it User
TECH & BUSINESS

nº 68
JUNIO 2021

CONTENIDOS↓

La seguridad se adapta a los nuevos escenarios

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

Nuevas corrientes alrededor de la impresión y gestión documental, a debate

it User TECH & BUSINESS

it televisión

Director Pablo García Reales
pablo.garcia@itdmgroup.es

Redacción y colaboradores Hilda Gómez, Arantxa Herranz, Reyes Alonso, Ricardo Gómez

Diseño revistas digitales Eva Herrero

Producción audiovisual Favorit Comunicación, Alberto Varet

Fotografía Ania Lewandowska

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

Director de Operaciones
Ángel Porras angel.porras@itdmgroup.es

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

El CFO:
cada vez más concienciado sobre la importancia de la tecnología

Uno de los principales lamentos en el que coinciden la mayoría de CIOs es su habitual sensación de incomprensión por parte del resto de directivos de sus compañías, ante la dificultad de hacerles entender, por un lado, la suma trascendencia que la tecnología ha de jugar entre sus planes estratégicos, y, por otro, la necesidad de que sus compañeros de comité de dirección también se erijan como interlocutores de los proveedores de tecnología, restando peso a la jerga técnica y sumando a la conversación terminología de negocio.

Si bien, una de las figuras con mayor capacidad de influencia en cualquier consejo de administración, el director financiero, cada día goza de un mayor nivel de comprensión y empatía hacia la tecnología y su potencial de influencia. En lo que respecta a la transformación digital, y según estudios recientes, el 80% de los CFOs del mundo la consideran como una de sus cinco principales prioridades profesionales, y se muestran más predispuestos a ayudar al CIO para encontrar vías eficaces con objeto de financiar proyectos de transformación digital, si estos van asociados a un retorno de inversión consistente. Lejos de hacerles retroceder, el 73% de los directores financieros reconocen que, con motivo de la pandemia, su inversión en transformación digital ha aumentado. Entre los proyectos de TI que personalmente querrían ver más por parte de su CIO, puesto que entienden que disfrutan de un claro valor de negocio y de un fuerte ROI, se encuentran los relativos a la optimización de las inversiones tecnológicas existentes, las iniciativas tecnológicas generadoras de ingresos, y las mejoras de los procesos y eficiencia de los empleados.

No obstante, hay que tener en cuenta que cerca de un 70% de los CFOs encuestados se niegan a malgastar recursos financieros en inversiones TI que no aporten un cambio importante a sus organizaciones. Al parecer, y como resulta lógico, los directivos financieros no quieren oír ni hablar de tener que implementar tecnología porque sí o de sentirse forzados por los grandes proveedores de ERP, tan propensos a migraciones y actualizaciones.

El CFO, un nuevo e interesante aliado. ■

Pablo García Reales

SUMARIO

Junio 2021

it User TECH & BUSINESS

EN PORTADA

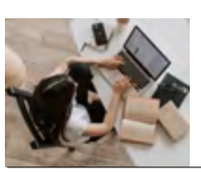
La seguridad se adapta a los nuevos escenarios

TENDENCIAS

Los ingresos de las empresas de servicios TIC siguen cayendo

Dos tercios de las empresas no están preparadas para afrontar un ciberataque

Los directores financieros necesitan acelerar la adopción de la IA

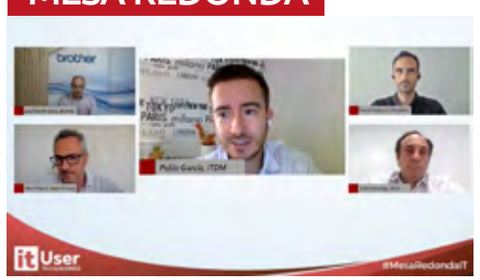


El 51% de las empresas en España ha adaptado su infraestructura TI al trabajo híbrido

ANUNCIANTES

REVISTAS DIGITALES

MESA REDONDA



Nuevas corrientes alrededor de la impresión y gestión documental, a debate

NO SOLO it

ACTUALIDAD

Dell Technologies y APEX, su catálogo de soluciones como servicio

ASLAN2021 celebra su edición más digital mostrando el camino hacia la modernización

A unas semanas de su inauguración, ¿qué sabemos del Mobile World Congress?

DES, la primera feria tecnológica que tiene lugar en España de manera presencial en 2021, cumple sus objetivos

IT WEBINARS

Conectando personas y datos: descubre HPE Data Services Cloud Console y HPE Alletra

CONTENT MARKETING

¿Están seguros tus datos de Salesforce?

SAMSUNG

Portable SSD T7

Super Fast External Storage

WORLD'S
No.1
FLASH MEMORY
SINCE 2002
SAMSUNG

* Source: 2019 Q2 IHS Markit data: NAND suppliers' revenue market share

DELL TECHNOLOGIES QUIERE ACELERAR LA TRANSFORMACIÓN DIGITAL CON APEX Y POTENCIAR LAS CAPACIDADES DE LAS EMPRESAS EN EL EDGE

Dell Technologies anuncia la disponibilidad de APEX, su catálogo de soluciones como servicio

Dell Technologies ha dado un paso más en su estrategia con el anuncio de la disponibilidad de APEX, una cartera de soluciones as-a-Service que simplifica la transformación digital aumentando la agilidad y el control de las TI. Asimismo, ha aprovechado la celebración de Dell Technologies World para anunciar nuevas soluciones que buscan potenciar las capacidades de las empresas en el Edge.

Michael Dell fue el encargado de inaugurar Dell Technologies World, evento que por segunda vez se celebra de forma virtual. Durante su intervención ha reconocido el papel fundamental de la tecnología para sostener a las empresas y a la economía en este año tan complicado, un paso que se ha podido dar por el camino recorrido hasta la fecha en lo que a transformación de los negocios e innovación se refiere.

Según Michael Dell, las compañías "comprenden los cambios fundamentales que se están produciendo en nuestro mundo y la importancia de invertir ahora para crear el futuro que queremos. Y en mis conversaciones con los clientes, se trata de acelerar a partir de aquí, utilizando este último año como trampolín hacia

un mañana mejor. Todos tenemos una gran cantidad de datos, y esto solo va a ir a más. El objetivo de todas organizaciones en este momento es averiguar cómo convertir sus datos en mejor información, acciones y resultados, y hacerlo más rápido".

"La transformación digital", continuaba, "se está acelerando, y no va a frenar. El impulso se dirige hacia un futuro híbrido y distribuido alimentado por el análisis de datos que se procesan en tiempo real y hacia procesos, operaciones y modelos de negocio digitales y seguros". En este mundo de hacer cualquier cosa desde cualquier lugar, cada vez más vemos un futuro que se desarrollará en el Edge. Mientras que el 10% de los datos se procesa hoy fuera de un centro de datos, será el 75% en 2025. Esos datos se generarán en el mundo real, en el Edge. Y para transformar esos datos en resultados se necesitarán análisis e inteligencia en tiempo real".

ACELERANDO LA AGENDA DIGITAL

Tal y como apuntaba Jeff Clarke, Vice Chairman & COO, Dell Technologies, "los clientes están acelerando su agenda digital, y sus TI deben estar preparadas para lo que viene, lo que se traduce en simplicidad, agilidad y control. Es la escala de la nube con la facilidad del servicio a medida. Este es el futuro del consumo de TI".

Es un viaje, continuaba, "en el que llevamos mucho tiempo, desde los productos hasta los servicios y los servicios gestionados, y ahora, todo consumido como servicio; APEX es la siguiente evolución de lo que hemos estado construyendo durante décadas".

Gartner predice que, para 2023, el 43% de la capacidad de almacenamiento recién desplegada se consumirá como OpEx, frente a menos del 15% actual. IDC predice que, para 2024, la mitad de la infraestructura del centro de datos se consumirá como servicio, y que el 75% de la infraestructura estará en el Edge.

EL NUEVO CATÁLOGO DE SOLUCIONES COMO SERVICIO YA ESTÁ DISPONIBLE

Y ahí es donde entra el principal anuncio de la sesión inaugural, APEX, un nuevo catálogo de soluciones como servicio.

Dell Technologies APEX, es una cartera de soluciones as-a-Service que simplifica la transformación digital aumentando la agilidad y el control de las TI. Las soluciones APEX pueden desplegarse en un centro de datos, una ubicación en el Edge o una instalación de on-premise, con la capacidad de escalar bajo demanda y pagar por la tecnología a medida que se consume.

La cartera de productos APEX incluye servicios tecnológicos integrales para los clientes que necesitan una experiencia gestionada, así como soluciones personalizadas para las organizaciones que necesitan más flexibilidad para entornos especializados. Así, encontramos los APEX Data Sto-

Michaell Dell mantuvo diferentes conversaciones durante la sesión inaugural de Dell Technologies World

> "La transformación digital se está acelerando, y no va a frenar. El impulso se dirige hacia un futuro híbrido y distribuido alimentado por el análisis de datos que se procesan en tiempo real y hacia procesos, operaciones y modelos de negocio digitales y seguros"
>
> MICHAEL DELL

rage Services, que ofrecen recursos de almacenamiento simplificados como servicio; los servicios APEX Cloud Services, que proporcionan recursos de nube híbrida y privada con una experiencia consistente; y APEX Custom Solutions, que permiten a las organizaciones crear su propio entorno bajo demanda para un consumo flexible.

La Consola APEX unifica la experiencia de APEX y ofrece a los clientes un acceso de autoservicio a un catálogo de servicios de infraestructura y de nube, a la vez que les guía a través de todo el ciclo de vida de la tecnología.

MÁS PROTAGONISMO PARA EL EDGE

Dell Technologies también ha presentado soluciones y acuerdos diseñados para extraer más valor de los datos en el Edge. Estas novedades, tal y como ha explicado la compañía, "forman parte de su estrategia para ofrecer tecnologías totalmente integradas que permitan que las cargas de trabajo se ejecuten y se gestionen en múltiples nubes y aplicaciones".

Y es que no podemos olvidar que los dispositivos del Edge son una fuente de datos cada vez mayor. De hecho, Gartner predice que el 75% de los datos empresariales se crearán y procesarán fuera del centro de datos o de la nube para 2025.

Jeff Boudreau, presidente y director general del Grupo de Soluciones de Infraestructura de Dell Technologies, comentaba que los datos "son la moneda del mundo digital y es hora de que los clientes les saquen partido. El Edge rivaliza rápidamente con los centros de datos y las nubes públicas como la ubicación donde las organizaciones obtienen información valiosa. Al colocar la computación, el almacenamiento y el análisis donde se crean los datos, podemos proporcionar esa información en tiempo real y crear nuevas oportunidades para las empresas".

Entre los anuncios destaca Dell EMC Streaming Data Platform (SDP), una plataforma de transmisión y analítica de datos que permite realizar análisis en tiempo real en el extremo.

Otro de los elementos de esta apuesta por el Edge son las Soluciones de fabricación edge de Dell Technologies. La Dell Technologies Manufacturing EDGE Reference Architecture con PTC ayuda a los fabricantes a obtener conocimientos de las estaciones de trabajo, ordenadores, dispositivos móviles y otros endpoints dentro del entorno de fabricación. La posibilidad de acceder a los datos del Edge en una sola ubicación "permite a las empresas aumentar la fiabilidad de la línea de producción, reducir los costes operativos y tomar decisiones más cercanas al tiempo real". Esta arquitectura, integrada con APEX Private Cloud, ofrece un marco edge-como servicio de alta disponibilidad para que las empresas puedan virtualizar y organizar aplicaciones, eliminando la complejidad y ahorrando tiempo. ■

MÁS INFORMACIÓN

Dell Technologies World 2021

Descarga este documento ejecutivo de IT RESEARCH

NUEVO INFORME

EL CONGRESO SE CELEBRÓ BAJO EL LEMA "DIGITALIZACIÓN ES FUTURO"

ASLAN2021 celebra su edición más digital mostrando el camino hacia la modernización

ASLAN2021 HYBRID abrió sus puertas con el acto inaugural que ha contado con la participación de Nadia Calviño, Vicepresidenta segunda del Gobierno y Ministra de Asuntos Económicos y Transformación Digital; Miguel Ángel García, Viceconsejero de Presidencia y Transformación Digital de la Comunidad de Madrid; y Fernando de Pablo, director general de la Oficina Digital del Ayuntamiento de Madrid.

ASLAN2021 HYBRID ha abierto sus puertas, en esta ocasión de forma virtual, con objetivos entre los que se encontraban profundizar en tendencias tecnológicas de alto impacto, alinear proyectos con los objetivos Next Generation EU y del Plan España Digital 2025, y detectar oportunidades de digitalización en sectores clave del tejido productivo.

Ricardo Maté, presidente de la Asociación @aslan, fue el encargado de comenzar el acto de inauguración del Congreso, destacando la importancia de una Asociación está compuesta por 140 empresas tecnológicas que buscan ayudar "en la digitalización de nuestra sociedad".

Maté recordó que "la pandemia ha tenido un impacto muy fuerte" en la economía española. "La transformación digital es el elemento que va a hacer que nuestro país salga adelante". El objetivo de @aslan es "ayudar a relanzar la economía del país", algo que representa "una oportunidad y una responsabilidad".

PALABRAS DE NADIA CALVIÑO

Tras Ricardo Maté intervino Nadia Calviño, Vicepresidenta segunda del Gobierno y Ministra de Asuntos Económicos y Transformación Digital, quien recordó que el sector tecnológico es "clave para el presente y futuro del país".

La pandemia "ha acelerado la transformación digital de España", aseguró Calviño que también destacó el papel que han jugado las redes de telecomunicaciones a la hora de permitir a los españoles seguir con su vida en los momentos más duros de la pandemia. "Nos encontramos ante una oportunidad única para modernizar España".

Calviño explicó que "encauzar bien el proceso de digitalización es una de las prioridades de este Gobierno desde hace tres años" y ha recordado que "desde el pasado mes de julio hemos presentado siete planes de digitalización" que afectan a las PYMES y Autónomos, a la Administración Pública, o a la conectividad, la ciberseguridad, el despliegue de 5G, o las competencias digitales.

La transformación digital de España es uno de los tres ejes del Plan de Recuperación, Transformación y Resiliencia, "la hoja de ruta para la modernización de la economía española", recordando que un tercio de las inversiones de este plan "20.000 millones de euros" se destinarán a la transformación digital. "Tenemos un reto muy importante ante nosotros", recordó Calviño, que confirmó que durante la segunda mitad del año "se acelerará el despliegue de las inversiones".

La economía española "está entrando en una nueva fase. La recuperación está en marcha". A la hora de realizar esta afirmación, Calviño se ha referido a los datos que se acaban de conocer del empleo durante el mes de mayo.

"Tenemos una oportunidad histórica para que la salida de esta crisis se convierta en digital. Éste es uno de los vectores para lograr una recuperación más fuerte, más justa, y más sostenible", afirmó Calviño quien ha asegurado que la transformación digital "es un proyecto de país".

Ricardo Maté, presidente de la Asociación @aslan

Nadia Calviño, Vicepresidenta segunda del Gobierno y Ministra de Asuntos Económicos y Transformación Digital

REPRESENTANTES DE MADRID

Miguel Ángel García, Viceconsejero de Presidencia y Transformación Digital de la Comunidad de Madrid, comenzó su intervención destacando que la región madrileña "se adelantó al resto de las Administraciones Públicas" a la hora de adoptar medidas en la lucha contra la COVID-19 durante el mes de marzo de 2020.

"Nos encontramos en un momento muy favorable para la digitalización", aseguró Miguel Ángel García, que también destacó que es necesario "liberar cuanto antes los fondos europeos" para la recuperación.

La Comunidad de Madrid "es una región de referencia" en lo que digitalización se refiere. "Un tercio de las empresas referentes del sector tecnológico están ubicadas en Madrid, "el 76% de las empresas y el 92% de los hogares de la Comunidad están conectados por fibra" y durante los meses más duros de la pandemia "65.000 empleados públicos (el 75% del total exceptuando a los sanitarios) continuaron prestando atención a los ciudadanos a través del teletrabajo. Hemos avanzado mucho en ámbitos como la telemedicina o la educación".

Asimismo, el representante de la Comunidad de Madrid remarcó que la "digitalización es uno de los ejes de los Fondos de Recuperación" que ha puesto en marcha la región y que cuenta con una inversión de "22.500 millones de euros". De éstos, el 27% se destinará a la transformación digital y el 5% a la digitalización de los servicios públicos. "Nuestro objetivo es ser capaces de acelerar la transformación digital de PYMES y autónomos", además de "avanzar hacia la administración digital".

La Comunidad de Madrid quiere ser el referente tecnológico europeo. "Estamos en una buena posición. La Comunidad de Madrid es un socio leal de las empresas para que nuestro país pueda liderar la transformación digital". Una oportunidad que "no podemos dejar escapar ya que contamos con empresas punteras".

Fernando de Pablo, director general de la Oficina Digital del Ayuntamiento de Madrid, aprovechó su intervención para destacar el papel que juega la Asociación @aslan. "Es un referente imprescindible para el futuro". Además, señaló que "una parte importante del futuro nos la vamos a jugar en la utilización eficiente de los fondos europeos" y explicó que, entre las preocupaciones del Ayuntamiento se encuentran "la brecha digital, la ciberseguridad, la gestión de los datos o el talento". Madrid "es una referencia de las infraestructuras digitales. Es una ciudad abierta e integradora y tenemos uno de los bienes más escasos: el talento. Madrid atrae talento".

EN QUÉ CONSISTIÓ EL EVENTO

La cita reunió a 114 ponentes en un amplio programa de conferencias en las que destacaron los dos encuentros de expertos en Tecnologías, uno enfocado en la Administración Pública y otro en sectores clave.

La sesión de apertura del IV Encuentro Anual Nacional de Expertos en Tecnologías en la Administración Pública corrió a cargo de Santiago Graña Domínguez, subdirector general de Impulso de la Administración Digital y Servicios al Ciudadano del Ministerio de Asuntos Económicos y Transformación Digital. En este foro participaron además

Miguel Ángel García, Viceconsejero de Presidencia y Transformación Digital de la Comunidad de Madrid

los responsables de innovación, tecnología y digitalización del Ministerio de Industria, Comercio y Turismo; Ministerio de la Presidencia; Ministerio del Interior; Seguridad Social; SEPE; Agencia para la Administración Digital de la Comunidad de Madrid; Centro Criptológico Nacional; los Ayuntamientos de Málaga, Madrid y Barcelona; la Sociedad Provincial de Informática; el Servicio Madrileño de Salud; el Hospital 12 de Octubre; y Correos.

Por su parte, en el III Encuentro Anual Nacional de Expertos en Tecnologías en Sectores Clave destacó la ponencia de Miguel Ángel Ariño, Profesor del IESE Business School. Junto a él, estuvieron los CIO y directores de TI de AON, COFAS, Hospital Ribera Povisa, EVO Banco, Adecco Group, CELSA; Prisa, Editorial Santillana, Gilmar, Grupo IFA, Betapack, Faes Farma y Nationale Nederlanden.

El congreso quiso ofrecer una visión 360° de los avances en innovación tecnológica y ciberseguridad

Además de estos encuentros, se celebraron dos fórums y conferencias en torno a gestión de los datos, ciberseguridad, cloud, puesto de trabajo digital y redes inteligentes.

El cambio de paradigma al que ha obligado la pandemia ha demostrado la importancia de la tecnología para crear organizaciones más resilientes. El congreso quiso ofrecer una visión 360° de los avances en innovación tecnológica y ciberseguridad, incrementar el networking y acercarse a las necesidades de digitalización de las pymes. Para ello, además del programa de conferencias, se crearon nuevos espacios digitales con los que superar las 3.000 interacciones de calidad entre profesionales y empresas participantes, como las reuniones de FastNetworking o los Business Spaces.

La edición de este año estuvo patrocinada como Global Sponsors por AWS, Cambium Networks, Dell Technologies, ESET, HPE y NFON; como Event Sponsors hay que mencionar a Aruba, Citrix, Deutsche Telekom, Dynatrace, Fastly, Infinidat, Infoblox, Kaspersky, Micro Focus, Nutanix, OVHCloud, Qlik, Samsung, SAP, SonicWall, Sophos, Wildix, Winncom y Zaltor. ■

Fernando de Pablo, director general de la Oficina Digital del Ayuntamiento de Madrid

MÁS INFORMACIÓN

- Toda la información de ASLAN2021
- 50 estrategias para 2050
- España Digital 2025

EL CONGRESO ABRIRÁ SUS PUERTAS EL 28 DE JUNIO EN BARCELONA

A un mes de su inauguración, ¿qué sabemos del Mobile World Congress?

El Mobile World Congress abrirá sus puertas el próximo 28 de junio en Barcelona. En las últimas semanas han sido muchas las empresas que han anunciado que no acudirán a la Ciudad Condal, aunque sí estarán de forma virtual. Mientras, la organización se afana en explicar que ha trabajado para que el Mobile sea un evento seguro y animan a la participación presencial con acciones como rebajas en algunas entradas. A un mes vista, ¿qué sabemos del Mobile World Congress?

Falta un mes para que el Mobile World Congress vuelva a abrir sus puertas en Barcelona. 16 meses después de cancelar la edición de 2020, una decisión que "aunque difícil, fue la correcta", según ha afirmado Mats Granryd, director general de la GSMA, el Congreso más importante del mundo de la tecnología volverá con unos objetivos mucho más discretos que los de ediciones anteriores. John Hoffman, CEO de la GSMA, ha explicado que espera que la asistencia se sitúe entre 30.000 y 50.000 personas (en la edición de 2019 se superaron los 109.000 visitantes).

Para animar la presencia local, la GSMA ha puesto en marcha la iniciativa "dar lo que recibimos", por la que pone a la venta una entrada a 21 euros para profesionales de industrias como automoción, transporte o medios de comunicación. An-

teriormente, la organización anunció una rebaja en el precio de entradas que, en algunos casos, pueden alcanzar el 27%.

CONNECTED IMPACT

Bajo el lema "Connected Impact" (Impacto Conectado) el Mobile World Congress pondrá de relieve cómo la tecnología está ayudando a sobrellevar la pandemia causada por la Covid-19. "El ecosistema de movilidad ha sido clave durante la pandemia. Ha permitido a la gente trabajar desde casa y mantener sus relaciones profesionales y personales y ha posibilitado que miles de empresas hayan podido mantener sus negocios abiertos", ha remarcado Mats Grandry.

Las principales empresas de base digital mostrarán así las últimas innovaciones relacionadas, no sólo con la telefonía móvil y las comunicaciones inalámbricas, sino también de sectores tan punteros como 5G, la Inteligencia Artificial, la robótica, la Realidad Virtual y la Realidad Aumentada, los drones, la innovación a través de startups y todo tipo de software y hardware. "El evento más importante del mundo regresa y esta vez de forma híbrida", resaltó Grandy.

MÁS DE 600 PONENTES

El MWC21 contará con ponentes de talla mundial, como es habitual en el evento. En esta edición, habrá más de 600 ponentes (el 70% acudirá físicamente a Barcelona), entre ellos un buen número de primeros espadas de empresas de una amplia variedad de sectores, como Julie Sweet, CEO de Accenture; Shuky Sheffer, CEO de Amdocs; Zina Jarrahi Cinker, director general de AMPT; Yang Jie, presidente de China Mobile; Mats Granryd, director general de GSMA; Arvind Krishna, CEO de IBM; Eugene Kaspersky, CEO de Kaspersky; Ana Maiques, CEO de Neuroelectrics; Sarah Wilkinson, CEO de NHS Digital; Stéphane Richard, director general y presidente de Orange; Cristiano Amon, presidente y CEO electo de Qualcomm Incorporated; Mathew Oommen, CEO de Reliance Jio; Nik Storonsky, fundador y CEO de Revolut; Anne Boden, CEO de Starling Bank; Danielle Royston, CEO de TelcoDR; José María Álvarez Pallete, presidente de Telefónica; Caroline Casey, fundadora de The Valuable 500; Hans Vestberg, presidente y CEO de Verizon ; Rima Qureshi, Board Deputy Chair, GSMA and Executive Vice President & Chief Strategy Officer de Verizon; Raffaele Annecchino, presidente y CEO de Viacom Networks International; Nick Read, CEO de Vodafone Group, o Xu Ziyang, director Ejecutivo y presidente de ZTE, etc.

EL MOBILE WORLD CONGRESS ESTÁ DE VUELTA

Además, el Mobile World Congress 2021 reunirá a los responsables políticos para debatir sobre la inclusión digital, la resiliencia de las redes y la maximización del potencial de 5G, el papel que tendrán estas tecnologías en la recuperación y cómo impactan las políticas que se ponen en marcha en el impulso del futuro digital

OLA DE CANCELACIONES Y MEDIDAS DE SEGURIDAD

¿La parte negativa? El Mobile World Congress abrirá sus puertas con la pandemia aún no controlada. Esto ha hecho que en los últimos meses se haya producido una ola de cancelaciones (Xiaomi, Samsung, Lenovo, Qualcomm, Ericsson, Nokia, Sony, Google, Facebook o Lenovo, entre otras, ya han anunciado que no estarán presencialmente en Barcelona) a pesar de que Hoffman ha recalcado que éste será un encuentro "seguro, híbrido y vibrante. Hemos trabajado con Fira de Barcelona, el Ayuntamiento de Barcelona, la Generalitat de Catalunya, el Ministerio de Industria, así como Turismo de Barcelona para mantener un ambiente seguro y controlado". Entre las medidas que se van a adoptar se encuentran la realización de pruebas, el rastreo de contactos, el diseño de "entornos sin contacto", la restauración, el monitoreo de asistentes, el incremento del personal médico y el distanciamiento social.

Los asistentes tendrán que descargarse la app My MWC, "una credencial digital que se activará y permitirá la entrada al evento una vez que se complete el registro, la autodeclaración y los test".

La organización exigirá pruebas negativas a asistentes de aquellos países con mayor número de contactos antes de viajar a España. "Serán las autoridades españolas las que dicten este requisito". Aquellos que decidan viajar a Barcelona en tren o coche "serán dirigidos a los centros de pruebas que se instalarán en el MWC para validar su estado de salud".

Participación española

Red.es e ICEX han dado a conocer el listado de las 26 empresas nacionales que integrarán el Pabellón de España del próximo MWC Barcelona 2021. Son de nueve comunidades y, de ellas, la mitad son de Cataluña, de donde proceden siete, y de Madrid, seis. También tendrán presencia tres dos andaluzas, una navarra, tres valencianas, una extremeña, dos gallegas y una balear.

En concreto son Core & Global IT Solutions y Petronics Tecnología (de Andalucía); Agile Content Inversiones, Alternative Energy Innovations, Amper S & C IoT, Masvoz Telecomunicaciones Interactivas, Netrivals, Nice People At Work, PayXpert Spain y Vintegris (de Cataluña); i3i Ingeniería Avanzada (de Navarra); Aoife Solutions, Kenmei Technologies y Pangeanic B I Europa, de la Comunidad Valenciana; e-Capture Research and Development (de Extremadura); Insurama Broker Online, Netun Solutions (de Galicia); Realisto Consulting (de Islas Baleares), y Alisys Digital, Co-Comm Servicios Telecomunicaciones, Datatronics, Dinero Por Tu Móvil, Netmetrix Solutions, Summa Networks Spain y Telecoming, de Madrid, y Wise Security Global, del País Vasco.

Estas compañías, que dispondrán espacio propio en el pabellón, mostrarán durante los cuatro días del evento sus servicios y soluciones en ámbitos de innovación como 5G, inteligencia artificial IoT, ciberseguridad o blockchain, entre otros.

Todos los participantes deberán presentar una prueba rápida negativa válida para acceder a la Fira que se tendrá que repetir cada 72 horas. La organización también realizará controles de temperatura en todos los puntos de acceso.

Las entradas y salidas se han duplicado para garantizar el distanciamiento social, no habrá credenciales y los restaurantes se han diseñado para garantizar el distanciamiento social. Asimismo, la Fira Gran Via ha incrementado los protocolos de higiene en todo el recinto (un nuevo sistema de ventilación mejorará el flujo de aire).

La GSMA ha resaltado la importancia de los eventos presenciales "para cambiar opiniones y hacer negocios" y reconoce "los esfuerzos extraordinarios que la gente está haciendo para asegurarse de que el MWC21 sea un evento indispensable".

como las inversiones durante el coronavirus, las OPV de fondos y la tokenización.

Finalmente, los organizadores han indicado que la edición de 2021 pretende ser neutro en carbono, al igual que la edición de 2019, que fue certificada oficialmente por AENOR International. Esta certificación convirtió al evento en la mayor feria del mundo con emisiones neutras de carbono y la GSMA está trabajando para reducir aún más el impacto ambiental y la huella de carbono del evento como parte de su liderazgo general en acción climática.

El Mobile World Congress incluirá como novedad Diversity4Tech, un programa que se desarrollará tras el acuerdo al que ha llegado la GSMA con Accenture que estará centrado en la diversidad y la inclusión. ■

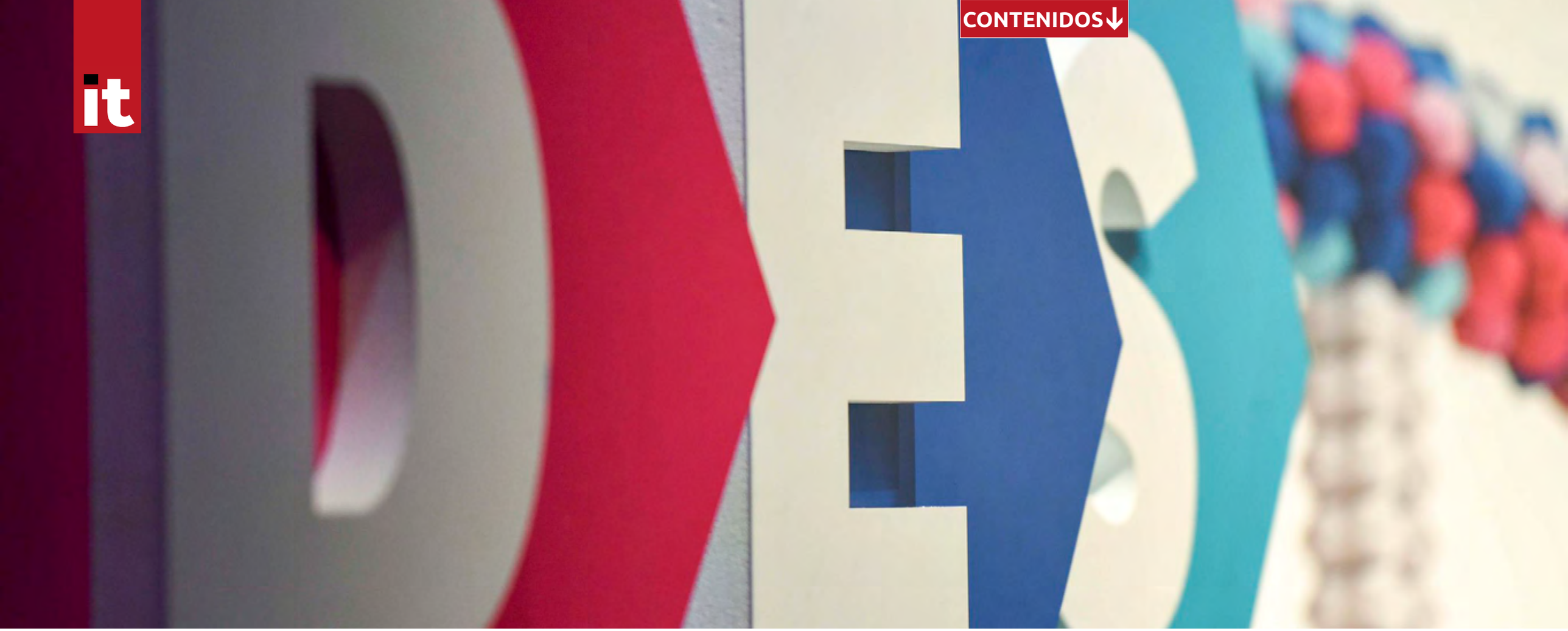
MÁS INFORMACIÓN

- Últimas novedades del Mobile World Congress 2021
- Información institucional del Mobile World Congress
- 50 estrategias para 2050

NUEVA EDICIÓN DE 4YFN

Dentro del marco del Mobile World Congress se celebrará el 4FNY. Este año el evento de startups reunirá en Fira Gran Vía a más de 400 startups internacionales expondrán sus últimos productos en el "Mercado de la Innovación", 150 ponentes compartirán ideas para impulsar el ecosistema móvil y 200 empresas harán sus presentaciones, esperando atraer la atención de los principales fondos e inversores de capital riesgo.

Como novedad de este año, el Programa de Inversores incluye una summit dedicado al intercambio de conocimientos entre la comunidad inversora. En él se debatirán tendencias recientes



EL EVENTO SE CELEBRARÁ EN MÁLAGA LOS PRÓXIMOS CINCO AÑOS

DES cierra sus puertas con 8.134 asistentes presenciales y un impacto para Madrid de 17 millones de euros

Esta edición de DES, Digital Enterprise Show, primer evento tecnológico presencial que se celebra en Europa desde el inicio de la pandemia, acaba de cerrar sus puertas con un buen sabor de boca: 8.134 asistentes presenciales y 11.489 conexiones únicas vía streaming de más de 30 países. El impacto económico para Madrid ha sido de 17 millones de euros.

El primer gran evento tecnológico europeo, que se ha celebrado en formado presencial, se ha cerrado este viernes con cifras que están lejos de las que manejaba antes de la pandemia, pero que dejan un buen sabor de boca. Al final, esta quinta edición "llena de retos", según dice la organización en un comunicado, ha reunido a 8.134 visitantes en IFEMA, a los que hay que sumar 11.489 conexiones únicas a través de streaming de más de 30 países. El impacto económico que ha dejado para Madrid ha alcanzado los 17 millones de euros.

La edición de 2019 se había clausurado, según informó la organización en con más de 26.000 visitantes internacionales, sobre todo portugueses, británicos, alemanes, estadounidenses e israelíes. En la edición de 2019, la feria supuso un impacto para la ciudad de 45 millones de euros, pero es cierto que la situación este año es bien distinta.

Al respecto de esta edición, Albert Planas, director de DES-Digital Enterprise Show, ha explicado que "ha sido un reto para la organización y para las empresas que han confiado en su celebración. Estamos orgullosos del trabajo realizado, que nos ha convertido en el primer evento tecnológico en formato presencial en el sur de Europa. Y por supuesto estamos felices de haber podido ayudar a las empresas que cada año nos acompañan en DES a reencontrarse con sus compañeros y colegas, en un entorno seguro".

DES VIAJA A MÁLAGA

Este es el último año que el evento se celebra en Madrid, tras cinco años teniendo lugar en IFEMA. La organización de DES, junto con representantes de la Junta de Andalucía, la Diputación, y el ayuntamiento de la ciudad andaluza, anunciaron que, a partir de 2022, el Palacio de Ferias y Congresos de Málaga (FYCMA) será la nueva sede del evento para los próximos cinco años.

Con el traslado hay también un cambio de planteamiento como sugiere el hecho de intentar dar a este foro más continuidad a lo largo del año. En este sentido, Alberto Planas, director general de DES y NEBEXT, ha recalcado que "el objetivo es trascender la celebración de DES durante tres días, y construir algo que dure todo el año, y para ello necesitamos administraciones que crean en ello, que estén liderando la digitalización y que tengan las tecnologías en sus fundamentos".

DES ha reunido a 8.134 visitantes en IFEMA, a los que hay que sumar 11.489 conexiones únicas a través de streaming de más de 30 países

Planas estuvo acompañado por Elías Bendodo, Consejero de Presidencia de la Junta de Andalucía; José Francisco Salado, Presidente de la Diputación de Málaga; y Francisco de la Torre, Alcalde de Málaga, que celebraron esta alianza y las oportunidades que se abren en el futuro cercano para impulsar a Málaga y a Andalucía como referentes en innovación en Europa.

Bendodo afirmó que "éste es un claro ejemplo de colaboración entre administraciones. La Junta de Andalucía, la Diputación y el Ayuntamiento de Málaga nos hemos puesto de acuerdo para impulsar esta iniciativa y convertir a Málaga en un referente internacional en innovación. Celebrar las siguientes ediciones de Digital Enterprise Show en Málaga va a potenciar la economía digital andaluza y por eso hoy estamos de enhorabuena".

En los cinco años en Madrid, DES ha reunido a 91.450 congresistas, procedentes de todo el mundo, con un impacto económico acumulado para la ciudad de más de 135 millones de euros. En total, por sus auditorios han pasado 2.400 expertos en liderazgo, tecnología e innovación, en más de 600 conferencias. El número de expositores ha superado los 1.200.

LA EDICIÓN DE 2021

DES 2021 ha contado con más de 434 expertos en tecnologías que han centrado sus intervenciones en las estrategias de liderazgo y en las tecnologías, que las empresas necesitan hoy para hacer negocios y generar riqueza y empleo en el mundo que ha llegado tras la crisis sanitaria. Inteligencia Artificial, 5G, Cloud, Ciberseguridad o Sostenibilidad han sido algunos de los grandes temas que se han abordado durante los tres días de congreso.

Además, ha acogido también la celebración del workshop 'Tecnología 5G: Oportunidades para la Industria 4.0' organizado por Barcelona Mobile World Capital, el Observatorio Nacional 5G y Nokia. De la mano de la asociación VR/AR, ha sido el escenario de presentación del proyecto 'A la música con los cinco sentidos' de la Escuela Superior de Música Reina Sofía, que está financiado por la Fundación Santander y desarrollado por One Digital Consulting, y que impulsa la educación musical a través de tecnologías de Realidad Virtual.

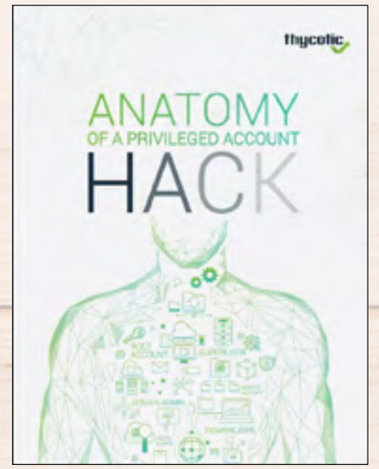
Empresas líderes han presentado soluciones y estudios para impulsar la digitalización y los resultados del ecosistema empresarial. Es el caso de Carat, que ha presentado su estudio Consumer Vision 2030, ofreciendo una imagen del consumidor post pandemia en primicia a los asistentes a DES2021; o T-Systems, que también ha elegido la quinta edición de DES para lanzar su solución ENAE que reduce los costes de implantación de proyectos IoT. ■

MÁS INFORMACIÓN

Digital Enterprise Show 2021

La documentación TIC, a un solo clic

Anatomía del ataque a una cuenta privilegiada



Este documento técnico realizado por Thycotic describe un ataque a una cuenta privilegiada; explica cómo los atacantes externos o los internos malintencionados pueden explotar las vulnerabilidades utilizando ejemplos como la contraseña de una cuenta de correo electrónico comprometida que se convierte en una violación total de la seguridad de la red.

7 consejos para proteger los datos de tu empresa y vencer al ransomware

La pérdida de datos no es una broma. Los ataques de ransomware y malware van en aumento, pero ése no es el único riesgo. Con demasiada frecuencia, las empresas piensan que sus datos están bien respaldados, pero en realidad no lo están. Este documento de Commvault muestra siete razones comunes por las que las empresas pierden datos, a menudo porque nunca estuvieron realmente protegidos, junto con consejos para ayudarte a evitar que te ocurra lo mismo.

Cloud Migration: Apuesta por el futuro de tu organización en la nube

En tiempos de incertidumbre, la migración a cloud supone una ventaja organizacional al obtener una mayor funcionalidad, escalabilidad y flexibilidad, además de accesibilidad en cualquier momento y lugar. Este documento de Making Science recoge las principales ventajas de la migración a la nube, ejemplos de migración y las capacidades que ofrece Google Cloud a las organizaciones.

Guía para implementar una CDN moderna

Este documento de Fastly señala la evolución de la relación de los desarrolladores con la CDN (Red de Distribución de Contenidos) y explica por qué las CDNs tradicionales están obsoletas. El texto también detalla los beneficios que pueden aportar las CDNs modernas, que van desde una mejor visibilidad de los patrones de tráfico hasta el diseño de APIs que potencian una experiencia de usuario personalizada.

Conectando personas y datos: descubre HPE Data Services Cloud Console y HPE Alletra

Transformarse apoyándose en los datos es el objetivo de muchas organizaciones. Sin embargo, no es sencillo cuando estás atado a la complejidad de los propios datos y de la infraestructura. HPE cumple con su visión unificada de la Gestión de los Datos con una nueva plataforma de servicios de datos que opera estos datos en la nube, independientemente de dónde se encuentren, y unifica las operaciones de datos.

Para hablar de cómo superar estos restos, en este IT Webinar, contamos con la participación de Susana Vila, responsable de la unidad de negocio de Almacenamiento de HPE, y Roberto Torres, responsable del grupo de preventa de Almacenamiento en HPE, quienes nos hablaron de Data Services Cloud Console, que ofrece un punto único donde unificar las operaciones de datos, desde el extremo de la red a la nube, aportando agilidad cloud a su infraestructura dondequiera que resida y simplificando la gestión de los datos en todo su ciclo de vida; y de HPE Alletra, que supone todo un cambio de paradigma en la infraestructura de datos, ya que ha sido creada como nativa para la nube y administrada por la consola de gestión cloud, con el objetivo de acelerar la innovación y ofrecer una arquitectura flexible para ejecutar cualquier aplicación.

UN MUNDO MOVIDO POR DATOS

La Transformación Digital está en la mente de todas las compañías, independientemente de su tamaño o sector de actividad, y el potencial de los datos es clave para su éxito, unos datos que no paran de crecer. Al día se crean 2,5 quintillones de bytes, una excelente materia prima para crear e innovar. Pero las empresas tienen que superar una serie de retos significativos. Tal y como explica Susana Vila, "los CIO tienen varias cosas en las que pensar, pero la primera de ellas es en sus clientes, que exigen una adecuada experiencia de uso, si bien crear una aplicación que ofrezca una gran experiencia de usuario pero no tenga detrás el almacenamiento de los datos para respaldarla, no serviría para nada. Desde HPE proporcionamos la tranquilidad de poder ofrecer una experiencia satisfactoria con el respaldo del almacenamiento que necesitan".

Pero, además, "el CIO tiene que pensar en la TI", continúa Susana Vila, "donde necesita mayor flexibilidad, menores gastos de administración, mayor disponibilidad de datos y aplicaciones, y que el gasto vaya acompasado con las necesidades de su negocio; y tiene que pensar en el propio negocio, tiene que sacar el mayor rendimiento de sus datos para convertirlos en mayor valor para su empresa".

CONECTANDO PERSONAS Y DATOS: DESCUBRE HPE DATA SERVICES CLOUD CONSOLE Y HPE ALLETRA

NUEVOS RETOS Y DESAFÍOS

La exigencia de la economía digital plantea una serie de retos y desafíos a los responsables de TI, y para ayudarles se han redefinido las reglas del almacenamiento. Según explica Susana Vila, "hay tres elementos fundamentales en esta redefinición. Primero, el almacenamiento tiende a ser completamente híbrido, lo que permite a las empresas tener las cargas de trabajo donde quiera tenerlas, tanto en la nube como on-premise, con una movilidad de datos inmediata, sencilla y sin paradas de servicio, para lo que nosotros proponemos HPE Cloud Volumes, que permite desplegar estas estas cargas en la nube e, incluso, replicarlas para una mayor disponibilidad".

El segundo de los elementos es, continúa, "una gestión sencilla, que indique al responsable, incluso,

dónde ubicar las cargas de trabajo en función de sus propis análisis, y, el tercero, y quizá más importante, es que esa experiencia la puedas consumir desde cualquier lugar, incluso desde el smartphone".

La propuesta de HPE para responder a estos retos y estas necesidades en una visión unificada de la gestión de los datos, que consiste en "reducir la complejidad y los silos de la infraestructura de la hibridación más convencional. Es una consola nativa en la nube con sistemas optimizados para la gestión de las cargas de trabajo de los clientes, tanto en nube como en infraestructuras tradicionales. Con esto, liberamos los datos y conseguimos sacar mayor valor para nuestras organizaciones".

EXPERIENCIA CLOUD Y REDEFINICIÓN DE LA ARQUITECTURA

Este planteamiento se materializa, según detalla Roberto Torres, "ofreciendo una nueva experiencia cloud para nuestros clientes con un hardware desplegado on-premise. Esta redefinición de la arquitectura se basa en varios elementos. Primero, un portal, Data Service Cloud Console, que incorpora una serie de aplicaciones que los clientes pueden desplegar para la gestión del dato. En primera instancia, será el Almacenamiento con Data Operation Manager. Además, tenemos unas arquitecturas hardware on-premise que se integran con esta nueva visión Cloud Experience, que nos permite dar a los clientes lo mejor de los dos mundos: una experiencia cloud sencilla de manejar, un time-to-market limitado, un compliance adecuado del dato al tenerlo en su data center, y, por supuesto, alta disponibilidad".

Por otro lado, continúa, "la infraestructura, HPE Alletra, con dos modelos que se van a poder desplegar en los centros de datos del cliente".

Data Service Cloud Console permite, apunta Roberto Torres, "gestionar el Almacenamiento desde un punto centralizado", independientemente de dónde esté desplegada la infraestructura, lo que proporciona "una visión generalizada del toda la TI".

Y esta consola se complementa con el anuncio de nuevas cabinas, basadas en Nimble y Primera, que permiten "conectarnos a esta nueva forma de gobernar el Almacenamiento. Incluye mejoras tecnológicas como una tecnología NVM extremo a extremo, lo que nos ofrece unos rendimientos y unas capacidades mucho más elevadas que hasta la fecha".

Clica para ver la intervención de Susana Vila

"El CIO tiene que sacar el mayor rendimiento de sus datos para convertirlos en mayor valor para su empresa"

SUSANA VILA, RESPONSABLE DE LA UNIDAD DE NEGOCIO DE ALMACENAMIENTO DE HPE

ALMACENAMIENTO COMO SERVICIO...

En palabras de Susana Vila, como los clientes están preocupados por

cómo alinear sus gastos de infraestructura con las necesidades que tienen, "no tiene sentido no ofrecer el almacenamiento como servicio, con lo que el nuevo lanzamiento se integra perfectamente con HPE GreenLake, porque permite tener una experiencia completa".

Y pensando en las necesidades del cliente, "HPE tiene previsto que tanto las cabinas HPE Primera como HPE Nimble se puedan integrar con la nueva consola, de forma que puedan tener un único punto de control para todo el almacenamiento que tienen con nosotros".

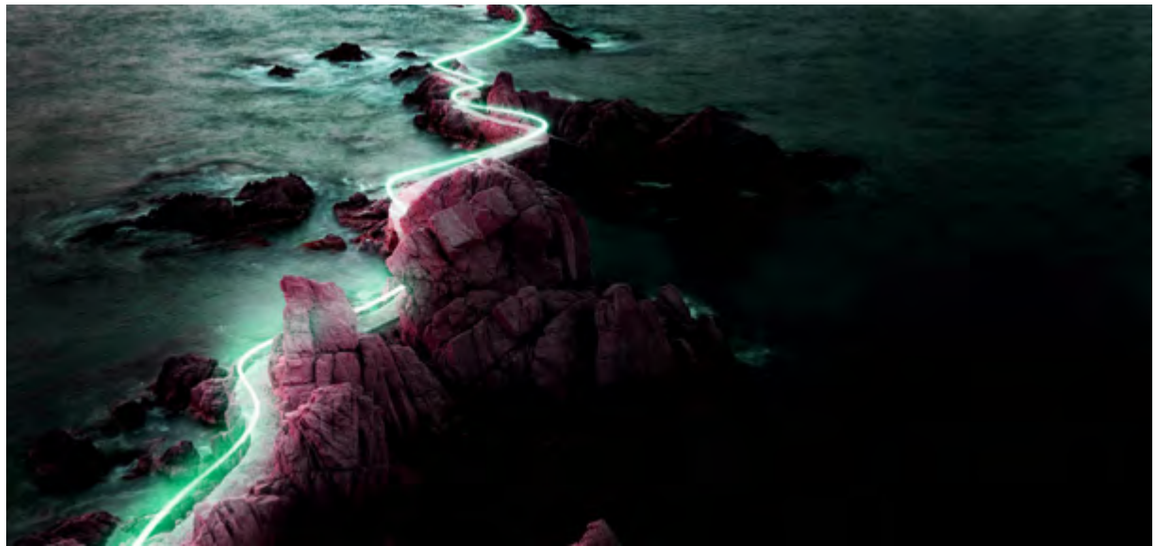
...Y, POR SUPUESTO, SEGURIDAD

Según comenta Roberto Torres, "en HPE tenemos experiencia a la hora de desacoplar la gestión y el governance de lo que son los dispositivos de TI en la nube pública. De hecho, seguimos la filosofía que ya teníamos en Aruba Central, todas las comunicaciones están encriptadas, hay doble factor de autenticación, hay acceso a nivel de roles, y, aunque la gestión está en la nube, el dato está en las cabinas del cliente, y no es visible desde la nube". ■

Clica para ver la intervención de Roberto Torres

"La nueva arquitectura ofrece una nueva experiencia cloud para nuestros clientes con un hardware desplegado on-premise"

ROBERTO TORRES, RESPONSABLE DEL GRUPO DE PREVENTA DE ALMACENAMIENTO EN HPE



MÁS INFORMACIÓN

- Conectando personas y datos: descubre HPE Data Services Cloud Console y HPE Alletra
- Data Services Cloud Console: Transformando el almacenamiento y gestión de datos del Edge a la Cloud
- Infografía HPE Alletra: Potencia tus datos del Edge a la Cloud
- HPE Alletra: Potencia tus datos del Edge a la Cloud

it User
TECH & BUSINESS

CONTENIDOS↓

FORO IT USER:

NUEVOS IMPULSOS PARA LA EVOLUCIÓN DE LA ADMINISTRACIÓN DIGITAL

Organiza

it Digital MEDIA GROUP

Socios estratégicos

Astic

Foro CPP colaboración público-privada TECNOLOGÍA & INNOVACIÓN

Patrocinador Platinum

salesforce

Patrocinadores Gold

aruba a Hewlett Packard Enterprise company

Forcepoint

MicroStrategy

PEGA

paloalto NETWORKS

VMRAY

V-Valley the Value of esprinet

Patrocinadores Silver

Bitdefender

CYTOMIC

SOPHOS Cybersecurity evolved.

THALES

TENDENCIAS TECNOLÓGICAS

QUE GUIARÁN LA TRANSFORMACIÓN DIGITAL DE LOS GOBIERNOS

LAS ORGANIZACIONES GUBERNAMENTALES SE HAN ENFRENTADO A GRANDES DIFICULTADES A CAUSA DE LA CRISIS SANITARIA, Y HAN RECURRIDO A LAS NUEVAS TECNOLOGÍAS PARA PODER PRESTAR MEJORES SERVICIOS A LOS CIUDADANOS. ESTA ESTRATEGIA HA DADO SUS FRUTOS, Y LOS EXPERTOS DE GARTNER CREEN QUE A PARTIR DE ESTE AÑO VAN A PROFUNDIZAR MÁS EN LA TRANSFORMACIÓN DIGITAL, GUIÁNDOSE POR UNA SERIE DE TENDENCIAS TECNOLÓGICAS QUE COGERÁN FUERZA EN 2021.

Ante la necesidad de imponer medidas de confinamiento y distanciamiento social, las organizaciones gubernamentales han tenido que recurrir a la tecnología para seguir prestando servicios de calidad a los ciudadanos. La clave principal de este cambio está en la necesidad de las administraciones públicas de habilitar canales de servicio a distancia, que permitan realizar todo tipo de trámites burocráticos sin tener que acudir a las instituciones. También está la imperiosa necesidad de contar con mecanismos de atención sanitaria telemática que permitan minimizar la fluencia de pacientes a los centros médicos y hospitales. Y también para proteger a los ciudadanos y trabajadores en otras áreas de servicios públicos, como el transporte, la hacienda pública, el paro, y un largo etcétera.

Las ventajas que proporcionan las nuevas tecnologías son enormes, pero su implementación se enfrenta a numerosos desafíos, que van desde el enorme costo potencial a la segu-

ridad de los datos confidenciales y al desarrollo de una buena experiencia del ciudadano. Para las administraciones está cada vez más clara la necesidad de avanzar en la transformación digital para lograr un nuevo nivel de optimización y personalización de los servicios públicos. Los expertos de Gartner identifican 10 tendencias tecnológicas en las que se apoyarán las agencias gubernamentales para avanzar en este camino a partir de 2021, ayudando a la recuperación posterior a la pandemia y a construir nuevos modelos de servicio público.

En su artículo, Rick Howard, vicepresidente de investigación y presidente de Gartner, explica que "la pandemia de COVID-19 ha estimulado la aceleración de la innovación digital en el sector gubernamental de todo el mundo, presentando a los líderes gubernamentales nuevas oportunidades para utilizar datos y tecnologías para generar confianza, agilidad y resiliencia en las instituciones públicas". Aunque la pandemia seguirá generando nuevos desafíos durante un tiempo, incluso más allá de 2021, Howard opina que "han surgido tendencias tecnológicas que abordan desafíos críticos en áreas como la seguridad, la contención de costos y la experiencia de los ciudadanos".

Con el fin de aportar una visión más clara de la situación y ayudar a las agencias gubernamentales a abordar la transformación digital en la que están inmersas, los expertos de Gartner han elaborado una lista con 10 tendencias tecnológicas estratégicas. Explican que están directamente relacionadas con las cuestiones de política y administración pública que los CIO gubernamentales deberán abordar de cara a la recuperación tras la pandemia. Y confían en que esta lista les permitirá identificar las tendencias tecnológicas que mejor se ajusten a sus necesidades concretas, sentando las bases del futuro.

MODERNIZACIÓN ACELERADA DE LAS INFRAESTRUCTURAS HEREDADAS

Las agencias gubernamentales se enfrentan constantemente a los riesgos y limitaciones de las infraestructuras heredadas, debido a la implementación fragmentada de tecnologías que no siempre trabajan bien juntas, y que pueden generar interrupciones. En algún momento deben romper con el círculo vicioso que ha mantenido esta situación desde hace décadas, y los expertos de Gartner creen que este año muchas agencias gubernamentales acelerarán la modernización de sus sistemas, adoptando arquitecturas modulares modernas.

Aunque la necesidad de modernizar ese legado es algo que conocen bien los CIO gubernamentales, la pandemia ha generado más conciencia sobre los riesgos de depender de una infraestructura anticuada. Por ello, Gartner pronostica que para 2025 más de la mitad de las

agencias gubernamentales habrá modernizado las aplicaciones centrales críticas heredadas, con el fin de mejorar su resiliencia y actividad.

SEGURIDAD ADAPTATIVA

Las estrategias tradicionales de seguridad se vuelven anticuadas, lo que genera importantes riesgos para las agencias gubernamentales. Sobre todo, teniendo en cuenta que la transformación digital obligará a trabajar con grandes cantidades de datos confidenciales. Los expertos destacan que las agencias gubernamentales van a adoptar una estrategia de seguridad adaptativa, que trata el riesgo, la confianza y la seguridad como un proceso continuo y adaptable. Esto le permite anticiparse a los problemas y reducir las constantes amenazas cibernéticas, dejando atrás las estrategias reactivas del pasado para adoptar un enfoque más proactivo y flexible.

Según explican en Gartner, este enfoque de seguridad incluye mecanismos de predicción, prevención, detección y respuesta. Y también supone abandonar las nociones tradicionales de perímetro, asumiendo que no existe un límite definido entre lo que es seguro y lo que no. Esto es fundamental en los entornos digitales gubernamentales, cada vez más conectados y heterogéneos, en los que el riesgo puede provenir de cualquier lugar. Las previsiones de Gartner son que, para el año 2025, el 75% de

LOS EXPERTOS DE GARTNER IDENTIFICAN 10 TENDENCIAS TECNOLÓGICAS EN LAS QUE SE APOYARÁN LAS AGENCIAS GUBERNAMENTALES PARA AVANZAR EN ESTE CAMINO DE TRANSFORMACIÓN A PARTIR DE 2021

los CIO gubernamentales será directamente responsables de la seguridad fuera de los entornos de TI, agregando entornos de tecnología operativos y de misión crítica.

TODO COMO SERVICIO (XAAS)

Ante las nuevas necesidades que han surgido a raíz de la pandemia, muchas instituciones gubernamentales necesitan dar un gran salto cualitativo en sus capacidades tecnológicas. Pero esto implica realizar grandes inversiones, sobre todo si se quiere lograr en un corto espacio de tiempo, por lo que muchas agencias gubernamentales están siguiendo el ejemplo del mundo empresarial, optando por modalidades as-a-Service.

Esto ha dado lugar a una corriente de "Todo como Serivicio" (XaaS), que se basa en adquirir todo un conjunto de servicios comerciales y de TI basados en la nube, bajo un modelo de suscripción. Según Gartner, para el año 2025, el 95% de las nuevas inversiones de TI de las agencias gubernamentales se realizarán bajo modalidades de suscripción. Esto permitirá a las organizaciones superar las limitaciones de la infraestructura heredada, adquirir más escalabilidad y reducir el tiempo requerido para brindar servicios digitales.

GESTIÓN DE CASOS COMO SERVICIO

En muchas agencias gubernamentales se emplea el estilo de trabajo basado en casos, y en muchos departamentos toda la gestión de casos se lleva a cabo desde una cartera de soluciones independiente y limitada. Pero mediante la Gestión de Casos como Servicio (CMaaS) las organizaciones disponen de una nueva forma de desarrollar la agilidad institucional, mediante la aplicación de principios y prácticas comerciales componibles. Esto permite reemplazar los sistemas de administración de casos heredados con productos modulares que pueden ser ensamblados, desensamblados y recompuestos rápidamente, según las necesidades de cada momento. Gartner prevé que, para 2024, las organizaciones que hayan adoptado una arquitectura de aplicaciones de gestión de casos componible podrán implementar nuevas funciones un 80% más rápido que las que no sigan este camino.

IDENTIDAD DIGITAL CIUDADANA

Uno de los requisitos fundamentales para lograr una buena experiencia de ciudadano es contar con un sistema de identidad digital que permita a las personas identificarse inequívocamente para acceder a los servicios públicos. Desarrollar una plataforma unificada de identidad digital es un gran desafío para los gobiernos, pero a raíz de la pandemia se ha convertido en una prioridad, lo que está impulsando la evolución de los ecosistemas de identidad digital.

Los expertos de Gartner creen que a partir de este año las agendas políticas de muchos gobiernos incluirán el desarrollo de un ecosistema de identidad digital para los ciudadanos. Y también la necesidad de vincularlo con todos los casos de uso más destacados para la Administración. Aunque no se espera que exista un verdadero estándar de identidad global, portátil y descentralizado hasta 2024. Esto permitirá abordar numerosos casos de uso emergentes, dentro del ámbito comercial, personal y social, entre otros.

INTERCAMBIO DE DATOS COMO PROGRAMA

Una de las principales barreras a las que se enfrentan los gobiernos de cara a la transformación digital es la falta de coordinación de datos entre las diferentes agencias. Así, tradicionalmente, los intercambios de información de los ciudadanos se realizan de forma puntual, solo en caso muy concretos. Debido a las regulaciones de privacidad mal enfocadas, y a que no existe una infraestructura diseñada para unificar la información de cada persona, casi cualquier solicitud de traspaso de información requiere un nivel de burocracia que acaba con cualquier aspiración de crear una buena experiencia del ciudadano.

Para romper con los conceptos tradicionales que frenan la digitalización de los servicios gubernamentales los expertos recomiendan adoptar el concepto de intercambio de datos como programa. Esto consiste en desarrollar una plataforma unificada con capacidad de escalar los servicios y reutilizar muchas capacidades, adoptando un enfoque más componible para los servicios gubernamentales. En Gartner creen que, para el año 2023, el 50% de las organizaciones gubernamentales establecerán estructuras formales de responsabilidad para el intercambio de datos, lo que incluirá los estándares necesarios para implementar la estructura, la calidad y la puntualidad de los datos.

SERVICIOS PÚBLICOS HIPERCONECTADOS

Siguiendo la misma estrategia del mundo empresarial, los gobiernos están avanzando para desarrollar una cartera servicios públicos hiperconectados, lo que abarca numerosas tecnologías, herramientas y plataformas para automatizar tantos procesos comerciales y de TI como sea posible. En este camino, los CIO gubernamentales adoptarán los principios y las prácticas de la hiperautomatización para desarrollar “nuevos procesos comerciales de extremo a extremo, hiperconectados y altamente automatizados”, así como servicios públicos que requieran la mínima intervención humana. Así,

para 2024, se espera que el 74% de los gobiernos habrá lanzado o estará preparando, al menos, tres iniciativas de hiperautomatización en toda la empresa.

PARTICIPACIÓN CIUDADANA MULTICANAL

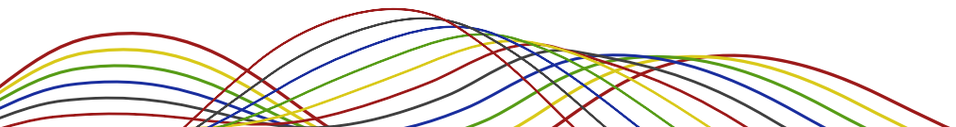
El año pasado se reveló la importancia de contar con la participación ciudadana para ayudar a combatir problemas como crisis sanitarias, eventos climáticos extremos y otras situaciones complicadas que afectan al conjunto de la sociedad. Los gobiernos han tomado nota de ello y a partir de ahora van a trabajar en construir un ecosistema de participación ciudadana multicanal, que permita a las personas y a la administración interactuar de forma fluida y segura. Esto será fundamental para construir una experiencia del ciudadano óptima y personalizada, en la que las personas puedan hacerse oír a través del canal que prefieran. Gracias a ello, Gartner prevé que, para 2024, el 30% de los gobiernos utilizarán métricas de participación para rastrear la cantidad y la calidad de la participación ciudadana en las decisiones políticas y presupuestarias.

ANALÍTICA OPERATIVA

Los datos son la base de cualquier estrategia digital, y los gobiernos necesitarán aprender a trabajar con la información de formas más creativas y provechosas. Esto implica apostar por tecnologías como la analítica avanzada, la inteligencia artificial y el aprendizaje automático. Aplicando esta estrategia de analítica operativa en todos los niveles de los servicios públicos, los gobiernos cuentan con información mucho más completa, precisa y fiable, que sirve para mejorar la eficiencia, la eficacia y la coherencia en la toma de decisiones. Además, esto mejora la calidad de la experiencia de los ciudadanos y, según Gartner, para el año 2024, el 60% de las inversiones gubernamentales en inteligencia artificial y análisis de datos tendrán como objetivo mejorar la toma de decisiones y los resultados operativos en tiempo real. ■

CONTENIDO RELACIONADO

10 Tendencias tecnológicas para agencias gubernamentales, Gartner



Foro Administración Digital 2021

EMPRESA GUBERNAMENTAL COMPONIBLE

Este concepto se basa en la aplicación del concepto de diseño componible a la organización, lo que permite ampliar la reutilización de capacidades y adaptarse de forma continua a los constantes cambios regulatorios, legislativos y de normativa pública. Ante esta situación, los CIO de las agencias gubernamentales están optando por modalidades de gobierno componible, lo que les permitirá superar las limitaciones de los tradicionales enfoques basados en silos independientes. En su lugar, el enfoque de gobierno componible les permite administrar servicios, sistemas y datos de forma mucho más ágil para adaptarse a las exigencias cada vez mayores de la sociedad digital. La investigación de Gartner revela que, para 2023, el 50% de las empresas de tecnología que trabajan con los gobiernos ofrecerán capacidades comerciales empaquetadas que admitirán aplicaciones componibles.

Acercamos el Gobierno a los Ciudadanos

NUEVOS IMPULSOS PARA LA EVOLUCIÓN DE LA ADMINISTRACIÓN DIGITAL

LAS NOVEDADES ALREDEDOR DE LOS FONDOS NEXTGENERATIONEU, ASÍ COMO LOS RETOS A LOS QUE SE ENFRENTA EL SECTOR PÚBLICO EN SUS PROCESOS DE TRANSFORMACIÓN, FUERON LOS HILOS CONDUCTORES DEL FORO IT USER: NUEVOS IMPULSOS PARA LA EVOLUCIÓN DE LA ADMINISTRACIÓN DIGITAL..

SI QUIERES REPASAR LO QUE PASÓ EN ESTE FORO IT USER, CLICA EN LA IMAGEN

El Plan España Digital 2025 recoge entre sus ejes el impulso a la digitalización de la Administración Pública. Según el informe de la Comisión Europea DESI, España se sitúa en el segundo lugar entre los 28 miembros de la UE en la clasificación de los países con mejor desarrollo de sus servicios públicos digitales.

No obstante, también reconoce que "la mera existencia de servicios electrónicos no produce eficiencia ni reducción de cargas administrativas, sino que requiere de una modernización de procesos y adaptación de los canales para lograr un uso masivo eficaz, y seguro por ciudadanía y empresas".

La llegada de los fondos europeos NextGenerationEU, la disponibilidad de tecnología y empresas tecnológicas preparadas en nuestro país para apoyar a la Administración Pública en su transformación, y la adaptación de los perfiles TIC que trabajan en los organismos públicos, constituyen una excelente oportunidad para potenciar ese objetivo de digitalización y, por tanto, de excelencia de las AA.PP. Y la oportunidad es ahora.

Estos tres ejes fueron analizados en el evento Foro IT User: Nuevos impulsos para la evolución de la Administración digital el pasado 18 de mayo, una cita en la que repasamos todas las novedades introducidas en la última versión del Plan de Recuperación, Transformación y Resiliencia. ■

“LAS PRIORIDADES SON LA DIGITALIZACIÓN DE LA ADMINISTRACIÓN Y LOS PROCESOS, LA TRANSICIÓN ENERGÉTICA Y LA PROPIA REFORMA DE LAS ADMINISTRACIONES PÚBLICAS”

JUAN JESÚS TORRES, SECRETARIO GENERAL DE ADMINISTRACIÓN DIGITAL

LAS PRIORIDADES DE LA ADMINISTRACIÓN CENTRARON LA ENTREVISTA INAUGURAL DEL EVENTO. CLICA EN LA IMAGEN PARA VERLA.

El Secretario General de Administración Digital ofreció en el Foro IT User. Nuevos impulsos para la evolución de la administración digital, más detalles del Plan de Recuperación, Transformación y Resiliencia, sobre todo lo relacionado con el plan para la modernización de la Administración.

Tal y como explicaba el Secretario General de Administración Digital, “este plan de modernización se enmarca en una serie de iniciativas estratégicas que se están poniendo en marcha con el objetivo de recuperar el PIB y crear puestos de trabajo. Todos estos planes, incluyendo el de modernización de la Administración, cuentan con cuatro principios básicos: transición ecológica, la dimensión digital, la igualdad de género y la cohesión social y territorial, con el objetivo que cualquier ciudadano o ciudadana goce de las mismas oportunidades en cualquier lugar del territorio”.

Este plan se articula alrededor de 10 políticas "palanca" y una de ellas es, "efectivamente, conseguir una Administración para el siglo XXI", y para ello está previsto que "en el período 2021-2023 se movilice un total de 4.315 millones de euros para inversiones relacionadas con la transformación de las Administraciones Públicas, lo que incluye el ámbito concreto de la digitalización como la transformación energética. En concreto, para la Transformación Digital se destinarán 3.165 millones de euros entre 2021 y 2023".

MÁS DE UN CENTENAR DE INICIATIVAS

Estas palancas se traducen en más de un centenar de reformas y focos de inversión. Tal y como explica Juan José Torres, las prioridades son "la digitalización de la Administración y los procesos, la transición energética y la propia reforma de las Administraciones Públicas".

En este sentido, la digitalización de la Administración y los procesos se centran en "dos ámbitos: uno transversal, con iniciativas que pueden afectar a toda la Administración; y otro en determinados ámbitos sectoriales, destinados a Ministerios con especial relación con la ciudadanía".

En cuanto a la transición energética busca "tanto el ahorro como la eficiencia energética, así como el incremento del uso de energías renovables y de una movilidad sostenible".

"ESTÁ PREVISTO QUE EN EL PERÍODO 2021-2023 SE MOVILICE UN TOTAL DE 4.315 MILLONES DE EUROS PARA INVERSIONES RELACIONADAS CON LA TRANSFORMACIÓN DE LAS ADMINISTRACIONES PÚBLICAS"

La modernización de las administraciones públicas persiguen "una mejora de la estructura organizativa como de la reforma normativa que es necesaria. Y hay tres ejes fundamentales. El primero, referido a la modernización de la Administración General del Estado, tiene como objetivo poner en marcha procesos de transformación de carácter transversal para abordar la mejora de los servicios públicos desde el punto de vista de la ciudadanía, incluyendo medidas que faciliten la usabilidad y mejoren la calidad de los servicios prestados. El segundo eje, son proyectos de alto valor por el impacto que tienen en los ciudadanos por la prestación de servicios, como son el caso de la Sanidad, la transformación digital de la administración de Justicia, la transformación digital del empleo, y la digitalización en el ámbito de la inclusión, Seguridad Social e inmigraciones, cuyo objetivo es evolucionar estos servicios públicos, incluyendo la Gerencia de Informática de la Seguridad Social. El tercer eje es el relativo a la transformación del Ministerio de Política Territorial y Función Pública, cuyos esfuerzos se centrarán en la mejora de las iniciativas en el propio departamento, como en Comunidades Autónomas y entidades locales, a través de proyectos que se realizarán coordinadamente con ellos".

UN PLAN CON VARIAS FASES Y DIFERENTES ENTIDADES

En palabras de Juan José Torres, "llevamos trabajando bastantes meses en el desarrollo de estos proyectos y en el Plan de Digitalización de las Administraciones Públicas. Son proyectos ambiciosos y en la primera fase se han determinado los objetivos, ahora estamos a la espera de la aprobación por parte de Bruselas, y estamos preparando las licitaciones y contratos públicos que van a aterrizar y materializar estos proyectos, así como en las reformas necesarias".

Además de los plazos, estos planes involucran a muchas entidades, "los planes son complejos, pero de la gobernanza se encarga ya el Real Decreto Ley 36/2020, que se aprobó para facilitar el modelo de gobernanza y la ejecución y desarrollo del Plan de Recuperación. ■

aruba
a Hewlett Packard
Enterprise company

LLEVE LA SEGURIDAD AL EDGE

Proteja su entorno de trabajo híbrido

FONDOS NEXTGENERATIONEU, ¿QUÉ SABEMOS HASTA AHORA?

JOSÉ MIGUEL MUÑOZ, DIRECTOR DEL FORO DE COLABORACIÓN PÚBLICA-PRIVADA (FORO CPP), NOS EXPLICA CON DETALLE CÓMO SE VAN A EMPLEAR LOS FONDOS EUROPEOS DE RECUPERACIÓN, QUÉ PLANES LOS VAN A ARTICULAR, Y QUÉ MEDIDAS SON FINANCIABLES.

LA PONENCIA DEL FORO DE COLABORACIÓN PÚBLICO-PRIVADA VERSÓ SOBRE LAS NOVEDADES DE LOS FONDOS NEXTGENERATIONEU. PARA VERLA, CLICA EN LA IMAGEN

Tal y como explicó en el Foro IT User: Nuevos impulsos para la evolución de la Administración digital, "los Fondos Next-GenerationEU son un mecanismo extraordinario que pone en marcha la Unión Europea con el objetivo de relanzar la economía tras el impacto de la Pandemia. Adicionalmente, se encuentra en marcha el Mecanismo Financiero Plurianual de la Unión Europea, que supone otra inyección de dinero para España".

Ahora mismo, "el Gobierno de España está trabajando sobre la parte de subvenciones, que suponen 69.528 millones de euros, más 12.800 del Fondo React-EU, que son los que tienen una prioridad mayor para consumirse".

Adicionalmente a los 154.996 millones de euros que España tiene disponible como país para poder gastar, "tiene dentro del Mecanismo Financiero Plurianual 43.813 millo-

nes, proveniente de lo que habitualmente denominamos como ayudas europeas. En resumen, España puede contar durante los próximos seis años con una cantidad ingente de dinero para poder desarrollar proyectos de inversión".

Todos estos fondos "no están para pagar proyectos de mantenimiento o servicios recurrentes, sino para lanzar proyectos tractores que tengan un impacto duradero en el tiempo y objetivo de permanencia en el tiempo. Las acciones tienen que cumplir una serie de requisitos, como pueden ser los relativos a la transición ecológica o la transición digital".

CUATRO EJES PRIORITARIOS PARA LAS INVERSIONES

Las inversiones tienen que apoyarse en "cuatro ejes transversales y en 10 políticas palanca, que ya eran conocidos desde hace tiempo, pero ahora aparecen más detalles de los 30 componentes, proyectos o iniciativas concretas que incluyen inversiones y reformas".

Asimismo, se han establecido los fondos asignados a cada una de las políticas palanca, y el Gobierno "ha mejorados los porcentajes en lo referido a la contribución ecológica y contribución digital, con un 39,12% y un 29%, respectivamente, que han de tener las diferentes iniciativas que surjan bajo esas políticas palanca".

EL OBJETIVO DE LOS PROYECTOS ES AVANZAR HACIA UNA ESPAÑA MÁS VERDE, MÁS DIGITAL, MÁS COHESIONADA DESDE EL PUNTO DE VISTA SOCIAL Y TERRITORIAL, Y MÁS IGUALITARIA

Además, "se han identificado seis Proyectos Estratégicos (PERTES), y el más avanzado de ellos es el de la Industria de automoción verde y conectada, que recientemente fue anunciado por el Gobierno y podría ser aprobado por el Consejo de Ministros a lo largo del mes de julio".

El objetivo de los mencionados 30 componentes es "avanzar hacia una España más verde, más digital, más cohesionada desde el punto de vista social y territorial, y más igualitaria. Y estos proyectos se concretan en 110 inversiones y 102 reformas".

Todos los componentes "tienen una contribución digital y una contribución ecológica", si bien el porcentaje de cada una de estas áreas en cada uno de los proyectos "es diferente".

PROYECTOS DE INVERSIÓN

Hablando de transformación de la Administración, existen tres principales líneas de inversión ya conocidas, esto es, modernización de la Administración General del Estado, proyectos tractores de digitalización de la Administración General del Estados y Transformación Digital y Modernización de la Política Territorial y Función Pública y de las Administraciones de las Comunidades Autónomas y las Entidades Locales, y dos nuevas, como son el Plan de Transición Energética en la Administración General del Estado y la Transformación de la Administración para la Ejecución de los Proyectos Estratégicos. ■

SOLEDAD CAMACHO, REGIONAL SALES DIRECTOR DE SALESFORCE

“NUESTRA ESTRATEGIA PARA LA ADMINISTRACIÓN DIGITAL, ES FACILITAR LA EXPERIENCIA DE LAS PERSONAS”

SALESFORCE ES UNA COMPAÑÍA ESPECIALIZADA EN LA RELACIÓN CON LOS CLIENTES Y, EN EL CASO QUE NOS OCUPA, LOS CLIENTES SON LOS CIUDADANOS. POR ESTE MOTIVO, SOLEDAD CAMACHO, REGIONAL SALES DIRECTOR DE SALESFORCE, NOS EXPLICA SU VISIÓN SOBRE CÓMO PUEDE LA ADMINISTRACIÓN PÚBLICA MEJORAR SU RELACIÓN CON LOS CIUDADANOS.

En su presentación en el Foro IT User: Nuevos impulsos para la evolución de la Administración digital, Soledad Camacho recordaba que los tres pilares fundamentales de su compañía son “confianza, éxito de nuestros clientes e innovación. Somos una compañía que nacimos en el cloud, fuimos pioneros, y, a partir de ahí, establecimos toda la relación con nuestros clientes. Somos conscientes de que la relación de la Administración Pública con los ciudadanos se tiene que basar en una tecnología fiable, robusta, escalable y segura, y eso es lo que somos para la Administración”.

La plataforma de Salesforce “se centra en las personas, esto es, tanto el ciudadano trabajador de una empresa o el empleado público, y nuestra visión, nuestra estrategia para la Administración digital, es facilitar la experiencia de estas personas. Entender por qué los ciudadanos y los empleados públicos prefieren trabajar con la Administración igual que lo hacen con cualquier empresa privada.

SOLEDAD CAMACHO, REGIONAL SALES DIRECTOR DE SALESFORCE, EN UN MOMENTO DE SU INTERVENCIÓN. CLICA EN LA IMAGEN PARA VER EL VÍDEO.

Que haya mayor involucración de la ciudadanía, lo que reporta un beneficio a la Administración, porque conoce mejor a las personas, y mayor satisfacción del empleado público, porque dispone de todas las herramientas y de todo el conocimiento que necesita en cada momento".

EFICIENCIA DEL EMPLEADO PÚBLICO

En el caso de Salesforce, "hablamos de eficiencia del empleado público, es decir, utilizar el mínimo tiempo y los menos recursos posibles. Sin olvidar la plataforma de datos abiertos para la analítica predictiva que podemos tener".

Salesforce está "alineada con la experiencia del ciudadano, tenemos que cambiar el paradigma de la Administración, basado en procesos, diferentes y complejos, con muchos silos departamentales y unos canales de acceso limitado. Desde Salesforce, pensamos que la Administración tiene que estar centrada en el ciudadano, pasar de una Administración centrada en el proceso a una Administración centrada en las personas, de forma que sea muy ágil y rápido poder ofrecer nuevos servicios a ese ciudadano; que cualquier canal que el ciudadano quiera utilizar esté puesto a su disposición, para ofrecer una experiencia integrada y poder tener una visión de 360º del ciudadano, que nos ayude a tomar mejores decisiones".

CONTENIDOS↓

"LA ADMINISTRACIÓN DEBE ORIENTARSE A LOS CIUDADANOS, NO A LOS PROCESOS ADMINISTRATIVOS" (SALESFORCE)

Tal y como recuerda Soledad Camacho, "contamos con diferentes casos de uso, desde Sanidad, con casos de gestión de pacientes públicos; proyectos de escucha activa, saber que está ocurriendo en las redes sociales y tomar decisiones sobre ello; casos de gestión de vacunas que se ha puesto en marcha en dos o tres semanas; teleasistencia; gestión de emergencias; ciudades conectadas; turismo inteligente; gestión de trámites... pero todos estos casos de uso no pueden hacer olvidar toda la plataforma con la que ya cuenta la Administración Pública, y Salesforce puede ayudar a ofrecer estos servicios de forma diferente".

UNA VISIÓN 360º DEL CIUDADANO

La apuesta de Salesforce pasa por poner al ciudadano en el centro "y ofrecer una visión completa, de 360º, para mejorar la relación con el ciudadano, digitalizar e integrar esta relación en la Administración, modernizar la experiencia del empleado público e innovar toda la TI del Gobierno". Pensando en la Administración, los beneficios de la plataforma de Salesforce son "implementación rápida, integración con las aplicaciones existentes, entornos híbridos, información centralizada, omnicanalidad, reducción de tareas manuales, seguridad, y mejora de la experiencia al ciudadano". ■

CONTENIDO RELACIONADO

Ponencia Salesforce

Solución de Gestión de Subvenciones

Foro IT User: Nuevos impulsos para la evolución de la Administración digital

TRANSFORMACIÓN DIGITAL Y TECNOLOGÍAS DISRUPTIVAS

SON MUCHOS LOS EJEMPLOS DE PROYECTOS DE TRANSFORMACIÓN QUE PODEMOS VER A DÍA DE HOY EN EL SECTOR PÚBLICO. Y PARA HABLAR DE ELLOS, NADIE MEJOR QUE LAS PERSONAS QUE LIDERAN ALGUNOS DE ELLOS DESDE LA PROPIA ADMINISTRACIÓN, CONOCEDORES, ADEMÁS DE DÓNDE MÁS HAY QUE SEGUIR PONIENDO EL FOCO DE ESTAS INICIATIVAS.

Participaron en esta mesa redonda: Ministerio de Sanidad, Ayuntamiento de Madrid, Gobierno de Cantabria y Ministerio de Asuntos Económicos y Transformación Digital. Clica en la imagen para ver el vídeo.

Para esta primera mesa de debate del Foro IT User: Nuevos impulsos para la evolución de la Administración digital, moderada por Jesús Galindo, Area Vice President Sales Public Sector de Salesforce, contamos con la presencia de Juan Fernando Muñoz Montalvo, Director General de Salud Digital y Sistemas de Información para el Sistema Nacional de Salud del Ministerio de Sanidad; Fernando de Pablo Martín, Director General de la Oficina Digital del Ayuntamiento de Madrid; Rocío Montalbán Carrasco, Subdirectora General de Transformación Digital y Relaciones con los usuarios de la Consejería de Sanidad del Gobierno de Cantabria; y Laura Flores Iglesias, Subdirectora General de IA y tecnologías Habilitadoras Digitales de la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital.

España se sitúa en segundo lugar en la clasificación de la UE en cuanto al desarrollo de los

"SE HA REALIZADO UN TRABAJO MUY IMPORTANTE, PERO NOS QUEDAN BASTANTES ESFUERZOS POR ACOMETER"

JUAN FERNANDO MUÑOZ MONTALVO

servicios digitales. En palabras de Juan Fernando Muñoz, "estamos bien situados porque ha habido un trabajo muy importante, pero nos quedan bastantes esfuerzos. No tanto en proveer estos servicios digitales, sino en promover su uso. Y aquí hay varios factores, como puede ser la brecha digital o la necesidad de flexibilizar y ajustar los procedimientos a las tecnologías. Evidentemente, no es algo sencillo, por la propia naturaleza de la Administración".

En opinión de Fernando de Pablo, "tenemos que estar orgullosos de donde estamos, porque es la muestra de un trabajo bien hecho. Pero lo importante no es la posición en los rankings, sino el impacto en la vida de las personas. Y, efectivamente, tenemos que mejorar. Esto no va de tecnología, sino de servicios, de la tecnología aplicada a los servicios, y, en este caso, hay que hablar de simplificación de los procesos, integración entre las diferentes Administraciones, simplificación en los modos de acceso, la personalización, la proactividad, la estandarización... tenemos un gran campo de mejora".

Desde la perspectiva de Rocía Montalbán, "algo a mejorar es la poca homogeneidad entre los servicios públicos de las distintas administraciones, incluso dentro de una Administración entre distintas entidades. Además, la formación de los empleados públicos es otra batalla que tenemos por delante. En el caso de los servicios tenemos la parte tecnológica, la de accesibilidad, la de los servicios... pero la de formación es la que tenemos que empujar más".

Finaliza esta primera ronda de opiniones Laura Flores, que apunta que "se ha notado durante esta pandemia que los servicios de administración electrónica han seguido funcionando, incluso habiendo crecido mucho en cantidad de usuarios. Pero hay que hacer más es esfuerzos para seguir modernizándonos y acercándonos al ciudadano, con temas como la usabilidad, la proactividad, la personalización, la sencillez de acceso... Convendría contar con equipos multidisciplinares, que sepan de tecnología pero también de la parte funcional, para que el servicio al ciudadano sea un éxito".

TECNOLOGÍAS DISRUPTIVAS

Destaca Laura Flores que la IA "va a ser la tendencia disruptiva que está ya llegando. Machine Learning, Deep Learning, Procesamiento de Lenguaje Natural, son algunos de las tecnologías que ya están en los proyectos de los Ministerios. Toda esa capa de datos que debe nutrir estos algoritmos será la que nos guíe en los próximos años". Y, en este caso, el Sector Público debe ser el elemento tractor "para el sector privado", continúa, "a que puedan introducirse

"APOSTAMOS POR TECNOLOGÍAS QUE APORTEN VALOR PARA MEJORAR LOS SERVICIOS A PARTIR DE DATOS DE CALIDAD POTENCIADOS CON LAS ADECUADAS HERRAMIENTAS DE GESTIÓN"

FERNANDO DE PABLO MARTÍN

en los entornos productivos y relanzar la economía del país. Se prevé que se inviertan en unos 600 millones de euros que podrían tener un impacto de hasta 3.300 millones de euros".

Añade Rocío Montalbán que estos meses "hemos estado todos muy cerca de los datos. Ha sido el año del manejo de los datos y, si bien esto ha puesto en valor a la tecnología para la gestión, primero, de la crisis Covid y, segundo, de los procesos de vacunación, no se trata solo de disponer de buenos datos, sino de ir más allá y apoyarnos en herramientas de IA para poder dar una respuesta adecuada".

"NO SE TRATA SOLO DE DISPONER DE BUENOS DATOS, SINO DE IR MÁS ALLÁ Y APOYARNOS EN HERRAMIENTAS DE IA PARA PODER DAR UNA RESPUESTA ADECUADA"

ROCÍO MONTALBÁN CARRASCO

Pero "también el vídeo nos está ayudando mucho en nuestros procesos", explica, "y lo mismo con las apps. Todo esto hay que madurarlo y ponerlo en funcionamiento de forma estable, no puntual". Coincide con ella Juan Fernando Muñoz, pero matiza que no cree que el Sector Público se ejemplo para el Sector Privado, "porque los requisitos, los contextos y la medición de resultados deben ser diferentes. Pero sí deben ser tractores, porque disponemos de muchos datos y mucho conocimiento, que es la base de lo que podemos hacer, y debe poder compartirse, con las adecuadas cautelas y seguridad, para generar beneficio para la sociedad".

Alrededor de estos tres elementos, "los datos como la base de todo, la IA como herramienta para explotarlos, y la ciberseguridad para proteger y potenciar la información, tenemos la oportunidad única de dar un paso adelante".

A nivel de los ayuntamientos, comenta Fernando de Pablo, se incorporarán "todas las tecnologías que aporten valor para mejorar los servicios a partir de datos de calidad potenciados con las adecuadas herramientas de gestión. Destaca todo lo que tiene que ver con la automatización, que es un camino fundamental para ser más eficientes; la seguridad, para proteger los datos; 5G, para dar servicios en tiempo real; y, todo ello, apoyado en la capacitación. La Administración debe ser la impulsora de la transformación de las pequeñas

"SE PREVÉ QUE SE INVIERTAN EN UNOS 600 MILLONES DE EUROS EN IA EN LA ADMINISTRACIÓN QUE PODRÍAN TENER UN IMPACTO DE HASTA 3.300 MILLONES DE EUROS"

LAURA FLORES IGLESIAS

y medianas empresas. Lo ha sido en ocasiones, y debe seguir siéndolo, porque la sensación de urgencia de la transformación digital no es solo para las grandes empresas del sector privado".

RETOS EN LA ADQUISICIÓN

Rocío Montalbán comenta que "hay retos importantes, como el normativo, sobre todo en un ámbito como el mío, el de la Salud. Pero también hay retos organizativos, como la necesidad de equipos multidisciplinares para que los proyectos lleguen a buen puerto".

Apunta Laura Flores que uno de los mayores retos, sobre todo cuando hablamos de tecno-

logías disruptivas, "es la escasez de especialistas, de talento, que necesitamos para todos estos proyectos. Otro de los retos es el de la ética y la confianza en estas tecnologías, que se pueden aplicar para el bien de la ciudadanía con las pautas adecuadas. A nivel de compra y ejecución, tenemos el reto de empezar a utilizar esos otros sistemas de compra que existen, como la compra pública innovadora, que permiten ir explorando soluciones antes de su implantación".

Coincide con ella Fernando de Pablo que a los retos organizativos, de talento, normativos, de confianza, añade "el uso ético de los datos, porque en todo lo que tiene que ver con el tratamiento de los datos es fundamental el componente ético de la Administración. Cada vez es más difícil ver la barrera de la IA, y su integración en el día a día da confianza a las personas, pero la Administración debe vigilar que el uso de estas tecnologías sea la adecuada".

Recalca Juan Fernando Muñoz que un reto es el "cambio de perspectiva de la Administración en lo referido al uso de los datos y de las herramientas de gestión alrededor de ellos. La pandemia ha demostrado que la colaboración y compartición de los datos han permitido el desarrollo de herramientas en días que en otras circunstancias hubieran precisado años. En cuanto a los procesos de contratación, se requieren nuevas fórmulas ligadas a la nube por la flexibilidad que se necesita, pero la complejidad del Sector Público hace complejo el encaje. Asimismo, durante la pandemia hemos creado grupos de trabajo específico y hemos visto que es un camino a seguir en algunos casos. Por último, la escasez de personal de perfiles cualificados, que es uno de nuestros mayores retos".

ALGUNOS CASOS DE USO

En este sentido, Juan Fernando Muñoz señala que hay muchas aplicaciones muy prometedoras, pero en esta pandemia "hemos podido desarrollar un modelo basado en redes neunorales recurrentes de predicción de ocupación de camas por provincia, para lo que necesitamos datos de diferentes sistemas de distintas entidades, públicas o privadas, de diferentes fuentes, de múltiples pruebas... y hoy tenemos un modelo que tiene un índice de error por debajo del 3%".

En palabras de Fernando de Pablo, "hay múltiples ejemplos en movilidad, seguridad y emergencias, en el área tributaria utilizando la IA en análisis predictivos, chatbots informativos, técnicas de lenguaje natural, un sandbox para realizar pruebas o un cluster de Inteligencia Artificial que se une a otros que teníamos de Big Data y Seguridad".

Para Rocío Montalbán, "nuestro tamaño nos permite realizar pilotos antes de implementar los proyectos, y vamos probando siempre que vemos que puede ser de utilidad para la ciudadanía. Destacan los proyectos de colaboración público-privada sobre datos anonimizados para poder hacer ensayos clínicos sobre ellos, como el proyecto Eden".

Finaliza Laura Flores apuntando que son varios los proyectos que estamos preparando la lanzar, como uno "centrado en la IA y el español para tratar de construir un ecosistema de negocio que nos permita competir con el inglés en los territorios hispanohablantes. Otro proyecto interesante es la creación de un laboratorio de innovación para crear nuevos servicios y aplicaciones de la IA en los diferentes ámbitos en colaboración con algunos servicios críticos, como puede ser el SEPE. Asimismo, un proyecto de I+D+i de IA, que pretende abordar grande desafíos sociales que puedan solucionarse con la Inteligencia Artificial con la implicación de diferentes actores".

Al hilo de estas afirmaciones, concluye Jesús Galindo señalando que la "Inteligencia Artificial y el dato, de calidad y seguro, van a ser lo que va a cambiar la Administración en los próximos años". ■

CONTENIDO RELACIONADO

Foro IT User: Nuevos impulsos para la evolución de la Administración digital

Forcepoint

Modelo de seguridad SASE y Zero Trust

Las soluciones de ciberseguridad de SASE permiten a sus usuarios que accedan de forma segura y sin importar donde estén, a la web, las aplicaciones en la nube y las aplicaciones internas.

forcepoint.com

FERNANDO GUTIÉRREZ CABELLO, RESPONSABLE DE SECTOR PÚBLICO DE MICROSTRATEGY

"EL DATO ES UN ACTIVO FUNDAMENTAL DE TODAS LAS EMPRESAS"

CUANDO HABLAMOS DE LA MODERNIZACIÓN DE LA ADMINISTRACIÓN PÚBLICA HAY QUE DETENERSE EN QUÉ TECNOLOGÍAS LA HACEN POSIBLE. FERNANDO GUTIÉRREZ CABELLO, RESPONSABLE DE SECTOR PÚBLICO DE MICROSTRATEGY, REPASA CÓMO DEBEN MODERNIZARSE LAS INSTITUCIONES APOYÁNDOSE EN UN ELEMENTO DE VALOR FUNDAMENTAL: LOS DATOS.

niciaba su intervención en el Foro IT User: Nuevos impulsos para la evolución de la Administración digital Fernando Gutiérrez, recordando que el dato "es un activo fundamental de todas las empresas, ya sean públicas o privadas", pero también los elementos diferenciadores de la Administración Pública. En primer lugar, "el tamaño, porque cuanto más grande es una empresa más complejo es gestionar los datos. El segundo, la dispersión territorial, que obliga a la información a moverse en varias direcciones y tener que consolidarse en un único lugar. En tercer lugar, mientras una empresa privada puede segmentar a los clientes para venderles un producto, la Administración Pública ofrece un servicio a toda la población, lo que hace que sea un público muy heterogéneo".

"LA MODERNIZACIÓN PASA POR UN ACCESO MÁS SENCILLO DEL CIUDADANO A LA INFORMACIÓN" (MICROSTRATEGY)

Pero también hay una parte positiva, y es que “el punto de partida es bueno, ya que España está posicionada en el número dos del ranking de digitalización (DESI), fruto de un excelente trabajo que se ha hecho en la digitalización de los servicios”, si bien hay “diferentes áreas de impulso tecnológico si queremos que las decisiones de la Administracion Pública estén dirigidas por el dato”.

ÁREAS DE MEJORA

MicroStrategy identifica tres áreas de mejora. La primera, “la gestión y el gobierno del dato; la segunda, cómo explotamos ese dato; y, la tercera, cómo damos acceso a ese dato, tanto para la ciudadanía como para los empleados públicos”, porque no podemos olvidar que en el Plan de Digitalización de España para 2025, hay “dos objetivos fundamentales, facilitar el acceso a la información a la ciudadanía, personalizando esa información, pero también al empleado público, con el fin de incrementar su productividad”.

“NUESTRA RECOMENDACIÓN ES CONTAR CON UNA HERRAMIENTA FLEXIBLE, UNA PIEZA QUE ENCAJE EN UN ECOSISTEMA COMPLEJO Y QUE ADMITA LO QUE PUEDA LLEGAR A POSTERIORI”

“HAY DIFERENTES ÁREAS DE MEJORA SI QUEREMOS QUE LAS DECISIONES DE LA ADMINISTRACION PÚBLICA ESTÉN DIRIGIDAS POR EL DATO”

La mejora en la gestión y el gobierno del dato, “es una problemática que tienen todas las instituciones y empresas grandes, debido, principalmente, a los sistemas legacy que hacen que la información esté repetida, dispersa y sea inconexa, lo que dificulta el acceso del ciudadano a la información, y al empleado, cuando tiene que tomar una decisión basada en el dato, tener que buscar información en diferentes lugares. Por eso hay que abordar un proyecto de gobierno del dato”.

Partiendo de este proyecto de gobierno del dato, llegamos a la segunda área de mejora, la explotación del dato. Contamos con fuentes variadas y dispersas de información que se explotan de manera diferente. Así que una vez que está consolidada la información, “nuestra recomendación es contar con una herramienta flexible, una pieza que encaje en un ecosistema complejo y que admita lo que pueda llegar a posteriori. Por eso, la solución debería contar con características de gobierno del dato, no solo al guardarlo, sino también al explotarlo, escalabilidad de datos, escalabilidad de usuarios, múltiples casos de uso y la flexibilidad, que puede venir proporcionado mediante API”.

El tercer punto es el del acceso al dato, “romper la brecha digital, para lo que el acceso debe ser sencillo, intuitivo y personalizado; reducir la brecha tecnológica en el caso de los empleados; y, por último, acceso multicanal a la información”.

Pensando en esta tercer área, la propuesta de MicroStrategy pasa por HyperIntelligence, una herramienta que enriquece las aplicaciones con información contextual que acelera el flujo de trabajo y relaciona las aplicaciones. ■

CONTENIDO RELACIONADO

Ponencia de MicroStrategy

HyperIntelligence

Novedades MicroStrategy 2021

Foro IT User: Nuevos impulsos para la evolución de la Administración digital

PEDRO MARTÍNEZ, DIRECTOR DESARROLLO DE NEGOCIO REGIÓN SUR DE EUROPA DE ARUBA

"NECESITAMOS CAMBIAR LOS MODELOS DE DISEÑO DE LAS ARQUITECTURAS DE RED"

UNA DE LAS TENDENCIAS MÁS CLARAS DE LA ACTUALIDAD ES EL INCREMENTO DE ACTIVIDAD EN EL EXTREMO DE LA RED. PERO ¿CÓMO PUEDE EL SECTOR PÚBLICO APROVECHAR TODO ESTE POTENCIAL DE DATOS QUE SE ESTÁ PRODUCIENDO EN EL EDGE? PEDRO MARTÍNEZ, DIRECTOR DE DESARROLLO DE NEGOCIO PARA LA REGIÓN SUR DE EUROPA DE ARUBA, NOS OFRECE SU VISIÓN.

Pedro Martínez aprovechó su participación en el Foro IT User: Nuevos impulsos para la evolución de la Administración digital para mostrar los que a juicio de su empresa son las principales oportunidades y retos de la Administración. Estos retos vienen motivados por un cambio significativo, "con un importante incremento de actividad en el extremo de la red", mientras que las oportunidades llegan, principalmente, por "los Fondos Europeos de Recuperación".

LOS RETOS QUE PLANTEA EL EDGE

En los últimos años ha cambiado mucho el paradigma, y hemos pasado "de un modelo con usuarios móviles en el extremo que accedían a nubes públicas o privadas que centralizaban el procesado de la información. Desde

"CADA DÍA LOS CIUDADANOS SON MÁS DIGITALES Y DEMANDAN SERVICIOS MÁS DIGITALES" (ARUBA)

el punto de vista de la red, necesitábamos velocidad y agilidad para poder llevar la información y procesarla. Pero esto ha cambiado en los últimos tiempos, por datos como los que muestra IDC, que indica que el año que viene habrá 55 billones millones de dispositivos en el extremo, de los que no más del 25% están asociados a personas. Por su parte, Gartner estima que el 75% de los datos se van a generar fuera del entorno tradicional, ya sea la nube o el centro de datos corporativo".

Este número creciente de dispositivos inteligentes están abriendo la puerta a nuevos servicios, "y necesitamos almacenar y procesar datos en el extremo, bien porque tenemos que tomar decisiones en tiempo real o porque el coste del ancho de banda necesario hace que sea inmanejable. Además, estos datos son cada vez más importantes para mejorar la experiencia que ofrecen los organismos públicos al ciudadano. Esto provoca que estos centros de proceso de datos que estaban organizados en el centro, se están acercando al extremo en un formato de centro de datos más pequeño. Por eso, necesitamos cambiar los modelos en base a los cuales están diseñadas estas arquitecturas de red".

La visión integrada del nuevo modelo incluye "un extremo inteligente, al otro lado entornos multinube híbrida con consumos ofrecidos como servicio y, en medio, actuando como pegamento, las nuevas arquitecturas SD-WAN que nos van a permitir conectar, de forma inteligente, los dispositivos del extremos con los servicios y aplicaciones desplegadas en la nube híbrida".

"DEBEMOS INCREMENTAR LA PROTECCIÓN DE LOS DISPOSITIVOS Y LAS COSAS, PORQUE, AL AUMENTAR LA DISPERSIÓN DEL EXTREMO, AUMENTA LA SUPERFICIE DE POSIBLES ATAQUES"

Con todo, la Administración se enfrenta a una serie de retos tales como "la protección de los dispositivos y las cosas, porque, al aumentar la dispersión del extremo, aumenta la superficie de posibles ataques; simplificar la red, mejorando la visibilidad y la automatización de las operaciones de red; optimizar los recursos económicos; y, por otro lado, la demanda de servicios más digitalizados por parte de ciudadanos cada vez más digitales".

INICIATIVAS PARA EL SECTOR PÚBLICO

Para Aruba, son tres principalmente, Ciudadano Conectado, tanto en lo relativo a las Ciudades Inteligentes como a los Edificios Públicos Inteligentes, donde es fundamental la convergencia de las redes IP e IoT, "donde destaca el rol de los puntos de acceso wi-fi como plataforma convergente de conectividad inalámbrica"; Administración Pública Segura, para lo que se propone "Zero Trust Networking y tecnologías de Microsegmentación", para que la red sea el primer punto de defensa, así como "Arquitecturas SASE para hacer frente a la seguridad en entornos distribuidos"; y Red como Servicio, para lo que es fundamental una arquitectura de red unificada e híbrida, "como la que posibilita Aruba Central". ■

CONTENIDO RELACIONADO

Ponencia de Aruba

Caso Éxito Bilbao City

Estudio sobre la gestión de la red desde el perímetro

Foro IT User: Nuevos impulsos para la evolución de la Administración digital

FERNANDO FELIU, DIRECTOR DE GLOBAL CUSTOMER SOLUTIONS DE V-VALLEY

“SE HA PROVOCADO QUE LA ÚLTIMA TECNOLOGÍA ESTÉ MÁS RÁPIDAMENTE AL ALCANCE DE TODOS”

LA ADMINISTRACIÓN PÚBLICA ESTÁ PROTAGONIZANDO UNA EVOLUCIÓN HACIA UN ENTORNO MÁS DIGITAL, Y SOBRE ELLO NOS HABLA FERNANDO FELIU, DIRECTOR DE GLOBAL CUSTOMER SOLUTIONS DE V-VALLEY, QUIEN EXPLICA QUE EL CAMBIO HA SIDO RADICAL Y SE HAN IDO CREANDO NUEVAS NECESIDADES.

En palabras de Fernando Feliu en el Foro IT User: Nuevos impulsos para la evolución de la Administración digital, “la pandemia ha acelerado la necesidad de transformación del entorno dentro de las Administraciones Públicas. Si bien, cuando hablamos de Administración Pública, hablamos de un compendio de necesidades muy diferentes. Hay que distinguir también las necesidades internas de la Administración y las de los servicios que hay que proporcionar a los ciudadanos. Y, en este caso, hablamos de muchísimos requerimientos diferentes, porque hay personas muy adelantadas digitalmente, pero hay otros que no están tan acostumbrados, lo que genera la necesidad de educar digitalmente al ciudadano”.

Tampoco podemos olvidar “los diferentes entornos en los que nos movemos”, porque

“LA ADMINISTRACIÓN HA EVOLUCIONADO MUCHO PARA OFRECER EL MEJOR SERVICIO AL CIUDADANO” (V-VALLEY)

no es lo mismo una ciudad que un entorno rural, ni es lo mismo un ayuntamiento o una diputación, o los diferentes segmentos (Defensa, Seguridad, Hacienda…), "cada uno tiene unas necesidades diferentes, pero lo que sí es común es que ha habido unos cambios radicales en cuanto a la digitalización, como, por ejemplo, el uso de la IA en Sanidad. Esto ha creado un entorno diferente a lo que teníamos antes, pero estos entornos son complejos de definir, implantar y formar".

Y un ejemplo claro es la digitalización de las aulas, que se ha vito superada "por las aulas remotas, donde las necesidades eran diferentes, los profesores han necesitados formarse y se ha creado un entorno diferente a la hora de comunicarse con los alumnos".

INTEGRACIÓN DE HERRAMIENTAS DISRUPTIVAS

Herramientas que antes considerábamos disruptivas, "se han integrado en nuestro día a día. La colaboración entre diferentes tecnologías y el impulso de procedimientos diferentes de actuación han sido los que han creado este cambio tan importante en la forma de actuar, interna y externamente, dentro de la Administración Pública". Esto ha provocado un cambio en los centros decisores de la tecnología de la Administración Pública, "que han tenido que estudiar tecnologías que pueden aportar un cambio radical en su forma de trabajo. Este cambio hay que verlo en diferentes ámbitos: recursos humanos, gestión del dato, securización del dato, captación del datos, o en cómo usar este dato para mejorar la atención al ciudadano".

"LA COLABORACIÓN ENTRE DIFERENTES TECNOLOGÍAS Y EL IMPULSO DE PROCEDIMIENTOS DIFERENTES DE ACTUACIÓN HAN SIDO LOS QUE HAN CREADO ESTE CAMBIO TAN IMPORTANTE EN LA FORMA DE ACTUAR, INTERNA Y EXTERNAMENTE, DENTRO DE LA ADMINISTRACIÓN PÚBLICA"

Asimismo, se han reducido los plazos en la toma de decisiones, y, con ello, "y con un foco más digital hacia el futuro, se ha provocado que la última tecnología esté más rápidamente al alcance de todos".

Y este cambio se extiende también a V-Valley, con la creación del departamento de Global Customers Solutions, "que unifica todas las soluciones, que hasta ahora estaban muy verticalizadas, en un grupo de trabajo para poder aportar los conocimientos necesarios en soluciones mucho más globales. Esto conlleva un compendio de formaciones y certificaciones, para lo que hemos creado V-Valley Academy, para poder formar en estas tecnologías a todos aquellos que quieran hacerlas accesibles".

TRANSFORMACIÓN PARA TODOS

En este momento, la interacción con la Administración es muy diferente a la que teníamos años atrás, "pero no todos los ciudadanos tienen el nivel tecnológico necesario para ello", lo que ha provocado que la tecnología ya no esté presente solo en los grandes centros de población, "porque la transformación digital tiene que ser para todos, accesible para todos, y es lo que veremos en los próximos años, porque las inversiones se están haciendo". ■

CONTENIDO RELACIONADO

Ponencia V-Valley

V-Valley Academy

Foro IT User: Nuevos impulsos para la evolución de la Administración digital

MESA REDONDA

GOBIERNO DEL DATO Y CIBERSEGURIDAD

SI HAY DOS PILARES FUNDAMENTALES EN LOS PROCESOS DE TRANSFORMACIÓN DE LA ADMINISTRACIÓN PÚBLICA SON LOS DATOS Y LA CIBERSEGURIDAD. POR ESO, QUISIMOS CONOCER, DE PRIMERA MANO, QUÉ IMPORTANCIA TIENE EL DATO PARA LA ADMINISTRACIÓN, CÓMO SE ESTÁN MEJORANDO LOS PROCESOS Y SERVICIOS ALREDEDOR SUYO Y CÓMO SE ESTÁ PROTEGIENDO.

Participaron en esta mesa redonda: Ministerio de Justicia, Instituto de Crédito Oficial, Ministerio de Asuntos Económicos y Transformación Digital y Ministerio de Hacienda. Clica en la imagen para ver el vídeo.

En esta mesa redonda del Foro IT User: Nuevos impulsos para la evolución de la Administración digital, moderada por Jesús Galindo, Area Vice President Sales Public Sector de Salesforce, contamos con la participación de Aitor Cubo Contreras, Director General de Transformación Digital del Ministerio de Justicia; Noemí García, CIO del Instituto de Crédito Oficial, adscrito al Ministerio de Asuntos Económicos y Transformación Digital; Alicia Herrero Fernández, Subdirectora General de Servicios Digitales para la Gestión de la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital; y Carmen García Roger, Subdirectora General de Estadística de Servicios de la Inspección General del Ministerio de Hacienda.

En primer lugar, quisimos saber cuál es el rol del dato en una Administración orientada al ciudadano. Para Aitor Cubo, "la Justicia orientada al dato es algo que está contemplado en el Plan Estratégico de Justicia 2020-2030, y está alineado con reformas estructurales, como las incluidas en la Ley de Eficiencia Judicial. Esta Justicia orientada al dato tiene dos vertientes. Por un lado, la gestión orientada al dato. Hasta ahora, la Justicia era electrónica, pero estaba orientada al documento, pero se

está haciendo un trabajo importante, primero, complementado los documentos con datos y metadatos, para, después, plantear sistemas de gestión procesal basados en conjuntos de datos. Por otro lado, la toma de decisiones de política pública basadas en datos, con explotación de información para poder tomar decisiones. Por último, estamos favoreciendo la interoperabilidad al tener un conjunto de datos común".

Por su parte, Noemí García indica que "es importante haber puesto unas bases dentro de la Administración para que se puedan compartir los datos de todas las entidades, pero debemos seguir avanzando para que los ciudadanos puedan tener cercanía con la Administración y sea sencillo realizar los trámites. Es importante tener claro el objetivo, que no es otro que mejorar la calidad de los datos y la interoperabilidad entre administraciones. Además, tenemos que superar la brecha digital que hay en la sociedad, para que los ciudadanos estén más cerca de la Administración".

"ES FUNDAMENTAL LA CO-GOBERNANZA DEL DATO, PORQUE NO PODEMOS QUEDARNOS CADA UNO CON NUESTROS DATOS Y TOMAR DECISIONES EN BASE A ELLOS"

AITOR CUBO CONTRERAS

EL DATO COMO ORIGEN DE LA MEJORA DE LA EXPERIENCIA DEL CIUDADANO

Para Carmen García, "muchas veces nos centramos en cómo gestionamos el dato, pero lo que buscamos es mejorar la experiencia del ciudadano. Los grandes proyectos centrados en el dato tienen ese objetivo. Los elementos clave alrededor del dato son la colaboración, la compartición y la transparencia. Es cierto que tenemos normas y reglamentos, pero necesitamos que sea refrendo de la actuación tecnológica de procesos, de personas, de estrategia, de datos y de tecnología, y si atendemos a estos cinco pilares, tendremos un proyecto de éxito".

En palabras de Noemí García, "tenemos unos principios de calidad y seguridad de los datos, y unos objetivos, que los datos estén accesibles, sean de calidad y compartidos por todas las administraciones. Y estos proyectos del gobierno del dato se tienen que apoyar en una serie de pilares. Por un lado, la vertiente organizativa, que tiene que ayudar a que todo esto vaya adelante. Por otro, una labor de análisis de los datos para catalogar la información. Todo esto, sustentado en una buena herramienta de gestión y seguir una metodología adecuada para llegar a unos datos seguros y de calidad. Y no podemos olvidar el cambio cultural necesario, porque el dato no es solo de TI, es de todos, y debemos poner las herramientas para avanzar en esta línea".

"TENEMOS UNOS PRINCIPIOS DE CALIDAD Y SEGURIDAD DE LOS DATOS, Y UNOS OBJETIVOS: QUE LOS DATOS ESTÉN ACCESIBLES, SEAN DE CALIDAD Y COMPARTIDOS POR TODAS LAS ADMINISTRACIONES"

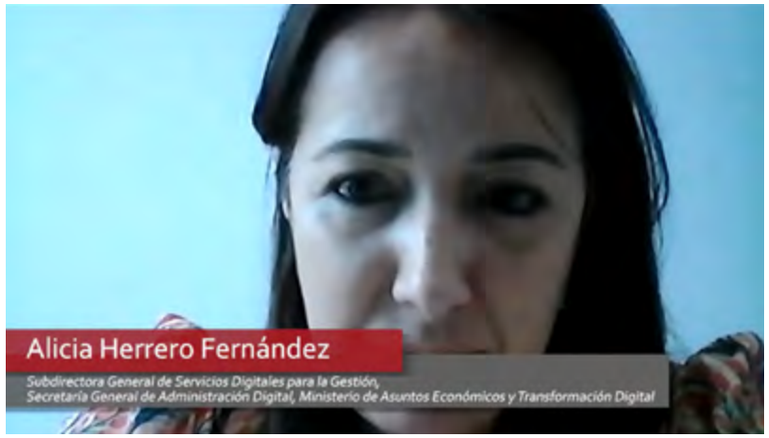
NOEMÍ GARCÍA

EL DATO, PRINCIPAL ACTIVO DE LAS ORGANIZACIONES

Según Alicia Herrero, “es importante definir el fin que se busca, porque los datos son el principal activo de las organizaciones, tanto públicas como privadas. Tenemos que poner el dato en valor entendiendo el ciclo de vida del mismo, cuestiones que no son meramente TI, sino de la misión de una organización. Es fundamental la interoperabilidad, por lo que, además de proyectos nacionales, no podemos olvidar Gaia-X o la European Data Act, pero siempre con una observancia total de la normativa y de la seguridad. Otro principio básico es crear confianza, contar con datos inclusivos, trabajar de forma transparente con ellos, así como que sean interpretables, sencillos de usar, dinámicos, que generen valor…”.

Se muestra de acuerdo con ellas Carmen García, “porque esto es algo que transciende las TIC. El volumen de datos del que disponemos es tal que corremos el riesgo de quedarnos atrapados y que nos supere. Deberíamos ir hacia organizaciones guiadas por el conocimiento, más allá que guiadas por el dato. Necesitamos embeber el valor del dato en las organizaciones. Debemos convertir esto en algo sistémico, y es hacia donde vamos, aunque el esfuerzo necesario es muy grande”.

“En Justicia”, apunta Aitor Cubo, “es fundamental la co-gobernanza del dato, porque no podemos quedarnos cada uno con nuestros datos y tomar decisiones en base a ellos. Hay que cruzar nuestros datos con los de otros, es fundamental. Eso sí, con una protección absoluta de los datos personales, si bien esto no tiene que servir de escusa para no compartir información. Tenemos que apostar por los datos abiertos, compartirlos. Debemos entender el dato como bien público, no solo es que no sea de TI, sino que tampoco debe ser de una entidad. Es un bien público que debe estar a disposición de todos”.



“NO NOS PODEMOS PERMITIR, NI LAS ADMINISTRACIONES PÚBLICAS NI EL SECTOR PRIVADO, TENER UN ATAQUE Y PERDER DATOS O TENER PÉRDIDAS DE SERVICIO”

ALICIA HERRERO FERNÁNDEZ

“LA INVERSIÓN EN SEGURIDAD NO ES QUE SEA PRIORITARIA, ES QUE ES UN BÁSICO A LA HORA DE PRESUPUESTAR”

CARMEN GARCÍA ROGER

EJEMPLOS DE BUEN USO DEL DATO

Carmen Garcia, “hay un ejemplo que se está gestando: el nuevo modelo de gestión informática en el Tribunal Económico Administrativo Central y la Dirección General de Tributos, estableciendo un sistema integrado y global de gestión tributaria. Hasta la fecha, se trata de organismos que funcionan de manera independiente, con silos de información y muy desintegrados, pero el nuevo modelo busca reducir tiempos y costes, para la Administración y los ciudadanos, basado en los datos y las metodologías y en la co-gobernanza entre las diferentes entidades. Es un modelo que podría estar operativo en 2024, pero creemos que cambiará la actuación administrativa”.

Apunta Noemí García que alrededor de las medidas surgidas frente a la pandemia, "estamos interactuando con muchos actores. Tenemos más de un millón de operaciones, un importe de más de 125.000 millones, una red de datos con muchas entidades de diferentes naturalezas y tamaños... pero la realidad es que la plataforma para la intermediación ha funcionado, y tenemos una red de colaboración público-privada con más de 100 entidades, así como con otros organismos públicos y ciudadanos".

Comenta Aitor Cubo que "destaca que en la Secretaría de Estado de Digitalización e Inteligencia Artificial están los indicadores de la Administración Digital en España, y son públicos, lo que facilita mostrar, de forma clara, el funcionamiento de la Administración digital en España, o la Central de Información del Ministerio de Hacienda. En la Administración de Justicia, estamos trabajando con diferentes entidades, como la mencionada Secretaría de Estado de Digitalización e Inteligencia Artificial, con quien tenemos, por ejemplo, un proyecto de Cita Previa Digital con 130.000 citas previas gestionadas con 82 órganos judiciales y 52 registros civiles".

Desde el punto de vista de Alicia Herrero, "podemos destacar datos.gob.es, una iniciativa que surgió en el ámbito europeo para la reutilización de información del Sector Público. Es información en formato abierto e interoperable, y habría que valorar el impacto que ha tenido en la sociedad. Otra iniciativa es el cuadro de mando que utiliza Función Pública para tomar sus decisiones, sobre todo en momentos de reposición cero en cuanto a empleo público, tomando medidas para poder cubrir este desajuste. Cabe incidir en la creación del data lake de la AGE para aprovechar la información con técnicas de IA, o la evolución de la plataforma de intermediación de datos, un puntal clave a la hora de facilitar la consulta y uso compartido de información".

PROTECCIÓN DE LOS DATOS

En palabras de Aitor Cubo, "los datos hay que blindarlos en todos los ámbitos, porque cada vez somos más interoperables. Es algo que debe ser prioridad, tanto en el Sector Público como en el privado. Tenemos que plantear un refuerzo claro en la ciberseguridad". Se muestra de acuerdo Noemí García, que añade que "todos estamos en el punto de mira, y se ve agravado por la tendencia hacia la nube o la interoperabilidad. Hemos de tomar medidas en muchos ámbitos, como la encriptación, los cifrados, los certificados de servidor... alineados siempre con el Esquema Nacional de Seguridad y contar con el Sistema de Alertas Tempranas. En esto la interoperabilidad es fundamental, al igual que el trabajo de los técnicos, que deben estar al día de cualquier novedad".

Para Carmen García, "la inversión en seguridad no es que sea prioritaria, es que es un básico a la hora de presupuestar. Ese debe ser el enfoque. No debe haber recortes en seguridad, porque lo importante es la prevención, porque no hay riesgo cero. Es la prevención la que te permite reducir riesgos y gastos a posteriori. Otro tema importante es la granularidad del acceso".

Añade Alicia Herrero que "no nos podemos permitir, ni las Administraciones Públicas ni el sector privado, tener un ataque y perder datos o tener pérdidas de servicio. Tenemos un marco como el Esquema Nacional de Seguridad, que apuesta por la integración de la seguridad como algo organizativo y en el diseño de los sistemas. Pretende definir un marco regulado de medidas a cumplir. Cabe destacar también el Centro de Operaciones de Ciberseguridad, que pretende establecer un sistema de seguimiento de ciberseguridad nacional, coordinación con otros organismos internacionales, y poner a disposición de las Administraciones Públicas los elementos tecnológicos y operativos necesarios para la protección de los servicios, infraestructuras y datos". ■

CONTENIDO RELACIONADO

Foro IT User: Nuevos impulsos para la evolución de la Administración digital

HYPERINTELLIGENCE®

Las respuestas
le encontrarán

MicroStrategy®
Intelligence Everywhere

FRANCISCO CARBONELL, ACCOUNT MANAGER PARA SECTOR PÚBLICO DE FORCEPOINT

"HAY QUE MODELIZAR LOS NUEVOS SERVICIOS PENSANDO EN LAS CAPACIDADES DIGITALES DE LA POBLACIÓN"

UNO DE LOS EJEMPLOS DE ESTOS PROCESOS DE TRANSFORMACIÓN DIGITAL QUE ESTÁN VIVIENDO LAS ORGANIZACIONES, Y LA ADMINISTRACIÓN PÚBLICA NO ESTA EXENTA, ES EL TELETRABAJO, QUE HA CRECIDO EXPONENCIALMENTE EN LOS ÚLTIMOS MESES. FRANCISCO CARBONELL, ACCOUNT MANAGER PARA SECTOR PÚBLICO DE FORCEPOINT, NOS OFRECE UNA VISIÓN MÁS DETALLADA DE ESTA REALIDAD.

"LA SEGURIDAD DEL DATO, HABLANDO DE TRABAJO REMOTO, ES FUNDAMENTAL Y DEBE REFORZARSE" (FORCEPOINT)

Explicaba en su ponencia en el Foro IT User: Nuevos impulsos para la evolución de la Administración digital Francisco Carbonell que "los servicios que proporciona la Administración a los ciudadanos son esenciales y ha

habido un incremento de demanda a lo largo de este 2020. Ha quedado claro que la evolución hacia nuevas forma de prestar servicios por parte de la Administración ha sido vital. Y es cierto también que los equipos de TI de los grandes organismos públicos han sufrido mucho para poder seguir manteniendo el servicio y la productividad de los empleados públicos".

NUEVOS RETOS PARA LA ADMINISTRACIÓN

Ahora, "surgen muchos retos", entre los que destacan la "modelización de los nuevos servicios pensando en las capacidades digitales de la población; la accesibilidad de estos servicios por parte de los ciudadanos, dejando atrás la complejidad de otras épocas; transformación de la forma de trabajo de la propia Administración; y aplicar mecanismos de seguridad a estos nuevos modelos de servicio y estos nuevos entornos de trabajo".

Pero, ¿qué es necesario para que esto sea un éxito? ¿Cuáles son las claves del éxito? La primera es "la capacitación y formación de empleados públicos y ciudadanos; la generación de valor a partir de la tecnología y los servicios; que las empresas pasen a ser socios tecnológicos, no meros proveedores; los modelos de contratación deben estar pensados para la búsqueda de valor y no solo en el precio; y la flexibilidad y escalabilidad de la tecnología

"EN LOS ÚLTIMOS MESES, HA QUEDADO CLARO QUE LA EVOLUCIÓN HACIA NUEVAS FORMA DE PRESTAR SERVICIOS POR PARTE DE LA ADMINISTRACIÓN ES VITAL"

para permitir la transformación en la Administración con plataformas que lo soporten, como los modelos cloud".

DIFERENTES NIVELES DE MADURACIÓN DIGITAL

Existen diferentes niveles de evolución digital en las empresas, y en la Administración Pública conviven realidades muy diferentes, por eso es importante que cada organismo opte por las soluciones tecnológicas que necesite, "pero es necesario que la tecnología los acompañe a lo largo de los diferentes estadios de la evolución".

Y esta es la premisa de la que parte la tecnología de Forcepoint, "acompañar a la Administración Pública en su transformación. Por un lado, todas nuestras soluciones de seguridad pueden ser desplegadas en la nube o en entornos on-premise, algo muy importante en el caso de la Administración, porque los modelos de digitalización no son inmediatos. Y, por otro, planteamos integrar todas soluciones de seguridad bajo una plataforma convergente, con una visibilidad integral y políticas de gestión y automatización que van a permitir reducir los costes operativos, junto con la última variable, la seguridad centrada en el usuario".

En los últimos meses "hemos visto que ha sido necesario adaptar la ciberseguridad a la nueva realidad, y el teletrabajo ha sido un ejemplo de ello", por lo que no podemos seguir ofreciendo las soluciones que estábamos ofreciendo hasta ahora. De ahí que la apuesta de la compañía pase por SASE, "que define mecanismos de acceso para recursos internos que permite al usuario trabajar de igual manera tanto si está dentro como fuera de la red corporativa. Y a esto le añadimos prevención de amenazas y prevención de fugas de información, muy importante en nuestro ADN". ■

CONTENIDO RELACIONADO

Ponencia de Forcepoint

Soluciones de seguridad

Dynamic Edge Protection

Dynamic Data Protection

Foro IT User: Nuevos impulsos para la evolución de la Administración digital

MIGUEL ÁNGEL TORRALBA, SENIOR ACCOUNT MANAGER DE PALO ALTO NETWORKS

"NECESITAMOS REACCIONAR ANTE LOS NUEVOS ATAQUES QUE EVOLUCIONAN CADA DÍA Y SON MÁS COMPLEJOS"

EL TODOS LOS PROCESOS DE TRANSFORMACIÓN DIGITAL, TANTO EN ADMINISTRACIONES PÚBLICAS COMO EN CUALQUIER TIPO DE EMPRESA, LA CIBERSEGURIDAD ES UN ELEMENTOS BÁSICO QUE SIEMPRE HAY QUE TENER EN CUENTA, TAL Y COMO NOS EXPLICA MIGUEL ÁNGEL TORRALBA, SENIOR ACCOUNT MANAGER DE PALO ALTO NETWORKS.

Según explicaba Miguel Ángel Torralba en el Foro IT User: Nuevos impulsos para la evolución de la Administración digital, "muchas empresas y Administraciones Públicas están acometiendo sus procesos de transformación digital, se están redefiniendo la forma en la que operar, innovar y conectarse, con clientes y ciudadanos e internamente. Y hemos visto que en esta pandemia muchas Administraciones han tenido que modificar y replanificar su forma de trabajar, y esta transformación ha sido una respuesta a esta situación".

Esta transformación se está fundamentando en tres pilares básicos, "la conectividad con más de 41 mil millones de dispo-

"LA ADMINISTRACIÓN PÚBLICA ESTÁ ACOMETIENDO SU TRANSFORMACIÓN A PASOS AGIGANTADOS" (PALO ALTO NETWORKS)

sitivos conectados, el paso hacia la nube y la evolución de los datos y la Inteligencia Artificial, y, de hecho, sabemos que se van a multiplicar por cinco la cantidad de datos alojados en la nube y analizados por la IA".

"EN ESTOS PROCESOS DE MODERNIZACIÓN Y TRANSFORMACIÓN, DONDE HAY QUE GARANTIZAR LA CONTINUIDAD DEL SERVICIO AL CIUDADANO, ES NECESARIO APOSTAR, DE FORMA DECIDIDA, POR LA CIBERSEGURIDAD"

MEJORAR EL ENFOQUE EN CIBERSEGURIDAD

Con todos estos procesos de modernización y transformación, "donde hay que garantizar la continuidad del servicio al ciudadano, es necesario apostar, de forma decidida, por la ciberseguridad. Y, a día de hoy, ya sea por falta de profesionales o de medios, la mayoría de las organizaciones debe apoyarse en socios que les permitan esa evolución de forma segura".

Para alcanzar este nivel de seguridad, es necesario que los responsables de TI "necesitan mayor visibilidad de lo que pasa en sus arquitecturas de seguridad cada vez más complejas, garantizar y confiar en que la automatización y la IA es capaz de remplazar ese trabajo humano no escalable, y avanzar a un modelo de mayor sencillez y flexibilidad, porque algunas organizaciones tienen una media de 25 tecnologías diferentes y esto hace que sea difícil de gestionar".

Con un perímetro que se está ampliando y una mayor complejidad en la gestión, se demanda "una respuesta frente a los ataques diferente a la tradicional que era manual. Necesitamos reaccionar ante los nuevos ataques que evolucionan cada día y son más complejos, reaccionar ante los nuevos dispositivos que se integran y hay que securizarlo, y reaccionar ante un entorno en constante cambio. Con lo que las organizaciones tienen que innovar apoyándose en la nube, liberando a los equipos de seguridad de las tareas tediosas y sin valor".

UN NUEVO ENFOQUE DISRUPTIVO

Con todo, desde Palo Alto se estima que es necesario acometer "esta evolución con un enfoque disruptivo, con una arquitectura Zero Trust, porque si bien cualquier entorno puede ser vulnerado, hay que ser proactivos en la reacción y la prevención, siendo conscientes de que cualquier elemento de la organización puede crear una brecha de seguridad".

El enfoque de Palo Alto se basa en una solución "integrada, que es capaz de unificar los diferentes elementos para dar a los CIO y los CISO esa visión global que necesitan; automatizada, para eliminar las tareas repetitivas liberando de tiempo rutinario a los equipos de seguridad; y sencilla. Una ciberseguridad que se mantenga por delante de las amenazas en vez de reaccionar ante ellas. Nuestra propuesta es una visión global de todo el entorno, defendiendo tanto el perímetro como la nube y el puesto de trabajo". ■

CONTENIDO RELACIONADO

Ponencia de Palo Alto Networks

Palo Alto Networks

Next Generation Firewall

Foro IT User: Nuevos impulsos para la evolución de la Administración digital

FRANCISCO LOVA, DIRECTOR DE SECTOR PÚBLICO DE PEGASYSTEMS

"TENEMOS QUE PERSONALIZAR LOS SERVICIOS PARA ADECUARLOS A LAS NECESIDADES ESPECÍFICAS DE CADA CIUDADANO"

LA ADMINISTRACIÓN PÚBLICA SE ENFRENTA A UNA SERIE DE RETOS EN SU CAMINO HACIA LA DIGITALIZACIÓN. FRANCISCO LOVA, DIRECTOR DE SECTOR PÚBLICO DE PEGASYSTEMS, NOS OFRECE LA VISIÓN DE SU COMPAÑÍA ALREDEDOR DE ESTOS RETOS Y QUÉ DEBE HACER LA ADMINISTRACIÓN PARA ACOMETERLOS.

"LA DIGITALIZACIÓN DE LAS AAPP DEBE SER EL MOTOR QUE IMPULSE EL CRECIMIENTO ECONÓMICO" (PEGASYSTEMS)

Tal y como explicaba Francisco Lova en el Foro IT User: Nuevos impulsos para la evolución de la Administración digital, "el mundo está cambiando, y no solo por la pandemia. Está cambiando la forma en la que los usuarios, en el caso de la Administración Pública los ciudadanos, reclaman esos servicios, que quieren que sean en tiempo real, personalizados, en cualquier lugar, con

cualquier dispositivo... Por otro lado, cambia el modelo, ya no se demandan productos, sino servicios. Y todo ello genera la necesidad de plataformas que soporten estos cambios".

LA RESPUESTA TECNOLÓGICA

Frente a esto, la respuesta debe ser doble. Por una parte, "personalizar los servicios que se ofrecen a los ciudadanos, haciendo uso de la IA para adecuarlos a las necesidades específicas de cada persona en tiempo real y a través de cualquier canal. Por otra, incrementar la eficiencia de los procesos tanto de cara al ciudadano como de cara al empleado público, y, para ello, nos apoyaremos en el hiperautomatización, la automatización del principio a fin. Combinando ambos elementos podremos asegurar el éxito de estos servicios".

Estamos, explica Francisco Lova, "ante el hito más importante de modernización de los últimos 30 años", un plan de transformación que busca tres objetivos, "mejorar la relación de la Administración Pública con los ciudadanos, incrementar la eficiencia operacional de los procesos administrativos, y tener disponibles el 50% de los servicios públicos en una versión móvil en 2025, para lo que la SGAD debe definir una estrategia global de digitalización, proponer una plataforma global de digitalización, generar esta app factory para poder desarrollar estas aplicaciones, y dotar

"ESTAMOS ANTE EL HITO MÁS IMPORTANTE DE MODERNIZACIÓN DE LOS ÚLTIMOS 30 AÑOS"

de un marco de gobernanza para que esta estrategia tenga éxito".

APRENDER DE LOS ERRORES

Tradicionalmente, tanto las organizaciones públicas como las privadas han cometido dos errores. El primero es "que hemos incrustado mucha lógica en los canales. Según hemos ido incorporando nuevos canales, hemos ido creando silos de relación con los ciudadanos, lo que complica la gestión y la capacidad de evolución. El segundo, ha sido poner toda la lógica junto a los datos en el back-end, lo que lleva la complejidad de esto a la lógica que se ofrece a los ciudadanos".

Por eso hay que pensar de forma diferente, y, en el caso de Pegasystems supone una Arquitectura Center-Out, "donde se aísle la lógica de negocio de los cambios de los canales y de la complejidad de los sistemas de back-end, y definamos lo que llamamos MicroJourney, un hito con un objetivo claro y un resultado definido que se puede alcanzar de forma sencilla".

Para este tipo de retos, "son necesarias tecnologías modernas. Con Pega Infinity se une la hiperautomatización y la IA en una única plataforma digital. Sobre ella, ya hemos creado algunos aceleradores, soluciones verticales para permitir el desarrollo de servicios, con componentes para mejorar la relación con el ciudadano, mejorar los servicios y mejorar la automatización inteligente de procesos". ■

CONTENIDO RELACIONADO

Ponencia Pegasystems

Soluciones para Sector Público

Casos de uso en Sector Público

Foro IT User: Nuevos impulsos para la evolución de la Administración digital

OVANES MIKHAYLOV, BUSINESS DEVELOPMENT MANAGER SOUTHERN EUROPE DE VMRAY

"LAS HERRAMIENTAS TRADICIONALES NO SON SUFICIENTES PARA REALIZAR UN ANÁLISIS DINÁMICO"

EN LOS ÚLTIMOS MESES SE HAN IDO PRODUCIENDO UNA SERIE DE NOTICIAS QUE HACEN INEVITABLE HABLAR DE CIBERSEGURIDAD EN EL SECTOR PÚBLICO. EN ESTE SENTIDO, OVANES MIKHAYLOV, BUSINESS DEVELOPMENT MANAGER SOUTHERN EUROPE DE VMRAY, HABLA DE LA PRINCIPAL TENDENCIA QUE DETECTAN A DÍA DE HOY, LAS AMENAZAS AVANZADAS.

Para Ovanes Mikhaylov, y así lo explicaba en el Foro IT User: Nuevos impulsos para la evolución de la Administración digital, "lo que vemos que está pasando a día de hoy son las amenazas avanzadas, una amenaza que utiliza tecnologías híbridas con un grado muy alto de penetración que es imposible detener con las estrategias tradicionales".

"LA ADMINISTRACIÓN PÚBLICA ES UN OBJETIVO MUY IMPORTANTE PARA LOS CIBERCRIMINALES" (VMRAY)

"LA PRINCIPAL TENDENCIA SON LAS AMENAZAS AVANZADAS, AMENAZAS QUE UTILIZAN TECNOLOGÍAS HÍBRIDAS CON UN GRADO MUY ALTO DE PENETRACIÓN QUE ES IMPOSIBLE DETENER CON LAS ESTRATEGIAS TRADICIONALES"

De hecho, existen organizaciones que no solo organizan ataques coordinados, sino que lo ofrecen como un servicio, explica este responsable, que recuerda que existen más de medio centenar de organizaciones que buscan generar ingresos con este tipo de ataques.

NUEVOS TIPOS DE ATAQUES Y NUEVAS RESPUESTAS

Un ataque avanzado "utiliza técnicas híbridas en tres etapas: entrada, establecimiento y actividades maliciosas. Para entrar, pueden utilizar un mensaje de correo o una noticia para que el usuario clique en un enlace. Tras esto, aprovechando una vulnerabilidad o brecha de seguridad existente se instalan en el sistema, algo que es imposible combatir sin un análisis dinámico". Con las herramientas tradicionales es muy complejo realizar un análisis dinámico por "la falta de recursos, porque son muchas las amenazas que llegan y existe una gran complejidad a la hora de gestionar las diferentes herramientas de distintos proveedores. Es muy importante en este punto automatizar las alertas de ciberseguridad para poder incrementar la capacidad de detección. Otro problema es que el malware entiende si está en un área controlada o no, y puede esperar hasta tener una oportunidad para actuar. Además, todavía las técnicas de análisis necesitan una mayor orquestación. Y, por último, la inteligencia de amenazas no es la más adecuada, por lo que nosotros tratamos de crear una inteligencia de amenazas relevante para nosotros".

SANDBOX

Las herramientas tradicionales no son suficientes para realizar un análisis dinámico, pero con una sandbox, "un entorno seguro para ejecutar cualquier tipo de aplicación, podremos ver qué hace cualquier elemento de software, lo que nos permitirá identificar las actividades maliciosas para poder ofrecer una respuesta adecuada".

En una sandbox, "primero se realiza un análisis de reputación del tipo de fichero, para, después, pasar a un análisis estático, y, posteriormente, a un análisis dinámico, donde dejamos ejecutar el software en un entorno controlado para saber si se taca de una actividad maliciosa o un fichero benigno".

El elemento diferenciador de VMray es "ser invisible para el malware", para que no cambie su naturaleza con el fin de engañar al análisis. ■

CONTENIDO RELACIONADO

Ponencia VMray

Data-sheet VMRAY

VMRAY Technology

Foro IT User: Nuevos impulsos para la evolución de la Administración digital

Palo Alto Networks®, el líder mundial en ciberseguridad, está dando forma al futuro centrado en la nube con tecnología que está transformando la forma en que operan las personas y las organizaciones.

paloalto® NETWORKS

PROPUESTAS DE MEJORA PARA FLEXIBILIZAR LA CONTRATACIÓN DE SERVICIOS TIC EN LA ADMINISTRACIÓN PÚBLICA

LA LLEGADA DE LOS FONDOS NEXTGENERATIONEU SUPONDRÁ UNA NUEVA OLEADA DE CONTRATOS Y LICITACIONES DE SERVICIOS TI EN LA ADMINISTRACIÓN PÚBLICA. FLEXIBILIZAR ESTOS PROCESOS PARA GANAR EN AGILIDAD EN LA ADJUDICACIÓN, SERÁ FUNDAMENTAL PARA AVANZAR EN LOS PROCESOS DE MODERNIZACIÓN Y TRANSFORMACIÓN DIGITAL. ELENA HERNÁEZ SALGUERO, VOCAL LETRADA DE LA COMISIÓN JURÍDICA ASESORA DE LA COMUNIDAD DE MADRID, EXPLICA LAS OPCIONES PARA FLEXIBILIZAR ESTAS LICITACIONES Y LAS NUEVAS VÍAS DE COLABORACIÓN.

EN ESTA PONENCIA SE ANALIZARON LOS RETOS A LOS QUE SE ENFRENTA LA ADMINISTRACIÓN PÚBLICA EN MATERIA DE CONTRATACIÓN. CLICA EN LA IMAGEN PARA VER LA PONENCIA COMPLETA.

Explicaba Elena Hernáez en el Foro IT User: Nuevos impulsos para la evolución de la Administración digital que "se trata de un reto muy importante que va a traer muchos quebraderos de cabeza a todos los implicados. Este Plan es un desafío, pero debemos afrontarlo desde el punto de vista de la oportunidad, no solo de recuperación, sino de establecimiento de nuevas formas de funcionamiento".

OPORTUNIDADES Y HÁNDICAPS

La llegada de los fondos europeos abre la puerta, entonces, a grandes oportunidades, pero plantea "una serie de hándicaps, especialmente en lo relacionado con la compra pública. Primero, que estos fondos deben aplicarse en un período corto de tiempo, algo que parece incompatible con los procesos largos y complejos de cualquier compra pública. En segundo lugar, el acceso a los fondos está sujeto a una condicionalidad, tanto desde el punto de vista macroeconómico como desde el punto de vista del proyecto concreto. El tercero es la complejidad de las materias a las que nos enfrentamos, porque las posibles líneas de acción son complejas en diferentes materias. Y, por último, el proceso de certificación, que es también complejo, y, como ejemplo, España solo logró certificar en 2019 el 39% de los proyectos presentados".

"ESTE PLAN ES UN DESAFÍO, PERO DEBEMOS AFRONTARLO DESDE EL PUNTO DE VISTA DE LA OPORTUNIDAD, NO SOLO DE RECUPERACIÓN, SINO DE ESTABLECIMIENTO DE NUEVAS FORMAS DE FUNCIONAMIENTO"

Partiendo de la realidad, lo mejor es buscar los puntos de mejora que podemos encontrar. En este caso, "tenemos la falta de capacidad de gestión de los centros encargados de licitar y ejecutar los proyectos en muchas ocasiones, la falta de profesionalización y complejidad de la normativa de compra pública, algo que se viene poniendo de relieve desde hace bastante tiempo. Si a la falta de capacidades añadimos la complejidad de algunas nuevas tecnologías, hay que profundizar en la profesionalización de la compra pública". Otro de los problemas es "la falta de costumbre de compras colaborativas, que permitiría captar más fondos con menos gestión, lo que haría una compra pública más eficiente. España tiene menos de un 10% en esta tipología de compra, algo que no ha evolucionado en los últimos años".

Por último, "podemos hablar de la falta de explotación de las posibilidades de colaboración con el sector privado. No solo se trata de flexibilizar procedimientos o de buscar la colaboración con el sector privado, sino de usar otras fórmulas que ya existen en nuestro ordenamiento jurídico y debemos aplicar".

Las fórmulas concesionales permiten apalancar la inversión, ofrecer neutralidad desde la perspectiva de la consolidación fiscal, permite formas de pago diferentes, y abren la puerta a la subcontratación, pero, en cambio, la tramitación es compleja o el reparto de riesgos adecuado en negocios no habituales".

Otra fórmula de adecuación a estas necesidades son los PERTES, pero la propia norma ya adelanta que será necesario "un adecuado marco normativo. No es en sí un modelo de colaboración público-privada, sino que permite articular estos modelos de colaboración".

La solución, por tanto, está en "las sociedades de economía mixta, con un 51% de capital público, que permiten la adjudicación directa de los contratos de concesión, o los consorcios entre instituciones públicas y privadas, una fórmula que permite la creación de una figura jurídica en la que participen instituciones de naturaleza pública y privada, y se ha flexibilizado para el acceso concreto a estos fondos Next-GenerationEU". ■

CONTENIDO RELACIONADO

Foro IT User: Nuevos impulsos para la evolución de la Administración digital

CREANDO UNA ADMINISTRACIÓN DIGITAL INNOVADORA Y DE CONFIANZA PARA EL CIUDADANO

UNO DE LOS PUNTOS DEL PLAN DE RECUPERACIÓN, TRANSFORMACIÓN Y RESILIENCIA ES LA NECESIDAD DE APOYAR LA MODERNIZACIÓN DEL TEJIDO EMPRESARIAL, SU MODERNIZACIÓN Y DIGITALIZACIÓN. LA CIBERSEGURIDAD SE MENCIONA, ADEMÁS, COMO UNO DE LOS ELEMENTOS ESTRATÉGICOS EN ESTA SEGUNDA OLEADA DE TRANSFORMACIÓN EN ESPAÑA.

En esta mesa redonda participaron: Bitdefender, Cytomic, ENISA, Sophos y Thales Digital Identity and Security. Clica en la imagen para ver la mesa redonda completa.

Por eso, en esta mesa redonda abordamos cómo crear una Administración Pública innovadora y de confianza para los ciudadanos. Para ello, contamos en este debate del Foro IT User: Nuevos impulsos para la evolución de la Administración digital con Sergio Bravo, Director Regional de Ventas para España de Bitdefender; Miguel Carrero, Vicepresidente de Cuentas Estratégicas y Proveedores de Servicio de Seguridad de Cytomic; José Bayón, CEO de ENISA; Álvaro Fernández, Responsable de cuentas empresariales de Sophos; y Alfonso Martínez, Country Manager de Thales Digital Identity and Security.

En primer lugar, quisimos saber cuáles son, en su opinión, los retos de las Administraciones Públicas para ser más seguras. Tal y como indica Sergio Bravo, “el reto del departamento de

“TIENE QUE HABER UNA INTERCONEXIÓN MAYOR PARA PROPORCIONAR SERVICIOS MÁS EFICACES Y EFECTIVOS AL CIUDADANO”

SERGIO BRAVO

seguridad es adaptarse y hacer frente al cambio que estamos viviendo con la digitalización. El reto principal pasa por terminar de modernizar sus infraestructuras. Específicamente en seguridad, proteger mejor la infraestructura y los datos. Lamentablemente, con la situación actual los perímetros se han destruido en las organizaciones, y las Administraciones Públicas no son diferentes. Se trabaja mucho desde casa, con lo que el perímetro inicial definido se diluye y se crean nuevas superficies de ataque. Esto es un reto importante a la hora de proteger. También hay que tener en cuenta el reto de la consolidación de los datos y la transición hacia la nube. Tiene que haber una interconexión mayor para proporcionar servicios más eficaces y efectivos al ciudadano, y esto crea un nuevo entorno que debe ser protegido con herramientas optimizadas y unificadas que no compliquen la labor de protección”.

DIFERENTES RETOS A ASUMIR EN SEGURIDAD

Para Miguel Carrero, “ha habido una aceleración de la modernización por la pandemia, y hay un elemento humano muy importante en las Administraciones Públicas, pero específicamente hay que hacer hincapié en un elemento diferenciados: los diferentes entornos dentro de la Administración. Son diferentes realidades y, además, tienen diferentes signos políticos que cambian cada cuatro años, pero en ciberseguridad hay dos elementos básicos. Cuando tienes un sistema poroso, esto es, con distintos entornos no coordinados, es más susceptible de ser atacado con éxito, de ahí que sea fundamental la labor de coordinación de herramientas, procesos y respuesta ante incidentes. Sin esta coordinación es difícil hacerlo. El otro elemento básico es la constancia en el tiempo. El componente humano madura con este plan de seguridad, y si el cambio es radical es como si reiniciaras cada vez”.

LA RESPUESTA DE LA ADMINISTRACIÓN A LOS RETOS DE CIBERSEGURIDAD

Por su parte, José Bayón apunta que “el mayor reto es querer hacerlo, tener voluntad, y el Plan de Digitalización de las Administraciones Públicas, dotado con 2.600 millones de euros, es una prueba de que la voluntad existe. Pero es importante que esto llegue a todos los niveles de la Administración. Tenemos que seguir avanzando, pero no podemos olvidar el valor del dato como habilitador de procesos e instrumentos, con lo

“LA CIBERSEGURIDAD ES UN JUEGO DE TALENTO QUE SE SITÚA EN LA INTERSECCIÓN DE LA TECNOLOGÍA, LAS PERSONAS Y LOS PROCESOS”

MIGUEL CARRERO

“NO PODEMOS OLVIDAR EL NECESARIO CAMBIO CULTURAL Y EL COMPONENTE HUMANO QUE, EN EL CASO DE LA ADMINISTRACIÓN, ES MÁS CRÍTICO”

JOSÉ BAYÓN

que, aún con la ciberseguridad, deben seguir pudiendo aprovecharse como un propio servicio público. Y no podemos olvidar el necesario cambio cultural y el componente humano que, en el caso de la Administración, es más crítico”.

Comparte la opinión de sus contertulios Álvaro Fernández, que señala que “el principal reto de la ciberseguridad en la Administración española está en tres áreas: proteger, detectar y responder. Creo que se ha puesto el foco tradicionalmente en proteger, tanto en herramientas como en recursos humanos, pero la transformación se está acelerando y creando una brecha en la detección y la respuesta, y ahora llega el momento de poner ese componente humano, altamente especializado, en la detección y la respuesta, con tecnologías como los EDR o los XEDR, tecnología adecuada pero que necesita personal especializado para dar respuesta a estas amenazas. Si no lo hacemos bien, nos enfrentaremos a algunos casos como los que ya hemos visto. Es un reto este cambio cultural para la Administración. Hay que invertir en el capital humano para detectar y responder”.

Concluye Alfonso Ramírez comentando que “la pandemia ha abierto una brecha entre donde queríamos estar y donde estamos. Los principales retos han sido dar seguridad a los funcionarios en el trabajo en remoto y la privacidad de los datos. Es cierto que hay que proteger a los usuarios privilegiados de ataques, pero lo primero que tenemos que proteger es el propio dato, porque, si todo lo demás, falla, pero los datos están cifrados, el problema es menor que si no lo están. El personal ha tenido que aprender a marchas forzadas por la situación vivida. Garantizar el acceso seguro y datos protegidos son, resumiendo, el principal reto a asumir”.

SERVICIOS INNOVADORES Y DE CONFIANZA

Además de segura, la Administración tiene que ser innovadora, así que nos preguntamos qué tipo de servicios de confianza se pueden ofrecer a los ciudadanos. Tal y como indica José Bayón, “debe ser innovadora y el cambio cultural es todavía más importante. En la Administración la confianza debe estar en el centro, porque el cliente es el ciudadano. Además, existen retos añadidos, porque la transformación está modificando las propias relaciones de las personas y empresas con la Administración, y la cantidad de servicios que se pueden ofrecer aumenta de forma importante. Son muchos los servicios a los que se puede acceder mediante autenticación segura para asegurar la confianza y proteger el dato”.

“NO SE TRATA DE COGER UN SERVICIO QUE YA ESTUVIERA OFRECIÉNDOSE Y SECURIZARLO, SINO DE EMPEZAR DESDE CERO PARA DISEÑARLO CIEN POR CIEN SEGURO”

ÁLVARO FERNÁNDEZ

Para Álvaro Fernández la clave es “la confianza. Los ciudadanos necesitamos confiar en las instituciones y en los servicios digitales que proporcionan. Cualquier servicio que se preste debe tener una base de seguridad. No se trata de coger un servicio que ya estuviera ofreciéndose y securizarlo, sino de empezar desde cero para diseñarlo cien por cien seguro”.

Añade Alfonso Martínez que, como ciudadano, “lo que me da confianza es que mis datos estén seguros. La Administracion debe unificar esfuerzos, desde arriba hacia abajo, para investigar estas herramientas de autenticación como servicio. E igual para el cifrado. La empresa privada está usando la nube por agilidad, eficiencia... y tenemos que conseguir que la Administración también la use, pero garantizando que se haga de forma segura y con datos cifrados, y tratar de que sean las propias agencias u organismos los poseedores de estas claves de cifrado, que no dependan de terceros”.

Según Sergio Bravo, “cualquier tipo de servicio que emplee datos sensibles de los ciudadanos debe depender de la seguridad para ser de calidad y confiable. En la pandemia hemos visto los límites de las plataformas de gobernanza digital y está claro que hay que seguir desarrollando. Cualquier modelo de gobierno digital eficaz va a necesitar la integración y funcionamiento en conjunto de estas plataforma con intercambio de datos que debe ser seguro. Un ejemplo concreto que hemos visto ha sido la Telemedicina. En la atención primaria va a ser importante seguir desarrollándolo para casos menos graves, descargando a los centros de salud”.

“LOS PRINCIPALES RETOS SON DAR SEGURIDAD A LOS FUNCIONARIOS EN EL TRABAJO EN REMOTO Y LA PRIVACIDAD DE LOS DATOS”

ALFONSO MARTÍNEZ

En opinión de Miguel Carrero, “la innovación tiene dos elementos: los servicios públicos que nos ofrece y cómo nos los ofrece. Puede haber servicios tradicionales que se ofrezcan de forma más eficiente, y eso tiene que ser seguro, y puede haber nuevos servicios que la Administración diseñe para los ciudadanos. La seguridad es una de las responsabilidades básicas de cualquier Administración, no solo de sus servicios, sino proporcionando un paraguas seguro para nosotros, como individuos o como profesionales. Y también debe establecer el marco legislativo que permita al sector privado innovar. Y ahí hay muchas cosas por hacer, y un ejemplo es permitir compartir información entre entidades para hacer frente a las nuevas amenazas”.

Si entramos en la seguridad del dato, añade Miguel Carrero, “la seguridad es un entorno multidimensional, donde el enemigo tiene complicaciones cuando la seguridad tiene diferentes dimensiones. Todas son relevantes, pero lo diferencial es cuando las combinas. En la seguridad física, usamos diferentes vectores de protección que impidan el éxito del atacante, y en ciberseguridad debe ser igual. La combinación de elementos en los XDR para una protección, detección y respuesta sigue siendo crítica”.

CAPTACIÓN DEL TALENTO

Uno de los objetivos del Gobierno es incrementar el mercado de la Ciberseguridad y atraer y retener talento. ¿Cómo afectará esto a la Administración Pública? Para José Bayón, “la ciberseguridad no ha tenido nunca más relevancia que ahora. Pero desde hace tiempo es una palanca de desarrollo y de mejora de la competitividad, y eso queda claro por la apuesta presupuestaria de la Unión Europea,

y por la importancia que le dan las empresas. Está en el core de la toma de decisiones. Así que es una oportunidad clarísima de negocio y de generación de empleo. Pero este empleo debe ser específico y especializado".

Apunta Alfonso Martínez que "no tenemos que perder de vista que detrás de las soluciones innovadoras tenemos personas que tienen que gestionarlas, con lo que la captación de talento es un reto. A los fabricantes se nos tiene que exigir que las soluciones sean sencillas de gestionar, y tenemos que facilitar a las Administraciones Públicas estos entornos de seguridad".

Álvaro Fernández recuerda que "la ciberseguridad es transversal a todas las tecnologías innovadoras, y tarea de los fabricantes debe ser simplificar la complejidad. Tenemos que hacer que algo complejo sea sencillo de administrar por parte de los usuarios. La seguridad debe estar en todas las áreas para dar confianza, y el esfuerzo del Gobierno en esta línea es una oportunidad para todos".

Según Miguel Carrero, "la ciberseguridad es un juego de talento que se sitúa en la intersección de la tecnología, las personas y los procesos, pero quien está detrás son las personas. El talento hay que atraerlo, manejarlo, pero no se trata de contar con una persona muy talentosa, sino de subir la media de los profesionales y del ciudadano en cuanto a los elementos de ciberseguridad. Es un tema de presupuesto, legislación, y de crear un entorno en el que podamos ganar la partida a los ciberdelincuentes".

Concluye Sergio Bravo, que comenta que "cualquier inversión para impulsar la ciberseguridad y captar talento es buena por definición. Es cierto que tenemos talento en España, pero es difícil retener el talento, y un esfuerzo para conseguirlo va a impactar positivamente en la mejora de la calidad de la ciberseguridad. Los proveedores tenemos que hacer la vida más fácil a los especialistas con herramientas integradas. Además, no todos los organismos están en el mismo punto de madurez, y debemos acompañarlos en el camino que tenga que recorrer cada uno de ellos. ■

CONTENIDO RELACIONADO

Foro IT User: Nuevos impulsos para la evolución de la Administración digital

NUEVAS CAPACIDADES PARA EL FUNCIONARIO TIC

EL TALENTO ES FUNDAMENTAL, Y NINGUNA TRANSFORMACIÓN O DIGITALIZACIÓN DE LA ADMINISTRACIÓN PÚBLICA PUEDE HACERSE SIN EL VALOR DEL CAPITAL HUMANO, SIN LOS PROFESIONALES QUE PARTICIPAN EN LOS DIFERENTES SERVICIOS DE TI. CARMEN CABANILLAS, PRESIDENTA DE ASTIC, DA CUENTA DE LOS IMPULSOS QUE NECESITA EL TALENTO EN LOS PROFESIONALES PÚBLICOS PARA AFRONTAR CON ÉXITO ESTOS PROCESOS MODERNIZADORES.

Señalaba Carmen Cabanillas en el Foro IT User: Nuevos impulsos para la evolución de la Administración digital que "la Administración está realizando un gran esfuerzo por captar talento y nosotros, dentro de nuestro colectivo, somos multidisciplinares, además de la experiencia profesional, con lo que podemos competir con cualquier profesional de las empresas privadas. Somos la entidad que mayor volumen de datos gestiona, y tenemos que hacer una apuesta por conseguir un directivo público profesional".

UNA POSICIÓN DE PRIVILEGIO

España ocupa una posición de liderazgo en los servicios públicos en Europa, "una meritoria segunda posición, gracias al esfuerzo de todos en estos pasados años. Superamos

"NECESITAMOS UN MODELO DE GOBERNANZA MÁS GRANULAR PARA TENER UN ÚNICO MARCO DE REFERENCIA" (ASTIC)

Foro Administración Digital 2021

a la media europea en casi todos los indicadores. También en datos abiertos, donde hemos hecho un gran esfuerzo para situarnos en el segundo puesto europeo. Según los datos de la OCDE, tenemos un séptimo puesto a nivel global. Además, nuestros servicios son ampliamente consumidos, algunos de ellos muy relevantes".

Otro de los logros ha sido "la implantación del teletrabajo en un tiempo récord. En apenas tres días conseguimos tener a 200.000 funcionarios trabajando desde sus casas, no solo manteniendo los trámites habituales, sino que hemos incrementado los servicios en un 180%, pasando de 5.000 a 90.000 trámites diarios".

LÍNEAS DE MEJORA

La pregunta es, ¿cuenta la Administración con muchos medios para alcanzar estos resultados? "Nuestro presupuesto es muy reducido, no hemos llegado al nivel que teníamos en 2016", de ahí que sea crucial emplear estos fondos europeos. Además, "el ratio de los empleados TIC en la Administración en España está en el 2%", cuando en Europa el ratio suele oscilar entre el 3 y el 5%. Con todo, "necesitamos estar en la toma de decisiones, y algunas organizaciones ya han optado por un profesional TIC como Director General, pero en otras ocasiones no se ha contado con nosotros, como en la recientemente creada Dirección General de Transformación, Digitalización e Inteligencia Artificial".

"NECESITAMOS ESTAR EN LA TOMA DE DECISIONES, Y ALGUNAS ORGANIZACIONES YA HAN OPTADO POR UN PROFESIONAL TIC COMO DIRECTOR GENERAL"

Otra de las líneas de mejora es conseguir "mayor representación de las mujeres. En la AGE, la presencia de las mujeres supera el 50%, pero en el colectivo TIC llegamos escasamente al 30% y en el CDTIC apenas alcanzamos el 24%. Es algo que tenemos que mejorar, tenemos que integrar más talento, y el talento femenino es muy importante. A nivel directivo, los TIC solo alcanzamos un 3% de los niveles 30, y las mujeres son solo el 15% de este pequeño grupo. Necesitamos una apuesta decidida por mejorar nuestra posición".

Otra debilidad es la Ley de Contratos, "que no está adaptada a lo que necesitan las Tecnologías de la Información. En el nuevo Decreto Ley hay mejoras, pero no es suficiente". Con los fondos Europeos "tenemos una gran oportunidad, pero no sabemos si vamos a ser suficientes profesionales TIC para crear y mantener estos servicios".

También hay que mejorar "en la capacitación digital y en el desarrollo de las carreras profesionales, con el fin de aportar y mantener talento a las organizaciones".

Para dar respuesta a estas realidades, la propuesta de ASTIC pasa por crear dos caminos. Por un lado, "para los compañeros más especialistas que prefieren continuar con su labor en su organización y seguir especializándose, y, por otro, para aquellos que tenemos una visión más generalista y podemos contribuir a la innovación. La formación que recibimos no es suficiente, hay que intensificar y conseguir una formación más práctica. Y esta formación es la mejor defensa ante las amenazas o en la protección de datos. Creemos que hay que colaborar con universidades y centros de formación para reforzar nuestras habilidades". ■

CONTENIDO RELACIONADO

Ponencia de Astic

Foro IT User: Nuevos impulsos para la evolución de la Administración digital

Se resiliente hoy Se fuerte mañana con Pega

Te acompañamos al éxito de tu estrategia de digitalización: de la robotización a la gestión dinámica de casos inteligente a largo plazo.

¡Para más información, pulse aquí!

PEGA®

TRES DESAFÍOS TECNOLÓGICOS PARA EL SECTOR PÚBLICO

JESÚS GALINDO

AREA VP, PUBLIC SECTOR, SALESFORCE IBERIA

Los acontecimientos del último año han llevado al límite a muchas organizaciones, tanto públicas como privadas. De la noche a la mañana ha sido necesario reestructurar procesos, organizar sistemas para poder trabajar en remoto, desarrollar mecanismos para la prestación de servicios a distancia o incluso desplegar nuevos servicios en cuestión de semanas o días.

El hilo conductor de todos estos cambios han sido las tecnologías digitales. Pero no todo el mundo ha podido reaccionar con la misma agilidad. Si bien las empresas tecnológicas, como en el caso de Salesforce, pudimos asegurar la continuidad de las operaciones con el 100% de nuestros empleados trabajando en remoto desde el primer momento, muchas empresas e instituciones se encontraron con problemas. Algunos básicos, como no contar con ordenadores portátiles y dispositivos móviles para todos los empleados, y otros estructurales, como no tener sistemas que permitieran su uso en remoto por parte de los empleados con las necesarias garantías de disponibilidad y seguridad.

En la Administración Pública estos problemas han sido notables. A pesar del fuerte compromiso de muchos responsables y funcionarios para superar la situación, la crisis de la Covid-19 ha puesto sobre la mesa carencias significativas en la infraestructura digital en todos los niveles de la administración, carencias que se han superado con éxito en muchos casos debidos al esfuerzo extra del personal de IT.

Conviene hacer una reflexión sobre cuáles son esas carencias y, por lo tanto, cuáles son los desafíos a los que se enfrentan las administraciones públicas en el entorno digital. No solo para hacer frente a posibles crisis, sino sobre todo para asegurar un mejor servicio al ciudadano a medio y largo plazo. Estos tres son los principales desafíos tecnológicos que hemos identificado:

1. SUPERAR LAS LIMITACIONES DE LOS SISTEMAS LEGACY. Los sistemas tecnológicos de las Administraciones Públicas están construidos sobre infraestructuras heredadas que, en muchos casos, están cercanas a la obsolescencia, en gran medida debido a los recortes de la pasada crisis, aunque a veces también se ha seguido la máxima de "si algo funciona, mejor no tocarlo". La falta de presupuestos y recursos y el hecho de trabajar con tecnologías anticuadas convierte la puesta en marcha de nuevos servicios en una cuestión casi heroica.

Por lo tanto, las administraciones tienen que apostar por un nuevo tipo de tecnología (normalmente con soluciones en la nube) que permita la puesta en marcha de nuevos servicios. Evidentemente, no es posible hacer un cambio drástico de todos los sistemas, pero sí es perfectamente factible –y mucho más eficiente en costes- añadir una capa adicional de soluciones y aplicaciones que actúen a modo de interfaz (con los funcionarios y con los ciudadanos) y que estén conectadas con los sistemas legacy. Desde Salesforce creemos que la solución pasa por soluciones híbridas, como Mulesoft, que permiten hacer esa conexión, desarrollar reglas de negocio de una forma ágil y programar prácticamente sin tener que invertir en desarrollo.

2. REDUCIR LOS TIEMPOS DE DESPLIEGUE. Para muchos responsables de tecnología del Sector Público debe resultar tremendamente frustrante encontrarse con un nuevo Real Decreto (o una instrucción de su Comunidad Autónoma o Ayuntamiento) que obligue a poner en marcha un servicio. Muchos de ellos saben, desde el primer momento, que tal desarrollo no va a ser posible o se va a retrasar de forma irremediable porque su infraestructura no está preparada para ello.

Las soluciones en la nube son, de nuevo, la respuesta adecuada. Los tiempos de despliegue se reducen de años a meses y de meses a semanas en la puesta en marcha de prácticamente cualquier servicio.

Hay ejemplos evidentes y donde la urgencia es una necesidad. Nuestras comunidades autónomas están luchando para gestionar de manera eficaz el programa de vacunación Covid. La solución desarrollada por nosotros, Salesforce Vaccine Cloud, se ha implantado en cuestión de semanas, permitiendo gestionar más 120.000 citas en un día con picos de cuatro citas por segundo.

“SUPERAR LAS LIMITACIONES DE LAS TECNOLOGÍAS LEGACY, REDUCIR LOS TIEMPOS DE DESPLIEGUE Y ADOPTAR UNA FILOSOFÍA CENTRADA EN LA EXPERIENCIA DEL CIUDADANO SON LAS PREMISAS FUNDAMENTALES PARA EL DESARROLLO FUTURO DE LAS TECNOLOGÍAS EN EL SECTOR PÚBLICO”

3. ADOPTAR UN ENFOQUE DE “EXPERIENCIA DEL CIUDADANO”. Bregar con páginas web de las administraciones es un reto para cualquier ciudadano de a pie. La gran mayoría están orientadas al proceso, el formulario que hay que rellenar, y no al ciudadano. Las páginas web de las administraciones reflejan en gran medida la complejidad de la organización pública, de reglamentaciones jurídicas y de procesos administrativos que el ciudadano no tiene por qué conocer. La experiencia del ciudadano hoy en día es realmente pobre, sobre todo si se compara con los enormes avances obtenidos por las empresas privadas en este terreno. Todos sabemos lo fácil que es comprar on line, por el ordenador, con el móvil y desde cualquier dispositivo.

Mejorar la experiencia del ciudadano o, mejor aún, poner la experiencia del ciudadano en el centro de la estrategia digital de la administración, debería ser el primer paso en cualquier desarrollo futuro o rediseño de los procesos existentes. Además, esa experiencia debe responder a los requerimientos habituales del moderno mundo digital. Debe ser, por lo tanto, omnicanal y, en la medida de lo posible, debe unificar los trámites y gestiones en un mismo lugar, incluso aunque pertenezcan a instituciones diferentes. Y esto requiere no sólo una adecuada respuesta tecnológica, sino una clara determinación política y un cambio de mentalidad colectiva.

Superar las limitaciones de las tecnologías legacy, reducir los tiempos de despliegue y adoptar una filosofía centrada en la experiencia del ciudadano son las premisas fundamentales para el desarrollo futuro de las tecnologías en el Sector Público. Con estas premisas las administraciones podrán sumarse al ritmo que imponen las tecnologías más innovadoras como la Inteligencia Artificial o el 5G, desarrollar en plenitud el modelo de Smart Communities y una administración inteligente y, sobre todo, incrementar la eficiencia y reducir los costes operativos, lo cual redundará en beneficio de todos. ■

UNA NUEVA ADMINISTRACIÓN PÚBLICA HIPERINTELIGENTE Y ACCESIBLE PARA TODOS

FERNANDO GUTIÉRREZ-CABELLO

ACCOUNT EXECUTIVE, MICROSTRATEGY

La Administración Pública española parte de una excelente posición, segundos en el ranking de digitalización DESI, pero como toda gran entidad tiene una dificultad inherente: el tamaño, la dispersión territorial y la diversidad de público al que ofrece un servicio, todo ello genera una gran brecha digital.

En el "Plan de Digitalización de las Administraciones Públicas 2021 -2025", dos de los retos fundamentales son salvar dicha brecha digital y aumentar la productividad del empleado público. Ambos retos son provocados en gran medida por cómo se realiza la gestión y explotación del dato.

La existencia de multitud de sistemas heredados, diversos canales de explotación que generan redundancia de datos y que carecen de interoperabilidad hacen que el acceso a la información sea complicado, tanto para la ciudadanía como para el empleado público.

Tres son las áreas de mejora que vemos desde MicroStrategy por nuestra experiencia tanto en el sector público como en el privado, donde se enfrentan a situaciones similares y donde hemos aplicado nuestra solución con éxito.

La primera de las áreas es en la gestión y gobierno del dato. Se busca un sistema informacional menos disperso con reglas de negocio que ordene, sea fiable, seguro y dé calidad al dato.

La segunda área es la explotación del dato. No vale de nada hacer el paso anterior, si a continuación se explota la información con herramientas que no permiten el gobierno de la misma, provocando de nuevo, el caos y la pérdida de todo el esfuerzo de tiempo y dinero invertido en el paso anterior. La tercera de las áreas es cómo se accede al dato. En muchas ocasiones es complejo, confuso y sin experiencia de omnicanalidad.

MicroStrategy con 30 años de experiencia en el sector de la explotación del dato, hemos creado una plataforma robusta que da solución a esos problemas a los que las organizaciones se enfrentan, concentrando nuestros esfuerzos sobre todo en la explotación, la seguridad y el acceso al dato. Disponemos de capacidades de gobierno también a la hora de la explotación, asegurando una versión única de la verdad a lo largo de toda la organización.

Por otro lado, nuestra capacidad de escalabilidad tanto de datos como de usuarios permite crecer según las necesidades que van surgiendo, pues no olvidemos que la cantidad de datos que se van a manejar y los usuarios que accederán a ella van a ser muy elevados.

MicroStrategy ha abierto la arquitectura al máximo para que encaje en el ecosistema de las instituciones y sea lo suficientemente flexible para admitir nuevos sistemas que vengan a futuro. Esto lo ha conseguido creando APIS para toda la plataforma. Esa arquitectura abierta permite leer de prácticamente todas las fuentes de datos posibles (bases de datos, datos en Cloud, Inteligencia Artificial, MDX...) como inyectar datos en cualquier dispositivo, se convierte en un proveedor de datos de otros aplicativos (aplicaciones móviles, portales, Phyton, Inteligencia Artificial...) Con respecto al acceso al dato, MicroStrategy permite acceso multicanal: chatbots, portales, móvil, otras herramientas de Business Intelligence... y ofreciendo una experiencia omnicanal.

“SE BUSCA UN SISTEMA INFORMACIONAL MENOS DISPERSO CON REGLAS DE NEGOCIO QUE ORDENE, SEA FIABLE, SEGURO Y DÉ CALIDAD AL DATO”

Siendo una característica fundamental para MicroStrategy la seguridad con la que se accede. MicroStrategy ofrece seguridad robusta y centralizada al dato. Queremos resaltar algo disruptivo e innovador que no se había visto antes, HyperIntelligence, que permite consolidar los datos más relevantes de diferentes fuentes en una tarjeta/ficha sin necesidad de programación ni de integración en el sistema.

HyperIntelligence ofrece respuestas inmediatas encima de cualquiera de las aplicaciones (en web, correo electrónico o dispositivo móvil) con las que se trabaja a diario, sin integración en el sistema. Permite “guardar” en el navegador: nombres, códigos, expedientes, CIF, DNI... y cuando aparezca uno de esos criterios, lo subrayará y simplemente con situar el ratón por encima, le abrirá una ficha.

Las tarjetas permiten un acceso rápido, seguro, sencillo y moderno tanto para la ciudadanía como para los empleados públicos. Además, las tarjetas permiten enriquecer aplicaciones de negocio existentes sin realizar integraciones físicas entre ellas, se trata de una integración visual. Esta capacidad de enriquecer otras aplicaciones (CRM, ERP, aplicativos, otras herramientas de Business Intelligence...), de simplificar el acceso y consumo del dato para la toma de decisiones, aumenta drásticamente la productividad y solventa la brecha digital existente.

La visión de MicroStrategy es disponer del dato de manera sencilla, rápida y segura en cualquier sitio y en cualquier canal para facilitar la toma de decisiones. ■

LA CLAVE PARA QUE UNA CIUDAD SEA INTELIGENTE ES LA CONECTIVIDAD

PEDRO MARTÍNEZ BUSTO

RESPONSABLE DE DESARROLLO DE NEGOCIO EN HPE ARUBA

Ninguna ciudad estudia para ser inteligente, de hecho, las ciudades no estudian… Son entornos urbanos que solo alcanzan a ser meritorias de tal calificación, cuando se establecen unos ciertos niveles y tipos de servicio que se apoyan de forma profusa en información generada en las interacciones entre Administración y ciudadanos o en datos generados por un ecosistema de “cosas” conectadas a las redes de las ciudades; estos servicios mejoran la experiencia del ciudadano cuando interactúa con la ciudad, siendo a ojos de este más inteligente.

Ya no basta con tener una conexión inalámbrica generalizada; la conectividad es un servicio de primera necesidad, y para aportar más valor a las personas, es necesario redefinir el papel de las redes para posibilitar nuevos servicios y modelos de intercambio de información entre la Administración, los ciudadanos, los visitantes y las “cosas”.

EL CIUDADANO REQUIERE SERVICIOS INNOVADORES

Agilidad, rapidez, comodidad: hoy en día el ciudadano exige servicios que requieren una arquitectura de red avanzada que permita habilitar servicios innovadores en todos los ámbitos de la ciudad: movilidad, cultura, deporte, trámites oficiales… Esto significa que la infraestructura de red debe garantizar una cobertura adecuada para proporcionar conectividad a las personas y a las cosas en cualquier localización , en el interior de los edificios públicos, en los museos, en las paradas de metro, bus y cercanías, incluso en entornos abiertos como calles, plazas y parques; debe poder ofrecer a los ciudadanos servicios de valor añadido, como notificar si hay retraso en una línea de metro, o atascos en una de las entradas a la ciudad y ofrecer rutas alternativas a la ciudadanía. Buen ejemplo de todos estos servicios los encontramos en Bilbao, que ha actualizado su conexión inalámbrica en apoyo de la continua evolución de su ciudad inteligente.

EL PAPEL DE LA SEGURIDAD ES CLAVE

La estrategia de seguridad debe ser integral, ofreciendo protección desde el extremo (donde se generan los datos) a la nube (donde se ofrecen los servicios). Es necesario buscar ese equilibrio entre servicios cada vez más innovadores y avanzados, y una adecuada protección de la red y de la información sensible de las personas.

La aplicación de políticas “Zero Trust” en la red que solo permiten la conexión a los dispositivos que se han identificado previamente, junto con políticas de “MicroSegmentación”, que definen de forma granular cuáles son los flujos de comunicación o acceso a aplicaciones autorizados para cada dispositivo, son claves para que la red se convierta en una barrera de contención eficaz, en un entorno en el que cualquiera de los dispositivos que se conectan puede ser una amenaza que comprometa la seguridad de toda la red.

EL DATO MEJORA LA EXPERIENCIA

Los proyectos de smart cities más exitosos aprovechan las funciona-

“HOY EN DÍA EL CIUDADANO EXIGE SERVICIOS QUE REQUIEREN UNA ARQUITECTURA DE RED AVANZADA QUE PERMITA HABILITAR SERVICIOS INNOVADORES EN LOS ÁMBITOS DE LA CIUDAD”

lidades avanzadas de la red, para obtener datos relevantes y sacar provecho de los mismos. Por ejemplo, la tecnología desplegada en la ciudad de Bilbao permite al Ayuntamiento generar información valiosa para los ciudadanos y los visitantes; la red WiFi recaba datos de localización de todas las personas que llevan un smartphone, esta información que se recoge de forma anónima, permite entender mejor y tener una visión en tiempo real de los patrones de comportamiento y movimiento de los ciudadanos y los visitantes a nivel global, facilitando una mejor planificación de servicios como Limpieza, Seguridad, Transporte Público o Emergencias.

LA RED EN MODO SERVICIO

Hace ya muchos años que se han consolidado los modelos de computación o almacenamiento en modo servicio por sus ventajas; en el caso de las redes estos modelos, aunque relativamente más novedosos, pueden aportar importantes beneficios a las ciudades.

Abordar una inversión en infraestructura de red puede convertirse en una barrera importante para su actualización, disponer de la red en modo servicio elimina este obstáculo al no requerir partidas presupuestarias específicas para acometer la inversión; el hecho de poder acompasar los pagos periódicos por el servicio con los ingresos recurrentes también periódicos, facilita enormemente el acceso por parte de la Administración. Las ventajas en términos de flexibilidad y adaptabilidad a nuevos requerimientos también son evidentes. La red como servicio garantiza unos plazos mucho menores para la renovación tecnológica, comparada con las redes en propiedad, asegurando la disponibilidad de las funcionalidades más avanzadas; por otro lado la administración no tiene que preocuparse de invertir en la capacitación de su personal de TI para que pueda beneficiarse de todas las posibilidades de la red durante la fase de operación, ya que es el proveedor del servicio el que asume este rol. ■

UN CAMBIO Y ACELERACIÓN EN TRANSFORMACIÓN DIGITAL DE LAS AAPP

FERNANDO FELIU

GLOBAL CUSTOMER SOLUTIONS DIRECTOR, V-VALLEY, THE VALUE OF ESPRINET GROUP

Cuando evaluamos las inversiones en las AAPP, actuales y en los próximos años, no debemos generalizar ni simplificar lo que ha supuesto y supondrá en los ciudadanos.

Empecemos por la implantación de los fondos de la UE, donde se ha dado un cambio en el proceso de aportaciones, debido a la situación provocada por la pandemia, llegándose a hablar de un "proceso hamiltoniano", lo que supone un hecho histórico en la recaudación de los fondos de inversión ya que, por primera vez en la historia de la UE, este endeudamiento es global y no contribuciones de cada uno de los países miembros que la componen.

Una vez recabados dichos fondos, se han repartido en los diferentes estados miembros para combatir o contrarrestar la pandemia producida por la COVID, y ha dado origen a la aceleración de la digitalización de muchos procesos y, por tanto, a la aplicación de nuevas tecnologías, hasta el momento no explotadas, acercándolas al ciudadano y dotándoles, independientemente de si eran zonas rurales, al tamaño de las ciudades, comunidades o en un ámbito nacional de modelos de interactuación disruptivas, pero más igualitarias.

Indiscutiblemente esto ha influido en la forma de interactuar con ellos, en el caso de que fuera necesario, ya que hay mucha inversión de tipo interno, prevaleciendo la seguridad de su salud debido a la pandemia.

En este punto había que crear primero las infraestructuras de intercomunicación segura y replantear nuevos métodos digitales para poder contactar con ellos y sus datos, ya que no todos, independientemente de la edad, estaban maduros en las herramientas digitales.

Así, áreas como la Educación o la Sanidad han sido foco en esta digitalización. ¿Quién no tiene un hijo en edad escolar que no haya recibido formación en remoto? ¿Quién no ha recibido una citación para vacunarse o hacer un cita para visitar al médico de forma telemática? Pensemos en estos casos con un poco de profundidad.

Replantearse las necesidades de colegios o universidades para poder interactuar con los alumnos ha supuesto un cambio de necesidades y de mentalidad, tanto de alumnos como del profesorado, que ha traído consigo un cambio en el modelo y las herramientas necesarias para poder mantener una "normalidad" en el sistema educativo donde la videoconferencia, herramientas de comunicación, redes o sistemas de software educativos han transformado "digitalmente" las aulas.

Esto mismo ha sucedido en la Sanidad, donde se intentaba minimizar los contagios tanto a los profesionales como a los pacientes, dotando de herramientas tan innovadoras como la Inteligencia Artificial (sistema de citas, por ejemplo) o la telemedicina para poder atender a posibles pacientes sin un contacto físico a menos de que fuera necesario, como replanteando la utilización de las herramientas internas de los hospitales a través del IoT.

Esta última tecnología es la que también se utiliza en la trazabilidad del medicamento o en el mantenimiento de la cadena de frio en las

“TODOS ESTOS CAMBIOS HAN HECHO QUE SE PRODUZCA, NO SÓLO UN CAMBIO INTERNO EN LAS AAPP, SINO TAMBIÉN EN AQUELLOS QUE LE APORTAN CONOCIMIENTOS Y SOLUCIONES EN SU CADENA DE VALOR”

vacunas que deben mantenerse a cierta temperatura.

No olvidemos inversiones que se están realizando para transformar nuestras ciudades en Smart Cities, con impactos en diferentes áreas de la AAPP como en las Fuerzas del Orden y Protección Civil (tanto preventivo como de tiempo de actuación ante incidente), el impacto de contaminación climática, acústica o lumínica (con resultado de ahorros de costes considerables) o el futuro de los coches autónomos con la entrada del 5G.

Todos estos cambios han hecho que se produzca, no sólo un cambio interno en las AAPP, sino también en aquellos que le aportan conocimientos y soluciones en su cadena de valor (fabricantes, reseller o mayoristas).

Dar soluciones digitales a los problemas de forma creativa y en tiempo récord, pero también cómo poder acceder a las ayudas para poder financiarlas, ha sido una de las prioridades que nos hemos planteado en V-Valley (proyecto de valor del Grupo Esprinet) desde su creación.

El contar con las marcas adecuadas en todas las tecnologías requeridas (Cloud, IoT, servidores, almacenamiento, networking, seguridad, autoidentificación, UCC…), con profesionales certificados focalizados en las ayudas en la preventa / postventa, una fuerza comercial formada e innovadora, con una gran cercanía al cliente, planteando las mejores soluciones en cada uno de los proyectos, la creación de Serviceland para poder cubrir todos los servicios que necesiten completar nuestros clientes de canal, la creación de V-Valley Academy para forma en todas las tecnologías, y casos de éxito, y a la vez informar de como acceder a estas ayudas (Next Generation y otras), hacen de V-Valley el pilar donde poder pivotar todas las necesidades que se dan en este nuevo entorno de las AAPP ayudando y colaborando estrechamente con los profesionales del canal que acercan la digitalización a las AAPP. ■

LA TRANSFORMACIÓN DIGITAL DEBE PRODUCIRSE EN TODOS LOS ÁMBITOS DE LA ADMINISTRACIÓN

FRANCISCO CARBONELL ACERA
ACCOUNT MANAGER SECTOR PÚBLICO, FORCEPOINT

El año 2020 será difícil de olvidar. La pandemia mundial y sus efectos han estresado nuestra sociedad y nos han puesto a prueba como colectivo. Durante el año pasado y lo que llevamos de este, ha quedado patente la criticidad e importancia de los servicios públicos prestados por la Administración a los ciudadanos, servicios que, en la mayoría de los casos y no sólo en los ámbitos de salud, han incrementado sensiblemente su demanda. En esta situación de incremento de demanda, que se ha visto acompañada de la necesidad de disponer de mecanismos de trabajo remoto no previstos para empleados públicos, los servicios y departamentos de TI de los distintos organismos públicos se han visto desbordados y han tenido que adaptar sus arquitecturas, con los medios disponibles en cada momento, para garantizar la continuidad de los servicios públicos digitales.

Las Administraciones Públicas han desarrollado, en mayor o menor medida, durante los últimos años importante procesos de transformación, procesos que han redundado en eficiencia y en mejoras en la forma en la que los ciudadanos se relacionan con la Administración. Sin embargo, tras la situación vivida se pueden sacar varias conclusiones:

* La importancia y criticidad de los servicios públicos deriva en la necesidad de disponer de más y mejores servicios digitales, que no sólo simplifiquen los trámites y la relación de los ciudadanos con la administración, sino que vayan más allá y aprovechen la "nueva" capacitación digital de la población. Adicionalmente, la Administración debe velar accesibilidad a estos servicios, su adopción, su penetración y su mejora continua.
* La Transformación Digital debe producirse en todos los ámbitos de la Administración y debe ser tractora para la transformación interna de procesos, modelos de trabajo, colaboración, sinergias y compartición de información entre Administraciones.
* El valor de la información es vital en esta transformación de cara a la definición de nuevos modelos de servicios. Es fundamental protegerla, en este punto, la Transformación Digital no tiene sentido sin seguridad.

Afortunadamente, nos encontramos en un momento en el que diversas vías de financiación van a redundar en un impulso hacia la digitalización de las Administraciones Públicas y bien dirigidas pueden llevar a la Administración a un siguiente nivel. Para lograr este objetivo, no se dispone una fórmula secreta, pero existen distintos factores claves de éxito. La formación y capacitación en los nuevos servicios digitales tanto a empleados públicos como ciudadanos será clave para la adopción y penetración de estos servicios, lo que redundará en información y métricas que permiti-

“LAS ADMINISTRACIONES PÚBLICAS HAN DESARROLLADO, EN MAYOR O MENOR MEDIDA, DURANTE LOS ÚLTIMOS AÑOS IMPORTANTE PROCESOS DE TRANSFORMACIÓN, PROCESOS QUE HAN REDUNDADO EN EFICIENCIA Y EN MEJORAS EN LA FORMA EN LA QUE LOS CIUDADANOS SE RELACIONAN CON ELLAS”

rán evolucionarlos y mejorarlos con el tiempo. Será necesario habilitar mecanismos de teletrabajo/trabajo flexible que permitan maximizar la productividad de los empleados de la Administración proporcionando a su vez todos los mecanismos necesarios de seguridad y protección de usuarios, servicios e información corporativa. La flexibilidad y adaptabilidad de la tecnología que sustente estos nuevos servicios digitales será fundamental, en la medida que debe permitir acompasar la capacidad con la demanda, así como ofrecer mecanismos de provisión flexibles y escalables. En este punto, las plataformas y servicios en cloud pública serán determinantes. Finalmente, el valor de la tecnología y los servicios profesionales ofrecidos por empresas con capacitación suficiente para abordar proyectos complejos e innovadores será igualmente fundamental, siendo clave que los mecanismos de contratación de la Administración estén alineados con esta búsqueda de valor y respuesta a las necesidades más que a un mero ahorro de costes.

En la medida en que estas nuevas vías de financiación se reciban, se deberían percibir efectos en la digitalización de la Administración a corto, medio y largo plazo. La tecnología y servicios elegidos deben aportar valor en estos tres periodos y deben ser capaces de acompañar a la Administración es su nuevo proceso de transformación digital. ■

ES TIEMPO DE INNOVAR, NO DE IMITAR

FRANCISCO LOVA

DIRECTOR DE SECTOR PÚBLICO DE PEGASYSTEMS

Estaréis de acuerdo conmigo en que el mundo actual no se parece en nada al que conocíamos hace tan solo unos meses. La incertidumbre y la disrupción de los últimos tiempos han afectado a todos los aspectos de nuestras vidas y nuestro trabajo. Por supuesto, las Administraciones Públicas no son ajenas a esta situación.

Las Administraciones Publicas en España se encuentran ante el reto más importante de modernización de los últimos 30 años. Es una situación sin precedentes y para la que todavía no estábamos preparados. La situación excepcional generada por las circunstancias actuales ha puesto de manifiesto la urgencia y necesidad de desarrollar una Administración Pública Digital.

Sin lugar a duda, la digitalización de las Administraciones Públicas impulsará la recuperación de la economía para salir reforzados de la crisis que estamos viviendo, ejerciendo de locomotora que estimule el desarrollo de la actividad empresarial y crecimiento económico, para asegurar la creación de empleo y el bienestar de todos en los próximos años.

Hay que garantizar que toda la sociedad tenga acceso a las oportunidades que brinda la digitalización de los servicios públicos, ofreciendo una experiencia personalizada, fácil de usar y de valor añadido. La innovación debe convertirse en el motor que mejore la experiencia de empresas y ciudadanía en su relación digital con la administración, creando un modelo centrado en el ciudadano que consolide las interacciones entre las diferentes administraciones con las que interactuamos para el desarrollo de nuestras vidas. Será clave apoyarnos en la Inteligencia Artificial para ofrecer servicios públicos más personalizados, cercanos y adecuados a las necesidades individuales, y, por supuesto, simplificar y optimizar los procesos, cara al ciudadano y funcionarios públicos, mediante la automatización de extremo a extremo.

Los modelos de prestación de servicios públicos se han desarrollado durante muchos años bajo un paradigma y enfoque “geográfico” (nacional, regional y local), y centrado en el “producto”. Por tanto, los Sistemas de Información actuales fueron desarrollados para respaldar ese modelo, que en la actualidad no favorece el cambio de paradigma que la situación actual exige.

Es tiempo de innovar, no podemos imitar, no hay de quien copiar. Tenemos que ser valientes y usar tecnologías modernas del siglo XXI, adecuadas para el reto al que nos enfrentamos, y que nos ofrezcan suficientes garantías de éxito.

La tecnología solo es una pieza más del gran rompecabezas de la modernización digital. La verdadera transformación exige contar con personas con visión de futuro capaces de definir una visión compartida, de inspirar a sus equipos y ser un ejemplo de constancia.

Se hace necesario combinar la automatización de procesos digitales e Inteligencia Artificial para mejorar la interacción con los ciudadanos y empresas en tiempo real, reduciendo la complejidad de los procesos de extremo a extremo, asegurando una entrega rápida de servicios digitales, y facilitando la construcción de

“TENEMOS QUE SER VALIENTES Y USAR TECNOLOGÍAS MODERNAS DEL SIGLO XXI, ADECUADAS PARA EL RETO AL QUE NOS ENFRENTAMOS, Y QUE NOS OFREZCAN SUFICIENTES GARANTÍAS DE ÉXITO”

aplicaciones móviles de una manera muy ágil.

Una plataforma de digitalización unificada y moderna no solo debe garantizar que las Administraciones Públicas puedan cumplir eficazmente con sus obligaciones sociales y económicas, sino que también debe servir de base para:

* Mejorar los servicios prestados.
* Simplificar y optimizar los procedimientos administrativos gracias a la digitalización de principio a fin.
* Reducir errores aplicando automatización a tareas repetitivas.
* Incrementar la agilidad para responder a los cambios, cuando aparecen y son necesarios ejecutarlos, pudiendo reutilizar, evolucionar y adaptar los procedimientos a las nuevas circunstancias.
* Garantizar los niveles de rendimiento y escalabilidad necesarios para ofrecer un servicio de calidad.
* Finalmente, como no pude ser de otra manera, sin poner en riesgo aspectos tan importantes como la seguridad jurídica o la transparencia.

La transformación del Sector Público es responsabilidad de todos. Tenemos una excelente oportunidad para hacer las cosas de una forma diferente y ofrecer unos servicios públicos digitales de calidad, que aporten valor real en el desarrollo de nuestras vidas, de una manera eficiente, trasparente, ética y justa.

Organismos públicos a lo largo de todo el mundo ya están en el camino de cambio de paradigma, como es el caso del Departamento de Trabajo y Pensiones en el Reino Unido, que haciendo un uso de la automatización inteligente, ha reducido errores y fraude en la asignación de prestaciones en un 20%, o como el Departamento de Hacienda e Impuestos de Reino Unido, que ha automatizado el 46% de las tareas manuales en su servicio de atención al contribuyente, consiguiendo reducir en tres minutos el tiempo de cada llamada, como el Gobierno de Baviera desarrolló un nuevo servicio digital para gestionar las prestaciones de ayuda urgente por COVID-19 en tan solo cinco días.

¿Vamos a desaprovechar esta oportunidad? ■

Expertos en Advanced Solutions

Seleccionamos e introducimos al mercado las **últimas tecnologías** para ayudar al **canal en el crecimiento** tecnológico y su **transformación digital.**

Ofrecemos desde soporte preventa hasta postventa, incluyendo la transferencia tecnológica y las **instalaciones específicas** de **formación** y testeo de **tecnologías.**

www.v-valley.es

V-Valley

the Value of esprinet

¿LUCHANDO CONTRA EL CIBERDELITO? RECURRE A LA COLABORACIÓN PÚBLICO-PRIVADA

M.K. PALMORE

VICEPRESIDENTE Y DIRECTOR DE SEGURIDAD PARA AMÉRICA EN PALO ALTO NETWORKS Y AGENTE JUBILADO DEL FBI

El ciberdelito es pernicioso. Es global, implacable y está impulsado por ciberdelincuentes ingeniosos. Aprovechan tecnologías como el aprendizaje automático o los kits de explotación económicos adquiridos en la web oscura. Y ahora, una pandemia mundial, el estrés económico y un repunte sin precedentes en el trabajo remoto han creado un entorno lleno de oportunidades para los ciberdelincuentes.

Lo que está en juego nunca ha sido tan grande. La investigación llevada a cabo por Accenture señala que en un solo año, el coste anual promedio del ciberdelito aumentó en un 29% en Estados Unidos, un 30% en Japón, un 26% en Australia y un 31% en el Reino Unido.

Las organizaciones están sufriendo. ¿Cuál es la respuesta? Sí, deberíamos invertir estratégicamente en herramientas y servicios de cibseguridad. También necesitamos más talento en el ámbito de la ciberseguridad. Pero incluso una inversión similar al Plan Marshall para contratar y capacitar a profesionales de la ciberseguridad no salvará ese abismo en años.

En cambio, debemos mirar hacia adelante y anticiparnos, en lugar de simplemente reaccionar ante lo que está sucediendo ahora. El legendario gran jugador de hockey Wayne Gretzky ha explicado muy bien esta estrategia: “Patina hacia donde va el disco, no hacia donde ha estado”.

Desde una perspectiva de ciberseguridad, debemos reconocer que el “disco” está yendo a lugares donde nunca había ido. Ataques de denegación de servicio globales. Ataques de ransomware. Un grupo de adversarios cibernéticos más decidido que nunca, incluidos los ciberterroristas patrocinados por el estado.

Mirar hacia el futuro y armar la defensa de ciberseguridad adecuada requerirá un nivel de colaboración más alto y comprometido. Los profesionales de la seguridad siempre han entendido que luchar contra las amenazas cibernéticas requiere un esfuerzo de equipo, y eso nunca ha sido más cierto que en la actualidad.

EL VALOR DE LAS ASOCIACIONES PÚBLICO-PRIVADAS

Los ciberdelincuentes son inteligentes, actúan rápido y, a menudo, son mucho más sofisticados que nosotros a la hora de aprovechar el poder de la colaboración. Para contrarrestar eso, necesitamos fomentar una alianza más fuerte y profunda entre el sector privado y el sector público, especialmente con los cuerpos de seguridad. Esta asociación público privada es esencial para superar las crecientes amenazas cibernéticas y ayudar a aligerar la carga de trabajo de los cuerpos de seguridad.

Gran parte de esta alianza público-privada conducirá a una mayor inteligencia sobre amenazas, un componente vital en un marco de ciberseguridad eficaz. La mayoría de organizaciones solo pueden obtener una vista de mosaico del panorama de amenazas al ingerir datos de numerosas fuentes y descubrir qué significa todo. Las organizaciones han comenzado a moverse cada vez más hacia la inteligencia artificial y el aprendizaje automático para adoptar un enfoque más automatizado de la inteligencia de amenazas. Pero ni

“ESTA ASOCIACIÓN PÚBLICO PRIVADA ES ESENCIAL PARA SUPERAR LAS CRECIENTES AMENAZAS CIBERNÉTICAS Y AYUDAR A ALIGERAR LA CARGA DE TRABAJO DE LOS CUERPOS DE SEGURIDAD”

las empresas de sector privado ni los organismos públicos de seguridad pueden hacerlo todo por sí mismos.

La asociación entre el sector privado y las fuerzas de orden público puede acelerar la recopilación, el análisis y la actuación de la inteligencia sobre amenazas. En mi anterior carrera como agente de FBI, mi prioridad era llevar a cabo actividades de divulgación con empresas de sector privado por dos razones simples. Primero, ninguna entidad ve el espectro completo de amenazas a la seguridad cibernética; y en segundo lugar, responder a brechas reales puede ser una propuesta aterradora, incluso para organizaciones muy grandes.

UN PANORAMA MÁS AMPLIO

Los organismos encargados de hacer cumplir la ley miran más allá de las fronteras locales e incluso nacionales para obtener una visión general de las actividades, tendencias y resultados. Pueden proporcionar un contexto crítico en torno a las actividades y compartir esta información de forma rutinaria entre sus compañeros en gobiernos amigos. Su inteligencia, las notificaciones y los boletines de la industria privada a menudo permiten que los analistas de ciberseguridad del sector privado mejoren su comprensión de las amenazas.

Y los profesionales de orden público comparten con el sector privado una creencia común y poderosa que guía nuestras acciones: todos queremos detener a los malos.

UNA CULTURA DE COLABORACIÓN

La colaboración entre los sectores público y privado no es nueva, como señalamos anteriormente: “En el mundo en evolución del delito cibernético y la manipulación de datos, la aplicación de la ley puede, y debe, desempeñar un papel fundamental en la prevención de la actividad delictiva”. Pero hoy, esta asociación es más imperativa. Y debe contar con el respaldo no solo de los ejecutivos comerciales, sino también de la alta dirección y la junta.

Las organizaciones del sector público y privado deben aprovechar todos los recursos disponibles, y las asociaciones deben ser una parte estratégica de su compromiso. Por supuesto, debe continuar garantizando el desarrollo y el avance de las capacidades propias de su organización maximizando el uso de tecnologías y técnicas de próxima generación, como el aprendizaje automático. Al mismo tiempo, debe adoptar una “cultura de colaboración” tanto dentro de su organización como con terceros.

Las asociaciones y la colaboración son esenciales en la ciberseguridad. Después de todo, incluso Gretzky, “The Great One”, confió en el talento y el arduo trabajo de sus compañeros de equipo en lugar de intentar anotar únicamente por su cuenta. ■

CIBER-RESILIENCIA: EL FACILITADOR DE LA TRANSFORMACIÓN DIGITAL

OVANES MIKHAYLOV

RESPONSABLE DE DESARROLLO DE NEGOCIO PARA EL SUR DE EUROPA, VMRAY

Al igual que la Transformación Digital crea nuevas oportunidades para las empresas, también crea oportunidades para hackers y ciberdelincuentes. Esto es aún más cierto cuando los procesos empresariales digitales deben ser implementados bajo limitaciones de tiempo y presión competitiva.

A menudo no hay suficiente tiempo para evaluar a fondo los riesgos cibernéticos que vienen con los nuevos procesos y revisar los planes de seguridad existentes. Muchas organizaciones simplemente asumen que las medidas de seguridad existentes seguirán ofreciendo suficiente protección después de todas las inversiones hechas en los últimos años ¿verdad?

Tenemos varias capas de defensa, que consta de firewall, WAF, SEG, Anti-spam, protección contra phishing, soluciones antivirus en los puntos finales, un VPN para acceso remoto... y, a pesar de todo esto, un día descubren que el malware avanzado ha entrado en su red. ¿Cómo puede ser esto?

De hecho, casi todas las organizaciones tienen varias tecnologías que pueden detectar malware, pero en la mayoría de los casos, la detección se basa en métodos de análisis estáticos, utilizando firmas, heurística o búsquedas de reputación para determinar la naturaleza del archivo sospechoso.

Las soluciones de análisis estático mantienen bibliotecas grandes y actualizadas regularmente de identificadores únicos ("huellas digitales") para muestras de malware conocidas. Es una manera eficaz de proteger contra el malware que se ha visto antes, pero no contra malware previamente desconocido, o malware avanzado que cambia sus características reconocibles para evadir la detección. Si aún no hay identificadores disponibles o las "huellas digitales" ya no coinciden, la solución de análisis estático no reconocerá el archivo por lo que realmente es.

LLEVE LA POSTURA DE SEGURIDAD DE LA ORGANIZACIÓN AL SIGUIENTE NIVEL

Las tecnologías Sandboxing añaden capacidades avanzadas de detección de malware y cierran la brecha "desconocida" que deja el análisis de malware estático.

El principio de funcionamiento de un entorno limitado es simple: el entorno aislado es un entorno aislado, que imita un sistema de usuario final o un servidor y permite que el archivo sospechoso se ejecute y realice todas sus operaciones.

Dado que la detección basada en el comportamiento no depende de firmas, heurística o datos de reputación, los entornos sandbox pueden detectar tipos de malware desconocidos y altamente sofisticados como malware evasivo o ataques dirigidos.

Por lo tanto, las tecnologías de sandbox desempeñan un papel importante en los conceptos maduros de ciberseguridad, pero no todos los sandboxes son iguales, y no todos los sandboxes cumplen con las expectativas de los equipos de seguridad.

CRITERIOS A CONSIDERAR

* **Alta resistencia a la evasión**. Las técnicas de evasión son omnipresentes en malware avanzado. Las amenazas están diseñadas para recono-

"LAS ORGANIZACIONES DEBEN ENFRENTARSE A LA TAREA DE TRANSFORMACIÓN DIGITAL O ARRIESGARSE A UNA GRAVE DESVENTAJA COMPETITIVA. LA TRANSFORMACIÓN DIGITAL, SIN EMBARGO, REQUIERE DE FUERTES DEFENSAS CIBERNÉTICAS"

cer cuándo se ejecutan dentro de un entorno de análisis y tomarán medidas evasivas para evitar ser detectadas. Para contrarrestar estas técnicas de evasión, es fundamental que los equipos de seguridad se aseguren de que utilizan entornos de análisis que replican con precisión con todo detalle los entornos reales de escritorio y servidor que están protegiendo. Es importante tener atributos pseudoaleatorios como parte del entorno de análisis de destino. Los entornos limitados genéricos que ejecutan entornos de destino estándar idénticos ya no son suficientes. Además, el entorno de análisis debe ser capaz de detectar consultas de entorno e identificar ramas de código oculto.

* **Ruido y falsos positivos.** Muchas soluciones de espacio aislado ofrecen resultados de análisis que contienen una gran cantidad de ruido de fondo irrelevante. Esto diluye y oscurece la información crítica en la que confían los equipos de seguridad para optimizar la respuesta a incidentes y desencadenar acciones de mitigación. El análisis solo debe capturar señales que sean relevantes para resolver la amenaza, y los informes deben proporcionar resultados inmediatamente procesables legibles por humanos, así como resultados fiables legibles por máquina que se pueden compartir con otros sistemas de seguridad en el entorno de la organización.

* **Automatización de procesos de análisis.** Las capacidades de automatización son un criterio importante, especialmente cuando los recursos del personal son limitados. La necesidad de intervención humana durante el proceso de detección y análisis debe eliminarse siempre que sea posible. La solución de espacio aislado debe tener una amplia gama de conectores para facilitar la integración con otras soluciones de seguridad. Los resultados del análisis y la inteligencia de amenazas se pueden compartir en todo el entorno de seguridad, aumentando la eficacia de los sistemas que ya están en marcha y protegiendo las inversiones existentes.

* **Soporte para requisitos de cumplimiento.** Esto es importante en industrias reguladas como la atención médica, las finanzas y el gobierno que están obligadas por la regulación del RGPD y otros requisitos de cumplimiento a tener control sobre dónde residen sus datos. Al decidir por una solución de espacio aislado basada en la nube, las organizaciones deben asegurarse de que se utilizan centros de datos dentro de la unión europea.

ES NECESARIO ACTUAR

Las organizaciones del Sector Público y Privado siguen impulsando la Transformación Digital, a menudo a un ritmo acelerado debido a las crisis de COVID. Pero a menudo permanecen inactivos cuando se trata de evolucionar sus conceptos de seguridad existentes para proporcionar el nivel de protección requerido para proteger sus nuevos procesos de negocio digitales. Especialmente las organizaciones que tienen información de identificación personal (PII) o información personal sensible (SPI) están cada vez más dirigidas a sofisticados ciberataques. Sin capacidades avanzadas de detección de malware en su lugar, sólo será cuestión de tiempo hasta que se produzca una infracción. ■

LA ADMINISTRACIÓN PÚBLICA, MODELO Y ELEMENTO TRACTOR DE LA SOCIEDAD

LEONOR TORRES MORENO

VICEPRESIDENTA DE ASTIC

Seguimos inmersos en una pandemia que nos ha cambiado para siempre; gracias a los avances científicos en el desarrollo de vacunas hemos conseguido descender los contagios y los fallecidos, y ya vislumbramos la luz al final del túnel.

La pandemia, como cualquier crisis, nos ha brindado nuevas oportunidades; gracias a ella hemos asistido a un despliegue tecnológico sin precedentes: hemos conseguido mantener activos los servicios, las clases online, el ocio y, especialmente, el contacto con nuestros seres queridos. Y aunque los trámites electrónicos y el comercio online han incrementado su uso, también esto ha hecho más evidente la brecha digital aún latente.

Me preguntaban el otro día si los avances tecnológicos seguirían produciéndose sin cesar o había posibilidades de que pararan o se estancaran. A pesar de no tener dotes de adivina, me cuesta creer que se vaya a ralentizar; todo apunta a lo contrario, pienso que los avances tecnológicos y científicos son imparables.

Es precisamente este hecho el que revela la relevancia de aprovechar el momento histórico en el que nos encontramos. Con el Plan de Recuperación, Transformación y Resiliencia tenemos una oportunidad única de mejorar nuestro país, de obtener recursos que nos permitan realizar transformaciones estructurales que nos faciliten seguir avanzando, adaptarnos a un mundo cada vez más globalizado y ágil. Realizando un uso adecuado de las tecnologías conseguiremos no sólo un mundo más sostenible e inclusivo sino también una economía más productiva.

El reto es extraordinario, tendremos que mejorar el actual modelo de gobernanza, coordinarnos mejor, conseguir dotarnos de mayor agilidad y eficiencia para conseguir aprovechar con éxtio las oportunidades que se nos brindan.

La Administración Pública tiene que servir de modelo y ser un elemento tractor de la sociedad. Debe seguir trabajando en su modernización, en la simplificación de sus estructuras y procedimientos y, especialmente, por un acercamiento más próximo a la ciudadanía. No olvidemos que la Administración debe atender todas y cada una de las necesidades, si cabe debe prestar mayor atención a quien más lo necesita (los colectivos más vulnerables, las personas mayores, las víctimas de cualquier tipo de violencia...).

La Administración no puede cerrar sus puertas escudándose en herramientas tecnológicas; debe estar abierta a todos, debe informar adecuadamente para que cualquier persona consiga realizar los trámites que necesite sin ayuda externa.

Los profesionales TIC de la Administración llevamos trabajando años en la digitalización de procesos, hemos hecho un buen trabajo, y los datos dan prueba de ello. Somos líderes en Europa, así lo evidencia el índice DESI 2020, hemos conseguido un segundo puesto en materia de servicios públicos digitales, nuestra posición global es también relevante, alcanzado el séptimo puesto en el índice de gobierno digital de la OCDE. Tenemos que estar muy orgullosos de estos logros, así como de haber conseguido mantener la continuidad de los servicios en este último año, sin por ello caer en la autocomplacencia pues es mucho aún

“TENEMOS QUE ESTAR MUY ORGULLOSOS DE NUESTROS LOGROS, PERO NO CAER EN LA AUTOCOMPLACENCIA. ES MUCHO EL CAMBIO QUE NOS QUEDA POR RECORRER PARA CONSEGUIR UNA ADMINISTRACIÓN CAPAZ DE ATENDER LAS NECESIDADES DE UNA SOCIEDAD COMPLEJA Y PLURAL”

el cambio que nos queda por recorrer para conseguir una Administración capaz de atender las necesidades de una sociedad compleja y plural.

Es cierto que “cuesta ser profeta en tu tierra” y que en España se tiende a rebajar los aciertos y agrandar las torpezas, pero debemos cambiar este modelo que nos perjudica como colectivo y como país, porque hacemos cosas muy bien que debemos apoyar y aplaudir y, aquellas otras mejorables deben ser revisadas bajo una mirada crítica constructiva, que siempre será agradecida y bien recibida; lo importante es aprender de los errores y colaborar para mejorar la coordinación, la gobernanza y lograr una Administración más moderna y eficiente.

Contamos con nuevos recursos que nos provisionarán los fondos NextGenerationEU, que nos permitirán reparar los daños económicos producidos por la pandemia. Se trata de un gran desafío, con un marco temporal bien definido y unos objetivos aún por terminar de precisar, una oportunidad histórica que no debe malgastarse. Alcanzar los objetivos implica impulsar un gran número de proyectos que necesitarán licitación ágil que debe enfrentar y superar dos grandes desafíos: agilizar la contratación en primer lugar (posiblemente la reducción de plazos no sea suficiente), y que las unidades TIC dispongan de efectivos suficientes para realizar el adecuado control y seguimiento de estos proyectos.

En el RD 36/2020 se han adoptado ya una serie de medidas interesantes enfocadas a reducir los plazos para agilizar el procedimiento de contratación. Pero necesitamos ir más allá, simplificar la preparación y fases previas de la contratación dotando el proceso de mayor flexibilidad a la vez que se garantiza la legalidad, para cumplir los objetivos en plazo.

No estamos acostumbrados a otras fórmulas de colaboración con el sector privado, socios fundamentales e imprescindibles que nos deben acompañar en este desafío. Es necesario explorar nuevos modelos, quizá podemos tomar ejemplo de las sociedades mixtas o los consorcios. Este hecho se une, además, al insuficiente número de recursos humanos que puedan gestionar los contratos a la vez que controlar y coordinar los proyectos. Actualmente, los departamentos se encuentran superados con la tramitación habitual y una carga mayor va a suponer un tremendo esfuerzo que irá en detrimento inevitablemente de la calidad del servicio.

En relación al modelo de selección, el cuerpo TIC presenta un modelo excepcional en el ámbito de la función pública, combinando pruebas de conocimiento y resolución de problemas sin dar preponderancia a las pruebas memorísticas. A nuestro juicio, el proceso selectivo es a priori adecuado, no obstante, conviene acortar los plazos de incorporación de los nuevos efectivos para facilitar su incorporación ágil a las unidades, necesitamos consiguir equilibrar el número de profesionales con la carga real de trabajo de cada departamento, y siendo aún más ambiciosos, deberíamos pensar en dotar a las unidades de suficientes recursos y tiempo para potenciar la innovación al objeto de evitar dependencias de monopolios extranjeros.

Desde ASTIC, Asociación Profesional de Cuerpos Superiores de Sistemas y Tecnologías de la Información de las Administraciones Públicas, estamos colaborando activamente con función pública para dar a conocer nuestros

“HAY QUE SUPERAR DOS GRANDES DESAFÍOS: AGILIZAR LA CONTRATACIÓN Y QUE LAS UNIDADES TIC DISPONGAN DE EFECTIVOS SUFICIENTES PARA REALIZAR EL ADECUADO CONTROL Y SEGUIMIENTO DE LOS PROYECTOS”

proyectos y hacer más atractiva la carrera administrativa a los y las jóvenes. Conviene comunicar de una forma más activa para conseguir captar más talento, sobre todo femenino, ya que la mujer sigue estando infrarrepresentada en el ámbito de la tecnología, especialmente en la Administración Pública, lo que incide negativamente en su acercamiento a la sociedad a la que presta sus servicios.

Si hablamos de sueldos, claramente no podemos competir con el mercado actual, las “startup” ofrecen condiciones salariales que claramente aventajan a la Administración, no obstante, la transcendencia de los proyectos desarrollados por las Administraciones públicas y su impacto directo en la sociedad, sí pueden ser un elemento atractivo, además de otras ventajas como las posibilidades de conciliación de la vida laboral y personal. El teletrabajo debería convertirse en una apuesta decidida por parte de las Administraciones públicas, permitir incorporar talento de cualquier región de España e incluso ser parte de la solución al problema de la España vaciada, dado que gozamos de una calidad y capacidad de penetración en nuestras infraestructuras de comunicaciones muy superior a otros países europeos.

El teletrabajo ha incrementado la superficie de exposición y nos ha hecho temporalmente más vulnerables. Afortunadamente, contamos con grandes profesionales que han sabido protegernos a pesar de los aún escasos medios disponibles en esta área, tanto en recursos humanos como en créditos presupuestarios; necesitamos continuar avanzado en la concienciación y en la mejora de las soluciones para evitar y minimizar los efectos negativos de los ataques que resultan cada vez más complejos.

La ciudadanía debe sentirse segura en su relación con la Administración, y en eso hay que seguir trabajando.

Contamos con una regulación en privacidad muy avanzada en Europa, que nos garantiza el respeto a decidir sobre el destino y uso de nuestros datos personales, debemos dotarnos de herramientas y profesionales suficientes para garantizar este derecho a todos los ciudadanos y, por supuesto, a los empleados públicos. Los principios de la protección de datos desde el diseño y por defecto deben ser nuestra prioridad, el adecuado uso de las tecnologías disruptivas respetando nuestros derechos está en juego.

Para mejorar la interacción con el ciudadano tenemos que buscar soluciones holísticas que proporcionen el gobierno del dato e ir incorporando los procedimientos necesarios para asegurar su calidad y aportación de valor.

Por último, insistir en la necesidad de innovación apoyando el uso ético de las tecnologías disruptivas bajo el prisma de nuestra cultura europea, apuesta imprescindible para posibilitar nuevos enfoques y soluciones. La alta carga de trabajo actual dadas las exiguas plantillas de empleados públicos técnicos de tecnologías de la información y comunicaciones, anteriormente mencionada, hacen prácticamente inviable esta tarea que se va postergando “sine die”; sin embargo, es prioritario disponer de recursos humanos con tiempo destinado a la innovación, fomentar un modelo de gobernanza que permita compartir las experiencias y posibilitar la reutilización de todas aquellas que supongan una ventaja clara tanto para la Administración como para la sociedad. ■

Foro Administración Digital 2021

Nuevos impulsos para la evolución de la Administración digital

PLAY

Disponible bajo demanda

Organiza

it Digital MEDIA GROUP

Socios estratégicos

Astic

Ford CPP colaboración público-privada TECNOLOGÍA & INNOVACIÓN

Patrocinador Platinum

salesforce

Patrocinadores Gold

aruba a Hewlett Packard Enterprise company

Forcepoint

MicroStrategy

PEGA

paloalto NETWORKS

VMRAY

V-Valley the Value of esprinet

Patrocinadores Silver

Bitdefender

CYTOMIC a WatchGuard brand

SOPHOS Cybersecurity evolved.

THALES

¿Están seguros tus datos de Salesforce?

Con un incremento del cibercrimen del 400%, según el FBI, y las amenazas internas que acechan a los sistemas corporativos (el error humano está detrás del 47% de las pérdidas de datos), proteger los entornos de datos que se generan con las aplicaciones SaaS debe ser una de las principales líneas a contemplar en un plan de recuperación.

Salesforce es el principal proveedor de software CRM del mercado, según IDC. Muchas compañías confían en esta solución de software como servicio para gestionar los datos de sus clientes y las nuevas oportunidades de negocio, convirtiendo esta suite en un activo crítico.

Por su preciado valor, las aplicaciones Salesforce se han convertido en uno de los objetivos de los ciberdelincuentes, que ven en estos sistemas un jugoso conjunto de datos al que sacar partido de no muy lícitas maneras.

Pero los riesgos no solo proceden de fuera. La gran mayoría de pérdidas de datos se producen por el borrado que hace el usuario final

o por errores de los empleados. Otras causas son acciones malintencionadas, como las que perpetran los hackers o trabajadores disgustados con la empresa, y errores de las propias aplicaciones. Las soluciones SaaS, como Salesforce, suelen tener servicios de recuperación nativos, pero dada la criticidad de los datos que contienen, es responsabilidad de los usuarios de Salesforce mantener a salvo esta información. Recurrir a productos de terceros para mejorar la protección de estos datos y recuperarlos, de manera automática, en caso de eliminación, corrupción o ataque, es una estrategia totalmente validada en el mercado.

Para dar una mayor protección a los entornos Salesforce, Commvault acaba de anunciar Metallic™ Salesforce Backup, una solución de copia de seguridad y recuperación para toda la suite de soluciones que incluye Salesforce Cloud.

Es una solución sencilla, que ofrece copias de seguridad 100% automatizadas y de alto rendimiento. Metallic™ Salesforce Backup de Commvault ofrece controles dedicados para salvaguardar los datos generados en el contexto Salesforce, ya sea contenido, archivos, perfiles, metadatos...

La seguridad de esta solución está reforzada con múltiples capas, como autenticación multifactorial, cifrado de datos avanzado y controles de acceso de usuarios de confianza cero, para evitar el acceso injustificado a los sistemas y datos.

"En Omega Peripherals somos conscientes del crecimiento exponencial de datos en el cloud y de su vulnerabilidad ante ataques de seguridad y ransomware. Por ello, apostamos por soluciones como Metallic, que aseguran la protección de datos críticos de forma simple, rápida y flexible", explica Javier Fernández, Chief Sales and Marketing Officer de Omega Peripherals, Partner Premier de Commvault. ■

Los ingresos de las empresas de servicios TIC siguen cayendo

La última edición del barómetro TIC Monitor, correspondiente al mes de febrero, vuelve a constatar la contracción de los ingresos de las empresas del sector TIC. En esta ocasión calcula que se ha producido una caída de la actividad del 9,4% en términos interanuales. Sin embargo, no ha mermado su capacidad de crear empleo ni el optimismo de las compañías de volver a crecer entre mayo y julio.

De acuerdo con los datos de febrero de este estudio que realizan todos los meses VASS y CEPREDE, el Centro de Predicción Económica, los ingresos de las empresas de servicios TIC se han contraído interanualmente un 9,5%, siguiendo la tendencia del año pasado, que concluyó con una caída de la actividad del 6,1%.

Sin embargo, el empleo resiste, y a que han sido capaces de crear nuevos puestos de trabajo y, entre los meses de febrero de 2020 y 2021, se ha producido un aumento del 0,5% en las contrataciones. Aunque el crecimiento es plano, las compañías TIC siguen distanciándose del sector servicios en su conjunto, que registró una caída del 5% en el mismo periodo.

Eso sí, como indica Antonio Rueda, director de VASS Research y responsable de TIC Monitor, “la merma de actividad ha derivado en una

caída interanual de la productividad por empleado del 9,8%".

Uno de los principales motivos por los que el sector de servicios TIC ha evitado la destrucción de puestos de trabajo es la previsión de crecimiento. En este sentido, a pesar del complicado inicio de año, los indicadores de clima mantienen un tono positivo.

A tres meses vista, los datos, tanto en España como en la Unión Europea, demuestran confianza en una recuperación progresiva que se espera concretar entre mayo y julio. Así lo piensan el 74,3% de los empresarios del sector se muestra optimista frente al 25,7% que percibe un empeoramiento en la facturación.

Asimismo, las expectativas de creación de empleo, aunque empeoran respecto al anterior registro (cuando marcaban +38,1 puntos), consiguen mantenerse en el terreno positivo con +12,3 puntos en una escala de +/-100. El balance de optimistas y pesimistas se decanta a favor de los primeros, y un 56,2% de las compañías espera una creación neta de puestos de trabajo entre mayo y julio.

Según Rueda, "otra razón por la cual las empresas se resisten a despedir es la escasez de profesionales para abordar la recuperación. Entre 2011 y 2019 España es, tras Italia, el país (entre los grandes de Europa) donde menos ha crecido el número de perfiles técnicos, lo cual contrasta con una demanda potente y sostenida: en los últimos cinco años, se han creado en España 195.000 empleos de especialistas TIC".

LA PANDEMIA ESTABILIZA LOS SALARIOS EN EL SECTOR TIC

La crisis económica ha hecho que los salarios en el sector TIC se estabilicen y, a la vez, se reduzca la brecha laboral en las TIC. Al respecto, Julien Mur, Senior Manager del área Information Technology, Digital e eCommerce en HAYS España, subraya que "es la primera vez en los últimos seis años que se estabiliza el aumento de los salarios en TI, debido principalmente a que hay un ligero aumento del pool de candidatos disponibles". Sin embargo, la realidad es que esta situación no es suficiente como para dejar de ser un mercado liderado por el candidato, es decir, que "sigue habiendo dificultades para reclutar perfiles de TI", señala.

En este sentido, "la crisis de la covid-19 no ha cambiado mucho el comportamiento global del mercado laboral de TI en España, y uno de los principales problemas sigue siendo la brecha entre la oferta y la demanda de candidatos, aunque ha dejado de crecer", reconoce Mur. Los datos de la Guía HAYS 2021 corroboran esta brecha ya

que al 72% de los empresarios les cuesta encontrar perfiles cualificados para determinadas posiciones y el 69% de los profesionales de telecomunicaciones valora y está dispuesto a trabajar en el extranjero.

BUENAS PERSPECTIVAS DE CONTRATACIÓN

A pesar de la pandemia, las perspectivas para las telecos y las TIC a corto y medio plazo son esperanzadoras ya que prácticamente el 79% empresas del sector tienen intención de contratar este año, según datos de la Guía HAYS 2021. En concreto, estas contrataciones van a suponer una subida respecto a las del año anterior en el 58% de los casos, se mantienen en el 35% y solo bajan en un 6% de las empresas.

En comparación con otras áreas de actividad económica, el sector de las Telecomunicaciones y la Sociedad de la Información es de los que presenta mejores perspectivas de crecimiento. El 60% de los empresarios encuestados para la Guía HAYS 2021 opinan que las TIC e Internet son el sector que tendrá más oportunidades de empleo en los próximos años, seguido de las Telecomunicaciones (44%, seis puntos porcentuales si se compara con los resultados del mismo estudio en 2020).

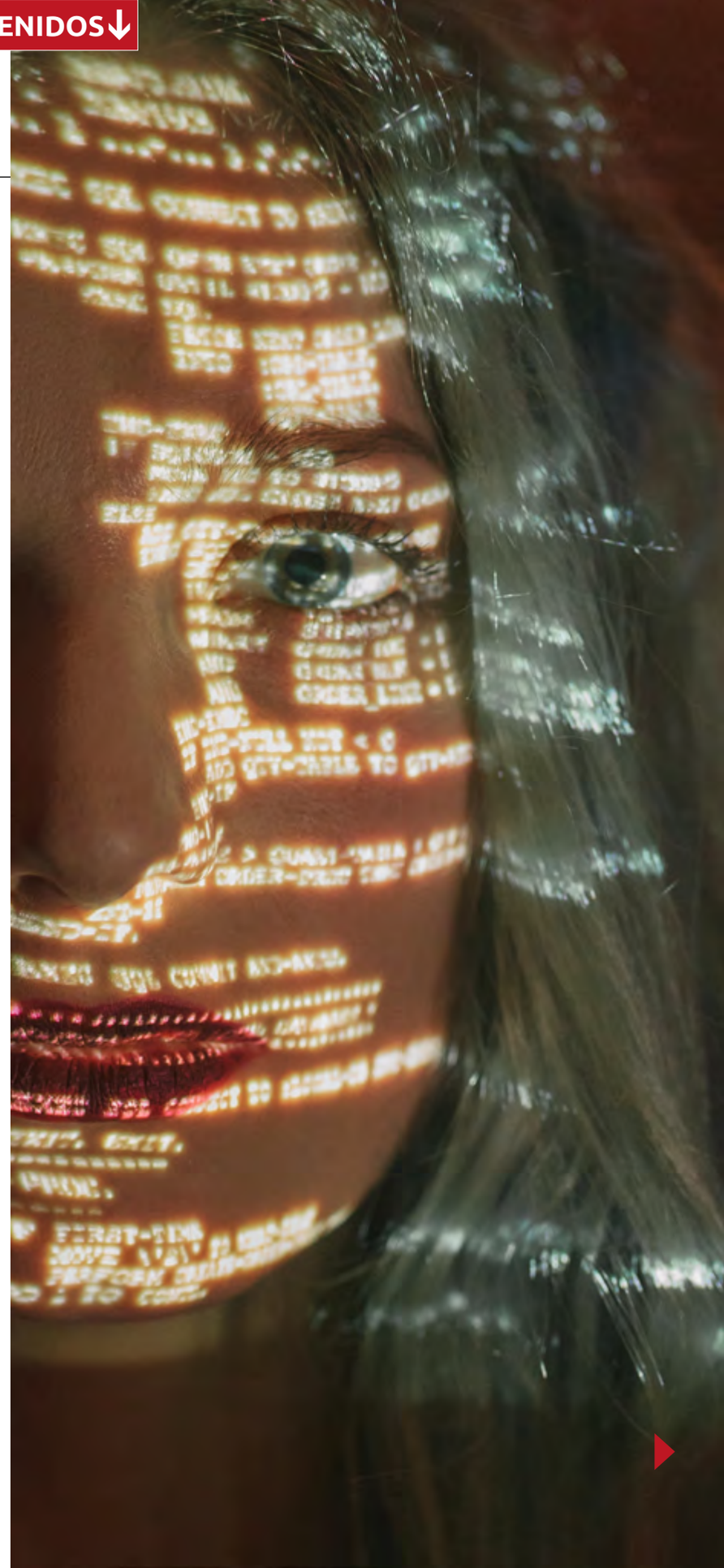
Por tipo de perfiles, el 84% de las empresas del sector requiere informáticos y especialistas en TIC, seguidos de Ingenieros (31%) y comerciales y ventas (28%). "Los perfiles especializados en datos son cada vez más necesarios para las empresas y se espera un gran boom en la demanda de estos profesionales, y esta es la razón por la que los ingenieros y científicos de datos son los únicos perfiles del sector que han observado un aumento de los salarios", explica Mur. ■

Se ha producido una caída de la actividad del 9,4% en términos interanuales. Sin embargo, no ha mermado su capacidad de crear empleo ni el optimismo de las compañías de volver a crecer entre mayo y julio

MÁS INFORMACIÓN

- TIC Monitor Mayo 2021
- Guía Hays 2021

Dos tercios de las empresas no están preparadas para afrontar un ciberataque



El panorama de amenazas es cada día más complejo y los responsables de seguridad de las organizaciones son conscientes del riesgo de ser atacadas. Según un estudio de Proofpoint, el 66% considera que su organización no está preparada para hacer frente a un ciberataque.

A tenor de los resultados de su informe 'Voice of the CISO', Proofpoint opina que el modelo de teletrabajo instaurado durante la pandemia ha puesto a prueba a los responsables de seguridad de la información como nunca se había visto. A un nivel general, dos tercios de los encuestados piensan que su organización no está preparada para hacer frente a un ciberataque y el 58% opina que su mayor vulnerabilidad en ciberseguridad está en el error humano.

El estudio se centra en tres áreas clave como son el riesgo de amenazas y los tipos de ciberataques con los que los CISO se encuentran a diario, la preparación de los empleados y de la organización para hacerles frente, así como el impacto de mantener un modelo de trabajo híbrido a medida que las empresas preparan su vuelta a la oficina. Asimismo, el informe repara en los distintos desafíos que puede haber en las funciones de los CISO, su posicionamiento dentro de la directiva de las organizaciones y las expectativas empresariales de sus equipos.

RESULTADOS EN ESPAÑA

En función de las respuestas de los CISO españoles, se concluye que el panorama de amenazas está siendo implacable y de ahí que la mitad de ellos se sienta en riesgo de sufrir un ciberataque material, es decir, que tenga impacto en su organización, durante los próximos doce meses. Al preguntarles por los tipos de ataques a los que

tendrán que enfrentarse, estos señalaron el compromiso del correo electrónico corporativo o Business Email Compromise (25%), el phishing (24%) y el compromiso de cuentas cloud en O365 o G suite (22%) como los más probables, junto con las amenazas internas y el ransomware (ambos con un 19%). No obstante, un dato sorprendente del estudio es que un 12% de los encuestados españoles fue incapaz de predecir cuáles serán las mayores amenazas de ciberseguridad que se avecinan por la incertidumbre de la pandemia, siendo este el porcentaje más elevado de la encuesta global.

Algo que les inquieta es la preparación de las empresas en este ámbito. Más de un año después de que la pandemia cambiase para siempre el panorama de amenazas, el 53% de los CISO españoles siente que su organización no está preparada para afrontar a un ciberataque dirigido en 2021. Mientras, el riesgo en ciberseguridad va en aumento y un 62% está más preocupado por las repercusiones que pueda tener un ciberataque este año que en 2020.

Además, pese a que el 58% de los encuestados piensa que los empleados entienden su papel a la hora de proteger la empresa frente a ciberamenazas, el 68% sigue considerando el error humano como la mayor vulnerabilidad en ciberseguridad de su organización. La filtración de datos de forma deliberada (amenaza interna maliciosa), hacer clic en enlaces maliciosos, descargar archivos comprometidos, así como reutilizar o no cambiar contraseñas son los comportamientos que aumentan el riesgo de ataque en las organizaciones.

El 63% de los encuestados coincide en que el trabajo en remoto ha hecho que su organización sea más vulnerable frente a ciberamenazas, con un 56% afirmando haber visto un aumento de los ciberataques dirigidos en los últimos doce meses.

Por otro lado, están convencidos que el panorama empeorará y, de acuerdo con el 61% de los participantes españoles en el estudio, el cibercrimen pasará a resultar más rentable para los atacantes.

En su mente está la adaptación de su estrategia de ciberseguridad y tienen la expectativa de que los presupuestos de ciberseguridad aumenten un 11% o más en los próximos dos años. Entre sus prioridades en este plazo está incrementar la concienciación sobre seguridad de los empleados (29%), perfeccionar también los controles de seguridad básicos (28%), así como consolidar las soluciones y controles de seguridad existentes (25%).

Por último, en 2020 la figura del CISO pasó a ser más relevante, pero también hubo mayor expectación dentro de la organización. El 52% de los encuestados en España califica las expectativas en torno a sus funciones como excesivas. Según el estudio de Proofpoint, persiste asimismo entre los CISO una sensación de falta de apoyo por parte de otros directivos, ya que solo un 22% afirma rotundamente que la junta directiva de su organización está alineada con ellos en cuestiones de ciberseguridad.

En esta primera edición del estudio se han analizado los resultados de una encuesta realizada por terceros en el primer trimestre de 2021 a

más de 1.400 CISO de organizaciones medianas y grandes de diferentes sectores. En concreto se ha entrevistado a un centenar de CISO en cada uno de los siguientes mercados: Estados Unidos, Canadá, Reino Unido, Francia, Alemania, Italia, España, Suecia, Países Bajos, Emiratos Árabes Unidos, Arabia Saudí, Australia, Japón y Singapur.

LAS ORGANIZACIONES AUMENTAN EL GASTO EN SEGURIDAD Y GESTIÓN DE RIESGOS

La implantación masiva del teletrabajo y de servicios en la nube pública fue clave para superar lo peor de la crisis el año pasado, pero las organizaciones se vieron forzadas a hacerlo de forma rápida y, en muchos casos, apresurada. Esto implica un gran aumento de riesgos en materia de seguridad informática, ya que al ampliar la superficie expuesta sin incluir adecuadamente estos entornos en la estrategia de ciberseguridad aumenta exponencialmente el riesgo de intrusiones, robo de datos y otras amenazas cibernéticas.

Según Gartner, para paliar estos riesgos las organizaciones aumentaron el gasto en seguridad y gestión de riesgos en un 6,4% en 2020, pero no es suficiente para hacerse cargo del aumento de amenazas. Por ello, se espera que las organizaciones incrementen el gasto mundial en un 12,4% este año, una cifra que podría alcanzar los 150.400 millones de dólares. Según los expertos, esto refleja la gran necesidad de tecnologías de seguridad para los trabajadores remotos y los entornos de la nube.

Para Lawrence Pingree, vicepresidente administrativo de investigación de Gartner, "las organizaciones continúan lidiando con las demandas regulatorias y de seguridad de la nube pública y el software como servicio. De cara al futuro, estamos viendo las primeras señales del mercado de una creciente automatización y una mayor adopción de tecnologías de aprendizaje automático en apoyo de la seguridad de la IA. Para combatir los ataques, las organizaciones ampliarán y estandarizarán las actividades de respuesta y detección de amenazas".

Como muestran los resultados de la última encuesta realizada por Gartner este año, la ciberseguridad se ha convertido en la principal prioridad de gasto para el 61% de los CIO, lo que les ha llevado a aumentar la inversión en seguridad cibernética y de la información en 2021. La categoría más grande de gasto será la de servicios de consultoría, soporte de hardware, implementación y servicios subcontratados, que sumarán casi 72.500 millones de dólares. Mientras tanto, el segmento más pequeño será el de seguridad en la nube, pero a la vez será el que más rápidamente crecerá este año, especialmente los agentes de seguridad de acceso a la nube (CASB).

Pingree explica que "el ritmo de las consultas de los clientes indica que CASB es una opción popular para las organizaciones que utilizan la nube. Esto se debe a la creciente popularidad del uso de dispositivos que no son PC para interactuar con los procesos comerciales centrales, lo que crea riesgos de seguridad que pueden mitigarse de manera efectiva con un CASB. Los CASB también permiten una interacción más segura entre las aplicaciones SaaS y los dispositivos no administrados".

Otra categoría que está creciendo con fuerza a raíz de la pandemia es la de tecnología de gestión integrada de riesgos (IRM), que según los expertos este año crecerá a una tasa de dos dígitos. Como explica John A. Wheeler, director sénior de investigación de Gartner, "las áreas de riesgo significativo que impulsan la demanda a corto plazo incluyen la llegada de nuevos productos y servicios digitales y los usos relacionados con la salud y la seguridad, así como los riesgos de terceros, por ejemplo, violaciones de datos de clientes o ataques a la cadena de suministro". ■

MÁS INFORMACIÓN

- The voice of CISO 2021
- 14 predicciones de seguridad para 2021, según Forbes

El mercado de impresión ha experimentado una profunda transformación ayudando a las empresas en sus procesos de digitalización.

¡Descubra en nuestro

Centro de Recursos it User

cómo está evolucionando un sector clave en la Transformación Digital!

ImpresiÓN Digital

Con la colaboración de: brother

Los directores financieros necesitan acelerar la adopción de la IA

En los próximos años la inteligencia artificial se habrá convertido en una parte fundamental de las tecnologías empleadas en las finanzas, pro actualmente muchos CFO no han progresado mucho en su adopción. Por ello, los expertos de Gartner recomiendan que aceleren sus planes para que su organización no pierda competitividad en un mundo de negocios cada vez más digitalizados.

Para los expertos en finanzas está claro que la inteligencia artificial es una de las tecnologías más disruptivas que llegan a su sector, pero muchas empresas están siendo tímidas en su estudio y en su adopción. Según una encuesta realizada por Gartner, la irrupción de la pandemia generó un impulso de aceleración en los proyectos de IA para los departamentos financieros de las empresas, y un 90% de los entrevistados afirmaba que seguirían invirtiendo en esta tecnología, aunque algunos menos de lo que lo estaban haciendo.

A día de hoy la situación no parece haber mejorado mucho, y los expertos de la consultora alertan de que los directores financieros deberían invertir más en IA en los próximos años, para acelerar la llegada de los beneficios que aporta esta tecnología y anticiparse a sus competidores. En palabras de Clement Christensen, director de la práctica de finanzas de Gartner, "no hay nada de malo en usar IA para modernizar la función financiera. Es un trabajo muy importante. Sin embargo, las recompensas más impresionantes de la IA recaerán en los directores financieros que piensan más en profundidad sobre cómo la tecnología puede cambiar fundamentalmente la forma en que su empresa hace negocios".

Por ello, afirma que la principal prioridad que deberían tener los CFO de las empresas para prepararse ante lo que viene es mejorar la arquitectura de datos de la organización para respaldar los futuros proyectos de IA. Además, invertir en científicos de datos especializados en los datos de los ciudadanos, lo que les permitirá escalar rápidamente sus proyectos de IA cuando se demuestre el éxito de los primeros

proyectos piloto. Y, finalmente, aconseja rediseñar el conjunto de informes de la organización para que se alinee mejora con las necesidades internas del cliente, en lugar de seguir centrados en las tareas financieras tradicionales.

Christensen cree que los directores financieros son conscientes de la necesidad de implementar proyectos de tecnologías digitales más avanzados y experimentales para alcanzar sus objetivos de transformación digital. Pero dice que, a pesar de ello, "siguen enfoques centrados en casos de uso para proyectos de IA que tienden a tener un sesgo hacia la modernización y mejora de procesos familiares, con el objetivo de impulsar ganancias de ROI fácilmente cuantificables", y esto no siempre es la mejor forma de enfocar la implementación de una tecnología de tanto impacto a medio y largo plazo como la IA.

Pone como ejemplo el uso del aprendizaje automático para anticipar los clientes que serán más propensos al impago, para emitir recordatorios de pago anticipado, y para perseguir a los morosos de forma automática. Esto tiene un retorno claro y medible, pero lo único que se consigue es hacer de forma automática algo que ya se podía hacer, lo que significa desaprovechar las enormes capacidades que tiene la IA para generar modelos y obtener mucha más inteligencia y datos para apoyar la toma de decisiones en áreas financieras más vitales para el negocio.

Para Gartner, un ejemplo de lo que sería usar la inteligencia artificial para algo realmente transformador sería aplicarla para identificar a los que probablemente paguen más tarde en la etapa de ventas, lo que permite elaborar proyecciones de ventas en base a cuál es más probable que pague con rapidez. Esto permite transformar el enfoque de la empresa para reducir el volumen de los pagos atrasados y mejorar el flujo de efectivo a mismo tiempo que se reduce la necesidad de perseguir a los morosos en el futuro. Y esto, a su vez, reduce el tiempo dedicado a estas tareas para dedicarse a otras de mayor valor.

Christensen explica que "la opción transformadora no tiene un ROI inmediatamente medible, como la opción de modernización, pero la recompensa final es potencialmente mucho mayor". Así, aconseja a los directores financieros que empiecen aplicando la inteligencia artificial a un problema que necesita solución, y no a uno que solo necesita una modernización de los procesos. Concluye su informe diciendo que "un pequeño cambio de mentalidad en la forma en que los directores financieros piensan sobre la implementación de IA puede marcar la diferencia entre un proyecto que moderniza una empresa y un proyecto que la transforma, que es donde residen las mayores ventajas competitivas".

LOS DEPARTAMENTOS DE FINANZAS NECESITAN REPLANTEAR SU INVERSIÓN EN ANALÍTICA

La analítica de datos es una tecnología fundamental para las finanzas en la era digital, y los líderes de la industria han actualizado sus capacidades y han invertido mucho en herra-

mientas de análisis en los últimos años. A raíz de la pandemia las capacidades digitales y de análisis han cobrado aún más importancia para las organizaciones, por lo que los líderes de los departamentos financieros se preparan para incrementar sus inversiones en análisis. Pero, según los expertos de Gartner, se arriesgan a hacer gastos innecesarios en tecnología que ya se está usando en la organización.

Esto podría suceder porque en muchos casos los lideres financieros pretenden ofrecer nuevas formas de análisis a la organización, más enfocadas a nivel comercial, empleando estrategias de precios o planificación de capacidad. Pero no son conscientes de que en paralelo la empresa ha logrado un mayor acceso a los datos desde otras áreas, y ya cuenta con herramientas sofisticadas para analizar estos datos.

En opinión de Alexander Bant, jefe de investigación de Gartner, "esto presenta un riesgo de que las finanzas inviertan en exceso en capacidades analíticas, en un momento en que los socios comerciales dependen cada vez menos del equipo de planificación y análisis financieros (FP&A) para recibir soporte. Esta es una situación que conducirá a la duplicación y a una menor confianza en qué conjunto de resultados de análisis es el correcto".

Esta es la conclusión que se extrae de una encuesta realizada recientemente a 127 líderes financieros, en la que se revela que los tomadores de decisiones de negocio ya estaban obteniendo una cantidad de datos cada vez mayor sobre el rendimiento y las operaciones comerciales, más allá del departamento financiero. Por ello, se mostraban cada vez más dispuestos a utilizar fuentes de datos ajenas a las finanzas como recurso, cuando los datos financieros no están disponible a tiempo.

Como explica Bant, "los planes de transformación financiera deben incorporar un mayor énfasis en el gobierno y la calidad de los datos en toda la empresa, y la voluntad de reducir las capacidades analíticas que están infrautilizadas o que ya están operativas en otras funciones". Y comenta que la duplicidad de fuentes de datos y de resultados de analítica implica una sobreinversión innecesaria que puede dañar la relación con los inversores y clientes.

Por ello, Gartner recomienda que se auditen las diferentes formas de análisis que utiliza la empresa, tanto propias como de terceros, identificando cuáles tienen un ROI cuestionable a los ojos del personal de FP&A. Para ello se pude solicitar a estos profesionales que identifiquen las formas de análisis que experimenten una baja demanda o que requieran demasiado tiempo para ofrecer resultados.

A continuación, recomiendan duplicar la gobernanza de los datos de rendimiento de las operaciones, y no la síntesis de estos datos. La idea, según Gartner, es promover una estrategia de lo que denominan "versiones suficientes de la verdad", en vez del enfoque actual de "una única fuente de verdad", que no refleja la realidad actual, en la que las fuentes de datos son cada vez más complejas y diversificadas.

Bant concluye que "los líderes financieros que no logran ajustar el tamaño adecuado de sus carteras de análisis corren el riesgo de una duplicación creciente y de aumentar la confusión en torno a la interpretación correcta de los análisis, lo que en última instancia pone en riesgo la reputación de las finanzas como asesor confiable sobre los datos económicos del negocio". ■

MÁS INFORMACIÓN

- Las inversiones en IA no se han visto alteradas desde el inicio de la Covid-19
- Tendencias estratégicas para 2021, según Gartner

¿Cuál es el futuro del mercado de almacenamiento?

¿Qué tecnologías son las más adecuadas para las empresas?

Descubra las últimas tendencias en el Centro de Recursos IT User

Almacenamiento it

Con la colaboración de: Synology® NetApp®

El 51% de las empresas en España ha adaptado su infraestructura de TI al trabajo híbrido

Nadie duda del impacto de la pandemia en los planes de infraestructura digital empresarial. Según un estudio de Equinix, el 51% de las empresas en España ha rediseñado su infraestructura de TI para satisfacer las nuevas demandas del trabajo en remoto e híbrido, con presupuestos tecnológicos que aumentan para acelerar la transformación digital.

La digitalización y la inversión empresarial en infraestructura digital han aumentado como consecuencia de la COVID-19. El 55% de los líderes digitales en España afirma haber acelerado los planes de transformación digital a causa de la pandemia, mientras que el 51% dice que sus presupuestos se han incrementado para satisfacer el rápido crecimiento de las demandas digitales.

También se ha producido una importante revisión de las estrategias de TI para hacer frente a los retos derivados de la pandemia. El 65% de los líderes encuestados en España afirma que han revisado su estrategia de TI como resultado de la COVID-19, mientras que el 73% dijo que quiere invertir en tecnología para ser más ágil después de la pandemia.

El 55% de los líderes digitales en España afirma haber acelerado los planes de transformación digital a causa de la pandemia, mientras que el 51% dice que sus presupuestos se han incrementado para satisfacer el rápido crecimiento de las demandas digitales

Cuando se les preguntó por las principales prioridades de la estrategia digital de su organización, el 87% de los encuestados afirmó que la digitalización de su infraestructura de TI era una prioridad principal y el 65% dijo que consideraba la interconexión como un facilitador clave de la transformación digital, un 11% más que el año pasado.

Por otra parte, la pandemia no ha frenado los planes de expansión de las empresas. Así, el 71% de los responsables de la toma de decisiones de TI en España afirman que su organización se está expandiendo a nuevas regiones, países o mercados, el 73% de los cuales tiene previsto conseguirlo virtualmente, en lugar de invertir en infraestructura informática física.

El 70% de los responsables de TI afirmó que cree que la interconexión –el intercambio directo y privado de datos entre organizaciones– les ayudará a superar los retos a los que se enfrentan debido a la COVID-19. Los que afirmaron que la interconexión era clave para la supervivencia de su organización crecieron al 58%, frente al 50% del año pasado.

Para Ignacio Velilla, managing director de Equinix España, "de los resultados se desprende de la confianza de los líderes digitales de nuestro país en la interconexión como habilitador clave de la transformación digital y su papel fundamental para superar los retos de la pandemia. En Equinix estamos trabajando para apoyar el futuro de España como nuevo hub de interconexión para el sur de Europa, algo que sabemos por este estudio que es importante para nuestros líderes digitales". ■

MÁS INFORMACIÓN

- Equinix 2020-21 Global Tech Trends Survey
- Mejorando la experiencia del trabajador remoto

Nuevos retos de seguridad en entornos financieros

Su impacto en el modelo de negocio

El sector financiero ante el reto de la ciberseguridad:

la digitalización abre la puerta a nuevas amenazas

Los riesgos de las TIC representan un enorme desafío para las entidades financieras y subrayan la importancia de implementar una adecuada estrategia de seguridad que abarque, desde la protección de infraestructuras hasta la seguridad de datos y usuarios. La formación y concienciación del usuario son también clave, a fin de que este se convierta en un eslabón más de la cadena en la protección.

NUEVOS RETOS DE SEGURIDAD EN ENTORNOS FINANCIEROS

A lo largo de la última década, las entidades financieras, principalmente los bancos, han acometido un importante cambio en su modelo de negocio, apostando claramente por la digitalización como motor de innovación y puntal clave en su relación con el cliente. Así las cosas, este sector ha ido avanzando desde una huella digital básica hasta un entorno basado en la omnicanalidad, con el desarrollo de nuevos productos y servicios y un mejor y mayor aprovechamiento de tecnologías disruptivas, como la inteligencia artificial, el blockchain, la analítica y las tecnologías basadas en la nube.

Sin duda, esta creciente digitalización ha favorecido importantes beneficios: el customer centric es una realidad cada vez más consolidada, pero también ha generado significativos retos y riesgos no financieros, como la dependencia de proveedores y nuevos jugadores y la proliferación de ciberataques y amenazas online, exposiciones que se han multiplicado por el aumento de dispositivos electrónicos, la migración a la nube y la apertura de puertas y ventanas que han terminado por diluir el perímetro de la red. En este sentido, datos facilitados por el Fondo Monetario Internacional (FMI) apuntan que el número de ciberataques se ha triplicado en la última década, convirtiéndose en una amenaza para la estabilidad financiera. Según esta organización, en 2020 se produjeron 1.500 casos, frente a los 400 de 2012.

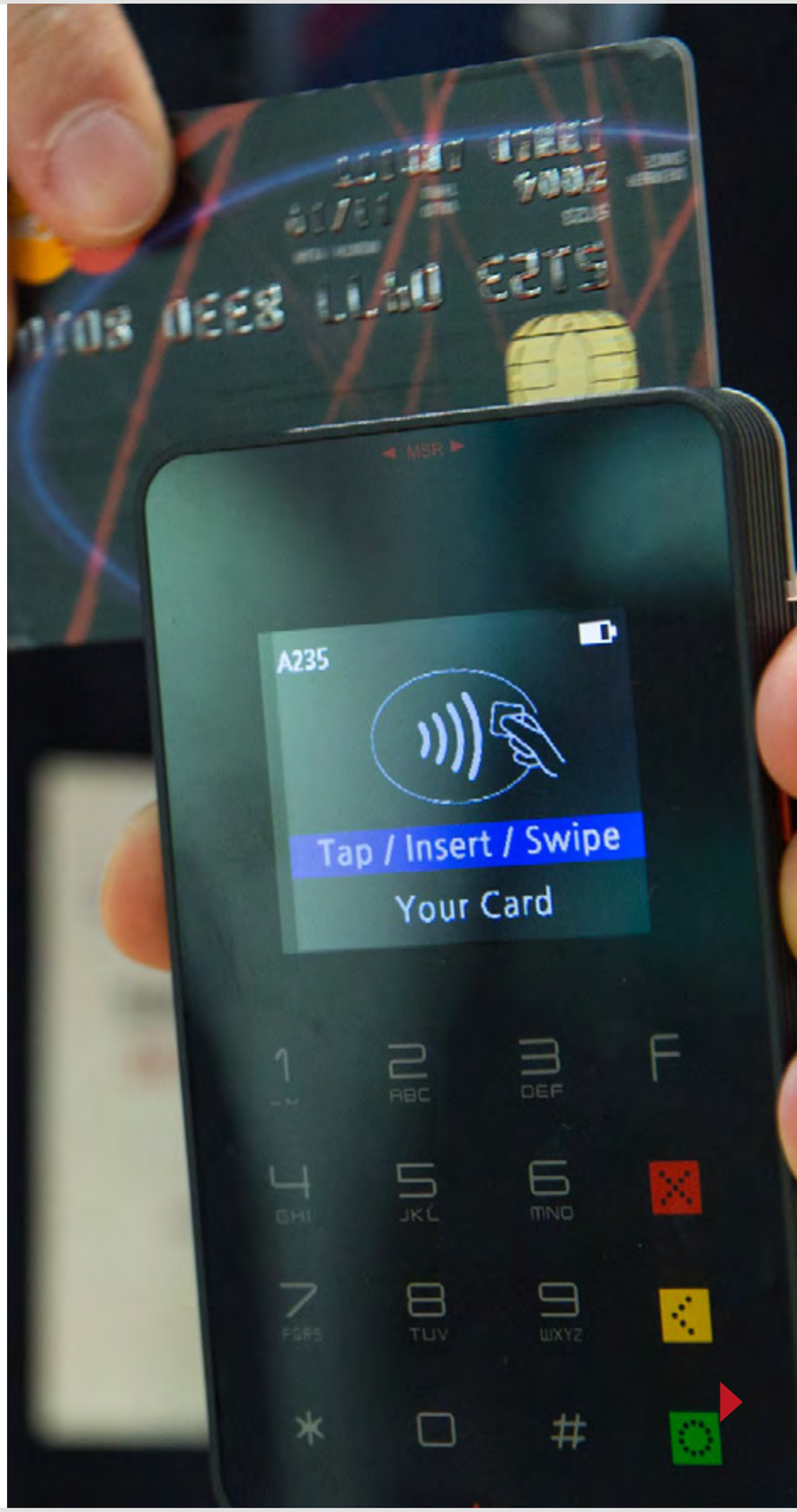
Del mismo modo, la aceleración de los planes de digitalización de estas compañías y, sobre todo, la generalización del teletrabajo a causa de la Covid-19, ha dilatado el nivel de riesgo, al abrirse nuevas vías de ataques que los ciberciminales han sabido aprovechar.

Así, este nicho ha experimentado la segunda mayor proporción de ciberataques relacionados con COVID-19, solo por detrás del sector de la salud, con un coste promedio por brecha de datos de 5.85 millones de dólares en 2020, frente a los 3.86 millones de dólares del promedio mundial, según datos de la última edición del informe anual Cost of a Data Breach Report de IBM.

EL DESAFÍO DE LA CIBERSEGURIDAD

La banca se enfrenta, por tanto, a un panorama difícil en materia de ciberseguridad, con ataques cada vez más complejos, muchos de los cuales se dirigen contra el usuario, el eslabón más débil, contra la propia infraestructura o hacia proveedores externos (ataques a la cadena de suministro). Así, a ofensivas de relleno de credenciales, fraude de apropiación de cuentas, correos electrónicos de phishing o malware (troyanos), se unen otras amenazas como el ransomware, que incluye vectores de doble extorsión y factor humano, junto con la creciente demanda de desencriptación de datos, y los ataques DDoS.

Detrás de estos ataques se esconden no solo criminales cada vez más osados, sino también estados y atacantes patrocinados por estados



NUEVOS RETOS DE SEGURIDAD EN ENTORNOS FINANCIEROS

que saben que por la sensibilidad de los datos que custodian, los bancos son un blanco fácil. Tanto es así, que, hoy por hoy, el ciber riesgo se encuentra en tercer lugar en el ranking de riesgos de entidades financieras, después de los lucros cesantes y el riesgo pandémico, según el 10º Barómetro de Riesgos de Allianz 2021.

Afortunadamente, y por los activos que gestionan (dinero, datos sensibles y reputación) en el sector financiero siempre ha existido una gran concienciación sobre la seguridad, tanto en la vertiente física como lógica. Se trata de un factor de confianza. Así, las entidades financieras destinaron en 2020 el 10,9% de su presupuesto a ciberseguridad, frente al 10,1% del año anterior. En términos de gasto por empleado, esto supone alrededor de 2.700 dólares, según una encuesta de Deloitte y FS-ISAC.

Ahora bien, es necesario que esta seguridad evolucione al mismo ritmo que lo hacen las tecnologías, los servicios provistos y la regulación (PSD2, Mifid2, CRD2...), sin olvidar, por supuesto, como lo hacen también la tecnología de ataque y los hackers, alumnos aventajados.

Por ello, y además de proteger infraestructuras como los ATMs, es necesario apostar por soluciones centradas en el resguardo del endpoint, la red, email, servidores o workloads en la nube, como antivirus, plataformas EDR, XDR o con capacidades de aprendizaje automático. Asimismo, estas entidades deben avanzar hacia un enfoque proactivo, que dé prioridad a la prevención, para interrumpir los ataques antes de que el malware o la amenaza maliciosa -sin archivos- pueda siquiera comenzar a ejecutarse. También, la monitorización y gestión de lo que ocurre en redes botnets o en la Deep Web ayudará a prevenir y a mejorar la seguridad, con planes de respuesta. Esto incluye la formación de los empleados en materia de concienciación sobre la seguridad, la limitación de los privilegios de los administradores y una estrategia de confianza cero que abarque la gestión de la identidad y el acceso, así como la seguridad de la red. Importante igualmente es la colaboración entre entidades y con terceros, a fin de garantizar la resiliencia operativa digital.

EL RIESGO DE LA BANCA MÓVIL

Adicionalmente, la expansión de los servicios basados en dispositivos móviles (banca móvil) y la mayor dependencia de los clientes de las aplicaciones de banca electrónica ha ampliado su vulnerabilidad, convirtiéndose estos usuarios en blancos potenciales para los actores maliciosos, que utilizan una variedad de técnicas, incluidos troyanos bancarios basados en aplicaciones bancarias falsas, para atacarles. Así, la actividad de los troyanos bancarios se ha intensificado un 15%, según un estudio de Check Point, y estos se orientan, sobre todo, a atacar el segundo factor

de autenticación, principalmente SMS, para además de robar datos de acceso o credenciales, hacerse con otros más personales.

Ante esta situación y para protegerse, los bancos deben integrar metodologías o tecnologías que ayuden a asegurar las transacciones electrónicas, como la criptografía, o que faciliten la autenticación del usuario para evitar la suplantación de identidad, como los sistemas de tokenización. Igualmente, y de cara a ser más precisos, es fundamental securizar y custodiar las claves que protegen esa información (claves de cifrado) y la gestión de su ciclo de vida, sobre todo ahora, cuando se está produciendo una clara orientación a los servicios en la nube. En este sentido, los HSMs, capaces de almacenar y proteger claves criptográficas en consonancia con las normas más rigurosas de la industria, como la Directiva Europea de Pagos PSD2, son una opción.

PROTEGER EL DATO

La progresiva implantación de modelos comerciales, como el open banking, asentado en el intercambio de datos entre bancos y terceros (Bigtech) a través de APIs, está ocasionando distintos problemas de protección, sobre todo en el ámbito de la seguridad (de usuarios y entidades) y el análisis de datos. Según McKinsey & Company, los bancos son responsables de mitigar el riesgo de fraude y deben implementar controles, que incluyan análisis avanzados (por ejemplo, para validar el origen de las llamadas entrantes a la API), modelos de

Blockchain: riesgo u oportunidad

Los bajos tipos de interés, la reducción de márgenes, y los nuevos requerimientos regulatorios están presionando a la banca para buscar nuevas fórmulas que le permitan ganar en competitividad y rentabilidad. En este contexto, tecnologías como blockchain, suenan cada vez con más fuerza, en tanto en cuanto permiten realizar directamente entre partes, transacciones seguras con el apoyo de máquinas y algoritmos.

Asociada esta tecnología a las criptomonedas, una de las formas más populares y conocidas de usar blockchain, sus capacidades van sin embargo más allá de su almacenaje e intercambio, desde transacciones en tiempo real hasta tokenización de activos, préstamos y créditos, valores, prevención del fraude e identificación de los clientes. Además, sus capacidades de seguridad, apoyadas en la descentralización de la información, así como, en la eliminación de intermediarios, y la implementación de criptografía y firma digital para asegurar las transacciones, favorecen que estas operaciones (y sus datos) tengan la mayor seguridad, privacidad y autenticidad posible.

Sin embargo, y aunque Blockchain es una tecnología bastante segura en su diseño, su incorporación en mercados y entornos regulados, como el financiero, está produciéndose lentamente. Aún se tienen que garantizar aspectos de su seguridad, muchos de ellos relacionados con la ausencia de estándares tecnológicos, la falta de interoperabilidad entre distintas plataformas de cadenas de bloques o el uso de contratos inteligentes, que puedan ser origen de fugas de datos de carácter personal, y que hace necesario incorporar metodologías de seguridad por diseño desde las primeras fases de desarrollo, para evitar riesgos como: minado de cadenas laterales o paralelas (sidechain) o ataques DDoS, entre otros.

También y en lo que tiene que ver con el sistema de autenticación de la gestión de accesos a los sistemas blockchain, y aunque la normativa europea obliga a la banca a tener sistemas de autenticación de doble o triple factor, es necesario avanzar, sobre todo, por su relación con otros sistemas de información de la empresa.

Estos aspectos podrían solucionarse con la creación segura de claves o que el proceso de firma de cada una de las transacciones que se lanzan al bloque sea invulnerable. Es necesario validar el uso de blockchain como registro fundamentado y vinculante de evidencias digitales, definiendo en qué condiciones es válido. No hay duda de que si alguien descuida la custodia de sus claves éstas podrían acabar en manos de un atacante que podría así suplantar su identidad en la aplicación correspondiente. También hay que tener en cuenta que, debido al potencial de esta tecnología, es previsible que los ciberdelincuentes busquen oportunidades para atacar cualquier vulnerabilidad, tanto humana como técnica, en el ecosistema de blockchain.

NUEVOS RETOS DE SEGURIDAD EN ENTORNOS FINANCIEROS

autenticación segura del cliente y herramientas sólidas para detectar ataques de fraude, de acuerdo a PSD2. Estas normas también requieren que los bancos proporcionen un "sandbox" protegido a los proveedores de servicios de pago para las pruebas y el desarrollo continuo de servicios que utilizan la interfaz del banco.

Además de involucrarse en oportunidades de negocio innovadoras y potencialmente lucrativas abiertas por PSD2, el sector financiero se ha lanzado de lleno hacia una mejora real en la eficiencia, escalabilidad y flexibilidad de la mano de la Nube, para asegurar, en tiempos de pandemia, una fuerza de trabajo a distancia y garantizar la capacidad de recuperación. De este modo, y con los usuarios, dispositivos, aplicaciones y datos fuera del centro de datos empresariales y la red, la necesidad de proteger esos activos, así como de poseer una visibilidad completa del entorno se ha hecho imperativo. A este respecto, IDC Research confirma que cualquier solución de seguridad para cloud ha de incluir tres elementos: integración nativa, protección amplia y gestión y automatización. En torno a esta premisa han surgido marcos de seguridad como SASE, que esboza una convergencia de múltiples funciones de seguridad, como acceso de red Zero Trust (ZTNA), Gateway Web Seguro (SWG) de próxima generación, Agente Seguro de Acceso a la Nube (CASB), Gestión de la Postura de Seguridad Cloud (CSPM) o Firewall como Servicio (FWaaS); entregados desde la nube.

Además de la nube, la externalización de las funciones y servicios de las TIC, que ha cobrado mayor importancia durante la actual crisis sanitaria, puede plantear también retos relacionados con la gestión del riesgo de terceros, la confidencialidad y la protección de los datos de los consumidores. Igualmente, la inclusión del aprendizaje automático y de la inteligencia artificial están acrecentando esta vulnerabilidad, cuando, por ejemplo, los datos corruptos no detectados se introducen en los algoritmos y se utilizan en la toma de decisiones, según Bank for International Settlements (BIS). Por último, y en el caso de sufrir un episodio de ransomware, la recuperación de los datos, podría tornarse muy compleja, y las dudas sobre la exactitud de la información recuperada podrían hacer que el problema se prolongue durante un largo periodo de tiempo.

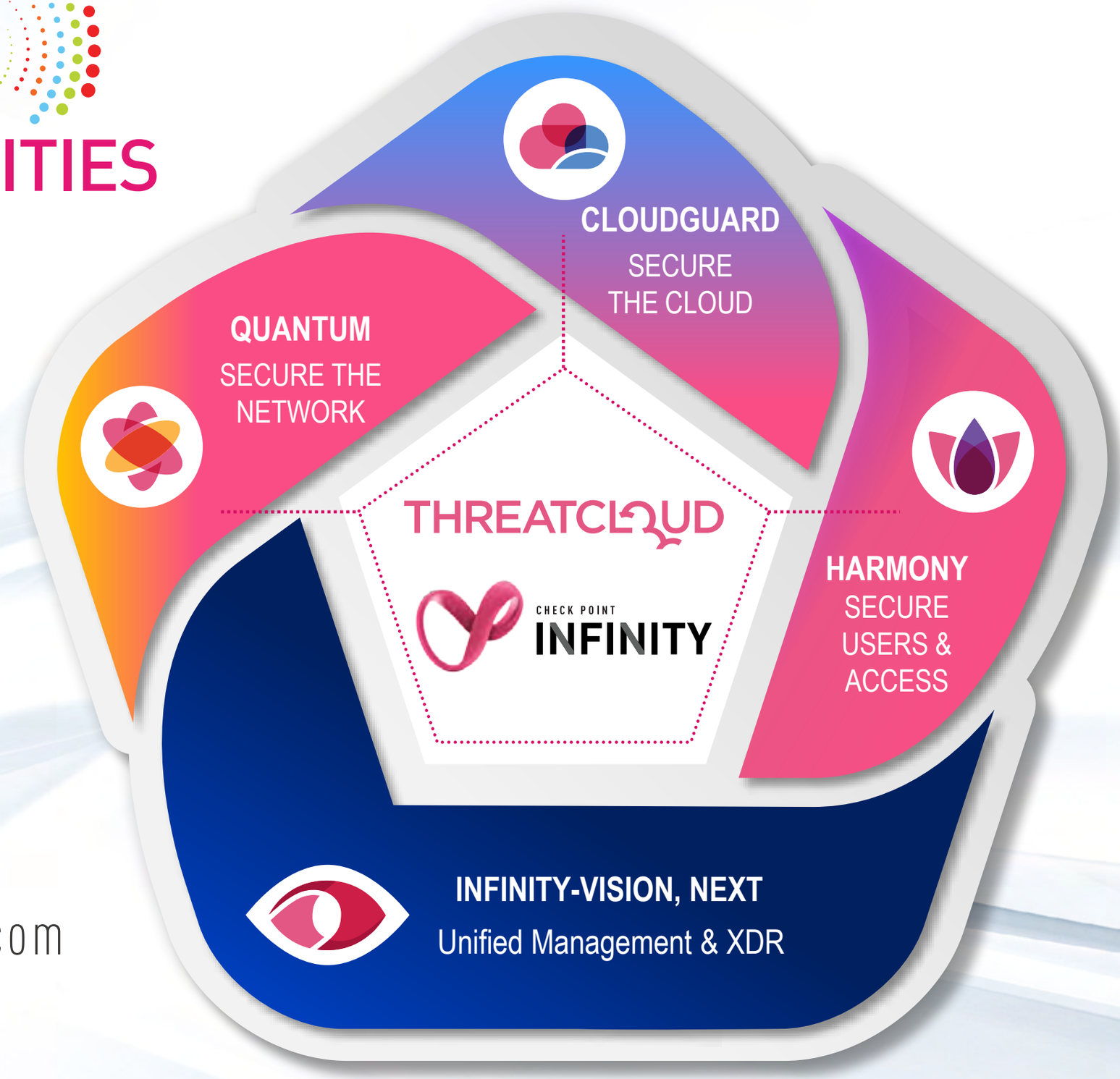
No hay duda, por tanto, que el gran volumen de datos generados por la banca requiere de la facultad de analizar y proteger dicha información, manteniendo y acatando, al mismo tiempo, las estrictas normas de la UE en materia de privacidad y protección de datos. Asimismo, el aumento de la demanda de servicios financieros en línea, y la progresiva modernización de los sistemas de pago, según el dinero en efectivo va perdiendo preponderancia, llevan a cuidar todos los aspectos de la seguridad. Cualquier incidente podría socavar la confianza del cliente, por lo que la ciberseguridad es más esencial que nunca. ■

MÁS INFORMACIÓN

- Incremento de ciberataques en la ultima década
- Ciberataques relacionados con la Covid-19
- Cost of a Data Breach Report
- 10º Barómetro de Riesgos de Allianz 2021
- Madurez en la ciberseguridad y riesgos en las instituciones financieras
- Actividad de los troyanos bancarios
- Directiva Europea de Pagos PSD2
- PSD2 y la disrupción en el open banking
- El efecto de los datos corruptos
- Bajos tipos de interés

Check Point®
SOFTWARE TECHNOLOGIES LTD

NEW WORLD
NEW OPPORTUNITIES
2021



MÁS INFORMACIÓN:

www.checkpoint.com/es

info_iberia@checkpoint.com

Nuevos retos de seguridad en entornos financieros;

su impacto en el modelo de negocio

Más tarde o más temprano las entidades financieras pueden ser víctimas de un ciberataque. Con esa idea en mente, deben prepararse para responder a las amenazas de hoy pero también a todas aquellas que van surgiendo al amparo de las nuevas tecnologías.

MESA REDONDA IT: Nuevos retos de seguridad en entornos financieros; su impacto en el modelo de negocio

El sector financiero, sobre todo la banca, lleva años sumido en una profunda transformación digital que le ha llevado a afrontar una serie de cambios, tanto en el modo de ofrecer y prestar sus servicios como en el de atender a sus clientes. Asimismo, la situación derivada de la COVID-19 ha transformado el comportamiento del consumidor, desde las preferencias de canal hasta el método de pago, y ha abierto una importante brecha en ciber-

“Las organizaciones tienen que actualizar o desarrollar sus propios sistemas de ciberseguridad según se detectan nuevos sistemas de ataque. Afortunadamente hay bastante concienciación en ciberseguridad”

EUSEBIO NIEVA,
DIRECTOR TÉCNICO DE CHECK POINT

seguridad, al incrementarse la digitalización y, por ende, la superficie de ataque. Por todo ello, ¿cuáles son los principales retos de ciberseguridad a los que se enfrentan actualmente entidades y servicios financieros? Para hablar sobre ello y conocer cómo afrontan los nuevos ataques y amenazas; su grado de concienciación al respecto de la ciberseguridad; cómo se ha adaptado este sector a tecnologías emergentes como blockchain o las nuevas normativas como PSD2; o cuál debe ser el siguiente paso en la adopción de nuevas tecnologías de seguridad, hemos contado con la participación en esta Mesa Redonda IT de Eusebio Nieva, Director Técnico de Check Point; Javier Sánchez, Territory Sales Manager de Entrust; Luis Javier Suárez, Presales Manager de Kaspersky; Jesús Rodríguez, CEO de Realsec; Igor Unanue, CTO de S21sec; Alfonso Martínez, Country Manager, Data Protection de Thales; y José de la Cruz, Director Técnico de Trend Micro Iberia.

RETOS EN CIBERSEGURIDAD

La creciente digitalización ha abierto la puerta a importantes retos en materia de ciberseguridad que, aunque extensibles a todos los verticales, en el financiero se perciben aún más. En este sector se maneja algo que todos los atacantes quieren: “dinero”, asegura Eusebio Nieva, por lo que no se debe confiar en sistemas tradicionales como protección frente a amenazas desconocidas. “Las organizaciones tienen que actualizar o desarrollar sus propios sistemas de ciberseguridad según se detectan nuevos sistemas de ataques”. Afortunadamente hay bastante concienciación en ciberseguridad.

Efectivamente, la cada vez mayor sofisticación por parte de los cibercriminales lleva a un nuevo paradigma en el que, según Luis Javier Suárez, “ya no basta con confiar en soluciones que aseguren un elevado grado de prevención, sino que se ha de plantear la hipótesis de poder estar siendo comprometido y no saberlo”. Aquí ya entra la parte de recoger ciertas métricas, telemetrías o anomalías para poder hacer un análisis y ver cómo cambian las normas del juego.

En idéntica línea, José de la Cruz recurre al planteamiento Zero Trust; “hay que asumir que

va a existir una brecha, y estar preparados para detectarla y actuar". Además, destaca dos retos que apuntan a la protección de las infraestructuras, donde hay una amalgama de tecnologías tradicionales y modernas combinadas, y a los usuarios, externos e internos. "Debemos dotarles de una seguridad que les aporte visibilidad sobre lo que ocurre en sus entornos".

Sobre estos retos, Igor Unanue considera, que, por el propio proceso de digitalización, estas organizaciones integran nuevas tecnologías, aplicaciones... que están atrayendo nuevos tipos de ataques, como los de tipo hacking, que permanecen en las redes internas largo tiempo sin ser descubiertos, causando importantes daños. "Van a seguir descubriéndose nuevas amenazas. La banca debe mantenerse alerta y estar corrigiendo para poder protegerse mejor".

UN NUEVO CONCEPTO DE BANCA

La progresiva digitalización ha marcado una senda de cambios. Se ha pasado del cliente físico al cliente móvil, de los centros de datos al cloud, ampliándose, al mismo tiempo, los vectores de ataque, lo que ha supuesto una mayor vulnerabilidad. ¿Cómo está enfocando la banca estos cambios?

Desde la perspectiva de este desarrollo, Javier Sánchez, observa que, en la actualidad, el vector de relación entre la banca y el usuario es la aplicación, por lo que hay que protegerla. "Las apps son un riesgo para los usuarios, que pueden ver comprometidos sus datos, y para los bancos, por el desprestigio para su negocio". Sobre la nube, donde cada vez residen más datos, incluso críticos, Sánchez estima que estarán seguros mientras el control de las claves que los cifran, no viaje con ellos.

Sobre este proceso de transformación, Jesús Rodríguez destaca que, a consecuencia de la pandemia, muchos desarrollos se han precipitado. "El uso del efectivo ha caído y canales que se iban a desarrollar de forma natural se han precipitado". Cada vez se hacen más operaciones utilizando dispositivos móviles y fórmulas, como el open banking, están cambiando el modo en que se utilizan los servicios bancarios. "Esto incide en la necesidad de proteger las transacciones (crip-

"Mediante la utilización de criptografía se van a proteger las transacciones, y con los sistemas de tokenización se va a autenticar a los usuarios. La suplantación de identidad es uno de los mayores riesgos para la banca"

JESÚS RODRÍGUEZ, CEO DE REALSEC

“La concienciación, incluso la formación, no dejan de ser responsabilidad del banco. El usuario tiene que ser un eslabón más de la cadena en la protección, no un habilitador de un ataque”

JOSÉ DE LA CRUZ, DIRECTOR TÉCNICO DE TREND MICRO IBERIA

tografía) y al usuario (sistemas de tokenización para evitar la suplantación de identidad).

Por su parte, Alfonso Martínez defiende la idea que con la gran evolución que ha tenido la banca en estos últimos años, esas entidades no pueden seguir protegiéndonos como hace 10 o 15 años. “Al igual que el abanico de opciones se multiplica, las amenazas también y son más sofisticadas. Los fabricantes no podemos quedarnos atrás. Tenemos que dar soluciones a las tendencias tecnológicas que van surgiendo, y ofrecer esa completa seguridad alrededor de la información”.

LA CONCIENCIACIÓN DEL USUARIO

El usuario es el centro de todo. Sin embargo, es importante encontrar un equilibrio entre la experiencia de usuario y la seguridad. ¿Cómo conseguirlo?

Para Eusebio Nieva, este equilibrio pasa porque el usuario perciba que la seguridad es útil. “Las medidas de protección pueden interferir en el usuario, en el acceso o en el dato”. Sin embargo, se debe intentar que el cliente distinga estas pautas como una ventaja, que aprecie que con estos mecanismos evita perder dinero, mientras consigue que las transacciones sean fiables y sus datos estén seguros. “A la vez que protege, la propia tecnología debe mostrar sus beneficios”.

Este componente de concienciación también es apreciado por Luis Javier Suárez, quien distingue dos desafíos para los bancos: conseguir que la experiencia del usuario no sea invasiva, mientras se recogen comportamientos y detectan anomalías que permitan tomar medidas para la detección temprana del fraude; y trabajar la concienciación, tanto dentro de la propia empresa como de cara al usuario. “Es importante trasladar las buenas costumbres adquiridas en la banca tradicional al mundo digital”.

La importancia de la concienciación, y de la formación, es destacada por José de la Cruz. “No deja de ser responsabilidad del banco proteger los activos de sus usuarios, que deben ser un eslabón más de la cadena en la protección, no un habilitador de un ataque”. Además, es clave comprender que la seguridad se ha de implementar en la fase de diseño, para que la integración sea mucho más transparente y sencilla y no interfiera en la agilidad o experiencia de usuario.

Para referirse al valor que le da el usuario a esta agilidad, Igor Unanue cita el doble factor

de autenticación, que no se implementó hasta que no fue obligatorio por ley, para no interferir en el acceso. “Es un tema de concienciación, de cultura. Cuando nos habituemos a utilizar determinadas tecnologías de seguridad también lo haremos en la banca”. No obstante, estas tecnologías han de resultar naturales para el usuario. “La seguridad debe ser cada vez más efectiva y más sencilla”.

PSD2 Y OTRAS REGULACIONES

Las entidades financieras siempre han estado a la cabeza en cuanto a modelos de transformación digital y en la adopción de medidas de seguridad, siempre han querido ir un paso por delante. Sin embargo, ha habido casos más complicados, como con la regulación PSD2. ¿Se ha logrado de una manera efectiva su adopción? Ahora, cuando ya se vislumbra el reflejo de PSD3, toca preguntarse si la banca está preparada para lo que está por venir.

Al respecto de la observancia de PSD2, Jesús Rodríguez refiere cómo las entidades se han estado preparando, primero, con el desarrollo de APIs para poner a disposición de terceros información de los clientes, y, después, con el establecimiento de un sistema de autenticación de doble factor. “En España no podemos hablar de incumplimiento, aunque la mayoría de entidades no han adoptado un sistema de tokenización; han optado por el envío de un SMS. A futuro, con la PSD3 en el horizonte, habrá que buscar otras soluciones basadas en token”.

Sobre la aceptación de estas medidas, Alfonso Martínez reconoce el gran esfuerzo realizado al abrir estas APIs para favorecer el open banking. Sin embargo, expone la importancia de implementar la seguridad desde el principio, en consonancia con PSD2, y para cumplir con otras nor-

“La seguridad debe estar habilitada desde el principio. Solo si los fabricantes ofrecemos las tecnologías adecuadas, las entidades van a poder acatar las distintas normativas y procurar los servicios (seguros) apropiados”

ALFONSO MARTÍNEZ, COUNTRY MANAGER, DATA PROTECTION DE THALES IBERIA

> "A causa de las normativas, los bancos están aplicando cada vez más niveles de seguridad sobre sus accesos a la red SWIFT. Pero hay que hacer más. Si ocurren ataques es porque detrás hay una vulnerabilidad, y los atacantes saben aprovecharlo"
>
> IGOR UNANUE, CTO DE S21SEC

mativas. En este punto el papel de los fabricantes es clave. "Debemos ofrecer las tecnologías adecuadas para que estas entidades puedan procurar los servicios (seguros) apropiados".

ATAQUES A LA RED SWIFT, UN RIESGO SISTÉMICO

Otro tema que cada vez está resultando más relevante son los ataques contra la red SWIFT, que se han multiplicado en los últimos tiempos. Ahora bien, ¿qué impacto están teniendo y en qué consisten estas ofensivas?

"Por tratarse de una red en la que fluye el negocio y circula el dinero, SWIFT es un claro objetivo para los hackers, que intentan interceptar transacciones para sacar beneficio", explica Eusebio Nieva. Para su salvaguarda, la tecnología puede ayudar muchísimo, sobre todo para el análisis de fraude y la securización de ciertos puntos que todavía son un poco débiles. "Al final se trata de aplicar la tecnología en esas transacciones. Protección y fiabilidad en todos los extremos".

Mitigar y securizar es crucial, pero antes hay que conocer cómo se producen estos ataques. En este sentido, Luis Javier Suárez, destaca que los más eficientes son los dirigidos contra la cadena de suministro. "Los atacantes manejan una cantidad abrumadora de inteligencia sobre los organismos que operan en la red SWIFT. Conocen qué vulnerabilidades pueden ser explotadas dentro de los sistemas y aprovechan esta información para saber dónde atacar y alcanzar ese objetivo".

Sobre las razones que explican los ataques a la red SWIFT, Igor Unanue revela que, por tratarse de una red externa, las medidas de seguridad son más laxas. "Sin embargo, ahora, sobre todo por las normativas, se están aplicando mayores niveles de seguridad a estos entornos, pero hay que hacer más. Si ocurren ataques es porque detrás hay una vulnerabilidad, y los atacantes la están aprovechando bien. Al final es una red de comunicación más, y como tal hay que protegerla".

La cadena de suministro es reconocida también por José de la Cruz, como el elemento más débil, y, dentro de ella, los bancos pequeños,

con medidas de seguridad menos robustas, el eslabón más frágil". No obstante, todos deben asumir que antes o después se producirá un ataque, por lo que las entidades deben dotarse de una visibilidad que les permita conocer lo que está ocurriendo, tanto en su entorno como con los flujos de información que existen con terceros.

TECNOLOGÍAS EMERGENTES

Tecnologías emergentes como blockchain, IA o IoT están empezando a impactar en los servicios financieros. ¿Cómo se están adaptando los bancos a ellas?

Sobre este punto, Javier Sánchez, expresa que "están en proceso". Los bancos custodian tanto el dinero como la confianza de sus clientes por lo que tienen que tomarse su tiempo a la hora de utilizar nuevas tecnologías y que formen parte de su proceso de negocio. En el caso de una blockchain pública no hay nadie al otro lado, por lo que los bancos no pueden comprometer su confianza con una tecnología que puede no ser segura.

Ahora mismo, la banca necesita ganar en competitividad y en rentabilidad por lo que, según Jesús Rodríguez, necesita hacer uso de tecnologías innovadoras como IA, donde están más adelantados. Otras como blockchain, muy ligada a las criptomonedas, y donde se "avanzará con una regulación", también son utilizadas para cifrar bloques o firmar smart contract, pero no cuando hablamos de claves, donde el nivel de exigencia es muy alto. Otras como IoP despegarán en un futuro.

Desde la perspectiva de representar a una empresa que fabrica tecnología que ayuda o habilita para el uso de innovaciones como blockchain, Alfonso Martínez considera que falta mucha labor de comunicación. "Estas tecnologías luego hay que aplicarlas a la vida real y, en ese sentido, falta información tanto, para los usuarios finales, que tienen que saber qué es blockchain y cómo utilizarlo como para las entidades financieras, para entender cómo lo pueden monetizar.

TECNOLOGÍAS IMPRESCINDIBLES

Ante toda esta innovación, el sector financiero no puede bajar la guardia en su seguridad. ¿Cuáles son aquellas tecnologías de seguridad que puede ser consideradas imprescindibles en la actualidad? Y ¿a futuro?

"Los bancos custodian tanto el dinero como la confianza de sus clientes. Tienen que tomarse su tiempo a la hora de utilizar nuevas tecnologías y que estas formen parte de su proceso de negocio"

JAVIER SÁNCHEZ, TERRITORY SALES MANAGER DE ENTRUST

“Cualquier organización tiene que asumir que puede ser comprometida. Este paradigma nos lleva a la gestión del incidente y al gobierno de algo que se ha impulsado desde el sector financiero: la gestión de indicadores de compromiso”

LUIS JAVIER SUÁREZ, PRESALES MANAGER DE KASPERSKY

Eusebio Nieva reconoce una alta concienciación en ciberseguridad, pero recomienda no bajar la guardia. “Estas entidades deben optar por tecnologías específicas para abordar amenazas actuales, como el ransomware, los ataques a la cadena de suministro o la protección del endpoint, pero también, por enriquecer sus sistemas con diferentes soluciones que protejan contra los peligros surgidos al calor de innovaciones, como las tecnologías cloud, y que las organizaciones financieras están convirtiendo en el core de sus servicios y de sus negocios”. Deben evolucionar y adaptarse según progresan sus tecnologías. La protección de la red o del endpoint era algo que había que hacer, y ahora hay que proteger las claves. En este sentido, Javier Sánchez respalda la importancia del cifrado, que ahora, además, es percibido tanto por otros fabricantes de seguridad como por las propias entidades del sector financiero como una solución necesaria para proteger la información. “Se ha producido una concienciación en torno a la importancia de securizar las claves, por lo que su adopción está ocurriendo de un modo natural en la banca”.

En línea con esta innovación hay un componente de concienciación importante. A este respecto, Luis Javier Suárez valora la trascendencia de que las empresas financieras desarrollen un plan de concienciación, ya sea de forma individual o con el respaldo de una empresa especializada. “También, deben asumir que su ciberseguridad puede verse comprometida, por lo que el uso de indicadores de compromiso resulta efectivo, sobre todo para compartir con terceros la información que contienen (inteligencia y patrones de ataques) y medir la afectación”. Asimismo, es esencial la explotación de inteligencia de amenazas, para ir a la par con los atacantes.

MEDIDAS PROPORCIONALES

Decidir qué solución o qué conjunto de recursos son los más adecuados para proteger las infraestructuras de las entidades financieras es complicado. “La realidad”, expresa Jesús Rodríguez, es que los riesgos están ahí, y las medidas han de ser proporcionales, así como las políticas

y los procedimientos de seguridad que se establezcan. No obstante, se deben proteger los activos de negocio, los riesgos de fraude e implantar medidas contra la suplantación de identidad o el malware. Por otro lado, el despliegue de nuevos canales de pago ha promovido un mayor uso de la criptografía, mientras que el crecimiento de los datos, precisa de medidas de protección que requieren el uso del cifrado, para cumplir con normativas como PSD2 o PCI DSS.

En la misma línea, Igor Unanue reitera que allí de donde vengan las amenazas es donde la banca más tendrá que invertir en ciberseguridad. En cuanto a futuro desafíos, señala la persistencia del malware (malware bancario) y de otros procedentes de servicios cloud, por el incremento de servicios de colaboración, que derivará en muchos riesgos. "Imperativo será también proteger el endpoint y, en general, todo aquello donde la banca perciba una amenaza".

Alfonso Martínez, coincide en que hay "mucho vector que proteger y el dato debe salvaguardarse así mismo con el cifrado". El cifrado puede ser en la nube, en máquinas virtuales, incluso en movimiento o viajando de una nube a otra. Lo importante es entender que detrás de esos sistemas tan complejos existe una inteligencia real a la que hay que ayudar para que la gestión sea sencilla y la criptografía no se convierta en un dolor de cabeza. "Debemos darles las herramientas para poder gestionarlo todo de manera centralizada y correcta".

Para José de la Cruz, la banca se enfrenta a un panorama heterogéneo, con diferentes tecnologías, proveedores y entornos, que le provocan un grado de exposición muy alto. La respuesta ante eso es visibilidad y control. "Visibilidad de lo que se protege, para conocer el origen y alcance de un ataque, y control sobre aplicaciones que no han sido diseñadas con la seguridad en mente y que hay que resguardar de un modo transparente". En lo que respecta a servicios como DevOps o cloud, un enfoque Cloud Security Posture Management ayuda a dar esa capa de visibilidad, y a identificar riesgos, para mitigarlos. ■

MÁS INFORMACIÓN

- Mesa Redonda IT: Nuevos retos de seguridad en entornos financieros; su impacto en el modelo de negocio

JOSE FRANCISCO PEREIRO, GLOBAL HEAD OF PRIVACY TECH | RISK, BNP PARIBAS

“Un equipo de profesionales de seguridad capacitado y motivado es el mejor control para mitigar los riesgos”

En una situación como la que nos está tocando vivir hay que entender que el riesgo cibernético, lejos de reducirse, ha aumentado. Estamos viendo a través de los medios de comunicación como el cibercrimen está atacando multitud de empresas privadas y administraciones públicas con ataques de tipo ransomware, incluyendo infraestructuras críticas.

¿Cuáles son los principales retos de ciberseguridad a los que se enfrentan actualmente los servicios financieros?

Uno de los principales retos es gestionar el riesgo de terceras partes, la cadena de suministro se está transformando con velocidad y creciendo en volumen. Adicionalmente a la colaboración histórica con grandes multinacionales tecnológicas, es cada vez más frecuente en el sector financiero la colaboración con startups, fintech y multitud de nuevos socios. Estas organizaciones aportan sin duda innovación y nuevos modelos de negocio, pero es necesario evaluar con detenimiento los riesgos de seguridad y ayudarles a mitigarlos antes de comenzar una iniciativa conjunta.

Otro de los retos es la evolución y sofisticación de los ataques informáticos, cada vez más dirigidos y mejor ejecutados. Contra esto, además seguir trabajando en el diseño e implementación de nuevos controles técnicos para detener los ata-

ques, es fundamental entender el factor humano, puesto que muchos de estos ataques tienen como base de entrada la ingeniería social, que intenta explotar las debilidades que todos tenemos cuando somos expuestos a una situación de falso peligro o urgencia con el objetivo de influir en nuestra conducta. Por esto, ya no es suficiente con disponer de un programa formación en ciberseguridad, sino que es necesario cubrir tres dimensiones: formación, concienciación y entrenamiento. La segunda, la concienciación, hace referencia a la capacidad de crear impacto emocional para protegernos de situaciones de peligro, como muy bien se hace por ejemplo en las campañas de tráfico. La tercera, el entrenamiento, es la más importante y consiste en simular situaciones cercanas a un ataque cibernético para desarrollar las habilidades necesarias y responder adecuadamente cuando se produzca un ataque real.

El tercer reto es la captación y retención del talento en ciberseguridad. Un equipo de profesionales de seguridad capacitado y motivado es el mejor control para mitigar los riesgos, pero es necesario competir en un mercado laboral de nicho en el que cada vez hay más empresas interesadas en reclutar este tipo de profesionales. Por eso, además de desarrollar políticas de atracción para las nuevas generaciones, es necesario darse cuenta de que, muchas veces, el talento está más cerca de lo que se piensa y que una alternativa interesante es formar en ciberseguridad a profesionales que estén trabajando en otras áreas.

¿Cómo se han adaptado los servicios financieros a tecnologías emergentes como Blockchain o IoT?

Las tecnologías emergentes, como el Blockchain, IoT, AI, Big Data, Cloud y muchas otras, ofrecen sin duda una gran oportunidad para desarrollar nuevos modelos de negocio y de relación con nuestros clientes. Las ventajas de estas tecnologías suelen ser evidentes y crean un alto nivel de interés en las áreas de negocio. Sin embargo, por tratarse de tecnologías emergentes, no siempre hay experiencia en la industria que nos permita modelizar y dimensionar los riesgos de ciberseguridad de una forma estándar.

Por ejemplo, las arquitecturas Blockchain o DLT, que son reconocidas como de las más seguras en la actualidad por su base criptográfica, tienen ya algún riesgo identificado como el asociado al compromiso del 51% de los nodos de la red. Si bien ejecutar este tipo de ataque es extremadamente difícil en aplicaciones basadas en Blockchain públicos con decenas de miles de nodos, como es el caso de la criptomoneda Bitcoin, si hablamos de una implementación privada con sólo decenas de sistemas y sistemas homogéneos, el riesgo de este tipo de ataque se incrementa, por lo que es necesario de dotarlo de medidas adicionales.

Un caso particular de tecnología emergente es la computación cuántica que, cuando ésta alcance cierta escala, pondrá en riesgo la seguridad de muchos sistemas a nivel global, al poder romper el cifrado de clave pública en el que se basan muchos algoritmos criptográficos.

Por tanto, la aproximación adecuada con las tecnologías emergentes es la basada en un análisis pormenorizado de los riesgos, mediante una aproximación consultiva, dedicando profesionales de seguridad al estudio de las posibles fallas y la definición de los controles y tecnologías de seguridad necesarios, así como la realización de pruebas exhaustivas antes de su salida a producción.

¿Qué regulaciones están afectando al sector financiero y cómo se está haciendo frente a ellas?
El sector financiero es el más regulado desde hace muchos años, teniendo que cumplir con numerosos requisitos de información y reporting a agencias y bancos centrales de todo el mundo. Esto nos ha permitido disponer de una estructura empresarial y cultura organizativa que permite asimilar nuevas regulaciones con relativa ventaja a empresas de otros sectores. Dicho esto, y con relación al tema que nos ocupa, las regulaciones de privacidad que están surgiendo a lo largo del planeta, y en particular la GDPR en la zona europea, están teniendo un impacto significativo en los sistemas de información y en las medidas de ciberseguridad asociada.

Por un lado, se ha regulado el concepto de protección de datos en el diseño de nuevas aplicaciones y servicios, que tiene inherentemente asociada un componente de ciberseguridad. De esta forma, cada vez que se desarrolle un nuevo producto que procese datos de carácter personal, este deberá tener en cuenta las necesidades regulatorias y de seguridad. Además, la GDPR, en su artículo 32, establece la obligatoriedad de implementar las medidas de seguridad necesarias para proteger los datos proporcionalmente a los riesgos a los que está expuesta. La privacidad debe ser embebida en todas las arquitecturas y soluciones IT, por ejemplo, cuando antes estábamos hablando de tecnologías emergentes, la GDPR afecta en mayor o menor media en diferentes aspectos: el derecho al olvido en Blockchain, las transferencias de datos internacionales en Cloud, las decisiones automatizadas en la Inteligencia Artificial o el tratamiento masivo de datos en el Big Data.

> "Uno de los grandes retos es la evolución y sofisticación de los ataques informáticos, cada vez más dirigidos y mejor ejecutados"

Por último, la privacidad ha tenido un efecto más sutil, pero no menos influyente en el mundo de la seguridad. Hasta ahora, si una tecnología de seguridad se consideraba como buena para mitigar riesgos, se implementaba; pero tras la llegada de las regulaciones de privacidad a diversas partes del mundo es necesario asegurar que dichas tecnologías cumplen con la regulación. Por ejemplo, las tecnologías de detección de anomalías en el comportamiento de usuarios, que permitían detectar si una cuenta de usuario había sido comprometida, ya no podrán ser implementadas si no garantizan los derechos y libertades en materia de protección de datos.

Tras un año de pandemia, ¿qué han aprendido los CISOs del sector financiero?
La enseñanza fundamental es que la seguridad no se puede poner en ERTE. En una situación como la que nos está tocando vivir hay que entender que el riesgo cibernético, lejos de reducirse, ha aumentado. Estamos viendo a través de los medios de comunicación como el cibercrimen está atacando multitud de empresas privadas y administraciones públicas con ataques de tipo ransomware, incluyendo infraestructuras críticas. Además, durante esta crisis ha sido necesario tomar decisiones transcendentes en un plazo muy breve de tiempo, como la de tener que poner centenares de miles de trabajadores españoles a teletrabajar de la noche a la mañana. Estas decisiones, necesarias para la continuidad de negocio, si no son acompañadas por medidas de ciberseguridad que mitiguen los riesgos del nuevo escenario, pueden tener efectos adversos. De igual forma, los servicios bancarios online han pasado de ser una mejora a ser una necesidad, por lo que garantizar su continuidad y fiabilidad 24 horas al día frente a ataques es una de las prioridades.

Es necesario concienciar a la sociedad sobre el peligro real que supone el cibercrimen y hasta donde está dispuesto a llegar. Hemos visto como en los peores momentos de la pandemia han sido atacados los sistemas de información de algunos hospitales.

¿Qué tecnologías de seguridad considera imprescindibles para una empresa perteneciente al sector financiero?
Todas las tecnologías de prevención de fuga de datos son esenciales para evitar la filtración ac-

"El sector financiero es el más regulado desde hace muchos años, teniendo que cumplir con numerosos requisitos de información y reporting a agencias y bancos centrales de todo el mundo"

cidental o intencionada de información sensible. Es fundamental que estas estén integradas en los canales de comunicación con el exterior para monitorizar y bloquear las transferencias de datos sospechosas. Debemos asegurar que cubren todos los canales, no solo el email sino la subida de información a través de servicios web, la extracción de información a través de los puertos del ordenador e incluso también la impresión.

Dicho esto, se debe tener en cuenta que estas tecnologías son inútiles si no se definen e implementan las políticas adecuadas de identificación y bloqueo de contenidos y, para esto, el equipo de ciberseguridad no puede trabajar de forma autónoma, necesitará de la colaboración del negocio y otras áreas. Además, hay que asegurar que se dispone de un equipo de profesionales de seguridad cualificado para analizar y responder a las alertas emitidas. Sin políticas y profesionales, la tecnología DLP tendrá las mismas capacidades de mitigación del riesgo cibernético que instalar un jarrón en nuestro centro de datos, eso sí, muy caro.

Existen muchas otras que son esenciales bajo mi punto de vista, como las tecnologías y servicios para proteger frente a ataques de denegación de servicio, la protección frente al malware, el cifrado, la protección del perímetro, y los cortafuegos de aplicación y bases de datos.

¿Qué tecnologías que todavía no están ampliamente adoptadas, cree que serán imprescindibles en los próximos años?

En los últimos tiempos han aparecido nuevas posibilidades tecnológicas para la protección de los datos que deben ser exploradas por las entidades financieras para mitigar, aún más, los ciber-riesgos asociados a estos. La información es almacenada por las organizaciones en dos formatos: de forma estructurada, como por ejemplo las bases de datos; y de forma no-estructurada, como por ejemplo las hojas de cálculo.

En lo relativo a la protección de la información estructurada, a las técnicas tradicionales de anonimización y pseudo-anonimización, ampliamente empleadas como la tokenización o el masking, se unen nuevas alternativas como el uso de la encriptación homomórfica o los datos sintéticos. Es importante disponer de un portfolio amplio y contrastado de estas técnicas, puesto que no hay ninguna de ellas que, de forma individual, pueda cubrir todos los casos de uso del negocio.

Cuando hablamos de información no estructurada la situación es todavía más compleja, puesto que existen numerosos ficheros que son intercambiados diariamente como parte de la operativa normal del negocio financiero en interacciones internas y externas. Para esto es necesario implementar tecnologías que nos permitan garantizar la seguridad de los datos durante todo su ciclo de vida, siendo especialmente importantes las tecnologías de descubrimiento de la información y clasificación de los datos. Son también muy interesantes las tecnologías denominadas genéricamente como IRM, que nos van a permitir insertar las políticas de seguridad dentro del dato (control de acceso, trazabilidad, caducidad...), disponiendo de esta forma de la capacidad de proteger la información con independencia de dónde se ubique. ■

MÁS INFORMACIÓN

BNP Paribas

Más visibilidad.
Más potencia.
Más control.

¿No pensó estar preparado/a para el EDR?
Ahora lo está.

go.kaspersky.com/es_optimum

kaspersky PREPARADOS PARA EL FUTURO

Objetivos de la ciberseguridad en las entidades financieras:

protección de clientes, dispositivos y empresa ante los ataques

EUSEBIO NIEVA,
director técnico de
Check Point Software para España y Portugal

La ciberpandemia es uno de los peligros que actualmente están amenazando a cientos de compañías. Tras los meses en los que la Covid-19 ha obligado a miles de personas a extremar las precauciones para evitar el contagio y el uso del pago por móvil o la tarjeta de crédito se han instaurado como opciones masivas. Por ello, las entidades financieras se están convirtiendo en uno de los principales objetivos de los ciberataques, sobre todo, por el rédito económico que puede llegar a reportar el atacarlas.

Desde el comienzo de la pandemia, empresas de todos los sectores se han visto obligadas a implantar el teletrabajo con el consecuente incremento de los dispositivos móviles conectados a la red, aumentando considerablemente las brechas de seguridad y mejorando las oportunidades de éxito de los cibercriminales. Los frentes para los negocios se multiplican y contar una buena defensa es la única opción.

Debido a la situación, ahora se están llevando a cabo diferentes tipos de fraude y extorsión contra la banca, para de esta forma vulnerar la privacidad de estas compañías con el objetivo de llenarse los bolsillos. Así los datos respaldan la realidad del sector, ya que según Informe Global de Amenazas DNS 2020 elaborado por IDC de la mano de EfficientIP, en el 2020 cuatro de cada cinco empresas del ámbito financiero (79%) sufrieron más de diez ciberataques DNS a lo largo del año y cada uno de ellos supuso un coste de 1,16 millones de euros de media.

Uno de los mayores desafíos que tienen que afrontar las entidades financieras es la

seguridad móvil, tanto por el lado usuario como por el de sus trabajadores. Ahora más que nunca, el acceso a redes corporativas a través de móviles no securizados es un objetivo. Para ello, Check Point Harmony Mobile protege los dispositivos móviles de los empleados de todos los vectores de ataque (aplicaciones, red y sistema operativo). Este software está diseñado para reducir los gastos generales de los administradores y aumentar la adopción del usuario, escala rápidamente, evita descargas de aplicaciones maliciosas, impide el phishing en todas las aplicaciones previene ataques Man-in-the-Middle, bloquea aparatos infectados para que no accedan a aplicaciones corporativas y detecta técnicas avanzadas de jailbreaking y rooting y vulnerabilidades del sistema operativo.

En la otra cara de la moneda encontramos cómo estas entidades financieras pueden proteger a sus clientes, sus credenciales y datos personales cuando acceden a sus apps. La mejor manera de mantenerlas a salvo de los cibercriminales es contar con una protección adecuada. Impulsado por el motor de IA contextual de Check Point CloudGuard, Check Point CloudGuard AppSec es una solución que bloquea los ciberataques contra las aplicaciones, incluyendo: la desconfiguración del sitio web, la fuga de información y el robo del inicio de sesión del usuario. Para ello, es capaz de analizar cada solicitud en su contexto y asignándole una puntuación de riesgo, para una prevención precisa, eliminando los falsos positivos y evitando los más sofisticados ataques contra una aplicación, incluidos los ataques OWASP Top 10.

> “Todas las empresas pertenecientes al sector de la banca deben contar con software de protección en el total de sus emplazamientos y en todos los dispositivos que tenga conexión a su red”

Es imprescindible señalar que la banca debe contar con un software que sea capaz de proteger a la empresa de cualquier tipo de ciberataque a sus centros de datos. Esta herramienta debe mantener a salvo todos los archivos, documentación y datos pertenecientes a la propia sociedad y también de los clientes que forman parte de la misma.

Para lograr el objetivo, en Check Point Software contamos con Check Point Quantum Maestro, una solución que posibilita a las compañías ampliar fácilmente sus gateways de seguridad bajo demanda y crear nuevos servidores y recursos informáticos en la nube pública. Además, este software permite que un solo gateway se extienda hasta alcanzar la capacidad y el rendimiento de 52 en cuestión de minutos, lo que proporciona flexibilidad dinámica y un rendimiento máximo del firewall Terabit/segundo. Esta escalabilidad casi ilimitada permite soportar la alta velocidad de datos y contar con la latencia ultra baja de las redes 5G, una red que lo va a cambiar todo desde este mismo año y que será clave para todas las entidades financieras. Asimismo, hay que destacar el hecho de que llega a proteger a los entornos más extensos y con más recursos, estableciendo nuevos estándares en la seguridad de redes a hiperescala. Finalmente, es importante especificar que Check Point Quantum Maestro tiene la habilidad de extender las capacidades de seguridad Gen V de nuestra arquitectura Check Point Infinity a los entornos de hiperescala.

Si algo ha quedado claro en este último año es que todas las empresas pertenecientes al sector de la banca deben contar con software de protección en el total de sus emplazamientos y en todos los dispositivos que tengan conexión a su red para mantener a salvo todos los datos confidenciales que manejan frente a los posibles ciberataques. ■

Salvaguardar las transacciones, proteger al usuario

El financiero es uno de los sectores más afectados por los ciberataques avanzados, ahora muy enfocados en la banca móvil. Proteger al usuario frente a estas amenazas es imperativo, pero sin descuidar otros vectores, como la red SWIFT o los cajeros. La ciberseguridad de la banca debe evolucionar en la misma medida en que lo hacen los servicios.

A causa de los desafíos ligados a la pandemia el uso de la banca móvil se ha incrementado, y con ello el aumento de las ciberamenazas dirigidas contra los dispositivos móviles. Ante esta realidad, Eusebio Nieva, director técnico de Check Point, explica la importancia que tiene para estas entidades desarrollar una estrategia de ciberseguridad que englobe también este canal, con la integración de soluciones avanzadas de ciberseguridad móvil en sus apps.

En Check Point trabajan con varias entidades bancarias a las que proporcionan sus servicios de seguridad en forma de un interfaz de programación de aplicaciones (API) o de un kit de desarrollo de software (SDK) que se pueda consumir. Con esto se consigue trasladar la seguridad al dispositivo desde el cual el usuario está accediendo a los servicios, pero en vez de instalarla en dicho terminal, se pone a disposición de las entidades bancarias, de modo que cuando ellos lancen su propia aplicación de consumo o de servicios bancarios esta estará asociada a los servicios de seguridad de Check Point.

Otra consecuencia de la evolución hacia una banca más móvil, y en general más digital, es que el uso de cajeros automáticos (ATM) ha descendido, al igual que el empleo de efectivo. Hoy en día, y a causa de la pandemia, el dispositivo ubicuo que casi todo el mundo utiliza para hacer pagos es un terminal móvil o una tarjeta de crédito o débito. Sin embargo, y aunque el uso de ATM se ha reducido, lo cierto es que aún se siguen produciendo ataques contra dichas máquinas, por lo que es necesario seguir invirtiendo en su protección. Asimismo, hay que tener en cuenta que la tecnología que integra el cajero es muy antigua, por lo que es trascendental ir actualizando los servicios proporcionados por el cajero, así como la tecnología asociada a los mismos.

Además de no descuidar la defensa de los cajeros automáticos, las instituciones financieras que utilizan el sistema de pagos SWIFT también deben permanecer vigilantes. Las ofensivas contra esta red se han multiplicado en los últimos años, por lo que los bancos están implementando no solo medidas de seguridad estándar, sino también protecciones avanzadas, tecnologías de análisis de fraude, machine learning… para disuadir a los atacantes sobre su explotación, y frenar o impedir las transacciones fraudulentas o los intentos de falsificación de esas transacciones en la red de comunicaciones financieras. Nieva distingue que la tecnología de protección de las tarjetas bancarias o de los dispositivos móviles aún no está a la par con la tecnología de ataque utilizada por los ciberdelincuentes. En este sentido, sería necesario que nuevas metodologías o herramientas entraran en funcionamiento a fin de asegurar las transacciones, sobre todo desde el punto de vista del usuario que es quien las realiza. Con ello se podrían evitarse los fraudes y los ataques a dispositivos móviles con troyanos bancarios, con troyanos de tarjeta de crédito, etc. que pueden ser utilizados contra los usuarios. Por tanto, esta evolución paralela de servicios y ciberseguridad debe ser prioritaria.

Protegeré las claves, protegeré las claves, protegeré las claves…

JAVIER SANCHEZ FUERTES,
Territory Sales Manager,
Data Protections Solutions Entrust

Las empresas de servicios financieros se enfrentan a desafíos únicos en sus esfuerzos por proteger la información sensible de los clientes y cumplir con las regulaciones en evolución. El Repositorio de Confianza es fundamental aquí. La identificación y la autorización de los dispositivos, el cifrado y la verificación de los datos y las actualizaciones del software tienen algo en común, y ese denominador común es la criptografía. Y la base de la criptografía son las claves de cifrado que se necesitan para firmar y validar los certificados de los dispositivos para su identificación y autorización.

La mayoría de la infraestructura desplegada en los servicios financieros utiliza claves para el correcto desarrollo de sus funcionalidades, y en la mayoría de los casos esas claves carecen de la protección adecuada.

Por lo tanto, asegurar estas claves es fundamental, y ahí es donde entra en juego el Repositorio de Confianza para proteger y gestionar las claves de cifrado a lo largo de su ciclo de vida, completamente separadas del resto del sistema con hardware robusto y controles duales para garantizar que ningún individuo o entidad pueda subvertir las políticas establecidas para el uso de las claves.

De esta manera nuestros Hardware Security Module (HSM) nShield forman parte de esta ecuación. ¿Cómo se traduce esto en el mundo financiero?

Los certificados digitales son la forma en que las diferentes partes del ecosistema de pagos establecen la confianza entre sí. Estos certificados suelen ser emitidos por una PKI que se apoya en un Repositorio de Confianza. En la raíz de una PKI se encuentran claves criptográficas fuertes y de confianza creadas en un Hardware Security Module o HSM. Los HSM de Entrust nShield proporcionan una garantía sólida y certificada a un despliegue de PKI al tiempo que facilitan la automatización de la renovación de certificados y firmas, manteniendo las claves criptográficas privadas en un entorno seguro. Pueden desplegarse en otras áreas del nuevo ecosistema de pagos allí donde se requieran servicios criptográficos desde un entorno seguro y de confianza.

Piense en monedas virtuales, seguros, préstamos, grandes minoristas, aplicaciones bancarias móviles, etc. Los HSM de uso general pueden realizar tareas como la protección y validación del PIN, y la gestión de claves, también se despliegan como parte de las soluciones de procesamiento de pagos y puntos de venta móviles con partners de la industria. No olvidando la protección de las claves de firma y el proceso de firma de código de las Apps, el elemento de relación principal entre cliente y entidad financiera.

> “Las empresas utilizan diariamente miles de claves en sus procesos de negocio que deben protegerse de forma conveniente y evitar que sean comprometidas”

Están surgiendo nuevos servicios de pago al realizar compras en línea o a través del teléfono móvil, especialmente en Europa. El cambio puede ser un resultado directo de la PSD2, la última Directiva de Servicios de Pago. Las organizaciones de servicios financieros se enfrentan a desafíos únicos en sus esfuerzos por proteger la información sensible de los clientes y cumplir con las normativas en evolución. Merece la pena recordar que la certificación de los HSM de nShield según NIST FIPS 140-2 y Common Criteria ofrece a los clientes la garantía de que están seleccionando un producto validado según algunas de las normas de seguridad más rigurosas.

Las organizaciones financieras también siguen adoptando tecnologías nuevas y emergentes, como la nube y los contenedores, que, si bien ofrecen posibles eficiencias y reducciones de costes, amplían la huella digital de la organización. Estas organizaciones necesitan tener el control sobre las claves de cifrado que utilizan los proveedores de nube pública y de esta manera será Entrust con el cliente quienes definan las políticas y permisos asociadas a las mismas. No es una cuestión de confianza sobre los proveedores de nube pública sino de control sobre los datos y a afrontar sus retos de seguridad en la nube.

Uno de los principales obstáculos para la adopción más amplia de Blockchain es la seguridad. A medida que las organizaciones continúan encontrando nuevos e innovadores casos de uso para Blockchain, la seguridad debe incorporarse desde el principio. Entrust ayuda a abordar los desafíos de seguridad fundamentales asociados con las implementaciones de Blockchain: creación de claves, protección del proceso de firma y protección de la lógica de consenso. Debido a que se encuentra alojado dentro de los límites seguros del HSM nShield, CodeSafe ofrece protección certificada FIPS 140-2 Nivel 3 para su código más confidencial.

En definitiva, las empresas utilizan diariamente miles de claves en sus procesos de negocio que deben protegerse de forma conveniente y evitar que sean comprometidas con los consecuentes riesgos que eso significa. ■

Proteger la clave para salvaguardar el dato

Los desafíos de la regulación y el cumplimiento de la seguridad de los datos son muy altos en el entorno financiero. Por ello y a medida que evolucionan las amenazas cibernéticas, la combinación de integración tecnológica y análisis avanzado es más necesaria nunca.

Por la naturaleza de su negocio, las compañías financieras siempre han tenido que ser pioneras en cuanto al uso de medidas de seguridad, y en concreto en lo que se refiere al uso de cifrado y de Módulos de Seguridad de Hardware (HSM). Ahora, cuando la digitalización avanza rápidamente y la información fluye por distintos entornos (local, cloud, IoT) esto es más importante que nunca. Sobre ello, Javier Sánchez Fuertes, Territory Sales Manager de Entrust, observa que esa actitud pionera sigue manteniéndose, y lejos de quedarse anclada en el medio de pago, ha ido extendiéndose a otros casos de uso dentro del mundo financiero, para, por ejemplo, la protección de la infraestructura de clave pública (PKI), de los procesos de firma electrónica o de los procesos de negocio, entre otros.

Por otro lado, se habla mucho de la seguridad de los datos de manera genérica, pero hay un aspecto específico que es la seguridad de los datos en reposo que a veces pasa desapercibida. ¿Cuál es el reto en estos casos?

Sobre su importancia, Javier Sánchez cree en las empresas en general y en las financieras en particular se realizan importantes inversiones para proteger el entorno de red o el endpoint, abandonando en muchas ocasiones al dato, que por sí mismo no puede defenderse. El desafío, por tanto, pasa por identificar cuáles son los datos críticos para una entidad financiera y, sobre ellos, aplicar medidas de cifrado y por supuesto de protección de las claves. No hay que olvidar que las políticas de cifrado son tan seguras como lo son la protección de las claves.

Parece que la tecnología de cadena de bloques, Blockchain, está llamada a transformar el mundo de la banca. Sin embargo, el despliegue de servicios financieros sobre esta tecnología presenta retos en cuanto a seguridad. A este respecto, Javier Sánchez explica que la adopción de Blockchain en el mundo de la banca debe hacerse con cuidado. Los clientes depositan su dinero en un banco porque confían en dicha entidad.

En este sentido, Javier Sánchez explica que en Blockchain cada transacción que se envía a un bloque va firmada y por ese motivo lleva asociada una clave, y como hay una clave necesariamente debería haber un Módulo de Seguridad de Hardware (HSM). Desde Entrust lo que se propone es la protección de esas claves criptográficas y de esos procesos de firma, incluso de consenso, para que se realicen de forma segura mediante el uso de HSMs.

Además de trabajar en la seguridad y privacidad de Blockchain, las organizaciones financieras deben cuidar y conservar también sus claves, que están más desamparadas. En este contexto, y a raíz del crecimiento de la banca digital y móvil, el número de transacciones a través de estos medios se ha multiplicado. Por ello, Javier Sánchez incide también en lo crucial que resulta salvaguardar la clave utilizada para firmar el código de una app bancaria. Es más, teniendo en cuenta que la aplicación es, al final, el instrumento de relación entre el banco y los clientes, extremar las medidas de seguridad para resguardar esta aplicación no es baladí. De hecho, hoy por hoy, es su principal herramienta de negocio, por lo que hay que custodiarla.

La amenaza del malware financiero

se mantiene constante en España

ALFONSO RAMÍREZ,
director general
Kaspersky Iberia

La seguridad financiera es una de las preocupaciones más comunes tanto para los usuarios finales como en el mundo empresarial. Y es que las ciberamenazas en este campo son cada vez más peligrosas, y afectan al bienestar económico de las víctimas, ya sean individuos u organizaciones.

Según señala nuestro último informe anual sobre Ciberamenazas financieras en 2020, España fue el tercer país del mundo y primer país europeo con mayor incidencia de amenazas financieras el año pasado. Los troyanos bancarios, que suelen emplear ingeniería social para engañar al usuario y que los descargue, implica que cualquiera pueda encontrarse en el buzón de entrada de su correo, su WhatsApp o su lista de SMS con mensajes maliciosos que pretenden infectarlo.

De hecho, la incidencia de los virus informáticos diseñados para robar credenciales bancarias se sitúa entre las principales amenazas que afrontan los usuarios en Internet y el correo electrónico es el vector de ataque más habitual. En el mismo los cibercriminales se hacen pasar por una empresa (banco, empresa de envíos…) o por un organismo oficial (la Agencia Tributaria, Correos, DGT…).

Otro de los enfoques habituales utilizados por los atacantes para obtener acceso a las cuentas de los usuarios incautos es asumir el papel de "rescatador", fingiendo ser expertos en seguridad. Los atacantes llaman a los clientes de los bancos haciéndose pasar por expertos de seguridad e informan de cargos o pagos sospechosos para posteriormente ofrecer su ayuda. Bajo ese disfraz, el atacante puede pedir a los clientes

“La clave reside tanto en la protección como en la concienciación, de manera que los distintos ataques a los datos financieros no lleguen a causar daños”

que verifiquen su identidad mediante un código enviado en un mensaje de texto o una notificación push, que detengan una transacción sospechosa o que transfieran dinero a una “cuenta segura”. También pueden pedir a la víctima que instale una aplicación para la gestión remota fingiendo que es necesaria para la resolución de problemas. Los estafadores suelen presentarse como empleados del mayor banco de la región de la víctima potencial y utilizan un identificador de llamadas falsificado para las llamadas entrantes para hacerse pasar por un banco real.

Un tercer caso clásico es aquel en el que los ciberdelincuentes actúan como “el inversor”. En este caso, los estafadores se hacen pasar por empleados de una empresa de inversión o por asesores de inversión de un banco. Llaman a los clientes ofreciéndoles una forma rápida de ganar dinero invirtiendo en criptomonedas o acciones directamente desde la cuenta del cliente, sin tener que personarse en una sucursal bancaria. Como requisito previo para prestar el “servicio de inversión”, el falso inversor pide a la víctima el código recibido en un mensaje de texto o en una notificación push. El objetivo final siempre es el mismo: engañar al usuario para que haga ‘clic’ y descargue el código malicioso en su equipo. A partir de ese momento, los ciberdelincuentes tienen acceso a la información.

En este tipo de ataques el objetivo principal suelen ser las credenciales bancarias, que luego se venden en la darkweb por precios realmente bajos. Datos de tarjetas de crédito, acceso a servicios bancarios y de pago electrónico son mercancía habitual en este tipo de mercados.

Ante este panorama, la clave reside tanto en la protección como en la concienciación, de manera que los distintos ataques a los datos financieros no lleguen a causar daños. Así, para ayudar a los particulares y a las empresas a estar protegidos frente a las técnicas de fraude en constante evolución, es importante adoptar una serie de medidas básicas como, por ejemplo, limitar el número de intentos para realizar una transacción, de manera que los ciberdelincuentes no pueden intentar introducir varias veces las credenciales. Otra recomendación que muchas entidades financieras ya han puesto en marcha es informar de forma periódica a sus clientes sobre los posibles trucos que pueden utilizar los ciberdelincuentes, con información para saber cómo identificar el fraude y la mejor manera de comportarse ante estas situaciones.

En cuanto a las medidas de protección, la recomendación es realizar auditorías de seguridad y pruebas de penetración anualmente con el fin de detectar problemas de seguridad en la red de la empresa, contar con un equipo de análisis de fraudes capaz de encontrar y analizar los métodos emergentes que utilizan los defraudadores, implementar la autenticación multifactor para minimizar la posibilidad del robo de cuentas e instalar una solución de prevención del fraude que pueda adaptarse rápidamente para identificar nuevos esquemas y métodos de ataque. ■

MÁS INFORMACIÓN

Todo sobre EDR y MDR

Inteligencia de amenazas para prevenir el fraude

En línea con su evolución tecnológica, el sector de los servicios financieros es un objetivo esencial para los ciberdelincuentes y soporta gran parte de sus ataques. Es por eso que las entidades financieras no deben bajar la guardia. Sobre este aspecto, Luis Javier Suárez, Presales Manager de Kaspersky Lab, destaca que se vienen observando una serie de tendencias dirigidas a integrar metodologías basadas en agile, en la constante evolución de los aplicativos, y que, aunque en ocasiones incluyen la seguridad en el punto inicial, no siempre es así. Por ello, es crucial no descuidar la protección y seguir estrategias DevSecOps que siempre tienen la seguridad en mente.

A esta problemática se unen otros asuntos como la heterogeneidad de sistemas o la persistencia de sistemas legacy, que contrastan con nuevos desarrollos y la evolución hacia otros entornos como cloud. Sobre la nube, Luis Javier Suárez cita la falta de visibilidad como un inconveniente acuciante, ya que no tener conocimiento de lo que allí ocurre puede derivar en peligros como el Shadow IT.

El ritmo de evolución de las tecnologías también tiene que ser tenido en cuenta, sobre todo, porque es bidireccional. Bajo esta premisa y para poder contrarrestar ataques cada vez más sofisticados, es importante contar con servicios o programas de inteligencia de amenazas que ayuden a identificar y analizar las ciberamenazas dirigidas contra la empresa.

Sin embargo, añadir mayor seguridad puede perjudicar la experiencia del usuario, algo que en este sector es muy importante. ¿Cómo se puede aplicar seguridad sin impactar en la experiencia de usuario?

Para Luis Javier Suárez transformar la seguridad en algo que no sea invasivo e incómodo para la experiencia del usuario es complicado, máxime cuando desde el punto de vista de gestión de proyectos se pone mucho foco en esta experiencia. En este sentido, observa que existe una tendencia en el mercado hacia la integración de plataformas o entornos que sean Secure by Design, los cuales, por otra parte, sería conveniente acompañar también de un ciclo de adopción y mantenimiento. Además, no hay que olvidar que la integración de nuevas tecnologías puede traer consigo nuevos vectores de ataque y que tanto el actual auge del comercio electrónico como la preponderancia del cliente como eje central de la experiencia (customer centric) hacen necesaria la existencia de sistemas para apoyar esa seguridad. También debe haber una capa de información (sistemas antifraude) que permita detectar posibles campañas a fin de poder actuar en la fase más temprana.

A raíz de la creciente digitalización y teniendo en cuenta la sensibilidad del activo que aquí se gestiona, el dinero, Luis Javier Suárez valora que, aunque no habrá grandes cambios en cuanto a técnicas de ataque, si se incrementarán las campañas de ransomware dirigido, ataques contra cajeros automáticos (ATMs) y otros fraudes derivados del aumento de los canales digitales. El auge del mercado cripto también traerá consigo campañas focalizadas, desde phishing a otras más sofisticadas.

Por ello, y para asegurar la protección de sus activos, Luis Javier Suárez incide en la importancia de la concienciación de empleados y usuarios, y en la resiliencia. En este contexto, recomienda la adopción de tecnologías Endpoint Detection and Response (EDR), que permiten tener una visibilidad extendida de lo que ocurre dentro del entorno, y también la implantación de un Plan de Respuesta a Incidentes para, llegado el momento, poder aplicar una serie de medidas para contrarrestar el incidente. Este plan ayudará a alcanzar un nivel mayor de resiliencia.

Pagos, transacciones y dinero digital:

una realidad que ha venido para quedarse

JESÚS RODRÍGUEZ,
CEO Realsec

Hace algo más de un año todo cambió en nuestras vidas y un claro ejemplo de ello es la diferente forma en la que hoy compramos y hacemos uso de los medios de pago, donde la transformación digital es la protagonista de esta nueva situación social y económica.

Todo esto, se evidencia en diferentes acciones como el incremento de las compras a través de los sistemas de comercio electrónico, cuyo crecimiento, durante 2020 en España, ha sido de un 67% junto con la proliferación de la banca electrónica y la banca móvil, que ha pasado de un 44% a un 57% en su ratio de uso. Así mismo, se ha multiplicado el uso de las Apps de pago sobre teléfonos móviles, lo que se conoce como Open Banking (Amazon Pay, Samsung Pay…), las tarjetas virtuales prepago, los sistemas wallets, los pagos contactless, el Internet de los Pagos (IoP) a través de dispositivos inteligentes conectados en la red de Internet de las Cosas y la tokenización de las tarjetas. Todo ello, sumado a una gran expansión de nuevos agentes financieros como las Fintechs y la consolidación de las "finanzas descentralizadas" o DeFi, donde tienen su origen las criptomonedas, los smarts contracts y las Apps construidas en tecnología Blockchain.

El número de transacciones de este nuevo ecosistema financiero digital representa un porcentaje superior a las operaciones de pago en efectivo, cuyo descenso en 2020 se cuantifica en un 45%, aunque no debemos olvidar que, para su efectividad, transparencia y confianza, es fundamental implementar una securización robusta.

“Esta nueva economía requiere avanzar hacia una situación en la convivan el dinero fiduciario y las monedas digitales en un marco regulado y ordenado por los Bancos Centrales”

El riesgo de fraude online crece, exponencialmente, asociado al crecimiento de los medios de pagos digitales; es por ello, que las entidades financieras necesitan reforzar la seguridad implementando medidas como la autenticación de doble factor en base a la Directiva PSD2 o mayor transparencia y gobernanza en el caso de utilizar tecnologías como Blockchain para realizar pagos digitales transfronterizos, operaciones de compensación bancaria o intercambio de cédulas de pago internacional. Así como en la gestión confiable de los cripto-activos o la securización de los entornos de pago asociados al Internet de las Cosas “Blockhain of Things”

Aunque hoy la tecnología disruptiva Blockchain por inmutabilidad, descentralización y transparencia puede considerarse confiable para determinados procesos de negocio, podemos robustecerla, en el ámbito financiero, con la implementación de módulos criptográficos HSM (Hardware Security Module) que fortalecen la infraestructura de la red Blockchain, ya sea ésta pública, privada o híbrida, tanto para las operaciones financieras, gestión de criptomonedas y la protección de otros procesos de negocio.

El crecimiento de los pagos digitales en más de un 30%, a nivel mundial durante el último año, junto con los nuevos canales digitales, en detrimento del uso del efectivo, sumado a la proliferación de las monedas digitales (CBDC) y criptodivisas en un mercado no regulado (salvo excepciones como el caso del e-Yuan chino, pero con anuncios y expectativas de una futura regulación por parte de muchos Bancos Centrales del mundo, como el BCE con la creación de Euro Digital) supone asumir la realidad de una nueva economía. La que muchos denominan “Cripto-economía”, puesto que aquí la criptografía desempeña un papel clave para la protección y la seguridad de los activos financieros que traerá consigo una mayor adaptación y confianza, tanto a los usuarios del nuevo espectro digital como a las entidades financieras, interesadas siempre en minimizar los riesgos de seguridad en los medios de pago, como la suplantación de la identidad o el fraude.

Sin duda, esta nueva economía requiere avanzar hacia una situación en la convivan el dinero fiduciario y las monedas digitales en un marco regulado y ordenado por los Bancos Centrales en el que las nuevas tecnología disruptivas, como el Blockchain, cumplan con los mismos o superiores niveles de exigencia, en materia de seguridad, a los exigidos por la Banca, como es el uso una criptografía robusta para proteger las transacciones financieras, avalada por un organismo acreditado internacionalmente, como la Certificación PCI HSM PTS en el ámbito de los medios de pago.

Para conocer más sobre la situación y el estado del arte de esta tecnología en España y América Latina les animamos a leer el II Informe de Blockchain de REALSEC, elaborado junto con IDC. ■

La ciberseguridad como factor de confianza

El sector financiero se enfrenta a un ambiente regulatorio estricto, con muchas normas que acatar y exigencias en cuanto a protección y seguridad muy explícitas. Tal situación, no obstante, ha favorecido que se haya convertido en uno de los nichos más avanzados en cuanto a ciberseguridad. A este respecto, Jesús Rodríguez, CEO de Realsec, destaca que, si bien antes de la pandemia la banca ya trabajaba en determinados procesos de transformación digital, el confinamiento ha acelerado extraordinariamente este desarrollo. Sin embargo, el crecimiento de la banca electrónica y móvil ha repercutido también en un incremento de los ciberataques y en un mayor riesgo de fraude, activando la demanda de soluciones y sistemas de cifrado para la protección de transacciones y de otros procesos de negocio.

No obstante, Jesús Rodríguez aclara que la banca siempre ha cuidado mucho todo lo relacionado con ciberdelincuencia. Es un factor de confianza, el mayor de todos, por lo que a medida que el nivel de ciberriesgo ha evolucionado, se han ido implantado soluciones de protección para mitigar estas amenazas. Adicionalmente, y en lo que respecta a la parte de medios o sistemas de pago, la tecnología de criptografía bancaria ha prosperado como sistema de protección, al igual que la orientada al tratamiento seguro de las transacciones electrónicas, la protección de la información y de los datos mediante el cifrado.

La usabilidad de la tecnología de blockchain también se ha extendido, y no solo para la gestión de criptoactivos, sino para otros procesos de negocio como la compensación electrónica o los pagos transfronterizos. Sin embargo, esta tecnología debe considerarse, además de por sus capacidades de eficiencia y trazabilidad, por sus características de seguridad. Los bloques pueden ser cifrados y dentro de la tecnología de blockchain se pueden utilizar contratos inteligentes (smart contract).

Aunque fue el año pasado cuando la normativa PSD2 entró en vigor, su acatamiento ha estado posponiéndose durante los últimos años a través de varias moratorias. En ese tiempo, las entidades bancarias han estado preparándose, trabajando en una doble dirección: el desarrollo de APIs, para permitir el acceso a nuevos actores en el ámbito financiero y en la autenticación de doble o triple factor para cumplir con la directiva de pagos PSD2. Al respecto de su acatamiento, y aunque no se puede decir que ningún banco español esté cumpliendo con la directiva en sí, si se puede aseverar que no todas las entidades financieras están utilizando soluciones de tokenización para su observancia. Dichas soluciones han sido reemplazadas por SMSs con una clave adjunta que el usuario utiliza para demostrar que es quién realmente dice ser durante la operación financiera.

La banca está ahora mismo viviendo una situación revuelta; una fase de adaptación. La crisis económica generada por la pandemia está obligando a sus entidades a adoptar una serie de medidas para no perder competitividad y rentabilidad. Así, y aunque los bancos llevan tiempo trabajando en la gestión de activos, en las criptomonedas, se está produciendo una tendencia creciente a cambiar activos financieros y efectivo por criptodivisas. Sobre ello, Jesús Rodríguez considera que según avance la regulación, esta realidad irá asentándose. Previsiblemente se avanzará hacia un euro digital regulado (algo en lo que está trabajando el Banco Central Europeo) y se extenderá la usabilidad del blockchain hacia otros procesos de negocio, como los arriba comentados.

Síguenos en:

SOLUCIONES DE CIBERSEGURIDAD_

- HSM de Propósito General
- HSM Financiero
- Remote Key Load
- Soluciones de Cifrado, Firma Digital y Sellado de Tiempo
- Soluciones PKI
- Ciberseguridad Blockhain&IoT

www.realsec.com

realsec
La clave para proteger su negocio

OFICINAS CENTRALES
C/ Infanta Mercedes 90. Planta 4. 28020 Madrid
Tfno.: +34 91 449 03 30 - E-mail: info@realsec.com

MÉXICO
Avda. Ejército Nacional, 1112 Despacho 404 Piso 4
Colonia Los Morales C.P. 11510. Ciudad de México
Tfno.: + 52 (55) 44 35 00 46 - E-mail: infomexico@realsec.com

USA
303 Twin Dolphin Dr Suite 600 Redwood City, CA 94065
Tfno.: +1 (650) 632 4240 - E-mail: sales@realsec.com

SINGAPUR
REALSEC Inc.12 Marina Boulevard.
MBFC Tower 3. Level 17-01. Singapore 018982
Tel. +65 6809 5001 • infoapac@realsec.com

El sector financiero, en el punto de mira de los cibercriminales

IGOR UNANUE,
CTO S21sec

La ciberdelincuencia es, desafortunadamente, un factor de riesgo para varios sectores como el sanitario, el público o el educativo, pero la industria financiera es y seguirá siendo uno de los sectores más vulnerables a los ciberataques. Desde siempre, el sector financiero ha estado expuesto al cibercrimen, ya que en el 90 por ciento de los casos la motivación de los atacantes es puramente económica. Tal y como detectamos en 2019, los ataques hacia entidades financieras aumentaron de forma notable y los cibercriminales encontraron vías muy sencillas de penetración en dichas organizaciones a través de simples ataques de ingeniería social vía correo electrónico. Desde entonces, los cibercriminales cuentan con más y mejores recursos.

Este año, además de sufrir el típico malware financiero, el sector financiero podría ser víctima de ataques de robo de información relacionada con credenciales bancarias, datos de tarjetas de crédito o sufrir ataques Zero-Day, donde los cibercriminales se aprovechan de las vulnerabilidades y utilizan códigos maliciosos para desplegar los ataques. Muchas entidades financieras ya cuentan con sus propios sistemas de protección para hacer frente a ataques recurrentes como el phishing o el envío de información falsa mediante correo electrónico. No obstante, hay muchos nuevos software maliciosos que van surgiendo y que no son tan fáciles de identificar.

En este sentido, desde S21sec nos encargamos de monitorizar la actividad de los cibercriminales y de detectar todas las nuevas

“Toda entidad financiera debería contar con un buen sistema de detección para así identificar malware, detectar movimientos laterales o cualquier otro tipo de ataque”

amenazas que puedan afectar al sector financiero. Cada día, se identifican casi 15.000 malware diarios y la clave reside en averiguar a qué tipo de entidades afectan y qué banco en concreto está siendo víctima de dicho ataque. Nos encargamos de recuperar la información robada, además de proporcionar nuestros servicios de SOC y equipos de servicios profesionales que trabajan en proyectos de integración, consultoría o en la parte de auditoría. La consultoría en entidades financieras es muy importante debido al cumplimiento normativo que les impone implantar medidas de seguridad.

Otro aspecto a tener en cuenta es que debe haber un equilibrio entre la seguridad y la experiencia del cliente; es decir, añadir mayor seguridad puede perjudicar la experiencia del cliente, y en el sector financiero, no es fácil limitar el acceso mediante seguridad porque las entidades deben seguir funcionando. Además, la pandemia ha impulsado el teletrabajo y el uso de la banca online, con lo que es complicado imponer una seguridad total en este sentido. La única solución al respecto es estar alerta y seguir controlando la seguridad en paralelo, identificando los puntos más débiles que puedan suponer un riesgo para la compañía. En S21sec consideramos que esa es la gestión del riesgo que toda entidad y compañía financiera debe realizar, ya que imponer medidas de seguridad extremas supondría entorpecer el funcionamiento de la compañía, debiendo hacer un esfuerzo por identificar correctamente el punto de entrada más vulnerable para así implantar medidas de seguridad, como por ejemplo establecer reglas de correlación, puntos de control y sistemas preventivos.

No hay que olvidar que los cibercriminales siempre llevan a cabo sus ataques aprovechando las vulnerabilidades de los grandes fabricantes y, por ello, es imprescindible mantener los sistemas parcheados y protegidos para evitar cualquier fuga de información; es algo que el sector financiero debe tener muy claro para protegerse contra los ciberataques. Asimismo, también es importante saber que muchos de los ataques recientes han sido silenciosos y difíciles de detectar porque utilizan nuevos sistemas de ataque, de manera que los ataques son lentos y no se identifican inmediatamente.

Por ello, desde S21sec recomendamos a todo el sector financiero tener un sistema de monitorización constante y estar siempre alerta ante nuevas amenazas. Toda entidad financiera debería contar con un buen sistema de detección para así identificar malware, detectar movimientos laterales o cualquier otro tipo de ataque. Además, también es recomendable que estén al tanto de todo lo que ocurre en las redes, visualizar las vulnerabilidades y tener en cuenta que las entidades financieras estarán siempre expuestas al riesgo de los ciberataques. ■

Seguridad gestionada para mitigar los riesgos

El sector financiero siempre ha estado en el punto de mira de los cibercriminales, dado que, además, en el 90% de las ocasiones estos actores se rigen por una motivación financiera. No obstante, Igor Unanue Buenetxea, CTO de S21sec, reconoce que no es el que sufre el mayor número de ataques, aunque si al que llegan los más tradicionales, como los dirigidos contra sus clientes.

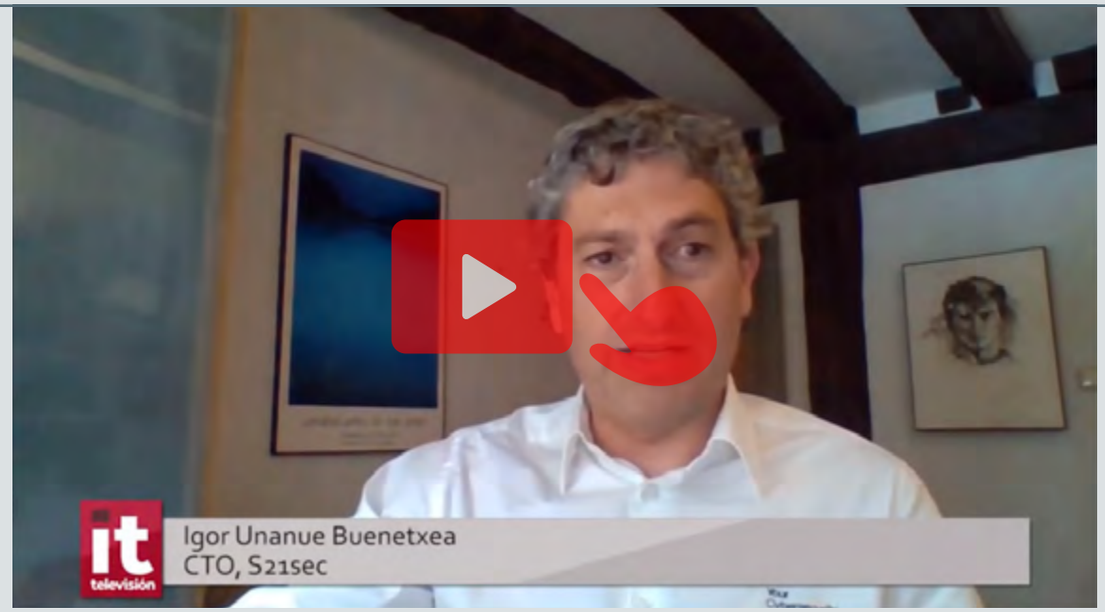
Aunque el malware financiero siempre ha existido y seguirá en activo, desde S21sec consideran que, durante 2021, tendrán mayor relevancia las vulnerabilidades Zero Day y los ataques dirigidos destinados al robo de información (credenciales, datos personales, tarjetas de crédito).

Asimismo, Unanue alerta sobre el cibercrimen bancario, el cual se está expandiendo sin pausa, y al que desde la propia empresa hacen frente a través de la monitorización de los cibercriminales, para no dejar escapar malware nuevo. En este contexto, S21sec analiza diariamente más de 15.000 muestras, lo que le permite averiguar a qué tipo de entidades afecta, incluso un banco concreto. Adicionalmente, S21sec recupera credenciales robados, monitoriza constantemente la Deep Web en busca de tarjetas de crédito e información robada a las entidades financieras (análisis en profundidad continúo). También ofrece servicios de seguridad gestionada en remoto (SOC) 24/7 y cuenta con un equipo de servicios profesionales que trabaja en proyectos de integración, auditoría y consultoría.

Sobre este último, Igor Unanue reconoce que la acción de consultoría es muy importante para este tipo de organizaciones, ya que deben implementar medidas de seguridad concretas para acatar el cumplimiento normativo. Estas, además, deben estar muy bien implantadas, ya que serán auditadas por el Banco Central Europeo (BCE).

No obstante, a veces, añadir mayor protección pueden perjudicar la experiencia del usuario; por lo que el reto está en obtener ese equilibrio para aplicar seguridad sin impactar en la experiencia de usuario

A este respecto, Igor Unanue comenta la dificultad que entraña conjugar ambos aspectos. Limitar el acceso o las comunicaciones con mecanismos de seguridad no es tan sencillo, más si cabe, ahora, con la mayor parte de las plantillas teletrabajando y los clientes operando a través de banca digital. Hay que dejar abiertas ciertas puertas para que la comunicación fluya, la economía funcione, mientras se controla la seguridad, sobre todo en los puntos de mayor riesgo. Para ello es necesario llevar a cabo una monitorización 24/7, desplegar sistemas preventivos, reglas de correlación… En definitiva, aplicar medidas de seguridad optimas sobre ese punto, para monitorizar y no siempre bloquear.



Además de desplegar una estrategia de gestión de riesgo basada en la defensa de los puntos más sensibles, desde S21sec recomiendan vigilar las vulnerabilidades Zero Day que se producen, ya que últimamente se han detectado un alto número en productos de grandes fabricantes (desplegados en organizaciones financieras). En este sentido parchear los sistemas es clave, así como mantenerlos actualizados y monitorizados. También el despliegue de un sistema de detección Endpoint Detection and Response (EDR) para poder detectar movimientos laterales, de malware y otro tipo de ataques en los puestos finales y servidores, además de monitorizar y gestionar todo lo que ocurre en las redes y que les pueda aplicar a ellos como entidades financieras. No en vano, siempre van a estar en el punto de mira de los ciberdelincuentes.

Gestión de la seguridad de los datos en tiempos de crisis para las instituciones financieras

ALFONSO MARTÍNEZ,
Country Manager Iberia, Thales Digital Identity & Security

En una crisis mundial sin precedentes como la de la COVID-19, las organizaciones que han implantado nuevas tecnologías y han elaborado un enfoque coherente de su planificación de la continuidad de la actividad y de gestión de crisis, parecen salir mucho mejor paradas.

Esto es especialmente cierto para las instituciones financieras que ahora se enfrentan a nuevos retos de ciberseguridad debido a la pandemia. Según el último informe Modern Bank Heists, la pandemia de COVID-19 se ha relacionado con un aumento del 238% en los ciberataques contra bancos de todo el mundo.

Dado que una filtración de datos puede afectar significativamente a múltiples funciones dentro de una organización, la protección de los datos debe ser responsabilidad de todos los departamentos, además del equipo ejecutivo, para garantizar la continuidad del negocio sin fisuras.

Para ilustrar esto aún más, a continuación se muestra cómo las brechas de datos pueden afectar a funciones cruciales en una institución financiera:

1. FINANZAS

Según el "Informe sobre el coste de una filtración de datos en 2019" ("2019 Cost of a Data Breach Report ") realizado por el Ponemon Institute, el coste medio de una brecha de datos se cifra en 3,92 millones de dólares a nivel mundial. Esta cifra es testimonio del importante daño financiero que cualquier in-

“La mitigación de los riesgos de los datos depende de las inversiones estratégicas en tecnologías de protección de datos y de la adopción de las mejores prácticas de ciberseguridad”

cidente de brecha de datos puede causar a una organización.

2. LEGAL

La mayoría de las normativas de protección de datos, como el Reglamento General de Protección de Datos (RGPD), el Estándar de Seguridad de Datos del Sector de las Tarjetas de Pago (PCI DSS)... obligan a seguir procesos estrictos para proteger los datos sensibles y prescriben sanciones rigurosas en caso de incumplimiento. El incumplimiento de estos mandatos legales puede costar caro a una empresa, como ha experimentado recientemente el operador de telecomunicaciones italiano TIM, que ha sido sancionado con 27,8 millones de euros por la Autoridad de Protección de Datos italiana, Garante, por incumplimiento del GDPR.

3. LÍNEA DE NEGOCIO (LOB)

Las brechas de datos pueden comprometer drásticamente las aplicaciones empresariales básicas, como los sistemas de gestión de créditos, los sistemas de gestión de las relaciones con los clientes (CRM), los sistemas de bases de datos de tarjetas de crédito/débito, etc. La indisponibilidad de estas aplicaciones críticas (que a menudo son el objetivo de los piratas informáticos) puede causar una pérdida significativa de la confianza de los clientes y del negocio.

En este contexto, es fundamental que las instituciones financieras refuercen su resistencia cibernética con herramientas y soluciones adecuadas.

La mitigación de los riesgos de los datos depende de las inversiones estratégicas en tecnologías de protección de datos y de la adopción de las mejores prácticas de ciberseguridad.

A continuación, se presentan tres mejores prácticas para construir una ciberseguridad sin fisuras para una óptima protección de los datos de la empresa.

1. Cifrar los datos sensibles

Busque en los servidores de archivos, las aplicaciones, las bases de datos y las máquinas virtuales los datos en reposo, y rastree los datos en tránsito que fluyen por la red corporativa entre ubicaciones lejanas. Una vez identificados y rastreados estos datos sensibles, es crítico cifrarlos para hacerlos inútiles a los hackers en caso de un ciberataque.

2. Almacenar y gestionar de forma segura las claves de cifrado

Las claves de cifrado pasan por múltiples etapas a lo largo de su vida: generación, distribución, rotación, archivo, almacenamiento, copia de seguridad y destrucción. Gestionar estas claves en cada etapa de su ciclo de vida a través de una solución de gestión de claves centralizada, es fundamental para la protección de los datos.

3. Implantar políticas sólidas de gestión de accesos

Implemente políticas sólidas de gestión de acceso para evitar el acceso no autorizado a los datos cifrados y a las claves de cifrado. Esto es especialmente importante en condiciones de trabajo remoto, para garantizar que sólo el personal autorizado pueda acceder a los datos sensibles en función de la necesidad de conocerlos.

Thales ha estado a la vanguardia para ayudar a las organizaciones a proteger de forma cohesiva sus datos empresariales, y continuar con la actividad habitual incluso en situaciones de crisis. Las soluciones de cifrado de datos y de gestión de claves de Thales, protegen los datos sensibles en todos los dispositivos, procesos, plataformas y entornos, cumpliendo al mismo tiempo con todos los mandatos normativos. ■

Proteger las claves y la gestión de su ciclo de vida

En un mundo cada vez más digital, el uso de certificados y claves criptográficas es imprescindible y por tanto las entidades financieras tienen que poner el foco en cómo se custodian esas claves, además de en la firma digital de las transacciones.

La banca lleva años embarcada en una evolución tecnológica orientada a la provisión de nuevos servicios de valor añadido que le permitan satisfacer las demandas y mejorar la experiencia de sus clientes, además de reducir costes. El avance de los servicios digitales es palpable, está ahí. Sin embargo, Alfonso Martínez, Country Manager España & Portugal del negocio de seguridad e identidad digital de Thales, advierte que tal desarrollo lleva aparejado un incremento de la complejidad, lo que a veces impide a estas organizaciones asegurarse de que las soluciones de seguridad de la información que implementan son realmente capaces de proteger los datos sensibles, confidenciales, que entran y salen de la entidad.

Al respecto de esta protección, Alfonso Martínez explica que las empresas financieras no deben plantearse si están cifrando bien o mal sus datos, si no, más bien, si tienen desplegada una adecuada estrategia de cifrado. De nada sirve implementar una solución de cifrado muy potente o novedosa si al final las claves criptográficas están expuestas o no están protegidas de manera conveniente. Conviene separar el tesoro de la llave, más aún cuando se está produciendo una creciente orientación a servicios en la nube. En este sentido, es primordial que los bancos mantengan la custodia y la propiedad de esas claves criptográficas con las que están cifrando datos sensibles en la nube.

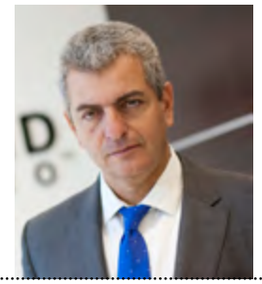
El financiero es un sector hiper-regulado, con muchas normativas a las que hacer frente: PCI DSS, P2PE, PSD2 o GDPR. Sin embargo, Alfonso Martínez explica que además de poner foco en su observancia y en la implantación de soluciones tecnológicas que, como los Módulos de Seguridad de Hardware (HSM), pueden ayudar en su cumplimiento, no hay que pasar por alto otras realidades muy en boga, como el blockchain (con las criptomonedas, los smart contract, IoT) y otras más sencillas, como las facturas electrónicas o el uso de los certificados SSL de los servidores. Al final, en este mundo digital, el uso de certificados y claves es imprescindible, por lo que es muy importante cuidar la forma en que se custodian esas claves y la firma digital de las transacciones.

Sin duda, las entidades financieras no solo se enfrentan a ciberataques, muchos problemas vienen también de las brechas de datos. Sobre ello, Alfonso Martínez especifica que se han visto casos muy cercanos de filtraciones en entidades financieras en las que no solo se han revelado datos bancarios sino también personales (nombre, DNI…). El problema aquí es claro: un número de tarjeta se puede cambiar, pero una identidad u otros datos personales asociados a una cuenta particular es imposible.

Para defender esta información, que también "viaja" a las nubes, ya sea privada, pública o híbrida, Thales propone una estrategia de seguridad que pasa primeramente por descubrir dónde reside la información sensible, por ejemplo, en qué servidores, y de qué tipo de datos se trata (una tarjeta de crédito, una dirección de correo…) para seguidamente proceder a su cifrado. No obstante, ese cifrado hay que asegurarlo poniendo el foco en la custodia de las claves criptográficas y, por supuesto, en una gestión de un ciclo de vida de esa clave para saber a quién pertenece, cuándo ha sido generada o cuando caduca. Se trata, por tanto, de proteger las claves criptográficas y la gestión de su ciclo de vida.

La industria financiera ante nuevos retos y viejas amenazas

JOSÉ BATTAT,
director general de Trend Micro Iberia



En 2020 las ciberamenazas no dieron tregua –la pandemia no ayudó–, y 2021 no está siendo diferente. El cambio de año no ha modificado las ciberamenazas de siempre, implicando que el robo de datos y el ransomware -a menudo en el mismo ataque-, así como el Business Email Compromise (BEC), los troyanos bancarios, el phishing o el malware de minado de monedas sigan copando titulares. Solo en 2020 Trend Micro detectó más de 62.600 millones de ciberamenazas, el 91% de las cuales se originaron en el email. Aunque la mayoría podrían estar vinculadas con ataques automatizados y básicos, podría decirse que son las más dirigidas y personalizadas las que suponen la mayor amenaza para los resultados y la reputación de la empresa.

Algunos sectores pueden verse más afectados que otros este año, pues los ciberdelincuentes siempre van a por el fruto más fácil: las oportunidades de generar el máximo rendimiento de los ataques. Así, aunque bancos y entidades financieras siempre han destacado que la seguridad está entre sus prioridades, el sector y sus clientes siguen estando entre los principales objetivos de los atacantes, a pesar de las nuevas normativas para reforzar aún más la ciberseguridad y la privacidad. Además de las florecientes oportunidades de negocio que han abierto las empresas de e-commerce y tecnología financiera (FinTech), la constante conectividad de los dispositivos móviles inteligentes conectados 24x7 supone para los ciberdelincuentes el acceso para estudiar y observar las lagunas de seguridad, lo que sitúa a los usuarios y a las empresas financieras como

“Los ataques online y offline amenazan constantemente al sector financiero y, a medida que el uso de la tecnología crece y se desarrolla, se presentan simultáneamente más oportunidades de negocio y de ataques”

blancos más fáciles para las transacciones fraudulentas y las brechas.

LA ESTRATEGIA DE SEGURIDAD COMIENZA AQUÍ

Si aún no lo ha hecho, evalúe los ciberriesgos para averiguar cuáles son sus puntos débiles y elabore un plan para solucionarlos.

El enfoque por adoptar dependerá de la predisposición al riesgo de la organización, del sector al que pertenezca y de la madurez de su posición actual de seguridad. Sin embargo, cualquier iniciativa debe incluir formación y concienciación de los usuarios; actividad que debe ser continua e incluir simulaciones de phishing y BEC del mundo real, y debe comunicarse regularmente al personal en pequeños fragmentos. Adapte las sesiones de formación a las últimas campañas de phishing y asegúrese de que sus herramientas ofrecen información detallada sobre las personas para centrarse en los empleados más débiles. Recuerde que todos los empleados, desde el director general hasta el último trabajador, deben asistir, incluidos los trabajadores temporales y los contratistas. Solo hace falta un clic erróneo para meter a la organización en problemas.

Otro enfoque que está ganando en popularidad es el de zero-trust. En un mundo de trabajo distribuido, dispositivos móviles y aplicaciones SaaS, la máxima de “nunca confiar, siempre verificar” se impone. Centre sus esfuerzos en la autenticación de los usuarios con herramientas multifactor (MFA), y despliegue la microsegmentación de red para restringir el acceso a recursos. Este enfoque también se relaciona muy bien con las herramientas SASE basadas en la nube para dar a los equipos de seguridad visibilidad de todo el tráfico entrante y saliente.

Los riesgos asociados a una plantilla distribuida también exigen herramientas de seguridad y gestión de endpoints basadas en la nube para obtener la máxima flexibilidad, visibilidad y control. La detección y respuesta a amenazas adquiere especial importancia, sobre todo las soluciones que incorporan IA para ayudar a los equipos de seguridad a priorizar la forma de hacer frente a los sofisticados ataques entrantes. De hecho, la IA seguirá facilitando la vida de los profesionales de la seguridad al detectar patrones sospechosos en el tráfico de red que los humanos podrían pasar por alto, detectando estilos de escritura anómalos en los emails de BEC y añadiendo automatización a la detección y repuesta.

En definitiva, los ataques online y offline amenazan constantemente al sector financiero y, a medida que el uso de la tecnología crece y se desarrolla, se presentan simultáneamente más oportunidades de negocio y de ataques. Como parte de la “vieja guardia” que se ve obligada por la tecnología a innovar y seguir desarrollándose, la concienciación en seguridad, la vigilancia, la formación y la integridad siguen siendo constantes sólidas en el sector en todo momento. ■

Protección y visibilidad de todos los vectores de ataque

Una mayor conectividad por parte de los usuarios y una evolución hacia una banca cada vez más digital han servido como reclamo para los ciberdelincuentes, que han incrementado el ritmo y la dureza de sus embestidas contra este mercado. Bajo esta situación, José de la Cruz, Director Técnico de Trend Micro, explica cómo la evolución de los ataques y amenazas contra este sector debe ser evaluada desde una doble dimensión.

Desde el punto de vista de TI, con empleados y usuarios interactuando permanentemente con aplicaciones, se aprecia cómo el ransomware ha cobrado una nueva dimensión, con campañas masivas para infectar al mayor número de compañías posible y la subasta de la información sustraída en la Dark Web. Estos ataques son cada vez más diversificados, sobre todo, en cuanto a la tecnología que utilizan para propagarse, y los vectores han cambiado. Así, y aunque el correo electrónico sigue siendo el más utilizado para iniciar un ataque, una vez emprendido este, otros vectores se involucran en el proceso, desde la comunicación a través de las distintas redes hasta la propagación desde endpoints a servidores, cloud, etc.

En lo que respecta específicamente a la banca, las amenazas se dirigen principalmente a tres elementos: infraestructuras, aplicaciones bancarias, y empresas de terceros.

Los cajeros automáticos (ATM) son las infraestructuras más atacadas, y aunque si bien es una tendencia descendente en España, no se debe bajar la guardia. Distinto es cuando se trata de aplicaciones bancarias, con ataques que se dirigen a aplicaciones de uso móvil, y donde el objetivo es el segundo factor de autenticación; y los destinados a los servicios de la entidad expuestos en Internet, aplicaciones y APIs. Por último, destacan las agresiones a la cadena de suministro, donde hay proveedores que interactúan con el banco y que, en muchos casos, no cuentan con las mismas medidas de seguridad.

Además de prepararse para luchar contra estas amenazas, la banca tiene que lidiar también con reglamentaciones como la PSD2, o incluso la futura PSD3. Sobre ello, José de la Cruz confirma que, si bien la PSD2 empezó con brío, por su orientación a fomentar la integración y el pago colaborativo, está empezando a quedarse obsoleta. Y es que, aunque los criterios de colaboración con los que fue creada sí se están cumpliendo, no se puede considerar que exista una homogenización en cuanto a estándares, APIs o modos de colaboración con terceros. En este punto, se espera que la PSD3 establezca una estandarización a nivel de API, lo que implicará además unas condiciones de seguridad más robustas.

A la luz de cómo están evolucionando los ataques y amenazas contra el sector financiero, es vital contar con una visibilidad total de la red, para luchar contra el ransomware; implementar mecanismos de control de dispositivos, de supervisión de integridad, para salvaguardar los ATMs; y optar por un segundo factor de autenticación mucho más robusto, y que no dependa de los SMS, para proteger las aplicaciones móviles.

De igual modo, sería recomendable contemplar el enforcement de políticas de seguridad, a fin de que los usuarios acaten unos requisitos mínimos cuando se conecten con el banco; proteger aplicaciones y containers; y, cuando se trate de cloud, vigilar el CSPM (Cloud Security Posture Management) para el cumplimiento de normativas. Por último, y para defender la cadena de suministro, es clave implementar mecanismos para proteger no solo a la entidad sino también a terceros.

S21 SEC

DFIR

Digital Forensics & Incident Response

¿Sabes cómo enfrentar un incidente grave de seguridad?

No serás juzgado por el incidente, sino por la velocidad en resolverlo.

¡Contáctanos ahora para obtener más información!

marketing@s21sec.com

www.s21sec.com/es/dfir-incidentes-seguridad/

Permitir la productividad en Internet con el más alto nivel de seguridad

La misión de Check Point es "proporcionar a cualquier organización la capacidad de realizar su trabajo en Internet con el más alto nivel de seguridad". Abordan las necesidades de ciberseguridad más inminentes de las organizaciones basándonos en tres principios básicos:

1. Enfoque de prevención en primer lugar: implementar protecciones de usuario preventivas para eliminar las amenazas antes de que lleguen a los usuarios.

2. Gestión Gold Standard: panel único para gestionar todo el patrimonio de seguridad.

3. Solución consolidada: obtenga una protección preventiva completa contra las amenazas más avanzadas mientras logra una mejor eficiencia operativa.

SECURE YOUR EVERYTHING CON CHECK POINT INFINITY

En esta nueva normalidad, permiten a los clientes mantener la productividad mientras permanecen protegidos en todo lo que hacen. Dondequiera que se conecte, a lo que se conecte y como quiera que se conecte: su hogar, sus dispositivos, su privacidad y los datos de su organización deben estar seguros y protegidos de cualquier amenaza cibernética. Para hacer realidad su visión, en 2021 han recalibrado su oferta de productos Infinity para enfocarlas hacia aquellas tecnologías y capacidades que brindarán seguridad sin concesiones basada en estos tres principios básicos.

Check Point consolida más de 80 productos y tecnologías y los ha organizado en tres pilares principales: Harmony, CloudGuard y Quantum, con Infinity-Vision como base.

HARMONY: EL MÁS ALTO NIVEL DE SEGURIDAD PARA USUARIOS REMOTOS

Check Point Harmony protege a los empleados remotos, los dispositivos y la conectividad a Internet de ataques maliciosos, al tiempo que garantiza un acceso remoto seguro y de confianza cero a cualquier escala y en cualquier aplicación corporativa. Check Point Harmony proporciona conectividad segura y de punto final (SASE), como una solución consolidada y unificada basada en la nube que incluye acceso remoto fácil y seguro (basado en la adquisición de Odo), navegación segura por Internet, punto final y seguridad mó-

vil y seguridad del correo electrónico. La solución ofrece la cobertura más amplia de vectores de ataque con la prevención de amenazas impulsada con Inteligencia Artificial.

Harmony presenta tecnologías que admiten entornos híbridos seguros de trabajo desde cualquier lugar (WFA). Asegurar a los empleados en el domicilio se ha convertido en una de las principales prioridades de las organizaciones de todo el mundo. La nueva familia de productos Harmony reúne más de siete categorías de productos para proporcionar una protección preventiva completa para los usuarios remotos. Incluye conectividad segura desde cualquier lugar y un entorno de trabajo seguro en cualquier dispositivo, incluidos los dispositivos móviles, personales y administrados por la empresa, tanto cliente como sin cliente.

CLOUDGUARD: NUBE SEGURA DE FORMA AUTOMÁTICA

CloudGuard optimiza la protección de las cargas de trabajo críticas en la nube, tanto públicas como privadas. Ofrece gestión de la postura en la nube, seguridad serverless y una nueva generación de firewalls de aplicaciones web con tecnología de Inteligencia Artificial contextual que protege las API, las aplicaciones web y los servidores web alojados y on-premise.

CloudGuard proporciona seguridad consolidada y prevención de amenazas en todos los entornos, activos y cargas de trabajo de la nube. Alineado con la naturaleza ágil del desarrollo y la implementación en la nube, CloudGuard ofrece una solución tanto para los profesionales de la seguridad en la nube como para las DevOps en la nube, desde la fase inicial de DevSecOps, pasando por la seguridad de la red en la nube hasta la seguridad de las aplicaciones en la nube (WAAP), así como la protección de contenedores y funciones sin servidor.

QUANTUM: SEGURIDAD DE LA RED EMPRESARIAL PARA EL PERÍMETRO Y EL DATACENTER

En 2021, la compañía seguirá aprovechando Maestro, su solución de rendimiento escalable única y disruptiva. Acelerarán la innovación en el firewall del centro de datos con la introducción de un gateway de firewall súper rápido con un rendimiento de firewall de 200 Gbps y una latencia de menos de 3 microsegundos.

Quantum refleja la solución de seguridad de red más completa para cada organización, perímetro y centro de datos, que abarca IoT Nano-Security hasta superredes Terabit y ofrece los más altos niveles de seguridad y rendimiento para administrar entornos de centros de datos.

Las puertas de enlace de seguridad de Check Point Quantum brindan una seguridad superior más allá de cualquier firewall de próxima generación (NGFW) y están diseñadas para administrar los requisitos de políticas más complejos. Con más de 60 servicios de seguridad, estos gateways previenen la quinta generación de ciberataques.

Además, tienen previsto el lanzamiento de una nueva serie de dispositivos para sucursales y oficinas dirigidos a las pequeñas y medianas empresas: Quantum SPARK.

INFINITY-VISION

Pensada para lograr una gestión de seguridad unificada y un 100% de prevención de brechas de seguridad. Permite la administración todo el patrimonio de seguridad con Check Point Infinity Portal, una gestión de seguridad como servicio (SMaaS) basada en la nube. Entregue políticas, supervisión e inteligencia unificadas desde un solo punto. Exponga, investigue y bloquee los ataques más rápido, con una precisión del 99,9% con las capacidades SOC y XDR utilizadas por Check Point Research. ■

MÁS INFORMACIÓN

- Quantum
- Harmony
- CloudGuard
- Infitiny Vision

Entrust ayuda a las empresas de servicios financieros a mejorar la seguridad de sus datos y el cumplimiento de la normativa

Empresas de servicios financieros de todo el mundo confían en Entrust para abordar sus desafíos de seguridad. Entrust cuenta con una gama de soluciones de hardware y software para ayudar a las empresas a reducir el riesgo, cumplir los distintos reglamentos y mejorar la agilidad mientras persiguen objetivos estratégicos en torno a tecnologías emergentes de pago y transacciones:

- Sólida administración de claves.
- Entorno de ejecución seguro.
- Alineación con los estándares regulatorios y de cumplimiento global en varios entornos.
- Listo para aplicaciones de Blockchain.

LA FAMILIA DE PRODUCTOS NSHIELD DE ENTRUST

Los módulos de seguridad de hardware (HSMs) nShield de Entrust son dispositivos reforzados y resistentes a manipulaciones indebidas que protegen los datos más confidenciales de su empresa. Estos módulos con certificación FIPS 140-2 realizan funciones criptográficas como la generación, administración, protección de claves y proceso de firma seguro, así como la ejecución de las funciones sensibles dentro de sus límites protegidos.

Para adecuarlos con su entorno específico, la familia de productos de HSM nShield incluye los siguientes modelos:

- **nShield Connect:** dispositivos conectados a la red
- **nShield Edge:** Módulo portatil con conexión USB
- **nShield Solo:** Tarjetas PCIe para integrar en dispositivos o servidores
- **nShield as a Service:** Solución por suscripción para acceder a HSM nShield en la nube

FUNCIONALIDADES DE LA FAMILIA DE PRODUCTOS NSHIELD DE ENTRUST

Interfaces de servicios web compatible con la nube

El nShield Web Services Option Pack optimiza la interfaz entre sus aplicaciones y HSM al ejecutar comandos a través de llamadas de servicio web.

Soporte contenerizado en instalaciones o en la nube

El nShield Container Option Pack proporciona un conjunto de scripts preempaquetados que simplifican en gran medida la integración de los HSM nShield y de esa manera proveed servicios

de criptografía a las aplicaciones desplegadas en contenedores.

✱ Administración de claves para sus datos en la nube con nShield BYOK

nShield BYOK (Bring Your Own Key) le permite generar claves robustas en el HSM nShield ubicado en las instalaciones y exportarlas de forma segura a sus aplicaciones en la nube, ya sea si utiliza Amazon Web Services, Google Cloud Platform, Microsoft Azure, o las tres.

✱ Optimización de operaciones utilizando Administración y Monitorización remota

nShield Monitor y nShield Remote Administration, disponibles para los HSM nShield Solo y Connect, le ayudan a reducir los costos operativos a la vez que se mantiene informado y en control 24x7 de sus estados de HSM.

✱ Configuración remota

Los modelos nShield Connect XC ofrecen una opción de consola en serie simplificando la instalación física del HSM para alinear, cablear y aplicar potencia. Esto facilita la implementación y la reimplementación sin necesidad de revisitar el centro de datos.

✱ Arquitectura altamente flexible de Security World

La arquitectura de Security World de nShield admite HSM nShield de Entrust mediante la creación de un entorno de administración de claves flexible y exclusivo. Con Security World de nShield, usted puede combinar diferentes modelos de HSM nShield para construir un ecosistema unificado que ofrece escalabilidad, perfecta tolerancia a fallos y balance de carga.

SOLUCIONES DE CIFRADO DE WORKLOAD, GESTIÓN DE CLAVES INTEGRADA PARA ENTORNOS MULTI-NUBE

Gestión universal de claves para workload cifrados

Entrust KeyControl es un servidor KMIP certificado por VMware, escalable y con muchas funciones, que simplifica la gestión de claves para los workload cifrados. Sirve como KMS para los clientes encriptados de VMware vSphere y vSAN, así como para otros productos compatibles con KMIP.

Cifrado de datos, gestión de claves multi-nube y seguridad del workload

Entrust DataControl asegura las workloads multi-nube a lo largo de su ciclo de vida y reduce la complejidad de proteger las cargas de trabajo a través de múltiples plataformas de nube. Funciona en las instalaciones y con las principales plataformas de nube pública, así como con soluciones de hiperconvergencia y almacenamiento. DataControl incluye el servidor de gestión de claves (KMS) de Entrust KeyControl, certificado por VMware.

ALIANZAS CON LÍDERES DE LA INDUSTRIA

Entrust a través del programa de sus socios tecnológicos, colabora para integrar los HSM nShield en una variedad de soluciones de seguridad incluyendo la creación de credenciales y PKI, seguridad de base de datos, firma de códigos, firmas administración, gestión de cuentas privilegiadas, entrega de aplicaciones, inteligencia en la nube y los big data. ■

MÁS INFORMACIÓN

- Uno de los diez bancos más importantes del mundo implementa los HSMs de Entrust para ofrecer servicios fiables y de confianza a sus clientes y colaboradores
- Protección de Blockchain
- Estudio Global de Tendencias de Cifrado 2021
- Protección de claves en entornos híbridos

cpl.thalesgroup.com

THALES
Building a future we can all trust

CipherTrust Data Security Platform

Localice, proteja y controle los datos sensibles de su organización en cualquier lugar gracias a la protección de datos unificada de última generación.

Localizar Proteger Controlar

Empiece a localizar, proteger y controlar sus datos hoy mismo

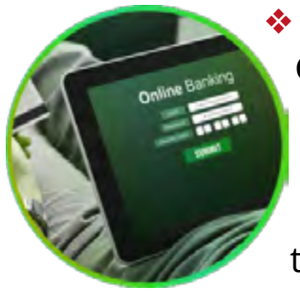
Protección para entornos financieros

RealSec dispone de una serie de soluciones de seguridad, tanto de propósito general como orientadas al segmento financiero. Aquí repasamos algunas de ellas.

SOLUCIONES DE CIBERSEGURIDAD

❖ **HSM de Propósito General/ Cryptosec LAN**

Se trata de un servidor criptográfico en red, de altas prestaciones y seguridad, diseñado para servicios de cifrado y aplicaciones de firma digital, independientemente del sistema operativo dónde éstas residan. Ofrece generación, almacenamiento y custodia de claves y certificados capaces de integrarse con aplicaciones de firma electrónica, PKI, cifrado de archivos y BBDD, blockchain...



❖ **HSM Financiero / Cryptosec Banking**

HSM financiero para pagos en red, de muy alto rendimiento, que proporciona toda la operativa y funcionalidad criptográfica específica para el ámbito de Banca, Fintech y la industria de los Medios de Pago. Cumple con todos los requerimientos y estándares definidos por el consorcio PCI (VISA, MASTERCARD...).

❖ **Remote Key Load / Cryptosec RKL**

Automatización de la carga de Claves en los ATM utilizando cifrado asimétrico, en sustitución del antiguo proceso de carga manual, tan costoso como ineficiente. Es la solución del mercado más avanzada, madura y eficiente que ofrece servicio multiempresa y está homologada por las marcas más importantes y reconocidas de ATM internacionales, cumpliendo con los requerimientos definidos por el consorcio PCI.

SOLUCIONES CIFRADO Y FIRMA DIGITAL

❖ **Servidor de firma digital/ CryptoSign Server**

Servidor Integrado de Firma Digital que incluye en un único dispositivo (hardware y software) los elementos necesarios para que, en un entorno de red, se pueda realizar cualquier proceso de firma con las mayores garantías de seguridad y gestionar los certificados digitales.

❖ **Autoridad de Sellado de Tiempo/ Cryptosec Openkey TSA**

La Firma Digital asegura quien ha realizado una determinada acción, pero no es válida para certificar que la acción se ha producido en un determinado instante de tiempo. Para ello, se requiere de una Autoridad de Sellado que afirme y certifique que los documentos electrónicos firmados han existido desde un determinado momento, y que son válidos desde ese instante.

❖ **Servidor de cifrado y firma digital de correo electrónico/ Cryptosec Mail**

Sistema centralizado de firma digital y/o cifrado del correo electrónico capaz de alma-

cenar y administrar, de forma segura, las claves de los certificados ya que está orientada a minimizar los riesgos del «Phishing» y a conseguir la total confidencialidad del contenido de los correos mediante su encriptación.

❖ **Autoridad de Validación/ Cryptosec Openkey VA**

Con la Autoridad de Validación podemos conocer el estado de revocación de los certificados digitales emitidos bajo una determinada infraestructura. ■

AUTORIDAD DE SOLUCIONES PKI

❖ **Certificación/ Cryptosec Openkey CA**

La Autoridad de Certificación es el elemento más importante y al que más hay que proteger en una infraestructura de clave pública (PKI). Es el componente de confianza emisor de los certificados y que determina su validez en el tiempo.

❖ **Autoridad de Registro/ Cryptosec Openkey RA**

La Autoridad de Registro es el punto de acceso de los usuarios finales a la Autoridad de Certificación. Al mismo tiempo que es el instrumento en el que se generan las solicitudes de certificación y las solicitudes de revocación.

MÁS INFORMACIÓN

- Segundo Informe Blockchain
- Cifrado y Firma Digital para Organizaciones Inteligentes
- Fintech y Banca. Tendencias de seguridad & HSM

Cobertura completa de riesgos de ciberseguridad en los procesos de negocio

El desarrollo de un mundo cada vez más hiperconectado, en el que las empresas enfrentan complejos procesos de transformación digital y dependen de un mayor de dispositivos conectados a Internet, resulta clave proteger los datos de las organizaciones, así como la operatividad de sus sistemas y cumplimiento con el RGPD.

S21sec es, tal y como se define a sí misma, "la compañía pure-player de ciberseguridad más grande de Iberia con una dilatada experiencia en el sector, lo que le permite ofrecer una cobertura completa de riesgos de ciberseguridad en los procesos de negocio de las organizaciones".

Una plantilla de más de 500 expertos refleja las capacidades de S21sec para investigar, detectar y prevenir amenazas; piezas clave para reaccionar con mayor rapidez ante cualquier ataque e identificar, diagnosticar y remediar eventuales incidentes en el menor tiempo posible.

Perteneciente al grupo Sonae, S21sec está entre las cinco principales compañías de ciberseguridad de Europa, con la aspiración de liderar el mercado europeo a medio plazo.

Además, cuenta con el primer SOC de España, convertido ahora en un multiSOC

global distribuido en cuatro localizaciones, garantizando la integridad de múltiples organizaciones en España, Portugal y México.

S21sec se guía por una serie de valores clave a la hora de desarrollar e implementar sus soluciones con éxito:

Una plantilla de más de 500 expertos re-fleja las capacidades de S21sec para inves-tigar, detectar y prevenir amenazas

- **Transparencia:** se pone a disposición la información necesaria para la colaboración y la toma de decisiones colectivas.
- **Excelencia:** se persigue ofrecer la más alta calidad gracias a encontrarse en un continuo proceso de aprendizaje.
- **Trabajo en equipo:** se dedica esfuerzo para encontrar la mejor forma de ayudarse entre sí, poniendo el rendimiento de la compañía por encima del rendimiento individual.
- **Innovación:** se busca la diferenciación a través de implementar cambios que mejoran su eficiencia y ventaja competitiva.
- **Confianza:** se construyen relaciones con las personas y las organizaciones basadas en la confianza y la honestidad.
- **Pasión:** se disfruta del trabajo porque siempre se busca de manera proactiva diferenciarse.

PROPUESTA DE SOLUCIONES

S21sec aúna soluciones diferentes de manera transversal y está diseñado en torno a cinco necesidades:

1. **Identificar:** análisis de riesgos y plan general de ciberseguridad, cumplimiento regulatorio, ciberseguridad en la nube y programas de transformación y Red Team.
2. **Proteger:** diseño y despliegue de arquitecturas y tecnologías, servicios de formación y concienciación, gestión de dispositivos de seguridad, seguridad de la información y seguridad ATM.

3. **Detectar:** SOC gestionado y SIEM como servicio, Unidad de Inteligencia de Ciberamenazas, EDR - Detección y respuesta End Point.
4. **Responder:** CSIRT - Gestión de incidentes de ciberseguridad 24x7, DFIR - Análisis forense digital y respuesta ante incidentes, plataforma de respuesta ante incidentes, SOAR - Automatización, Remediación y Orquestación de la Ciberseguridad y amenazas emergentes - evaluación y perfilación.
5. **Recuperar:** Continuidad de negocio y planes de respuesta ante ciber-desastres. ■

MÁS INFORMACIÓN

- Threat landscape report
- Test autoevaluación cyberGRC

Soluciones de cumplimiento y seguridad de datos para la banca y servicios financieros

Los proveedores de servicios financieros de todo tipo están ampliando sus ofertas para competir a escala global, ahorrar costes y mejorar la experiencia del cliente con servicios de valor añadido. Pero a medida que evolucionan los servicios financieros, deben asegurarse de que sus soluciones de seguridad TI sean realmente capaces de proteger los datos confidenciales que se adquieren y transmiten.

Thales ofrece soluciones integrales de gestión de acceso y protección de datos que aseguran los datos en dispositivos, procesos y plataformas in situ y en la nube. Estas soluciones ayudan a las organizaciones a cumplir con los requisitos de cumplimiento de los servicios financieros, facilitan la auditoría de seguridad, protegen a sus clientes y evitan el daño a su reputación causado por brechas de datos.

En cuanto a seguridad, el sector financiero se enfrenta a varios desafíos:

- **Cubrir los requisitos de cumplimiento de los servicios financieros.** El cumplimiento normativo puede llegar a ser abrumador para los servicios financieros. Las normativas que abarcan requisitos de seguridad de datos incluyen PCI DSS para información relacionada con tarjetas de crédito, el RGPD y PSD2 en la UE, SOX/J-SOX, leyes de notificación de brechas de datos y de residencia locales, y muchas más en todo el mundo.
- **La protección de los datos.** Para evitar multas costosas y proteger su reputación, las empresas del sector bancario y financiero y sus ejecutivos deben salvaguardar los datos financieros confidenciales contra la exposición accidental, información privilegiada deshonesta, APT y otras amenazas conocidas y desconocidas. Y no solo deben existir procedimientos para proteger los datos, sino también para identificar y alertar a la organización cuando se produce un acceso no autorizado.

¿CÓMO THALES LES PUEDE AYUDAR?

Thales cuenta con una oferta de soluciones en diferentes áreas que incluyen:

✱ **Soluciones de cifrado.** Las soluciones de protección de datos CipherTrust Transparent Encryption y CipherTrust Application Data Protection , incluídas en la solución CipherTrust Data Security Platform de Thales, proporcionan un único marco extensible para proteger los datos en reposo bajo los diversos requisitos de la industria de servicios bancarios y financieros en la más amplia gama de plataformas de sistemas operativos, bases de datos, entornos de nube e implementaciones de Big Data. El resultado es un bajo costo total de propiedad, así como una implementación y operación simples y eficientes.

✱ **Administración de claves robusta.** Las soluciones de administración de claves de Thales, permiten la gestión centralizada de claves de cifrado para otros entornos y dispositivos, incluido el hardware compatible con KMIP, claves maestras TDE de Oracle, SQL Server...

✱ **Protección de datos de pago.** Las soluciones de Thales están diseñadas específicamente para aplicaciones de pago. El módulo payShield 10K, la quinta generación de HSM de pago de Thales, ofrece un conjunto de funciones de seguridad de pagos comprobadas en entornos críticos y que incluyen el procesamiento de transacciones, protección de datos confidenciales, emisión de credenciales de pago, aceptación de tarjetas móviles y tokenización de pagos. payShield 10K de Thales atiende lo último en requisitos de seguridad obligatorios y en mejores prácticas para una amplia gama de organizaciones que incluyen EMVCo, PCI SSC, GlobalPlatform, Multos, ANSI, así como las varias marcas y redes de pago globales y regionales.

Por otro lado, CipherTrust Tokenization with Dynamic Data Masking permite a los administradores establecer políticas para devolver un campo completo tokenizado o enmascarar dinámicamente partes de un campo. Con las capacidades de tokenización de la solución que preservan el formato, los administradores pueden restringir el acceso a activos confidenciales y, al mismo tiempo, formatear los datos protegidos de una manera que les permita a muchos usuarios hacer su trabajo.

VENTAJAS DE LAS SOLUCIONES THALES

Las soluciones de Thales ofrecen:

❖ **Cumplir las obligaciones reglamentarias.** Con sus productos de Data Security, la industria bancaria puede cumplir con los estándares regulatorios y de seguridad de datos en reposo mientras protege la información de brechas de datos en toda la empresa, en la nube y en entornos de Big Data.

❖ **Rápida de instalar.** Thales puede instalar las soluciones de seguridad de datos CipherTrust en semanas en lugar de meses. Las soluciones de Thales funcionan con la mayoría de los principales sistemas operativos, incluidos los servidores Linux, UNIX y Windows en entornos físicos, virtuales, en entornos de datos de titulares de tarjetas (CDE) de la nube y Big Data.

❖ **Fácil de usar.** Su oferta CipherTrust Data Security Platform simplifica la resolución de problemas de seguridad y cumplimiento al proteger simultáneamente los datos en bases de datos, archivos y nodos de Big Data, en nubes públicas, privadas, híbridas e infraestructuras tradicionales. La administración centralizada de toda la plataforma de seguridad de datos, facilita la ampliación de la protección de seguridad de los datos, y la satisfacción de los requisitos de cumplimiento en toda la empresa, creciendo según sea necesario, sin agregar nuevo hardware ni aumentar las cargas operativas. ■

MÁS INFORMACIÓN

- Cifrado Total
- The Key Pillars for Protecting Sensitive Data
- payShield Brochure

Soluciones más robustas gracias a la inteligencia de amenazas compartida

Trend Micro trabaja para ayudar a que el mundo sea seguro para el intercambio de información digital. Aprovechando los más de 30 años de experiencia en seguridad, investigación de amenazas globales e innovación continua, la firma permite la resiliencia de las empresas, gobiernos y consumidores con soluciones conectadas a través de cargas de trabajo en la nube, endpoints, correo electrónico, IIoT y redes.

Su estrategia de seguridad XGen impulsa sus soluciones con una combinación intergeneracional de técnicas de defensa frente a amenazas que están optimizadas para los entornos clave y aprovecha la inteligencia de amenazas compartida para una mejor y más rápida protección.

SOLUCIONES Y PRODUCTOS

Trend Micro ha innovado para adaptar su oferta a la evolución de las amenazas y a las necesidades de empresas y usuarios. Cuentan con un amplio catálogo de productos que permiten ofrecer protección en cualquier entorno, ya sea físico, virtual, en la nube y en contenedores.

El catálogo de Trend Micro ofrece una mayor cobertura, pues busca cubrir todos los vectores de ataque posibles (endpoint, cloud, navegación, email, entornos colaborativos, redes privadas/cloud, OT...), y por tecnología, ya que combinan tecnología de última generación junto con la experiencia que les aporta su trayectoria en el mercado.

Un ejemplo de esta evolución es la Tecnología XDR, introducida en el mercado por Trend Micro, que aprovecha la información recabada por los distintos vectores (endpoint, servidores, correo, red...). XDR extiende las capacidades del EDR tradicional aportando contexto a los ya citados ataques multivector, permitiendo a los clientes identificarlos y bloquearlos de manera prematura.

Por otro lado, Trend Micro estructura su oferta en torno a los siguientes ejes:

❖ **Solución Hybrid Cloud Security:** agrupa seguridad cloud simplificada gracias a la plataforma de servicios Trend Micro Cloud One. Protege entornos físicos, virtuales, en la nube y en contenedores con control y visibilidad centralizados; proporciona un conjunto completo de prestaciones de seguridad; reduce el número de herramientas de seguridad necesarias para proteger entornos híbridos y satisfacer los requisitos de cumplimiento; ahorra recursos y reduce los costes con una seguridad optimizada del entorno y políticas automatizadas. Disponible como software, como servicio, o en los marketplaces de AWS y Microsoft Azure, cuenta con tecnología de seguridad XGen, que ofrece un conjunto intergeneracional de controles de seguridad optimizados para entornos líderes.

❖ **Network Defense Solution:** área desde el que ofrece protección contra amenazas conocidas, desconocidas y ocultas, es decir, aquellas vulnerabilidades de las que no se tiene visibilidad y que residen en la red. Mediante la integración de las soluciones de Intrusion Prevention (IPS) y Advanced Threat Protection (incluido sandboxing), Trend Micro proporciona una combinación de técnicas intergeneracionales y de detección de defensas avanzadas para aumentar al máximo la protección e ir más allá de lo conocido y desconocido, ofreciendo protección más inteligente, logrando tiempos de reacción más rápido, mayor rendimiento y protección automatizada que se adapta a entornos híbridos.

❖ **User Protection Solution:** brinda protección avanzada e inteligente a los usuarios con la técnica adecuada en el momento adecuado, en cualquier dispositivo, aplicación y lugar. Se trata de una seguridad conectada y que utiliza varias capas para detener las amenazas emergentes y reducir los gastos de gestión. Seguridad optimizada para funcionar en su entorno por un proveedor de confianza y con visión de futuro que siempre trabaja en una nueva generación de seguridad. Gracias a Smart Protection Suite, son capaces de proteger a los usuarios desde el gateway hasta el endpoint.

Este catálogo de soluciones, que también abarca el segmento de la pyme, se ve complementado con servicios de soporte al cliente para garantizar un funcionamiento sin problemas y una asistencia superior. ■

MÁS INFORMACIÓN

- The Banking and Finance Industry Under Cybercriminal Siege: An Overview
- Banks Under Attack
- Mobile Banking Trojan

THE ART OF CYBERSECURITY

Trend Micro Vision One™

Mayor visibilidad para una respuesta más rápida

Una plataforma especialmente diseñada para la defensa contra amenazas que va más allá que otras soluciones XDR

Más información en:
www.trendmicro.com

CONTENIDOS↓

Tecnología para tu Empresa

CENTRO DE RECURSOS

it

La pyme pone rumbo al mundo digital

KIO Networks · NetApp · NFON Cloud Telephone System · SAMSUNG · servicenow

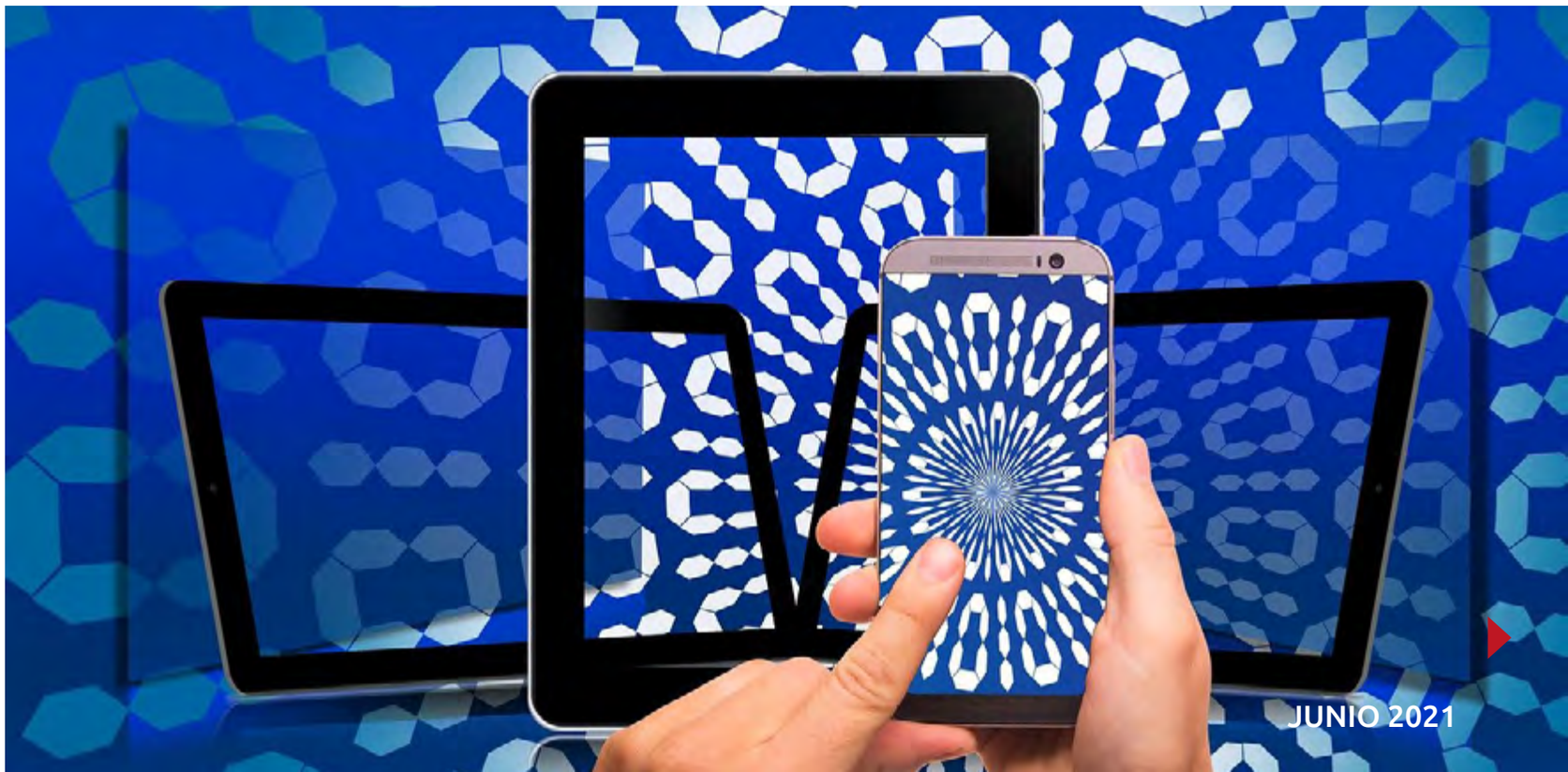
La pyme pone rumbo al mundo digital

2020 supuso una dura prueba para los pequeños negocios y autónomos que, en muchos casos, habían postergado su decisión de digitalizarse. Sin embargo, con la irrupción de la pandemia, han tenido que empezar este proceso, que está continuando este año tratando de impulsar más el comercio electrónico y el marketing digital, y prestando atención a la seguridad de los datos.

GoDaddy ha presentado los resultados de su observatorio "Estado actual de la digitalización las pequeñas empresas y autónomos españoles 2021" en el que destaca que, aunque estos meses han sido tremendamente complicados, está claro que han sabido adaptarse a la situación para superar las dificultades de los cierres y restricciones derivadas de la pandemia poniendo en el centro de su actividad la digitalización y sus herramientas.

Estos negocios están abiertos a la innovación y a la mejora y, contra todo pronóstico, han logrado hacer frente a esta crisis sin precedentes, pues muchas se han beneficiado de la digitalización y de la venta de sus productos y servicios online. La tecnología se ha convertido en protagonista y única salvación para un significativo número de pequeños empresarios españoles. Tanto es así que uno de cada cuatro ha llegado a ampliar sus áreas de negocio en estos meses y un 12% ha iniciado o expandido su tienda online.

"Esta ha sido una crisis sin precedentes, nadie ha visto, ni vivido, nada parecido y esa es la principal razón por la cual esto ha sido tan complicado, porque nadie contaba con una experiencia similar en la que basarse. Pero si algo ha logrado salvar el negocio de la gran mayoría de estos pequeños empresarios españoles ha sido la digitalización y sus herramientas, ya que el comercio electrónico se ha convertido en su principal canal de venta", señala Gianluca Stamerra, director regional de GoDaddy para España, Italia y Francia.



Aunque son muchas las dificultades con las que se están encontrando este tipo de negocios desde que comenzaron las restricciones, más del 48% de las pequeñas empresas esperan resurgir con más fuerza que antes de la COVID-19. Además, destaca la manera en la que están aclimatándose a los nuevos canales digitales para aumentar las ventas y continuar: el 52% dice utilizar la página web de su empresa, para el 39% lo son las redes sociales y un 20% manifiesta que utiliza su propia tienda online.

Las pequeñas empresas españolas encuestadas afirmaron que los principales retos a los que se enfrentaron durante la pandemia de la COVID-19 fueron mantener el negocio (32%), aumentar el número de nuevos clientes (20%) e incrementar la fidelidad de los clientes (13%). Y, para enfrentar estos desafíos, destacan que se han dedicado parte de sus recursos a contabilidad/finanzas y RRHH e informática (35%), ventas y marketing (36%) y en atención al cliente (15%). Para el 71% de los pequeños empresarios es importante ampliar los conocimientos tecnológicos y soluciones digitales.

LA EMPRESA ESPAÑOLA ESTÁ LISTA PARA UNA DIGITALIZACIÓN EXITOSA

LA IMPORTANCIA DE LA TECNOLOGÍA

El IV Estudio sobre el estado de digitalización de las empresas y administraciones públicas españolas de Vodafone, muestra el creciente protagonismo que ha desempeñado el teletrabajo durante los meses de la pandemia. En el caso de las grandes empresas la implantación del teletrabajo asciende al 94%, mientras que el teletrabajo en microempresas se ha duplicado hasta alcanzar un 30% durante los meses de pandemia.

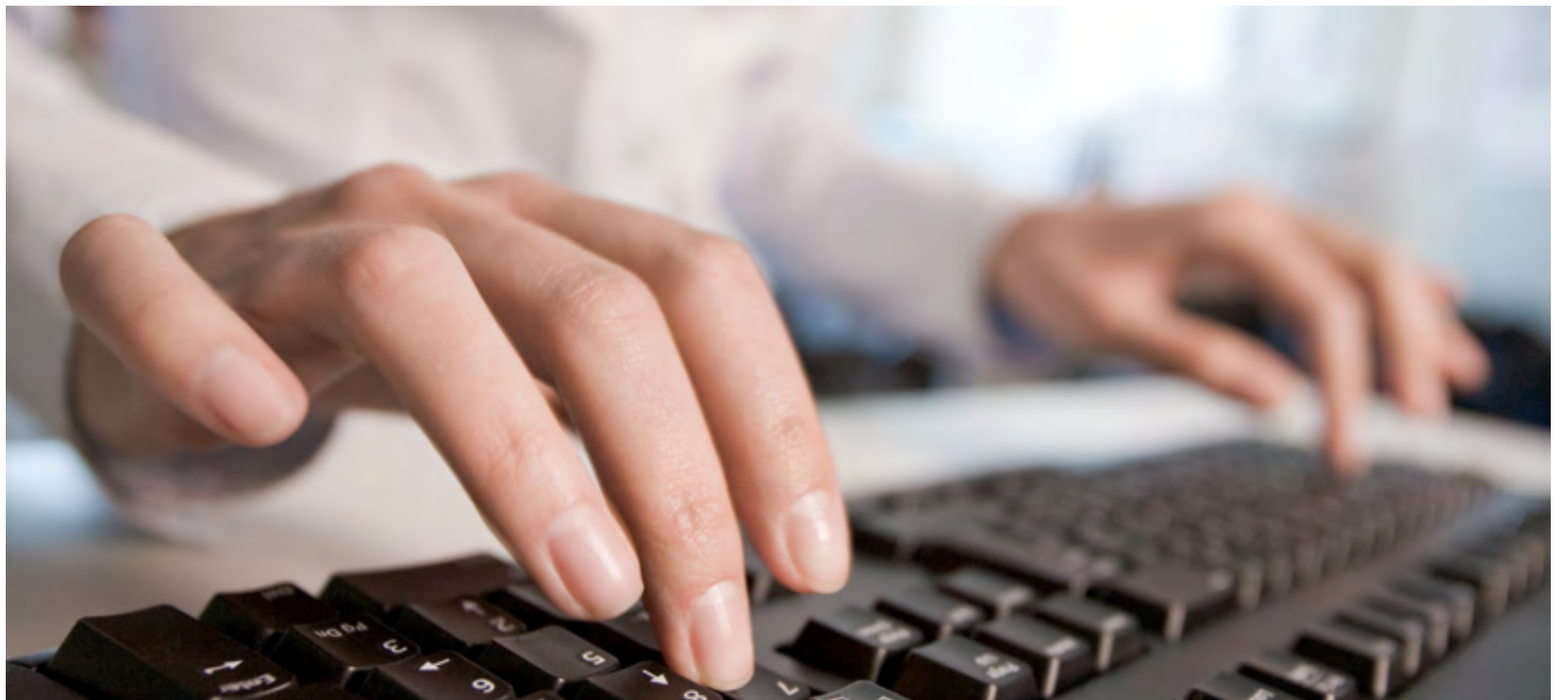
Las empresas españolas consideran que contaban con las soluciones necesarias para la implementación del teletrabajo en la pandemia. De hecho, la mayoría de las empresas se autopercibe como “preparada”, siendo el segmento de las grandes empresas y las pymes donde esta percepción obtiene sus mayores porcentajes (87% y 84% respectivamente).

Para facilitar el teletrabajo, las tecnologías que han aportado una mayor utilidad han sido las soluciones de conectividad, servicios en la nube (pública y privada), aplicaciones de videoconferencia, herramientas de colaboración, acceso remoto al puesto de trabajo y sistemas de seguridad en

red o en la nube. También han tenido una gran transcendencia aquellas tecnologías que han permitido llegar de forma remota a los clientes como el marketing digital, el comercio electrónico y las aplicaciones de pago. En general, los servicios vinculados a nube o cloud y, en un segundo lugar, aquellos que tienen que ver con la conectividad son los más implantados en las empresas y Administraciones Públicas españolas. Las pequeñas empresas y autónomos disponen de 2,4 servicios frente a los 6,7 de las grandes empresas y también son quienes menos contratación de este tipo de soluciones han hecho desde que comenzara la pandemia del Covid-19.

En el futuro todas las organizaciones planean reducir el teletrabajo, pero las empresas de todos los tamaños continuarán en niveles ligeramente superiores a la situación previa a la pandemia. Sin embargo, en el caso de las Administraciones Públicas el porcentaje de teletrabajo podría mantenerse en un 55%, previéndose así un incremento notable respecto a la situación previa.

A mayor tamaño de la empresa se incrementa la importancia atribuida a las nuevas tecnologías para un futuro inmediato. Consideran estas como muy importantes o bastante importantes un 57% de las microempresas, un 68% de las pymes, un 82% en el caso de las grandes empresas y para el 84% de las AAPP.



Todos los tipos de empresas coinciden en citar la crisis del Covid-19 como su mayor preocupación, seguida de la preocupación por la situación económica general y la pérdida de facturación/ventas y la evolución de su sector como otros aspectos relevantes. Si bien la digitalización no aparece como una preocupación de las empresas, la inquietud por la ella va incrementándose según aumenta el número de empleados de la empresa. Hay que destacar aquí que son las Administraciones Públicas, las que mayor preocupación muestran por este aspecto, otorgándole una nota de 7,8 sobre 10.

La digitalización beneficia a las empresas aportando principalmente eficiencia en procesos y mejoras en la comunicación con clientes. Las organizaciones estudiadas consideran que están aún inmersas en el proceso de digitalización de sus organizaciones y solo una parte de ellas ha llegado a un nivel avanzado. En este contexto, es el segmento de las microempresas las que se perciben menos preparadas, donde un 48% reconoce estar en un nivel 'básico'. Son las grandes empresas donde se sitúa el mayor porcentaje de nivel 'avanzado', con un 42%, aunque siguen reconociendo una amplia margen de desarrollo. Respecto a las barreras para avanzar en la digitalización, la necesidad de contar con el talento adecuado se hace más patente.

Respecto a la presencia de planes de digitalización, aumenta ligeramente en todas las empresas, en mayor medida en las grandes organizaciones, aunque el porcentaje que asigna una partida específica para el desarrollo de este plan se estabiliza y se mantiene en un 47% en las pequeñas empresas, un 49% en las pymes, un 60% en las grandes empresas y un 57% en el caso de las Administraciones Públicas que afirman tener asignado un presupuesto para desarrollar su plan.

TRES IMPRESCINDIBLES PARA LA PYME

Del análisis de las respuestas a una encuesta llevada a cabo por GoDaddy se desprende que la digitalización es más importante ahora que hace un año, tras la irrupción de la pandemia. Un 56% de los encuestados está convencido de que la digitalización es importante para el porvenir de su negocio, y a la pregunta de cuáles son esas tecnologías que consideran más relevantes para este 2021, los autónomos y las pequeñas empresas españolas han destacado las siguientes:

❖ **Tienda online:** hasta hace poco eran muchas las empresas que no tenían siquiera en mente la idea de implantar una tienda online en su página web y, hasta antes de la pandemia, solo el 7% contaba con un e-commerce propio. Pero ahora la situación ha cambiado de manera radical y el 22% de las pequeñas empresas y autónomos que han participado en el estudio declaran que les habría gustado contar con un canal de venta propio o marketplace creado antes de la llegada del coronavirus para haber mantenido abiertas otras vías de negocio. En 2021 contar con una tienda online puede suponer la diferencia entre continuar con el negocio o cerrar las puertas definitivamente.

❖ **Diseño web 'responsive':** contar con una página web para una pequeña empresa se está convirtiendo en una herramienta básica para una mayor visibilidad en la web, mantener la actividad y hacer crecer el negocio hoy en día. Pero dado que el acceso a la información, las compras online, etc. se realiza a través de múltiples dispositivos diferentes, es fundamental que la página web de una empresa esté diseñada para adaptarse a cualquier pantalla.

❖ **Certificado SSL:** son muchos los usuarios que evitan realizar alguna transacción en una web sin garantías, lo cual indica la importancia que le dan los clientes a contar con todas las medidas de seguridad a la hora realizar una compra online. El protocolo HTTPs o certificado SSL ofrece la máxima seguridad web, permitiendo que el intercambio de información sea completamente seguro, protegiendo la transferencia de datos personales desde el sitio web al servidor. Además, tener un certificado SSL instalado en un sitio web, proporciona un plus de profesionalidad a una página, mejora el posicionamiento SEO y aumenta, de manera significativa, la confianza de los clientes.

MÁS INFORMACIÓN

- Toda la información sobre las tendencias tecnológicas en las empresas
- Cómo está evolucionando la cloud
- El mercado de las comunicaciones unificadas crece
- El mercado de almacenamiento SMB se transforma
- ¿Cómo serán los nuevos espacios de trabajo?
- Cuál es la propuesta de KIO Networks para el mercado cloud
- Cuál es la propuesta de NFON para el mercado de la telefonía en la nube
- Cuál es la propuesta de Samsung para el almacenamiento SMB
- Cuál es la propuesta de ServiceNow para el nuevo entorno laboral

¿SABES CUÁNTO PERDERÍA TU EMPRESA SI SE PARASEN LOS ENTORNOS DE IT CRÍTICOS?

Garantiza la Continuidad de Negocio con la nube de **KIO** y las soluciones de **NetApp**, expertos en la gestión de datos en el **Cloud**.

KIO NetApp

“LA CLOUD AYUDA A LAS EMPRESAS A SER MÁS COMPETITIVAS”

Que los sistemas y aplicaciones de una compañía garanticen sus operaciones y aseguren la continuidad de negocio siempre ha sido algo prioritario. ¿Una economía digital como la actual amplía los desafíos empresariales en este campo?

El nivel de exigencia sobre los sistemas informáticos de organizaciones y consumidores se ha elevado exponencialmente, los problemas informáticos, de toda índole, se han convertido en noticias de primera página por la repercusión económica que tienen.

Las empresas se han dado cuenta de que no pueden enfrentarse solas al reto que ha traído la transformación digital y empiezan reparar en que es mejor concentrar los esfuerzos en las áreas funcionales y buscar servicios que les garanticen la alta disponibilidad de sus Sistemas de Información.

Este escenario ha abierto una puerta a crear servicios que sostengan y garanticen la economía digital. El cloud computing ya es una fórmula aceptada y adoptada por muchas empresas, pero ahora ya se exige que sean servicios de altísima disponibilidad, ese es el gran desafío empresarial, unido a la seguridad.

¿Cómo han evolucionado el mercado de data centers para adaptarse a la nueva realidad?

El mercado de data centers sigue creciendo y poniendo a disposición de las empresas una cantidad im-

JAVIER JARILLA, DIRECTOR GENERAL DE KIO NETWORKS SPAIN

"LA CLOUD AYUDA A LAS EMPRESAS A SER MÁS COMPETITIVAS"

portante de metros cuadrados, sin embargo, llama la atención que las certificaciones de alta disponibilidad sigan siendo las mismas de hace 7 años. Creo que la verdadera evolución del centro de datos llegará cuando estas instalaciones se especialicen por tipos de servicio y cliente; no tiene las mismas necesidades a nivel de centro de datos un cloud provider que un cloud privado. En nuestro caso, concebimos nuestro cpd como centro de dato exclusivo como nube.

La informática en la nube avanza como parte fundamental de la transformación digital que están llevando a cabo la mayoría de las organizaciones, ¿cómo está afectando al mercado de centros de datos en general el auge de la nube pública?

Entendiendo la pregunta como una comparación entre servicios cloud y housing de sistemas o colocation, está claro que cuando un cliente opta por servicios de cloud computing como IaaS, por ejemplo, deja de necesitar espacio o racks en un centro de datos para pasar a consumir recursos de una nube que también está alojada en un centro de datos. Una empresa que opta por subirse a la nube reduce drásticamente sus necesidades de espacio en un centro de datos.

Toda la información sobre la situación TI de las empresas españolas en @TIyEmpresa_ITDM

No obstante, los proveedores de centros de datos de máximo nivel están teniendo un importante papel en el suministro de clouds privadas. ¿Qué ventajas ofrecen frente a otras alternativas?

Un ejemplo de cloud privado es trasladar la infraestructura que tiene la empresa en sus instalaciones a un centro de datos. Salvo por razones estrictas de certificación existentes en algunos sectores, como el financiero (pci/dss) o alguno más, creo que no le aporta ventajas a la empresa porque sigue teniendo los problemas derivados de la infraestructura pero lejos de sus instalaciones. Para mí, la elección no es cloud privado frente a cloud público, la verdadera elección debe estar basada en cuestiones como disponibilidad, seguridad y facilidad. Creo que lo que demandan las empresas es dejar atrás los problemas derivados de la infraestructura y centrarse en la parte funcional que es donde se encuentra la verdadera transformación.

¿Cuáles son las consecuencias a las que se enfrentan las empresas que no dispongan de un plan de continuidad de negocio?

Hay voces que dicen que la empresa que no disponga de un plan de continuidad se enfrenta a la desaparición y creo que no andan desencaminadas. Cuando los procesos de la compañía dependen de los sistemas de información es imposible operar sin ellos y el valor de las caídas anuales se cifra en cientos de miles de euros de pérdidas para las empresas.

Lamentablemente, hemos visto demasiados casos en el último mes con elevado impacto para los que los han sufrido.

¿Cuáles son los factores críticos que cualquier organización debe tener en cuenta a la hora de ase-

gurar la alta disponibilidad de los sistemas y la continuidad de negocio?

Son muchos; la energía, la climatización, las comunicaciones, el hardware, el software, las ubicaciones, la seguridad y la operación de todos ellos vista como un factor crítico. A estos hay que añadirles los problemas derivados de la seguridad física, riesgos de catástrofes, etc.

Cualquiera de ellos es capaz de poner en jaque la continuidad de negocio. Cuando diseñas un servicio de alta disponibilidad para ofrecerlo a tus clientes te das cuenta de la cantidad de disciplinas que se deben contemplar, que por ellas mismas no aportan valor, y que cualquiera de ellas te puede producir un problema de disponibilidad.

Como hemos mencionado con anterioridad, en un escenario de incertidumbre cobra especial importancia disponer de un plan integral que garantice la continuidad del negocio. ¿Cuál es la propuesta de KIO Networks en este sentido?

Kio es un proveedor de infraestructura como servicio (IaaS). Entre los servicios que presta se encuentra VDC+ que es una infraestructura que incluye replica síncrona de la información del cliente en dos centros de datos separados 200Kms. Ello permite que ante una incidencia en una de las ubicaciones el sistema arranque de manera automática con un RPO= cero, es decir sin pérdida de datos, y con un RTO (tiempo que tarda en recuperarse el sistema) inferior a cuatro minutos. Este servicio permite a las empresas adoptarlo de manera inmediata y en régimen de pago por uso. Además de la réplica de la información, proporciona la réplica del backup y la configuración automática de las comunicaciones. Se trata de alta disponibilidad geográfica totalmente automatizada. ■

MÁS INFORMACIÓN

- Toda la información sobre Tecnología para tu Empresa
- ¿Cómo está evolucionando el modelo cloud?
- Toda la información sobre la propuesta de KIO Networks

LO QUE FALTABA... ¡LOS NÚMEROS SALEN!

Me sorprendió el éxito de uso que tuvieron las iniciativas de bicicletas compartidas; para alguien criado en la cultura de la propiedad ver que había público encantado de pagar por usar un servicio como la bicicleta fue revelador. El pago por uso se ha convertido en la clave económica de la revolución digital.

Según Wikipedia, la computación en la nube (del inglés cloud computing), conocida también como servicios en la nube, es un modelo que permite ofrecer servicios de computación a través de una red, que normalmente suele ser internet.

Entre los servicios de cloud computing que podemos contratar el primero que encontramos es el IaaS (infraestructura como servicio, en inglés). Consiste en dejar de comprar servidores, licencias de sistemas operativos, cabinas de discos y elementos de red, entre otros elementos, para pasar a contratar un servicio a cambio de una cuota mensual. Si este servicio permite aumentar o reducir las cantidades de los elementos que lo componen, actualizando su precio en función de las variaciones, se considera que estás pagando por el uso.

JAVIER JARILLA, director general de KIO Networks

Puedes leer la tribuna de opinión completa en este enlace.

CONTENIDOS↓

cloudya

¡Pruébalo gratis!

Tu negocio siempre conectado en la “nueva” normalidad.

Más información en **nfon.com**

La nueva libertad en la comunicación empresarial.

Con Cloudya, NFON ofrece una solución de centralita cloud que permite teletrabajar con una sencilla y rápida configuración. Como solución 100% 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

partners.iberia@nfon.com

NFON
Cloud Telephone System

"LA VERSIÓN 2.0 DEL SERVICIO DE SIP TRUNK PRESENTA NOVEDADES SIGNIFICATIVAS EN FLEXIBILIDAD Y CONTINUIDAD DE NEGOCIO"

La telefonía IP ha ido ganando cada vez más popularidad, y son cada vez más las empresas que emplean una combinación de sistemas de telefonía convencional e IP. ¿Cuáles son los motivos que están llevando a realizar esta transición en sus comunicaciones?

La telefonía IP lleva entre nosotros más de un cuarto de siglo. La tendencia previa a la pandemia en la que la conciliación laboral/familiar, el ahorro de costes en dietas y la sostenibilidad a la hora de reducir la huella de CO2, reduciendo los viajes innecesarios, sentaban unas bases para que la migración hacia una solución de comunicaciones "todo IP" permitiese esa flexibilidad del empleado a la hora de utilizarla. Pero es cierto que la situación generada por la pandemia ha reactualizado, dado mayor visibilidad y relanzado este mercado, en el que algunos proveedores llevamos ya hace muchos años. Por eso, todo tipo de empresas, pequeñas, medianas o grandes, están buscando esa transición.

Un sistema SIP Trunk sirve de intermediario entre los sistemas de telefonía convencionales y los de VoIP. ¿Qué requisitos tiene que cumplir una empresa para poder adoptar este sistema?

Los enlaces SIP Trunk presentan requisitos tanto hacia el operador que lo proporciona como hacia la PBX con la que se conecta.

❖ Por un lado, hacia el operador que lo presta, se debe disponer del

DAVID TAJUELO, country manager de nfon Iberia

ALBERTO DOMARCO, Director de Operaciones y Preventa de nfon Iberia

ancho de banda necesario para soportar el número de canales, o conversaciones simultáneas, que deban proveerse. Este ancho de banda dependerá también del códec empleado para el transporte de la voz. Algunos minimizan este consumo a costa de reducir la calidad de la voz, pero con los anchos de banda disponibles en la actualidad es preferible, en general, dedicar uno mayor y no perder calidad en la voz.

❖ Por otro lado, y hacia el sistema PBX, se precisa que este soporte la tecnología SIP trunk tal como hacen la mayoría de sistemas actuales. En los casos en que no lo soportan, se puede continuar usando la tecnología de SIP trunk mediante la instalación de un sistema Gateway intermedio, capaz de "hablar" SIP trunk hacia el exterior y típicamente RDSI hacia la PBX.

"LA PANDEMIA HA ACELERADO LA ADOPCIÓN DEL SIP TRUNK", David Tajuelo, NFON Iberia

NFON acaba de presentar Nconnect Voice 2.0, la nueva versión de SIP Trunk, que proporciona una transición fluida hacia comunicaciones IP flexibles y escalables. ¿Cuáles son las principales novedades que ha incorporado NFON a esta nueva versión?

La nueva versión 2.0 del servicio de SIP trunk presenta novedades significativas en lo referente a la flexibilidad y a la continuidad de negocio principalmente. Por destacar algunas novedades:

❖ Respecto a la flexibilidad, permitimos la asignación de números y rangos de numeración internacionales a los trunks, de cualquiera de los países en los que prestamos servicios.

❖ En lo referente a la continuidad de negocio, permitimos la definición de múltiples PBXs asociadas a un trunk, de modo que en caso de indisponibilidad de alguna PBX las llamadas continúen entregándose en una PBX alternativa del cliente. Incluso en caso de indisponibilidad total de todas las PBXs, continuamos pudiendo entregar las llamadas en números públicos alternativos, fuera de nuestra propia red.

❖ Por añadir una novedad más, soportamos también la integración de nuestros trunks en la plataforma Teams de Microsoft, de modo que somos una pasarela entre la misma y los servicios públicos de telefonía.

¿Cuáles son los elementos diferenciales de Nconnect Voice 2.0 en comparación con otras soluciones que están en el mercado?

Respecto a la competencia, y además de las funcionalidades ya mencionadas que en muchos casos otros proveedores no proporcionan, ofrecemos una solución basada en infraestructura cloud altamente redundada para garantizar la disponibilidad del servicio. Valoramos igualmente la calidad de la voz que transportamos, por lo que usamos siempre códec G711 sin compresión. Además, soportamos el cifrado total de las comunicaciones mediante el uso de TLS y SRTP.

Entre los beneficios que obtienen las empresas que eligen un sistema SIP Trunk se encuentran el ahorro en cuotas, llamadas más económicas y mayor movilidad. ¿Qué perfil de empresa es el que más partido puede sacar a este tipo de solución?

En realidad cualquier empresa puede sacarle partido a estas características y a la mayor flexibilidad del modelo de conexión respecto a los modelos tradicionales, pero evidentemente será mayor el beneficio para aquellas que usen las funcionalidades diferenciales ya presentadas: Empresas con varias PBXs entre las que balancear el tráfico de voz, con necesidades de numeración internacional, o con necesidad de integrar MS Teams son candidatas ideales ya que sacarán partido a todas estas funcionalidades.

Con el lanzamiento de Nconnect Voice 2.0 ¿van a lanzar algún tipo de acción concreta para su canal de distribución?

Por supuesto, estamos tan seguros de que nuestra solución renovada, y ya probada durante muchos años en el exigente mercado alemán, será del gusto de nuestros partners y clientes que vamos a poner en marcha una promoción, tanto en canales como en tráfico, de 2 meses gratis. Sabemos que después de este tiempo, nuestros clientes seguirán confiando en nosotros. Tenemos la menor tasa de churn de todo el mercado europeo, y eso hace que sepamos que el que prueba NFON, se queda con nosotros.

Nconnect Voice 2.0, ¿puede ser comercializado por cualquier reseller de NFON o está orientado a un tipo concreto de partner?

Por cualquiera de nuestros partners, pero lógicamente está pensado para aquellos partners y clientes que quieran hacer una transición "suave" al "todo IP". Trabajando con NConnect Voice 2.0 se podrá acercar al mundo IP prácticamente toda la base instalada de centralitas tradicionales. Y de esta manera, enseñando al cliente /partner todas las posibilidades que una plataforma de comunicaciones, o simplemente una centralita, en la nube pone a la disposición de nuestros futuros clientes y partners.

¿Cuáles son las principales ventajas que podrán obtener los clientes de su canal de distribución?

Como decía, cualquier partner puede ofrecer y revender nuestros nuevos SIP Trunks. Es un mercado realmente en auge y abre múltiples posibilidades de generar beneficios para el partner. Lógicamente hablamos de comisiones recurrentes, tanto para los canales de voz que se quieran activar, como para el tráfico generado, y con las características técnicas más avanzadas para este tipo de soluciones. Pero también hablamos de la posibilidad de integrarlos con las licencias de Microsoft Teams que sus clientes ya tengan, generando valor añadido tanto para la venta de servicios adicionales, como de las posibles licencias de Microsoft necesarias para que el sistema corra sin ningún tipo de sobresalto. ■

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

SAMSUNG

NVMe SSD 980 PRO

Unstoppable speed

PCIe 4.0

WORLD'S
No.1
FLASH MEMORY
SINCE 2003
SAMSUNG

* Source: 2003-2019 IHS Markit data:
NAND suppliers' revenue market share

“EL ALMACENAMIENTO SSD ES UN PRODUCTO MÁS SEGURO, MÁS RÁPIDO, Y MÁS VIABLE”

EUGENIO JIMÉNEZ CARRASCO, BRANDED MEMORY BUSINESS HEAD EN SAMSUNG STORAGE IBERIA

Según los últimos datos de las consultoras, el mercado SSD crecerá en torno a un 15% anual hasta 2026. ¿cuáles son los motivos que están llevando a los usuarios a adquirir este tipo de almacenamiento?

Las previsiones de las principales consultoras es que este mercado crecerá notablemente en los próximos años y esto se debe a varios motivos.

Los crecimientos esperados en SSD siguen basándose en la renovación del parque antiguo de portátiles y equipos de sobremesa cuyo almacenamiento siguen dependiendo del histórico HDD. Los ciclos de compra de un portátil/PC suele estar en torno a los 6-7 años, por lo que muchos consumidores prefieren darle un lavado de cara a sus equipos sustituyendo el HDD por el SSD y no comprando un equipo nuevo, afectando tanto al canal profesional como al de consumo.

No obstante, el abaratamiento que se ha producido está hacien-

do que muchos usuarios decidan adquirir nuevas soluciones.

Además, otro de los motivos es que existen usuarios que están renovando el parque de SSD de la primera generación.

Nos hemos encontrado con una demanda cada vez más creciente. Este mercado está creciendo a doble dígito en todos los segmentos y prevemos que vaya a continuar en los próximos años.

Poco a poco, el SSD está reemplazando el uso de otros soportes más convencionales. ¿Por qué es mejor adquirir almacenamiento SSD en vez de otro tipo de soporte?

Las ventajas del almacenamiento SSD frente a otros soportes más convencionales son múltiple.

El almacenamiento SSSD es un producto más seguro, más rápido, y más viable. Las garantías son bastante amplias y de cara al usuario todo son ventajas, ya que se aumenta la productividad, la eficiencia de los equipos, el consumo de batería de los portátiles, la seguridad de los dispositivos al contar con tecnología de cifrado, la velocidad de acceso a determinados programas, la velocidad de arranque de los propios equipos...

Esta transición supone un incremento de la demanda de componentes. ¿Cómo va a afectar esto a la hora de comprar un SSD? ¿Se espera un incremento de precios?

Lo que estamos comprobando en Samsung es que, en el mercado de almacenamiento, en la primera mitad del año va a haber cierta escasez, no de los componentes en general, sino de la parte de controladoras.

Esta realidad está afectando al mercado, pero a Samsung en menor medida. ¿El motivo? Samsung fabrica el 100% de sus componentes. Esto nos lleva a ofrecer un producto de mayor garantía y terminado, mientras que otros fabricantes lo que hacen es recurrir a un mercado de terceros y es precisamente este mercado de terceros el que está teniendo escasez de producto.

Desconocemos si esta situación va a llevar a un encarecimiento de productos. Por lo menos, nuestra política está siendo mantener los precios.

Samsung dispone de un amplio abanico de soluciones tanto para entornos empresariales como de consumo para el mercado SSD. ¿Cuáles son las principales diferencias de esta propuesta frente a la de sus principales competidores?

En SSD, la propuesta de valor de Samsung radica en la fiabilidad de sus productos. Samsung se preocupa por entregar la mejor calidad en sus productos. En este sentido, hemos de destacar tan-

Toda la información sobre la situación TI de las empresas españolas en @TIyEmpresa_ITDM

"DE CARA AL USUARIO, EL ALMACENAMIENTO SSD SOLO OFRECE VENTAJAS"

to las velocidades ofrecidas dada nuestra fuerte apuesta por los SSD con tecnología NVMe como las amplias garantías de nuestros SSD, permitiendo un ciclo de vida de nuestros productos más alargado y sostenido en el tiempo.

El último lanzamiento de Samsung es el modelo 870 EVO. ¿Cuáles son las principales características de esta solución?
El 870 EVO es nuestro caballo de batalla, al ser el disco más vendido del mercado. En este sentido, hemos mantenido el listón de la anterior generación en cuanto a garantías, velocidad o fiabilidad. Además, hemos actualizado el software de gestión. La demanda está siendo muy alta.

¿Qué ventajas son las que ofrece Samsung frente a la competencia?
Samsung dispone de una variedad de producto lo suficientemente amplía para poder adaptarse a cualquier escenario y satisfacer las demandas más exigentes de los clientes tanto en el mercado de consumo como en el profesional. ■

UN SSD QUE ACELERA LAS TAREAS INFORMÁTICAS DIARIAS

El SSD 870 EVO une rendimiento, fiabilidad y compatibilidad para los usuarios ocasionales de ordenadores portátiles y de escritorio, pero también para aquellos usuarios de almacenamiento conectado a la red (NAS). La unidad ofrece una mejora de casi un 38% en la velocidad de lectura aleatoria con respecto al modelo 860 anterior, lo que mejora la experiencia de usuario mediante la realización de múltiples tareas, como navegar por la web o simplemente arrancar un PC. EL SSD está disponible con 4TB, 2TB, 1TB, 500GB y 250GB de capacidad.

La solución SATA posee el último controlador y tecnología V-NAND 3-bit MLC (TLC) de la compañía, lo que le permite alcanzar velocidades máximas de lectura y escritura secuencial de 560 y 530 MB/s, respectivamente. Al utilizar un búfer SLC variable, la tecnología Intelligent TurboWrite de la unidad mantiene sus niveles máximos de rendimiento.

Samsung diseña todos los componentes de SSD internamente para garantizar que todas las partes funcionen de manera unificada, lo que permite que 870 EVO ofrezca alrededor de un 30% de mejora en el rendimiento sostenido con respecto a 860 EVO, así como una clasificación de terabytes escritos (TBW) líder en su categoría, de 2.400 TB, o una garantía limitada de 5 años, para su modelo de 4 TB.

Al ofrecer una amplia compatibilidad con muchos dispositivos informáticos, así como con las funciones de PC más actualizadas, la unidad se puede utilizar con todos los dispositivos que tengan una conexión de interfaz SATA de 2,5 pulgadas. Además, con su modo de suspensión de ahorro de energía, 870 EVO es compatible con dispositivos que admiten la función Modern Standby de Windows, lo que ofrece una mayor comodidad a los usuarios de PC.

MÁS INFORMACIÓN

- Toda la información sobre las tendencias tecnológicas en las empresas
- El mercado de almacenamiento SMB crece
- Cuál es la propuesta de Samsung para el mercado de almacenamiento SMB

SERVICENOW MUESTRA EL PODER TRANSFORMADOR DE LOS FLUJOS DE TRABAJO EN KNOWLEDGE 2021

Imaginar ser capaz de resolver cualquier problema al que tu negocio se enfrente. En Knowledge, ServiceNow mostró el poder transformador de los flujos de trabajo, los cuales pueden hacer crecer a las empresas más resilientes y remodelar industrias.

El pasado 11 de mayo arrancó una nueva edición de Knowledge, el evento estrella de ServiceNow, una experiencia digital donde los visitantes pudieron descubrir como la Now Platform ofrece experiencias modernas a clientes y empleados que aceleran el valor y la innovación.

Durante el evento, los asistentes pudieron descubrir cómo las empresas más innovadoras hacen que el mundo del trabajo funcione mejor para las personas a través de las charlas de líderes digitales, socios y expertos. Entre los ponentes destacan Bill McDermott, presidente y CEO de ServiceNow; Dave Wright, director de Innovación de ServiceNow; Chirantan 'CJ'Desai, director de producto de ServiceNow; Kimberly Quan, jefa global de eDiscovery & Digital Forensics de Juniper Networks; Dave Hellman, director de ITSM de Levi Strauss; y Amedeo Guarraci, vicepresidente de PepsiCo.

PALABRAS DE BILL MCDERMOTT

"ServiceNow se encuentra en el centro de la revolución del flujo de trabajo", aseguró Bill McDermott, quien recordó que, gracias a su propuesta, las empresas pueden desarrollar negocios digitales del Siglo XXI. "Quere-

mos que éstas faciliten grandes experiencias a las personas".

Bill McDermott también tuvo palabras para la pandemia. Ésta ha provocado toda una revolución en la forma en la que trabajan, y viven, las personas y tras un periodo en el que el teletrabajo se impuso, ahora su compañía está facilitando "la vuelta segura a las oficinas".

En su opinión, "la plataforma Now está haciendo fluir soluciones que hacen que el trabajo y la vida sean mejores para las personas. El mundo trabaja con ServiceNow".

UN PROGRAMA COMPLETO

En Knowledge 2021 los más de 40.000 registrados pudieron elegir entre cientos de sesiones en las que descubrieron cómo otros clientes y socios utilizan flujos de trabajo para transformar su negocio, y aprender de expertos de la industria y líderes de ServiceNow a abordar temas centrados en el futuro.

Asimismo, también pudieron maximizar sus habilidades en Now Platform con discusiones interactivas y profundas de 30 minutos con expertos de ServiceNow, y acelerar la innovación, aumentar la agilidad y mejorar la productividad con la versión Now Platform Quebec.

Los patrocinadores premier de Knowledge 2021 fueron Accenture, Deloitte, DXC Technology, EY, KPMG y Microsoft.

UN ALUVIÓN DE LANZAMIENTOS

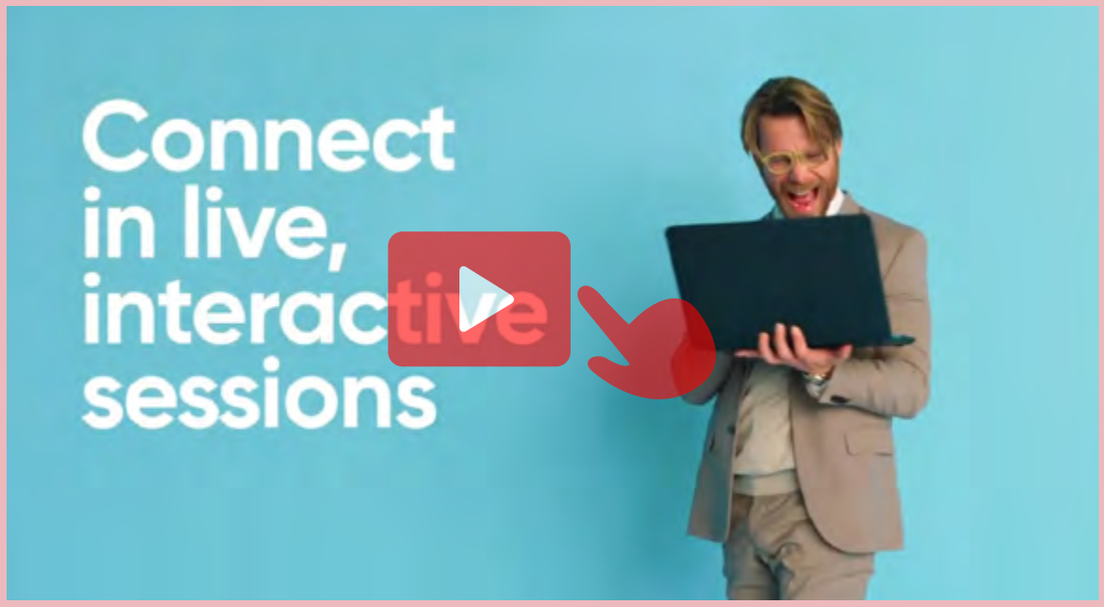
Durante la celebración de Knowledge 2021 ServiceNow anunció nuevas soluciones, innovaciones y movimientos estratégicos que tienen el fin de extender el potencial transformador de los flujos de trabajo para afrontar los grandes cambios a los que se enfrentan tanto los negocios como las personas.

Y es que, para ofrecer una experiencia de servicio al cliente óptima, se debe tener en cuenta todas las personas, los procesos y las herramientas que participan en ka organización. Para ServiceNow debes implementar flujos de trabajo digitales inteligentes que conecten tu front office con los equipos de middle y back office, y los equipos de servicios de campo.

Entre las novedades destacan aquellas orientadas a las industrias de fabricación, salud y "ciencias de la vida", como Operational Management (que ayuda a las empresas de fabricación a hacer que las operaciones sean más eficientes y seguras a la par que mejora la experiencia de los empleados), o Healthcare and Life Sciences Service Management (simplifica las gestiones para mejorar la experiencia del paciente); las que impulsan los esfuerzos que se están realizando en la vacunación (se han anunciado nuevas capacidades en la solución de Gestión y Administración de Vacunas (VAM) de ServiceNow).

Con las nuevas funciones que se han añadido a la solución Workplace Service Delivery y Safe

Toda la información sobre la situación TI de las empresas españolas en @TIyEmpresa_ITDM



ÚNETE A KNOWLEDGE 2021

SERVICENOW ANUNCIA LA COMPRA DE LIGHTSTEP

Consolidando aún más su posición como la plataforma preferida para las empresas digitales, ServiceNow ha anunciado la adquisición de Lightstep, una compañía emergente centrada en la monitorización y observabilidad de aplicaciones de última generación. ServiceNow espera completar la adquisición en el segundo trimestre de 2021.

En un mundo basado en la nube y en DevOps, el software que impulsa a las empresas de hoy en día es cada vez más complejo. Sin embargo, se prevé que las empresas aumentarán su innovación y velocidad sin sacrificar la fiabilidad y el rendimiento. En este sentido, la combinación de ServiceNow y Lightstep ofrecerá una visión operativa exhaustiva para que las empresas puedan utilizar de forma más eficaz las pilas de la tecnología moderna.

"Las empresas están apostando por digitalizarse para prosperar en el siglo XXI, pero la transición a menudo es difícil de afrontar", explica Pablo Stern, SVP & GM, IT Workflow Products, ServiceNow. "Con Lightstep, ServiceNow transformará la forma en que se entregan las soluciones de software a los clientes. Esto, en última instancia, facilitará a los clientes la innovación rápida. Ahora serán capaces de construir y operar su software más rápido que nunca y afrontar la nueva era del trabajo con confianza".

La solución de Lightstep analiza las métricas de todo el sistema y los datos de seguimiento en tiempo real para comprender la causa y los efectos de los cambios en el rendimiento, la fiabilidad y la velocidad de desarrollo de las aplicaciones. Now Platform coordina la respuesta técnica y del equipo, vinculando los conocimientos con las acciones necesarias para impulsar la transformación digital. De esta forma, los clientes podrán supervisar y responder más fácilmente a las alertas e indicadores de criticidad sobre el estado del software aprovechando las capacidades de Lightstep junto con las soluciones de flujos de trabajo de TI de ServiceNow para conectar elementos dispares en una estructura digital sin fisuras. Ello confiere a las empresas la confianza y la claridad necesarias para impulsar una innovación más rápida y mejorar los resultados en el ámbito de la experiencia digital.

Fundada en San Francisco en 2015, Lightstep fue cofundada por el consejero delegado, Ben Sigelman, el director de operaciones, Ben Cronin, y el arquitecto jefe, Daniel Spoonhower, quienes ayudaron a definir la observabilidad moderna con su trabajo previo en materia de rastreo y monitorización de métricas en Google.

"Hoy en día, la observabilidad beneficia principalmente a los equipos de DevOps que crean y despliegan aplicaciones de misión crítica", afirma Ben Sigelman, CEO y cofundador de Lightstep. "Siempre hemos creído que el valor de la observabilidad debería extenderse a toda la empresa, proporcionando una mayor claridad y confianza a todos los equipos involucrados en estos negocios modernos y digitales. Al unirnos a ServiceNow, juntos haremos realidad esa visión para nuestros clientes y ayudaremos a transformar el mundo del trabajo en el proceso, y no podríamos estar más entusiasmados con ello".

Workplace Suite de ServiceNow, las empresas facilitarán la vuelta segura al trabajo de sus empleados. En Knowledge 2021 también se pudo ver la nueva herramienta de planificación Safe Workplace Dashboard, así como se habló de la última adquisición de la firma: Lightstep. ■

MÁS INFORMACIÓN

- Toda la información sobre las tendencias tecnológicas en las empresas
- ¿Cómo está evolucionando el puesto de trabajo?
- Cuál es la propuesta de ServiceNow para ayudar en la transformación del puesto de trabajo

¿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 Centro de Recursos itUser

Tecnología para tu Empresa

KIO Networks

NetApp

NFON Cloud Telephone System

SAMSUNG

servicenow

En tu casa y en mi oficina:

cómo la seguridad se adapta a nuevos escenarios

EN PORTADA

La pandemia de la Covid-19 ha cambiado y transformado los modelos de las empresas en todo el mundo. Se ha constatado un cambio significativo en las prioridades tecnológicas de las organizaciones y se ha impulsado la apuesta por lo digital. Tendencias clave como la adopción de múltiples nubes también conllevan un nuevo panorama de amenazas nuevas y la necesidad de una mejor colaboración.

Al mismo tiempo que se ha acelerado la adopción de los servicios en la nube, ha habido un cambio en las amenazas de seguridad dirigidas a la infraestructura de la nube. El trabajo desde el hogar y los requisitos de continuidad comercial durante la pandemia se correlacionan con un crecimiento en ciertos tipos de ataques maliciosos.

La rápida transición al trabajo remoto y un mayor uso de la tecnología digital ha expuesto a las organizaciones a mayores riesgos de ataques cibernéticos. No es de extrañar, por tanto. que el panorama de la ciberseguridad sea una de las mayores preocupación de los CIOs a nivel mundial.

Según Ángel Ortiz, Director de Ciber-Seguridad en Cisco España, la pandemia ha acelerado la transformación digital del puesto de trabajo. "Seis de cada diez organizaciones han tenido a más de la mitad de la plantilla tele-trabajando durante el confinamiento, y el 37% esperan mantener esta tendencia. Según los datos de Cisco, El acceso seguro es el principal reto para el trabajo remoto (62% de los consultados), seguido por la privacidad de datos (55%) y el control y reforzamiento de las políticas (50%)", detalla.

Mientras, Rubén Vega, Cybersecurity Expert de Excem Technologies, cree que estos cambios dependen de la situación de cada empresa. "Aquellas que ya estaban inmersas en procesos de transformación digital hacia modelos cloud e híbridos las necesidades de cambio han sido mínimas o se han acelerado", explica. "Aquellas en las que su modelo de negocio se basaba única y exclusivamente en modelos on premise han tenido que adaptarse a toda velocidad con los riesgos que eso conlleva".

Tony Hadzima, Country Manager Palo Alto Networks España, asegura que se ha visto una "aceleración de la transición hacia la nube y, también, de la transformación digital, que se ha convertido ahora en una prioridad máxi-

NUEVOS RETOS EN CIBERSEGURIDAD: LA AMENAZA HÍBRIDA

ma para las empresas. Además, dado que los usuarios ahora tienen que acceder a la información empresarial o de la nube desde casa en lugar de la red corporativa, esto también ha llevado a la transformación de la arquitectura de acceso remoto".

Por eso, y como es probable que muchos trabajadores sigan trabajando desde casa, considera que es "importante ampliar la visibilidad de la red empresarial. Como proveedores de seguridad, nuestro objetivo es ayudar a las organizaciones de nuestros clientes a pensar en la red doméstica como una nueva extensión de la red empresarial; una red con un perímetro más amplio".

CAMBIA TAMBIÉN LA SEGURIDAD

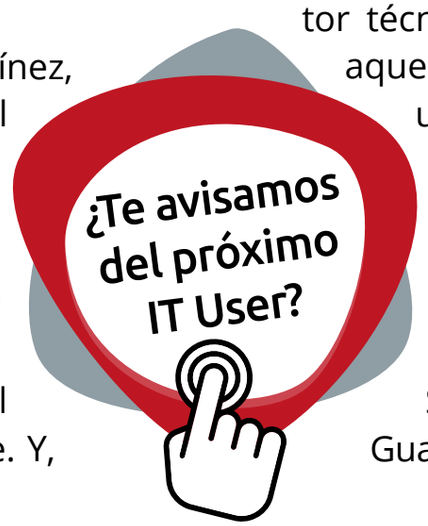
Como vemos, la pandemia ha cambiado muchos negocios, procesos, tecnologías y prioridades. Unos cambios que también se dejan notar en el ámbito de la seguridad y de las necesidades que tienen las empresas para proteger sus activos.

En este sentido, Sergio Martínez, Country Manager de SonicWall para Iberia, argumenta que "la superficie de exposición ha crecido (y crece) exponencialmente, el teletrabajo se ha impuesto y ha venido para quedarse, y el cibercrimen dispone de un arsenal de armas cibernéticas inacabable. Y, además, como decía Margaret Tatcher a un interlocutor del IRA, dispone de todo el tiempo del mundo para acertar una sola vez. La situación es muy preocupante e irá a peor en los próximos años".

Estos cambios en la seguridad han sido, en muchas ocasiones, sobrevenidos. Según Eduardo García Sancho, Sales & Channel Manager de Syneto para Iberia, la mayoría de las empresas españolas han tenido que "adaptarse sobre la marcha al nuevo entorno de trabajo, acelerando en muchos casos los despliegues que tenían previstos para los próximos años". Porque, tal y como expone, en gran parte del tejido empresarial Eesta nueva situación ha venido por sorpresa sin tener realmente un plan realmente elaborado" por lo que, en la mayoría de los casos, "han tenido que llevarse a cabo estrategias sobre la marcha, solventando parcialmente las necesidades que iban surgiendo".

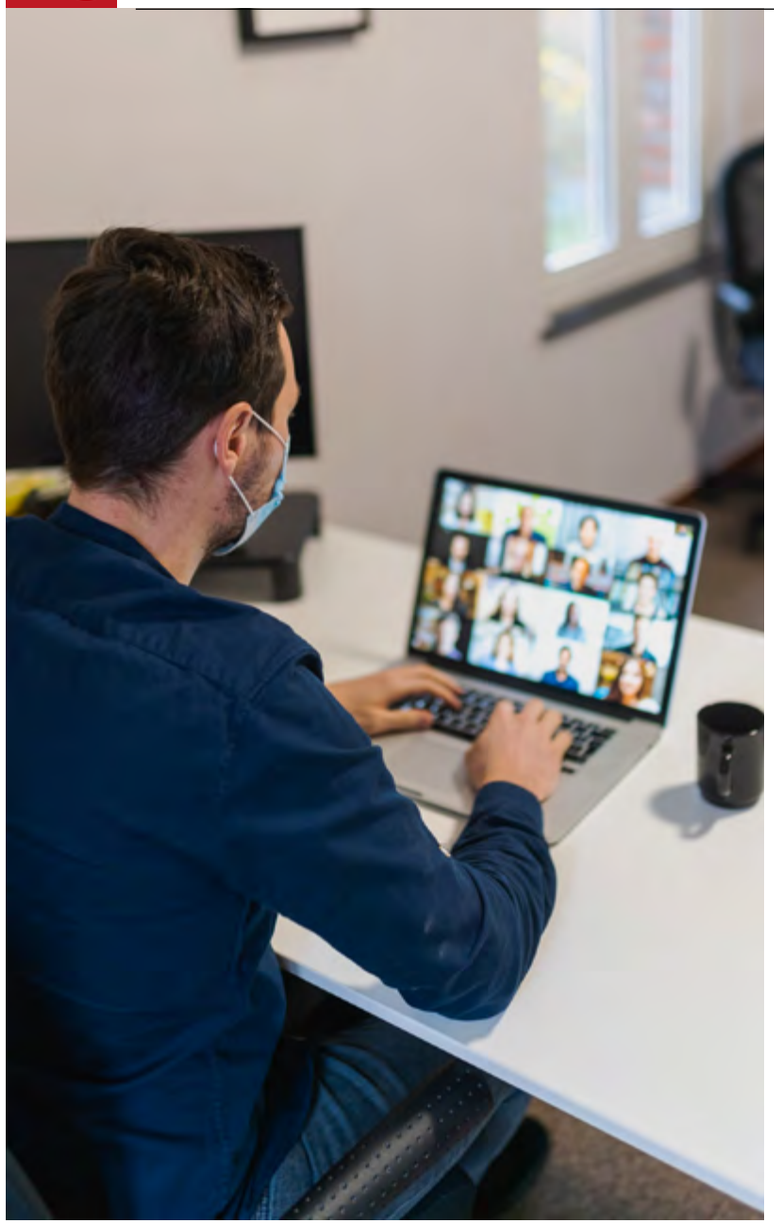
Tal y como resume José de la Cruz, director técnico de Trend Micro Iberia, "salvo aquellas pocas empresas que tuvieran un modelo completo de teletrabajo implementado, podemos afirmar que no estaban preparadas" para los cambios en seguridad que ha provocado la pandemia.

Guillermo Fernández, Manager Sales Engineering Iberia WatchGuard, coincide en que en general, las



"Hay que ir más allá y proteger lo que en Cisco denominamos 'las tres W' del modelo 'zero trust': Workforce, Workload y Workplace (fuerza de trabajo, cargas de trabajo y lugar de trabajo)"

ÁNGEL ORTIZ, DIRECTOR DE CIBER-SEGURIDAD EN CISCO ESPAÑA



empresas no estaban preparadas para algo así, entre otras cosas porque “no era habitual que el trabajador accediera de forma remota a los recursos dentro la compañía, cosa que ahora se produce prácticamente a diario a través de las VPN, aspecto que también entraña sus riesgos”, explica. “La gran mayoría de las empresas, especialmente las pymes, no tenían habilitadas políticas de teletrabajo. Ante esta tesitura provocada por la pandemia, la principal preocupación y la prioridad de las organizaciones era la de dar continuidad al negocio, con lo que las empresas se volcaron en dotar a los trabajadores de herramientas para poder teletrabajar.

En una primera fase, las compañías se preocuparon por dar acceso a esos recursos críticos e información que tenían dentro de la empresa, pero quizá descuidando un poco toda la parte de la securización de esos accesos. Por desgracia, los atacantes siempre están alerta de las nuevas formas que pueden aprovechar para lanzar sus ataques y, en este caso, el trabajo remoto les ha abierto nuevas ventanas para cometerlos”.

Además, Fernández cree que, una vez se cubrió esa primera fase, las empresas “sí han optado por estudiar fórmulas para proteger a los empleados desde el punto de vista de la seguridad, pues se han dado cuenta de que con el teletrabajo están más expuestas a ataques de phishing, ransomware, y otras amenazas”. Tras esa primera fase, “se ha puesto de relieve la necesidad de ampliar la seguridad más allá del perímetro de la red corporativa y llevarla al endpoint y a proteger los accesos. La empresa tiene que tener garantías de que sus empleados se conectan a sus sistemas desde dispositivos seguros y también tener la certeza de que quien se conecta es realmente quien dice ser, y esto solo es posible utilizando una solución de autenticación multifactor (MFA)”.

“Muchas empresas tuvieron que hacer frente al teletrabajo o a un modelo híbrido casi de un día para otro por lo que no pudieron prepararse para los nuevos desafíos que esta modalidad de trabajo conlleva”

RUBÉN VEGA, CYBERSECURITY EXPERT DE EXCEM TECHNOLOGIES

ESTA POLÍTICA YA NO ES TECNOLOGÍA

Los cambios que se han ido produciendo han llegado de forma tan rápida y masiva que a veces puede resultar difícil pararse a pensar cómo ha cambiado la empresa, el negocio y las infraestructuras tecnológicas con las que contamos. Tanto como para que alguna se haya quedado desfasada para dar respuesta a las nuevas necesidades.

El Manager Sales Engineering Iberia WatchGuard se refiere, por ejemplo, a la gestión de las políticas de las contraseñas. "Hasta hace un tiempo la práctica de establecer contraseñas con una cierta complejidad se consideraba más que suficiente, pero a día de hoy si roban la contraseña pueden acceder a todos los recursos críticos de la empresa, incluso remotamente. Por tanto, la identificación o autenticación de los usuarios basándose únicamente en la contraseña es una política que ha tenido que cambiar, pues está demostrado que las contraseñas son una de las vías de entrada principales de vulnerabilidades en las empresas. Solo el año pasado el 80% de las infracciones comenzaron con ataques de fuerza bruta o con la pérdida o el robo de credenciales", relata.

Por tanto, todas las organizaciones, independientemente de su tamaño, deberían, según este responsable, "contar con políticas de seguridad adicionales para las contraseñas. Aquí, MFA ha demostrado ser una fórmula poderosa y eficaz cuando se trata de reforzar

"La automatización y la racionalización de entornos de herramientas de seguridad es clave"

JOSÉ ANTONIO CANO, Director de Análisis y Consultoría de IDC Research España

La pandemia ha hecho que los modelos híbridos de TI sean una realidad en el 90% de las empresas españolas. Este responsable cree que en los primeros momentos de la pandemia, las empresas apostaron por la adopción de soluciones como VPN y autenticación de doble factor, que han sido "determinantes para adoptar una política de seguridad que hiciera frente a esta nueva situación de ruptura de fronteras de seguridad debido al teletrabajo masivo y la adopción acelerada de nuevas herramientas, aplicaciones y servicios en modo digital".

Por eso, cree que en la actualidad las empresas "están más y mejor protegidas frente a las amenazas. Sin embargo, el número ataques y brechas de seguridad y su variedad se incrementa de manera considerable (hay más de 500 ataques semanales a las empresas). Ataques como la suplantación del CEO, Malware, Phising o BEC (business email compromise) se han incrementado de manera espectacular como consecuencia de la masiva adopción de herramientas de colaboración empresarial y el paso a digital de las empresas".

Cano también detalla que el incremento del número de amenazas de seguridad y la falta de habilidades de seguridad son "los principales drivers de cambio en el mercado y el cuello de botella que hace que las empresas necesiten evolucionar su política de seguridad hacia una racionalización del entorno de seguridad que facilite la gestión de las alertas e incidentes de seguridad. Por tanto, en este escenario la automatización y la racionalización de entornos de herramientas de seguridad es clave, así como la automatización y orquestación de la seguridad".

Además, teniendo en cuenta los escenarios híbridos de trabajo, cada vez más populares, considera que hay que tener presente que la seguridad "se mueve de la seguridad perimetral hacia la seguridad del dato. Y el dato se mueve en la nube. Por ello, mover cargas de trabajo y datos a un entorno de nube significa que las responsabilidades de seguridad se comparten entre la empresa y el proveedor de nube. Es lo que se llama modelo de responsabilidad compartida".

Recuerda que en este modelo, "la seguridad de la infraestructura en la nube es suministrado por el proveedor. Es responsabilidad de la empresa utilizar las herramientas nativas del proveedor para proteger los activos y cargas de trabajo que ejecuta en la nube, incluido el código de la aplicación, datos de aplicaciones y acceso a las aplicaciones, todo ello al mismo tiempo que se mantiene el cumplimiento de los requisitos reglamentarios y las mejores prácticas de seguridad".

Porque, tal y como concluye, "el riesgo está asociado a la gestión de la privacidad y seguridad del dato. Por eso es tan importante que el entorno tecnológico híbrido de la empresa esté orquestado y gestionado (de ahí se deriva la soberanía del dato), así como la progresiva integración y racionalización del entorno de seguridad, donde la automatización simplique y ayude a las empresas a gestionar de una forma global las alertas y amenazas de seguridad. De hecho, según datos de IDC en 2023 el 50% del presupuesto de seguridad se destinará a mantener un framework unificado de seguridad".

la seguridad corporativa e individual. La autenticación es la piedra angular de una buena seguridad, y la autenticación multifactor significa que los usuarios deben proporcionar al menos un token adicional, además de su contraseña, para acceder a una cuenta. Estos tokens de autenticación suelen ser algo que uno es (huellas dactilares biométricas o escaneos faciales), algo que uno tiene (como una llave hardware o un teléfono móvil) y algo que uno sabe (como una contraseña). MFA permite garantizar que, incluso si un atacante consigue acceder a uno de estos tokens, como una contraseña de usuario, no podrá iniciar sesión sin el segundo (y a veces tercer) token de autenticación". Además, concluye que "es una solución sencilla cuando se trata de abordar los problemas generalizados y persistentes relacionados con la falta de seguridad de las contraseñas, y debería ser un objetivo prioritario para reforzar la seguridad en las empresas".

Mientras, José de la Cruz cree que todas aquellas políticas que se basaban en la premisa de que el empleado trabaja únicamente desde la oficina han quedado desterradas. "El famoso perímetro ha quedado completamente difuminado y se ha trasladado a las conexiones a Internet de los empleados. Ahora más que nunca es prioritario aplicar una protección multicapa y del endpoint".

Un punto en el que parece coincidir con el Sales & Channel Manager de Syneto para Iberia, quien considera que al haber nuevos hábitos "se han tenido que desarrollar nuevas políticas de seguridad para solventar los nuevos problemas relacionados con el tele trabajo. Los accesos remotos, la seguridad de los mismos y la preparación de los sistemas a esta nueva realidad han tenido que adaptarse en tiempo récord para poder seguir adelante con la nueva normalidad, provocando una aceleración de la transformación digital".

Para Sergio Martínez, más que cambiar las políticas, lo que ha cambiado radicalmente es el entorno. "Las ideas siguen siendo las mismas, pero el modelo a defender no es el mismo. De un modelo bastión, se ha pasado a un modelo aeropuerto en pocos días. Y las credenciales, más que nunca, son la joya de la corona y el nuevo perímetro a defender. Y no estamos preparados para este nuevo paradigma", detalla.

PRINCIPALES AMENAZAS

Lo que también parece que están cambiando son algunas de las amenazas. Desde Palo Alto explican que, dado el rápido aumento de la adopción de la nube pública, "existe una mayor necesidad de proteger los datos corporativos almacenados allí. Muchas empresas tienen proveedores de nube diferentes, por lo que también es importante garantizar políticas consistentes en entornos de múltiples nubes". Pero, además, creen que otro riesgo es que el usuario acceda desde fuera de la red corporativa. "Hay que autenticar a los usuarios, asegurar ese tráfico, asegurarse de que los sistemas

"Con el rápido aumento de la adopción de la nube pública, también existe una mayor necesidad de proteger los datos corporativos almacenados allí"

TONY HADZIMA, COUNTRY MANAGER
PALO ALTO NETWORKS ESPAÑA

CONTENIDOS

puedan hacer frente a esa demanda y también es importante que tengan el mismo nivel de control y seguridad en la nube tal como lo hacen en los sistemas centrales corporativos. Esto destaca la necesidad de extender la seguridad de los sistemas corporativos centrales a la nube pública".

Para Rubén Vega, muchas empresas tuvieron que hacer frente al teletrabajo o a un modelo híbrido casi de un día para otro por lo que "no pudieron prepararse para los nuevos desafíos que esta modalidad de trabajo conlleva. Por ejemplo, es el caso de las VPNs, que en la mayoría de los casos cuentan con infraestructuras de seguridad antiguas y desactualizadas que conllevan vulnerabilidades no cubiertas por estas infraestructuras no actualizadas".

Poniendo datos sobre la mesa, el Director de Ciber-Seguridad en Cisco España asegura que el 61% de las organizaciones han sufrido un incremento de ciber-ataques superior al 25% desde el inicio de la pandemia. "Empresas y Administraciones se enfrentan a tres retos principales: más vectores de ataque, mayor sofisticación y proliferación de las amenazas y mayor complejidad de las soluciones para defenderse. Con usuarios, dispositivos y nubes extendiéndose fuera del perímetro de red tradicional, se requieren nuevas aproximaciones de seguridad para un acceso seguro y fiable y que no afecte a la experiencia de usuario".

> "El modelo ha cambiado, y la forma de asegurarlo, también. La defensa de las credenciales es uno de los puntos más relevantes"
>
> SERGIO MARTÍNEZ, COUNTRY MANAGER DE SONICWALL PARA IBERIA

LO IMPORTANTE Y LO URGENTE

Hay veces que lo urgente nos hace descuidar lo que es importante, algo que puede tener importantes consecuencias cuando hablamos de seguridad. En este sentido, el director técnico de Trend Micro Iberia puntualiza que quizás el punto más olvidado sea el de la visibilidad. "Es importante proteger los datos, pero debemos asumir que, en algún momento nuestros datos, sistemas, aplicaciones, etc. estarán comprometidos", nos cuenta, añadiendo que es precisamente aquí donde el concepto de XDR cobra fuerza "para ayudar a dotar a las empresas de visibilidad sobre lo que ocurre en sus entornos. Esto les ayudaría a detectar de manera prematura ataques o efectuar una investigación en detalle de cualquier incidente de seguridad".

Mientras, Ángel Ortiz cree que si algo se está descuidando son las soluciones de autenticación y control de accesos "que protegen cómo los usuarios y los dispositivos acceden a las aplicaciones, los recursos y los servicios desde cualquier lugar". En su opinión, "hay que ir más

allá y proteger lo que en Cisco denominamos las 'tres uves dobles' del modelo 'zero trust': Workforce, Workload y Workplace (fuerza de trabajo, cargas de trabajo y lugar de trabajo)".

Como nos cuenta el responsable de Syneto, "siempre hay que incidir en los aspectos principales para evitar y prevenir los ataques de ciberdelincuentes". Más concretamente, según esta empresa hay 5 grandes medidas de implantación imprescindible para la PYME:

1. **Educación y formación** de los trabajadores en medidas de ciberseguridad
2. **Copias de seguridad automatizadas,** frecuentes y protegidas de ciberataques
3. **Minimizar las superficies de ataque** y protegerlas en la medida de lo posible
4. **Crear un plan de respuesta a incidentes** (recuperación anti desastre) garantizado, rápido y lo más automatizado posible para minimizar las paradas de producción
5. **Supervisión y protección** de los puntos finales

EL PELIGRO QUE LLEGÓ CON LA NUBE

Como es bien sabido, las tecnologías en la nube han tenido su espaldarazo definitivo durante la pandemia. Por eso hemos querido saber si este uso masivo de las tecnologías en el cloud ha conllevado que aparezcan nuevos desafíos en materia de seguridad.

El Cybersecurity Expert de Excem Technologies expone, por ejemplo, muchas empre-

> "El famoso perímetro ha quedado completamente difuminado y se ha trasladado a las conexiones a Internet de los empleados"
>
> JOSÉ DE LA CRUZ, DIRECTOR TÉCNICO DE TREND MICRO IBERIA

SEGURIDAD EN LA INFORMACIÓN - CRIPTOGRAFÍA SIMÉTRICA Y ASIMÉTRICA

sas han escogido apostar por un almacenamiento en la nube que facilita el acceso a los documentos por parte de la plantilla que se encuentra teletrabajando. "No obstante, las empresas deben tener en cuenta que estas nuevas herramientas requieren de controles de protección adecuados ya que, si llegan a sufrir un ciberataque, éste podría provocar la inhabilitación total o parcial de los servicios. La forma de prevenir esto es contar con un colaborador homologado de cloud y ciberseguridad que ofrezca soluciones que se adapten a las necesidades de cada compañía. También es importante formar y concienciar a los empleados de los riesgos que conlleva el trabajar en entornos en la nube".

Es decir, que como constata Guillermo Fernández, la nube "ha traído nuevos riesgos y estos están principalmente relacionados con las credenciales y su gestión. Es clave insistir en la importancia que tienen las políticas de autenticación multifactor (MFA) para confirmar que la persona que accede a la red y recursos corporativos es realmente quién dice ser".

Ante estos nuevos escenarios, Tony Hadzima señala que las empresas deben considerar la necesidad de "tener políticas de seguridad consistentes tanto en entornos físicos como en la nube, porque los equipos de seguridad son a menudo bastante pequeños, pero tienen que lidiar con muchos ataques y operar muchos sistemas de seguridad, herramientas, tecnologías y proveedores. Esto destaca otra área clave en la que pensar: tratar de reducir la cantidad de proveedores y herramientas. Si una empresa tiene 50 o 100 herramientas de seguridad diferentes, pero no tiene la integración adecuada, aumenta mucho la complejidad".

> "Siempre hay que incidir en los aspectos principales para evitar y prevenir los ataques de ciberdelincuentes"
>
> EDUARDO GARCÍA SANCHO, SALES & CHANNEL MANAGER DE SYNETO PARA IBERIA

Porque, como determina el responsable de Trend Micro, "cuanto más compleja y heterogénea sea nuestra arquitectura, más relevancia cobrará la visibilidad". José de la Cruz considera que, "asumiendo la premisa establecida por Zero-Trust (asumir que vamos a ser atacados y probablemente con éxito) debemos implementar mecanismos que nos ayuden a detectar esos ataques lo más temprano posible, independientemente de su origen y destino (red, endpoint, cloud, correo, etc.) y dotando de una capa de correlación que simplifique las alertas recibidas mostrando únicamente aquellas que sean relevantes".

Tal y como concluye el Director de Ciber-Seguridad en Cisco España, "estamos en la era multi-cloud. Con un 60% de las organizaciones que esperan que la mayoría de las aplicaciones

estén en la nube para este año 2021 y en torno al 50% de la fuerza de trabajo operando de forma remota, el nuevo modelo SASE (Secure Access Service Edge) que converge servicios de red y de seguridad permite conectar de forma segura a cualquier usuario o dispositivo a cualquier aplicación. Y con la mejor experiencia. SASE se basa en la convergencia de SD-WAN administrada desde la nube y la seguridad Cloud, dos capacidades clave en las que Cisco es pionero y un líder contrastado, ayudando a las fuerzas de trabajo distribuidas a mantenerse conectadas y seguras. Más de 20.000 organizaciones de todo el mundo han comenzado el camino hacia SASE mediante la implementación de SD-WAN de Cisco, y más de 22.000 han adoptado los servicios de seguridad en la nube de Cisco Umbrella".

"La digitalización, necesaria para formar parte del mercado global y digital, no es concebible sin ciberseguridad"

ELISA VIVANCOS, técnico de Ciberseguridad para Empresas de INCIBE

A río revuelto, ganancia de pescadores. El impulso de tecnologías "que hasta entonces no eran masivos, entre otros, el teletrabajo, el BYOD, el ecommerce, el cloud y las teleconferencias" hizo que los ciberdelincuentes se esmeraran en aprovechar la ocasión para su beneficio con "señuelos y falsos reclamos relacionados con las preocupaciones de las empresas (hidrogel, pantallas protectoras, ayudas públicas, etc.) y explotando las vulnerabilidades de esas tecnologías que empezaron a usarse de forma intensiva".

Elisa Vivancos, técnico de Ciberseguridad para Empresas de INCIBE, cree que la dependencia tecnológica de los negocios "es lo que condiciona sus necesidades de seguridad. En este sentido, las empresas que hayan adoptado algún grado de digitalización superior al que tenían antes de la pandemia, las cuales se espera vayan a mantenerlo o incluso aumentarlo, tendrán necesidades crecientes de ciberseguridad. Así, habrán de incorporar a sus análisis de riesgos de ciberseguridad los cambios en sus procesos de negocio derivados de estos nuevos o reformados usos de la tecnología".

Por eso, considera que todas aquellas empresas que hayan adoptado nuevos usos de la tecnología "se han de actualizar las políticas de seguridad afectadas", aunque sean cambios que "trastocan los procesos de negocio y los empleados han de conocer y aplicar las restricciones y los usos permitidos en cada caso".

"Las empresas han de revisar las políticas relacionadas con los usos tecnológicos que afectan, en particular, a los procesos que llevan consigo un tratamiento de datos personales para proteger la privacidad de los usuarios. Revisarán, entre otras, las políticas de almacenamiento en la nube, o en dispositivos en local, políticas de teletrabajo, uso de herramientas de teleconferencia, de cifrado o políticas de control del acceso remoto".

Tras recomendar las consultas en el canal especializado en empresas de INCIBE, Protege tu Empresa, cree que antes de valorar los riesgos hay que hacer un inventario de activos, es decir, "listar y localizar todo lo que tiene valor para la empresa, en el momento actual" para, posteriormente, determinar para cada activo "la importancia de los parámetros de ciberseguridad, al menos, de la confidencialidad, integridad y disponibilidad necesarias". Esto permitirá, según esta responsable, analizar las amenazas existentes para cada activo, la probabilidad de que ocurran, con la ayuda de técnicos con experiencia, y el daño que en este caso pueden producirnos.

Esta experta reconoce que durante todo este tiempo las demandas de >>

ANTE LOS MODELOS HÍBRIDOS

Rubén Vega, Cybersecurity Expert de Excem Technologies, considera que, ante la popularización de los modelos híbridos, además de los básicos en materias de seguridad como son los antivirus, firewall y VPNs, "las empresas deberían apostar por los servicios de un Centro de Operaciones de Seguridad. Asimismo, es recomendable realizar simulacros y pruebas periódicamente, que sirvan para evaluar y conocer el estado real de las infraestructuras de seguridad y evitar así futuras brechas. Por otro lado, no hay que olvidar las soluciones que protegen a todos los equipos frente a las amenazas más comunes como los ataques de ransomware".

Mientras, Guillermo Fernandez, Manager Sales Engineering Iberia WatchGuard, cree que es necesario interiorizar que, independientemente de la situación, "el trabajo de formación y concienciación de los empleados y su educación en temas de ciberseguridad es algo crucial y, por

>> charlas de sensibilización sobre ciberseguridad en teletrabajo han sido altas, "lo que demuestra un alto nivel de preocupación por el posible incremento de incidentes ante las nuevas situaciones, lo que se constata con los datos de la Línea de Ayuda en Ciberseguridad e INCIBE-CERT sobre ataques que aprovechan vulnerabilidades de VPN y otros mecanismos de acceso remoto, herramientas de teleconferencia o servicios en la nube usados en esta situación. También hemos apreciado un incremento de casos de fraude o intentos de distribución de malware con temáticas relacionadas con la pandemia, lo que, a pesar del riesgo, ha supuesto una interesante oportunidad para concienciar sobre estas amenazas".

Antes de la pandemia, no todas las empresas eran conscientes de su creciente dependencia de la tecnología y de cómo ésta es inseparable de la ciberseguridad para mantener su negocio en un escenario digital. La pandemia ha puesto sobre la mesa que la digitalización, necesaria para formar parte del mercado global y digital, "no es concebible sin ciberseguridad que es imprescindible para la prosperidad de los negocios y de la sociedad en su conjunto".

Además, cree que se está produciendo un cambio de mentalidad respecto a la ciberseguridad gracias, en parte, a la pandemia. "Se están abandonando modelos de adopción de la ciberseguridad puramente reactivos, cosméticos o basados en el cumplimiento, es decir, para evitar sanciones y cubrir el expediente. Cada vez son más evidentes la seriedad y los graves daños económicos y reputacionales que producen los incidentes de ciberseguridad en las organizaciones, siendo no pocas las que no pueden superarlos. Esperamos que esto se convierta no solo en una mejor protección de sus activos, una mayor sensibilización de sus plantillas y mayores inversiones en soluciones de ciberseguridad, sino también en un mayor apoyo a los esfuerzos colectivos por desenmascarar a los ciberdelincuentes y hacer posible, junto con los avances legislativos, un entorno digital más seguro", señala.

Respecto a la creciente adopción de sistemas en la nube, cree que es "necesario elevar la cultura de ciberseguridad de empresarios y empleados para no caer en engaños. La nube puede ser segura pero también puede tener riesgos, por lo que hemos de ser precavidos y analizarlos antes de implantarla". Además, y dado que cada proveedor va a fijar unas condiciones, también en materia de seguridad, recomienda que cada negocio valore si los servicios "no solo cumplen la funcionalidad necesaria, si no nuestros requisitos de ciberseguridad que han de ser exquisitos por nuestra propia supervivencia. Estos requisitos de confidencialidad, integridad y disponibilidad hemos de plasmarlos en los acuerdos de nivel de servicio, de manera que podamos exigirlos cuando sean necesarios, incluso después de finalizado el servicio con aspectos tan importantes como cuánto tiempo van a mantener nuestros datos o las opciones de portabilidad a otros proveedores".

Por último, Elisa Vivancos cree que los principales riesgos de los entornos híbridos se derivan de "la pérdida de control sobre nuestros activos en particular si están distribuidos entre la parte pública y la privada, la confidencialidad y seguridad de nuestros datos, máxime si son datos de carácter personal, la disponibilidad del servicio y el acceso remoto con su dependencia de terceros".

eso, insistimos para que las empresas para que establezcan programas de educación para a sus empleados -remotos o no-, ya que estos pueden desempeñar un papel crítico en la defensa".

Más concretamente, en el caso de los trabajadores remotos, "nuestro consejo es que preparen una lista de verificación centrándose en las buenas prácticas que los teletrabajadores pueden adoptar". Por eso, ofrece una serie de consejos para la seguridad del trabajo remoto:

- **Hacer que la red doméstica sea privada:** proteger la oficina doméstica asegurando la red inalámbrica
- **Utilizar contraseñas robustas y seguras** para proteger la identidad y las credenciales de la empresa para evitar malware
- **Tener cuidado con el phishing:** evitar los ataques de phishing revisando cuidadosamente los correos electrónicos que parecen extraños o inesperados
- **Usar una conexión VPN:** utilizar una conexión VPN para redirigir el tráfico de Internet a través de un servidor protegido.
- **Proteger el endpoint**

Tal y como concluye Eduardo García. "el trabajo inteligente se ha convertido en una práctica casi común" por lo que "las empresas necesitan poder ofrecer un acceso seguro, rápido y sencillo a las aplicaciones y datos corporativos". Además, entiende que los modelos híbridos "son mucho más flexibles y económicos, pero es cierto que hay que tomar medidas básicas para protegerlos correctamente y establecer los planes de contingencia que permite esta flexibilidad de sistema". ■

MÁS INFORMACIÓN

- Cómo la nube híbrida cambia el juego de la seguridad
- 7 consejos para proteger los datos de tu empresa
- Las bases para la protección de datos sensibles en cualquier organización
- Descubriendo SASE y las últimas tecnologías de detección de amenazas
- 2020 Cyber Threatscape
- Anatomía del ataque a una cuenta privilegiada

"Se ha puesto de relieve la necesidad de ampliar la seguridad más allá del perímetro de la red corporativa y llevarla al endpoint y a proteger los accesos"

GUILLERMO FERNANDEZ, MANAGER SALES ENGINEERING IBERIA WATCHGUARD

Solución de impresión para entornos hiperdistribuidos

Para la mediana y gran empresa con empleados en **teletrabajo**

9,90 € empleado/mes*

Descubre más >

*Precio por puesto de trabajo basado en 25 equipos, modelo MFC-L2710DW, con un contrato a 4 años y un volumen de 200 páginas/mes. Impuestos no incluidos.

Nuevas corrientes alrededor de la impresión y gestión de documentos, a debate

La inmensa mayoría de las organizaciones espera que la digitalización del papel sea importante para sus negocios. El crecimiento en la digitalización también impulsará un aumento de la necesidad de flujos de trabajo de información digital e impresa mejor integrados. Los proveedores de impresión y gestión documental necesitan aprovechar esta oportunidad para construir una ventaja competitiva con servicios de mayor valor.

De éstas y otras cuestiones debatimos junto a José Ramón Sanz, responsable de marketing de producto de Brother Iberia; Gabriel Salafranca, responsable del equipo Digital DNA en Paradigma; Albert Pitarch, director de desarrollo de Negocio de Seidor Printing; y Carlos Santiago, director del área Context & Cognitive en VASS.

Y para comenzar, quisimos saber cómo está siendo 2021 y, en este sentido, José Ramón Sanz nos explica que "en lo referido a la venta de hardware, el año ha empezado fuerte. La tendencia que veíamos en 2020 del incremento de la demanda de productos destinados al teletrabajo se ha mantenido, y la vuelta paulatina de las empresas a las oficinas también ha generado que la demanda de los productos orientados a este segmento se incremente. La demanda de producto compacto sigue siendo fuerte, pero la demanda de producto un poco

NUEVAS CORRIENTES ALREDEDOR DE LA IMPRESIÓN Y GESTIÓN DE DOCUMENTOS, A DEBATE

más grande, para oficina, también tiene fuertes incrementes, un 40% de crecimiento sobre el año anterior, y por encima de lo que eran las ventas en 2019. La parte más débil son los equipos grandes, donde sigue habiendo un decremento de las ventas con respecto a 2020 y 2019. La vuelta paulatina a las oficinas convive con un modelo híbrido, lo que lleva una gran complejidad al trabajo de los equipos de TI por tener que mantener servicios tanto en la oficina como en el domicilio".

Gabriel Salafranca explica que "vemos una apuesta por lo digital y los documentos físicos tienen cada vez menos sentido, si bien la identidad de la compañías estaba muy influenciada por los documentos físicos. La vuelta a la normalidad nos ha traído grandes cementerios de información digital, con muchos archivos deslocalizados, en muchas ubicaciones, y es un terreno que hay que explorar, si bien hemos alcanzado un nivel de digitalización que no habíamos conseguido en años anteriores. Estamos, en definitiva, en un momento de cambio, con entornos híbridos y los cambios necesarios para adaptarse a él".

Para Albert Pitarch, "el año ha empezado con optimismo. Había ganas de volver a lo físico, a la oficina, aunque no sea al 100%".

Concluye Carlos Santiago esta primera ronda de opiniones señalando que "2020 fue un año de reducción de costes para las empresas con un modelo de teletrabajo. Todos hemos estamos en la misma realidad. Los empleados han sido más productivos y hemos solventado con nota la realidad. Y en este contexto, había que acometer proyectos para reducir el consumo de papel, lo que implica cambios muy profundos. A lo largo de este año, las empresas que ya han emprendido la transformación la culminarán de forma correcta, pero aquellos que no han empezado lo tendrán más complicado".

PROCESOS DE DIGITALIZACIÓN DE LA GESTIÓN DE DOCUMENTOS Y FLUJOS DE TRABAJO

Muchas empresas se han encontrado con mucha información en formato físico y eso ha dificultado las tareas de personas que tenían que trabajar en remoto. En opinión de Gabriel Salafranca, "las compañías que dieron pasos en la digitalización tienen un camino recorrido que les ha facilitado las cosas, si bien hay empresas que por la reducción de costes no han podido avanzar en estos proyectos".

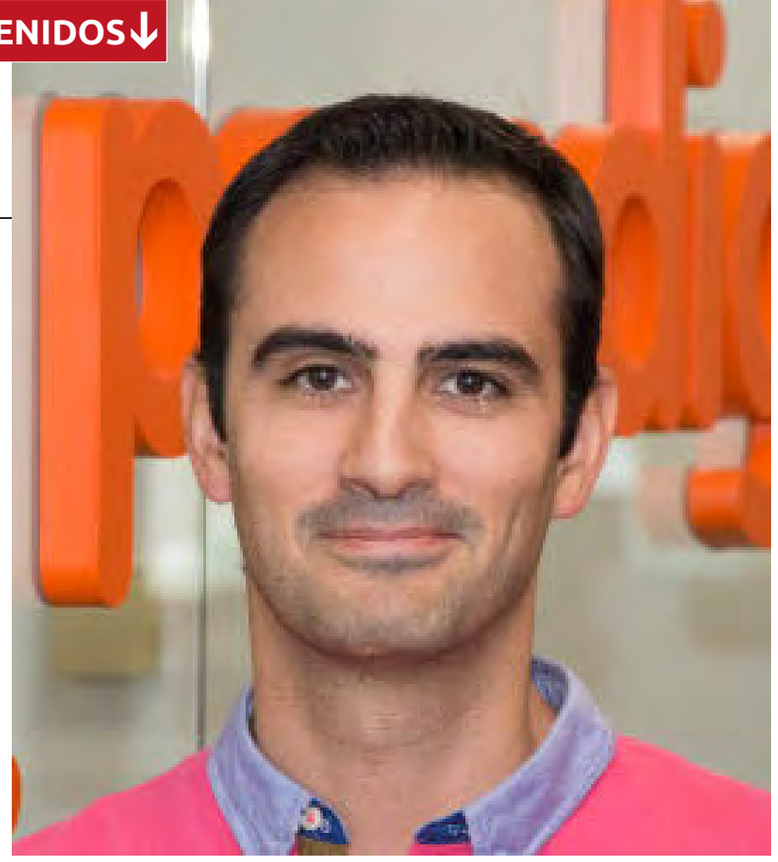
En palabras de Albert Pitarch, "todos estamos de acuerdo en que hay que digitalizar, aunque algunas empresas no tenían la capacidad financiera necesaria. El mercado está ayudando mucho, tanto las empresas grandes como las pequeñas, que emplean herramientas para avanzar en sus proyectos de digitalización".

"La vuelta paulatina a las oficinas convive con un modelo híbrido, lo que lleva una gran complejidad al trabajo de los equipos de TI por tener que mantener servicios tanto en la oficina como en el domicilio"

JOSÉ RAMÓN SANZ, RESPONSABLE DE MARKETING DE PRODUCTO DE BROTHER IBERIA

“La vuelta a la normalidad nos ha traído grandes cementerios de información digital, con muchos archivos deslocalizados, en muchas ubicaciones, y es un terreno que hay que explorar”

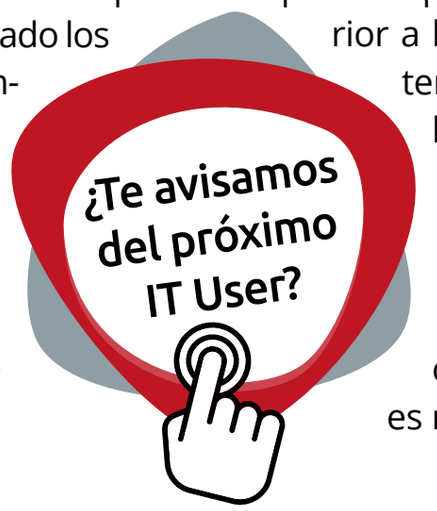
GABRIEL SALAFRANCA, RESPONSABLE DEL EQUIPO DIGITAL DNA EN PARADIGMA



Añade Carlos Santiago que “la oficina sin papeles es un avance hacia lo digital, y el uso de herramientas adecuadas ayuda mucho a incrementar la ingesta de datos en los sistemas, ahorrando tiempos a los trabajadores. Por otra parte, la gestión de documentos sigue avanzando, tanto en la empresa privada como en la Administración Pública”.

NUEVO MODELO DE TRABAJO

Todo parece indicar que avanzamos hacia un modelo híbrido de trabajo, y, en esta nueva realidad, deben integrarse los procesos de gestión documental e impresión. En palabras de Albert Pitarch, “las herramientas están disponibles para cualquier necesidad, pero han cambiado los mecanismos que adoptamos para encontrar la mejor solución para cada cliente. Tenemos una realidad con un puesto de trabajo diferente, que es móvil, y necesita las mismas capacidades cuando está en remoto. Debemos ofrecerle soluciones para que el trabajo sea igual esté donde esté”.



Para José Ramón Sanz, “en este nuevo modelo híbrido vemos que la impresión no está siendo crítica para las empresas. No es crítico para los procesos. Hemos visto procesos de digitalización interna de las empresas como normativas que las afectan, y la impresión es una herramienta que confiere productividad al empleado, porque la empleamos para tomar decisiones. Vemos muchos ejemplos en que el que imprime el documento es el único que lo lee, y algunos informes apuntan a que la vida media de un documento impreso es de 1 día”.

“Es clave”, continúa, “el acceso a los datos, porque muchas empresas estaban informatizadas pero no permitían el acceso desde el exterior a la información, y es algo que han tenido que cambiar. Destacan también las soluciones cloud para la captura, más si estamos haciendo trabajo en un entorno híbrido. En el día a día, tenemos la necesidad de capturar información desde cualquier tipo de dispositivo, pero es necesario poder trabajar con esos datos, y son necesarias herramientas para ello, herramientas efectivas y seguras”.

Añade Carlos Santiago que estos modelos híbridos implican que las personas “estén preparadas para trabajar de forma híbrida. Es lo que denominamos smart working”.

Está claro, apunta Gabriel Salafranca, “que actualmente tenemos una conciencia mucho más ecológica, pero lo físico va a seguir existiendo, porque provoca una sensación que lo digital todavía no ha llegado a alcanzar. Para trabajar en equipo, por ejemplo, es más efectivo contar con documentos impresos. Así que debemos aprovechar la tecnología para poder conectar lo físico y lo digital”.

SERVICIOS GESTIONADOS DE IMPRESIÓN

Una de las tendencias que más ha avanzado en los últimos trimestres son los servicios ges-

tionados de impresión porque, como apunta Albert Pitarch, "estos servicios gestionados son los que mejor se adaptan a un entorno cambiante. Si hay que ofrecer servicios en ubicaciones diferentes o asistir equipos en el domicilio de los trabajadores, la tecnología está disponible, solo es necesario implementarla de forma diferente. Lo importante es aportar valor, ya sea de una forma o de otra".

Por su parte, José Ramón Sanz indica que "la evolución de la impresión gestionada, con el uso de tecnologías cloud, ha sido fundamental para poder atender las necesidades independientemente de dónde estuviera ubicada la impresora. En un entrono disperso, con personas trabajando en cualquier ubicación, con gran variedad de marcas y modelos, el hecho de que las empresas pudieran tener servicios gestionados para cuestiones tan básicas como el control y reposición de consumibles, ha sido algo que ha adquirido mucho valor ante los decisores, tanto de TI como de servicios generales".

IMPRESIÓN RESPONSABLE

José Ramón Sanz explica que la impresión responsable "va a ser una realidad en poco tiempo. Toda la industria de impresión va a ser neutra en todos los niveles. Nosotros hemos trabajado mucho para concienciar a clientes y distribuidores a la hora de elegir el dispositivo más adecuado con las características necesarias, como la impresión a doble cara, frete a la elección del dispositivo más barato. Esto es fundamental, como el resto de impulsos y acuerdos globales para el uso de papel sostenible. Tenemos que estar eco-concienciados a la hora de imprimir".

En palabras de Albert Pitarch, "en ocasiones es mayor el valor que aporta una impresión que el posible efecto medioambiental que pueda llegar a generar".

En muchas ocasiones, comenta Carlos Santiago, se han dejado de imprimir trabajos en algunos entornos que generaban un gran consumos de recursos, "pero la implementación de flujos digitales ha permitido que la información circule".

"Las herramientas están disponibles para cualquier necesidad, pero han cambiado los mecanismos que adoptamos para encontrar la mejor solución para cada cliente"

ALBERT PITARCH,
DIRECTOR DE DESARROLLO DE NEGOCIO DE SEIDOR PRINTING

AVANCES EN LA GESTIÓN DOCUMENTAL

Si hablamos de avances en la gestión documental, Carlos Salafranca apunta al "segmento del Retail y, por extensión, el comercio electrónico", pero también la Administración Pública es un claro ejemplo, tal y como comenta Gabriel Salafranca. "Hace diez años los usuarios en la Administración te pedían un botón que les permitiera imprimir todo. A medida que hemos evolucionado en las medidas digitales, hemos ganado en conciencia de lo que es necesario imprimir, porque el problema no es la impresión, sino lo que se hace con los documentos impresos. Muchas veces necesitan mover información y adecuarse a las normativas, lo que ha provocado grandes cambios".

Apunta Albert Pitarch "la gran oportunidad de la PYME, para que avancen en su optimización. Hay herramientas para ayudarles a controlar y gestionar su información".

En el caso de José Ramón Sanz, "destaca también lo relacionado con la micrologística, esos pequeños establecimientos tradicionalmente locales que han tenido que dar el paso a lo digital y adaptar, no solo el acceso de los clientes, sino también sus procesos de gestión. Hacerlo todo digital ha sido la esencia para mantenerse en un mercado tan competitivo".

Y AHORA ¿QUÉ?

Desde Brother esperan "que tras un año de grandes cambios, la realidad se asiente y pase a formar parte de lo cotidiano. A nivel de producto esperamos que tome protagonismo el equipo multifunción, en empresa y domicilio, en detrimento de las impresoras y los escáneres documentales. A nivel de gestión, todo lo relacionado con la nube o la impresión remota es lo que más se va a desarrollar, impresión sin drivers, adecuada y segura. Hablando de gestión documental, seguirá siendo importante la gestión de flujos de trabajo, pero como van a ser más digitales, el papel estará en la salida de la información más que en la entrada, con dispositivos más complejos en su funcionamiento pero sencillo para el usuario".

En Paradigma abogan "por los entornos híbridos y es ahí donde debemos buscar el valor. Estamos en la era de las decisiones basadas en los datos y, para ello, hay que aprovechar lo digital, pero no todo tiene que serlo". A nivel de servicios gestionados, estiman en Seidor Printing que lo importante captar la transversalidad "y, sobre todo, transformar esta solución en algo fácil e inteligente, porque digitalizar por digitalizar no tiene sentido, como imprimir por imprimir tampoco. Además, no podemos olvidar la conciencia ecológica: quizá hay que imprimir menos, pero hay que imprimir mejor".

Finalizamos con la opinión de VASS, cuyo portavoz comenta que "la consecuencia de la transformación está generando un crecimiento exponencial de los contenidos, y esta información es necesario que sea indexada y gestionada para aportar valor, así que las herramientas basadas en IA que sean capaces de gestionar información, independientemente del formato, son las que harán triunfar a las compañías". ■

> "La gestión de documentos sigue avanzando, tanto en la empresa privada como en la Administración Pública"
>
> CARLOS SANTIAGO, DIRECTOR DEL ÁREA CONTEXT & COGNITIVE EN VASS

MÁS INFORMACIÓN

Nuevas corrientes alrededor de la impresión y gestión de documentos, a debate

18
JUNIO
11:00 CET

REGISTRO

El fenómeno del Device as a Service y las oportunidades para el canal TI

24
JUNIO
11:00 CET

Mejorando la experiencia del trabajador remoto

REGISTRO

#ITWEBINARS

29
JUNIO
11:00 CET

Entendiendo la Era del dato: tecnologías y propuestas para gestionar la “datificación”

REGISTRO

NO SOLO it

PANEL DE EXPERTOS

TECNOLOGÍA Y NEGOCIO

Verdades y falacias del estado real de la digitalización empresarial y transformación digital en España

Jorge Díaz-Cardiel,
socio director general de
Advice Strategic Consultants

ENCUENTROS Y DESENCUENTROS CON LA COMUNICACIÓN

Los seis sombreros en la comunicación

Manuel López,
asesor de comunicación

REFLEXIONES éTICas

Un café con el Homo Virtualis

Màrius Albert Gómez,
Experto en digitalización
e Innovación y humanista
por convicción

MARKETING Y CONSUMO

Neurociencia y medios de pago

José Manuel Navarro,
CMO MOMO Group

CIBERSEGURIDAD 4.0

El Amanecer de la Humanidad Digital

Mario Velarde Bleichner,
Gurú en CiberSeguridad

Verdades y falacias del estado real de la digitalización empresarial y transformación digital en España

“La digitalización ha avanzado en los últimos meses 4, 6 o 10 años en España durante la pandemia”, afirmaba un ejecutivo de CEPYME, patronal de las pymes españolas, en la presentación de la cuarta edición del Observatorio de la Empresa de Vodafone, mediante encuesta personal a 3.500 personas en el último cuatrimestre de 2020. El universo de análisis (y sus muestras correspondientes) fue el de grandes empresas, pymes, autónomos y administraciones públicas.

Las conclusiones de la encuesta no podían ser más positivas... para quienes han hecho el estudio, aunque obviaran al resto del sector tecnológico o se refirieran a él en genérico arrogándose el mérito de lo que han hecho otros: “hemos hecho un gran esfuerzo en el despliegue de redes, de fibra”. Cierto, pero lo ha hecho Telefónica, Orange...

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.

400.000 asalariados trabajan en el sector tecnológico, y ellos sí viven en una burbuja digital, la suya, pero que no es la de todos los asalariados ni de los 3,4 millones de autónomos

En ninguna ocasión en la presentación del estudio se habló de la crisis económica, sanitaria y social que vive España, ni que tenemos una tasa de paro del 16,1% (versus el 6% de Estados Unidos) o que el PIB cayó en 2020 un 11% y la renta per cápita un 11,6%. Es como si alguien hubiera dicho que "ya está bien de penas, vamos a contar un mensaje optimista". El problema de un análisis hecho desde premisas que no son reales es que las conclusiones del estudio acaban siendo igualmente sesgadas. Es como aquello de "tienes muchas razones, pero no tienes razón". O cuando alguien escribe un libro de historia conocida por todos y orienta sus datos para obtener una conclusión premeditada: "todos los datos que cita son ciertos, pero la historia no es verdad".

Al decir de un directivo de Google y una directiva que representa en España al MIT Harvard Review, España es un paraíso de la digitalización. Desde su punto de vista esa utopía es cierta porque, para ellos, el teletrabajo es lo normal ("su normalidad", ignorando que "su" realidad no es la de todos los trabajadores de España. Un buen análisis sociodemográfico y socioeconómico empezaría por reconocer que España tiene 11 millones de personas mayores que, en su gran mayoría, están alejados de la transformación digital. O que en España hay cuatro millones de parados y más de medio millón en ERTE, cuya prioridad tampoco es la digitalización. Y que si los 19 millones de asalariados tuviesen todos un "smartphone", tampoco eso equivaldría a una mayor digitalización de la fuerza laboral. Pero algunos, torticeramente, lo equiparan.

Sí, en Google trabajan con ordenador y utilizan herramientas colaborativas como Zoom y Teams, pero ellos son una minoría comparada con toda la fuerza laboral del país. Supongo que es lógico que quieran vender las bondades del producto que ofrecen, como el vendedor de manzanas dice que sus manzanas son las mejores del mundo, aunque no tenga por qué ser necesariamente cierto.

Según el estudio, la crisis económica no ha afectado a los proyectos de digitalización en marcha en ninguno de los segmentos de mercado empresarial analizados. Es más, según dicen, en administraciones públicas y en microempresas han aumentado. Las pymes afir-

man disponer de un presupuesto "del 60% para digitalización", como si les sobrara el dinero.

Los datos del Instituto Nacional de Estadística que hace públicos ONTSI-Red.es sobre la penetración de las TIC y la digitalización en las empresas son de todo el ejercicio 2019, por tanto, antes de la pandemia. Luego no admiten comparación con el cuarto trimestre de 2020, cuando se hizo esta encuesta y, desgraciadamente, se produjo la mayor caída del PIB español y el menor gasto en tecnología por parte de las empresas, excepto en la compra de ordenadores, como anticipamos en IT User, con datos reales, en noviembre pasado.

Pero, ni siquiera el INE, cuyo rigor estadístico está fuera de toda duda, se atreve a afirmar que las pymes españolas (que en 2020 hay tenido una única misión: la supervivencia) destinen 60% de presupuesto a proyectos digitales. Simplemente, no es creíble.

Como tampoco lo es la vieja táctica de proponer un ejemplo concreto como exponente de un fenómeno generalizado: una anciana que pide a su nieta le ayude a bajarse la app de la Seguridad Social (¿los once millones de ancianos españoles han hecho eso mismo?); los hijos de una directiva de redes de la operadora "que han tenido formación online durante la pandemia, como antes, pero frente al ordenador" (¿es el caso de todos los niños de España? No. La escuela pública, 14 meses después, aún está en mantilla, según datos del ministerio que dirige la ministra Celaá y la educación privada y la concertada tardaron una media de seis meses en "ponerse las pilas" y 12 en completar el proceso de digitalización: when on earth are you coming from, you people?); "una escuela de negocios que pasa al online a la mitad de los chavales que no lo estaban" (la mayor parte de las escuelas de negocios del mundo tardaron mucho tiempo en acomodarse porque, precisamente, "la gracia" de Harvard, Stanford o Yale es el prestigio del profesorado y no la conexión a Internet y, por eso y no por otro motivo, se resistieron al cambio, pero no porque no tuviesen medios económicos o tecnológicos).

Y poner un ejemplo del campo y otro de la industria para ilustrar, con condescendencia, que también esos sectores se digitalizan...; por Dios, el INE y Eurostat niegan la mayor.

Pintar un escenario en que, en España, reina 5G, el teletrabajo, la inteligencia artificial, big data, Internet de las Cosas, Cloud Computing, centralita virtual y 24 horas como herramientas de digitalización que ya están ampliamente extendidas es una falacia, o no, y todos vivimos en 1) Matrix, 2) Charlie y la fábrica de chocolate con Johnny Depp.

Lo que sí es verdad es que de 19 millones de cotizantes a la Seguridad Social, 400.000 trabajan en el sector tecnológico (TIC, Telecomunicaciones, Contenidos, Digital) y, esos sí, viven en una burbuja digital: la suya, pero que no es la

de todos los asalariados ni de los 3,4 millones de autónomos (54% de los cuales son autónomos sin asalariados, según datos de la Seguridad Social de marzo de 2021).

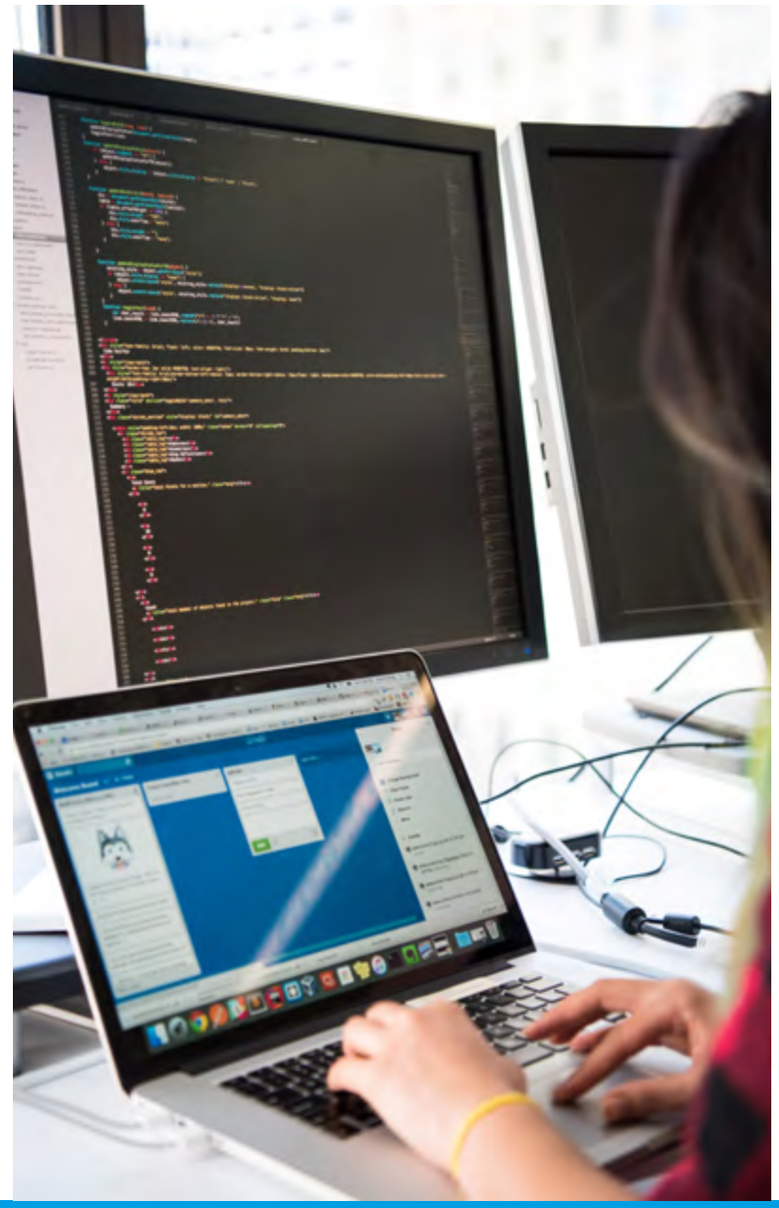
¿Hay que recordar a los autores del estudio que la economía más digitalizada del mundo, la norteamericana, lo está en un 30% de su PIB, ergo le falta el restante 70%? Si eso es así en la única economía que mide el impacto de la digitalización en su PIB desde 2013 a día de hoy y con carácter retroactivo desde 1939 hasta hoy… ¿qué porcentaje del PIB español es digital? Los autores del estudio no lo dijeron (no lo saben). Y, si ellos no lo dijeron, yo tampoco se lo diré, aunque sí lo sé, que no en vano he publicado cinco libros sobre digitalización, realizado 600 informes y estudios y más de 730 proyectos de consultoría en digitalización.

Hay extensa literatura reciente de 2016 al primer trimestre de 2021 que explica pormenorizadamente el estado real de la transformación digital en los países más ricos del mundo, que pertenecen a la OCDE. Y hay cientos de estudios bien hechos, como los realizados por los premios nobeles de economía Robert Solow, Michael Spence y Paul Romer, que se reirían si leyeran este estudio. O Klaus Schwab, fundador del World Economic Forum, orientado a la transformación digital en los últimos cinco años, autor de dos libros sobre la Cuarta Revolución Industrial y de cientos de estudios sobre digitalización. ¿Qué le cuesta a la gente formarse un poquito, estudiar? Si algo (entre otras muchas cosas) logró Juan Soto Serrano (primer presidente de Hewlett-Packard) en España es que "los trabajadores de HP no fueran vendedores de coches de segunda mano". Y la misma política de elevación han seguido Helena Herrero en HP y José María de la Torres en HPE.

Decir que estamos digitalizados, al mismo tiempo que nuestro Producto Interior Bruto cae un 11% y la tasa de paro real es del 20% (Datos EPA, 16,1% + empleados en ERTE, 4% de la fuerza laboral) es como decir que tenemos autopistas maravillosas, las mejores del mundo…, pero ignoramos que están todas en quiebra, porque nadie las utiliza. Esto último tampoco es una opinión, sino un dato.

¿Saben cuál es la realidad? Que España ha avanzado en digitalización, sí, especialmente entre las grandes empresas y el sector público, aunque ambos sectores luchan por sobrevivir, las primeras por su elevada deuda corporativa (que no tienen Big Tech en EEUU: Google, Amazon, Apple, Microsoft, Facebook) y por la falta de demanda; el Estado se nutre de impuestos y, un concepto que ignoran los autores del estudio, "la presión fiscal en España es del 43%". Y nuestra deuda pública supera el 122% sobre el PIB. Cruzando ambos datos, la resultante es que muy difícilmente es sostenible el sistema actual de AAPP en España, porque no genera, sino que recibe. Y recibe del sector privado, del cual sabemos que el Turismo ha perdido 81.000 millones de euros; el Retail y

La realidad de la digitalización en España es un "work in progress", con datos objetivos y reales



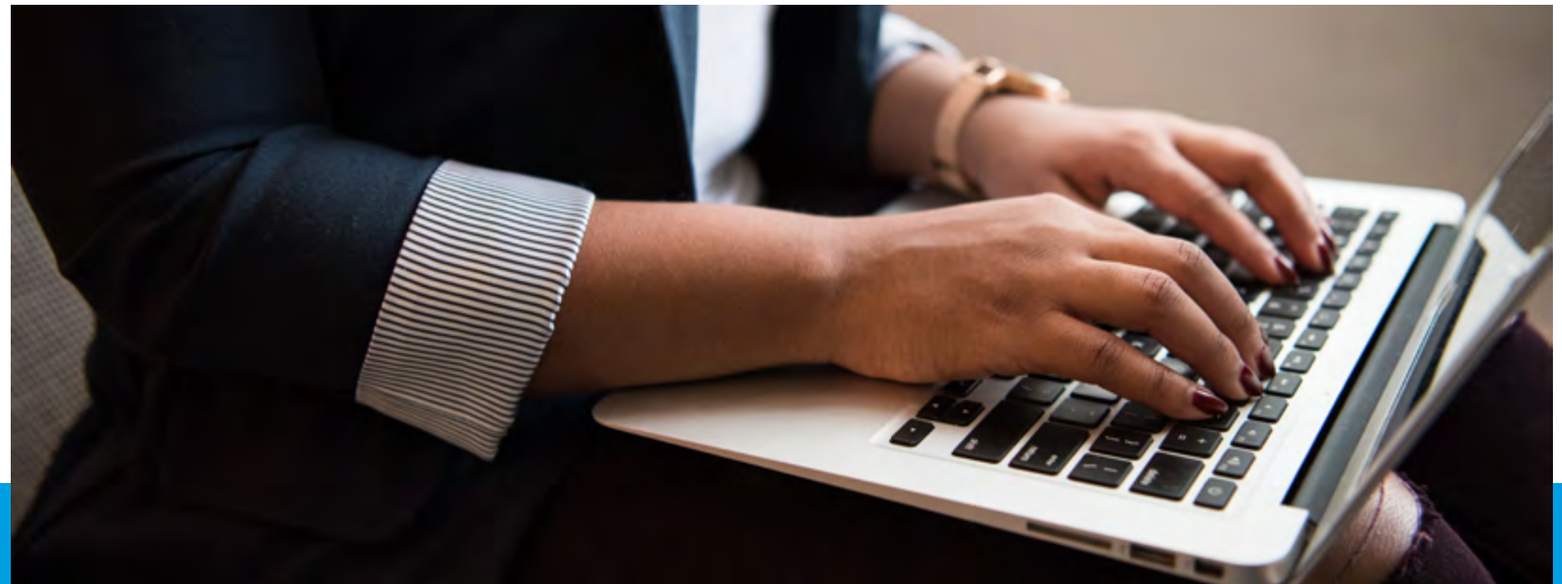
la Distribución no alimentaria está en crisis, junto a HORECA, que tiene medio millón de pymes al borde de la quiebra y 1 millón de trabajadores en ERTE. Para las cadenas hoteleras es aún peor, pues no dejan de cerrar hoteles y despedir empleados, con 800.000 trabajadores en ERTE. La industria... ¿qué industria? Cuando no cierra Abengoa lo hace Alcoa y ojo a Duro Felguera... ¿ilustran estos ejemplos la situación de la industria? Sí, cito a FUNCAS (20 servicios de estudios económicos):

"La caída más intensa del PIB se observó, como cabía esperar, en los sectores más afectados por las restricciones impuestas para controlar la extensión de la pandemia, es decir, en las ramas de comercio, transporte y hostelería, cuyo VAB descendió un 40,4%, y en actividades artísticas, recreativas y culturales, con una caída del 33,9%.

La contracción de la actividad ha sido una de las más acusadas de Europa. El resultado se debe, en parte, al peso del turismo y de otros servicios especialmente afectados por la pandemia. Estos sectores representan el 28% del PIB, más que el total de la industria, la construcción y el sector primario".

Nuestro objetivo no es sacar los colores a nadie, sino decir la realidad de la digitalización en España, que es un "work in progress", con datos objetivos y reales. La pandemia ha cambiado las prioridades de las empresas, especialmente de la mayoría: el 99,88% de pymes españolas, cuya prioridad no es digitalizarse, sino sobrevivir, debido a los cierres, confinamientos y falta de demanda. ¿Tan difícil es de entender? Los fondos de reconstrucción europeos, cuando lleguen, podrán ayudar a levantar la economía española y, cuando esto suceda, podremos hablar del cambio de nuestro modelo productivo hacia la economía del conocimiento.

Y, entonces, como Estados Unidos ahora, podremos hablar de que la digitalización es la fuerza motriz del crecimiento económico, el empleo y la digitalización.



Hasta que llegue ese momento, por favor, seriedad intelectual, trabajo esforzado, rigor en las fuentes y trabajar para mejorar España y el nivel de vida de los españoles, también con la digitalización, pero no como un valor absoluto, sino como un componente motriz más de la generación de riqueza en España. ■

MÁS INFORMACIÓN

- España en la era post-COVID: TI para transformar el negocio
- Producto Interior Bruto español en el primer trimestre de 2021
- Previsiones sobre la economía española y mundial
- IT Trends 2021. Asimilando la aceleración digital
- Previsión del PIB en España para 2021 y 2022
- Funcas: previsiones para la economía española para 2021 y 2022

HACIA LA EMPRESA HIPERINTELIGENTE

PATROCINADO POR

MicroStrategy®

Descarga este documento ejecutivo de

itResearch

Se intuye el final del túnel de la pandemia, ¿y ahora qué?

Los seis sombreros en la comunicación

Parece que por fin estamos viendo un poco de luz al final del túnel o al menos vemos unas pequeñas luces que nos indican el camino de salida. Incluso podemos distinguir a lo lejos gente que está ya cerca de la luz.

Después de mucho tiempo en las tinieblas y con pocas ganas de mirar atrás (está muy oscuro), llega el momento de pensar en que pronto podremos estar en una situación similar a la de la prepandemia, en la que debemos olvidarnos de los malos tiempos y mirar al futuro con ilusión y con la convicción de que la situación económica repuntará.

Manuel López

Asesor de comunicación

Madrileño 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 starups en temas relativos a la comunicación, desde su posición de partner en la plataforma de profesionales goXnext.

NO SOLO it

Encuentros y desencuentros con la Comunicación

Pensando en cómo deberíamos afrontar esta situación desde el punto de vista de la comunicación, me vino a la cabeza una teoría de hace muchos años (queda un poco extraño decir que es del "siglo pasado") que yo descubrí en el libro del gran escritor y psicólogo Edward de Bono, "El pensamiento creativo". La teoría se llama "Los seis sombreros para pensar".

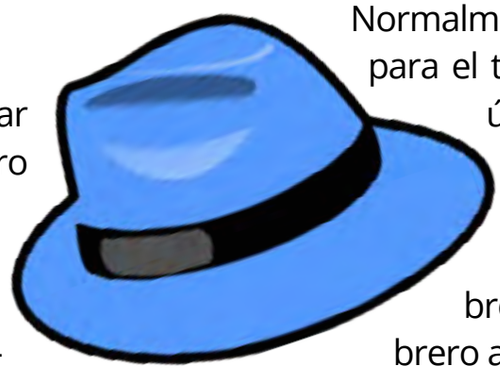
Yo la he utilizado en múltiples ocasiones en mi vida profesional y aunque está orientada para desarrollar un pensamiento creativo, creo que es muy adecuada para reflexionar sobre lo que se nos viene encima desde el punto de vista de la comunicación en el mundo post-COVID.

Dice Edward en su libro que "el método de los seis sombreros es extremadamente simple, pero esa simplicidad resulta poderosa". Yo creo que la simplicidad y la comunicación forman la mejor pareja para afrontar la crisis que nos amenaza en el mundo post-COVID.

Voy a describir brevemente el método y después lo utilizaremos como ayuda para la situación actual. Obviamente, buscamos como usar este método para tener un "Encuentro con la Comunicación", siguiendo con el leitmotiv de esta serie de artículos que bajo el paraguas de "Encuentros y Desencuentros con la Comunicación" llevo ya tiempo publicando en este medio.

El método básicamente describe como afrontar problemas e indica la función a ejecutar en función del color del sombrero que nos pongamos.

La simplicidad y la comunicación forman la mejor pareja para afrontar la crisis que nos amenaza en el mundo post-COVID



❖ **Sombrero blanco:** Datos e información. Objetividad. Analizar hechos, cifras e información de forma lo más neutral posible.

❖ **Sombrero rojo:** Emoción sentimiento y pasión. Analizar la situación desde la intuición, buscar el aspecto emocional sin necesidad de justificarlo.

❖ **Sombrero negro:** Miedo, pesimismo y negatividad. Actuar como "abogado del diablo", juzgar con opinión crítica, explicar por qué no va a funcionar algo.

❖ **Sombrero amarillo:** Sueños, optimismo e ilusión. Enfocarse en el optimismo, en por qué va a salir bien, enfoque constructivo, buscando la oportunidad.

❖ **Sombrero verde:** Ideas, imaginación y creatividad.

Buscar el punto de vista original, diferencial, provocativo incluso.

❖ **Sombrero azul:** Gestión, control y visión panorámica. Organizar, sacar conclusiones y planes de acción.

Normalmente es una metodología pensada para el trabajo en equipo, pero también es útil para el trabajo individual de creación de soluciones. Cuando afrontamos un problema es importante que nos pongamos todos los sombreros y que nos cambiemos de sombrero a lo largo del proceso.

Bien, pues pongámonos los distintos sombreros para describir un punto de vista singular acerca de lo que se supone que nos vamos a encontrar al final del túnel. Salgamos del túnel con cada uno de los sombreros puestos y describamos la visión.

Si nos ponemos el sombrero blanco, tenemos una situación difícil. Los datos económicos no son nada positivos y parece que encontraremos dificultades para recuperar la economía. Da la impresión de que fuera del túnel hay tormenta y nos vamos a mojar. También es cierto que la llegada de fondos europeos de recuperación, abren la puerta al

NO SOLO it

Encuentros y desencuentros con la Comunicación

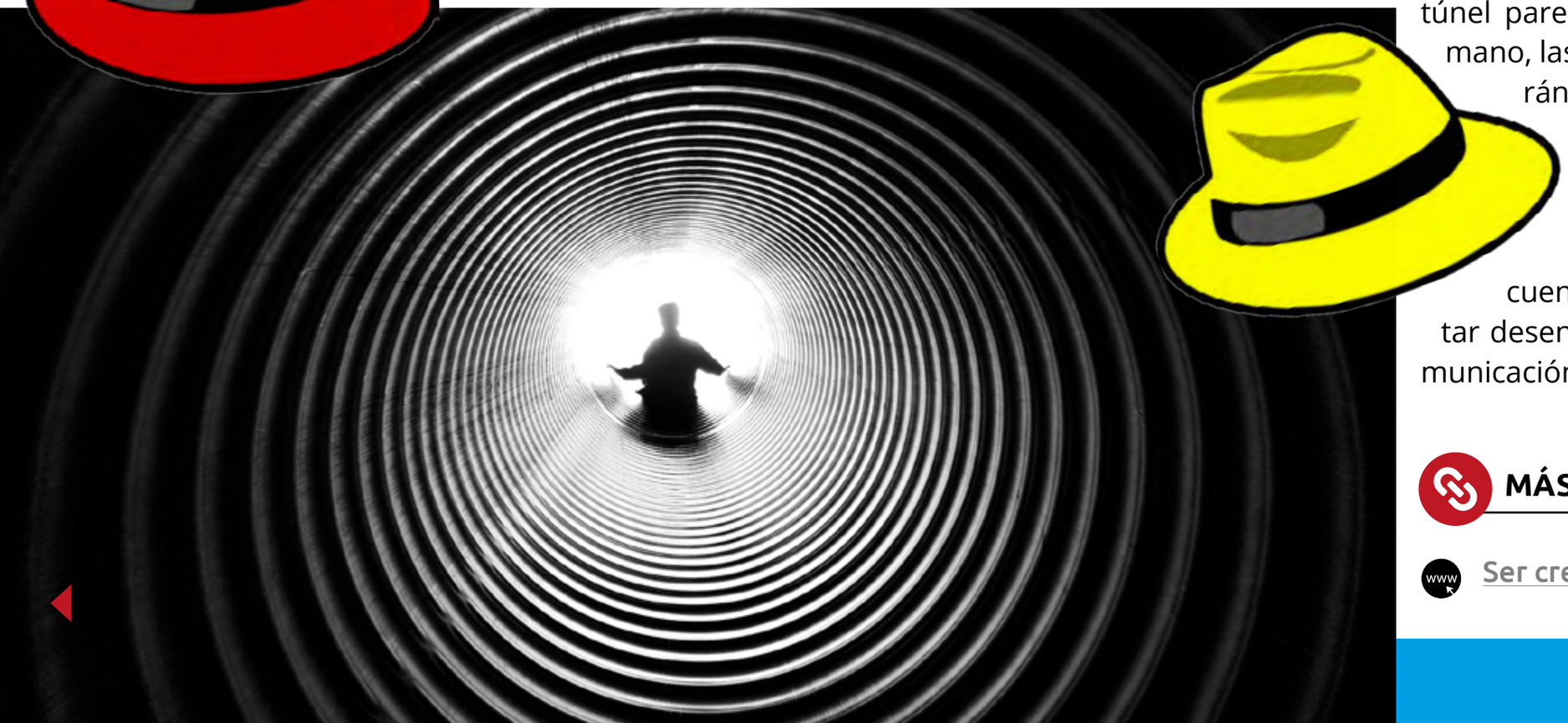
desarrollo de la economía en un horizonte próximo.

Si nos ponemos el sombrero rojo, llevamos más de un año de contención, de desesperación, incluso, y tenemos unas ganas tremendas de trabajar, de aportar y de desarrollar nuestro negocio. Con el sombrero rojo no nos importa la lluvia, ni mojarnos al salir, queremos salir y comernos el mundo.

Con el sombreo negro puesto, parece que no es buena idea salir del túnel, donde bajo un ERTE o similar se está más o menos calentito y no parece lo mejor salir, mojarse y quizá hasta pillar un catarro.

Si nos ponemos el sombrero amarillo, solo nos concentraremos en la luz, en las tremendas oportunidades que nos esperan ahí fuera, con un mercado ansioso por consumir nuestros productos y servicios y con cierta capacidad adquisitiva que no ha sido posible emplear durante la pandemia.

Siguiendo con la luz, nos ponemos el sombrero verde y lo que empieza a bullir en nuestra cabeza son nuevas formas de comunicar, nuevos clientes objetivo, ideas para conseguir un rápido crecimiento y ganar cuota de mercado. Y por qué no, ¿qué tal si vendemos paraguas para la lluvia?



Por último, nos ponemos el sombrero azul y evaluamos las posibilidades que tenemos de ejecutar las ideas, de soportar el crecimiento, de gestionar los recursos necesarios para conseguir el éxito.

Así pues, y volviendo al principio, el final del túnel parece que está al alcance de nuestra mano, las oportunidades están afuera, esperándonos, pero antes de salir y exponernos a la tormenta, pongámonos los sombreros y salgamos lo más protegidos posible.

Y en esto es en lo que estamos: Encuentros con la comunicación, para evitar desencuentros y frustraciones con la comunicación. ■

MÁS INFORMACIÓN

Ser creativo: Seis sombreros para pensar

DESCUBRE LAS **TENDENCIAS** QUE DEFINEN EL **FUTURO DIGITAL**

it TRENDS

Un café con el Homo Virtualis

Reflexionaba recientemente de la mano de L. Floridi, en cuanto a la evolución social y humana respecto las TIC, con un planteamiento que establece tres grandes fases: la prehistoria, la historia y la hiperhistoria. En la prehistoria no hay TIC. En la historia hay TIC, simplificadamente caracterizada por sistemas de información que gestionan y procesan datos. En la hiperhistoria hay TIC que gestiona y procesa datos de forma cada vez más ubicua, automatizada, autónoma e inteligente, estableciendo en el día a día de las personas, una dependencia inherentemente tecnológica en su relación social y laboral. Y es que realmente parece que vamos progresivamente a una realidad que cada día más se conforma como

Màrius Albert Gómez

Marius Gómez en su columna éTICa, sintetiza la voluntad de compartir unas reflexiones que nos ayuden a entender un mundo digital caracterizado con esos grandes "trending topics" actuales como son el Big Data, la Inteligencia Artificial, la IOT o la computación en general, y que son vistos desde un marco de consideraciones éticas, humanistas y sociales. Dichas reflexiones se realizan desde la actitud y el desempeño multidisciplinar, tanto individual como empresarial, y tienen el objeto de contribuir a "aportar un pequeño granito de arena en el proceso de repensar el papel que las TIC deben jugar en la vida de nuestros hijos, en su formación, en su trabajo, en su día a día... con un punto de vista que supere el meramente tecnológico".

una suma combinada e indistinguible de realidad física y virtual. Es más, seguramente la componente virtual ya podría ser dominante en muchos casos por su facilidad y rapidez de "consumo", aventajando un proceso reflexivo mucho más "lento", de mayor transcendencia y producción intelectual.

Y es que, dentro de la red, en la infoesfera virtual, la tecnología no contiene ética ni inteligencia en sí misma, la adopta de nosotros. Construimos sistemas automatizados de decisión, redes sociales, apps móviles, bots, sistemas biométricos, integramos en IOT nuestro día a día, híper conectamos sistemas... y en ellos volcamos cada día más una parte que nos define, de nuestro conocimiento, de nuestras relaciones, de nuestro aprendizaje. Fácilmente, espontáneamente, sin cuestionarnos nada. Pero ¿ocurre lo mismo con nuestros valores éticos? Nadie se debería extrañar si en unos años un artículo rompedor nos estremece con el titular "¿dónde o cuándo perdimos parte de nuestra humanidad en la red?". Está claro que la digitalización nos ofrece muchas oportunidades como sociedad: eficiencia, sostenibilidad, resiliencia, equidad, nuevos modelos productivos... pero siempre y cuando el talento que "consume" las TIC y que "produce" con las TIC, lo haga desde una vertiente mucho más humana, ética e intelectualmente comprometida para que forme parte del proceso de transformación digital.

Necesitamos en estos momentos y para los nuevos retos de digitalización mucho talento, sí, y más aún si cabe en el contexto de los nuevos fondos de recuperación, transformación y resiliencia. Sí, necesitamos talento STEM, ingenieros, científicos y matemáticos y nuevas fórmulas de colaboración conjunta entre todos los actores (sector público, privado, universidades...). Pero necesitamos también invertir en capacitación ética y humanidades, filosofía y cultura. Necesitamos más capacidades Homo en la constitución del Homo Virtualis. Si cogemos perspectiva y pensamos en la transformación del sector productivo que pretendemos, ¡reflexionemos un instante sobre el modelo social y económico que queremos! Reflexionemos por un modelo inherentemente definido por talento digital sí, en un mundo virtual y físico muy imbricados sí, pero también diseñado por talento ético organizativo y social.

Daniel Kahneman, autor americano-israelí y premio Nobel, analizando los procesos de toma de decisiones en situaciones de alta incertidumbre, donde tanto los beneficios como las pérdidas son inciertas, nos aporta un nuevo punto de vista basado en lo que se denomina ya la teoría de las perspectivas.

NO SOLO it Reflexiones éTICas

Reflexionemos por un modelo inherentemente definido por talento digital sí, en un mundo virtual y físico muy imbricados sí, pero también diseñado por talento ético organizativo y social

Según esta teoría, en dichos momentos de alta incertidumbre nos alejamos de la racionalidad a la hora de tomar decisiones y tomamos lo que se denomina atajos heurísticos. Uno de los criterios de los atajos heurísticos, por ejemplo, es la aversión a la pérdida, aunque, en el fondo, todos estos atajos podríamos entenderlos bajo una perspectiva de que al final nos domina la parte intuitiva, lo simplificamos a lo binario, sin considerar alternativas. En este sentido, por tanto, resulta fundamental afrontar una reingeniería de nuestras propias ideas reconociendo tal carencia, rechazando la facilidad de adoptar en muchos casos los atajos heurísticos, y promoviendo nuevas decisiones y soluciones que nos ayuden con el reto digital. Debemos dotarnos de unas herramientas y un talento holístico que nos permita visualizar y definir una transformación digital, con optimismo ético y digital.

El café siempre ha sido una piedra angular de la cultura social y empresarial, de su bienestar, de la reflexión, de la relación con nuestros colaboradores, de establecer nuevas relaciones, de la escucha activa de nuevos puntos de vista... Quizá necesitemos unas buenas dosis de café con el Homo Virtualis en los nuevos puestos de trabajo híbridos del futuro para poder crear una hiperhistoria digital y virtual, ética, e intrínsicamente humana por definición en sus valores. ■

MÁS INFORMACIÓN

The Onlife Manifesto - Being Human in a Hyperconnected Era, L. Floridi

¿Por qué decides lo que decides? Así afectan los sesgos cognitivos a nuestro pensamiento racional

it 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!!!

Neurociencia y medios de pago

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).

2020 ha sido el año en el que los medios de pago electrónicos han tenido la oportunidad de consolidar su posicionamiento y asentar las bases para un futuro cercano sin dinero físico o, al menos, con un volumen de transacciones reducido a la mínima expresión. El miedo al contagio y el cierre temporal de establecimientos calificados como "no esenciales" ha determinado, por un lado, un menor uso de dinero en metálico y de lectores de banda o chip de tarjetas para TPV y ATM y, por otra parte, ha impulsado la utilización de EMV/NFC tanto de tarjetas como de billeteras móviles, a pesar del crecimiento que han tenido sistemas emergentes como los pagos P2P (en el que ha tomado especial relevancia el modelo Bizum) y con código QR.

Las predicciones que hicieron el año pasado Research and Markets y el gabinete de estudios de Deutsche Bank situaban a las billeteras móviles y al efectivo como los principales medios de pago a final de la actual década, pero recientes informes de Payments, Cards & Mobile vaticinan otro escenario en el que las tarjetas de crédito y de débito mantendrán su liderazgo a nivel global avaladas por la costumbre y la confianza del usuario que,

Estudios de neuropsicología han analizado las reacciones que, a nivel fisiológico, se producen en nuestro cerebro cuando realizamos un pago con efectivo o con tarjeta

en tiempos de pandemia, ha preferido su uso (en su versión contactless) como recurso seguro ante el contagio y ante el incremento del fraude en canales digitales.

A esta situación también está ayudando la contracción de las redes de sucursales y de cajeros automáticos (y de casi un 30% de entidades financieras en el período 2008-2019), ya que cada día se reducen los puntos para obtener efectivo y, por otro lado, desde estas instituciones se recomienda insistentemente a los clientes el uso de los canales de banca digital, las tarjetas de débito para compras y las tarjetas de crédito como alternativa a la financiación del consumo (aunque éstas están mostrando una clara desventaja respecto a las múltiples alternativas de aplazamiento del pago ofrecidas por muchos proveedores de bienes y servicios y empresas de crédito rápido para bajo importe y elevados tipos de interés). De hecho, Anne Boden, directora de Starling Bank, predice la desaparición del efectivo en 2030 ya que este hecho podría acarrear más beneficios que perjuicios si se proporciona a toda la población las herramientas y la formación digital necesarias para que se produzca una adopción completa de los sistemas financieros electrónicos.

No obstante, esta visión, para hacerla más consistente, habría que completarla con lo que diversos estudios de psicología aplicada al consumo nos desvelan acerca del comportamiento de los usuarios cuando se enfrentan a la decisión de compra utilizando uno u otro medio de pago. Son conocidos los que apuntan que con el efectivo se controla más el gasto que con las tarjetas y, dentro de éstas, más con las de débito que con las de crédito. Ello es debido a que con el efectivo vemos disminuir directamente nuestro dinero y con las tarjetas de débito nuestro saldo en cuenta en el momento del pago. En cambio, con las de crédito, aplazamos la disminución de nuestra tesorería, descontando el tiempo de "dolor" hasta el momento del cargo en cuenta.

Estudios de neuropsicología han analizado las reacciones que, a nivel fisiológico, se producen en nuestro cerebro cuando realizamos un pago con efectivo o con tarjeta. Las áreas que intervienen son diferentes y ello implica que las decisiones de gasto también sean distintas; mientras que cuando pagamos en efectivo se activan los núcleos relacionados con la aversión a la pérdida (amígdala, ínsula, hipotálamo y locus coruleus), cuando lo hacemos con tarjeta se implican los relacionados con el sistema de recompensa (córtex prefrontal y núcleo accumbens). Por ello, es más fácil caer en la tentación de comprar más y gastar más dinero con tarjeta

que con dinero efectivo. Esto ya lo saben muchas empresas, por lo que estimulan el uso de tarjeta, sobre todo para artículos de importe bajo, ya que no ponen en marcha los circuitos de anticipación a la pérdida futura.

Este hecho lo corroboran varios autores en el artículo "Mecanismos neuronales del gasto con tarjeta de crédito", en el que exponen las evidencias de que este medio de pago aprovecha los sesgos cognitivos y otros mecanismos psicológicos por los que los consumidores sobreestiman su capacidad futura de reembolso, aunque luego se sorprenden por el cargo con elevados intereses en el momento del vencimiento. Añaden que los estudios empíricos muestran que los compradores con tarjetas de crédito están dispuestos a comprar más y más caro, al tiempo que se centran más en los beneficios que obtienen del producto que en su coste. Por ello, toman decisiones de compra más indulgentes e impulsivas.

Otro estudio realizado por varios autores, "Efectivo, tarjeta o teléfono inteligente: los correlatos neuronales de los métodos de pago", confirma lo expuesto en la investigación anterior, pero además tiene en cuenta el mecanismo de autorregulación que dispara el pago en efectivo, por lo que para la administración pública puede ser una herramienta para ayudar a los ciudadanos a controlar las compras compulsivas y la ludopatía.

¿Y qué sucede en el entorno digital? A.K. Kar ha identificado que los determinantes de la satisfacción en el uso de los sistemas de pago móviles eran el costo, la utilidad, la confianza, la influencia social, la credibilidad, la privacidad de la información y la capacidad de respuesta ante incidencias. Estos atributos, alejados de los instrumentales dominados por justificaciones racionales, son los que las empresas proveedoras de servicios de pago móviles deberían tener en cuenta para incentivar e incrementar la adopción de sus sistemas, valorando también cómo manejar la ventaja que les puede aportar el estímulo de los mecanismos de recompensa que se activan en el caso de uso de las tarjetas para crear acciones promocionales y de fidelización orientadas a potenciar este efecto.

Aunque la tecnología ayuda a mejorar la experiencia de usuario, es necesario tener en cuenta otras consideraciones que pueden parecernos banales o que la intuición nos indica que pueden facilitar el proceso de pago móvil y que, en realidad, lo que pueden hacer es activar la aversión a la pérdida como en el pago en efectivo. Es el caso de la vibración háptica en el proceso de compra con el móvil, la cual reduce la disposición a gastar de los participantes en el estudio llevado a cabo varios autores, en comparación con un grupo de control que no recibía ninguna retroalimentación mediante la vibración del móvil.

NO SOLO it Marketing y consumo

Aunque la tecnología ayuda a mejorar la experiencia de usuario, es necesario tener en cuenta otras consideraciones que pueden parecernos banales o que la intuición nos indica que pueden facilitar el proceso de pago móvil

Estos detalles de diseño que, aparentemente, mejoran la experiencia de usuario pueden volverse en contra si no se tiene en cuenta la reacción inconsciente que provoca. Algo parecido sucede en el comercio electrónico y la percepción de seguridad durante el proceso de pago, como han analizado J. Sánchez Fernández y otros en un reciente estudio en el que han concluido que los pagos con tarjeta que se realizan en plataformas que se perciben como no seguras activan las áreas cerebrales relacionadas con el procesamiento emocional negativo (aversión a la pérdida). En cambio, en las que se perciben como seguras se involucran las áreas que procesan las emociones positivas (anticipación de recompensa). Y en el caso de PayPal, en el que el usuario no aporta los datos de su tarjeta, se produjo además una activación mucho mayor del cerebelo, lo que se puede traducir como una valoración más positiva y correlacionada con una mayor intención de uso.

Aunque las tendencias del mercado y las predicciones sobre la evolución de la tecnología a corto plazo apuntan hacia la "omnidigitalización", con especial intervención de los sistemas soportados por inteligencia artificial, realidad aumentada, virtual y mixta, internet de las cosas, bots de soporte... es necesario tener en cuenta, como señala KPMG en su reciente informe sobre la nueva realidad de las experiencia de cliente, que el consumidor en este último año se ha vuelto más reflexivo y selectivo en su toma de decisiones, valorando más la integridad y la confianza como atributos esenciales para elegir la empresa a la que adquirir sus productos. Factores como la marca, el propósito y la reputación se están incorporando en el proceso de toma de decisiones en igualdad de condiciones con la seguridad, la garantía, la conveniencia y la certidumbre.

Al conocimiento de estos factores, todos ellos en el marco de las emociones, nos podremos acercar con métodos de investigación convencionales vía test y focus group, pero será la neurociencia las que nos aporte la información más relevante sobre la respuesta neuronal que realmente condicionará la decisión de un individuo acerca de la compra de un producto o servicio a una empresa en concreto y del medio de pago con el que lo va a adquirir. ■

MÁS INFORMACIÓN

- Predicciones Research and Markets
- El futuro de los pagos, Deutsche Bank
- Payments, Cards & Mobile
- Desaparición efectivo en 2030
- Mecanismos neuronales del gasto con tarjeta de crédito
- Efectivo, tarjeta o teléfono inteligente: los correlatos neuronales de los métodos de pago
- A.K. Kar
- Vibración háptica en el proceso de compra con el móvil y su efecto en el gasto
- Comercio electrónico y la percepción de seguridad durante el proceso de pago
- Nueva realidad en la experiencia del cliente

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 Calculo 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.

El Amanecer de la Humanidad Digital

Estamos viviendo el amanecer de la Humanidad Digital, pero no quiere esto decir que los seres humanos estén sufriendo mutaciones que los estén convirtiendo en individuos diferentes a los que han vivido en previamente al advenimiento de la nueva Humanidad Digital.

Este amanecer es más bien fruto del trabajo y esfuerzo de todas las generaciones anteriores que han ido evolucionando desde sus primeros individuos, que, al adquirir conciencia de sí mismos, han iniciado un camino que nos ha traído hasta este maravilloso momento en el que vislumbramos los primeros rayos del nuevo sol de la Digitalización como catalizador de avances en la evolución humana que trascienden de los puros logros materiales que traen estas tecnologías.

Veremos, por ejemplo, como, por primera vez desde la aparición del lenguaje, toda la humanidad se podrá comunicar en un único lenguaje digital; esto no quiere decir que perdamos nuestros idiomas nativos, que ganaran todos en hacerse universales. Cada persona comunicará en su idioma y cada persona recibirá esa comunicación en su propio lenguaje nativo mediante dispositivos digitales que realizaran la traducción instantáneamente con el apoyo de la Inteligencia Artificial que realizará un trabajo impecable.

La nueva Humanidad Digital podrá por fin superar por fin el mito de la Torre de Babel y la confusión de los pueblos con idiomas distintos que tanto daño ha hecho hasta ahora dividiendo y enfrentando a la humanidad.

Podemos pensar, sin pecar de un optimismo exagerado, que el hecho de que toda la humanidad se pueda ya comunicar libremente sin la limitación idiomática mejore el entendimiento entre los pueblos y, siendo optimistas, nos permita dar los primeros pasos hacia una única Humanidad Digital Global nueva que evolucione a partir esa premisa.

Hay agoreros que dirán que esta tecnología digital eliminará miles o tal vez millones de puestos de trabajo de traductores, cuando en realidad lo que hará será dar a todos los seres humanos la libertad de comunicarse con cualquier otro ser humano, que ahora es un privilegio reservado a las elites que disfrutan de “esclavos” humanos que traducen sus muy importantes comunicaciones. En fin, cambiará el paradigma de la comunicación humana en un sentido que jamás habíamos imaginado.

Veremos, por ejemplo, un gran salto en la sanidad y, aun cuando los avances en la curación de enfermedades malditas como el cáncer irán mucho más rápido con la utilización de las tecnologías digitales, el gran avance de la Humanidad Digital estará en la Medicina Preventiva, que podrá ser realmente Universal con la llegada de dispositivos digitales de bajo coste que hagan un seguimiento continuo de parámetros médicos a todos los humanos digitales del futuro. Esta inmensa cantidad de datos, analizada por nuevos y mejores algoritmos de Inteligencia Artificial permitirán conocer y hacer previsiones del estado de salud de toda la población del planeta sin perder de vista la situación sanitaria de cada individuo de esta nueva Humanidad Digital.

¿Cómo podemos ser tan optimistas cuando en la actualidad tantos niños mueren todos los días de desnutrición o de enfermedades comunes? Porque en un futuro no muy lejano las Tecnologías Digitales de micro y nano sensores unidos a los avances de las comunicación digital inalámbrica llegarán, sin duda, a una plataforma capaz de cubrir todos los puntos del planeta con un ancho de banda inimaginable capaz de proveer a todos los habitantes de Medicina Preventiva apoyada por sistemas de Inteligencia Artificial que puedan atender a cada individuo y, al mismo

tiempo, evaluar continuamente el estado sanitario de todas las poblaciones del planeta e, incluso, tener una visión clara del estado sanitario de todo el planeta como una unidad.

Solo estos dos rayos de luz en el amanecer de la Humanidad Digital, lenguaje de comunicación universal y sanidad preventiva universal, son suficientes para tener la esperanza en una evolución exponencial de la especie humana. Imaginad cuando todo el potencial de la tecnología Digital esté a disposición de los futuros ciudadanos digitales hasta dónde puede llegar esta nueva fase evolutiva de la Especie Humana.

Pero este amanecer, como todos los amaneceres de cada día en nuestro bello planeta, viene con nubarrones que, sin duda, provocaran lluvias o tormentas que pueden entorpecer, retrasar o incluso terminar con este maravilloso viaje de la Especie Humana Digital.

No olvidemos esa terrorífica herencia que nos ha dejado la era industrial, que, en su faceta nuclear, habiéndonos traído avances como la medicina o la energía eléctrica de origen nuclear, nos deja un arsenal de bombas y misiles con capacidad de aniquilar todo tipo de vida en nuestro precioso planeta. Este horrible Armagedón debe ser eliminado por la Humanidad Digital si quiere tener un futuro.

Otro regalo de las revoluciones industriales son los desastres ecológicos, con el calentamiento global como el más peligroso de todos ellos. Estoy seguro de que, según avance la Humanidad Digital, estos problemas serán corregidos y volveremos a un equilibrio con nuestro entorno.

> El gran avance de la Humanidad Digital estará en la Medicina Preventiva, que podrá ser realmente Universal con la llegada de dispositivos digitales de bajo coste que hagan un seguimiento continuo de parámetros médicos a todos los humanos digitales del futuro

A pesar de ser estos dos nubarrones graves problemas en el amanecer de nuestra Humanidad Digital, podemos decir sin ánimo de culpar de todo al pasado que, a pesar de todo, ha sido necesarios para que Tecnologías Digitales nacieran y fueran madurando hasta llevarnos a este nuevo amanecer y es un peaje que sabremos llevar para eliminar estas amenazas tan graves a toda la humanidad.

Hay un nubarrón que no proviene de los avances tecnológicos necesarios en el pasado y es la mala utilización de la comunicación digital en las plataformas de redes sociales donde los Ciudadanos Digitales encontraron por fin un espacio donde comunicarse directamente, hacer visible su opinión y crear tendencias sin la tutela de los grandes medios de comunicación ni siquiera de los medios de comunicación públicos al servicio de los gobernantes de turno.

La mala utilización de la comunicación digital, en particular en las redes sociales, la protagonizan los ciberdelincuentes que, aprovechando la buena fe de los ciudadanos digitales les roban dinero, secuestran sus perfiles y les llegan a someter a chantajes para recuperar sus datos , en fin delitos típicos de delincuentes comunes.

Más grave es la mala utilización de la comunicación digital, en particular en las redes sociales, la que protagonizan los gobiernos de unos países en contra de otros intentando, y a veces consiguiendo, manipular procesos electorales usando noticias falsas, creando falsas historias que son compartidas masivamente por ejércitos de usuarios fantasmas manipulados desde organizaciones paragubernamentales para eludir su responsabilidad ante el mundo; vemos que son mucho peores que los ciberdelincuentes comunes.

Todavía más grave aún es la mala utilización de la comunicación digital, especialmente en redes sociales la que perpetran los partidos políticos ya no solo en dictaduras declaradas sino incluso en las democracias consolidadas incluso en aquellas con tradiciones democráticas de

Cada persona comunicará en su idioma y cada persona recibirá esa comunicación en su propio lenguaje nativo mediante dispositivos digitales que realizaran la traducción instantáneamente con el apoyo de la Inteligencia Artificial

varios siglos. Todos los partidos políticos sin excepción hacen sin ninguna vergüenza lo que los gobiernos tratan de ocultar, crean falsas historias, insultos de grueso calibre e incluso amenazas de todo tipo, todo lo que sea necesario para desacreditar a sus adversarios democráticos, que han pasado a ser enemigos en un ejercicio indigno que ensucia y pervierte la política y deshumaniza esta actividad humana.

Menos mal que con el paso de cada día los Ciudadanos Digitales vamos aprendiendo y reconociendo el peligro de los ciberdelincuentes, gobiernos delincuentes digitales y políticos delincuentes digitales y nos vamos inmunizando de tanta delincuencia como si nos vacunaran del peor virus pandémico.

La Humanidad Digital solo evolucionará por nuevos y más potentes avances de las tecnologías, que de manera aún más acelerada que lo que hemos visto hasta ahora irán afectando, cambiando y estableciendo nuevos paradigmas en todas y cada una de las actividades de la especie.

Estos cambios de paradigmas, provocarán indudablemente un gran cambio en los nuevos ciudadanos digitales, en su forma de relacionarse, en los valores individuales y colectivos, avanzando, como ha pasado con todos los cambios tecnológicos del pasado desde la invención de la rueda o el descubrimiento del fuego, hacia sociedades más complejas pero también más respetuosas con la propia especie humana.

Hay que tener confianza en que los nubarrones que estamos viendo en este amanecer sean superados por la nueva Humanidad Digital y de la misma manera tener confianza en que dificultades mayores y aún desconocidas que seguramente aparecerán en un futuro serán superadas hasta llegar a un brillante futuro de la especie humana en su fase digital. ■

MÁS INFORMACIÓN

- Traducciones en tiempo real con Android
- Una salud orientada a la prevención

it Reseller
TECH&CONSULTING

Cada mes en la revista, cada día en la web.