que las empresas van a modificar sus estrategias para adaptarse mejor a las condiciones actuales. Debido a ello, se espera que prio-

ricen la implementación de aquellas tecnologías capaces de optimizar sus operaciones en el estado actual, de modo que puedan proporcionarles ventajas operativas a corto y medio plazo, lo que supondría mucho valor de cara al futuro.

Hasta hace escasamente un mes, Occidente todavía veía el coronavirus como una enfermedad más de las que han azotado a los países de Oriente en la última década. Por ello, los expertos basaban sus estudios y predicciones sobre transformación digital en lo que se podría considerar como las "condiciones normales" de la economía. Según esta lista con las cinco principales tendencias de transformación digital, publicada en Forbes por Sanjay Srivastava, miembro del consejo de tecnología de la publicación, lo importante para los clientes es enfocar adecuadamente las inversiones en las tecnologías destinadas a la digitalización del negocio, de modo que no se incurra en gastos excesivos o innecesarios. Esto es especialmente importante ahora, cuando las organizaciones se enfrentan a una escasez de actividad e incluso al cierre. Un panorama que, sin embargo, no implica la devaluación de las siguientes cinco tendencias como las principales en la transformación digital para 2020:

1 LA GOBERNANZA COMO PRINCIPAL PRIORIDAD. Gracias al valor que proporcionan los datos y la automatización, la digitalización proporciona grandes oportuni-



des de mejora para los sectores productivos, los entornos de trabajo, los servicios y la propia vida de las personas. En este sentido, durante los próximos años, Internet of Things jugará un papel clave en la digitalización de los tres sectores económicos tradicionales, abarcando la producción de materias primas, la manufactura y los servicios al consumidor final.

Los dispositivos IoT de última generación proporcionarán gran parte de las nuevas fuentes de datos que impulsarán los procesos digitales en las principales industrias. Al mismo tiempo, la inteligencia artificial será fundamental para manejar todos estos datos, extraer el valor que encierra y aprovecharlos para proporcionar mejores servicios dentro y fuera de la organización.

Pero esto también entraña un riesgo considerable para las organizaciones, que necesitan basarse en información fiable para tomar buenas decisiones de negocio. Y también es vital que esta información sea categorizada, organizada y protegida según su naturaleza particular. Por ello, las organizaciones necesitarán contar con una gobernanza de datos a la altura de las circunstancias, en la que se deberán aplicar unas normas éticas básicas que encajen con la legalidad y con la filosofía de la organización.

Según los expertos, las empresas que aprovechen las herramientas de inteligencia artificial para estas tareas deberán asegurarse de que los casos de uso sean seguros, no encierren

sesgos ocultos y sigan unas reglas éticas sólidas. Esto les permitirá evitar la corrupción de datos o la mala interpretación de los mismos, para lo que aconsejan diseñar las herramientas digitales capaces de buscar resultados tanto positivos como negativos, lo que redundará en una predicción más precisa.

2 LA INTELIGENCIA ARTIFICIAL SERÁ CRÍTICA PARA LA SUPERVIVENCIA DEL NEGOCIO. Al pensar en un ecosistema digital evolucionado es inevitable considerar la inteligencia artificial como uno de sus pilares fundamentales, y las organizaciones están comenzando a darse cuenta de que su negocio no podrá sobrevivir sin esta tecnología. Según las últimas encuestas realizadas por los especialistas de Genpact, hacia el año 2025, las empresas que apliquen la inteligencia artificial para impulsar su negocio lograrán ser 10 veces más eficientes y obtendrán el doble de cuota de mercado que las que no usen la IA.

Esto da una muestra de cómo esta tecnología se ha convertido en estratégica para la transformación hacia los nuevos modelos de negocio digitales, así como para acelerar la innovación y gestionar la propia supervivencia de la empresa en un entorno cada vez más competitivo. Para lograr estos objetivos será preciso acelerar la adopción de la inteligencia artificial, algo para lo que los expertos recomiendan estudiar estrategias basadas en la modularidad, un concepto que



IT TRENDS 2020, EL AÑO DE LA CONSOLIDACIÓN DIGITAL

2020 se presenta como el año de consolidación para muchas de las estrategias de digitalización puestas en marcha por las organizaciones. Esta nueva edición del Informe IT

Trends muestra la realidad digital de la empresa y sus planes de inversión y despliegue tecnológico en 2020. Según esta encuesta, seguridad y cloud serán las principales áreas de inversión en TI durante 2020. La primera es una preocupación que las empresas manifiestan a todos los ámbitos, y que justifica las previsiones de continuo crecimiento para el mercado de la seguridad en los próximos años. La inteligencia artificial se revela, además, como el siguiente paso en la evolución tecnológica. Descubre otros datos en el informe.



consideran esencial de cara al futuro. Se trata de comenzar la adopción de la tecnología a través de aceleradores de IA previamente entrenados que sirven como bases independientes para acometer la transformación digital de las tareas más importantes dentro de cada proceso. Esto permite a las organizaciones desarrollar aplicaciones más rápido, acelerando la capacidad de implementar la IA en la organización.

3 LOS HUMANOS GANARÁN RESPONSABILIDAD EN LA ERA DIGITAL. Muchas voces afirman que la transformación digital, y concretamente el mayor uso de la inteligencia artificial, generará una importante destrucción de empleo y un desplazamiento del papel que tienen

las personas en las organizaciones. Y no se puede negar que las aplicaciones empresariales son mucho más precisas que los humanos en el 80% de las tareas, especialmente en el manejo de datos y en los trabajos administrativos y burocráticos.

Pero, según los expertos, la digitalización y la automatización reforzarán la posición de los humanos dentro de las empresas, quienes se encargarán del 20% restante, que es la parte más importante de las operaciones de negocio, es decir, de la toma de decisiones finales. Esto significa que en el futuro los humanos trabajarán "mano a mano" con las máquinas, aportando cualidades que de momento sólo tienen las personas, como es la empatía, la intuición, la creatividad y la capacidad de emitir juicios de valor, entre otras habilidades avanzadas.

Por ello, es aconsejable que los líderes se replanteen cómo quieren que sea el entorno de trabajo en su organización, potenciando las capacidades de los humanos para trabajar en colaboración con las tecnologías inteligentes, que serán la norma en el futuro. En este sentido, deben apostar por la capacitación de los empleados, un campo en el que las nuevas tecnologías digitales están introduciendo grandes mejoras. Por ejemplo, la realidad virtual y aumentada aplicada a la capacitación, que permite recibir formación teórico-práctica en entornos inmersivos más eficaces que los sistemas tradicionales.

Los responsables de esta investigación recalcan que sólo el 53% de los líderes de las organizaciones está enfocándose en potenciar las capacidades



El progreso de la transformación digital depende directamente de la adopción de las nuevas tecnologías que permitan extraer valor de los datos que genera o recibe la organización

de sus trabajadores de cara al futuro tecnológico de la compañía. Y que el 35% de los trabajadores cree que estos planes formativos están a su alcance. En cualquier caso, las organizaciones que deseen mejorar su capacidad de trabajo con las tecnologías digitales y mantener un ritmo de innovación que les permita seguir siendo competitivas en el futuro, deberán adoptar un enfoque de aprendizaje e innovación constante.

4 TRANSFORMACIÓN ENFOCADA A MEJORAR LA EXPERIENCIA. Para muchas empresas la experiencia del usuario es una parte vital del negocio, especialmente en el sector servicios, donde la fidelidad de los clientes está ligada a su experiencia de uso a todos los niveles. En este sentido, las tecnologías digitales están introduciendo grandes cambios, y no todos provienen de las propias empresas, sino que son los mismos usuarios y consumidores los primeros en demandar una modernización de los servicios y una mayor integración con su estilo de vida y sus hábitos de consumo digital.

Ante esta nueva realidad, se prevé que en el futuro los beneficios en muchas industrias vayan a estar menos relacionados con la reducción de costes y el crecimiento de los precios, y más con una experiencia satisfactoria, tanto para los clientes como para los socios y empleados. Se pueden obtener ejemplos muy ilustrativos de las empresas digitales más exitosas del mundo, como son algunos minoristas destacados, pero esto sólo ofrece una muestra de lo importante que es enfocar la adopción de nuevas tecnologías hacia la experiencia del cliente.

En el futuro, esta forma de entender los negocios será fundamental para la supervivencia, ya que la comercialización de productos y la entrega de servicios a través de canales digitales superará a la forma tradicional de hacer negocios. Y en este camino las organizaciones necesitarán dirigir importantes esfuerzos hacia la mejora de la usabilidad de las tecnologías, tanto en los clientes como en los empleados, para apostar definitivamente por una interacción digital más satisfactoria que les dirija hacia una mejor experiencia del cliente



que se traduzca, más tarde, en beneficios económicos y reputacionales.

5 ADOPCIÓN DE NUEVAS TECNOLOGÍAS COMO SERVICIO. El progreso de la transformación digital depende directamente de la adopción de las nuevas tecnologías que permitan extraer valor de los datos que genera o recibe la organización. Pero esto no se logra de un día para otro, y tampoco sin realizar importantes inversiones en tendencias digitales y las habilidades para trabajar con ellas. Puesto que los algoritmos tardan tiempo en aprender de los datos y proporcionar resultados útiles, las organizaciones necesitan comenzar a usar estas tecnologías lo antes posible.

Por ese motivo, los expertos indican que una buena solución es recurrir a proveedores de tecnología como servicio, que les proporcionan capacidades digitales de nueva generación sin necesidad de que inviertan directamente en ella y acortando los tiempos de entrega. En el caso de la IA y el aprendizaje automático, estos servicios consisten en aceleradores de IA preentrenados para entornos y tareas específicas. Estos pueden ponerse en funcionamiento rápidamente y ofrecer resultados útiles en poco tiempo, a la vez que aprenden para adaptarse cada vez más al entorno específico del cliente.

EL CAMBIO CULTURAL COMO BASE PARA LA TRANSFORMACIÓN DIGITAL

La digitalización no consiste simplemente en adoptar la tecnología en nuevos ámbitos del ne-

gocio, ya que esta evolución no parte de las organizaciones, sino que es la sociedad en su conjunto la que impulsa el cambio. Por ello, son las empresas quienes deben adaptarse para ofrecer lo que demandan los clientes y avanzar hacia el futuro con el signo de los tiempos. Pero esto supone afrontar profundos cambios en la organización, que van mucho más allá de poner en marcha nuevas máquinas y saber usarlas.

Para convertirse en una organización digitalizada y poder competir con las empresas emergentes, muchas de ellas nativas digitales, es preciso acometer una transformación que comienza en la propia cultura de la empresa. El efecto disruptivo que tienen tecnologías como la inteligencia artificial o la automatización robótica de procesos genera una resistencia importante en diferentes niveles de la organización. Desde los directivos a

los trabajadores del nivel más bajo, que muchas veces no son conscientes de la necesidad de realizar esta evolución, ni tampoco son conscientes de sus implicaciones ni de sus beneficios, tanto para la empresa como para ellos.

Esto se manifiesta en una resistencia a la adopción de tecnologías digitales, que en ocasiones es activa y relativamente fácil de combatir, pero que muchas veces se encuentra oculta. Porque en bastantes casos los trabajadores no manifiestan abiertamente sus inquietudes, lo que aclara su desconexión con los objetivos de la empresa en cuanto a la transformación digital. Por ello, los principales expertos recomiendan abordar esta situación comprendiendo que la raíz del problema se encuentra en la cultura de la empresa, algo en lo que intervienen todos los eslabones de la jerarquía corporativa.

Y esto no es un problema que afecte solamente a las compañías que están dando sus primeros pasos hacia la digitalización, sino que la resistencia al cambio se manifiesta muchas veces en etapas posteriores, a medida que los cambios van sucediéndose y los trabajadores se sienten más desconectados de la organización y sus objetivos. La solución es que los líderes impulsen el cambio cultural, fomentando la implicación de los todos los empleados en la nueva visión del negocio y teniendo en cuenta sus necesidades de cara a la transformación digital del espacio de trabajo.

Esto está directamente relacionado con la ten-



Con la irrupción del coronavirus, las organizaciones están replanteándose su hoja de ruta en cuanto a la transformación digital



dencia antes mencionada de mejorar la experiencia del trabajador, y no sólo la del cliente. Según los expertos, el cambio cultural es fundamental para avanzar con éxito en la transformación digital, y esto debe estar encabezado por los líderes digitales de la organización. Estas figuras deben erigirse como catalizadores del cambio hacia una cultura más afín a las tecnologías digitales, lo que facilitará la supresión de las brechas de habilidades que impulsan la resistencia de los trabajadores.

FORMACIÓN E INNOVACIÓN CONSTANTE

La transformación digital y cultural en las organizaciones se asienta sobre varios pilares fundamentales, y dos de ellos son la innovación continua y la gestión del talento digital. Para evolucionar digitalmente las empresas necesitan mantenerse al día en los conocimientos necesarios para manejar las nuevas tecnologías, y también para seguir

mirando hacia el futuro a través de proyectos de innovación. En este sentido, este año serán más las organizaciones que incrementen los recursos destinados a la innovación y a la gestión y refuerzo del talento interno.

Según indican las investigaciones más recientes de consultoras especializadas en transformación digital, como IDC, el uso de tecnologías como la realidad virtual y aumentada o la inteligencia artificial en el campo de la formación y los recursos humanos, va a aumentar a partir de este año. Esto ayudará a las empresas a formar más rápidamente a los trabajadores en nuevas áreas digitales, lo que les permitirá abordar los cambios de la transformación digital con paso más firme.

Al mismo tiempo, son cada día más las empresas que están percibiendo la innovación como un factor fundamental no sólo en lo tocante a la transformación hacia nuevos modelos de negocio digitales, sino también para mantener su com-

petitividad de cara al futuro. Así, se espera que a partir de 2020 se incremente la inversión de las empresas en la innovación continua. Gracias a esto podrán prepararse con antelación para la futura integración de nuevas tecnologías en la organización, reduciendo el impacto y el tiempo de implementación.

NUEVAS OPORTUNIDADES EN MOMENTOS DE CRISIS

En estos tiempos es imposible hablar de tendencias digitales sin tener en cuenta el "factor coronavirus", ya que la pandemia está impactando directamente en los negocios de casi todos los sectores. La demanda de los clientes se está resintiendo mucho y la cadena de suministro se está viendo afectada en toda su extensión, lo que complica las cosas para cualquier plan de las organizaciones. El temor al contagio conduce a una contracción de la economía, y las empresas no

quieren arriesgarse a continuar con sus planes de inversión en tecnología sin saber qué será de su negocio en los próximos meses.

Esto está paralizando en gran medida los planes de digitalización de las empresas, ya que lo importante es sobrevivir a lo peor de la crisis con los recursos suficientes como para afrontar un futuro en el que la demanda podría seguir siendo débil. Pero donde hay crisis también hay oportunidades, y esta situación está beneficiando a varias estrategias de transformación, que están cobrando

mucha importancia para las organizaciones que no pueden contar con toda su plantilla por motivos de seguridad.

❖ **Avance de las herramientas de trabajo remoto:** Como ya han experimentado los primeros países en sufrir la epidemia, especialmente China, las restricciones de movimiento de las personas están obligando a las empresas a implementar rápidamente tecnologías de trabajo remoto. Éste era uno de los objetivos de la transformación digital del espacio de trabajo, pero no necesariamente

te uno de los principales. Ahora, la situación actual está llevando a más organizaciones a adoptar diferentes tecnologías de trabajo remoto, lo que, según los expertos, tendrá un efecto positivo en países como España, donde muchas empresas se han resistido tradicionalmente a implementar esta modalidad de trabajo.

Ahora, muchas de ellas se ven obligadas a mandar a los trabajadores a casa para evitar contagios sin perder capacidades operativas fundamentales. Esto implica recurrir a herramientas habilita-

Las organizaciones buscan ayuda para rediseñar su organización

La transformación digital implica un cambio organizativo, ya que determinadas tareas son asumidas por las máquinas, mientras que los trabajos desempeñados por los humanos se vinculan más a las nuevas tecnologías. En algunos casos los cambios son profundos, pues modifican el rol de los trabajadores y generan un cambio organizativo radical que afecta a numerosos departamentos.

Este año, una vez pasada esta crisis, las organizaciones tratarán de seguir con sus planes de transformación digital, aunque estos hayan sufrido cambios a raíz de situación

actual. Pero no todas tienen los conocimientos o la experiencia necesaria para rediseñar por sí solas la estructura de su organización de cara al futuro de los negocios digitales. Por ello, como informan los expertos de Forrester, las empresas están tratando de asesorarse a través de ejemplos de otras empresas y solicitando la ayuda de profesionales en transformación digital.

Esto les permite tomar decisiones mejor informadas sobre las inversiones que necesitan realizar y sobre el tipo de arquitectura empresarial que deben adoptar para adaptarse a

la era digital. Las principales dudas de muchos negocios giran en torno a cómo orientar el negocio hacia el cliente o cómo pueden seguir el mismo camino que otras empresas de éxito de su sector. Los expertos de Forrester recomiendan consultar varios informes publicados por sus colaboradores para obtener orientación sobre aspectos concretos de la transformación digital o sobre sectores específicos. Por ejemplo: “La anatomía de un modelo operativo”, “El futuro del trabajo en seguros” o “La experiencia de los empleados es crucial para el éxito en la era de la

inteligencia artificial, la automatización y la robótica”.

Este tipo de recursos ofrece orientación valiosa a las empresas que deben cambiar su estructura organizativa a raíz de la digitalización. Aunque, para llevar a cabo un rediseño con éxito se necesita comprender cómo será el negocio en el futuro y planificar sabiamente los cambios que vendrán con la transformación digital. Esto puede ser muy complicado, y lo más recomendable es buscar el asesoramiento de empresas especializadas, preferentemente con experiencia en el sector.

doras del trabajo remoto, ya sean tecnologías de uso más general, como la nube, o herramientas específicas de trabajo colaborativo y comunicaciones unificadas.






Todo ello, previsiblemente, les forzarán a analizar el impacto de estas modalidades de trabajo en su organización, demostrado que en muchos casos es posible otra forma de trabajar: una no presencial. Aunque el alcance de este cambio dependerá directamente del tiempo que duren las medidas de contención del virus, los expertos creen que esta situación contribuirá decisivamente a impulsar un cambio de mentalidad hacia el trabajo remoto y la colaboración.

❖ **La automatización ayuda a afrontar la crisis:** Una parte fundamental de las estrategias de transformación digital es la automatización, que permite a las organizaciones ser más

efectivas en muchos trabajos, liberando a los trabajadores de tareas que las máquinas pueden llevar a cabo a la perfección. Esto abarca muchas de las labores administrativas que se realizan en la mayoría de las empresas y que ahora recaen en soluciones de automatización robótica de procesos.

Pero también muchos trabajos manuales propios de la industria manufacturera, el transporte o la logística, donde las nuevas tecnologías de robótica y los drones están permitiendo nuevos niveles de automatización. A raíz del avance del coronavirus, muchas organizaciones están reforzando su apuesta por estas tecnologías para mantener sus operaciones. Por ello, se espera que, en 2020, sus respectivos mercados sufran menos de lo previsto, aunque, como en otros casos, esto dependerá del progreso de la pandemia. ■

MÁS INFORMACIÓN

-  [10 tendencias de transformación digital para 2020](#)
-  [Las pymes españolas abordan la digitalización a su manera](#)
-  [Factores que ralentizan la transformación digital](#)
-  [De qué manera IA y Big Data están acelerando la transformación empresarial](#)
-  [¿Estás listo para la era post-digital?](#)

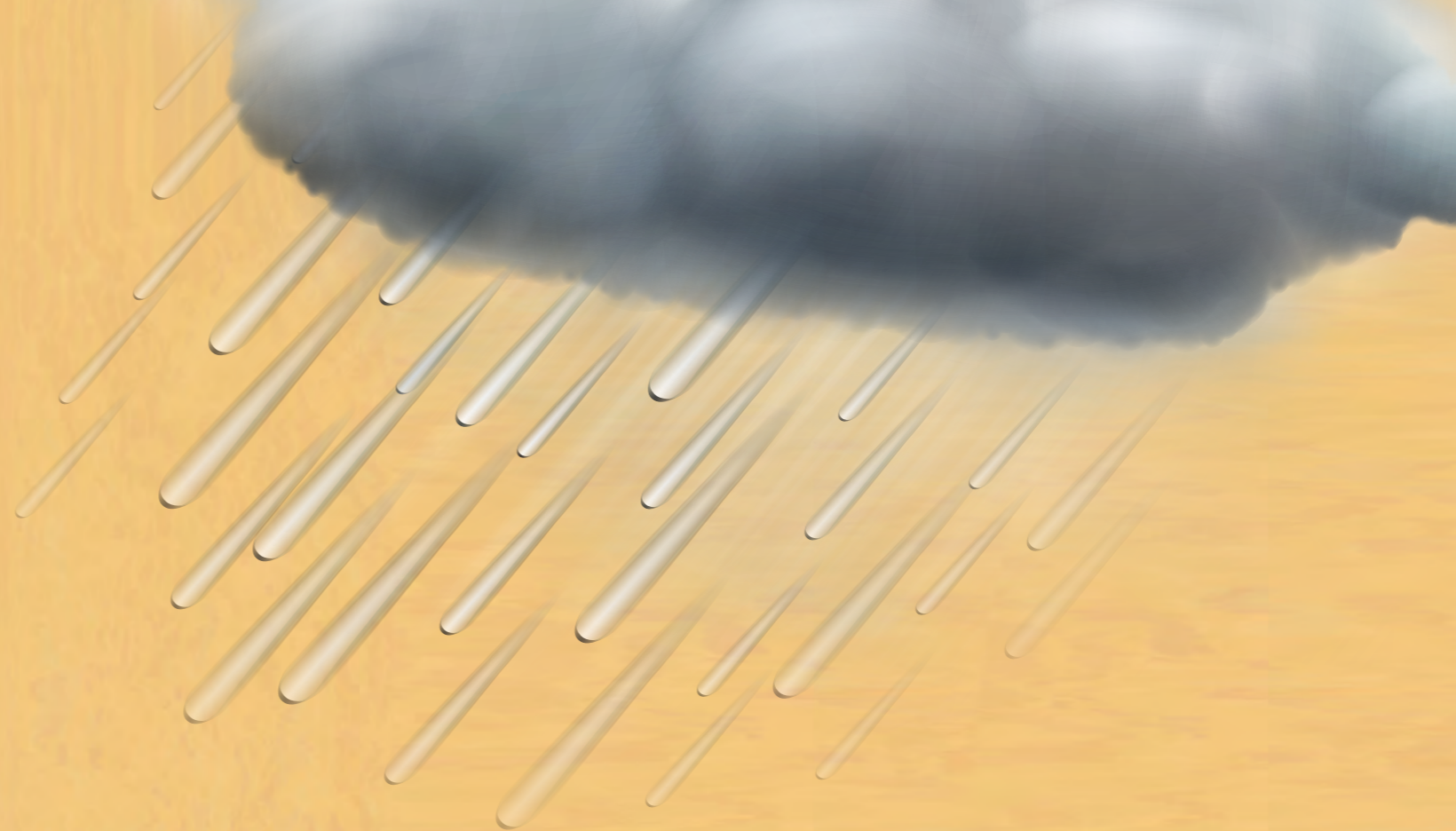


Si te ha gustado este artículo,
compártelo



¿Imaginas a tu empresa protegida por una
compañía que cuenta con las certificaciones
ISO20.000, ISO27.000 y ENS Nivel Alto,
y presta servicios a las mayores empresas
y administraciones públicas del país?

¿Te parece una protección fuera
de tus posibilidades?
¿Crees que es solo para las grandes?



Pregúntanos.
**Te demostramos que tu nivel de seguridad
puede ser tan alto como el de una gran empresa.**

**Siempre la mejor Seguridad.
Para todos.**



Sothis

www.sothis.tech



Transformación digital: casos prácticos

La transformación digital es el proceso que integra las tecnologías digitales en todos los ámbitos del negocio para cubrir las necesidades del mercado y los cambios empresariales. El objetivo es incrementar la efectividad de las operaciones y de las relaciones con el cliente.

Hoy las tecnologías de la información permiten a las empresas lograr esos objetivos: competir, diferenciarse y superarse. E ir de la mano de proveedores tecnológicos que entiendan sus necesidades, que planifiquen, que superen retos mano a mano, hace más fácil el camino y reporta más rápido un retorno de la inversión tangible.

Con el objetivo de abordar desde una visión práctica es transformación digital en las organizaciones y conocer las mejores estrategias para llevarlo a cabo, se

celebró el IT Webinars Transformación Digital: casos prácticos, con la participación de Citrix, Sothis, HPE, Nutanix, Micro Focus, F5, Veeam y Wolters Kluwer. Cada una de las compañías nos aportó su visión de esas tendencias tecnológicas que están potenciando la transformación digital de las organizaciones, así como ejemplos de clientes y casos de uso de la tecnología para conseguir esos objetivos que mencionábamos al principio: competir, diferenciarse y superarse.

En este artículo recogemos un resumen de las intervenciones de estas compañías. Pinchando en la imagen de cada portavoz accederás a su intervención, pero también [puedes ver la sesión completa aquí](#) (y acceder desde la plataforma a cada uno de los capítulos). ¡Consúmelo como quieras, pero no te pierdas nuestro IT Webinars! ■



Iván Rodríguez Santos, Citrix



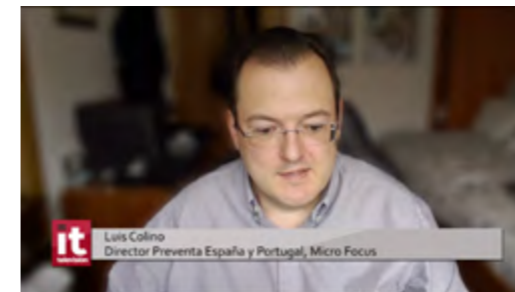
María del Mar Pedroche, Sothis



Galo Montes, HPE



Alejandro Solana, Nutanix



Luis Colino, Micro Focus



Juan Rodríguez, F5 Networks



Víctor Pérez, Veeam Software



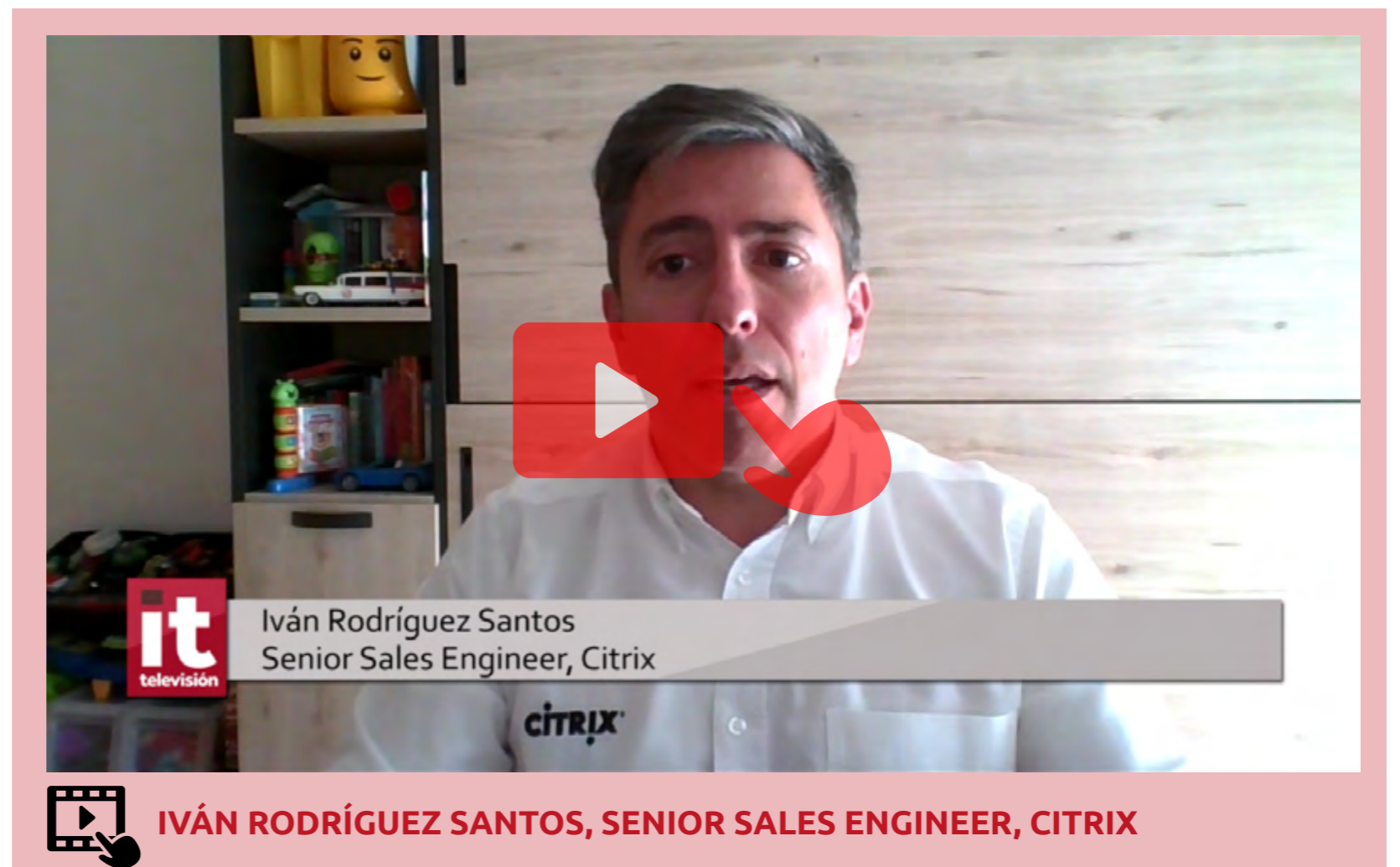
Èlia Urgell, Wolters Kluwer

IVÁN RODRÍGUEZ SANTOS, SENIOR SALES ENGINEER, CITRIX

“El entorno Citrix garantiza un acceso rápido a las aplicaciones”

Las empresas se digitalizan, ¿pero lo hacen correctamente? El ingente número de aplicaciones, la falta de preparación para usarlas y el cambiante contexto entre las mismas implican una pérdida de tiempo fundamental para cualquier negocio. Workspace Intelligence es la apuesta de Citrix para paliar estos tres obstáculos.

Nos encontramos en un tiempo de continuo cambio gracias al impacto de la digitalización en cada área de nuestra sociedad. Sobre todo, en la de negocio, donde la tecnología ha transformado los entornos hasta hacerlos “extremadamente



complejos”, como asegura Iván Rodríguez Santos, Senior Sales Engineer de Citrix, en el webinar [Transformación Digital, casos prácticos](#), para quien las empresas hoy manejan “demasiadas aplicaciones de las que sólo se usa una parte, y en un contexto muy cambiante entre ellas a la hora de buscar un determinado dato, lo que implica una ingente pérdida de tiempo”.

Porque el tiempo es, sin duda, el elemento diferencial en un mundo digital. “Imaginemos que cada usuario trabaja, al cabo del día, con 12 aplicaciones distintas de media, de las que se usa sólo un 1%, y en un contexto que cambia cada 2 minutos. Esto supone consumir tiempo de recursos y del trabajador a la hora de realizar determinadas tareas. Todo ello ocurre porque la mayoría de las aplicaciones que conocemos están desconectadas, lo que no nos permite ser eficientes en el trabajo diario”, argumenta Iván Rodríguez Santos.

La propuesta de Citrix para paliar esta problemática atiende al diseño de una inteligencia en el puesto de trabajo llamada Citrix Workspace Intelligence donde, ante todo, “se garantiza una organización del usuario en su entorno para que todo el mundo tenga acceso rápido a las aplicaciones”. Además, la herramienta “guía al usuario en todo momento para que no tenga que estar buscando qué dato tiene que consumir en una determina-

da tarea, y automatiza el entorno para no tener que cambiar entre aplicaciones”.

UNA EXPERIENCIA MÁS SEGURA

Respecto a la seguridad, Iván Rodríguez Santos subraya la importancia de securizar el entorno de los usuarios. “Pongamos, por ejemplo, que hay un usuario trabajando con Salesforce. Éste se pone a teclear. Nosotros protegemos ese entorno anti-kill over, de modo que no se va a entender lo que se ha tecleado. Y si lo que quiere es capturar una pantalla para tratar de obtener información, no va a poder, porque la pantalla se le queda automáticamente en negro”, explica.

El representante de Citrix asegura que “en este momento están ayudando a sus clientes a desarrollar la continuidad de sus negocios mediante la creación de un único punto de acceso desde el que se entrega al usuario todas esas aplicaciones que necesita para poder trabajar”. “Nosotros podemos dar acceso a cualquier aplicación SaaS, como las que están corriendo en cualquier nube, o podemos conectar con todas esas webs locales de nuestro departamento IT, como puede ser una intranet. Lo que hacemos es proteger esa publicación de la intranet hacia afuera para que nadie la pueda usar a no ser que use Citrix Workspace Intelligence”, sostiene. [Aquí puedes ver la sesión de Citrix.](#) ■



DIRECTRICES PARA MANTENER LA CONTINUIDAD DEL NEGOCIO EN SU ORGANIZACIÓN

Cada organización se enfrenta a la posibilidad de interrupciones mayores o menores de todo tipo, desde eventos planeados como reubicación de oficinas y mantenimiento de TI, a aquellos no planificados que aparecen sin previo aviso. Este



documento presenta un planteamiento completo para mantener a las personas productivas durante interrupciones planificadas o no planificadas, incluyendo las mejores prácticas para una estrategia completa de continuidad del negocio, así como tecnologías para proporcionar acceso seguro a aplicaciones y datos en cualquier dispositivo, sobre cualquier red o nube.

Si te ha gustado este artículo, compártelo



MARÍA DEL MAR PEDROCHE, CONSULTORA DE APLICACIONES MICROSOFT, SOTHIS

“La crisis actual ha supuesto un cambio definitivo en el puesto de trabajo”

El confinamiento en casa por culpa del coronavirus ha disparado el valor del teletrabajo y, así, el de las herramientas para trabajar desde el hogar. María del Mar Pedroche, Consultora de aplicaciones Microsoft de Sothis, destaca en este sentido Microsoft Teams, “un software capaz de aumentar un 20% nuestro tiempo productivo”.

El puesto de trabajo digital precisa de la colaboración para crecer. Más aún en los tiempos de crisis actuales, que han forzado a nuestro lugar de trabajo al cambio de ubicación. ¿Cómo ha impactado esto en la forma de trabajar? ¿Cómo lo ha hecho en las infraestructuras



de las organizaciones? ¿De qué manera hemos reformulado la cooperación laboral para ajustarla a la presente situación? Y yendo más allá: ¿supone este cambio forzoso una inspiración a la hora de abrazar novedosas fórmulas de colaboración en el futuro?

En el webinar [Transformación Digital: casos prácticos](#) participó María del Mar Pedroche, consultora de aplicaciones Microsoft de Sothis, quien no tiene dudas de que la crisis del coronavirus “ha supuesto un cambio en las empresas, tanto a nivel de puesto de trabajo como de infraestructura”, pues se ha hecho forzoso “permitir unas conexiones en remoto a los servicios que ofrece la empresa que antes no existían”. Un panorama que también “ha obligado a la dotación de equipos portátiles y teléfonos móviles para el personal, además de la incorporación de un nuevo software que haga posible la colaboración”. “Los presentes cambios han supuesto para los trabajadores dos cosas: por un lado, se han tenido que adaptar a una nueva situación en su puesto de trabajo; por otro, han tenido que aprender una herramienta nueva”, afirma Pedroche.

HERRAMIENTAS PARA LA COLABORACIÓN

De todas estas nuevas herramientas, la representante de Sothis destaca Microsoft Teams, “un hub de colaboración que incorpora todos los servicios de Office 365, y que nos permite trabajar en equipo mediante su sistema de chats, llamadas

y videoconferencias”. “El sistema crea grupos de trabajo donde es posible la incorporación de aplicaciones de terceros. Este ecosistema de aplicaciones nos va a permitir personalizar esas áreas de trabajo para cubrir las necesidades de los distintos equipos. Además, el hecho de tenerlo todo sobre una misma aplicación nos permitirá ahorrar tiempo y ganar en seguridad, pues el trabajo queda bajo el marco de Office 365, lo que permite a los departamentos de informática gobernar estas aplicaciones”, asegura la entrevistada.

La consultora Forrester afirmó hace meses que Microsoft Teams es capaz de mejorar nuestra productividad, pues, como nos recuerda la responsable de Sothis, “con la herramienta tenemos toda nuestra información integrada en un único escritorio, aumentando un 20% nuestro tiempo productivo”; una bondad disponible en cualquier dispositivo y con la mayor facilidad. “Con un navegador web es suficiente para conectarte, lo que lo convierte en accesible en cualquier momento. Aparte, la herramienta también disminuye el número de reuniones, ya que el escritorio es, en sí mismo, un lugar de trabajo común”, comenta Pedroche al respecto.

Asimismo, Pedroche destaca cómo debe ser ese proceso de digitalización del puesto de trabajo junto a un partner como Sothis, donde las personas juegan un papel importante en el plan de desarrollo. [Puedes ver aquí la intervención de Sothis en el webinar.](#) ■



COMPETITIVIDAD EMPRESARIAL: EL PUESTO DE TRABAJO DIGITAL

La transformación digital ha cambiado los modos de trabajo y producción hasta hacerlos colaborativos y universales, cimentándose la economía digital en el trabajo en equipo, el intercambio y la asociación de ideas y proyectos, y la actividad en la nube. La apertura,

la expansión y la colaboración son los elementos que marcan la competitividad empresarial en la economía digital, y los objetivos de las modernas herramientas digitales creadas específicamente para las empresas. Hoy no se puede hablar de competitividad empresarial sin hablar de alcance, trabajo en equipo, inmediatez, continuidad, colaboración y seguridad.



Si te ha gustado este artículo, compártelo



GALO MONTES, DIRECTOR DE TECNOLOGÍA Y CTO DE IOT, HPE

“Para que cloudless sea una realidad se han de garantizar tres puntos: unas infraestructuras seguras; una conectividad inteligente y que los servicios provean valor”

El mundo digital que estamos construyendo es también un mundo hiperconectado que requiere de plataformas robustas, flexibles y rápidas. ¿Cómo son esos soportes tecnológicos que apoyan hoy a los negocios?

El mundo IT está sufriendo una transformación increíble en los últimos años. En todo ese tiempo, los clientes se han visto obligados a desplazarse por diversos ecosistemas para trabajar de forma simultánea. Todo ello ha generado un enorme problema que Galo Montes, Director de tecnología y CTO de IoT de HPE, resumió así de fácilmente en el webinar [Transformación digital: casos prácticos](#): “Los entornos, al final, no confluyen”. ¿La solución? Dar con una



GALO MONTES, DIRECTOR DE TECNOLOGÍA Y CTO DE IOT, HPE

transformación digital en la que todas las cosas sean mucho más sencillas. Por ejemplo, entendiendo, como hacen en HPE, “que la nube no es un destino, sino una forma de trabajar”.

Montes insiste en que, de no ser así, “habrá problemas a la hora de desarrollar aplicaciones”. “Si desarrollamos una aplicación en función del lugar en el que la vamos a instalar, estamos obligados a tener un conocimiento distinto dependiendo del espacio, lo que hace que el proceso sea extremadamente complejo. Necesitamos, pues, una herramienta que haga que todo sea uniforme. Nosotros llamamos a la nuestra Cloudless. Es un sistema que transformará por completo el enfoque en el que vamos a operar en un futuro próximo. Así, las cargas de trabajo serán trabajadas de la misma manera con independencia de dónde estén. Esto implicará una simplificación brutal para todo el mundo. Tú indicarás a tus desarrolladores dónde van a trabajar, pero, para ellos, el espacio será transparente. Es allí hacia donde nos dirigimos”, explica.

Para llevar todo esto a cabo es necesario confirmar tres puntos: “el primero, la creación de unas infraestructuras seguras; el segundo, tener una conectividad automática, inteligente y resiliente a través de cada nube y dispositivo; y el tercero, y más importante, que todos los servicios provean valor. Algo que se consigue asegurando que los servicios simplifiquen el entorno”.

CASO PRÁCTICO: SUNSUNDEGUI

Entre las soluciones que siguen esa filosofía de HPE se encuentra SimpliVity, sobre la que pivota la transformación digital del fabricante de equipamiento automovilístico Sunsundegui. Miguel Sanz, su responsable tecnológico, intervino en la sesión: “Hace años pensamos en dar el salto a la digitalización, y lo hicimos de la mano de HPE. Su solución hace lo que promete, y lo hace perfectamente. Es supereficaz a la hora de gestionar los anchos de banda, las conexiones remotas, etc. Desde que lo implementamos hemos notado que ciertos aplicativos de gestión o de ingeniería, sólo por alojarlos en este tipo de infraestructura, obtienen un rendimiento mayor”, confesó. Un trabajo conjunto que ha crecido sobre tres claves, como apunta el entrevistado: “Para mí, uno de los temas más importantes es la ciberseguridad. Con la solución de HPE, sé que cada hora de trabajo voy a tener una copia completa de mi infraestructura. Y sé, además, que, si hay algún desastre, recuperaré mi información muy rápida y fiablemente. Otro aspecto interesante es que me permite conectarme con muchas plataformas a la vez, sin importar cuánto crezcan éstas en un futuro. Y el tercer punto es su escalabilidad. Si necesito más recursos, es tan fácil como desplegar otro nodo, y en prácticamente unas horas duplicas las capacidades en un entorno operativo al 100%”. [Puedes ver la intervención de HPE y Sunsundegui en este enlace.](#) ■



GUÍA DE PLANIFICACIÓN DE VIRTUALIZACIÓN DE CLIENTES HPE SIMPLIVITY

El desafío para las organizaciones que han planificado una implementación de virtualización de clientes se encuentra en proporcionar la experiencia de usuario correcta a un coste que sea justificable en función de los beneficios esperados, sin comprometer ningún imperativo. La intención de este informe es brindar orientación sobre la planificación de las implementaciones de virtualización de clientes para lograr ambos objetivos –la mejor experiencia del usuario de su categoría y ROI positivo– con énfasis en las ventajas de la infraestructura hiperconvergente de HPE SimpliVity para dichas implementaciones.

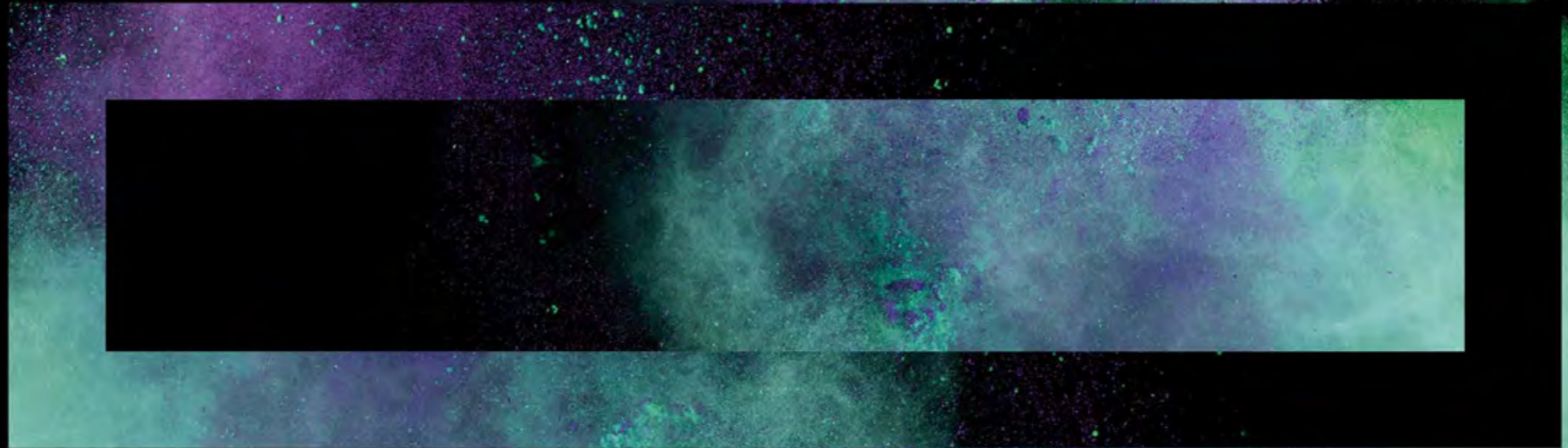


Si te ha gustado este artículo, compártelo





Hewlett Packard
Enterprise



DESCUBRE HPE SIMPLIVITY

Infraestructura hiperconvergente para VDI



Saber más



ALEJANDRO SOLANA, GSI/SO SOLUTION ARCHITECTURE & PRACTICES, NUTANIX

“Hacemos la transición del mundo tradicional al nativo de la nube de forma sencilla, con el foco en las nuevas necesidades de aplicaciones y datos”

La transformación digital de las organizaciones se ha visto enormemente impulsada por el uso de cloud, pero estas arquitecturas tecnológicas también han ido evolucionando a medida que ha ido avanzando la propia digitalización.

La transformación digital ha cambiado el foco de negocio de las organizaciones a las aplicaciones, los servicios y los datos, lo que plantea que las nuevas infraestructuras van a ser más consumidas que gestionadas. Un paradigma que ha llevado a Nutanix a trabajar en una arquitectura “fundamentalmente invisible”, en palabras de Alejandro Solana, GSI/SO Solution Architecture & Practices de la compañía, según explicó en el webinar [Trans-](#)



formación Digital, casos prácticos. El objetivo, “facilitar ese consumo bajo tres claves: que sea fácil de gestionar, que la infraestructura sea inteligente para aprender de los servicios que ejecuta y que sea resiliente para poder adaptarse a situaciones incluso adversas”.

“Todo esto lo ponemos en marcha para que el negocio del cliente pueda trabajar sin necesidad de abordar cambios significativos”, admite Solana. “Con nuestra solución evitas tener que cambiar la aplicación en sí o incluir nuevos procesos operativos. Además, aseguramos que las organizaciones tengan capacidad total de elección a la hora de ejecutar lo que quieran cuando quieran”, asegura el entrevistado.

Con todo ello, Nutanix asegura “una experiencia para las organizaciones sobresaliente”. “Nuestra solución ayuda en la transición del mundo más tradicional al nativo de la nube de forma sencilla, con el foco puesto en las nuevas necesidades de las aplicaciones y de los datos. Todo ello con la garantía de que, en cualquier caso, las empresas deciden cuáles son las piezas que van a componer ese viaje”, afirma Solana.

TRABAJO REMOTO ÁGIL

La pregunta ahora es, ¿cómo puede ayudar Nutanix a los departamentos de IT en una situación crítica como la que atravesamos actualmente? Para el responsable de Nutanix son precisamente este tipo de plataformas las que realmente marcan la diferencia en un momento como el de ahora. “En el contexto del COVID-19, las organizaciones necesitan cambiar las prioridades de negocio y facilitar el acceso al teletrabajo de todos sus empleados. Este tipo de tecnologías, que nos ayudan a componer una infraestructura y cambiarla rápidamente para ajustarse a nuevas prioridades, nos ha permitido, en cuestión de una semana, una organización bastante grande con una capacidad de teletrabajo por encima de los 5.000 usuarios”, declara.

Una arquitectura montada en un tiempo récord de cinco días; una agilidad sustentada en tres puntos, según el entrevistado: “Uno, la facilidad que suponen este tipo de tecnologías a la hora de provisionar el servicio; dos, plantean un modelo escalonado en el tiempo para ir abordando las necesidades de la organización a nivel de número de usuarios; y tres, garantizan una experiencia en el acceso remoto de los servicios de workplace”.

[Puedes ver la intervención en este enlace.](#) ■

Si te ha gustado este artículo,
compártelo



CAPACITAR A LOS USUARIOS FINALES Y OFRECERLES MEJORES EXPERIENCIAS

¿Por qué después de una planificación técnica detallada, una inversión significativa y una selección cuidadosa de los proveedores, casi la mitad de las iniciativas de puesto de trabajo

virtual se enfrentan al muro del rendimiento poco después de pasar a producción, y los usuarios empiezan a reclamar sus viejos entornos de escritorio? ¿De quién es la culpa cuando las cosas no salen tan bien como se esperaba? El problema reside en la naturaleza aislada de la infraestructura del centro de datos.



LUIS COLINO, DIRECTOR PREVENTA ESPAÑA Y PORTUGAL, MICRO FOCUS

“Nuestra herramienta RPA permite hacer validaciones en horas en lugar de días”

A la hora de acometer sus procesos de transformación digital, las empresas parten de entornos heterogéneos. Analizar, automatizar, o predecir son algunas de las capacidades que les permitirán vivir mejor en dichos entornos de TI.

El entorno actual de trabajo es híbrido. Luis Colino, Director Preventa España y Portugal de Micro Focus, comenta en el webinar [Transformación Digital: casos prácticos](#) que esto implica una enorme complejidad para las organizaciones de TI, ya sea desde entornos legacy, proyectos cloud o añadidos como IoT. ¿Cómo gestionar todo esto de la manera más óptima? “Nosotros trabajamos con cuatro puntos. El primero sería el entorno legacy, que no tienen por qué tenerlo todas las empresas. El segundo, la expectativa del cliente, que en nuestro caso son las unidades de negocio, las cuales nos piden una mayor velocidad; el siguiente punto es el mercado, que es superdinámico y enormemente competitivo; y, ya al final, es cuando entra la tecnología, que nos fuerza a meter nuevos componentes que antes no teníamos”.

“Como compañía pura de software, Micro Focus ayuda a las organizaciones a la adopción de nue-



LUIS COLINO, DIRECTOR PREVENTA ESPAÑA Y PORTUGAL, MICRO FOCUS

vas formas de trabajo de la manera más rápida posible con el menor riesgo”, afirma el entrevistado, para quien “transformar no es cambiarlo todo, sino adaptar lo que se necesita a un nuevo entorno para poder ejecutarlo”. “En este diálogo se encuentra un equilibrio fundamental”, recalca.

Un equilibrio que Micro Focus consigue atendiendo a tres grandes aspectos:

1. Tener claro que son una empresa que vende sólo software (a escala global).
2. Una plataforma potente para competir en el mercado.
3. Una focalización en una serie de áreas para la transformación digital.

Profundizando en el tercer punto, Colino apunta, asimismo, cuatro sectores de innovación fundamentales:

1. **Velocidad:** “Las organizaciones necesitan acelerar la puesta en marcha de nuevos productos y servicios para ser competitivos. Ahí nosotros hemos apostado por Enterprise DevOps. Creemos que nuestras soluciones aportan un gran valor a las empresas”.

2. **Agilidad:** “No sólo se trata de acelerar en la creación, sino también en la disposición para el cliente final. Ahí es donde nuestras soluciones de gestión de la IT híbrida permiten a las organizaciones poner fácilmente en marcha esos nuevos productos”.

3. **Seguridad:** “Fundamental en cada paso. Hay que ser más ágil y veloz, pero siempre de

una manera segura. Desde el código fuente a la gestión del día a día”.

4. **Predictive Analytics:** “Gracias a Machine Learning estamos embebiendo predicción analítica en cada solución. Tanto en la gestión IT como en DevOps”.

ACELERACIÓN DE PROCESOS

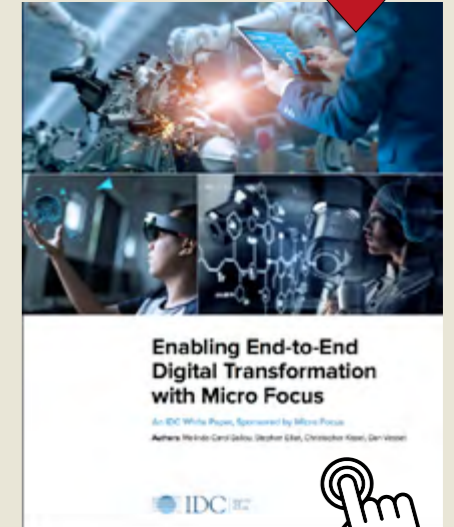
¿Y de qué manera pueden los clientes beneficiarse de estas bondades? “Pues hay buenos ejemplos en la automatización de procesos. Un cliente en concreto, que desplegaba entornos cloud para sus clientes, tardaba en desarrollar el proceso entre uno y dos meses. Bien, ahora les lleva ocho horas. ¿Cómo puede ser esto? Básicamente gracias a dos estrategias. Por un lado, ha habido una automatización de despliegues mediante nuestras soluciones, y por otro, todo el proceso manual que requieren las aplicaciones ha sido automatizado igualmente con nuestra herramienta RPA, que permite hacer validaciones en horas en lugar de días”, concluye Colino, cuya [intervención puedes ver en este enlace](#). ■

Si te ha gustado este artículo,
compártelo



CÓMO HABILITAR LA TRANSFORMACIÓN DIGITAL DE EXTREMO A EXTREMO

La transformación digital (DX) es esencial para las empresas que desean seguir siendo relevantes en un panorama competitivo y en constante evolución. Sin embargo, la complejidad, velocidad, coste y dinamismo de la innovación puede ser



abrumadora. En este libro blanco, IDC recomienda que las empresas evalúen y adopten un enfoque estratégico y metódico que coordine cuatro pilares clave de DX: Enterprise DevOps; Gestión de TI híbrida; Seguridad, riesgo y gobernanza; y análisis predictivo.

JUAN RODRÍGUEZ, DIRECTOR GENERAL, F5 NETWORKS

“En el mercado digital triunfará quien aborde el cambio en tres fases: digitalización, transformación y desarrollo de aplicaciones”

Las aplicaciones constituyen la parte más visible de las organizaciones, puesto que las utilizan empleados y clientes.
¿Cómo está evolucionando este mundo y cuáles son sus principales tendencias?

Este panorama ha encontrado nuevos estímulos en la situación de confinamiento actual. “Hemos advertido un boom tremendo en las compras online. El alza de las empresas de e-commerce es tremenda, lo que repercute en la seguridad, que debe ser mayor”, afirma Juan Rodríguez, director general de F5 Networks, en el webinar [Transformación Digital: casos prácticos](#). “Por eso, para nosotros, las empresas que van a triunfar en el mercado digital son aquellas que aborden el cambio en tres fases: digitalización, transformación y desarrollo de aplicaciones”, añade.

Un buen ejemplo lo encontramos en mundo del desarrollo de la aplicación nativa, tipo Amazon o Netflix, que tiene mucho más control sobre el usuario, ya sean sus privilegios o sus usos de consumo. “Ese universo está experimentando una gran evolución, hasta el punto de desarrollar



JUAN RODRÍGUEZ, DIRECTOR GENERAL DE F5 NETWORKS

varias versiones de sus aplicaciones por día. Anteriormente no era así. Entonces, en entornos legacy, los clientes desarrollaban una o dos versiones en un año. Hoy tenemos clientes que sacan hasta 15 y 20 aplicaciones diarias, lo que implica un control brutal sobre la producción”, asegura el director de F5.

Se trata de un cambio de paradigma notable, ya que la aplicación cada vez se desarrolla más cerca del usuario, justo en el extremo, lo que le otorga al cliente un mayor control sobre la misma. Y es que las aplicaciones “hoy se consumen en cualquier sitio, ya sea en modo on-premise o en la nube privada, en entornos de nube pública o mediante aplicaciones tipo SaaS”.

Además, la crisis provocada por el COVID-19, ha generado una enorme demanda de teletrabajo. Un contexto complejo que nos obliga a realizar varias acciones, como elegir una nube, el tipo de herramientas que voy a utilizar, el modo de servicios y la gestión en la seguridad de estos. Por eso es tan importante la seguridad en los entornos cloud. “El usuario no tiene que notar ninguna diferencia a nivel de servicio, incluso en entornos multinube. Durante esta crisis, muchos clientes se encuentran con verdaderos problemas cuando quieren regresar a su CPD. Ahí es donde nosotros les damos mecanismos a los usuarios para poder tener la misma experiencia a nivel de usuario tanto en modo on-premise como en cualquier entorno de nube pública”, afirma Juan Rodríguez.

CASO PRÁCTICO: SHAWBROOK BANK

Durante la sesión, Rodríguez expuso el caso de Shawbrook Bank, una entidad británica especializada en pymes y banca personal, con una gran carga de infraestructura legacy. Bajo la presión del crecimiento, había desarrollado sus servicios en torno a procesos manuales no automatizados, y ahora con la transformación digital, quería agilizar estos desarrollos. El plan fue simplificar las operaciones, aprovechar los beneficios de la computación en la nube, mejorar su estrategia de seguridad y llevar sus capacidades de servicio al cliente al siguiente nivel. Todo ello se logró con la implementación de múltiples ADC F5® BIG-IP® con multi-procesamiento en clúster virtual (VCMP) para proporcionar una separación virtual de servicios mientras se mantiene la capacidad de acceder a la aceleración de alto rendimiento SSL. El resultado: las aplicaciones están siempre disponibles en cualquier dispositivo y sin comprometer la seguridad; y se han mejorado la seguridad y resistencia mitigando amenazas clave de ciberseguridad. [Aquí puedes visualizar la intervención de F5 en el webinar.](#) ■

Si te ha gustado este artículo,
compártelo



INFORME SOBRE EL ESTADO DE LOS SERVICIOS DE APLICACIÓN EN 2020

La sexta edición del informe State of Application Services (SOAS) de F5 muestra cómo la floreciente economía de las aplicaciones está resultando clave a la hora de impulsar

los procesos de transformación digital de las organizaciones de la zona EMEA. De esta forma, un 91% de los encuestados en EMEA afirma que en estos momentos sus organizaciones ya están ejecutando planes concretos de transformación digital. Un porcentaje superior al registrado en Estados Unidos (84%) y en la zona APCJ (82%). Lee todos los datos en el informe.



VÍCTOR PÉREZ DE MINGO, SENIOR SYSTEMS ENGINEER, VEEAM SOFTWARE

“En el proceso de digitalización es fundamental desbloquear todo el potencial del dato”

Los datos se están multiplicando como producto de la transformación de las organizaciones. Estos necesitan ser protegidos desde cualquier punto. ¿Cuál es la mejor estrategia a seguir para securizar la información en la era digital?

● ¿Qué cuestiones está generando el mundo de los datos y qué respuestas tienen las empresas a ellas? Víctor Pérez de Mingo, Senior Systems Engineer de Veeam Software, lo ve todo como un camino que nos ha llevado a un nuevo escenario, y así lo describe en el webinar [Transformación Digital: casos prácticos](#). “Nosotros lo llamamos Cloud Data Management, algo así como la culminación del proceso de digitalización del que llevamos

**VÍCTOR PÉREZ DE MINGO, SENIOR SYSTEMS ENGINEER, VEEAM SOFTWARE**

años hablando. Un paradigma cambiante: antes estábamos todos pendientes de los requerimientos necesarios a nivel hardware para hacer funcionar las cosas, luego pasamos a un escenario donde lo que importaban eran los niveles de servicio y ahora, por fin, somos conscientes de que lo verdaderamente importante es el dato”, afirma.

Porque es el dato lo que hace que las empresas puedan sacar beneficio real de la transformación digital. Una asunción de la que surgen una serie de retos a tener en cuenta que, desde Veeam, distribuyen en cinco escenarios: backup y recuperación de datos, movilidad del dato, monitorización del dato, orquestación del dato y el cumplimiento de los requisitos legales. “Nuestro control de estos puntos nos coloca como los aliados perfectos en la gestión del Cloud Data Management, de modo que conseguimos unos niveles sin precedentes de disponibilidad del dato”, sostiene el entrevistado.

Un desarrollo que precisa, por encima de cualquier otra cosa, de una automatización. Bien lo explica el representante de Veeam: “Es necesario que todas las tareas se puedan realizar de una manera automática. También que podamos lanzar las recuperaciones y las segundas copias cuando las necesitemos. O que, llegado el caso, podamos respetar GDPR mediante una eliminación de algún dato de forma automática. En definitiva, se trata de desblo-

quear toda la potencia del poder del dato de los clientes, para lo que se precisa de una disponibilidad altísima de la información, con una agilidad muy grande para moverlos. Todo ello redundará en la aceleración del negocio de las compañías”.

CASO PRÁCTICO: INCHCAPE

Durante la sesión online, Pérez de Mingo explicó el caso de uno de los clientes de la compañía, Inchcape Australia, entre los mayores retailers de automoción del mundo, con presencia en 30 países. La firma buscaba una solución para la gestión de sus datos en una infraestructura que soporta más de 200 aplicaciones. Carecían de sistemas de recuperación ante desastres y el backup en cinta fallaba constantemente, por lo que cualquier caída podía significarles pérdidas de millones de dólares. Los responsables buscaban un software para automatizar los procesos de recuperación y reducir costes en caso de fallo, y optaron por Veeam Availability Orchestrator, que les proporcionó un backup 100% automatizado para todos los flujos de trabajo, aumentando así la confianza en la capacidad de la compañía para salvaguardar los datos del negocio y de sus clientes. Asimismo, les ahorró 166.000 dólares en sistemas de almacenamiento al año. [Puedes ver aquí la intervención de Veeam en el webinar.](#) ■



MEJORAR EL ROI DE LA TI MEDIANTE LA PROTECCIÓN DE DATOS MODERNA

A medida que aumenta el volumen de datos que recopilan las organizaciones, crecen también los problemas para acceder a la información correcta, de una forma oportuna, y a la vez protegerla y preservarla. Los requi-



sitos de disponibilidad en todas las organizaciones digitales han ralentizado los sistemas de backup y recuperación tradicionales, convirtiéndolos en un lastre para la agilidad del negocio. Este documento reflexiona sobre cómo puede la protección de datos convertirse en un centro de creación de valor para el negocio.

Si te ha gustado este artículo, compártelo



ÈLIA URGELL, ACCOUNTING & TAX PRODUCT MANAGER, WOLTERS KLUWER TAX & ACCOUNTING

“Cloud da acceso desde cualquier lugar a las aplicaciones que necesita un despacho, con actualizaciones totalmente transparentes y una securización de los datos”

Todos los sectores de la sociedad están llamados a la transformación digital, y una pieza clave en ese viaje la constituyen las aplicaciones. Los despachos profesionales y empresas han confiado en el software para la gestión de su día a día y éste debe dar la respuesta que necesitan en el entorno actual digital.

Si hay un espacio que, en estos momentos, esté sufriendo una transformación meridiana, ése es el despacho profesional. ¿Cuáles son los principales pilares de este cambio? Èlia Urgell, Accounting & Tax Product Manager en Wolters Kluwer Tax & Accounting, señaló cuatro durante el webi-



“Necesitas un modelo flexible en esa nueva relación que se establece entre el cliente y el despacho; una capacidad que proporciona el software en cloud”

nar [Transformación Digital: casos prácticos](#), todos ellos contenidos en a3innuva, la solución de su compañía para facilitar la transformación empresarial en la que estamos hoy inmersos.

Los cuatro pilares en los que se sustenta esta suite son los siguientes:

❖ **Innovación:** “Hemos logrado reenfoque los servicios contables del despacho para acercar el servicio al cliente”.

❖ **Cloud:** “Permite el acceso desde cualquier lugar, con actualizaciones totalmente transparentes y una securización importante de los datos”.

❖ **Colaboración:** “Mediante la colaboración nos aproximamos al mercado. De hecho, a3innuva es el paradigma máximo de este modelo, pues tanto clientes como organización o entidades bancarias comparten un único espacio”.

❖ **Eficiencia:** “La plataforma permite la entrada de datos de facturación vía Excel y garantiza una autonomía total para que el cliente conozca el estado de su negocio”.

a3innuva “permite que el despacho se acerque al cliente y le pueda ofrecer servicios de valor añadido. A la vez, la herramienta facilita la búsqueda de nuevas oportunidades de negocio. También hace posible el acceso directo del cliente al despacho en cualquier momento, así como la captación de clientes nativos digitales, es decir, nuevo talento”, asegura Urgell. “Al final, se trata de utilizar las nuevas tecnologías para crecer. Para ello, necesitas un modelo flexible en esa nueva relación que se establece entre el cliente y el despacho. El resultado final es la obtención de la máxima rentabilidad, tanto en el negocio del despacho como de la empresa”, añade. [Conoce todas las capacidades de a3innuva viendo la intervención de Wolters Kluwer en el webinar.](#) ■

Si te ha gustado este artículo,
compártelo



¡Gracias, Asesores!

Por ser siempre apoyo incondicional para Pymes y Autónomos, el 99,8% de las empresas del país



Nuestro aplauso es también para vosotros
#AplausoAsesores



Movilidad e IoT, la nueva frontera de la ciberseguridad



Mucho se ha hablado de la pérdida de perímetro. La llegada de los dispositivos móviles, el cloud y más recientemente el IoT ha marcado la disolución definitiva entre las redes corporativas privadas y el Internet público. Junto con un aumento de las amenazas y la falta de recursos, los responsables de la seguridad empresarial tienen que hacer frente al BYOD, a que los empleados utilicen sus propios dispositivos móviles para trabajar, aunque a menudo eso signifique que se conectan a los recursos empresariales desde WiFi públicas y redes móviles.

Según datos de Strategy Analytics, este 2020 el 42% de la fuerza laboral mundial será móvil. El robo o pérdida del dispositivo es sólo una de las amenazas de seguridad que genera el uso de estos dispositivos móviles en las empresas. Apps de entretenimiento, muchas de las cuales requieren más permisos de los necesarios, conviven alegremente con las que permite acceder a los recursos empresariales. ¿Estás preparado para hacer frente a esta problemática?

Y junto con los dispositivos móviles, los conectados, esos miles de aparatos que a veces ni siquiera sabemos

que existen, capaces de acceder a datos, de paralizar una empresa en un ataque conjunto y de servir como puerta de entrada a las amenazas más diversas. En este IT Webinars hemos reunido un grupo de expertos para hablar de la seguridad de la movilidad y el IoT. Contamos con Sophos, VMware, Sarenet y Samsung Knox. A continuación, puedes leer un resumen de sus intervenciones, con los puntos más destacados. También puedes pinchar en cada una de las imágenes de sus portavoces para acceder a su intervención en el webinar o ver la [sesión completa aquí](#). ■



Óscar López, Sophos



Eugenio Gil, VMware



Aitor Lejarzegi, Sarenet



Isabel López, Samsung Knox

ÓSCAR LÓPEZ SÁNCHEZ-MATEOS, SALES ENGINEER IBERIA, SOPHOS

“Una de cada diez amenazas se detecta en los dispositivos móviles”

“A veces se nos olvida que los dispositivos móviles son como los portátiles, que desde ellos podemos hacer cualquier cosa”, dice Óscar López Sánchez-Mateos, Sales Engineer Iberia, Sophos, durante la sesión online [Movilidad e IoT, la nueva frontera de la ciberseguridad](#). Dice también Óscar López que una de cada diez amenazas se detecta en los dispositivos móviles, y que algunos de los ataques típicos son los man-in-the-middle, “porque se nos olvida que las wifis gratuitas no son la mejor idea para conectarnos al banco”, o a través de los código QR, “que te pueden llevar donde no deberías ir”.

Apunta el experto de seguridad de Sophos que la privacidad es importante también en los dispositivos móviles, y por eso hay que tener cuidado con los permisos que se conceden a las aplicaciones que descargamos. Y es que cualquier amenaza puede saltar a la red empresarial.



Sophos Intercept X Mobile aborda la parte de defensa contra amenazas, mientras que la parte de UEM se trabaja con Sophos Central Mobile, una plataforma que nos va a permitir gestionar todo desde una única consola

A la hora de hacer frente a la seguridad de la movilidad se habla de dos conceptos: UEM (Unified Endpoint Protection) y MTD (Mobile Threat Defense). El primero es la parte de la administración de los móviles que permite, entre otras cosas, eliminar permisos que impidan que el usuario se instale programas o añada cuentas de Google, mientras que la parte de MTD es la que se centra más en la seguridad, es la que permite protegernos contra los ataques man-in-the-middle que se mencionan al principio. “Necesitamos ambas cosas para securizar el dispositivo móvil, que puede ser un Android, un iPad, un Windows 10...”, dice Óscar López.

Sophos Intercept X Mobile aborda la parte de Mobile Threat Defense, mientras que la parte de UEM se trabaja con Sophos Central Mobile, “una plataforma que nos va a permitir gestionar todo desde una única consola”.

Explica también el ingeniero de ventas de Sophos que la suma de ambas soluciones “permite conseguir la seguridad que estamos persiguiendo” y que las empresas están tomando conciencia de la seguridad de la movilidad porque el número de ataques y amenazas no deja de crecer. Asegura también Óscar López que las empresas se están empezando a dar cuenta de que tener productos de seguridad implica un coste, “pero es un coste mucho menor que el recuperarse de un ataque de este tipo”.

[Vea aquí la intervención de Sophos en Movilidad e IoT, la última frontera de la ciberseguridad.](#) ■

Si te ha gustado este artículo,
compártelo



SOPHOS INTERCEPT X FOR MOBILE

Intercept X para dispositivos móviles protege a los usuarios, sus dispositivos y los datos corporativos de amenazas móviles conocidas y desconocidas al aprovechar el motor de Intercept X basado en Deep Learning. Todo se gestiona sin proble-

mas a través de Sophos Central, junto con toda la cartera de soluciones de ciberseguridad de próxima generación de la compañía.

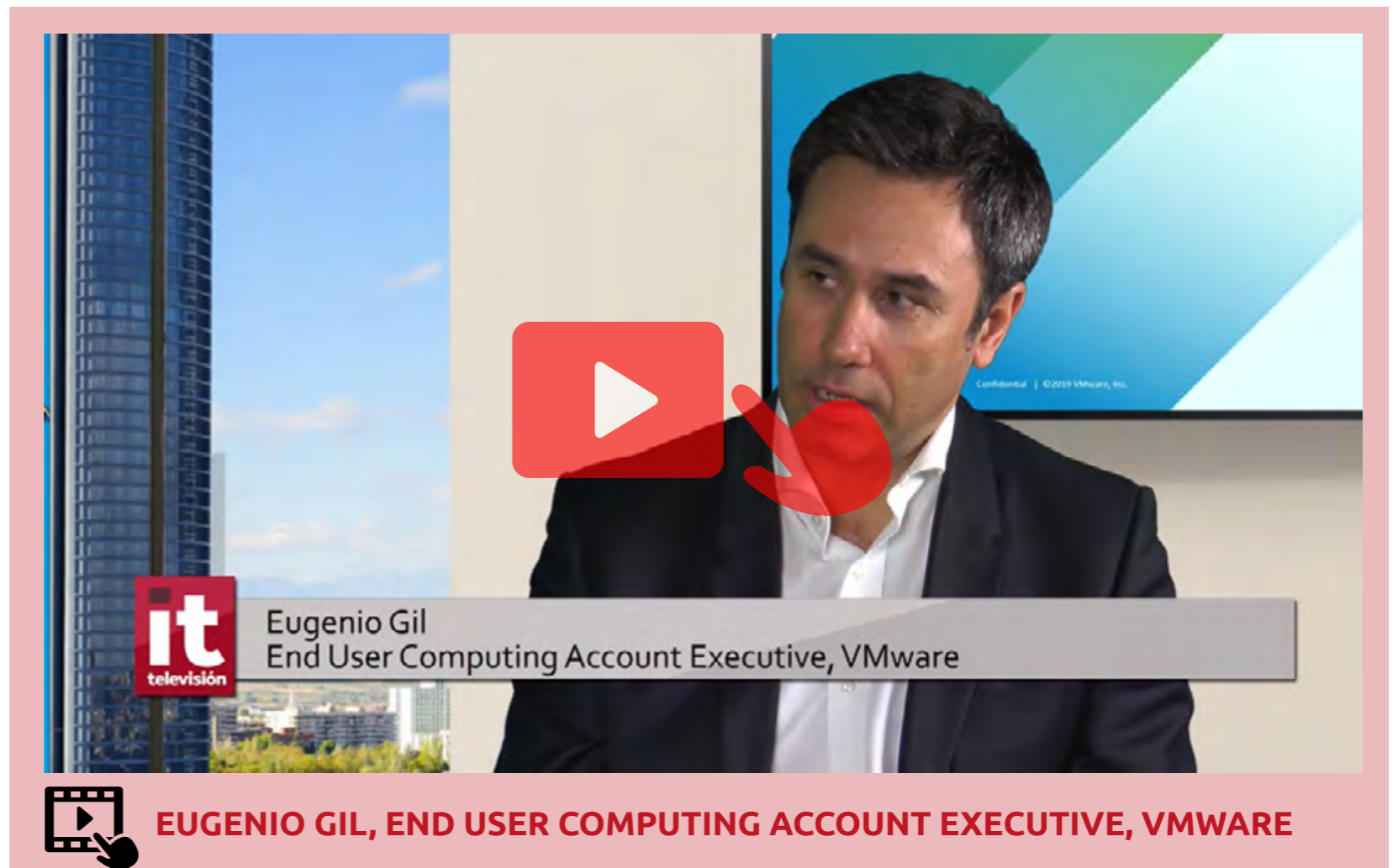


EUGENIO GIL, END USER COMPUTING ACCOUNT EXECUTIVE, VMWARE

“La movilidad significa acceder a aplicaciones y a datos, y hay que securizar ese acceso”

Detrás de un acceso en movilidad hay un caso de uso para acceder a un dato o aplicación. Lo dice Eugenio Gil, End User Computing Account Executive de VMware, durante la sesión online [Movilidad e IoT, la nueva frontera de la ciberseguridad](#). Añade el directivo que la movilidad ha acabado con el perímetro de seguridad y que lo que se propone ahora es un modelo Zero Trust de verificación constante de diferentes parámetros: dispositivos, aplicación e identidad del usuario. La idea es que una vez que hemos determinado de forma segura que un usuario puede acceder con un determinado dispositivo a una aplicación, “asegurémonos de que sólo se accede a esa aplicación”.

Asegurando que hay que unificar equipos y estrategias comunes, dice Eugenio Gil que Workspace ONE Platform permite hacer una gestión global del dispositivo, mantenerlo actualizado para que sea compliance con las



VMware propone la seguridad de la movilidad basado en un modelo Zero Trust de verificación constante de diferentes parámetros: dispositivos, aplicación e identidad del usuario

políticas de seguridad de la compañía, identificando quién es el usuario no sólo con las plataformas de la compañía, sino también con sistemas de gestión de identidades de terceros. Workspace ONE Platform permite “tener un canal seguro de acceso a la información y controlar a qué estoy accediendo”.

La estrategia para la seguridad en la movilidad de VMware parte de una gestión unificada de dispositivos haciendo uso de la información de amenazas y alertas que permite, en el momento de acceso, determinar el grado de seguridad que tiene un usuario en una determinada ubicación accediendo a esa aplicación, de tal manera que no se pueda permitir ese acceso, o bien se tenga que lanzar un doble factor para verificar la seguridad de ese usuario; “si ese usuario no cumpliera con alguno de los requisitos podríamos automáticamente remediarlo, instalando por ejemplo un parche para

solucionar una vulnerabilidad, o directamente rechazarlo. Y una vez que hemos autorizado el acceso, lo que podemos hacer es limitar esa superficie”.

Sobre si este año habrá más conciencia de la seguridad de la movilidad, Eugenio Gil apunta que los departamentos de seguridad lo tienen muy claro: la movilidad significa acceder a aplicaciones y a datos y que hay que securizar ese acceso, “y lo importante es hacerlo desde un marco único”.

[Vea aquí la intervención de VMware en Movilidad e IoT, la última frontera de la ciberseguridad.](#) ■

Si te ha gustado este artículo, compártelo



CUATRO MANERAS DE CONSEGUIR LA SEGURIDAD ZERO TRUST CON OFFICE 365

Un espacio de trabajo digital moderno ofrece una plataforma unificada que se integra con aplicaciones ampliamente utilizadas como Office 365 para proteger cargas de trabajo y dispositivos, sin importar dónde se encuentren. Con un espacio de trabajo digital bien administrado, no sólo puede alcanzar los objetivos para su negocio y clientes, sino ofrecer experiencias digitales funcionales y satisfactorias para los empleados, y todo sin poner en riesgo los datos críticos. ¿La clave? Un espacio de trabajo digital basado en el principio de seguridad Zero Trust.



AITOR LEJARZEGI, RESPONSABLE DE IOT INDUSTRIAL, SARENET

“Cualquier industria que quiera vivir muchos años necesariamente tiene que acercarse a soluciones IoT”

La digitalización ha llegado a los entornos industriales. Dice Aitor Lejarzegi, responsable de IoT Industrial de Sarenet que la industria está apostando por soluciones IoT debido al beneficio que aporta en cualquier negocio. No significa que haya que acercarse a estos nuevos entornos sin las debidas precauciones como veremos en durante la sesión online [Movilidad e IoT, la nueva frontera de la ciberseguridad](#).

Según Aitor Lejarzegi, “todos los días hay amenazas e incidentes que muchas veces acaban en una parada de fabricación”. Una experiencia de 25 años, y contar con servicios de consultoría y con un centro de datos orientado exclusivamente al sector industrial han llevado a la compañía a orientar cualquier proyecto IoT a diferentes fases: Inventario y trazabilidad de activos IP; Implantación; y Monitorización.

El primer paso es “hacernos un selfie”, detectar las vulnerabilidades, saber qué se necesita



Sarenet aborda cualquier proyecto de IoT en tres fases: inventario y trazabilidad, implantación y monitorización

mejorar. Cuenta para ello Sarenet con herramientas que permiten diagnosticar los activos IP y las vulnerabilidades asociadas a esos activos IP. El análisis de red, explica Lejarzegi, permitirá saber cómo proteger nuestra red corporativa y nuestra red de producción para poder implementar soluciones IoT adecuadamente.

“Una vez controlada la fase de inventario y trazabilidad IP, pasamos a la Fase 1, que es la implantación, y lo primero es saber dónde vamos a implantar ese proyecto IoT”, dice el responsable de IoT Industrial de Sarenet. Esto supone hacer una separación entre la red IT y la red OT, creando una zona de vigilancia para todo aquello que hable con la red de oficina y con la red de producción, como puede ser un ERP.

Una vez finalizada la fase de implantación “pasaríamos a hablar de vigilancia y monitorización”. El responsable de IoT Industrial en Sarenet apunta que, como proveedor de comunicaciones y entendiendo que la monitori-

zación es necesaria, su compañía proporciona una plataforma IoT en la que se pueden ver los datos que llegan desde cualquier punto, así como estudiar las comunicaciones entre el tráfico entrante y saliente, latencia, retardos...

Por último, el directivo de Sarenet apunta que se está pasando a la fase de implementación de proyectos de IoT. “Vemos más inquietud y más ganas. El nuevo mundo del IoT llega con una cultura digital y una innovación que puede llevar a la competitividad. Cualquier industria que quiera vivir muchos años necesariamente tiene que acercarse a soluciones IoT”.

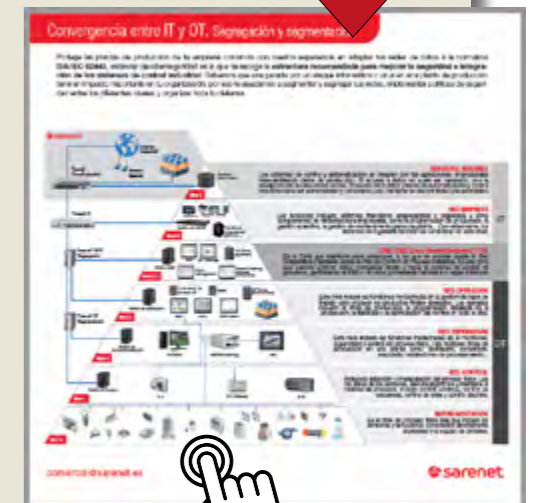
[Vea aquí la intervención de Sarenet en Movilidad e IoT, la última frontera de la ciberseguridad.](#) ■

Si te ha gustado este artículo, compártelo



CONVERGENCIA ENTRE IT Y OT. SEGREGACIÓN Y SEGMENTACIÓN

Una parada por un ataque informático o virus en una planta de producción tiene un impacto importante en cualquier organización. Sarenet te ayuda a segmentar y segregar tus redes, implementar políticas de seguridad entre los diferentes niveles y organizar toda tu defensa.

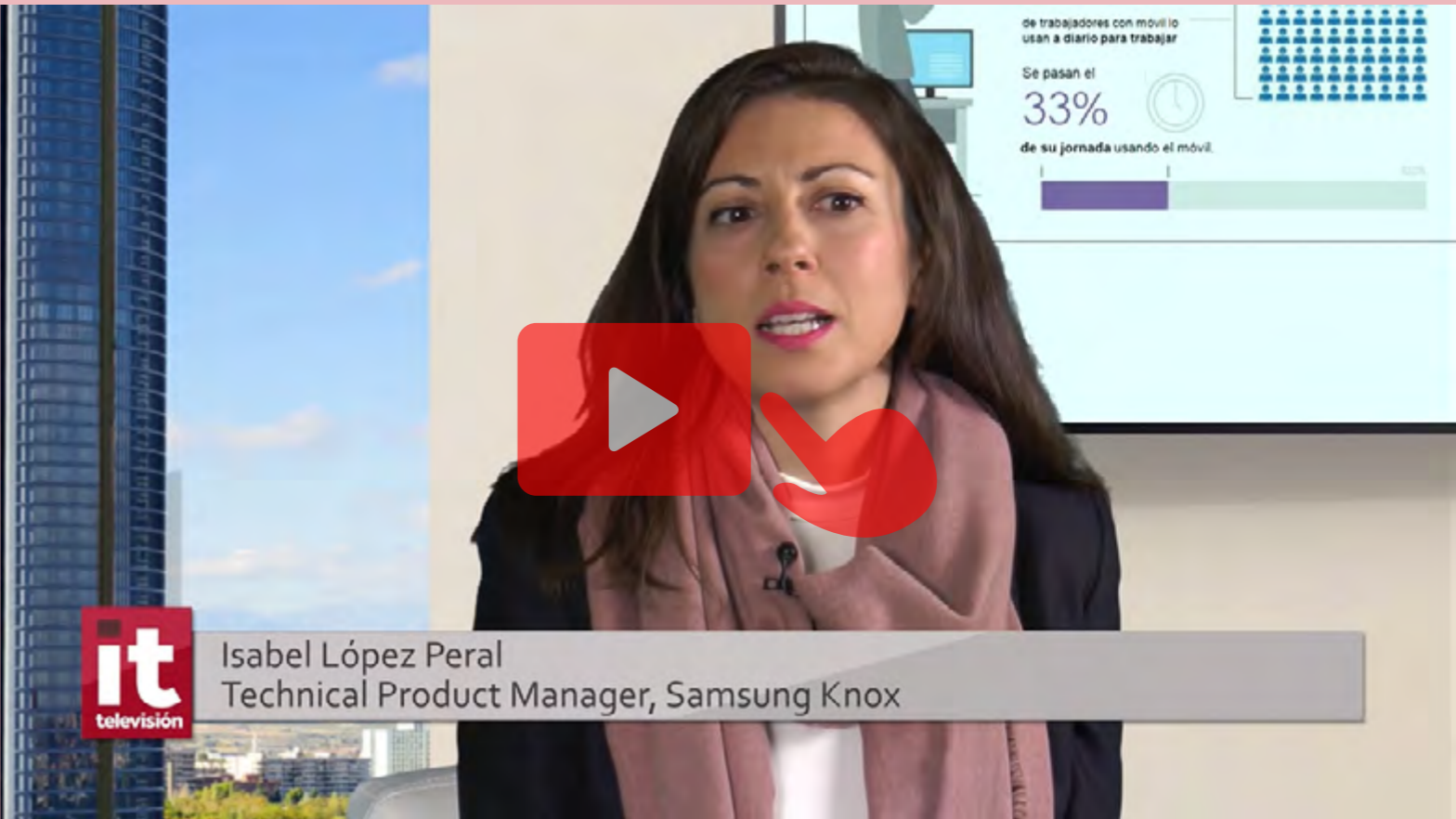


ISABEL LÓPEZ PERAL, TECHNICAL PRODUCT MANAGER, SAMSUNG KNOX

“Samsung Knox aporta dos tipos de servicios: despliegue de terminales y gestión de los dispositivos”

El 93% de los empleados, independientemente del rol que ocupen, tienen un dispositivo móvil, y el 33% de su tiempo están manejando el terminal. La seguridad es importante, pero no debe penalizar la productividad, asegura Isabel López Peral, Technical Product Manager de Samsung Knox durante la sesión online [Movilidad e IoT, la nueva frontera de la ciberseguridad](#).

Explica López Peral que Samsung Knox es una plataforma que viene precargada en todos los dispositivos Samsung; una suite de soluciones que está presente en más de 50 millones de dispositivos y aporta dos tipos de servicios: por una parte, el despliegue de terminales y, por otra, la gestión de los dispositivos. Todo comienza en el momento de fabricación, cuando se graba una clave a nivel de hardware que se utilizará para cifrar otras claves utilizadas en aplicaciones, servicios y para garantizar la integridad del sistema operativo.



de trabajadores con móvil lo usan a diario para trabajar

Se pasan el **33%** de su jornada usando el móvil.

it
televisión

Isabel López Peral
Technical Product Manager, Samsung Knox

ISABEL LÓPEZ PERAL, TECHNICAL PRODUCT MANAGER, SAMSUNG KNOX

Presente en más de 50 millones de dispositivos, Samsung Knox y aporta dos tipos de servicios. Por una parte, el despliegue de terminales y, por otra, la gestión de los dispositivos

En la parte del despliegue se cuenta con Knox Mobile Enrollment, que permite hacer un despliegue masivo y automatizado, de manera que cuando el dispositivo se enciende, se conecta a internet y carga el perfil del MDM que se ha dado de alta. Además, Knox Configure es una consola que permite definir perfiles o establecer la configuración del terminal empresarial, incluidos los ajustes por defecto que se quieran establecer.

En la parte de gestión del dispositivo móvil se cuenta con Knox Manage, una solución que no solo trabaja con dispositivos Samsung, sino con todo tipo de dispositivos Android, e incluso iOS o Windows y que permite hacer la gestión y configuración de terminales de forma fácil. En cuanto a Samsung Knox E-Fota, permite gestionar los binarios que se instalan en los terminales; es decir, se podría decidir qué versión del sistema operativo se quiere gestionar.

Además de todas estas soluciones de Knox, Samsung cuenta también con una serie de servicios empresariales que permiten dar un paso más allá. Como ejemplo pone Isabel López Peral que haya una empresa que necesite un sistema operativo personalizado, "al que podríamos hacer con un soporte premium".

Para Isabel López Peral, este es el año en que las empresas están apostando por la seguridad. Desde Samsung se apuesta por la misma sin dejar de lado la experiencia del usuario y el hacer productivo el entorno empresarial.

[Vea aquí la intervención de Samsung Knox en Movilidad e IoT, la última frontera de la ciberseguridad.](#) ■

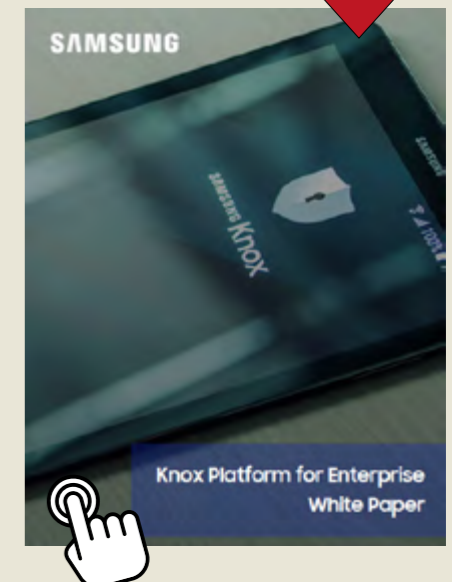
Si te ha gustado este artículo, compártelo



KNOX PLATFORM FOR ENTERPRISE

La plataforma Knox ayuda a evitar las brechas de seguridad comunes en muchas plataformas móviles. No sólo defiende contra las amenazas de seguridad y protege los datos empresariales a través de capas de seguridad creadas sobre un entorno

confiable respaldado por hardware, sino que es capaz de aislar las aplicaciones para evitar que aplicaciones no autorizadas accedan de manera intencional o inadvertida a datos no autorizados. Knox Platform proporciona varias formas de aislamiento de aplicaciones para crear un espacio contenedor de aplicaciones protegidas en dispositivos Samsung.



Encuentros **it** TRENDS

#ITWebinars #ITTrends

28 de abril de 2020
11:00 CET

Teletrabajo:
productividad, flexibilidad y
seguridad a pleno rendimiento

The poster features a teal background with an illustration of a person's legs and feet sticking out from a laptop screen, symbolizing remote work. A hand cursor icon is positioned over the bottom right corner of the poster.

#ITWebinars #ITTrends

Autenticación y
gestión de identidades,
el nuevo perímetro
de seguridad

29 de abril de 2020
11:00 CET

it TRENDS

The poster has a dark green background with a circuit board pattern and a large fingerprint graphic. A hand cursor icon is positioned over the bottom right corner of the poster.

TELETRABAJO: PRODUCTIVIDAD, FLEXIBILIDAD Y SEGURIDAD A PLENO RENDIMIENTO

La opción del teletrabajo ha dejado de ser una alternativa para las empresas; cualquier tipo de organización –desde las más pequeñas a las más grandes– se han visto forzadas a adoptar esta medida y no todas estaban preparadas para llevar sus plantillas al trabajo en remoto. ¿Qué estrategias hay que tener en cuenta? ¿Qué tecnologías posibilitan y garantizar la productividad y la seguridad del teletrabajo? ¿Cómo medir el rendimiento?

A todo ello daremos respuesta en esta sesión online, en la que contaremos con diferentes expertos tecnológicos y de recursos humanos para dar respuesta a estas cuestiones.

28 de abril de 2020

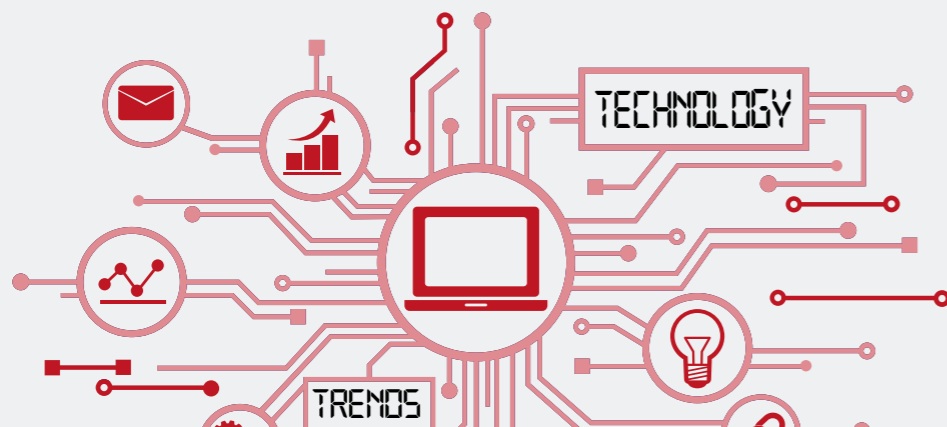
¡APÚNTATE!

AUTENTICACIÓN Y GESTIÓN DE IDENTIDADES, EL NUEVO PERÍMETRO DE SEGURIDAD

La identidad se ha convertido en el nuevo perímetro de seguridad. Saber quién accede, desde dónde, con qué dispositivo y a qué recursos es uno de los pasos más complicados de la migración a la nube. La manera de afrontarlo pasa por la autenticación basada en contexto y de múltiples factores, una autenticación no sólo de las personas, sino también de las aplicaciones y dispositivos, y de una manera centralizada. Además, las empresas necesitan mejorar la protección de las identidades, amenazas por una gestión poco hábil de las contraseñas, un panorama digital en constante cambio o una gran rotación de los empleados, lo que genera la necesidad de gestionar el aprovisionamiento y el desaproveamiento de credenciales.

29 de abril de 2020

¡REGÍSTRATE YA!!



La improvisación como estrategia de continuidad

Raúl Prieto,
Responsable Dpto.
Gobierno de Seguridad de
la Información en Sothis



"Situaciones extremas requieren medidas extremas". Tan sencillo de entender como complicado de aplicar.

En medio de una pandemia, hemos aterrizado de improviso en un escenario disruptivo con un impacto sin precedentes sobre la continuidad de los procesos de negocio de las organizaciones; un escenario que está poniendo a prueba a aquellas que, con recursos suficientes para permitírselo, hayan hecho los deberes.

Solo las entidades que hayan considerado la continuidad de negocio como un proceso más, y por tanto sigan las buenas prácticas establecidas en la norma ISO 22301 – Sistema de Gestión de la Continuidad del Negocio- o incluso

que estén certificadas de la misma, están hoy en condiciones de afrontar esta crisis aplicando medidas extremas analizadas, definidas y probadas previamente.

¿Cuál es ese proceso? En cada caso, el que dicte el plan de contingencia establecido y asociado al escenario de indisponibilidad de acceso a la sede corporativa.

Como procedimiento habitual, en primer lugar y como consecuencia de una buena definición previa de los roles y responsabilidades, se reunirá el comité de crisis para activar el Plan de Contingencia apropiado. A continuación, se decidirá el equipo de trabajo implicado en esta actuación, así como la posterior activación del

plan de comunicación interno y externo previamente establecido. Una vez implicadas todas las partes interesadas, el objetivo primordial será velar por la salud de las personas. A partir de este momento, se seguirá la estrategia definida para poder cumplir con los acuerdos de servicios requeridos por los clientes.

Sin embargo, esta no es la realidad que está experimentando la mayoría de las organizaciones. De hecho, el último informe realizado por [Gartner](#) indica que solo el 12% de las 1.500 empresas encuestadas están preparadas para afrontar esta crisis.

Las situaciones reales más comunes en el escenario actual son:

“Solo las entidades que hayan considerado la continuidad de negocio como un proceso más, y por tanto sigan las buenas prácticas establecidas en la norma ISO 22301 –Sistema de Gestión de la Continuidad del Negocio o incluso que estén certificadas de la misma, están hoy en condiciones de afrontar esta crisis”

1 Organizaciones que disponen de un Plan de Continuidad de Negocio, pero no han realizado simulacros sobre este escenario por motivos variopintos y están improvisando de la mejor forma posible.

2 Empresas que NO disponen de un Plan de Continuidad de Negocio y por tanto se encuentran ante una situación sin previo análisis y donde cualquier decisión que se tome se realizará bajo la improvisación, con la mejor de las intenciones, pero sin ningún tipo de certeza de que puede ser efectiva.

En función de la tesitura en la que se encuentre cada empresa, el perjuicio económico y re-

putacional será menor o mayor. Ahora mismo, considero que no es el momento de sacar a relucir las bondades de definir, implementar y mantener un Sistema de Gestión de Continuidad de Negocio; en estos momentos, con tan solo revisar el estado actual de los índices bursátiles mundiales, queda claro que las prioridades son otras. ■

Si te ha gustado este artículo, compártelo



CIBERSEGURIDAD EN LA CADENA DE SUMINISTRO

Para que una empresa extendida funcione, los partners y colaboradores necesitan acceso a información y sistemas críticos. Y eso se convierte en un gran problema para los responsables de seguridad, pues, aunque esto supone un aumento de la



productividad enorme, esta forma de trabajo aumenta exponencialmente los riesgos de ataques y fallos de seguridad. En este documento encontrarás cómo evaluar el riesgo de ciberseguridad que introducen tus proveedores.

De la excepción a la norma: teletrabajo de forma remota, rápida y segura

Sergio Oropeza,
Senior Manager
Solution Engineer
de VMware Iberia



La actividad empresarial como la habíamos conocido ya no es una opción. A medida que la pandemia del COVID-19 se ha extendido agresivamente por todo el mundo, todos intentamos adaptarnos a lo que es una situación en constante evolución. A medida que las escuelas y los lugares de trabajo cierran y el autoaislamiento se convierte en el entorno obligatorio, continuar con las operaciones es un desafío, pero es absolutamente necesario para superar la pandemia.

Necesitamos prepararnos para el aquí y el ahora, pero también mirar hacia el futuro, más allá de esto, donde organizaciones de todos los tamaños y sectores puedan seguir adelante.

Para muchas empresas, las últimas semanas han sido caóticas. Para continuar satisfaciendo las necesidades de los clientes, al tiempo que

cumplen con el deber de cuidar a sus empleados, muchos han adoptado el trabajo remoto. Pero incluso así, no es suficiente para algunas empresas que tienen que someterse a un replanteamiento total sobre cómo debe ser el modelo operativo de su negocio si quieren sobrevivir.

Puede parecer abrumador. Y aún más cuando las empresas y sus equipos de TI tienen que tomar decisiones en horas, días y semanas que, en otras circunstancias, pueden llevar un año.

DÍA 1: LAS BASES DE LA NUEVA NORMALIDAD

Cada organización tendrá su propio punto de partida, pero la seguridad y el bienestar del personal serán, y deberían ser, la prioridad. Para aquellos que están acostumbrados y aprecian la vida de oficina convencional y una cantidad

constante de interacciones sociales en la oficina, el cambio al trabajo remoto como resultado del distanciamiento social puede causar un impacto sorprendente, aunque relativamente leve, en el bienestar mental. La comunicación es clave, por lo que plantear “coffee breaks” virtuales para los equipos durante las horas de trabajo para fomentar la colaboración y crear un ambiente de trabajo más cómodo o un canal específico para charlar en el tiempo de descanso será vital ahora y, en los próximos meses.

Otra cuestión vital es el poder acceder a las herramientas de trabajo. Ser capaz de proporcionar una forma fácil de tener acceso a aplicaciones y servicios, y garantizar que los usuarios puedan hacerlo sea cual sea el dispositivo que tengan y hacerlo de forma segura. Eso signifi-

ca elegir un enfoque que garantice un acceso seguro y simple a las herramientas que los empleados necesitan, independientemente del dispositivo. Esta opción, que es la única en estos casos, tiene que poder evolucionar a medida que lo hace la situación de emergencia: a medida que la primera quincena se convierte en el primer mes y más allá. En pocas palabras, esto solo se puede lograr a través del software.

Las empresas que puedan adaptarse rápidamente son las que continuarán operando de manera efectiva, y esto significa darse cuenta de que no necesitan ser perfectas. Es más importante que una vez que tengan su espacio de trabajo digital, identifiquen a su personal crítico y las herramientas que necesitan lo más rápido posible. Una vez que estos estén identificados, el resto del negocio y los servicios menos críticos pueden incorporarse a la plataforma a medida que se escala.

PRIMERA SEMANA: 5 PRIORIDADES A ESTABLECER

Poner en marcha a los empleados de manera rápida y segura, cuando la oficina ya no es una opción, es una cuestión de priorizar. Podemos resumir esto en cinco pasos clave que creemos que las empresas deben seguir para establecer una base que brinde continuidad operativa de manera segura, tanto ahora mismo como a medida que la situación evoluciona.

“Una solución de espacio de trabajo digital basada en el software puede permitir a los empleados ser productivos desde el primer día en sus dispositivos”

En primer lugar, las organizaciones deben definir políticas y límites, con equipos de recursos humanos y de TI que colaboren para crear procesos que protejan a los empleados y a las propias organizaciones. Pocos equipos de TI tendrán el tiempo o los recursos para pensar quién necesita acceso a qué aplicación o carpetas, por lo que necesitarán que sea el propio usuario quien lo solicite. Este modelo de autoserivicio puede ayudar a determinar si cada usuario tiene el nivel de seguridad adecuado para acceder a las herramientas y aplicaciones que requieren.

Tener acceso al servicio remoto es un punto de partida ideal para algunos trabajadores, pero otros necesitarán su ordenador portátil y seguirán trabajando como lo hacen en la oficina con una conexión a Internet. Eso requiere un nivel de control.

En las prisas por la transición de los trabajadores, puede haber presión para desplegar nuevas herramientas sin la debida consideración de las implicaciones, que podrían presentar riesgos de seguridad, ya sea en los primeros días o en el futuro. Si la seguridad no está

en el centro, entonces el resto se anula. Las amenazas de seguridad no van a desaparecer durante esta situación.

La colaboración, y tener la capacidad de comunicarse de forma fluida, también es fundamental, tanto desde una perspectiva de continuidad operativa como para mantener la cultura de la empresa.

Finalmente, la simplicidad lo es todo. Es fundamental tener un único punto de acceso para todo el trabajo, es decir, la cantidad mínima de esfuerzo y conocimiento técnico necesario para que los empleados lleguen a lo que necesitan para hacer su trabajo, independientemente del dispositivo o la ubicación.

Una solución de espacio de trabajo digital basada en el software puede permitir a los empleados ser productivos desde el primer día en sus dispositivos. Permite el acceso inmediato a un conjunto completo de aplicaciones empresariales con inicio de sesión único sin interrupciones en todas las aplicaciones según sea necesario en función de las características del trabajo. Mientras tanto, la seguridad intrínseca “zero trust” garantiza que se consideren el cumplimiento y el

riesgo antes de otorgar acceso a las aplicaciones, protegiendo su infraestructura y datos.

DESDE LA PRIMERA SEMANA HASTA LOS MESES POSTERIORES

Tener esas prioridades en el despliegue de una solución de espacio de trabajo digital significa que las organizaciones habrán sentado las bases desde las cuales pueden continuar trabajando. Eso significa que, en las próximas semanas, el requisito de inmediatez en el trabajo remoto será reemplazado por la necesidad de formalizar esta nueva situación. A medida que los empleados se sientan más cómodos con su nueva normalidad, las empresas tendrán la oportunidad de ver lo que alguna vez fue un desafío como una oportunidad y ver cómo pueden aprovechar los beneficios de tener equipos distribuidos y conectados.

PARA TODOS LOS TRABAJADORES, NO SOLO LOS DE OFICINA

También es importante recordar que las conversaciones sobre el trabajo flexible en términos de ubicación principalmente se centran en los trabajadores de oficina, sin embargo, para muchas empresas, este segmento de empleados es solo uno de los muchos que participan en su fuerza de trabajo. Inicialmente, para los que son de primera línea, no poder ir al trabajo tiene ramificaciones económicas significativas.

Además de usar sus espacios de trabajo digitales para mantener a esos trabajadores comprometidos con el negocio, cuando los sitios se vuelvan a abrir, existe la oportunidad de redistribuir al personal a sus puestos con herramientas digitales y acceso para ofrecer un nivel diferenciado de servicio y experiencia. Las empresas necesitan tener los cimientos correctos y la situación actual de necesidad inmediata lo está haciendo posible.

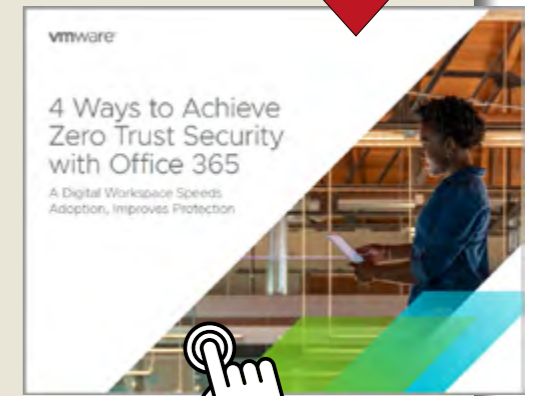
ANALIZAR LOS PRIMEROS DÍAS PARA MANTENER LA EFECTIVIDAD OPERATIVA

Son tiempos difíciles para cualquier operación comercial. Ser capaz de ofrecer a los empleados y clientes un sentido de continuidad queda solo superado por la necesidad de mantenerles a salvo. A medida que las empresas exploran formas de equilibrar las dos, el trabajo remoto se está haciendo con el protagonismo. Todas las empresas se enfrentan a un período significativo de incertidumbre, por lo que es vital que las decisiones que tomen ahora y cómo establezcan su organización para trabajar en un sistema descentralizado, fuera del lugar habitual, proporcionen las bases para lo que se avecina y brinden una oportunidad para el futuro. Eso significa un espacio de trabajo digital que ofrezca acceso seguro a las aplicaciones y servicios que los empleados necesitan, independientemente del dispositivo o la ubicación. ■



CUATRO MANERAS DE CONSEGUIR LA SEGURIDAD ZERO TRUST CON OFFICE 365

Un espacio de trabajo digital moderno ofrece una plataforma unificada que se integra con aplicaciones ampliamente utilizadas como Office 365 para proteger car-



gas de trabajo y dispositivos, sin importar dónde se encuentren. Con un espacio de trabajo digital bien administrado, no sólo puede alcanzar los objetivos para su negocio y clientes, sino ofrecer experiencias digitales funcionales y satisfactorias para los empleados, y todo sin poner en riesgo los datos críticos. ¿La clave? Un espacio de trabajo digital basado en el principio de seguridad Zero Trust.

Si te ha gustado este artículo,
compártelo



¿Tienes un ordenador, tablet o móvil que te sobre?

En la Comunidad de Madrid hay niños que los necesitan

¿Nos ayudas?



No queremos que ningún niño se quede desconectado y pierda este curso.

Puedes escribirnos y organizamos una recogida y entrega:
mercedes@fundacionadelias.org



Sending, generosamente recogerá y entregará los equipos donados a los niños que lo necesitan

El teletrabajo: de utopía a realidad



El teletrabajo: de utopía a realidad

Cuando el teletrabajo se vuelve una necesidad y los hogares deben transformarse en oficinas, es fundamental saber cómo organizarse para encontrar un equilibrio entre lo laboral y lo personal. Potenciar el uso de video llamadas y buscar formas de cohesionar a los equipos son algunos de los consejos que recomiendan los expertos.

Año tras año, la flexibilidad laboral y fórmulas como el teletrabajo son valoradas por los trabajadores entre los principales factores para elegir una empresa en la que trabajar, pero en España no hay cultura del teletrabajo: en 2019 solo el 3% de los empleados españoles trabajaba a distancia de forma habitual. En los últimos días, son muchas las empresas que han pedido a sus equipos que trabajen desde casa y la causa no es otra que el coronavirus.

Ya sea para prevenir contagios y frenar la epidemia de Covid-19, ya sea porque comienzan a aparecer los primeros casos, las compañías envían a sus trabajadores a sus casas, y no es lo algo propio de las grandes multinacionales como Google, Amazon o Facebook. Por citar solo alguno de los muchos casos locales, Telefónica anunció el 4 de marzo que tras detectar un afectado por el virus, siguiendo las recomendaciones de las autoridades sanitarias y en aplicación del protocolo de actuación de la compañía, se ha decidido que “los compañeros que mantuvieron contacto estrecho



con este empleado se queden en su casa teletrabajando y observen sus síntomas”.

Un día después, EY realizaba el mismo anuncio con un alcance más amplio: todos sus todos sus profesionales en Madrid teletrabajen tras identificar un caso positivo. En la misma jornada transcendía que Indra ha cerrado de forma temporal dos plantas de su sede en Barcelona por contagio

de dos de sus empleados, y que los compañeros de estos profesionales trabajarían desde casa.

Como ellas, muchas otras organizaciones, grandes o pequeñas, han tenido que enviar a sus empleados a trabajar en casa, si la actividad de la empresa se lo permitía. Las grandes compañías, ya tienen activos programas de teletrabajo pero, en la pyme, más reticentes, esta situación puede ser-

vir para impulsar un cambio de cultura y propiciar que utilicen la tecnología digital disponible para que sus empleados teletrabajen.

NO ES TAN FÁCIL

En realidad, todas las compañías que cuentan con un plan de continuidad de negocio tienen que tener contemplado el teletrabajo para tener capacidad de respuesta en caso de incidentes, lo que pasa por tener herramientas digitales de colaboración y garantizar comunicaciones seguras vía VPN, además de que sus trabajadores dispongan de los dispositivos adecuados para hacer su trabajo, claro está.

Resulta ilusorio pensar que la totalidad de empresas españolas dispone de un plan o que hayan dotado a su plantilla de los recursos necesarios para realizar su trabajo con seguridad.

Con un ordenador y una conexión Wi-Fi como base, se puede dar el primer paso para que los trabajadores trabajen desde fuera de la oficina. Además, como explica la consultora Prodware, “cloud computing ha permitido desarrollar soluciones de movilidad en la nube, que posibilitan una mayor flexibilidad y disponibilidad de los datos y herramientas de la empresa. Esto se traduce en una mejora de la productividad, también en el ámbito del teletrabajo”.

Con estas herramientas digitales, cada día es más fácil trabajar únicamente con un ordenador



VENTAJAS DEL TELETRABAJO



BENEFICIOS DEL TELETRABAJO

con conexión wifi, pero “la oferta de sistemas de comunicación para las empresas es tan amplia que en ocasiones es difícil escoger la que mejor se ajusta a las necesidades de cada compañía”, explica. Esta compañía aconseja que, a la hora de elegir una, se tengan en cuenta la facilidad de uso, que el sistema sea rápido y personalizable, que garantice el acceso a la información de la empresa, los contactos, el calendario y las diferentes aplicaciones de productividad, que pueda conectarse desde cualquier lugar y cualquier dispositivo es necesario que la solución sea accesible, y que garantice la privacidad de las conversaciones y la confidencialidad de los procesos.

RECOMENDACIONES DE CIBERSEGURIDAD

La firma de seguridad Kaspersky recomienda a las organizaciones examinen la seguridad en torno al acceso remoto a los sistemas corporativos porque, como explica la compañía, “los riesgos se amplían y aumentan” cuando los dispositivos se sacan de la infraestructura de red de una empresa y se conectan a nuevas redes y Wi-Fi.

La recomendación es que las empresas se aseguren de que los empleados que teletrabajan extremen la cautela. “Deberían comunicarse claramente con los trabajadores para asegurarse de que estos sean conscientes de los riesgos, y hacer todo lo posible para asegurar el acceso remoto para aquellos que trabajan

El teletrabajo ofrece nada menos que 10 beneficios palpables:

- 1 EVITA DISTRACCIONES.** Muchos empleados prefieren la tranquilidad de su casa para trabajar, frente a otros espacios que pueden suponer una fuente de distracción, incomodidad o incluso estrés.
- 2 REDUCE DESPLAZAMIENTOS.** El 39% de los europeos tarda más de 45 minutos en llegar al trabajo. Trabajar desde casa te evita estos desplazamientos y este tiempo se puede dedicar a otras actividades de interés.
- 3 FACILITA LA CONCILIACIÓN.** Los trabajadores españoles solo disponen de dos días de permiso por accidente, enfermedad grave u hospitalización de familiares de primer grado. El teletrabajo facilita la recuperación y conciliación familiar.

4 AHORRO DE COSTES. El teletrabajo supone un ahorro para las empresas de hasta un 30% en coste de infraestructura.

5 AUMENTA LA PRODUCTIVIDAD. En caso de tener que ausentarse del trabajo por un tema personal, el teletrabajo consigue, por ejemplo, que los empleados puedan asistir a esa reunión que tenían programaba y que por lo tanto su productividad no se vea afectada.

6 EVITA LAS REDUCCIONES DE JORNADA. El 95% de las reducciones de jornada por cuidado de hijos o familiares dependientes siguen correspondiendo a mujeres, y el teletrabajo evita tener que acogerse a esta medida.

7 IMPULSA LA MOVILIDAD. El AVE o los trenes de cercanías se pueden convertir en nuestra segunda oficina si tenemos

las herramientas adecuadas para poder teletrabajar.

8 SE PUEDE ESTAR PERMANENTEMENTE CONECTADO. Las herramientas de control remoto permiten que los empleados estén conectados en todo momento, por lo que si surge una situación de crisis cualquier trabajador puede estar conectado y así reducir el nivel de impacto.

9 REDUCE EL ABSENTISMO. Las condiciones meteorológicas (lluvias, nieve...) pueden llegar repercutir en la productividad de una empresa. Con el fin de compensar el absentismo y los retrasos, muchas compañías optan por el teletrabajo.

10 ACABA CON EL ESTRÉS. Según la Agencia Europea para la Seguridad y la Salud en el trabajo entre el 50 y el 60% de las jornadas laborales perdidas son por causas de estrés.



desde casa”, explica David Emm, investigador principal de seguridad de la firma.

CONSEJOS PARA SER MÁS PRODUCTIVOS

La crisis que ha provocado el coronavirus deja patente la importancia de fomentar el teletrabajo, pero se vuelve necesario sentar unas bases que permitan a los trabajadores seguir desarrollando sus funciones de manera productiva de cara a poder cumplir sus objetivos sin perjudicar su bienestar físico, cognitivo y emocional. Para ayudar en este proceso, desde Steelcase dan unas pautas para trabajar desde casa y continuar manteniendo la rutina y la productividad.

1. La importancia del equilibrio entre estar conectado y mantener la concentración. Las redes son básicas a la hora de poder hacer el trabajo, pero es importante reservar momentos para poder concentrarse y avanzar en las labores diarias. Para los casos en que tengan que realizarse conferencias o videollamadas, es clave establecer una guía para que las per-

sonas puedan seguirla y que las reuniones resulten productivas. En este sentido, se recomienda programar igualmente reuniones regulares con los equipos para saber qué tal van y mantener los vínculos con ellos.

2. Enfocar el teletrabajo para los profesionales acostumbrados a moverse. Muchas empresas cuentan con trabajadores que dedican bastante tiempo a viajes de empresa, por lo que pasar a trabajar desde casa durante todo el día puede ser un cambio drástico. Para poder enfrentarse a ello de la mejor manera posible se les aconseja moverse y cambiar de estancias. El espacio es fundamental a la hora de trabajar y ser productivos, por lo que estar en sintonía con el lugar de trabajo puede fomentar en gran medida la creatividad. Siempre de manera organizada y lógica, disponer de varios puntos dentro de la casa permite cambiar de ambiente y mejorar la concentración.

3. El nuevo teletrabajo para quienes ya teletrabajaban. El teletrabajo es un fenómeno que lleva unos años evolucionando y que ha cobrado más popularidad recientemente, pero hay profesionales que llevan funcionando de este modo años y deben adaptarse a esta nueva situación. El principal consejo para ellos es aprender a crear rutinas para adaptarse a este extraño periodo: dar prioridad al tiempo de concentración, realizar actividad física, trabajar las relaciones







¿Te gusta este reportaje?

Compártelo en redes



personales y crear maneras de relacionarse con compañeros de equipo que permita mantener el contacto de manera natural. ■

MÁS INFORMACIÓN

-  [Toda la información sobre las tendencias tecnológicas en las empresas](#)
-  [El mercado de la telefonía en la nube crece](#)
-  [Cuál es la propuesta de NFON para el mercado de la telefonía en la nube](#)
-  [Reto de las empresas a la hora de afrontar su digitalización](#)
-  [Empresas y transformación digital: mucho camino por recorrer](#)
-  [La digitalización del puesto de trabajo. Una oportunidad para las empresas](#)

cloudya

Con NFON, tu negocio siempre conectado

cloudya

El sistema de telefonía en la nube que garantiza la continuidad de tu negocio y las comunicaciones de tu equipo, desde cualquier lugar y desde cualquier dispositivo.

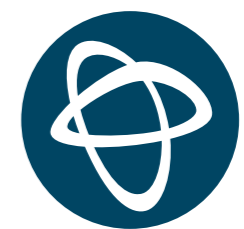


La nueva libertad en la comunicación empresarial.

Con Cloudya, NFON ofrece una solución estable para teletrabajar con una sencilla y rápida configuración. Como solución en la nube, puedes llamar a través de IP o GSM, sin importar desde dónde estés trabajando: desde tu oficina en casa o de forma remota usando la aplicación en el móvil o en el ordenador, usando teléfonos de sobremesa o auriculares. Usa el mismo número desde todos tus dispositivos. Más de 40.000 empresas en Europa ya lo están usando. ¡Pídenos tu prueba gratis! nfon.com

910 616 600

info.spain@nfon.com



NFON
Cloud Telephone System

“NUESTRO SERVICIO EN LA NUBE RESPONDE A LAS EXPECTATIVAS DE TODAS LAS EMPRESAS”

DAVID TAJUELO, COUNTRY MANAGER DE N FON IBERIA

Según las principales consultoras, el mercado global de comunicaciones en la nube crecerá a doble dígito los próximos tres años. ¿Cuáles van a ser los motivos de esta subida?

La tendencia hacia la transformación digital y la migración a la nube de cada vez más servicios históricamente ligados al HW era clara ya antes incluso de la situación que tenemos encima. El empuje venía dado tanto por el problema de la reducción de la contaminación, como por el cada vez más introducido y extendido modelo de conciliación laboral en el trabajo. Si a estos dos factores añadimos las cada vez mejores infraestructuras de transporte, el apagón RDSI por parte de los grandes operadores históricos de toda Europa, la ne-

cesidad de digitalizar las administraciones públicas (por ejemplo en UK se han destinado más de 200 millones de Libras para esto) y, por supuesto, el movimiento sísmico a nivel mundial que ha supuesto el Covid19 en cuanto al modelo de teletrabajo, con todo lo que eso conlleva, el escenario es un tormenta perfecta para la implantación a gran escala de esta tecnología. En EEUU, el líder, hablamos de una penetración de alrededor del 35%, en Europa de algo más del 20%; la palanca para el crecimiento está ahí, y eso es innegable.

¿Cómo va a ser el comportamiento en España?

España históricamente ha sido un país donde el presencialismo la-



bora siempre ha estado muy presente, valga la redundancia. Como comentaba al hilo de la pregunta anterior, la situación en la que nos encontramos sin duda va a hacer que muchas empresas se planteen adoptar de una manera estable ese modelo de teletrabajo, para el cual las comunicaciones en la nube es la tecnología que se adapta como anillo al dedo. En nuestro país la penetración es de algo más del 6% actualmente, como ves muy por debajo de la media europea y la previsión pre-Covid hablaba de más del 9% estimado para final de 2020. Claro la situación actual y la expectativa es que ese crecimiento se acelere bastante. No sé exactamente hasta donde, pero si las expectativas más optimistas pre-Covid hablaban de una penetración del 12% a finales de 2020, probablemente se situará por encima de ese número. Pero desde luego la incertidumbre no nos permite adivinar como de rápido será esta adopción de la tecnología, sobre todo por parte de la Administración Pú-

blica, quizá el sector más reticente al teletrabajo y a sacar fuera de sus instalaciones, y que supondría un espaldarazo muy importante para ese crecimiento del que hablamos, como ya está sucediendo en otros países de Europa, nuestro mercado natural.

Dentro de las ventajas que ofrece este tipo de soluciones, como seguridad o simplicidad ¿cuáles

son las que más valoradas por las empresas?

Básicamente las empresas quieren poder dedicarse a su negocio que, excepto en casos puntuales, no tiene que ver con gestionar el teléfono. Por tanto, lo más valorado es no tener caídas del servicio, que sea estable y que permita poder contactar con clientes y proveedores en cualquier momento y, por supuesto, no perder

ninguna llamada que pueda suponer no atender a un posible nuevo negocio o contrato. Lógicamente debe ser un servicio sencillo, que no sea necesario ser ingeniero de la NASA para poderlo gestionar y, por último, pero no menos importante, de una manera segura, sin tener que preocuparse de que alguien pueda hackear su sistema y entrar en el momento del aprovisionamiento de los terminales.

Las comunicaciones pueden suponer para las pymes un elevado coste para su gasto mensual. Las comunicaciones en la nube, ¿reducen los costes para las empresas? ¿De qué forma?

Por supuesto que sí, según distintos fabricantes entre el 40% y el 70% del coste de una instalación de PBX estándar contando todos los costes; es decir, la propia centralita, ajustes estacionales, soporte y mantenimiento, actualizaciones de SW, pérdidas de llamadas, el tiempo que se tarda en efectuar todas esas modificaciones con el coste de oportunidad

David Tajuelo
Country manager, NFON Iberia

Diálogos it #ContentMarketingIT

“CLOUDYA ES NUESTRO BEBÉ”



que acarrea... Si todos esos factores se suman, siempre saldrá más caro que una solución en la nube, donde para empezar no hay un gran desembolso inicial y realmente es un servicio donde pagas por lo que utilizas. Hay un término anglosajón que es el llamado TCO o "Total Cost of Ownership" que recoge todos estos factores y otros muchos que quizá no se ven de manera tan aparente, y pese a que hay algunos defensores, aún a día de hoy, del modelo tradicional, los números hablan por si solos.

¿Qué perfil de empresa es la que más partido puede sacar a la telefonía en la nube?

Cualquiera en realidad. En nuestros más de 40.000 clientes empresariales por toda Europa tenemos de todo. Y lo que si es cierto es que nuestra tasa de abandono es la menor de toda Europa, supongo que significa que nuestro servicio en la nube responde a las necesidades y expectativas de todas esas empresas. Aún hay gran-

des compañías que prefieren tener una solución On-premise, pero una vez se superen ciertos miedos históricos, esto convencido de que el modelo de telefonía en la nube se impondrá. Y más si tenemos en cuenta que ya no solo hablamos de telefonía sino de una platafor-

ma completa de comunicaciones unificadas, capaz de integrarse con ERPs, CRMs, herramientas de colaboración o de correo electrónico, y así poder llevar tu puesto de trabajo a cualquier lugar, sin ningún coste oculto y de una manera muy rápida e "indolora".

La apuesta de NFON para este mercado es Cloudya. ¿En qué consiste esta solución?

Un poco lo que te adelantaba en la respuesta anterior. Cloudya es nuestro bebé; nuestra pequeña PBX en la nube que ha crecido fuerte, inteligente y robusta; y poco a





poco, en su crecimiento, va aprendiendo. Pasó a ser una adolescente que no solo tenía las funcionalidades de una PBX tradicional (más de 150) sino que aprendió a grabar llamadas, a gestionar colas, a manejar call centers. Ahora está aprendiendo idiomas y se puede comunicar con un PMS, con un CRM, con un ERP, con Microsoft Teams... Y se ha convertido en una plataforma inteligente, robusta, pero a la vez sencilla de utilizar, capaz de responder a las necesidades de cualquier empresa que utilice el teléfono para comunicarse. Y cuando digo teléfono, me refiero al terminal tradicional, o al softphone que puedes instalar en tu PC mediante una app o simplemente acceder mediante un portal web con la tecnología WebRTC, o

a una app para tu teléfono móvil o Tablet; independientemente de qué sistema operativo utilices o de donde estés. Está claro que el concepto de teléfono ha cambiado por completo desde que Graham Bell lo patentase y comercializase en el sXIX, pero su objetivo es el mismo; poner en contacto a personas.

¿Cuáles son los motivos que llevan a las empresas a decantarse por una solución como la de NFON?

Siempre nos hemos enfocado en tres de las necesidades y peticiones de nuestros clientes, la sencillez de uso, la flexibilidad de la solución y la estabilidad del servicio. Pero no solo es eso lo que mueve a las empresas a una solución de nube; también creemos que hay que hacer hincapié en tener una plataforma abierta y compatible, en el sentido de ser capaz de integrarse con soluciones líderes de terceros; por supuesto que permite ahorrar al cliente en su día a día; que aporte una solución segura y a prueba de fallos (ahí siempre jugamos con nuestra ingeniería

Made in Germany) y, por último, con actualizaciones gratuitas de por vida, por denominarlo de alguna manera, inalterable a lo que traiga el futuro. En resumen, proporcionando una solución que haga que nuestros partners y clientes, parafraseando al gran Bobby McFerrin piensen, "Don't worry, be NFON".


¿Qué papel juega el canal de distribución en el crecimiento y consolidación del mercado de comunicaciones unificadas?

Por supuesto no podemos pensar en crecer si no disponemos de un canal de distribución sano y comprometido. Si te fijas, no he dicho grande. Mi padre siempre me ha dicho que es bueno conocer a mucha gente porque eso te hará aprender de las distintas formas de ver la vida que tiene cada uno, y te ayudará a tomar las decisiones correctas (con suerte, claro) pero que serán menos con lo que tengas una relación de confianza; es ley de vida. Nuestra idea en NFON Iberia es algo así, por supuesto estamos encantados de que muchos




partners trabajen con nosotros y nos ayudemos a generar negocio conjunto, pero también somos conscientes que serán menos los que se comprometan en formarse, en adquirir un compromiso, en invertir en NFON para de la mano crecer nuestro negocio común. ■

MÁS INFORMACIÓN

 [Toda la información sobre las tendencias tecnológicas en las empresas](#)

 [El mercado de la telefonía en la nube crece](#)

 [Cuál es la propuesta de NFON para el mercado de la telefonía en la nube](#)

¿Cuál es la situación de la empresa española en relación con la digitalización?

¿Qué tecnologías son las que están impulsando la transformación digital?

Descubra las últimas tendencias en el **it** Centro de Recursos **User**

»»»»»»
»»»»»»

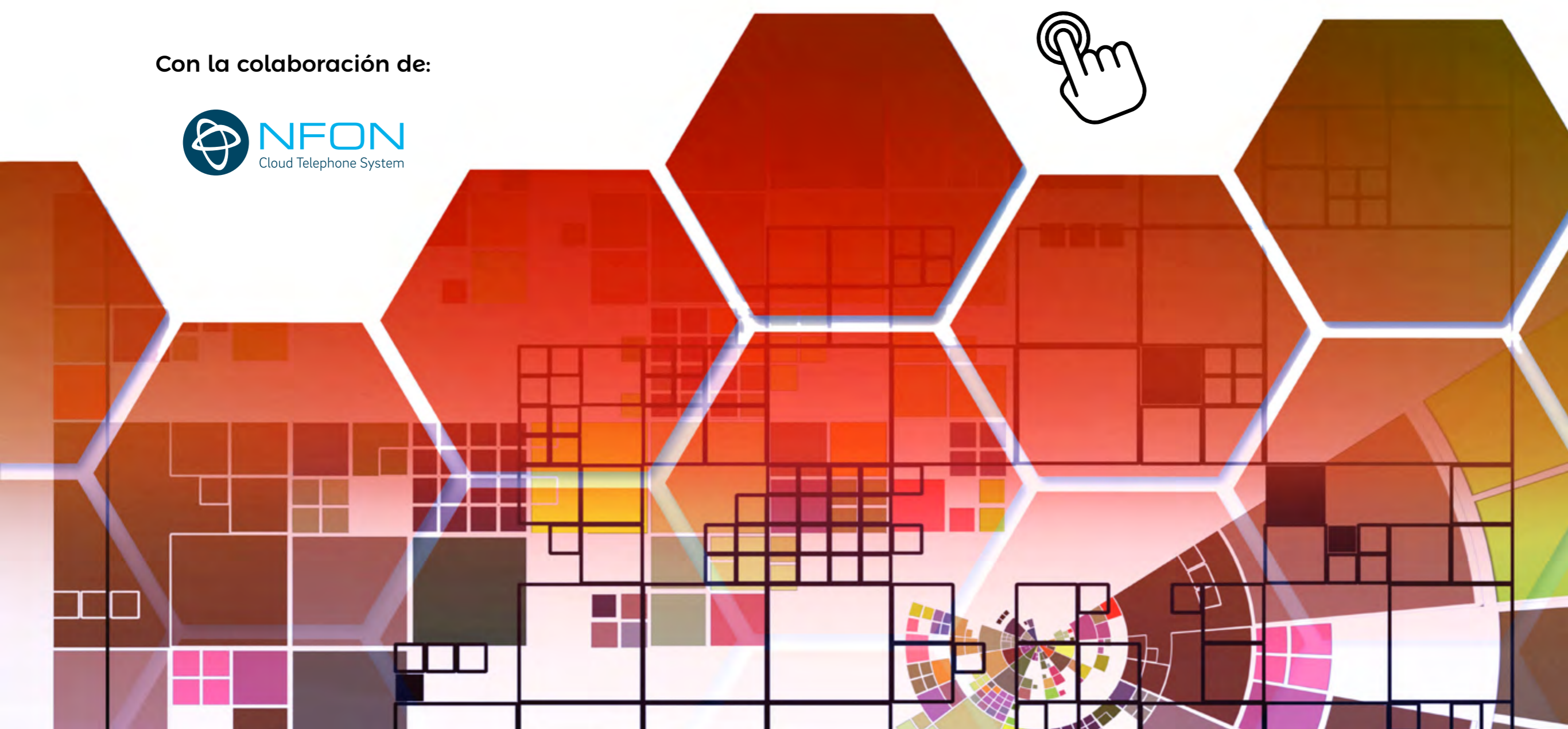


Tecnología

para tu **Empresa**

««««««
««««««

Con la colaboración de:





Impresión Digital

CENTRO DE RECURSOS



**Inteligencia artificial,
¿como afecta al mundo
de la impresión?**

brother



Inteligencia artificial, ¿cómo afecta al mundo de la impresión?

La industria de la impresión se enfrenta a la realidad de la disrupción digital. Muchas empresas son muy conscientes del valor potencial de la IA, y están introduciendo esta tecnología en la automatización de impresoras inteligentes. Los proveedores de impresión deben invertir en esta tecnología que mantendrá sus dispositivos relevantes.

La inteligencia artificial (IA) está impulsando una nueva ola de disrupción digital. Según Tractica, para el año 2025, los ingresos anuales globales de los productos y servicios basados en IA alcanzarán los 59.750 millones de dólares. Los mercados verticales más grandes para IA incluyen fintech, salud,



La automatización de procesos de impresión será clave en la oficina del futuro

Los avances tecnológicos, la evolución de nuestros propios roles laborales y la configuración de la oficina predominan cuando pensamos en el futuro lugar de trabajo, pero el impacto que la tecnología conectada tiene en la experiencia del cliente será nada menos que transformacional.

Los signos de esta evolución ya son evidentes. La convergencia de la nube y la tecnología predictiva están conduciendo a un servicio al cliente rápido, impecable y altamente personalizado, abriendo así nuevas y enormes oportunidades de crecimiento para los negocios visionarios.

La inteligencia artificial pronto apoyará una serie de nuevas tecnologías que nos ahorrarán tiempo y nos harán más productivos en el trabajo. Así, por ejemplo, a nivel de auto reaprovisionamiento, las impresoras multifunción inteligentes ya pueden encargarse de su propia tinta cuando empieza a escasear. Además, las impresoras con capacidad de impresión biométrica conocerán las preferencias individuales de los trabajadores. Todo esto ahorrará tiempo, elevará a los trabajadores en la cadena de valor, liberando a las personas para que centren sus esfuerzos en proporcionar el mejor servicio posible a los clientes.

transporte y venta minorista. Si bien la búsqueda de inteligencia artificial ha perdurado durante los últimos 70 años, es solo los avances tecnológicos dramáticos que están acelerando su despliegue. Hoy en día, la disponibilidad de unidades de procesamiento gráfico (GPU) de alto nivel, las mejoras en los algoritmos y el aumento exponencial y la abundancia de datos han acelerado la eficacia de la IA.

QUÉ ES LA INTELIGENCIA ARTIFICIAL

La IA se ha convertido en un término general para la tecnología que simula la inteligencia de los humanos en las máquinas, lo que les permite aprender de la experiencia, adaptarse a

los nuevos hechos y realizar tareas similares a las de los humanos. Como señala Quocirca, el uso de estas tecnologías puede capacitar a las máquinas para realizar tareas específicas mediante el procesamiento de grandes cantidades de datos y el reconocimiento de patrones en los datos. Es importante tener en cuenta que la IA no es una sola tecnología, sino una combinación de varias, que incluyen el aprendizaje automático, el aprendizaje profundo, el procesamiento del lenguaje natural (PNL) y la computación cognitiva.

Sin embargo, la combinación de aprendizaje automático y técnicas de aprendizaje profundo son prometedoras para ayudar a impulsar la in-



novación, la productividad y la eficiencia para las empresas y sus empleados. A medida que la IA gana impulso, las compañías deberán considerar los beneficios de aplicar estas tecnologías a sus productos y servicios, incluida la impresión.

CÓMO AFECTA LA IA A LA IMPRESIÓN

La combinación de Big Data e IA permite a las empresas impulsar una mayor eficiencia al realizar un mantenimiento predictivo de manera más efectiva. El mantenimiento predictivo no

es nada nuevo en la industria de la impresión, y la calidad y eficiencia del servicio es la razón principal por la que las organizaciones recurren a un servicio de impresión gestionado (MPS).

La mayoría de los dispositivos (impresoras en red, copiadoras e impresoras multifunción) tienen tecnología de sensores incorporada que permite recopilar y analizar datos. Sin embargo, el volumen de datos que generan los dispositivos de impresión conectados aún no se ha explotado completamente, más allá de la

supervisión continua. En muchos casos, las herramientas analíticas de gestión de impresión no están diseñadas para el análisis masivo de datos y, a menudo, no son lo suficientemente flexibles para incorporar el aprendizaje automático. La clave para mejorar la eficiencia del negocio es dar el siguiente paso y combinar algoritmos avanzados con el aprendizaje automático para tomar medidas en tiempo real. Los fabricantes de impresión deben determinar las mejores formas de integrar la inteligencia en sus dispositivos y luego desarrollar las técnicas óptimas para recopilar y analizar datos para generar información útil.

OJO A LA SEGURIDAD

Por otro lado, la IA tiene el potencial de ser tanto un amigo como un enemigo cuando se trata de seguridad. Se piensa que la próxima generación de malware utilizará la IA para comportarse como un atacante humano, identificando objetivos y evitando la detección. Dado que las impresoras y dispositivos multifunción son dispositivos conectados exigirá una nueva clase de seguridad que utilice IA para permitir que los dispositivos se monitoricen a sí mismos y se curen automáticamente.

En lugar de parches ocasionales a nivel de dispositivo, el aprendizaje automático combinado con una toma de decisiones de IA más avanzada ayudará a los fabricantes a propor-



CÓMO INFLUYE LA INTELIGENCIA ARTIFICIAL EN NUESTRA VIDA

Todas las novedades sobre el mercado de impresión en **#IMPRESIONIT**



¿Te gusta este reportaje?

Compártelo en redes



cionar análisis de comportamiento a nivel de red y detección de anomalías en tiempo real. Cuando se produce una brecha en la seguridad, una respuesta efectiva y rápida utilizando el aprendizaje automático en combinación con un motor de análisis avanzado puede optimizar los esfuerzos de remediación.

HACIA UN MUNDO DIGITAL











Finalmente, si bien muchos negocios siguen dependiendo del papel, la aceleración de las iniciativas de digitalización está en marcha. La automatización de procesos robóticos (RPA) es complementaria a la IA, ya que es una clase de software que replica las acciones de los seres humanos para ejecutar procesos de negocios. Aunque los robots RPA no tienen la capacidad de autoaprender, cuando la tecnología se combina con la IA, puede ser extremadamente potente.

Aunque no es necesariamente verdadera la inteligencia artificial, la tecnología RPA utili-

za algoritmos para comprender documentos complejos no estructurados, como información escrita a mano y escrita, y convertirlos en archivos digitales legibles y categorizados. Los trabajos manuales repetitivos, como el procesamiento de facturas, pueden manejarse de manera efectiva utilizando este enfoque. La automatización de los procesos basados en papel es tanto un desafío como una oportunidad para la industria de la impresión: si la IA puede integrarse en las plataformas de captura de documentos, proporcionará un puente muy necesario entre el mundo del papel y el digital.

En definitiva, en el ámbito de la impresión, la IA tendrá aplicaciones a través de la técnica de Machine Learning con el objetivo de hacer que el equipo de impresión se adapte a la forma de imprimir de cada usuario concreto. De hecho, mediante la incorporación de IA en la impresión se conseguirá automatizar tareas y eliminar cuellos de botella, lo que redundará en empleados más productivos. ■

MÁS INFORMACIÓN

-  [Toda la información sobre el mercado de impresión](#)
-  [Cuál es la propuesta de Brother para el mercado de impresión](#)
-  [Cuál es la propuesta de LRS para el mercado de impresión](#)
-  [La importancia de la seguridad en el mundo de la impresión](#)
-  [De la impresión 3D a la 4D](#)
-  [La impresión, pieza clave para conseguir un mundo más sostenible](#)
-  [El mercado de impresión, más allá del papel](#)
-  [La transformación del mercado de impresión](#)
-  [La impresión como herramienta para mejorar la productividad](#)
-  [El mercado de impresión ¿preparado para la disrupción digital?](#)

Diseñadas para empresas

Gama profesional
de impresoras multifunción

brother.es/gama-profesional



Equipos de impresión pensados para satisfacer las necesidades de cualquier negocio

Las impresoras multifunción láser y tinta profesionales proporcionan a las empresas una solución de impresión perfecta y a su medida. Sea cual sea su tamaño o actividad, si necesitan monocromo o color, A4 o A3, en Brother encontrarán el equipo idóneo. Disponibles con servicios de impresión gestionados.

“LA INFORMÁTICA SOSTENIBLE ES UNA TENDENCIA EN ALZA, TAMBIÉN EN LA IMPRESIÓN”

JOSÉ RAMÓN SANZ, RESPONSABLE DE MARKETING DE PRODUCTO DE BROTHER IBERIA

● **Cómo va a evolucionar el mercado de impresión tanto a nivel global como en España?**

El mercado de impresión tradicional, en términos generales, es un mercado maduro. Esto hace que no esperemos que se produzcan grandes crecimientos en los próximos años.

En cambio, sí que esperamos que se produzca una evolución continua tanto en el desarrollo de los dispositivos como en la forma de comprar de las empresas.

¿Qué factores son los que van a marcar la evolución de los hábitos de compra de las empresas?

Las empresas cada vez valoran más las características de los dispositivos. En este sentido, los multifunción cada vez va ganando más peso en las empresas. Esta



tendencia no es sólo a nivel global, sino que también se está produciendo en España.

El color es otra de las tendencias que se están imponiendo en las empresas y es un factor muy valorado en las decisiones de

compra de los clientes. Más allá de la impresión tradicional, existen áreas dentro de este mercado que tienen un amplio recorrido y un grandísimo crecimiento, como son las soluciones de identificación y etiquetado.

¿Cuáles van a ser las principales tendencias que van a marcar el mercado de impresión este año?

Las tendencias que se han consolidado en años anteriores continuarán siendo las que marcarán el desarrollo del mercado de impresión este año.

Por ejemplo, la movilidad seguirá siendo esencial para las empresas, que ven imprescindible que los equipos de impresión permitan imprimir o digitalizar documentos desde dispositivos móviles.

La seguridad y el cloud también van a predominar. No hay que olvidar que la información que trabajamos se encuentra alojada en servidores, que no tienen que ser físicos. Incluso, a la hora de digitalizar, la información la guardamos no en nuestro dispositivo, sino en la nube. Todo esto tiene que ser

compatible con soluciones de seguridad cada vez más evolucionadas que aseguren que nadie que no tenga permiso va a acceder a esos datos.

¿De qué manera influye el Green IT en el mercado de impresión?

Sin lugar a dudas, el Green IT, o la tecnología verde, está adquiriendo importancia en el mundo de la impresión. Ésta es otra tendencia que evolucionará este año y que será cada vez más considerada por las empresas a la hora de adquirir un determinado equipo de impresión.

La informática sostenible es una tendencia en alza. Las empresas buscan proteger el medio ambiente en todos sus aspectos, desde la producción al uso.

Es decir, la sostenibilidad es un factor cada vez más relevante para las empresas de todo tipo, sector y tamaño y está siendo cada vez más demandada por éstas.

La inteligencia artificial es una de las grandes tendencias de mercado. ¿Cómo va a ser su evolución en el mercado de impresión?



A día de hoy es difícil predecir cómo la inteligencia artificial influirá en el mercado de impresión debido a que todavía estamos en los inicios de esta tecnología. El potencial de esta tecnología, y la capacidad de

innovación, es tan grande que hay cosas que ahora mismo nos pueden parecer ciencia a ficción que es posible que en unos meses estén implementados.

Por ejemplo, la capacidad predictiva ya es una funcionalidad que se encuentra en muchos modelos de impresión. Gracias a esta capacidad, las impresoras pueden detectar cuándo van a necesitar un consumible e, incluso, pueden llegar a hacer el pedido por sí mismas, cuando están

dentro de los servicios gestionados de impresión.

La inteligencia artificial va más allá e incluso ya está ligada a la parte de protección de la impresión. Por poner otro ejemplo, los documentos que puede imprimir un determinado usuario ya dispone de pautas para que no se impriman hasta que éste pueda recogerlos personalmente.

La inteligencia artificial también permitirá que el equipo pueda reconocer al usuario a medida que éste se acerca e imprima sus documentos o acceder a sus servicios sin que éste tenga que identificarse.

¿Todas estas tendencias van a impulsar la transición de lo físico a lo digital?

En estos momentos ya no existen barreras entre lo físico y lo digital. Si entendemos lo físico como el papel, éste, ahora mismo, es temporal. El papel es una información que estaba en digital y que volverá a digitalizarse, con lo que todos los sistemas que tenemos en la actualidad ya son digitales.



“EL GREEN IT VA A INFLUIR CADA VEZ MÁS EN EL MERCADO DE IMPRESIÓN”

“La sostenibilidad es un factor cada vez más relevante para las empresas de todo tipo, sector y tamaño y está siendo cada vez más demanda por éstas”

¿Cuáles van a ser las principales novedades de Brother en este 2020?

En la actualidad nos encontramos en medio de una evolución de los distintos productos y servicios.

En la parte de producto, en este año habrá muchas novedades en la parte de etiquetado y movilidad. No sólo vamos a renovar equipos o gamas existentes, sino que vamos a incorporar nuevas gamas que nos permitan acceder a mercados en los que no estamos actualmente.

En lo que respecta a los servicios, nuestro trabajo se está centrando en ofrecer nuevos servicios a productos de impresión disponibles. Aquí también tendremos muchas novedades. ■

MÁS INFORMACIÓN

[www](#) Toda la información sobre el mercado de impresión

[www](#) Cuál es la propuesta de Brother para el mercado de impresión

¿Te gusta este reportaje?

Compártelo en redes



PARQUES DE IMPRESIÓN DISTRIBUIDOS, LA MEJOR OPCIÓN PARA LAS EMPRESAS

Nos encontramos en un momento en que cualquier empresa tiene que hacer frente a ritmos casi frenéticos y se afanan por evitar el caos de tal forma que su productividad no se vea mermada. Es en este punto donde sacar el máximo partido a cada recurso se vuelve vital y donde disponer de un parque de impresión adaptado a las necesidades de cada empresa puede suponer un plus a la hora de lograr maximizar la

productividad. Si echamos la vista atrás, hace no mucho tiempo las empresas se decantaban por una política de impresión centralizada. Es decir, adquirirían un par de equipos para toda la compañía pensando que así se cumplían con las exigencias de sus empleados. ¿Cuál era el resultado? Un caos aún mayor debido a las idas y venidas hasta la impresora, colas de empleados esperando para recoger sus documentos,

confusiones y hasta olvidos de información que, en muchas ocasiones, no debe estar disponible para todo el mundo.

Es por ese motivo que contar con un parque de impresión distribuido es, sin lugar a duda, la mejor opción para las empresas. Así se logra satisfacer las necesidades de cada departamento (no hay que olvidar que ni todos trabajan al mismo ritmo ni tienen las mismas demandas de impre-

sión) logrando incrementar la eficiencia operativa y, por ende, la productividad.

Puedes leer la tribuna de opinión entera en [este enlace](#)



JOSÉ RAMÓN SANZ,
Responsable de Marketing de
Producto de Brother Iberia



Facilite un puesto de trabajo digital

Documentos | Impresión | Escaneo



Puesto de trabajo del futuro
Mejore la experiencia de usuario
Estandarice infraestructura

- Elimine hardware y soluciones puntuales
- Cree una capa de servicio independiente del fabricante
- Simplifique infraestructura y habilite la nube



LRS[®]
OUTPUT MANAGEMENT

www.LRSoutputmanagement.com/puesto-de-trabajo-digital

2020 Levi, Ray & Shoup, Inc. Todos los derechos reservados. Los logos de LRS y LRS Chevron son marcas registradas de Levi, Ray & Shoup, Inc. Todas las demás marcas son propiedad de sus respectivos propietarios.

“LA TRANSFORMACIÓN DIGITAL DEFINE EL MERCADO DE IMPRESIÓN Y GESTIÓN DE DOCUMENTOS”

El mercado de la impresión y gestión documental está en constante evolución. ¿Cuáles son las tendencias que están marcando la forma en que los usuarios gestionan sus documentos?

En general, el mercado está buscando una gran flexibilidad en relación con “cómo” y “desde dónde” trabajan los empleados. Esto encaja perfectamente con la visión de Gartner del Puesto de trabajo digital: “El puesto de trabajo digital permite formas de trabajo nuevas y más eficaces; aumenta el compromiso y la agilidad de los empleados; y explota estilos y tecnologías orientados al consumidor “. Esta definición se centra en la experiencia del individuo, así como en el entorno más amplio en el que trabaja. Es deliberadamente amplio, evitando la trampa de centrarse en un conjunto actual de tecnologías porque seguirán evolucionando con el tiempo.

El puesto de trabajo digital se extenderá más allá de la intranet corporativa y sus aplicaciones y herramientas relacionadas, cubriendo todas las herramientas de productividad personal, conectividad, sistemas comerciales y el lugar de trabajo físico. Esto se debe a que la línea entre la oficina física tradicional y el lugar donde el trabajo realmente sucede está en constante evolución.

¿Cuál va a ser el papel de la impresión y gestión documental en las empresas? ¿Cuál va a ser la función del papel en el futuro?

La Transformación Digital va a continuar definiendo el mercado de impresión y gestión de documentos. Lo primero será poder identificar qué debe seguir imprimiéndose y qué documentos pasan a ser visualizados, de ahí la necesidad de una auditoría a nivel corporativo.

De esta manera, para aquellos documentos que sea necesario im-



EVA MARÍA SÚAREZ, LRS COUNTRY MANAGER

primir, será necesario asegurar su trazabilidad, monitorización y control para proporcionar agilidad y soporte completo a los procesos de negocio que soporten. En el caso de los documentos que pasen a ser visualizados, será imprescindible poder realizar el cambio a visualización sin interrumpir las operaciones de negocios y con el menor coste en esfuerzo y tiempo. La agilidad de IT

será clave en ambos casos, de ahí la necesidad de estandarizar y securizar el flujo de documentos, sea cual sea su origen y destino.

Nuestro rol será continuar gestionando todo el ciclo del documento, ya sea para atender requerimientos de documentos impresos, distribución electrónica o digitalización de documentos (workflows de captura de datos)

¿Cuál va a ser el rol de la seguridad?

La seguridad ha sido una de las grandes olvidadas por las empresas a la hora renovar sus equipos de impresión y gestión documental, las cuales han dado prioridad a otros factores como el ahorro de costes.

Las organizaciones de TI deben salvaguardar la información valiosa y sensible y garantizar que solo el personal autorizado acceda a ella y la use de acuerdo con las pautas establecidas. Esta información incluye tanto propiedad intelectual y secretos comerciales como relaciones comerciales con proveedores y socios o detalles personales sobre sus empleados y los clientes que atiende. La seguridad ha sido un desafío continuo durante años.

Cuando se habla de "seguridad de impresión" la reacción inicial es preguntarse si la impresión realmente tiene riesgos de seguridad. Los CIO y CISO deben garantizar que se apliquen las medidas de seguridad adecuadas en toda la empresa, especialmente en las aplicaciones y en la infraestructura de TI.

Las amenazas no están necesariamente evolucionando, han exis-

tido por mucho tiempo. Lo que está evolucionando es el mayor enfoque organizacional para abordar las amenazas conocidas.

La movilidad y el cloud son otras tendencias que están marcando la evolución del mercado de impresión y gestión documental. ¿Cómo van a evolucionar estas tendencias? ¿Son dos de los principales reclamos de las empresas?

La movilidad empresarial va más allá de los teléfonos inteligentes, tabletas y portátiles. Por supuesto que son importantes y desempeñan un papel vital para la movilidad, pero los dispositivos informáticos evolucionarán con el tiempo.

Nuestro enfoque está en el trabajador móvil, por lo que debemos comprender sus requisitos específicos en función de sus responsabilidades laborales. Hoy, los trabajadores esperan conveniencia y facilidad de uso

Todas las novedades sobre el mercado de impresión en #IMPRESIONIT



cuando interactúan con aplicaciones y tecnología. Se trata de la famosa "experiencia del usuario". También esperan que las aplicaciones y la infraestructura de TI estén disponibles todo el tiempo. Esto da como resultado una situación de beneficio mutuo para los empleados y las empresas porque los trabajadores son más productivos y además están más satisfechos con sus trabajos. Aunque los trabajadores móviles prefieren usar documentos en formato electrónico, requieren la capacidad de

imprimir y escanear documentos impresos cuando sea necesario. Los servicios en la nube proporcionan capacidad de proceso generalizada, bajo demanda y rentable para los trabajadores móviles. La combinación de dispositivos móviles y servicios en la nube permite a las personas trabajar en cualquier lugar, en cualquier momento y en cualquier dispositivo.

En resumen, la movilidad y la nube están entrelazadas, y son elementos clave del puesto de trabajo digital moderno.

it Eva María Suarez, Country manager, LRS para España y Portugal

Diálogos it
#ContentMarketingIT

“LA LÍNEA ENTRE LA OFICINA FÍSICA Y EL LUGAR DONDE SE TRABAJA SE ESTÁ DIFUMINANDO”

¿Cuál es la propuesta de LRS para optimizar el ciclo de vida del documento? ¿Qué beneficios son los que obtienen las empresas en relación a la oferta de otros fabricantes?

LRS proporciona middleware que captura y entrega documentos generados desde cualquier aplicación que se ejecute en cualquier plataforma a cualquier destino físico o virtual. Esta arquitectura de middleware optimiza todo el ciclo de vida del documento, desde la captura y el procesamiento de imágenes, hasta los flujos de trabajo y la gestión de documentos o todo lo que tenga que ver con la gestión de impresión. En resumen, nuestra arquitectura constituye una capa de servicio que gestiona la captura y entrega de documentos electrónicos o en papel a dispositivos de impresión y a aplicaciones. Dicho de otra manera, permitimos que las organizaciones muevan documentos electrónicos a formato de papel impreso (es decir, un documento impreso) y documentos en papel a formato electrónico (es decir, digitalización). La digitalización convierte los do-

cumentos en papel a un formato electrónico útil, como PDF con capacidad de búsqueda. Cuando todo está en formato digital, es posible ahorrar en mano de obra, innovación y automatización de procesos de negocio. También es más fácil salvaguardar, buscar, analizar, compartir y administrar los datos.

Nuestras soluciones de middleware son independientes del hardware, por lo que ofrecemos a los clientes muchas opciones respecto al hardware de impresora que estén considerando utilizar.

¿Cuáles son las principales novedades de LRS para este 2020?

Impresión segura a través de Internet público sin una conexión VPN/WAN: hoy en día, muchas organizaciones permiten a los empleados remotos y a organizaciones de terceros acceder a aplicaciones de negocio críticas a través de Internet a través de HTTPS. Este es un buen ejemplo de informática basada en Internet. Sin embargo, imprimir desde la aplicación de negocio a un dispositivo en la ubicación remota no es sencillo debido a problemas

¿Te gusta este reportaje?

Compártelo en redes



de seguridad y firewall. Por lo tanto, no sorprende que las organizaciones quieran aprovechar la infraestructura pública de Internet en todo el mundo para imprimir de forma segura en ubicaciones de oficinas remotas, sin la necesidad de una conexión WAN o VPN dedicada. LRS está trabajando en una nueva solución para abordar este requisito del mercado. Nos referimos a esta solución como "impresión de afiliados" porque el proveedor de hosting de aplicaciones y la oficina remota tienen una relación comercial (es decir, afiliada de alguna manera).

Mejora de nuestra solución MFP-secure / Scan para admitir plataformas de proveedores de hardware adicionales. Hoy, la solución LRS MFPsecure / Print admite 10 plataformas de proveedores de hardware con un "agente de software integrado" para una impresión segura (pull). LRS está trabajando

para desarrollar soporte para más plataformas de proveedores, para que podamos ofrecer una solución segura de flujo de trabajo de escaneo a clientes adicionales. Con la solución de escaneo seguro de LRS,

Proporcionar capacidades adicionales para los usuarios a través de un nuevo componente software. Muchas organizaciones de TI desean mejorar la experiencia del usuario con respecto a las funciones de TI cotidianas para sus trabajadores. La impresión es una de estas funciones. LRS está desarrollando una nueva aplicación de escritorio o "cuadro de mando de impresión" para usuarios. Esta aplicación les permite ser más autosuficientes con respecto a las tareas de impresión y las opciones personalizadas. ■



MÁS INFORMACIÓN



[Toda la información sobre el mercado de impresión](#)



[Cuál es la propuesta de LRS para el mercado de impresión](#)

El mercado de impresión ha experimentado una profunda transformación ayudando a las empresas en sus procesos de digitalización.

¡Descubra en nuestro



cómo está evolucionando un sector clave en la Transformación Digital!



Impresión Digital

Con la colaboración de:

brother



it

EN PORTADA

El dato, la empresa y su negocio: claves del éxito

La cantidad total de datos creados en el mundo aumentará dramáticamente en los próximos años, llegando a 175 zetabytes en 2025. Solo en este 2020, cada uno de nosotros generará 1,7 megabytes en solo un segundo y los usuarios de Internet alrededor de 2,5 quintillones de bytes de datos cada día. Según el estudio de IDC "El universo digital en 2020", este año deberíamos tener alrededor de 40 billones de gigabytes de datos, es decir, 40 zetabytes. Un informe que también auguraba que el universo digital se duplicaría cada dos años hasta 2020.

Pero todo este volumen de información no deja de ser ruido salvo que se haga una buena gestión de los datos. ¿Cuántos datos se etiquetan y analizan? En 2012, solo se analizaba el 0,5% de los datos, mientras que el porcentaje de datos etiquetados era un poco más alto, con el 3%. Solo el 22% de todos los datos tenían el potencial de análisis. Esto incluye datos de diferentes campos como la vigilancia, el entretenimiento y las redes sociales, etc. Sin embargo, ya entonces se esperaba que para 2020 el porcentaje de datos útiles, es decir, la

información que tiene el potencial de análisis, aumentaría al 37%.

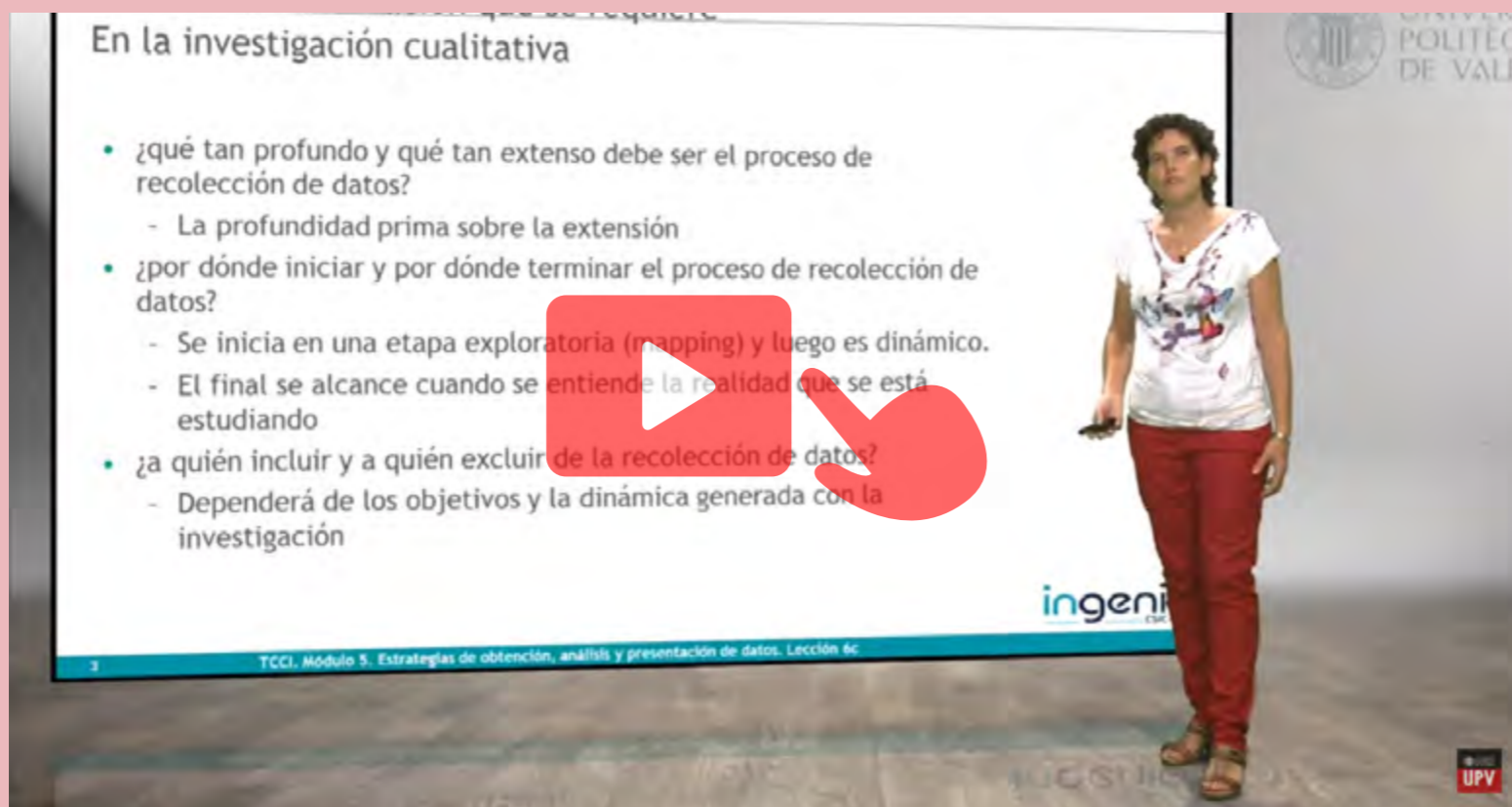
¿Dónde se realiza ese análisis? Algunas estadísticas de Big Data indican que más del 30% de los datos se cargan en la nube, lo que puede mejorar la agilidad de una empresa (en un 29%) y acortar los tiempos de recuperación en un 30%.

Parece claro que las empresas han empezado a ser conscientes del valor que se puede extraer de todo ese volumen de información que no dejamos de generar. Sin embargo, también es cierto que, según las estadísticas, aún queda mucho camino por recorrer para que las empresas estén realmente basadas en datos.

Por eso, el análisis predictivo se está volviendo cada vez más crucial para el éxito de los negocios. El 79% de los ejecutivos cree que no adoptar los grandes datos conducirá a la bancarrota. Esto explica por qué el 83% de las empresas invierten en proyectos de big data o que las compañías Fortune 1000 pueden obtener más de 65 millones de dólares de ingresos netos adicionales, solo aumentando su accesibilidad a los datos en un 10%. Pero una cosa son las empresas del Fortune y otra la realidad del día a día de los negocios locales.

EL PUNTO DE PARTIDA EN NUESTRO PAÍS

Sergio Blas Morente, IBM Analytics Software Leader, asegura que aunque ha habido un boom con el Big Data y los datos no estructurados, "actualmente, la mayor parte de los datos sobre los que



ESTRATEGIAS DE OBTENCIÓN, ANÁLISIS Y PRESENTACIÓN DE DATOS (UPV)



se siguen tomando decisiones en las empresas son estructurados. La excepción son las empresas nacidas en los últimos años, basadas en redes sociales". Además, augura que "cada vez se tendrán más y mejores datos de valor no estructurados en las empresas".

Fuentes de Huawei en España aseguran que la mayoría de las empresas en nuestro país tienen en su poder mucha información relevante para su negocio. "Tienen tanto dato estructurado como dato no estructurado, aunque aún el peso del negocio se pone sobre la información estructurada y previamente procesada en detrimento de aquella que no lo es".

Ana Manzanares, Business Development en Keeper Data Tech, tira de una encuesta de Gartner para afirmar que alrededor del 80% de los datos que poseen las compañías de hoy en día son desestructurados. "Entre ellos podemos encontrar desde emails o formularios con campos de texto libre, hasta documentos escaneados, pasando por toda una serie de información digital (imágenes, grabaciones de llamadas al call center, vídeos, etc.), que las empresas recogen fundamentalmente desde sus departamentos de transformación digital y atención al cliente. También hay una gran cantidad de datos provenientes de IoT, en este caso estructurados, procedentes, en su gran mayoría, de la industria 4.0, donde los procesos de manufacturing cobran gran importancia".

Pero para Gwendoline Huret, Global Technical Product Manager Secure Content Management Portfolio Micro Focus, habría que hablar de dónde está la mayoría de los datos y dónde la mayoría de los datos importantes o confidenciales, es decir, los datos "sensibles". "No siempre coinciden, y los datos sensibles son los que importan, a no ser que se trate simplemente de un proyecto de "limpieza" para reducir costes de almacenamiento". En su opinión, "aunque ahora están creciendo de forma exponencial los datos "no estructurados", es decir Outlook, Word, PDF, videos, llamadas, etc., los datos más cruciales para el negocio suelen seguir estando en las bases de datos de las apli-

caciones claves del negocio. Por eso, cuando se hace un proyecto de privacidad, la gran mayoría de las empresas empiezan con la gestión de los datos estructurados. En mi experiencia, depende mucho también de la geografía y del sector de la empresa. Los sectores públicos tienen más papel que los sectores privados por ejemplo. Y cada también cada cultura tiene más o menos tendencia a mantener procesos con papel. El papel y dato físico van desapareciendo, pero todavía queda una cantidad importante de datos en formato físico que también hay que gestionar, sobre todo al momento de la destrucción".

Así pues, quizá la pregunta a hacerse es si las empresas saben cuántos datos poseen o si la mayoría de ellos siguen sin ser etiquetados. "Esto va a

"Todavía hay trabajo por hacer, pero las empresas cada vez son más conscientes de que los problemas en el manejo de los datos pueden afectar a la toma de decisiones en el negocio"

**SERGIO BLAS MORENTE,
IBM ANALYTICS SOFTWARE LEADER**



depender de cada empresa”, afirma Juan Chinchilla, director de la Unidad de Negocio de Business Applications de Microsoft en España, para quien “lo ideal sería que todas supieran de la cantidad e importancia de los datos que poseen. El factor clave y diferencial reside en cómo gestionamos y usamos los datos que tenemos, y la mejor forma de hacer esto es a través de herramientas como el Big Data y la Inteligencia Artificial. Lo que ocurre es que existe un porcentaje de empresas que se pierden en el camino debido al desconocimiento, se cree que estas tecnologías son costosas y son difíciles de implementar y usar, lo que dista mucho de la realidad”.

Mar Montalvo, Directora de Desarrollo de Negocio de Big Data y Analytics, Oracle Ibérica, cree que “los datos estructurados están, en términos generales, muy bien controlados por las organizaciones. Y también hemos visto en los últimos años un gran crecimiento de la capacidad de las empresas para capturar y gestionar grandes volúmenes de datos de otras fuentes. Pero el desafío está en su aprovechamiento, en encontrar los mecanismos para extraer todo su valor y convertirlos en algo útil para el negocio”.

Por su parte, Jorge Pérez, Head of Platform & Technologies SAP España, pone como ejemplo a las empresas más valiosas del mundo, que “empiezan a ser conscientes de los datos que poseen, y también de todos los datos a los que pueden tener acceso. De su uso inteligente están surgiendo los modelos de negocio que es-

tán transformando nuestra visión del mundo. Es crítico para toda empresa y todo empresario tomar plena conciencia de que el activo más valioso con el que cuentan son los datos y de que es crítico tomar este parámetro como base para la definición de sus estrategias de negocio y de sus inversiones”. En su opinión, las barreras más relevantes hoy en día “proviene de dos aspectos muy diferentes. Por un lado, la presión regulatoria en cuanto al uso ético y legal de los datos y de los algoritmos, que limitan su uso a



**LOS DATOS NOS DAN SUPERPODERES -
Nagore de los Rios, TEDxLeon**





lo permitido por la normativa en vigor, que sigue siendo insuficiente e inmadura. Y por otro lado de las propias limitaciones técnicas de las empresas, tanto en infraestructuras como en conocimiento”.

LO DIGITAL VA POR BARRIOS

También hemos querido conocer si hay algunos sectores que estén más avanzados que otros en esto del aprovechamiento de los datos. Y podemos decir que en algunos casos sí.

El Head of Platform & Technologies SAP España asegura que todos los sectores están profundamente impactados por la revolución digital. “Aquellos cuyos modelos de negocio son más intensivos en datos, o más “digitalizables”, se han visto más impactados. Es el caso del sec-

tor financiero, los retailers, la manufactura de gran consumo o las telco. Pero están surgiendo realidades digitales paralelas en prácticamente todos los ámbitos de nuestra sociedad. La administración pública digital, la asistencia sanitaria, la utilización de gemelos digitales en multitud de actividades, como las relacionadas con la construcción, la gestión de infraestructuras, la manufactura discreta, el empleo masivo del IoT (Internet of Things) en todas las industrias...”, señala.

En su opinión, el gran potencial no lo determina el sector sino la creatividad “a la hora de reinventar modelos de negocio que hasta ahora no existían basándonos en la tecnología digital y su combinación con un número cada vez mayor de disciplinas. La banca gana hoy día más dinero con la venta retail que por comisiones, los nuevos modelos de comercio on-line y las redes están obligando a repensar los espacios físicos en función de la experiencia de los clientes. La economía colaborativa está transformando el paradigma en la utilización de activos como los inmuebles, o los

“Por desgracia estamos aun viendo cómo se siguen utilizando sistemas tradicionales para el tratamiento de datos que no lo son, lo que les impide aprovechar esos datos en tiempo y forma”

HUAWEI



medios de transporte. Los ejemplos son innumerables, y esto es lo relevante”.

Es decir, que como resume la directora de Desarrollo de Negocio de Big Data y Analytics de Oracle Ibérica, “hemos visto una gran concienciación y un gran avance en muchos sectores. Yo destacaría el sector financiero, el de telecomunicaciones, el retail y el turismo, por poner solo algunos ejemplos. En general, todo el mundo está apostando fuerte por el aprovechamiento de los datos y el grado de implementación depende más de un establecimiento de prioridades de negocio que de otra cosa”.

Juan Chinchilla también coincide en que cada día existen más empresas que le sacan todo el partido posible a los datos, “debido a la gran ayuda que prestan a la hora de adecuar las empresas a los clientes. Siempre se piensa en primera instancia en los bancos y las aseguradoras, pero existen ejemplos menos convencionales como, por ejemplo, las compañías que se dedican al calzado deportivo. La inclusión de acelerómetros o podómetros y la gestión de los datos que estos recogen pueden ser de gran ayuda para conocer cómo se desgasta el calzado y mejorarlo en consecuencia”. “Perso-



“Establecer una buena política de gobierno del dato hará que los procesos de inteligencia y analítica construidos alrededor de ellos sean fiables, seguros y precisos”

ANA MANZANARES, BUSINESS DEVELOPMENT EN KEEPLER DATA TECH



EL GOBIERNO DEL DATO Y LA EVOLUCIÓN DEL MODELO BANCARIO, ESIC DIGITAL THINKING

nalmente”, añade, “no diría que lo están desaprovechando, pero sí que diría que realizar un uso adecuado de los datos aumenta significativamente las posibilidades de las organizaciones. Se pueden llegar a convertir en una ventaja competitiva y aumentar de forma muy notoria la productividad. Sectores donde vamos a poder ver un mayor beneficio, tanto empresarial como para la sociedad, son, por ejemplo, el sanitario o el educativo”.

INDAGUEMOS EN LA GESTIÓN DE LOS DATOS

Parece, pues, que en términos generales podemos decir que las empresas de casi todos los sectores son conscientes de la importancia de los datos. Pero, ¿se está haciendo una buena gestión? ¿Se están utilizando las herramientas y aplicaciones apropiadas?

“No creo que haya aplicaciones correctas o no correctas”, explica la Global Technical Product Manager Secure Content Management Portfolio Micro Focus. “Lo importante es buscar aplicaciones que, cumpliendo las necesidades del negocio, tengan también un ROI evidente, o un coste de mantenimiento bajo. Lo ideal, para un proyecto de gestión de datos o de privacidad, es buscar un vendedor que tenga el portfolio o la solución más amplia, porque esto influye mucho en el tiempo de implementación y el coste de mantenimiento del proyecto. Cuando hablamos de gestión de datos, hablamos de gestionar muchas aplicaciones y datos de muchos formatos a la vez. Lo ideal es algo que lo pueda hacer todo,

para no tener soluciones de software que no se hablan entre sí. Lo que quiere un DPO o un data owner, es una vista universal de los datos de su empresa, y no 5 interfaces distintas para entender como su empresa está cumpliendo la GDPR o tratando datos sensibles”.

Por su parte, Ana Manzanares cree que si hablamos de la estrategia que tradicionalmente han seguido las empresas “todas las grandes corporaciones tienen un área de analítica tradicional (Business Intelligence) que lleva trabajando años en la analítica descriptiva y de diagnosis, apoyada en DWH corporativos. En base a esta información, el negocio puede realizar una toma de decisiones apoyada en datos y, la mayor parte de las

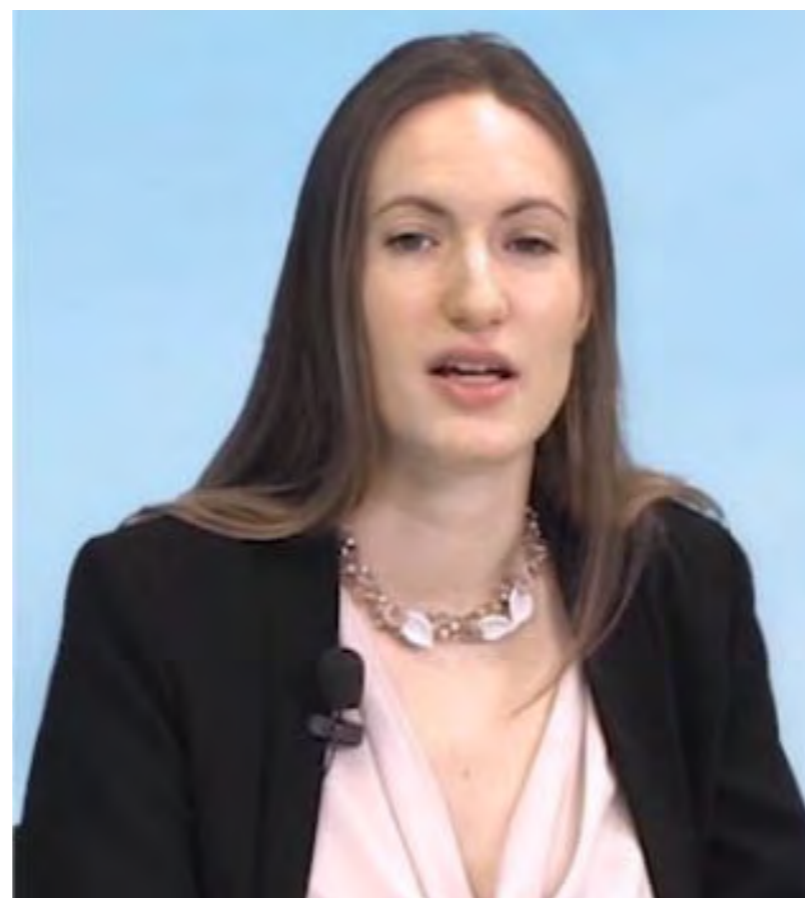


Data Governance

Data Governance es la capacidad que habilita a una organización a gestionar los datos de forma eficiente a lo largo de todo su ciclo de vida.

LOGICALIS

CICE: LA CALIDAD Y EL GOBIERNO DE LOS DATOS COMO VENTAJA COMPETITIVA



“Muchas empresas todavía no han llegado al estado de la implementación técnica, porque ni siquiera han logrado definir el proceso de gestión de dato que buscan”

GWENDOLINE HURET, GLOBAL TECHNICAL PRODUCT MANAGER SECURE CONTENT MANAGEMENT PORTFOLIO MICRO FOCUS



¿Te avisamos
del próximo
IT User?

veces, realizando acciones derivadas de esa descripción de la situación". Sin embargo, para poder sacar todo el partido a los datos, sobre todo en la era del Big Data en la que nos encontramos, "las grandes empresas están empezando a dar pasos en la dirección del Machine Learning o de la Inteligencia Artificial, apoyados fundamentalmente en las capacidades de almacenamiento y cómputo que ofrecen las plataformas de nube pública, que han sido uno de los grandes aceleradores de esta transición", señala la Business Development en Keeper Data Tech. "Así, encontramos compañías que gestionan las campañas hacia sus clientes a través de modelos de ML que predicen con una alta fiabilidad la probabilidad de fuga éstos, o que recomiendan un contenido digital o una prenda de ropa en función de nuestros gustos (aprendidos a través de nuestro historial de compra o navegación) u otras que realizan un mantenimiento predictivo de sus equipos o herramientas en base al comportamiento de cada una de las piezas que lo forman y no realizando revisiones periódicas cuando la condición es buena (evitando con ello generar un gasto recurrente)".

Mientras, fuentes de Huawei aseguran que "por desgracia" no todas las empresas están empleando las herramientas correctas. "Estamos aun viendo cómo se siguen utilizando sistemas tradicionales para el tratamiento de datos que no lo son, lo que les impide aprovechar esos da-

tos en tiempo y forma". La opinión de los expertos de Huawei es que una buena plataforma de Big Data "es la base para construir todo el ecosistema de gestión de datos. A su alrededor deben orbitar sistemas analíticos, sistemas de visualización de datos y por último sistemas que permitan implementar procesos de IA sobre esos datos, para optimizar los procesos de negocio de la empresa".

Desde IBM, Blas Morente señala que las organizaciones, en general, "tienen sistemas maduros de gestión de la información, con diferentes tecnologías y servicios" por lo que cree que el reto actual es "poder operacionalizar los sistemas, automatizarlos, y así conseguir tener un ROI claro con los datos". Para ello, pone un ejemplo: "muchas organizaciones están empezando a trabajar con soluciones de inteligencia artificial. Pero son pruebas en innovación o áreas usuarias que no están integradas con los sistemas informacionales de la compañía. Esto hace que sean complicadas de escalar, de integrar y de flexibilizar. No están teniendo el ROI necesario, ni la escalabilidad necesaria", explica.

LA IMPORTANCIA DE LA POLÍTICA

Es posible que antes de ver si se utilizan las herramientas adecuadas o no debamos ir a la base y saber si existe una política del dato que sustenten todo lo demás para poder maximizar el valor de la información.



“El factor clave y diferencial reside en cómo gestionamos y usamos los datos que tenemos, y la mejor forma de hacer esto es a través de herramientas como el Big Data y la Inteligencia Artificial”

JUAN CHINCHILLA, DIRECTOR DE LA UNIDAD DE NEGOCIO DE BUSINESS APPLICATIONS DE MICROSOFT EN ESPAÑA



Para el director de la Unidad de Negocio de Business Applications de Microsoft en España nos encontramos con el escenario de que hay una cierta cantidad de empresas que desconocen en qué punto del cumplimiento de la normativa con relación al uso de los datos se encuentran. “En Microsoft contamos con un proceso basado en cuatro fases que permite que cada organización pueda adoptar de manera rápida y cómoda las tecnologías necesarias. Este proceso se basa en servicios cloud”, e incluye cuatro puntos básicos: 1- Descubrir: “El objetivo de esta fase es identificar qué datos personales tiene la empresa, crear un inventario, así como identificar los sistemas donde se recopilan y almacenan”; 2- Administrar: “En esta fase, las organizaciones definen la gobernanza de los datos y la clasificación de éstos, así como la definición de políticas, roles y responsabilidades”; 3- Proteger: “Las empresas y entidades públicas deben establecer mecanismos para prevenir, detectar y responder a vulnerabilidades y violaciones de la información; y 4- Informar: “Las organizaciones deberán mostrar mayor transparencia en la forma en que controla los datos personales, así como garantizar que mantiene documentación completa sobre sus procesos y el uso de sus datos personales”.

Desde Oracle nos aseguran que todas las grandes organizaciones han designado Chief Data Officers o perfiles similares y “están implementando políticas de datos, que cubren tanto los

aspectos normativos y regulatorios, como la seguridad y la explotación de los datos para el negocio”. Además, Mar Montalvo declara que todas están abordando procesos para garantizar la unicidad del dato. “En una organización ideal, el mismo dato que se ha generado en una campaña de marketing, se utiliza en los análisis de planificación financiera, en las herramientas de ventas, en las órdenes que se emiten a los proveedores, en el plan de compensación del comercial que ha hecho la operación. Y es el “mismo dato”, no un dato que se replica en diferentes sistemas y aplicaciones, lo que podría acabar provocando divergencias. El matiz es importante. La base de un uso inteligente de la información está en que los diferentes sistemas de la empresa compartan recursos comunes, como los repositorios de datos, los sistemas

“Las empresas se han dado cuenta de que tienen que llevar la transformación basada en datos al corazón de sus organizaciones”

MAR MONTALVO, DIRECTORA DE DESARROLLO DE NEGOCIO DE BIG DATA Y ANALYTICS, ORACLE IBÉRICA



de seguridad, el control de accesos y gestión de identidades, etc.”, concluye.

Por su parte, el IBM Analytics Software Leader considera que las políticas de datos “han ido tomando cada vez más importancia dentro de las organizaciones, independientemente de su sector o tamaño. Todavía hay trabajo por hacer, pero las empresas cada vez son más conscientes de que los problemas en el manejo de los datos pueden afectar la toma de decisiones en el negocio”. En su opinión, hay una serie de puntos que son indispensables para que una organización sea realmente “data-driven”: Que los datos estén centralizados y organizados; Que exista una buena política de gobierno de datos (Data Governance) establecida, clara y alineada a todos los niveles; y Que la analítica esté integrada en las herramientas.

La Business Development en Keeper Data Tech recuerda que llevamos ya unos años viviendo en la era de la transformación digital y el Big Data y “la mayor parte de las empresas tienen o están trabajando en una buena política del gobierno y tratamiento del dato. Sin embargo, todavía queda camino por recorrer”. Para esta responsable, establecer una buena política de gobierno del dato, “donde se asegure el linaje y la calidad de este, así como el acceso, siempre basado en el principio de menor privilegio, hará que los procesos de inteligencia y analítica construidos alrededor de ellos sean fiables, seguros (cumpliendo con las leyes de protección de datos actuales) y precisos,

convirtiéndose en la principal palanca de toma de decisiones de los directivos”.

LA CULTURA Y OTROS OBSTÁCULOS

Tener una buena política del dato se sustenta, en muchas ocasiones, en una cultura empresarial que soporte y de cabida a todo lo relacionado con la estrategia del dato.

Gwendoline Huret cree que, aunque el presupuesto siempre es importante, “no es el mayor reto porque con la cultura actual se está dando importancia a la protección del dato. Recientemente en una reunión con muchos de nuestros clientes hice esta pregunta exacta, y la respuesta más frecuente desde luego fue que el reto más grande es entender al nivel del negocio y funcional qué es lo que se tiene que hacer”. Es decir, que muchas empresas “todavía no han llegado al estado de la implementación técnica, porque ni siquiera han logrado definir el proceso de gestión de dato que buscan. En este trabajo es útil saber que un vendedor tecnológico puede aportar mucho con su experiencia, y no es necesario tenerlo todo definido antes de empezar la conversación tecnológica, al contrario”.

Jorge Pérez, Head of Platform & Technologies SAP España, explica que muchas empresas siguen afrontando sus negocios como siempre lo han hecho. “Y todas tienen una sana intuición sobre la relevancia de la llamada Transformación Digital. No obstante, la gran mayoría hacen una aproximación reactiva a la cuestión de los datos



“El gran potencial no lo determina el sector sino la creatividad a la hora de reinventar modelos de negocio que hasta ahora no existían basándonos en la tecnología digital y su combinación con un número cada vez mayor de disciplinas”

JORGE PÉREZ, HEAD OF PLATFORM & TECHNOLOGIES SAP ESPAÑA



¿Te avisamos
del próximo
IT User?

y la Transformación Digital. Solo las más audaces tienen auténticas historias de transformación que se traducen en resultados empresariales impresionantes”.

Por eso, y citando a Peter Drucker, señala que principal problema que afrontan todas las empresas a la hora de ejecutar sus estrategias basadas en datos es “una falta de cultura en la organización y en los diferentes stakeholders sobre el valor del dato, y una gran dificultad en gestionar el ciclo completo de la información. Cuando hablamos de transformación, no hablamos de la introducción de cambios operativos sino de cuestionar los fundamentos de nuestro modelo

de negocio, de cómo vamos a nuestros mercados o cómo queremos atender a nuestros clientes. Transformarse significa cambiar quiénes somos y esto implica un profundo cambio cultural y entrar de lleno y sin reservas en el nuevo paradigma digital”.

Como resumen desde Huawei, “quizá el mayor problema sea la cultura del dato, que arrastra a modelos poco eficientes. Desde Huawei apostamos por un modelo donde los datos son el centro de la información, y ofrecemos servicios de almacenamiento y gestión de datos para optimizar su uso y su valor. Con ello queremos decir, que nuestras soluciones permiten que los datos

se mantengan almacenados en un único sitio, y que sean los servicios de las distintas capacidades de extracción, gestión, análisis, comprensión y visualización las que giren en torno a este dato. Por tanto, nos encontramos con el pensamiento erróneo de que esta información es poco útil, con la creación de silos por departamentos, con la utilización de sistemas traicionales muy caros y difíciles de gestionar y con el complejo proceso de encajar todas las piezas del puzzle”.

Pero la cultura no es la única gran barrera. La Directora de Desarrollo de Negocio de Big Data y Analytics, Oracle Ibérica cree que el problema de los silos ha sido uno de los más acuciantes para muchas organizaciones, “que tampoco pueden desprenderse de la información que lleva años en la organización. Hay que hacer una transición ordenada, estableciendo un sistema de gobierno y migrando, en función de las prioridades de negocio, hacia soluciones avanzadas en la nube, pues es en el cloud donde mejor se pueden integrar las herramientas y soluciones y aprovechar las ventajas de la economía de los datos en toda su extensión”.

QUIENES VAN POR DELANTE

Hablando de silos... casi todas las áreas de negocio dependen de los datos y su análisis para poder operar. Pero, ¿hay algunas que estén tomando la delantera?

“Marketing y Ventas son dos áreas que suelen adquirir esta conciencia del dato y nuevas



formas de explotarlo, quizás porque históricamente es algo que ya vienen haciendo, con técnicas o volúmenes de información con mayor o menor limitación”, explica Ana Manzanares, que también señala a Fraude o Customer Engagement como los que están a día de hoy

“en la cresta de la ola, aprovechando la información generada por los propios clientes para aprender de sus comportamientos y utilizarlos de vuelta para proporcionar mejores y más atractivos servicios o realizar una mejor criba de clientes”.

Además, “las áreas de Producción de empresas de manufactura también están aprovechando el Big Data para hacer más eficientes, más fiables y menos costosos sus procesos de producción y no cabe duda que en este área, a través del IoT y de la inminente aparición del 5G, será donde más ca-

Algunos casos de éxito

Hemos querido aprovechar para preguntarles a todos nuestros interlocutores por algunos casos de éxito que conozcan de empresas que estén haciendo un buen uso y gestión de sus datos.

Desde Microsoft hablan del proyecto del Hospital del Mar. “El centro es el primero de España que utiliza una herramienta de minería de datos para analizar y mejorar el seguimiento de los pacientes del Servicio de Nefrología”. Para ello utilizan una herramienta que emplea los servicios cognitivos de Microsoft Azure, para analizar los informes de alta de los pacientes. Así, es posible extraer de forma automatizada la información relevante contenida en los mismos y analizarla en su conjunto, permitiendo al personal sanitario extraer conclusiones de una

forma ágil y sencilla, que redundan en una mejora de la calidad asistencial.

Otro caso, de un sector completamente distinto, es el de la cervecera Carlsberg, que ya utiliza un método para crear nuevas fórmulas de cerveza basado en inteligencia artificial e Internet de las cosas (IoT, siglas en inglés). “La compañía danesa, que comercializa 140 productos distintos en 150 países, necesitaba generar nuevas propuestas a partir de la investigación química para mantenerse competitiva. Sin embargo, el proceso de creación de nuevas cervezas hasta ahora suponía un esfuerzo de tiempo importante, que gracias a la IA se ha reducido considerablemente. La cervecera emplea sensores avanzados y métricas de datos para no tener que probar litros y litros de cerveza antes

de decidir su comercialización. Se traza una huella del sabor para cada muestra y se reduce hasta un tercio el tiempo que se tarda en investigar sus diferentes combinaciones. De esta forma, la compañía puede obtener un mayor número de tipos de cervezas que pueden ser comercializadas más rápidamente”, añade Chinchilla.

Desde Keeper Data Tech nos hablan de uno de sus principales clientes, compañía energética global, que “ha conseguido mejorar sus procesos de manufactura gracias a la ingesta de datos, en tiempo casi real, de cientos de miles de sensores instalados en sus refinerías y al enriquecimiento de estos. Esta ingesta de datos crece cada mes incorporando al Data Lake más sensores y más fábricas continuamente. Esta ingesta en tiempo

casi real permite una monitorización por los analistas enfocada a optimizar los procesos productivos, identificando desviaciones de forma temprana. De forma adicional, permite que sistemas basados en aprendizaje automático detecten anomalías con el fin de realizar un mantenimiento predictivo sobre los equipos y evitar así la generación de un producto de mala calidad, que se tenga que vender en mercados secundarios con la consiguiente pérdida de beneficio, o la parada de la producción por el mal funcionamiento de uno de estos equipos monitorizados”.

Desde IBM aseguran estar ayudando a muchas empresas con las nuevas tecnologías. “En telecomunicaciones, por ejemplo, con asistentes virtuales que mejoran el ROI de los call >>

mino queda por recorrer". También hay otras que podrían transformarse si los emplearan, "áreas quizás menos involucradas directamente en Negocio pero igual de importantes en organizaciones grandes, como puedan ser RRHH o Finanzas, empiezan a apalancarse en el dato para su trans-

formación como parte de la transformación global de las compañías enfocadas en convertirse en Data-Driven, ya que la cultura del dato debe ser transversal a toda la organización para que sea efectiva. La primera lo utiliza para optimizar sus procesos de selección, para ser más preciso en la

contratación y acortar tiempos de reclutamiento; en el segundo caso, mejorando ratios de cobro, el control de gasto por parte de las distintas áreas, la rentabilidad de cada una de ellas...".

Mar Montalvo cree que la explotación de los datos ha comenzado tradicionalmente en las ac-

>> centers y ayudan al usuario final. En banca y finanzas con gestión del fraude, donde con motores y algoritmos en tiempo real se gestionan acciones frente a fraudes. En recursos humanos se está ayudando a la gestión del empleado, su formación personalizada, gestión de currículos, asistentes virtuales para los empleados. En general, las empresas se han dado cuenta de que pueden cambiar su mundo y el mundo en general gracias a los datos".

Oracle pone como ejemplo a empresas como Prosegur o Grupo Piñero, que "están abordando ambiciosos proyectos de transformación digital basadas en los datos. También están los ejemplos de Acerinox, que está transformando su cadena de suministros, la Autoridad Portuaria de la Bahía de Cádiz, que está desarrollando el concepto Puertos 4.0 de Puertos

del Estado con tecnología Oracle y muchos otros".

Desde Huawei aseguran trabajar con una amplia variedad de empresas, "que a su vez gestionan datos de sus clientes y necesitan unas plataformas que les permitan no solo seguir mejorando en los productos o servicios que venden, sino también mejorar cada vez más la experiencia de usuario y la seguridad. En este aspecto, y para poder continuar como una de las empresas líderes en I+D del mundo, utilizamos estos sistemas de análisis inteligentes para retroalimentar a los equipos de ingeniería con la información sobre el comportamiento de dichas plataformas. Esto nos permite mejorar las cadenas de diseño y fabricación, así como la seguridad de todo nuestro equipamiento y finalmente, la satisfacción de partners, clientes y la experiencia de usuario".

Mientras, desde SAP abordan casos como Airbnb, "ejemplo de redefinición de la utilización de activos en el sector turístico sin poseer ningún activo en sí. O el de Uber, la mayor compañía de taxis del mundo sin poseer ni un solo taxi. Y algunos ya vislumbramos una segunda oleada de disrupción de los disruptores. Piénsese por ejemplo cómo afectará a Uber la entrada en el negocio de la conducción autónoma, que puede volver a redefinir el modelo de negocio de transporte por carretera. Este mismo modelo de transporte por carretera basado en economía colaborativa como Uber, hiperflexibilizado en costes por la conducción autónoma cambiará los patrones de consumo del vehículo privado, reduciendo la demanda. Esto ya está afectando a toda la industria automovilística, y a su cadena logística hasta las propias

materias primas. Y a su vez este nuevo modelo de transporte por carretera cambiará drásticamente el modelo de infraestructuras y de carreteras e incluso el paisaje de nuestras ciudades".

Como resumen desde Micro Focus, "cuando permites a una organización de analizar a sus datos sin riesgo, no solamente quitas el riesgo si no que a la vez aumentas enormemente a la productividad. Por ejemplo: a la hora de compartir datos y trabajar con sus compañeros, no pierden tiempo pensando en la seguridad, ya que hemos quitado el riesgo del dato durante la "anonimización". En general, se puede mejorar mucho la productividad de una empresa cuando se cambia la forma de usar los datos. Y se puede reducir mucho también el coste de operación, simplemente con un trabajo previo de limpieza y retirada de aplicaciones antiguas".

tividades que estaban frente al cliente (el front office). “Nos referimos a proyectos piloto en las áreas de marketing, ventas y atención al cliente, principalmente. Pero hoy en día vemos que la transformación digital está ya en el back office. Las empresas se han dado cuenta de que tienen que llevar la transformación basada en datos al corazón de sus organizaciones. Hoy, todos los procesos de las empresas están interrelacionados e interconectados. Una campaña de marketing no termina en el momento en que se lanza a los clientes o se recopilan los datos sobre su efectividad. Ni siquiera termina cuando se produce una venta. Toda la información que se genera en ese proceso alimenta también los sistemas de

gestión financiera, planificación, cadena de suministro...”. En su opinión, “el hilo conductor de la transformación empresarial es el dato. Y, por ejemplo, los sistemas de gestión financiera (ERP/EPM) están cobrando una relevancia central en el proceso, así como las herramientas analíticas que permiten extraer todo su valor”.

Es decir, que todas las áreas están impactadas. “El área de ventas y marketing, por la gran capacidad que los datos nos dan de conocer a nuestros clientes y mejorar su experiencia con nosotros, es una de las áreas más impactadas y, además, con más impacto en el top line de la cuenta de resultados. La hiperconectividad, la nube, la telegestión y la robótica inteligente posibilitan también capacidades asombrosas de automatización en las operaciones, lo que implican importantes incrementos en la productividad e importantes reducciones de costes. Imaginemos cómo cambiará la conducción autónoma el modelo productivo del transporte por carretera. Imaginemos una automatización total de la función operativa de finanzas, qué significaría respecto del valor y la función operacional que el CFO debe tener en la empresa. Imaginemos el papel que puede jugar un Dpto. de Recursos Humanos al organizar todo un nuevo modelo digital de teletrabajo para una gran compañía en el contexto de la epidemia de coronavirus que estamos viviendo. ¿Hasta qué punto puede encontrar modelos de gestión que puedan desembocar en nuevas formas de entender las relaciones laborales y los importantes ahorros

¿Te gusta este reportaje?

Compártelo en redes



que se pueden generar para las empresas e incluso en la mejora de la calidad de vida de los trabajadores?”, se pregunta el responsable de SAP. “Cualquier área sufre una transformación radical cuando hace una reflexión profunda sobre cómo los datos pueden transformar su actividad, y probablemente tenga que redefinir completamente su modelo operativo, o incluso su función real”. ■

MÁS INFORMACIÓN

-  [Cinco elementos esenciales de una estrategia de datos](#)
-  [Diez claves para definir tu estrategia corporativa de gestión de datos](#)
-  [Desarrollando una estrategia de datos](#)
-  [Estudio sobre la gestión y explotación del dato](#)
-  [Libro para el desarrollo para la estrategia de datos](#)
-  [Una estrategia europea para los datos](#)





Digital Security



Todo lo que necesitas saber de Ciberseguridad está a un clic

Una propuesta informativa compuesta por una publicación digital, una página web para profesionales de la seguridad, así como Dialogos ITDS, Webinars o desayunos de trabajo con los principales referentes del sector... ¡¡¡Y no te pierdas nuestras entrevistas!!!

El fenómeno de la Industria 4.0 en 2020, a debate

Este mes en nuestra **#MesaRedondaIT** hemos querido analizar en qué estadio se encuentra el concepto de Industria 4.0 en España, en un año tan complejo como el que nos encontramos; cómo se pueden utilizar los datos de manera más inteligente en el IoT Industrial; si veremos ya este año una aplicación masiva del 5G en estos ecosistemas; en qué verticales el cambio de paradigma generado por la Industria 4.0 y el Internet de las Cosas Industrial (IIoT) está mejorando significativamente las capacidades digitales y de conectividad de sus Sistemas de Control Industrial; o cuáles son sus principales retos, como son, sin duda, las amenazas de ciberseguridad.

Y en esta ocasión nos han acompañado Alejandro Gómez, sales manager en Ekon; Galo Montes, director de Tecnología de HPE España; Gonzalo Valle, presales manager en IFS Ibérica; Borja Pérez, country manager de Stormshield España; y Luis Casero, field marketing director de Vertiv para España y Portugal, para debatir sobre cómo está evolucionando en Es-



it User
TECH & BUSINESS

#MesaRedondaIT

EL FENÓMENO DE LA INDUSTRIA 4.0 EN 2020, A DEBATE

paña el fenómeno de la Industria 4.0 este año.

Lo primero que quisimos saber es en qué punto se encuentra el desarrollo de Industria 4.0 en nuestro país. En palabras de Alejandro Gómez, “la Industria 4.0 sigue manteniendo la hoja de ruta que estaba preparada para este año y los que viene. Esta situación actual ha marcado un punto de inflexión para aquellos que antes lo trataban a alto nivel, y que ahora se dan cuenta de que necesitan un enfoque mucho más proactivo. Quizá, por tanto, esta situación ha motivado que algunos empresarios presten especial atención a lo que deben incorporar para evolucionar en el mercado”.

¿Te avisamos del próximo IT User?



Para Galo Montes, “veíamos una evolución muy clara en la que muchos clientes implantaban soluciones para la toma de datos y estos datos eran llevados a la nube, pero les estaba costando bastante obtener valor. Aplicaban algunos modelos probados en la industria, como el mantenimiento predictivo, por ejemplo, pero no estaban logrando tener una visión holística de toda su industria. Además, la incorporación de la imagen estaba siendo muy limitada, sin sacar todo el valor que podía llegar a obtenerse. Nosotros veíamos este año como un ejercicio en el que iba a haber una transformación sobre lo que se hacía hasta ahora. Primero, con una vuelta de datos desde la nube, porque estos empezaban a ser demasiados y la necesi-

dad de cálculo en la nube era muy elevado, lo que provocaba que el coste ya no fuera tan atractivo como inicialmente. Además, la incorporación de la imagen necesita mucha computación para sacar valor de ella. De todas formas, habrá que ver cómo evoluciona cuando volvamos a ponernos en marcha después de esta situación actual”.

En opinión de Gonzalo Valle, “la situación no es igual en todos los niveles y sectores. En las grandes empresas se ve que están avanzados, pero en las medianas y pequeñas están muy retrasados. Además, en muchos clientes observamos que tienen un núcleo tecnológico muy antiguo, lo que les impide avanzar rápidamente e incorporar las nuevas tecnologías que quieren incorporar. Nosotros estimamos que va a haber una renovación de sistemas para poder abordar los cambios

“Industria 4.0 sigue manteniendo la hoja de ruta que estaba preparada para este año y los que viene. La situación actual ha marcado un punto de inflexión para aquellos que antes lo trataban a alto nivel, y que ahora se dan cuenta de que necesitan un enfoque mucho más proactivo”



“Veíamos este año como un ejercicio en el que iba a haber una transformación sobre lo que se hacía hasta ahora, con una vuelta de datos desde la nube y un incremento de la incorporación de la imagen en muchos segmentos”

GALO MONTES, DIRECTOR DE TECNOLOGÍA DE HPE ESPAÑA



de Industria 4.0, porque, si no, en muchos casos, están limitadas. Observamos que en estos cambios se está pasando de una concepción de software de un solo proveedor, a software de varios fabricantes pero estándar, lo que incrementa las necesidades de integración”.

Se muestra de acuerdo Borja Pérez, que apunta que “es un sector heterogéneo, no sólo por su orientación, sino también hay diferencias en el mismo sector o, incluso, en un mismo cliente, que puede tener líneas 4.0 y otras, incluido el núcleo, 1.0. Esto es un reto importante, la convivencia de diferentes niveles de avances, con el riesgo de que muchas veces no se es consciente del nivel de conectividad de una industria al exterior”.

Finaliza esta primera ronda de opiniones Luis Casero, comentando que coincide con el resto, “en la industria española queda un gran camino por recorrer, y esto lo reflejan las cifras. Un informe de PcW, que mide el grado de digitalización de la industria, concluye que el 68% de las indus-

trias españolas tienen un grado de digitalización bajo o muy bajo. Le otorga un índice a la industria española del 43,6, frente al 43,3 de la media mundial. Estamos por encima de la media pero no en el lugar que correspondería a nuestra economía. Otro informe del Foro Económico Mundial, sobre el grado de preparación para el futuro, indica que España tiene un nivel de 6,3 sobre 10, lo que indica que quedan muchos pasos por dar todavía”.

“No podemos olvidar”, añade, “que el diseño del panorama industrial no estaba pensado para esta explosión de generación y uso de datos, por lo que hay que cambiar mentalidades y, sobre todo, tecnología para recoger y aprovechar todo este tipo de datos”.

APROVECHAMIENTO DE DATOS EN EL IOT INDUSTRIAL

Muchos de estos datos llegan de lo que ha venido en denominarse IoT Industrial. En este sentido, Galo Montes explica que “crear una visión

holística de todos los datos de la empresa es la única forma de obtener un valor añadido importante, pero esto exige una muy alta capacidad de computación y muchas personas obteniendo y analizando los datos. El gran límite que vemos actualmente es la falta de personal especializado en analizar estos datos, son perfiles caros y tienen un retorno no excesivamente alto. Solo el 10% de los proyectos que se inician en utilities producen verdaderamente valor. Vemos que empieza a haber herramientas que permiten hacer análisis rápida y económicamente. Puede que no sean análisis perfectos, pero se pueden ir actualizando. Pero, para ello, necesitamos contar con la infraestructura que nos permita gestionar estos datos de forma rápida. Y vemos que las empresas emplean tecnología de contenedores con herramientas automáticas de despliegue y análisis que te permitan crear proyectos rápidos sin grandes inversiones, y que puedan pararse de forma eficiente. Ahí estamos nosotros ha-



Gonzalo Valle
Presales Manager, IFS Ibérica

“A partir de este año, vamos a ver una aceleración de Industria 4.0, porque muchas empresas se han dado cuenta de que se juegan la supervivencia si se ven obligadas a parar”

GONZALO VALLE, PRESALES MANAGER EN IFS IBÉRICA

ciendo un gran esfuerzo para proporcionar plataformas de este tipo para permitir a los clientes hacerlo de forma optimizada”.

En este sentido, Gonzalo Valle explica que “vemos varias áreas donde se puede aprovechar. Una de ellas es en Calidad. Podemos ver cómo está siendo la producción, para poder encontrar posibles problemas que se produzcan, inspeccionando también lo que se ha producido. Otra área podría ser el mantenimiento, llegando a niveles óptimos de mantenimiento predictivo, que no tiene que darse desde el primer momento, sino que puede ser paulatino, garantizando, al principio, el nivel productivo de nuestros equipos y minimizando el posible sobremantenimiento. Una tercera área, podría ser ver cómo se usan sus productos para retroalimentar sus propios diseños, ver lo que usan y cómo los clientes, para mejorar con ello. Y otro ejemplo podría ser el pago por uso, ver el uso que se hace de las máquinas y

de los procesos para pagar por este uso, algo muy importante para ver los réditos y monetizar lo que estamos haciendo”.

Para Alejandro Gómez, “observamos que la mayoría de los clientes tienen la necesidad de buscar nuevas herramientas colaborativas. Hasta ahora, estaban acostumbrados a trabajar con información integrada y centralizada, pero ahora creemos que deben orientarse a entornos colaborativos, manejando toda la información necesaria y prestando mucha atención a dónde tiene esa información y de dónde obtenerla si no la tiene en su sistema. En entornos industriales vemos empresas que están empezando a implementar un sistema de obtención de información, hasta clientes a los que sus propios clientes les exigen toda la información relativa a la trazabilidad y a las condi-

ciones exactas del producto en todos los pasos del proceso. Para ello, tienen que enfrentarse a entornos colaborativos y de análisis de la información, tanto interna como de fuentes externas. Y el problema en muchos casos es que no ven claro el retorno, necesitan que les ayu-



Alejandro Gómez
Sales Manager, Ekon España

ENTREVISTA A ALEJANDRO GÓMEZ, DE EKON

“No todos los segmentos avanzan al mismo ritmo, pero lo más importante es que se acometen los proyectos y no siempre se tiene en cuenta la seguridad”

BORJA PÉREZ, COUNTRY MANAGER DE STORMSHIELD ESPAÑA

demos en esto, porque para ellos supone una gran inversión que deben aprovechar”.

Desde la perspectiva de Luis Casero, “hablamos mucho de tener datos para obtener valor, pero este valor no deja de ser ventajas competitivas para la empresa. Creo que hay dos vertientes a la hora de que estos datos generen valor. Por una parte, optimizando costes, reduciendo gastos, y, la otra, incrementando ingresos a partir de los datos obtenidos. La mentalidad de las empresas está más enfocada a la opción de costes en vez de la generación de ingresos, y creo que deberían ir más allá, y espero que tarde o temprano llegaremos a ellos, pero ahora no estamos ahí”.

EL IMPACTO DE 5G

¿Va a ser este el año del despliegue definitivo de 5G? ¿Será un impulsor del desarrollo de Industria 4.0? Para Borja Pérez, “si pensamos en la situación geopolítica, hemos visto la guerra comercial entre EE.UU. y China por esta tecnología, y cómo cambia ahora la foto con esta pandemia. Habrá que ver cómo queda la foto de proveedo-

res de 5G, pero no creo que vayamos a ver este año en industria este año, salvo proyectos piloto. No creo que lo veamos hasta 2021 o 2022”.

En la misma línea se sitúa Galo Montes, que comenta que a raíz del coronavirus “toda la industria va a parar en lo que se refiere a la implantación de proyectos 5G. Y hay dos frenos principales. Primero, no hay una cobertura global de 5G en las ciudades o en los entornos industriales, y, segundo, no encontramos una gran variedad de dispositivos capaces de tomar datos y enviarlos a través de 5G. Creo que queda año y medio o dos años hasta que veamos una implantación industrial de 5G”. Para Gonzalo Valle, “queda tiempo y, además, no va a ser una adopción generalizada. Actualmente hay diferentes tecnologías, en el caso de IoT, que cubren bien una serie de necesidades. Creo que 5G empezará a tener aplicaciones de nicho, y hasta 2022 o 2023 no va a tener una aplicación generalizada”.

En opinión de Luis Casero, “en esa fecha creo que veremos la implantación general de 5G. Acabará llegando, pero esta explosión en el envío de datos, va a necesitar habilitar una capacidad de alimentación eléctrica que en este momento no existe. Por tanto, a la falta de infraestructura 5G debemos sumar la necesidad de preparar la infraestructura eléctrica que permita alimentar todo ello”.



ENTREVISTA A GONZALO VALLE, DE IFS



“Un informe del Foro Económico Mundial, sobre Industria 4.0 y el grado de preparación para el futuro, señala que España tiene un nivel de 6,3 sobre 10, lo que indica que quedan muchos pasos por dar todavía”

LUIS CASERO,
FIELD MARKETING DIRECTOR DE VERTIV PARA ESPAÑA Y PORTUGAL

ALGUNOS SEGMENTOS QUE MARCAN EL RITMO

¿En qué áreas o verticales se está viendo un mayor ritmo de implantación? Para Gonzalo Gómez, “en los sectores que normalmente operamos, es algo notorio en automoción, aeronáutica, en el sector agroalimentario pero desde un punto de vista más de marketing... pero en los últimos proyectos no estoy notando tanta intensidad hacia el ahorro de costes, sino más inquietud para ver otras formas de aportar valor. Siempre se ha hablado de la diferencia entre la visión tecnológica de un empresario español y otro inglés, de cómo llegaban las novedades y cómo los ingleses optaban por una integración rápida para buscar ventajas competitivas, mientras que los españoles preferían no integrarlo hasta ver referencias reales de uso. Pero esto ha cambiado. Creo que

ahora seguimos un plan de ruta definido. Vamos por detrás de otros países, pero sí hay una conciencia en los empresarios de este país”.

En palabras de Gonzalo Valle, “vemos implantaciones y desarrollos en áreas como el reconocimiento de imágenes, algo que vemos en automoción, en alimentación, en el sector sanitario, en sistemas distribuidos geográficamente... y otro área donde vemos más desarrollo en los centros productivos externos, como plataformas petrolíferas, parques de energía eólica o solar... donde hacen uso de los datos

para mantener los niveles de producción”. Desde el punto de vista de Borja Pérez, “nosotros tenemos el foco en un aspecto muy concreto de la Industria 4.0: la ciberseguridad. Pero coincido con ambos en los sectores que van avanzando más. Hay veces que se acometen los proyectos y no siempre se tiene en

cuenta la seguridad. Vemos grandes avances en aeronáutica, Defensa...”.

Añade Luis Casero que “todo lo que tiene que ver con la digitalización es muy horizontal. Afecta a muchos verticales. Me llama la atención la digitalización de la cadena logística, algo que afecta a muchos verticales”.

Finaliza esta ronda de opiniones Galo Montes mostrándose de acuerdo con el resto de interlocutores, y añadiendo que “estamos viendo una gran introducción de la imagen en Industria 4.0, sobre todo en industria básica y en Utilities, tanto para gestionar su producción como para interactuar con los clientes. Vamos a vivir una explosión brutal de todo lo relacionado con la imagen”.

¿Y LA SEGURIDAD?

Evidentemente, con estos desarrollo aparecen nuevos riesgos para la seguridad. Tal y como explica Borja Pérez, “ataques tenemos todas la semanas, pero algunos se conocen pública-

¿Te avisamos del próximo IT User?



mente y otros no. Hay muchos casos en los que la empresa cree tener una línea aislada, pero resulta que OT e IT están conectados, por ejemplo, a través del ERP, o los PLC que se están manteniendo de forma remota... o como en el caso de una refinería que se dio hace un par de años, que el ataque llegó a través de una máquina de café conectada al exterior. Las conexiones desconocidas pueden ser un problema

para las empresas". A la hora de securizar estos entornos, continúa, "es necesario conocer los procesos y las necesidades de estos. Por ejemplo, hay que tener muy en cuenta las latencias, las paradas deben ser programadas... prima la continuidad de la producción sobre la seguridad. En resumen, la realidad es diferente, pero algunas estrategias pueden ser replicables de IT a OT". ■

Conclusiones

A modo de conclusión, en palabras de Alejandro Gómez, "esto es una corriente imparable, y en muchos casos son los propios clientes de las empresas los que lo van a demandar. EL I+D va a tener que evolucionar, porque la seguridad de los datos y su aprovechamiento es vital para las empresas".

Para Galo Montes, "la seguridad es fundamental, y no siempre se pone el interés que se debería; hay que minimizar los riesgos financieros, estandarizando modelos de pago por uso; vemos una vuelta de la nube, por la cantidad y coste

de gestionar los datos; y vemos que las empresas se están tomando muy en serio la digitalización, y la situación actual es un claro ejemplo, con incremento muy importante de las soluciones de teletrabajo".

En opinión de Gonzalo Valle, "hay que luchar para mantener la apuesta por los niveles de calidad, de la seguridad... desde el comienzo de los proyectos, y esto es algo del mundo IT que tiene cabida en el mundo OT. Además, creemos que, a partir de este año, vamos a ver una aceleración de Industria 4.0, porque muchas empresas

se han dado cuenta de que se juegan la supervivencia si se ven obligadas a parar por situaciones como la actual".

Finaliza Luis Casero señalando dos elementos. "Primero, para una plena digitalización es necesario que la infraestructura crítica se desarrolle como tiene que ser. Si todas las empresas españolas se digitalizaran, la red eléctrica no podría soportar todos los dispositivos y procesos necesarios. Segundo, el reto está en la dificultad para encontrar talento para interpretar y analizar los datos".

¿Te gusta este reportaje?

Compártelo
en redes



MÁS INFORMACIÓN



[El fenómeno de la Industria 4.0 en 2020, a debate](#)



[¿Quieres saber cuál es la propuesta de Ekon en Industria 4.0?](#)



[¿Quieres saber cuál es la propuesta de HPE en Industria 4.0?](#)



[¿Quieres saber cuál es la propuesta de IFS en Industria 4.0?](#)



[¿Quieres saber cuál es la propuesta de Stormshield en Industria 4.0?](#)



[¿Quieres saber cuál es la propuesta de Vertiv en Industria 4.0?](#)



TECNOLOGÍA Y NEGOCIO

**Investigación tecnológica
contra el coronavirus**

Jorge Díaz-Cardiel,
socio director general de
Advice Strategic Consultants



**ENCUENTROS Y DESENCUENTROS
CON LA COMUNICACIÓN**

**Y si no tengo nada que
comunicar, ¿qué hago?**

Manuel López,
asesor de comunicación



MARKETING Y CONSUMO

La catarsis de la tecnología

José Manuel Navarro,
CMO MOMO Group



LEGAL IT

**El derecho de ocupación de la
propiedad privada y despliegue de
redes físicas, según la normativa (I)**

Juan Pedro Peña,
Asesor jurídico TIC



CIBERSEGURIDAD 4.0

**Estado de alarma digital:
limitación de los derechos digitales
individuales**

Mario Velarde Bleichner,
Gurú en CiberSeguridad



MEJORANDO LAS TI

**¿Qué nos aporta esta crisis
para nuestro liderazgo?**

Javier Canal,
director de GO4aVision

Investigación tecnológica contra el coronavirus

Los gigantes tecnológicos de Estados Unidos se han unido a la Casa Blanca en un grupo de trabajo para combatir el nuevo coronavirus, a medida que Silicon Valley intensifica sus esfuerzos para hacer frente a la pandemia.

Las compañías TI más relevantes de USA, incluidas Facebook, Google de Alphabet, Microsoft y Amazon.com, realizaron el domingo 15 de marzo una reunión de casi una hora con funcionarios de la Casa Blanca, incluido Michael Kratsios, director de tecnología de EE.UU. Según una persona presente en la reunión, el número de asistentes fue 45, representantes del más alto nivel de las empresas TI norteamericanas.

Entre los temas: cómo se podría diagnosticar a los ciudadanos sin visitar a un médico, y cómo las empresas podrían trabajar con los Centros para el Control y la Prevención de Enfermedades en sus principales prioridades, de acuerdo con una agenda establecida.

El Grupo de Trabajo de Tecnología e Investigación es parte de un amplio impulso por parte de compañías tecnológicas grandes y pequeñas en todo



Jorge Díaz-Cardiel

Socio director general de
Advice Strategic Consultants

Economista, sociólogo, abogado, historiador, filósofo y periodista. Autor de más de veinte mil de artículos de economía y relaciones internacionales, ha publicado más de una veintena de libros, cinco sobre Digitalización. Ha sido director de Intel, Ipsos Public Affairs, Porter Novelli International, Brodeur Worldwide y Shandwick Consultants.



NO SOLO



Tecnología y negocio

Silicon Valley para encontrar formas de resolver la miríada de problemas relacionados con la rápida propagación del coronavirus. Las compañías tecnológicas están compitiendo para descubrir todo, desde por qué tan rápido se está propagando el virus, hasta predecir cuántas camas de hospital estarán disponibles en un momento dado.

El grupo de trabajo comenzó hace aproximadamente dos semanas, pero sus esfuerzos han adquirido mayor urgencia en los últimos días, incluso después de una reunión que algunos ejecutivos de tecnología tuvieron con funcionarios de la Casa Blanca hace unos días, dicen estas personas. "Ya ha empeorado", dijo una de las personas involucradas en el esfuerzo. El grupo de trabajo es distinto del grupo de ejecutivos que habló en primer lugar con funcionarios de la Casa Blanca.

El presidente ejecutivo de Amazon, Jeff Bezos, quien en el pasado tuvo una relación difícil con el presidente Trump, es uno de los principales ejecutivos de tecnología que está en contacto con la Casa Blanca, seguramente porque va a recuperar la mitad del mayor contrato de cloud computing de la historia, primero otorgado a Microsoft y ahora dividido entre ambas compañías.

SILICON VALLEY EMPUJA INICIATIVAS CONTRA CORONAVIRUS

Fuera de los esfuerzos del grupo de trabajo, Ron Conway, uno de los "business angels" más conocidos en Silicon Valley, ha estado pidiendo a los



ejecutivos de tecnología, otros inversores y legisladores, que recauden dinero para la investigación y los esfuerzos de la comunidad científica, en particular los de la Universidad de California, San Francisco (UCSF), que está ejecutando un Fondo de Respuesta Covid-19, recaudando dinero para ampliar la capacidad de diagnóstico y pruebas, así como asegurando la vivienda necesaria para los pacientes.

"Estoy orgulloso de contribuir a este esfuerzo crítico junto con otros líderes tecnológicos que algún día salvarán millones de vidas aquí en los Estados Unidos y en todo el mundo", escribió el Conway en un discurso por correo electrónico. Dijo que hasta ahora ha recaudado alrededor de 5 millones de dólares en dos semanas.

Sam Altman, quien dirigió el famoso acelerador de startups Y-Combinator de Silicon Valley, publicó en Twitter y su blog el domingo 15 de marzo que quiere financiar más empresas nuevas que ayuden a combatir el virus porque "es básicamente lo único que sé hacer que puede ayudar."

Altman publicó una hoja de cálculo en la que otros podían escribir sus ideas de nuevas empresas para financiar y rápidamente incluyeron más de tres docenas de compañías.

"Silicon Valley ha querido que el gobierno tome esto en serio por un tiempo", dice Altman. "Todavía pienso que una estrategia agresiva de contención sería genial. Pero dado que eso no sucedió lo suficientemente rápido, debemos pensar en el Plan B".

Una de las compañías en las que invirtió Altman es Helix Nanotechnologies, con sede en Cambridge, Massachusetts. Durante los últimos dos años ha estado trabajando en una nueva vacuna contra el cáncer, pero el martes el equipo se reunió por videoconferencia y decidió usar la tecnología que están desarrollando para combatir el coronavirus, como están haciendo en España La Caixa a través de IrsiCaixa, tras su investigación en la lucha contra el sida y la Clínica Universidad de Navarra a raíz de sus décadas de experiencia en la investigación para combatir el cáncer.

Las vacunas tardan un tiempo en desarrollarse y esperan poder crear una que combata las diferentes mutaciones del coronavirus que podrían surgir el próximo año. Para ayudar a acelerar el nuevo esfuerzo, Altman y otros patrocinadores anteriores de la compañía están invirtiendo más dinero, dijo Hannu Rajaniemi, cofundador y CEO de Helix: "¿Qué pasa si el Covid-19 estacional vuelve cada año y puede ser mucho más letal? Necesitamos protección a largo plazo".

Parte de los esfuerzos del sector tecnológico proviene de la frustración de algunos ejecutivos

sobre la lentitud del gobierno de los Estados Unidos para reaccionar, o la irritación por lo aparentemente al azar que han tenido lugar algunas acciones para combatir el virus en todo el país.

Navegar por las complejidades de las grandes empresas tecnológicas también puede ser un desafío. El esfuerzo de la fuerza de trabajo fue provocado en parte por Josh Mendelsohn, socio gerente de Hangar Ventures, una firma de capital de riesgo con sede en Nueva York. Mendelsohn había trabajado anteriormente en Google, gestionando su equipo de respuesta a desastres.

La respuesta de la industria TIC también sigue a una conferencia de prensa del viernes 13 de marzo en la que Trump pareció exagerar una iniciativa de Google para construir un sitio web que ampliaría las pruebas para detectar el virus. Dijo que el gigante de la búsqueda tenía 1.700 ingenieros trabajando en el proyecto y que habían hecho "un progreso tremendo".

Los comentarios del presidente llevaron a una confusión generalizada dentro de Google, dijeron

¿Te avisamos del próximo IT User?

los empleados, donde los ingenieros hicieron publicaciones burlonas en los tableros de mensajes internos sobre el proyecto y las promesas de Trump. En realidad, la unidad Alphabet Verily de Google se encuentra en las primeras etapas de un

proyecto piloto en conjunción con las autoridades de California para ayudar a establecer sitios de prueba en el Área de la Bahía de San Francisco y construir una herramienta online para aumentar la detección y pruebas para personas con alto riesgo, según una publicación del CEO de Alphabet, Sundar Pichai en su blog, el pasado domingo 15 de marzo.

INVESTIGACIÓN EN ESPAÑA

En España hemos visto cómo empresas tecnológicas (Microsoft, por boca de su director de comunicación y desarrollo corporativo, Carlos de la Iglesia) prometen compromiso con la sociedad española en la lucha contra coronavirus. Y Telefónica ofrece 30 GB gratis de datos a sus clientes de Movistar Fusión, cada mes durante dos meses. Se supone que las infraestructuras de telecomunicaciones (la fibra óptica de Telefónica, mayor que la tendida en el resto de los países europeos juntos; la inalámbrica de Cellnex Telecom, líder europeo por número de torres y emplazamientos...) españolas deberían soportar el incremento de tráfico en la red que se está produciendo. Aunque esto no es lo más importante. A no ser que hablemos

La carrera contrarreloj por conseguir una vacuna contra coronavirus une, bajo el paraguas de la Fundación Bancaria La Caixa, a IrsiCaixa, al Centro Nacional de Supercomputación, al MIT y laboratorios y hospitales pioneros en investigación

del intercambio de información médica entre científicos, investigadores y médicos.

La carrera contrarreloj por conseguir una vacuna contra coronavirus une, bajo el paraguas de la Fundación Bancaria La Caixa, a IrsiCaixa, de la Obra Social de La Caixa, al Centro Nacional de Supercomputación, al Instituto Tecnológico de Massachusetts (MIT) y laboratorios (Merck) y Hospitales pioneros en investigación en la búsqueda de vacunas contra virus pandémicos.

El Instituto de Investigación del Sida IrsiCaixa es un instituto de referencia internacional, líder en la investigación para la erradicación del VIH/sida y las enfermedades relacionadas. La investigación que lleva a cabo afronta también otros retos de la

biomedicina actual, como el estudio del microbioma o de las enfermedades infecciosas emergentes, como coronavirus: la supercomputación ayuda a la provisión de ingentes cantidades de datos.

La fundación IrsiCaixa mantiene una constante colaboración científica con los Institutos Nacionales de Salud de Estados Unidos (NIH), el Instituto Tecnológico de Massachusetts (MIT) y la Universidad de Harvard, la Universidad de Oxford, el Instituto Médico Howard Hughes, el Instituto Pasteur de París, el Scripps Research Institute, el Instituto de Salud Carlos III (ISCIII).

Un fármaco para la malaria y la artritis reumatoide y un antiviral de los que se usan frente al VIH podrían ser un freno a los contagios de

coronavirus. No pretende curar la enfermedad en su manifestación más grave, sino frenar los contagios de una forma sencilla y asequible. Y colaborar así en acortar el confinamiento. La propuesta llegó hace un par de semanas al Departamento de Salud de Cataluña por parte de Oriol Mitjà, el infectólogo que saltó a la fama al encontrar una solución factible para evitar el piau en Papúa Nueva Guinea, y Bonaventura Clotet, director de IrsiCaixa (Fundación Bancaria La Caixa, a través de la Obra Social La Caixa) de la lucha contra el sida, en el hospital Germans Trias.

El ensayo se ha aceptado rápidamente por las partes implicadas, incluida la Agencia del Medicamento, y empezó el lunes 16 de marzo: lo van a probar 199 personas positivas al coronavirus, que tomarán el combinado durante siete días, y



Ojalá que los esfuerzos del sector TIC y el de entidades que se dedican a la investigación médica, como IrsiCaixa de La Caixa, para desarrollar vacunas contra el coronavirus den fruto muy pronto

NO SOLO



Tecnología y negocio

sólo el de la malaria un total de 2.850 contactos, durante 4 días. El Instituto de Investigación del Sida IrsiCaixa es un instituto de referencia internacional, líder en la investigación para la erradicación del VIH/sida y enfermedades relacionadas. La investigación que lleva a cabo afronta también otros retos de la biomedicina actual, como el estudio del microbioma o de las enfermedades infecciosas emergentes, de ahí que esté investigando en la lucha contra coronavirus.

Es un modelo de investigación colaborativa, impulsado por la "Fundación Bancaria La Caixa" y el Departamento de Salud de la Generalitat de Cataluña. IrsiCaixa se constituyó en 1995 como fundación privada sin ánimo de lucro y su director es el antes citado doctor Bonaventura Clotet, que también es presidente de la Fundación Lucha contra el Sida y jefe del Servicio de Enfermedades Infecciosas del Hospital Universitari Germans Trias i Pujol de Badalona.

IrsiCaixa está ubicado en el entorno de estas dos instituciones, lo que permite un modelo

único de colaboración entre investigadores, profesionales asistenciales, pacientes y representantes de la comunidad. Esta transferencia de conocimiento entre los actores sociales implicados en permite aportar soluciones y facilitar los avances hacia la erradicación de la infección.

Cuántas veces nos acordamos de Santa Bárbara cuando truena. Nos pusimos a buscar quién estaba, en España -en el caso que hubiera alguien, entidad pública o privada- investigando, para encontrar una vacuna, un medicamento contra coronavirus y contrarreloj. Puesto que nuestra especialidad es la economía y la empresa, y no la medicina, dimos con La Caixa porque "Fundación Bancaria La Caixa" es la entidad privada de España que más invierte en el avance de la investigación médica, con 42 millones de euros invertidos en 2019.

Ojalá que los esfuerzos del sector TIC y el de entidades que se dedican a la investigación médica, como IrsiCaixa de La Caixa, para desarro-

¿Te gusta este reportaje?

Compártelo en redes



llar vacunas contra el coronavirus den fruto y muy, muy, muy pronto. Nos jugamos mucho en vidas humanas, sufrimiento, dolor y otras consideraciones más allá de las emocionales, pero que, al largo plazo, tienen un impacto brutal, como una depresión económica como la de 1929, según nos apuntan los economistas norteamericanos más reputados. ■



MÁS INFORMACIÓN



[IrsiCaixa](#)



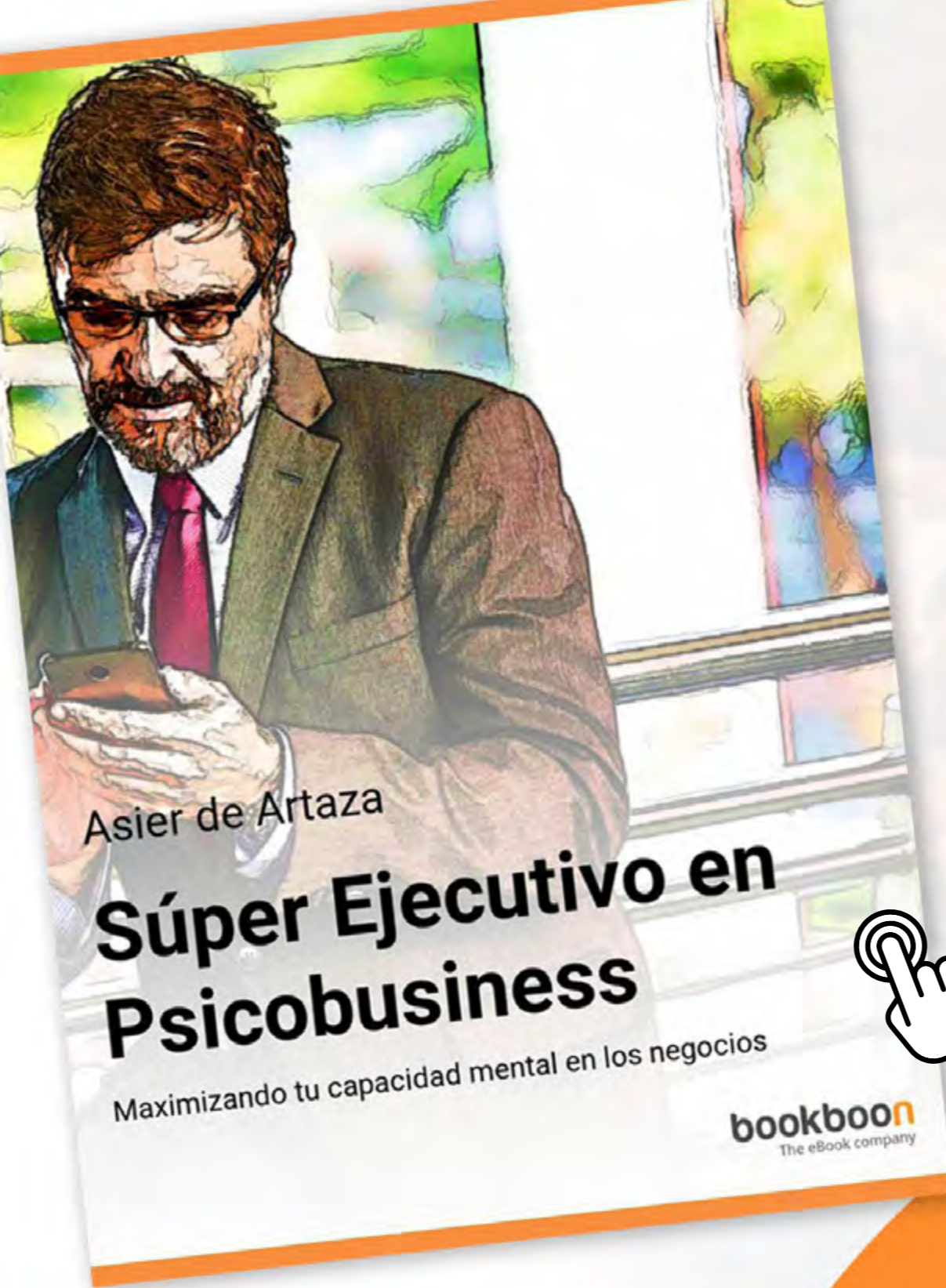
[Verily](#)



IMPRESIÓN 3D, TENDENCIA DE PRESENTE, NEGOCIO DE FUTURO

Si en algo se ponen de acuerdo las consultoras cuando hablan de presente y de tendencias de futuro es que la impresión 3D no es flor de un día, y que los pasos que se han ido dando hasta la fecha han consolidado sus capacidades para un mañana que muestra un crecimiento explosivo en base a una ampliación de los proveedores, pero, sobre todo, gracias a la aparición de casos de uso en un mayor número de sectores y negocios.





Súper Ejecutivo en Psicobusiness

Maximizando tu capacidad mental en los negocios.

El nuevo libro de **Asier de Artaza** y primera publicación sobre el **Psicobusiness** a nivel internacional, **¡ya está disponible!**



Adquiérelolo a través de:
bookboon.com

La editorial digital más grande del mundo.

“He compilado para ti esos aspectos que han ayudado a los mejores ejecutivos a ser más eficaces, productivos y a dejar atrás la ansiedad y el estrés”.

-Asier de Artaza

NO SOLO



Encuentros y desencuentros con la Comunicación

Y si no tengo nada que comunicar, ¿qué hago?

En la vorágine diaria de una startup, hay demasiadas tareas que realizar, preocupaciones que soportar y problemas que resolver. En medio del maremágnum que significa sacar adelante una startup, se suele tener la tendencia a dejar de lado, procrastinar es la palabra de moda, aquello que tienes más dificultad, o nos aporta menos valor... o eso pensamos. En las startups, la comunicación suele ser una de esas cosas tediosas que siempre se pone la



Manuel López

Asesor de comunicación



Madriileño de nacimiento, horchano de adopción, informático de profesión, con más de 35 años de experiencia en el sector de TI, ha desarrollado la mayor parte de su carrera profesional en Hewlett-Packard, donde ocupó cargos de responsabilidad en diferentes áreas como consultoría, desarrollo de negocio, marketing, comunicación corporativa o PR. Actualmente dedica la mayor parte de su tiempo a asesorar a startups en temas relativos a la comunicación, desde su posición de partner en la plataforma de profesionales goXnext.



primera en las actividades que se dejan para otro momento. La batería de excusas para procrastinar es casi infinita: no hay tiempo, no es importante en este momento, no tengo recursos, es perjudicial ahora...

Hoy quiero centrarme en la excusa final, cuando ya has desmontado una por una todas las excusas que te plantean. La excusa final es: "no tengo nada que comunicar". Y a partir de aquí las coletillas: porque no es el momento, porque tenemos este riesgo o aquel otro, porque el cliente x me ha dicho que..., porque tengo un viaje, porque...

Hablando en el lenguaje de esta serie de artículos, a la mínima dificultad que aparece, llega el desencuentro con la comunicación, cuando debería ser lo contrario, debemos encontrarnos con la comunicación como parte de la solución de los problemas y no como la primera tarea que apartamos.

Si somos capaces de convencernos que la comunicación nos va a ayudar y va a ser parte de la solución y no del problema en cualquier circunstancia, estamos en disposición de que la comunicación aporte el valor necesario para ayudar al negocio de la startup.

Llegado este punto y teniendo en cuenta de que venimos desde un posicionamiento negativo (no tengo nada que comunicar), debe-

Si somos capaces de convencernos de que la comunicación nos va a ayudar y va a ser parte de la solución y no del problema en cualquier circunstancia, estamos en disposición de que la comunicación aporte el valor necesario para ayudar al negocio de la startup

mos ser muy precavidos en cómo abordamos la comunicación. No quiero centrarme ahora en aspectos técnicos de la comunicación: qué mensaje, a quién, por qué medio... sino en la parte emocional para gestionar la comunicación. Y es que la inteligencia emocional juega un papel importantísimo en la gestión de la comunicación en casos como el que describo aquí.

Entonces, ¿cuál es mi recomendación? Se resume en una palabra: Prudencia.

No quiero decir que la prudencia lleve a decir que es más prudente no comunicar o comunicar "en vacío" para no generar problemas.

Quiero decir que la prudencia controle las emociones. Y me explico.

Cuando llegamos a una situación difícil en la que estamos en dificultades y creemos que comunicar es lo último que debemos hacer y alguien (normalmente un asesor de comunicación), nos convence de lo contrario, la parte emocional

de nuestro cerebro suele actuar a la ofensiva y nos lleva a exagerar, es decir a lanzarnos de forma desenfrenada a enviar grandes titulares, anuncios imposibles, negocios inexistentes, grandes estrategias, maravillosas soluciones a problemas...

En mi vida profesional, cuando me he encontrado en situaciones como esta, siempre he recurrido al consejo de los sabios. En mi caso, en los años 90 mi compañía de siempre, Hewlett-Packard, invirtió mucho en mi formación en lo que hoy se llama "soft skills" y tuve la oportunidad de asistir a muchos seminarios sobre gestión de emociones, solución de problemas, autoconocimiento y muchas otras cosas interesantísimas. Por esa época y en ese entorno de desarrollo, me tope con una de las personas que más ha influido tanto en mi vida personal como profesional. Nació en 1601 y se llamó Baltasar Gracián. Gracián publicó en 1647 por primera vez un compendio de aforismos que tituló "El arte de la prudencia". Desde que un

¿Te avisamos del próximo IT User?



NO SOLO



Encuentros y desencuentros con la Comunicación

gran amigo me regaló ese libro (allá por 1994, como reza la dedicatoria que me hizo), ha sido compañero fiel de mi vida y, sobre todo, consejero al que acudir cuando lo he necesitado.

Volviendo al problema que nos ocupa, dejemos que Baltasar Gracián nos ayude a generar valor en la situación descrita. Permitidme que reproduzca el aforismo nº 41:

NUNCA EXAGERAR

Es importante para la prudencia no hablar con superlativos, para no faltar a la verdad y para no deslucir la propia cordura. Las exageraciones son despilfarros de estima y dan indicio de escasez de conocimiento y gusto. La alabanza despierta vivamente la curiosidad, excita el deseo. Después, si no se corresponde el valor con el precio, como sucede con frecuencia, la expectativa se vuelve contra el engaño y se desquita con el desprecio de lo elogiado y del que elogió. Por eso el cuerdo va muy despacio y prefiere pecar de corto que largo. Lo exce-

lente es raro: hay que moderar la estimación. Encarecer es una parte de la mentira. Por esto se pierde la reputación de tener buen gusto y, lo que es más grave, la de ser entendido.

La sabiduría que encierra este aforismo es muy grande. Para el caso que nos ocupa, yo lo resumiría en los siguientes puntos:

- ❖ La comunicación nunca debe exagerar la realidad.
- ❖ La comunicación nunca debe faltar a la verdad.
- ❖ La comunicación debe equiparar valor y precio.
- ❖ Si exageramos, la expectativa que genera puede volverse en nuestra contra.
- ❖ Si exageramos podemos llegar a no ser entendidos.

Podríamos seguir extrayendo conclusiones sobre las enseñanzas que podemos sacar de este aforismo, pero eso os lo dejo para vosotros.

Como conclusión, respondo a la pregunta inicial: Si no tengo nada que comunicar, ¿qué hago?

¿Te gusta este reportaje?

Compártelo en redes



La respuesta es simple, aunque nada sencilla de hacer realidad: Comunica con Prudencia

Y en esto es en lo que estamos: Encuentros con la comunicación, para evitar desencuentros y frustraciones con la comunicación. ■



MÁS INFORMACIÓN



[El arte de la prudencia; Baltasar Gracián](#)



[How to be a powerful better human](#)



[Teoría de la Inteligencia Emocional de Daniel Goleman](#)



DATOS Y APLICACIONES, SOPORTE DE LOS NUEVOS MODELOS DE NEGOCIO

¿Cómo están tratando las empresas sus datos? ¿Qué aspectos son fundamentales para sus estrategias alrededor de los datos? ¿Cómo están gestionando sus aplicaciones? ¿De qué manera están incorporando nuevas tendencias a la administración de datos y desarrollo de apps?



La catarsis de la tecnología



José Manuel Navarro

CMO MOMO Group



José Manuel Navarro Llena es experto en Marketing. Durante más de treinta años ha dedicado su vida profesional al sector financiero donde ha desempeñado funciones como técnico de procesos y, fundamentalmente, como directivo de las áreas de publicidad, imagen corporativa, calidad y marketing. Desde hace diez años, basándose en su formación como biólogo, ha investigado en la disciplina del neuromarketing aplicado, lo que le ha permitido dirigir, coordinar e impartir formación en diferentes masters de neuromarketing en escuelas privadas y en universidades públicas. Es Socio fundador de la agencia de viajes alternativos [Otros Caminos](#), y de la entidad de dinero electrónico con licencia bancaria otorgada por el Banco de España [SEFIDE EDE](#) de la que en la actualidad es director de Marketing. Autor de "El Principito y la Gestión Empresarial" y "The Marketing, stupid", además de colaborador semanal desde 2006 en el suplemento de economía Expectativas del diario Ideal (Grupo Vocento).

Salvo las generaciones más mayores que tuvieron que sufrir las consecuencias de las últimas guerras que asolaron naciones y segaron la vida de millones de personas (y que aún siguen reproduciéndose en diferentes países por cuestiones geoestratégicas y de control de los recursos naturales), la memoria colectiva no recuerda haber experimentado una situación como la que estamos viviendo a consecuencia del COVID-19 y su expansivo contagio, cuyos devastadores efectos se están dejando notar en la salud de cientos de miles de personas en todo el mundo y en una recesión económica de imprecisas dimensiones.

El obligado confinamiento de una gran parte de la población, en el momento de escribir esta columna, tendrá como primer resultado un deseable control de la curva de crecimiento de los contagios para que el sistema sanitario no colapse, pero también un terrible deterioro del tejido productivo que nos abocará a un nuevo escenario de cierre de pequeñas y medianas empresas, de incremento del paro entre asalariados y autónomos, y de

una desconfianza generalizada en los mercados como fruto del pánico de los inversores y de la incapacidad de los gobiernos de abordar la situación protegiendo antes a las personas que al sistema.

En este tránsito, muchas cosas cambiarán, desde las relaciones personales que han tenido que



NO SOLO



Marketing y consumo

ser reformuladas al forzar el aislamiento, a los criterios de asignación de los presupuestos generales a las áreas de investigación y sanidad, hasta los modelos de trabajo y de consumo. Muchas variables que dábamos por supuesto se tendrán que ajustar a una nueva realidad, en la que habrá sectores que pierdan y otros que ganen, y no en la misma proporción.

Uno de los sectores que ya han notado los efectos del COVID-19 es el del eCommerce, en el cual (según el informe publicado por Geotelecom) la inversión publicitaria se ha reducido en un 35% al cambiar drásticamente la conducta de los consumidores hacia la contención del gasto como previsión de ahorro frente a un futuro incierto. Ello ha redundado en la consiguiente caída del 50% en las compras, desviándose éstas hacia los productos de primera necesidad. La consiguiente caída de ingresos (40%) ha implicado la pérdida de rentabilidad de las inversiones publicitarias, provocando una huida de los canales digitales.



Sectores como el textil han sufrido un importante retroceso, mientras que otros han experimentado un incremento de ventas como el de alimentación (20%) ya que los consumidores prefieren abastecerse desde casa; las parafarmacias (50%) por miedo a no encontrar los productos en los puntos de venta físicos; los productos para mascotas han quintuplicado las ventas debido a que el número de tiendas no está cerca del domicilio; los artículos de fitness también multiplicado su comercialización por el cierre de gimnasios y la prohibición de hacer deporte en la calle; otros como ferreterías, material escolar y muebles para el hogar, crecen también al incrementarse las tareas en casa.

En el sector financiero, aunque los bancos mantienen sus estructuras activas, están realizando un importante esfuerzo por ayudar a sus clientes en el uso de la banca digital lo que ayudará a condicionar conductas de uso de sus servicios que, más tarde, podrán permanecer en el tiempo porque los usuarios con menor índice de adopción habrán comprobado la eficiencia de este canal. En este sentido, Ant Financial ha dado un paso "más largo" creando la plataforma Ant Duo-Chain, basada en tecnología blockchain, para potenciar la cadena de suministro financiero a pequeñas y medianas empresas con necesidades de tesorería, facilitándoles la solicitud de préstamos de rápida tramitación en condiciones preferentes.

¿Te gusta este reportaje?

Compártelo en redes



Respecto del uso del dinero físico, a pesar de la controversia creada acerca de las manifestaciones realizadas o no por la OMS, el miedo a poder contagiarse a través de éste ha favorecido el incremento de los pagos digitales, sea con tarjeta, móvil u otros dispositivos contactless. En algunos casos por usuarios ya habituados y en una gran mayoría por otros con baja costumbre, la adopción de las nuevas tecnologías para preservar la salud ha infundido mayor confianza en éstas que en los métodos tradicionales. Este cambio de conducta, en un período de alto estrés, generará la consolidación de la adopción de soluciones tecnológicas en segmentos de población más amplios y en sectores que no terminaban de despegar en entornos digitales y que tendrán que aprovechar para generar una asociación positiva de su solución con la conveniencia para el consumidor. ■

MÁS INFORMACIÓN

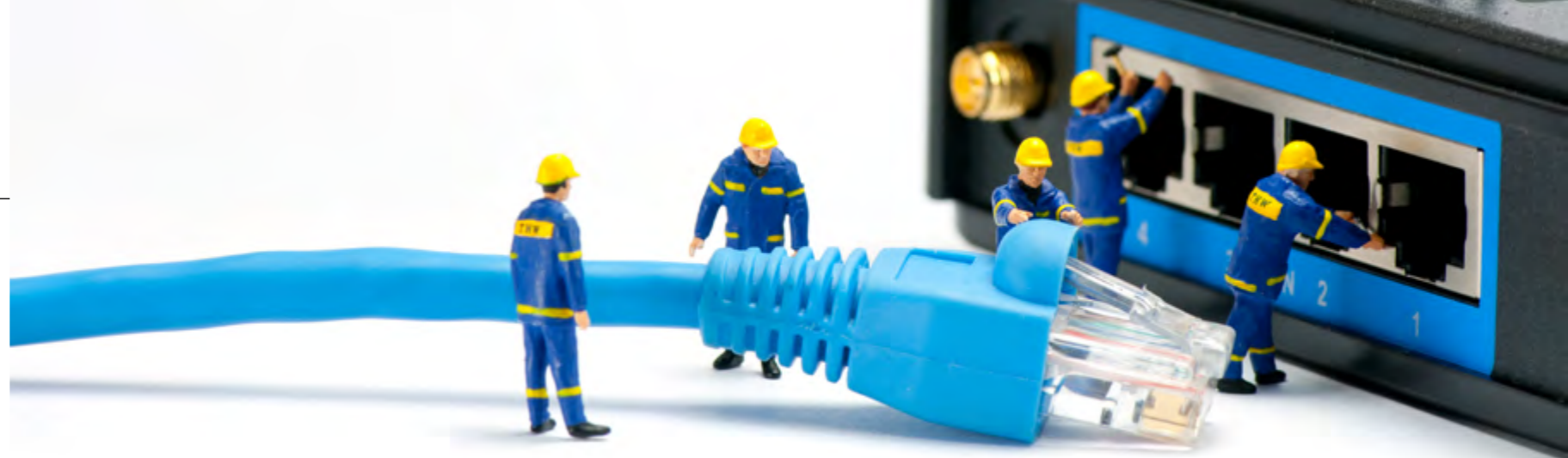
[Impacto del coronavirus en el e-commerce](#)

[Ant Duo-Chain](#)

NO SOLO



Legal IT



El derecho de ocupación de la propiedad privada y despliegue de redes físicas, según la normativa (I)



Juan Pedro Peña

Asesor jurídico TIC



Abogado especializado en TIC, rama relativamente novedosa del ejercicio del Derecho que engloba las Tecnologías de la Información y la Comunicación, así como del Entretenimiento Digital, ejerciendo desde el año 2002.

Ayuda a emprendedores y empresas a adaptar su idea o negocio tecnológico a las exigencias legales. Su labor es principalmente la prevención, planificando el camino a seguir para evitar cualquier injerencia que impida lograr metas, aunque también acude cuando las piedras del camino son inevitables.

El BOE del 10 de mayo de 2014 publicó la nueva Ley 9/2014, de 9 de mayo, de Telecomunicaciones (LGTel). Esta norma nació no sólo con la intención de mejorar a la anterior, promulgada once años antes, sino también para adaptar y homogeneizar la principal normativa surgida entre ambas, como el Real decreto-ley 13/2012, de 30 de marzo, por el que se transponen directivas en materia de mercados interiores de electricidad y gas y en materia de comunicaciones electrónicas y la transposición de las directivas europeas Directiva 2009/136/CE, del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009 (Derechos de los Usuarios), y la Directiva 2009/140/CE, del Parlamento Europeo y del Consejo, de 25 de noviem-

bre de 2009 (Mejor Regulación), que ya introducían medidas destinadas a crear un marco adecuado para la realización de inversiones en el despliegue de redes de nueva generación, de modo que se permita a los operadores ofrecer servicios innovadores y tecnológicamente más adecuados a las necesidades de los ciudadanos.

Pero, sobre todo, surgió como necesidad de cumplir con la llamada Agenda Digital para Europa, principal instrumento para el cumplimiento de los objetivos de la Estrategia Europa 2020, que busca que para 2020 todos los europeos tengan la posibilidad de acceder a conexiones de banda ancha a una velocidad como mínimo de 30 Mbps, y que, al menos, un 50% de los hogares europeos

¿Te avisamos
del próximo
IT User?



estén abonados a conexiones de banda ancha superiores a 100 Mbps. Estos objetivos han quedado incorporados a la agenda digital española, aprobada por el Gobierno en febrero de 2013.

Por otro lado, con anterioridad, la Ley 12/2012 de 26 de diciembre de medidas urgentes de liberalización del comercio y de determinados servicios, ya establecía en su Artículo 3.1 que “no podrá exigirse la obtención de licencia previa de instalaciones, de funcionamiento o de actividad ni de otras clases similar o análogas, en los términos indicados en la citada ley”.

El 16 de septiembre de 2016 entró en vigor el Real Decreto 330/2016, de 9 de septiembre, relativo a medidas para reducir el coste del despliegue de las redes de comunicaciones elec-

trónicas de alta velocidad y, como se indicará más adelante, entre dichas medidas, se encuentra el desarrollo del despliegue de redes desde el punto de vista de la relación con las administraciones públicas.

Sin embargo, han transcurrido casi 6 años desde la promulgación de la LGTel y más de tres desde el citado Real Decreto y aun así, los distintos agentes que intervienen en el Despliegue de redes de comunicaciones electrónicas, no lo tienen nada claro.

EL DERECHO A LA OCUPACIÓN

❖ Ocupación del dominio privado y la expropiación forzosa

El artículo 29 de la LGTel establece el derecho de los operadores a la “ocupación de la propie-

dad privada cuando resulte estrictamente necesario para la instalación de la red en la medida prevista en el proyecto técnico presentado y siempre que no existan otras alternativas técnica o económicamente viables, ya sea a través de su expropiación forzosa o mediante la declaración de servidumbre forzosa de paso para la instalación de infraestructura de redes públicas de comunicaciones electrónicas. En ambos casos tendrán la condición de beneficiarios en los expedientes que se tramiten, conforme a lo dispuesto en la legislación sobre expropiación forzosa”.

Los operadores, continúa indicando el citado precepto, asumirán los costes a los que hubiera lugar para esta ocupación y ésta se llevará a cabo tras la instrucción y procedimiento marcado por el Ministerio de Industria, Energía y Turismo (en adelante MINETUR) y que en la actualidad se encuentra pendiente de desarrollo.

El MINETUR recabará informe al órgano competente de la comunidad autónoma en materia de ordenación del territorio que deberá ser emitido en un plazo máximo de 30 días, pudiendo ser ampliado a 3 meses en caso de afectar a un área geográfica relevante o pudiera tener afecciones medioambientales y también se recabará informes a los Ayuntamientos afectados sobre la compatibilidad del proyecto técnico con la ordenación urbanística vigente, contando también con un plazo de 30 días para responder.



Han transcurrido casi 6 años desde la promulgación de la LGTel y los distintos agentes que intervienen en el despliegue de redes de comunicaciones electrónicas, no lo tienen nada claro



La aprobación del citado proyecto técnico finalmente por MINETUR, llevará implícita, en su caso, la declaración de utilidad pública y la necesidad de ocupación para la instalación de redes.

❖ Derecho de ocupación del dominio público

El artículo 30 de la LGTel determina que los operadores tendrán derecho a la ocupación del dominio público “en la medida en que ello sea necesario para el establecimiento de la red pública de comunicaciones electrónicas de que se trate” garantizando por parte de los titulares de ese dominio público “el acceso de todos los operadores a dicho dominio en condiciones neutrales, objetivas, transparentes, equitativas y no discriminatorias, sin que en ningún caso pueda establecerse derecho preferente o exclusivo alguno de acceso u ocupación de dicho dominio público en beneficio de un operador determinado o de una red concreta de comu-

nicaciones electrónicas. En particular, la ocupación o el derecho de uso de dominio público para la instalación o explotación de una red no podrá ser otorgado o asignado mediante procedimientos de licitación”.

El artículo 31 de la LGTel establece que normativa dictada por cualquier Administración Pública que afecte al despliegue de redes públicas de comunicaciones electrónicas deberá, en todo caso, reconocer el derecho de ocupación del dominio público o la propiedad privada para el despliegue de las redes públicas de comunicaciones electrónicas

Dicho reconocimiento supondrá, entre otros, que la normativa debe prever un procedimiento rápido, sencillo, eficiente y no discriminatorio de resolución de las solicitudes de ocupación, que no podrá exceder de seis meses contados a partir de la presentación de la solicitud, salvo en caso de expropiación.

Como apunta dicho artículo, existe la posibilidad, como hemos visto anteriormente, que en caso de que no se alcance acuerdo para la ocupación del dominio privado, el operador solicite la ocupación de la propiedad privada cuando resulte estrictamente necesario para la instalación de la red, estando sujeto a un procedimiento, que también hemos indicado anteriormente.

Caso distinto es la ocupación de las fachadas de los edificios privados, cuya regulación ha dado un giro totalmente radical con la nueva ley, que no sólo la contempla expresamente, sino que hasta es fomentada. Lo veremos más adelante.

ELIMINACIÓN DE LAS LICENCIAS DE OBRA

La Ley 20/2013 de 9 de diciembre, de garantía de la unidad de mercado, estableció el llamado “Principio de necesidad y proporcionalidad de las actuaciones de las autoridades competentes” e indica que aquellas autoridades que en el ejerci-

cio de sus respectivas competencias establezcan límites al acceso a una actividad económica o su ejercicio o exijan el cumplimiento de requisitos para el desarrollo de una actividad, motivarán su necesidad en la salvaguarda de alguna razón imperiosa de interés general: “la seguridad pública, la protección civil, la salud pública, la preservación del equilibrio financiero del régimen de seguridad social, la protección de los derechos, la seguridad y la salud de los consumidores, de los destinatarios de servicios y de los trabajadores, las exigencias de la buena fe en las transacciones comerciales, la lucha contra el fraude, la protección del medio ambiente y del entorno urbano, la sanidad animal, la propiedad intelectual e industrial, la conservación del patrimonio histórico y artístico nacional y los objetivos de la política social y cultural”. Todo límite o requisito establecido, deberá “ser proporcionado a la razón imperiosa de interés general invocada, y habrá de ser tal que no exista otro medio menos restrictivo o distorsionador para la actividad económica”.

Esta norma viene a establecer que para todo lo que se salga de las reglas y supuestos anteriormente indicados, bastará con una declaración responsable y entre dichos supuestos se encuentra el despliegue de redes y equipos de comunicaciones electrónicas.

El fruto más reciente de esa normativa es, como decimos, la actual LGTel, que menciona expresamente la obligatoriedad de que la normativa de

las administraciones públicas que afecte al despliegue de redes y los instrumentos de planificación territorial o urbanística deberán impulsar o facilitar el despliegue en su ámbito territorial y en particular, garantizar la libre competencia en la instalación de redes y en la prestación de servicios.

El Art. 34.3, párrafo 2, menciona también la imposibilidad de que las administraciones impongan restricciones absolutas o desproporcionadas al derecho de ocupación del dominio público y privado de los operadores ni tampoco soluciones téc-



¿Te avisamos del próximo IT User?



nicas concretas, itinerarios o ubicaciones y contribuirán a garantizar y hacer real una oferta suficiente de lugares y espacios físicos en los que los operadores decidan ubicar sus infraestructuras.

Este precepto, por cierto, fue recurrido por inconstitucional por parte de la Generalitat de Catalunya por entender que se estaban invadiendo sus competencias, pero el Tribunal Constitucional desestimó esta pretensión

La supresión del régimen de autorización tiene su materialización en el Art. 34.6, objeto también de recurso de inconstitucionalidad por la citada administración autonómica y desestimado. Pese bien, este precepto indica que para la instalación de estaciones o infraestructuras radioeléctricas y para la instalación de redes públicas, no podrá exigirse por parte de las administraciones públicas competentes la “obtención de licencia o autorización previa de instalaciones, de funcionamiento o de actividad o de carácter medioambiental ni otras licencias o aprobaciones de clase similar o análogas que sujeten a previa autorización dicha instalación”.

La prohibición anterior se llevará a cabo en caso de que el operador haya presentado a dicha administración un plan de despliegue o instalación de red en la que se contemplen dichas infraestructuras o estaciones y que el plan haya sido aprobado por dicha administración. El modelo de contenido de dicho plan y sus condicio-

NO SOLO

it Legal IT

nes técnicas serán acordados mediante Real Decreto por el Consejo de Ministros, circunstancia que aún no se ha producido, alimentando en opinión del que escribe, la confusión y/o desconocimiento del marco normativo actual.

El plan de despliegue o instalación se entenderá aprobado si transcurrido dos meses desde su presentación la administración competente no ha dictado resolución expresa. En cualquier caso, dicho plazo podrá ampliarse con carácter excepcional conforme a la normativa del procedimiento administrativo común.

Para hacer más divertida la configuración, el Tribunal Constitucional si que admitió la pretensión de la Generalitat de Catalunya en lo relativo al plazo, de ahí que se haya indicado como tachado, pero no se indica nuevo plazo. Pero es que, además, posteriormente se promulga el citado Real Decreto 330/2016, de 9 de septiembre, que en su Art. 8.1. establece el plazo de cuatro meses máximo para resolver en el caso de que el despliegue implique obra civil.

Por lo tanto, y teniendo en cuenta lo establecido en el Art. 21.3 de la Ley 39/2015 de 1 de octubre, que indica que "Cuando las normas reguladoras de los procedimientos no fijen el plazo máximo, éste será de tres meses", como es este caso, tenemos dos supuestos marcados por dos plazos máximos para resolver:

1. En el caso de Planes de Despliegue en el que no se indique obra civil: 3 meses.
2. En el caso de Planes de Despliegue en el que sí que impliquen obra civil: 4 meses.

Las licencias o autorizaciones serán sustituidas por declaraciones responsables y el declarante debe haber abonado el tributo/tasa correspondiente cuando así sea preceptivo pues así se contemple en la Ordenanza Municipal, adaptada ésta a estas nuevas circunstancias. En dicha declaración, el presentante deberá manifestar de forma explícita que ha cumplido los requisitos antes indicados (plan de despliegue y pago de tributo). En el caso de que sean varias las actuaciones a realizar, se deberán, en la medida de lo posible,

¿Te gusta este reportaje?

Compártelo en redes



presentar en la misma declaración responsable. La declaración responsable habilita para la instalación a partir de su presentación pero no implicará de entrada el cumplimiento de la normativa aplicable ni limitará la potestad de inspección y en su caso sanción de la administración competente. Así mismo, la inexactitud, falsedad u omisión de cualquier dato o documento en la declaración responsable o que acompañe a esta o la no presentación de esta implicará la imposibilidad de explotar la instalación y la obligación de su retirada. ■

 **MÁS INFORMACIÓN**

 [Ley General de Telecomunicaciones](#)



CLOUD, LA PLATAFORMA QUE LO CAMBIA TODO

Pocas son las empresas que hoy no tengan alguno de sus elementos de TI en la nube. El modelo de cloud, con sus diferentes sabores, está avanzando entre las organizaciones con una clara tendencia hacia modelos híbridos (combinación de nubes privadas y públicas), y multicloud, donde se disponen de varios contratos con proveedores de cloud público. IT Research tiene como objetivo conocer la realidad digital de las empresas y con este estudio, ha buscado aquellos datos que reflejan el estado de los modelos cloud.



Estado de alarma digital: limitación de los derechos digitales individuales

Estamos inmersos en la primera Pandemia Global de la era Digital de la especie humana. Todas las pandemias que ha sufrido la especie humana desde que aprendió a andar a dos patas han ocurrido antes de esta Era Digital y Global. Hasta el año 1500, la población mundial llegó a ser de unos 400 millones, en agrupaciones pequeñas y aisladas, y los sistemas de información y comunicación eran limitados, verbales y presenciales.

A la primera Revolución Industrial llegamos con 1.000 millones de habitantes y habiendo añadido a la comunicación e información el medio escrito.

En 1900 con 1.500 millones de habitantes y la llegada del teléfono y la radio, aparece la comunicación e información verbal remota, en medio ya de lo que se llamó la segunda Revolución Industrial.

A mediados del siglo XX, con 2.500 millones de habitantes, después de la Segunda Guerra Mun-

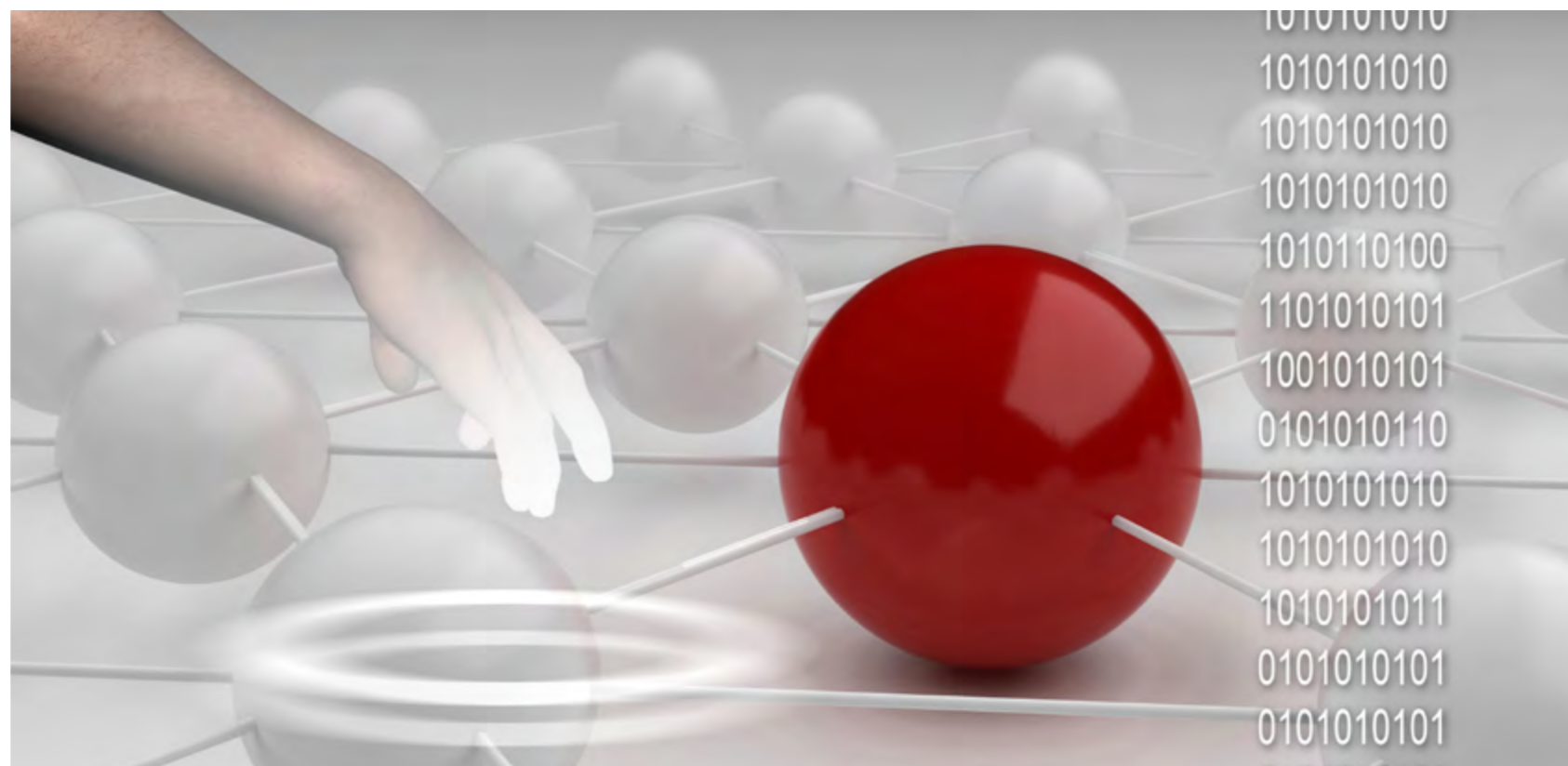


Mario Velarde Bleichner

Gurú en CiberSeguridad



Con más de 20 años en el sector de la Ciberseguridad, Mario Velarde Bleichner, Licenciado en Ciencias Físicas con especialidad en Cálculo Automático y PDG por el IESE, ha participado en el desarrollo de esta industria desde la época del antivirus y el firewall como paradigma de la Seguridad IT, dirigiendo empresas como Trend Micro, Ironport, Websense, la división de Seguridad de Cisco Sur de Europa y la división Internacional de Panda Software.



dial, y con la tercera Revolución Industrial, nos llegó la televisión y la primera globalización de la telefonía y, por tanto, una nueva dimensión de los sistemas de información y comunicación.

Las pandemias hasta entonces han transcurrido con los sistemas de información y comunicación fácilmente centralizables y cuando por la situación se tuvieron que tomar medidas como el estado de alarma, estado de sitio, cuarentenas, toques de queda... que limitan libertades básicas de los ciudadanos, nadie tenía en cuenta las libertades de expresión y opinión de los ciudadanos, simplemente porque los sistemas de información y comunicación eran controlados por los gobiernos responsables en cada momento.

En 2020 estamos con 7.750 millones de habitantes, muy avanzados en la cuarta Revolución

Industrial que, con sistemas de información y comunicación digitales y globales, ha dado a todos y cada uno de los ciudadanos del planeta los medios para para que puedan ejercer su derecho de libertad de comunicación, expresión y de opinión digital individual plenamente, sin más limitaciones que las existentes en el código penal.

Cuando, por circunstancias que lo justifiquen, se decreta el Estado de Alarma o su equivalente en otros países, entre otras medidas se limitan libertades individuales tan importantes como es la libertad de movimiento o la libertad de reunión. No parece por tanto extraño, por las mismas circunstancias excepcionales, que se pueda pensar en limitar o incluso llegar a suprimir libertades de nuevos derechos digitales individuales como la comunicación, expresión y opinión.

No voy a entrar en detalle sobre qué circunstancias excepcionales pueden llevar a suprimir o limitar derechos digitales individuales, es un debate tan amplio que es imposible abordarlo aquí y corresponde a muchos otros estamentos diferentes de la Ciberseguridad. Solo voy a mencionar algunos motivos que podrían llevar a la limitación o supresión de los derechos digitales individuales, si bien creo que no voy a ser capaz de mencionar más de un 5% de los que se pueden encontrar.

¿Te avisamos del próximo IT User?



Desde los más obvios y aparentemente inofensivos, como la disseminación de Fake News, bulos, falsificación de la información oficial, suplantación de identidades de científicos, suplantación de organismos públicos, saturación de los sistemas digitales...

Hasta acciones menos obvias, pero mucho más perniciosas, como el aprovechamiento de la ciberdelincuencia para lanzar campañas de virus con el fin de ganar control de gran número de PC, móviles y otros dispositivos para uso inmediato o en el futuro; campañas de peticiones fraudulentas de dinero; llamamientos a la desobediencia; desprestigio de autoridades; desprestigio de los servicios públicos...

Voy, en cambio, a elucubrar sobre posibles niveles de mantenimiento, limitación o supresión de los derechos digitales individuales, basándome en la factibilidad tecnológica de realizarlos, desde el nivel 0 de supresión de todos los derechos hasta el nivel N de normalidad con todos los derechos en vigor.

NIVELES DE LIBERTAD DIGITAL INDIVIDUAL

❖ **Nivel 0:** Este nivel plantea la suspensión máxima de la libertad de comunicación, expresión y opinión digital individual. Tecnológicamente significa que los únicos servicios que quedan disponibles son los telefónicos fijos y móviles,



NO SOLO



Ciberseguridad 4.0

para permitir la comunicación de las familias. El uso de internet queda restringido a los servicios básicos, redes especiales para los servicios sanitarios, redes militares, policiales y aquellos servicios que considere necesarios la autoridad que decreta este nivel de alarma digital.

❖ **Nivel 1:** Además de los servicios telefónicos fijo y móvil, se permite el acceso a los medios de comunicación digital, medios de entretenimiento, sin posibilidad de interacción, quedando suspendidos los derechos de libertad de expresión digital individual y opinión digital individual.

❖ **Nivel 2:** Además de los servicios de los niveles previos, se permite el acceso a servicios de chat que cumplan las condiciones de impedir el reenvío de información, solo se permite el envío de información texto elaborado por el remitente. Se restringe el derecho a opinión individual similar al distanciamiento social. Solo se permitirá el funcionamiento de chats que cumplan con este nivel de Alarma Digital.

❖ **Nivel N:** Situación normal con acceso a todos los servicios digitales y todos los derechos digitales individuales en pleno vigor.

Solo he descrito los niveles 0, 1 y 2 por su facilidad tecnológica de realización con las herramientas que cuenta el Estado en estos momentos, aunque debo decir que estos niveles me parecen para momentos de una gravedad tan extrema que solo de imaginarla se me erizan los pelos.

Entre el nivel 0 y el nivel N pueden existir tantos niveles como números naturales que permitan el uso de redes sociales y otras plataformas de expresión, comunicación y opinión aplicables a las determinadas situaciones que se puedan dar.

La complejidad tecnológica para definir niveles entre el 2 y N no debe ser un obstáculo para no hacerlos porque no es cierto, las plataformas son personalizables absolutamente, a la medida de lo que pueda necesitar cualquier estado para defenderse en situaciones excepcionales.

¿Te gusta este reportaje?

Compártelo en redes



Esta colaboración entre el estado y las empresas globales de redes sociales u otras plataformas de comunicación, opinión o que permitan la difusión de información debe realizarse con antelación a los periodos extraordinarios, de otra forma en muchos casos la única alternativa, será la limitación o cese de disponibilidad de redes sociales u otras plataformas que no se adapten a la situación extraordinaria que requiera limitar o suspender los derechos digitales individuales. ■



MÁS INFORMACIÓN

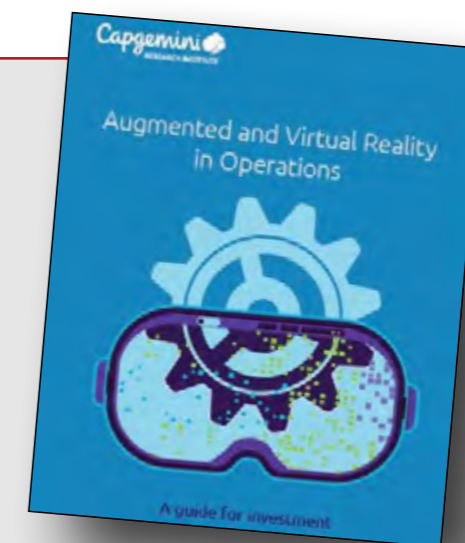


Población Mundial



REALIDAD AUMENTADA Y REALIDAD VIRTUAL EN OPERACIONES DE NEGOCIO

Capgemini Research Institute desvela en este informe que la Tecnología Inmersiva (Realidad Aumentada, AR, y Realidad Virtual, VR) incrementará la eficiencia, productividad y seguridad para las empresas, lo que la convierte en una nueva vía para fortalecer las operaciones de negocio.



¿Qué nos aporta esta crisis para nuestro liderazgo?

En cuántas entrevistas de trabajo has preguntado o te han preguntado: “¿cuál fue el momento más difícil de su carrera profesional y qué aprendió de ello?”.

Cuántas veces has pensado o has oído a alguien decir “hoy yo no sería la persona que soy

sin la experiencia de aquel momento tan difícil que atravesé”.

Hay algunos elementos en el liderazgo de personas y en el autoliderazgo que son importantes bajo situaciones cambiantes y de presión. La crisis actual nos permite distinguirlos con más



Javier Canal

Director de Go4aVision



Coach ejecutivo y de equipos. Formador internacional de PNL de código clásico y código nuevo, certificado por la ITA (John Grinder). Director de Go4aVision. Presidente de la asociación Apoyar a los que Apoyan. Formador y supervisor de Coaching en la Universidad Francisco de Vitoria. Colaborador habitual de la Fundación Rafael del Pino en sus programas de formación en Liderazgo. Especialista en Inteligencia Emocional y Eneagrama. 25 años de experiencia profesional previa en posiciones directivas en multinacionales del sector tecnológico.



claridad, también desde los ejemplos cotidianos de la convivencia familiar durante el confinamiento. Me detengo a profundizar en tres de ellos que son clave y que podemos extrapolarlos a nuestro propio estilo de liderazgo en la empresa, para reforzarlos y aplicarlos durante los próximos meses en los que se van a poner a prueba nuestras mejores capacidades.

En primer lugar, con motivo de la pandemia, todos somos muy conscientes de que tenemos que protegernos y cuidarnos para cuidar y proteger a los demás de los contagios. Este pensamiento, aun siendo muy necesario, no siempre ha estado presente en nuestro día a día profesional.

Para alguien que quiere poder ejercer su liderazgo de forma sostenida y bajo situaciones

habitualmente de mucho stress es indispensable autorresponsabilizarse de su autocuidado físico y emocional. El autoliderazgo consiste también en elegir conscientemente qué pensamientos y actividades escogemos o permitimos que ocupen nuestro tiempo y energías disponibles, para que contribuyan a construir nuestro mejor estado interno y poder estar al servicio de los demás ofreciéndoles apoyo y dirección.

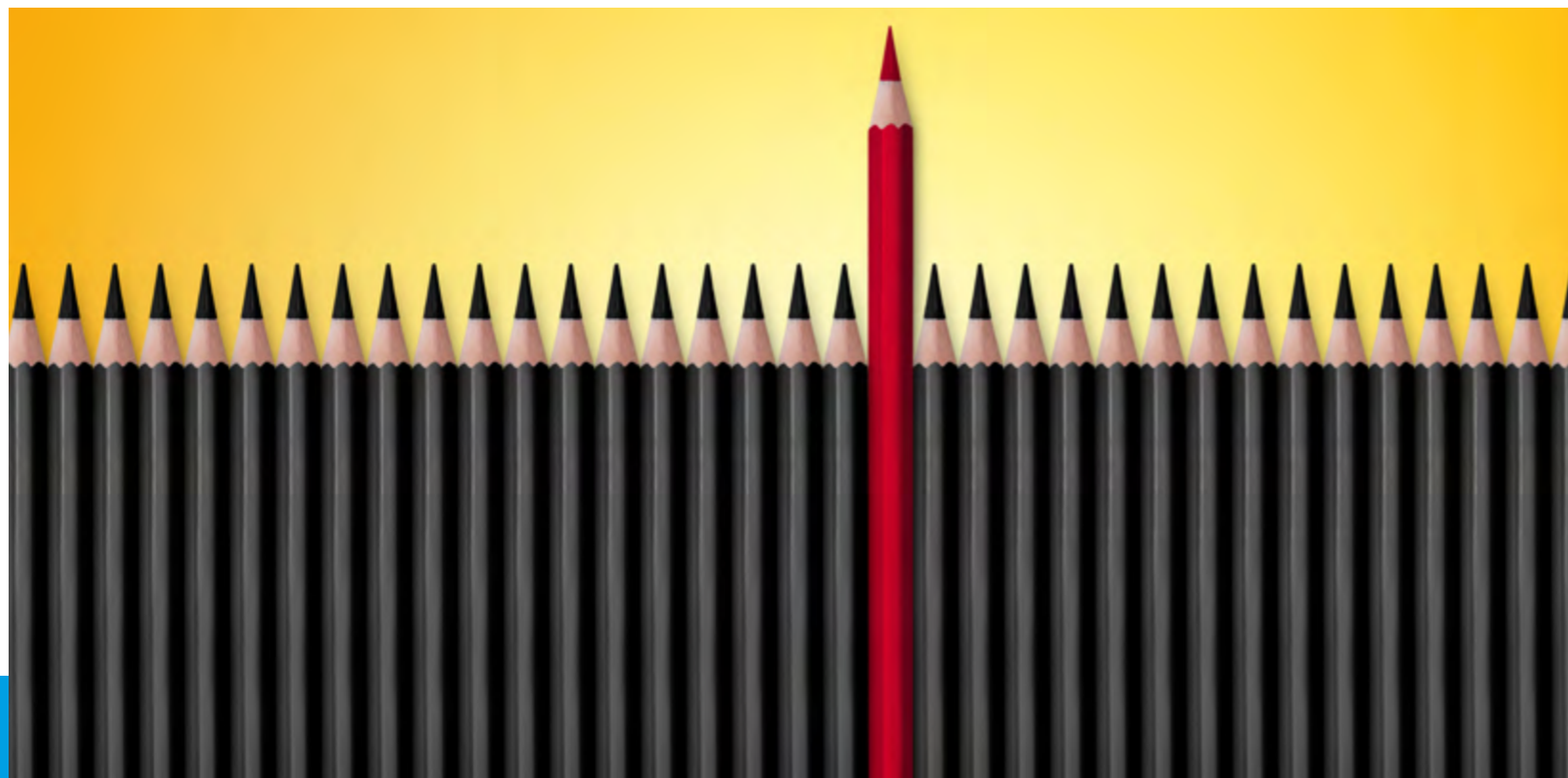
En segundo lugar, los que en estos días convivimos intensamente con nuestras familias, o nos comunicamos con ellas en la distancia, sabemos lo importante que es cuidar de cómo influimos en nuestros seres queridos y en sus estados de ánimo y positividad. El cuidado de las relaciones

¿Te avisamos del próximo IT User?



se ha convertido en algo indispensable. No solo es relevante qué les decimos y qué actividades les proponemos durante el aislamiento, sino también cómo lo hacemos, la forma en la que interactuamos con ellos. Esa sonrisa y voz amable que procuramos que nos salga, esa paciencia que conscientemente alimentamos, esos componentes lúdicos y de buen humor orientados a cuidar y preservar la buena relación, son totalmente necesarios cuando pasamos tantas horas seguidas juntos en un ambiente incierto y extraño para todos.

¿Y acaso no pasamos muchísimo tiempo con nuestros colaboradores y compañeros en la empresa en entornos a veces muy inciertos? ¿No se merecen esas situaciones el mismo nivel de cuidado y atención? Uno de los mantras que a mí personalmente me ayudó en momentos de gran cambio y desarrollo profesional como líder de equipos es: "La relación es lo primero". La razón de ser de nuestras organizaciones es poder conseguir objetivos mucho más grandes de los que individualmente podemos alcanzar de forma agregada. Es decir buscamos que el conjunto sea más que la suma de las partes. Sin embargo, en demasiadas ocasiones me encuentro (y yo personalmente lo experimenté en alguna etapa personal) con líderes mucho más enfocados a las tareas que los colaboradores tienen que realizar, que a



Hay algunos elementos en el liderazgo de personas y en el autoliderazgo que son importantes bajo situaciones cambiantes y de presión. La crisis actual nos permite distinguirlos con más claridad, también desde los ejemplos cotidianos de la convivencia familiar durante el confinamiento

las relaciones existentes con ellos y entre ellos como equipo.

En tercer lugar, estamos escuchando por doquier visualizaciones de la nueva etapa, de cuando todo esto ya esté pasado. Se lo oímos a nuestros líderes políticos y del gobierno, a líderes espirituales y religiosos, a pensadores y a multitud de personas con sus reflexiones en las redes sociales. Nosotros mismos hacemos planes con nuestros hijos o seres queridos para cuando termine el confinamiento, trayendo un rayo luminoso de esperanza e ilusión que contrasta con la gravedad de la situación presente. Es el arte de la visualización del objetivo anhelado. Siempre formulado en positivo, siempre como algo que no ha ocurrido aún pero que ya vemos y escuchamos como si ya estuviese ocurriendo en nuestras mentes.

Una de las funciones del líder es dibujar y componer esos escenarios futuros para que los demás, y él (ella) mismo, puedan empezar a paladearlos, a tocarlos con la mano, a dis-

frutar anticipadamente de los beneficios que están por venir. El tener clara esta visión es clave para asegurar la resiliencia de los equipos durante los momentos difíciles y es también necesario para que las personas puedan desplegar su máxima energía durante el trayecto hasta que el objetivo se alcance.

Una recomendación a este respecto: siempre formula tu visión en "positivo", es decir, visualiza lo que ocurrirá, no visualices lo que no ocurrirá. Tiene un impacto muy diferente cuando le dices a tus hijos "Iremos a la playa y nos bañaremos y jugaremos y disfrutaremos", en vez de "y ya no tendremos que estar en casa sin poder salir y desaparecerán todas estas dificultades que tenemos ahora", ¿verdad? El cerebro de los seres humanos sigue procesando la información igual y los mecanismos de motivación siguen siendo los mismos sin importar la edad que tengamos.

Durante los próximos meses seguirá habiendo grandes cambios. Cuando regresemos del aislamiento social y volvamos a nuestra acti-

¿Te gusta este reportaje?

Compártelo
en redes



vidad profesional presencial, nos espera un escenario diferente al que había antes de la pandemia del COVID-19. En ese momento podremos aplicar todos estos aprendizajes para la construcción de un nuevo futuro. Un futuro que estaba sin imaginar, un libro del cuál ni siquiera habíamos pensado aún el prólogo. La gran oportunidad que esta crisis nos trae es la posibilidad de elegir mucho más conscientemente cómo queremos visualizarnos a nosotros mismos, a nuestros equipos y a nuestros negocios, cuando todo esto deje de ser actualidad y se convierta en experiencia.

Tantas veces hemos enfrentado grandes resistencias cuando hemos querido incorporar cambios y mejoras en nuestras organizaciones. Ahora se abre una gran ventana de oportunidad para cambiar cosas que antes de la crisis no era posible.

Os deseo salud, consciencia y actitud de servicio en nuestro liderazgo. ■



MÁS INFORMACIÓN



G4V



**Negocio
como
servicio:**
Las TI en la era cloud



Cada mes en la revista,
cada día en la web.