it User
TECH & BUSINESS

nº 73
DICIEMBRE 2021

CONTENIDOS

La Inteligencia Artificial fluye entre las organizaciones

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

10 claves para los CIOs en los próximos 5 años

Seguirá creciendo el gasto en transformación digital

EDITORIAL

it User TECH & BUSINESS

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

Las prioridades del CIO para los próximos años

De todos es sabido que el peso específico del CIO está creciendo notablemente en el seno de las empresas. De hecho, en una encuesta reciente, cuando a diversos CEOs españoles se les preguntaba sobre quiénes serán sus directivos más relevantes en los próximos años, nombraban a sus jefes de tecnología (CIOs y CTOs) más del doble de veces que a los CMOs, CHROs o CXOS de cualquier otra posición, excluyendo a CFOs y COOs. En este nuevo rol juega un papel fundamental las prioridades para los próximos años del CIO, que considera que el área de experiencia del empleado será en la que tendrá mayor impacto la tecnología, seguido de los nuevos modelos de trabajo y de las habilidades profesionales. Además, uno de cada siete CIOs reconoce que la mayor inversión tecnológica que se realizará en sus empresas en los próximos 3 años se concentrará en el IoT, seguido del 5G y de la automatización.

Aunque los CIOs siguen prestando desde sus departamentos servicios de TI que necesitan las operaciones empresariales, también se espera que ayuden a impulsar la innovación y el crecimiento corporativos. Y muchos de ellos han destacado la importancia de los datos y de la automatización para acabar con los silos y crear nuevos flujos de valor, apoyándose de manera creciente en la inteligencia artificial y en el modelo de nube híbrida.

Otro de los objetivos corporativos que el CIO pretende ayudar a cumplir a través de la tecnología es el de la sostenibilidad. Y aquí hay mucho camino por recorrer. Pero, sin duda, será uno de sus propósitos más ambiciosos pero también moralmente más satisfactorios. ■

Pablo García Reales

CONTENIDOS↓

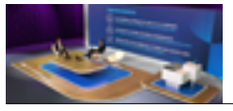
SUMARIO

Diciembre 2021

EN PORTADA

La Inteligencia Artificial fluye entre las organizaciones

ACTUALIDAD



"Muchas empresas creen que se basan en datos, pero no lo hacen", R. Labarga (Dell Tech.)

AWS acelerará la transición de los clientes del mainframe a la nube

La UE sigue muy lejos de los objetivos marcados en digitalización para 2030

1 de cada 4 empresas tuvieron dificultades para contratar a perfiles TIC

La nube pública y el segmento IaaS impulsan el mercado de servicios cloud

El 70% de las compañías españolas aumentará su gasto en ciberseguridad

REVISTAS DIGITALES

ANUNCIANTES

INFORME CLOUD

IT WHITEPAPERS

IT DIGITAL SECURITY

TECNOLOGÍA Y EMPRESA

IT TRENDS

TECNOLOGÍA Y EMPRESA

IT RESELLER

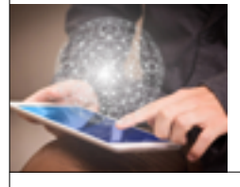
NO SOLO it

TENDENCIAS

10 claves para los CIOs en los próximos 5 años

Seguirá creciendo el gasto en transformación digital

3 claves para competir en la economía de los datos



Cómo construir una organización más orientada a los datos

Ventajas que las empresas perciben cuando utilizan IA

Claves de usabilidad web para no dañar la experiencia del cliente

“Muchas empresas creen que se basan en datos, pero no lo hacen”

RICARDO LABARGA, DELL TECHNOLOGIES

La sobrecarga de datos que están experimentando las empresas supone para las organizaciones un gran desafío que no siempre saben cómo gestionar. Aprovechando la celebración de Dell Technologies Forum, la compañía presentó las conclusiones del informe “The Data Paradox”, que pone de relieve la diferencia entre la percepción y la realidad que viven las empresas en cuanto a sus estrategias de datos.

“Puesto de trabajo moderno, entornos multicloud, ciberseguridad y ciber-recovery e hiperconvergencia” son los principales temas de conversación con los CIO, afirmó Ricardo Labarga en su intervención durante la apertura de Dell Technologies Forum 2021, que un año más se celebró de forma online. “También los datos: Muchas organizaciones españolas están mostrando avances claros en sus procesos de transformación digital trabajando, fundamentalmente, en tres frentes: la modernización de sus infraestructuras IT, de sus puestos de trabajo y utilizando técnicas de análisis que les permiten aprovechar el valor de sus datos para generar nuevos ingresos y optimizar sus operaciones, además de nuevas herramientas para proteger su información”.

Como muestra de estos avances, Dell Technologies contó en este evento con la aportación de varios de sus clientes, quienes explicaron las capacidades que el uso de la tecnología de la compañía les ha reportado. Concretamente, VDC - Telefónica Tech, MGC Mutua, Sanitas, Abanca y el Servicio Global de Vídeo de Telefónica.

Y en esa evolución tecnológica de las compañías, el director de Dell Technologies en nuestro país destacó algunos puntos clave como son la computación periférica o Edge computing, y la prestación de tecnología como servicio. Respecto al primer punto, señaló Labarga que "en 2025, el 75% de los datos computarán fuera del CPD y habrá que llevar el análisis del dato al lugar donde se crea el dato". En este sentido, también resaltó la importancia de "5G para habilitar las comunicaciones entre el edge y el data center",

El 63% de los encuestados españoles afirma que su negocio se basa en datos y que son vitales para su organización, pero solo un 25% trata los datos como un capital

y el papel que está jugando la firma como socio de las operadoras.

En cuanto al consumo de tecnología como servicio, la propuesta de Dell Technologies se enmarca en el Proyecto APEX, "del que hay algunas ofertas en España y el resto llegará en los próximos meses y años". Labarga atribuyó el retraso de su despliegue en nuestro país a las pruebas y testeo que se está haciendo fuera, aunque "la oferta de FlexOndemand para la parte de storage está funcionando bien, con casos como el de Gobierno vasco, la sede española de Naciones Unidas o la Agencia Espacial Europea".

En la propuesta multicloud, el compromiso con VMware, a pesar de la separación, se mantendrá intacto. Como en años anteriores, María José Talavera, directora general de la compañía en España, intervino también en el evento de Dell Technologies, destacando "2021 como el año de consolidación de la estrategia multicloud que empezamos a trabajar hace unos años. El mundo es más híbrido que nunca. Ayudamos a los clientes a hacer el viaje de ida y vuelta a la nube con garantías de seguridad". Por su parte, Labarga comentó en rueda de prensa que "no hay un impacto desde el punto de vista operativo ni de propuesta de valor del mercado. Ganamos flexibilidad, eso sí, pero se han atado los acuerdos tecnológicos. Ahora podremos aprovechar las inversiones en I+D de los dos mundos".

LA PARADOJA DE LOS DATOS

Aprovechar el valor de los datos circulan por las organizaciones es uno de los principales retos que tienen las empresas por delante. Un desafío que ni siempre es fácil ni es como se piensa. Los resultados del estudio "The Data Paradox", realizado por Forrester tras la encuesta a 4.000 directores y responsables de estrategia de datos de organizaciones de 40 países de todo el mundo, entre ellos España y cuyos resultados presentó Dell Technolgoies en su fórum, revela que, a pesar de que existe un consenso generalizado sobre el hecho de que los datos son vitales para los negocios, la variedad y el crecimiento de los mismos los está convirtiendo más en una carga que en una oportunidad.

Algunos datos del informe a destacar son

❖ El 63% de los encuestados españoles afirma que su negocio se basa en datos y que "los datos son el elemento vital de su organización", pero solo un 25% declara tratar los datos como un capital y priorizar su uso en toda la organización.

❖ El 85% de las compañías españolas aún tiene que progresar en su tecnología y en sus procesos relacionados con los datos, así como en su cultura y habilidades de datos.

❖ Solo un 15% de las empresas españolas podría formar parte en estos momentos de la categoría Data Champions.

❖ El 70% de los encuestados en España está recopilando más datos de los que puede gestionar; el 62% afirma que su negocio aún necesita más datos de los que en estos momentos puede conseguir.

❖ El 59% de los profesionales españoles se queja de que tiene tal exceso de datos que no puede cumplir con los requisitos de seguridad y cumplimiento.

❖ El número de empresas que ha trasladado la mayoría de sus aplicaciones e infraestructuras a un modelo como servicio es todavía pequeño (16% en España)

❖ El 68% de los encuestados españoles ve que este modelo es una oportunidad para poder escalar y adaptarse a las cambiantes demandas de sus clientes.

❖ El 79% de los consultados nacionales dicen estar experimentando dificultades a la hora de capturar, analizar y gestionar sus datos. ■

MÁS INFORMACIÓN

- Dell Technologies Forum 2021
- Estudio "The Data Paradox"
- "La estrategia con VMware no está cambiando. Tenemos una misma hoja de ruta" (Aongus Hegarty, Dell Technologies)

it whitepapers

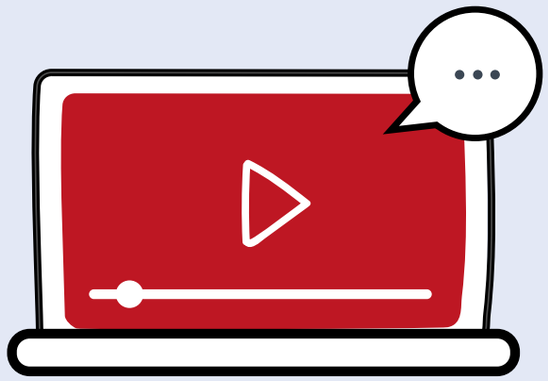
ESPAÑA EN LA ERA POST-COVID: TI para transformar el negocio

La COVID-19 ha trastocado la vida de empresas y ciudadanos que ven con incertidumbre el futuro. A la preocupación sanitaria se le unen unas previsiones económicas, y de desempleo, nada esperanzadoras. Descubre en este IT Research cuáles son las principales previsiones para España y cuál es el papel que va a jugar la tecnología en la recuperación a través de más de 40 gráficos, divididos en seis bloques (Perspectivas Económicas para España, Evolución del Empleo, Situación de las Empresas Españolas, La Transformación Digital en España, la I+D, y la Importancia de los Fondos Europeos), y las opiniones de diversos analistas del sector.

Tendencias de ciberseguridad 2022.
La ciberinteligencia entra en escena

Los ciberataques llevan creciendo en cantidad y en sofisticación desde hace años, y nada hace pensar que el año próximo vaya a cambiar la tendencia. Los ciberdelincuentes se esmeran cada vez más, han creado un negocio extremadamente rentable y siguen estando lejos de las autoridades. Todo apunta a que en 2022 veremos más ataques de ransomware porque siguen funcionando y porque se ha dado una vuelta de tuerca con la doble extorsión que provoca una situación insostenible. Ahora la ciberinteligencia entra en escena.

REGISTRO

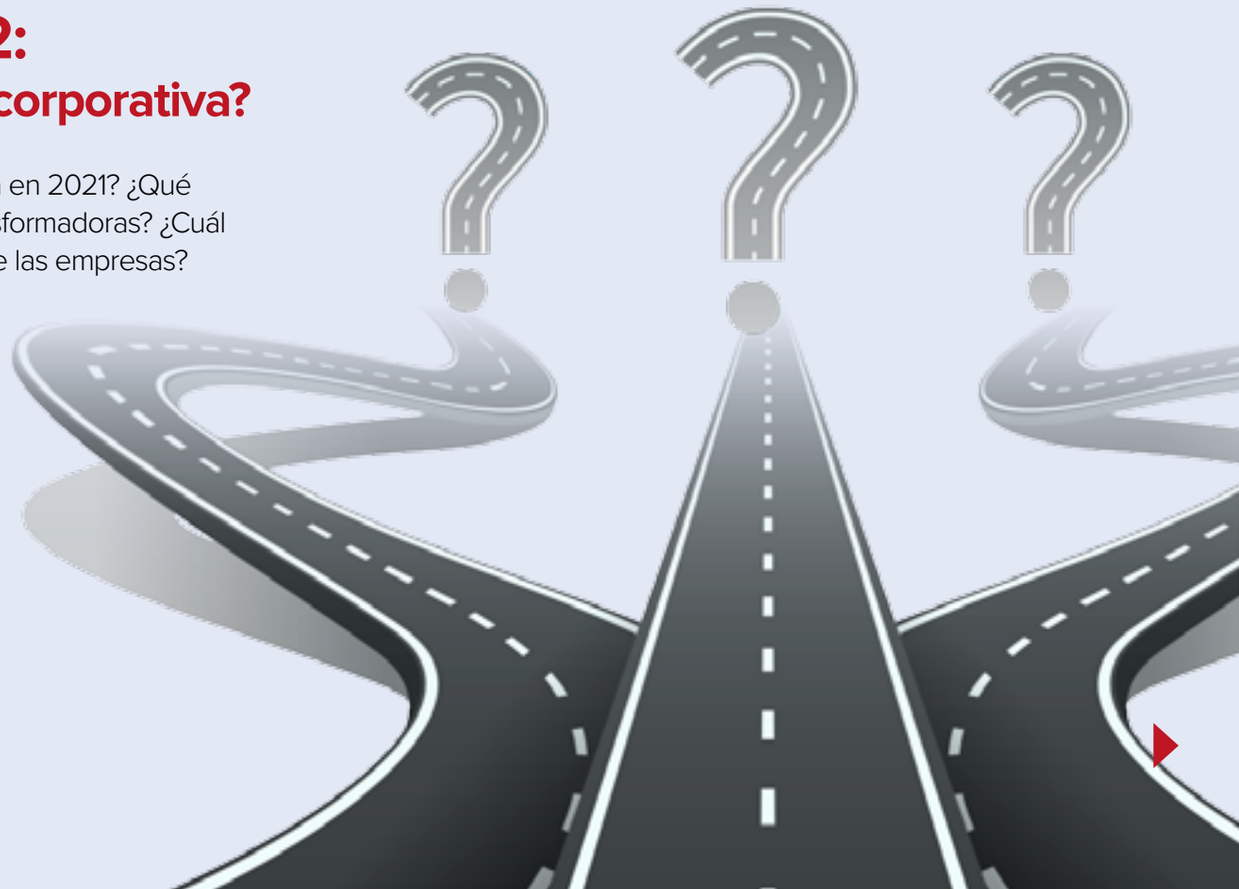


#ITWEBINARS

Tendencias IT 2022:
¿qué impactará en la TI corporativa?

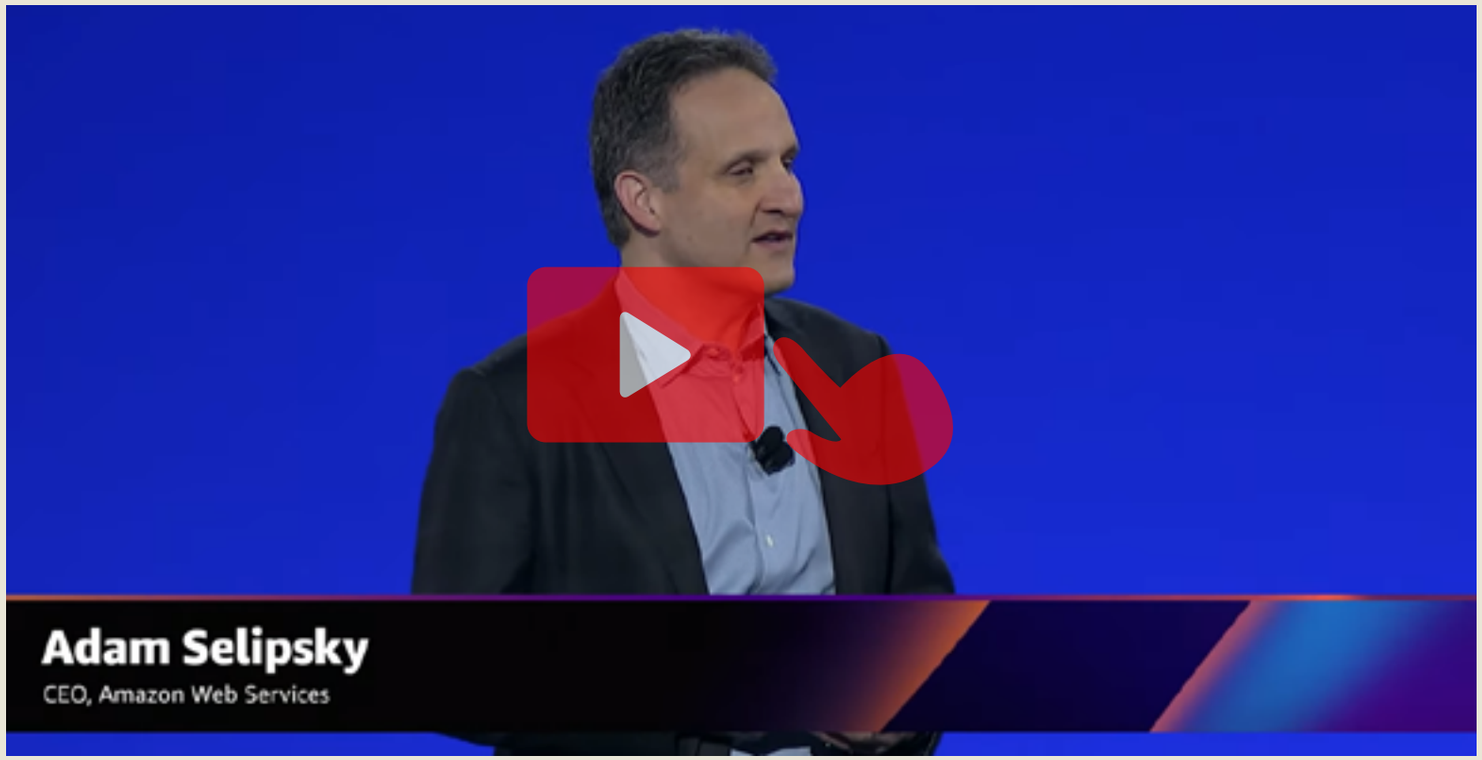
¿Cómo se ha comportado la TI corporativa en 2021? ¿Qué tecnologías han asumido el papel de transformadoras? ¿Cuál es el estado de la transformación digital de las empresas? ¿Cómo continuarán evolucionando en 2022? Todas estas serán cuestiones a abordar en esta sesión online junto a expertos del mercado y la empresa.

REGISTRO



AWS acelerará la transición de los clientes del mainframe a la nube

Un servicio para ayudar a los clientes a migrar sus cargas y datos del mainframe a la nube, soluciones para el despliegue de redes 5G privadas, herramientas para facilitar las labores de las compañías en IoT e IA o nuevas iniciativas de formación, son algunas de las novedades que se han anunciado en AWS re:Invent 21, junto con el compromiso de Amazon Web Services con la energía renovable, plasmado en la puesta en marcha de 18 nuevos proyectos de energía eólica o solar, cuatro de ellos en España.



SESIÓN DE APERTURA DE ADAM SELIPSKY, CEO DE AMAZON WEB SERVICES, EN AWS RE:INVENT 2021

AWS ha celebrado en Las Vegas, Estados Unidos, la décima edición de su evento AWS re:Invent, y son muchos los anuncios que se han ido realizando. Entre ellos destacan algunos de los realizados por Adam Selipsky, CEO de la compañía, como AWS Mainframe Modernization, AWS Private 5G, AWS Outpost Servers, AWS IoT TwinMaker, nuevas funcionalidades para SageMaker y dos iniciativas para fomentar el conocimiento alrededor de la Inteligencia Artificial.

AYUDAR A LOS CLIENTES EN SU TRANSICIÓN DEL MAINFRAME A LA NUBE

AWS Mainframe Modernization es un servicio que acelera y facilita a los clientes migrar su mainframe y cargas de trabajo heredadas a la nube, ya sea mediante la refactorización de

¿Te avisamos del próximo IT User?

estas cargas para ejecutarlas en AWS o bien transformando las antiguas aplicaciones en servicios de nube basados en Java.

En palabras de William Platt, director general de servicios de migración de AWS, "cada vez más clientes están modernizando sus aplicaciones trasladándolas a la nube para aprovechar la elasticidad y agilidad de AWS y reinventar las experiencias de los clientes a un menor coste. Pero, para la mayoría de las empresas, la migración de sus aplicaciones de mainframe a la nube es un territorio desconocido. Con el lanzamiento de AWS Mainframe Modernization, los clientes e integradores de sistemas pueden modernizar rápidamente sus cargas de trabajo de mainframe heredadas de forma predecible y deshacerse de gran parte de la complejidad y el trabajo manual que conllevan las migraciones".

CREACIÓN DE REDES 5G PRIVADAS Y SOLUCIONES PARA SUCURSALES

La segunda novedad es AWS Private 5G, pensada para que las empresas puedan configurar y escalar redes móviles 5G privadas en sus instalaciones, mediante la automatización de la configuración y puesta en marcha de la red, que escala la capacidad bajo demanda para admitir dispositivos adicionales y un mayor tráfico. Tal y como ha adelantado la firma, el precio de esta solución se basa en el consumo de datos, no en el número de dispositivos.

Y con la idea de expandir el modelo cloud más allá de la nube, AWS ha anunciado Outpost Servers, que proporcionan servicios de red y computación locales para ubicaciones con limitaciones de espacio, pero con necesidades de proceso de datos locales y baja latencia. Los primeros modelos tienen configuraciones de 1U, 2U y 4U, y se gestionan, al igual que el resto de los servicios, con la consola de AWS.

NOVEDADES PARA ENTORNOS IOT

AWS IoT TwinMaker es un nuevo servicio para los desarrolladores que acelera y simplifica la creación de gemelos digitales de sistemas del mundo real, como edificios, fábricas, equipos y líneas de producción. En entornos de alta complejidad, los gemelos digitales, represen-

AWS Mainframe Modernization es un servicio que acelera y facilita a los clientes migrar su mainframe y cargas de trabajo heredadas a la nube

taciones virtuales de sistemas físicos que se actualizan regularmente con datos del mundo real para replicar la estructura, estado y comportamiento de los objetos que representan, son complicados de crear y actualizar, y este servicio está definido para facilitar esta labor.

Pero no ha sido la única novedad para el mundo IoT, porque también se ha dado a conocer AWS IoT FleetWise, un servicio para los fabricantes de automóviles que simplifica y rentabiliza recopilar, transformar y transferir datos de los vehículos a la nube casi en tiempo real. Con AWS IoT FleetWise, los fabricantes de automóviles pueden recopilar y organizar los datos en cualquier formato presente en sus vehículos y estandarizar su formato para analizarlos más fácilmente en la nube.

NUEVO RESPALDO A LA FORMACIÓN

Con el foco puesto en su servicio de aprendizaje automático Amazon SageMaker, se han puesto sobre la mesa seis nuevas opciones, como un entorno sin código para realizar predicciones de

PONENCIA DE SWAMI SIVASUBRAMANIAN, VP MACHINE LEARNING DE AMAZON WEB SERVICES, EN AWS RE:INVENT 2021

Amazon Web Services acelera en su apuesta por las energías renovables

Durante el evento, AWS ha anunciado 18 nuevos proyectos de energía eólica y solar en Estados Unidos, Finlandia, Alemania, Italia, España y el Reino Unido, con un total de 5,6 gigavatios (GW) de capacidad adquirida hasta la fecha. Amazon cuenta ahora con 274 proyectos de energía renovable en todo el mundo y sigue avanzando en su objetivo de alimentar el 100% de sus operaciones comerciales con energía renovable para 2025, cinco años antes de su compromiso original para 2030.

En España son cuatro nuevos proyectos solares que sumarán más de 630 MW a la red. De hecho, estos se unen a las dos instalaciones actuales de energía solar en nuestro país en Andalucía y Aragón, y a otras que ya están en fase de desarrollo, con lo que el número definitivo se elevará a 9. Tal y como señalaba Carlos Carús, responsable técnico de AWS para el sur de Europa, la compañía está comprometida con la energía sostenible, una iniciativa donde la filial española quiere ser pionera.

aprendizaje automático, un etiquetado de datos más preciso mediante anotadores cualificados, una experiencia de notebook universal de Amazon SageMaker Studio para una mayor colaboración entre dominios, un compilador para la formación sobre aprendizaje automático que hace que el código sea más eficiente, una inferencia de aprendizaje automático de selección de instancias de computación y una computación sin servidor para la inferencia de aprendizaje automático.

A esto se unen dos nuevas iniciativas que hacen más accesible el aprendizaje automático. Por una parte, la beca AWS AI & ML, un nuevo programa de educación y becas, con una inversión de 10 millones de dólares, cuyo objetivo es preparar a estudiantes de áreas desfavorecidas para carreras profesionales centradas en el aprendizaje automático. Por otra parte, AWS está ampliando el acceso al aprendizaje automático a través de Amazon SageMaker Studio Lab, un servicio que ayuda a los clientes a crear, entrenar e implementar modelos de aprendizaje automático.

OTRAS NOVEDADES DE AWS RE:INVENT 21

Junto con estos anuncios principales, sobre el escenario también se han mostrado otras propuestas, como tres nuevas opciones sin servidor para su suite de servicios analíticos que simplifican el análisis de los datos a cualquier escala sin tener que configurar, escalar o gestionar la infraestructura subyacente. La opción para Amazon Redshift configura y escala automáticamente recursos, con lo que los clientes tienen la capacidad de ejecutar cargas de trabajo de análisis de alto rendimiento sobre petabytes de datos sin tener que gestionar clústeres de almacenes de datos. La opción para Amazon Managed Streaming para Apache Kafka (Amazon MSK) escala recursos para simplificar la ingesta de datos en tiempo real y el streaming. Amazon EMR ofrece ahora una opción sin servidor para que los clientes ejecuten aplicaciones analíticas usando marcos de Big Data de código abierto como Apache Spark, Hive y Presto, sin tener que aprovisionar, gestionar y escalar la infraestructura subyacente.

Asimismo, también han anunciado tres nuevas instancias de Amazon Elastic Compute Cloud (Amazon EC2) con la tecnología de los chips diseñados por AWS, que ayudan a los clientes a mejorar el rendimiento, coste y eficiencia energética de las cargas de trabajo que se ejecutan en Amazon EC2. Las nuevas instancias C7g, con la nueva generación de procesadores AWS Graviton3, aportan hasta un 25% más rendimiento que la generación C6g con los procesadores AWS Graviton2. Las nuevas instancias Trn1 con los chips AWS Trainium ofrecen la mejor relación precio/rendimiento y los tiempos más rápidos para el entrenamiento de modelos de aprendizaje automático en Amazon EC2, mientras que las nuevas instancias optimizadas para el almacenamiento Im4gn/Is4gen/I4i basadas en los AWS Nitro, ofrecen tasas de I/O elevadas ejecutándose en Amazon EC2. ■

MÁS INFORMACIÓN

- AWS re:Invent 21
- Proyectos de sostenibilidad de AWS en España

Siguen los trabajos para la Región AWS en España

De forma paralela a estos anuncios, y con el foco en nuestro país, Amazon Web Services sigue trabajando en la apertura de su nueva región en España, anunciada hace ahora un año, y prevista para mediados de 2022. Ubicada en Aragón, la nueva región contará con tres zonas de disponibilidad, para asegurar la redundancia, y podría llegar a generar hasta 1.300 empleos en 10 años, para lo que AWS tiene previsto realizar una inversión de 2.500 millones en esta década.

La UE sigue muy lejos de los objetivos marcados en digitalización para 2030

Los datos del último Índice de Intensidad Digital, publicado por Eurostat, ponen de relieve que queda mucho camino por recorrer para cumplir con la visión de la UE para la transformación digital. Este indicador, que mide el nivel de digitalización de las compañías, muestra que, en 2020, solo el 1% de las empresas de la Unión con al menos 10 empleados alcanzaron un nivel muy alto de intensidad digital, mientras que el 14% alcanzó un nivel alto.

La Unión Europea ha fijado la transición digital como uno de los ejes que marcarán la recuperación y ha marcado como objetivo acelerar la digitalización hasta 2030 para avanzar en una Europa adaptada a la era digital. De hecho, uno de los ejes de su programa de trabajo para 2022 es la digitalización. La adopción de tecnologías digitales por parte de las empresas tiene el potencial de mejorar los servicios y productos, así como de aumentar la competitividad. Sin embargo, el punto de partida muestra que el objetivo se antoja lejano, si tenemos en cuenta los datos del último Índice de Intensidad Digital (DII), publicado por Eurostat, solo el 1% de las empresas de la Unión con al menos 10 empleados alcanzaron un nivel muy alto de intensidad digital, mientras que el 14% alcanzó un nivel alto.

La mayoría de las empresas registraron niveles bajos (46%) o muy bajos (39%) y, eso que,

en comparación con los resultados 2018, ha experimentado una mejora general a nivel de la UE, con incrementos tanto en niveles muy altos (+5 puntos porcentuales) como altos (+0,4).

El DII mide el uso de diferentes tecnologías digitales por parte de las empresas y su puntuación (0-12) está determinada por cuántas de las 12 tecnologías digitales seleccionadas utilizan las empresas. Cuanto mayor sea la puntuación, mayor será la intensidad digital de la empresa, que va de muy baja a muy alta.

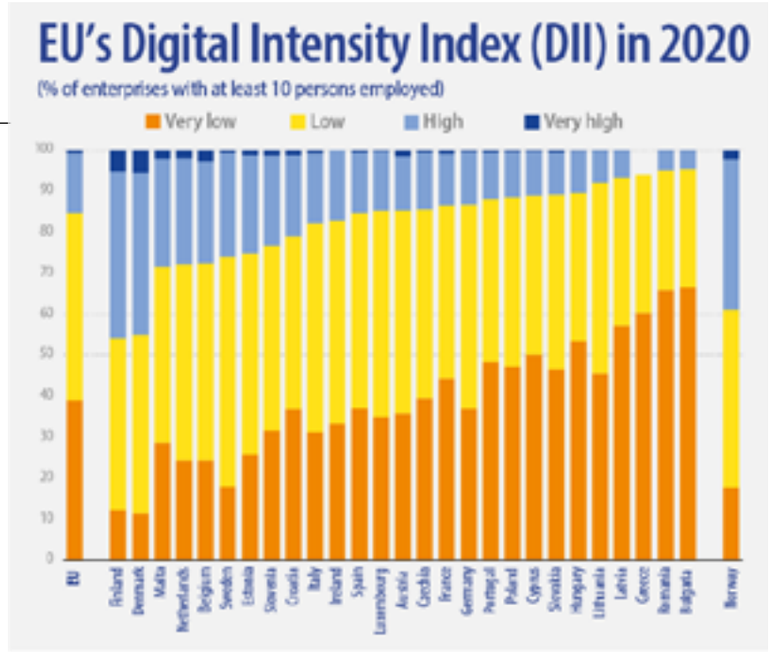
Los datos de Eurostat muestran que el 9% de las grandes empresas de la UE tenían un DII muy alto y el 42% un nivel alto, mientras que solo el 2% de las empresas medianas registraron un nivel de intensidad muy alta y una cuarta parte (25%) un IDI alto. Solo el 0,4% de las pequeñas empresas alcanzó una intensidad digital muy alta, y solo el 12% obtuvo un DII alto.

Casi la mitad de las empresas medianas (47%) y pequeñas (46%) mostraron un bajo nivel de intensidad digital.

Finlandia y Dinamarca (ambos 5%) y Bélgica (3%) son los países de la UE con las mayores proporciones de empresas altamente digitalizadas, mientras que el resto de países tenían como máximo un 2% de empresas con un nivel muy alto de DII.

España se encuentra en la parte media de la tabla, con un 1% de empresas en el nivel máximo. El 35% de las empresas se encuentran en un nivel muy bajo y el resto, y el porcentaje asciende al 80% si sumamos a las que están en un nivel bajo. El 19% restante se encuadran en el alto.

Por el contrario, en Bulgaria y Rumanía (ambos 66%), Grecia (60%), Letonia (57%) y Hungría (53%), la mayoría de las empresas muestran un DII muy bajo, lo que indica una pequeña inversión en tecnologías digitales. Según uno de los objetivos de la visión de la UE para la transformación digital , al menos el 90% de las pequeñas y medianas empresas (PYME) de la UE deberían alcanzar un nivel básico de intensidad digital para 2030. El nivel básico implica el uso de al menos cuatro tecnologías e incluye empresas con DII bajo, alto y muy alto. En 2020, tres de cada cinco pymes (60%) de la UE alcanzaron al menos un nivel básico de intensidad digital, frente al 89% de las grandes empresas.



Clica en la imagen para ver la infografía más grande

LA COMISIÓN EUROPEA INVERTIRÁ CERCA DE 2.000 MILLONES EN EL PROGRAMA EUROPA DIGITAL

La Comisión realizará inversiones estratégicas para avanzar en el transición digital dentro del programa Europa Digital, que tiene como objetivo reforzar la soberanía tecnológica de Europa y aportar soluciones digitales al mercado en beneficio de los ciudadanos, las administraciones públicas y las empresas. Las partidas se destinarán a tres programas de trabajo. Uno de ellos, el principal, que está dotado con 1.380 millones de euros, invertirá sobre todo en los ámbitos de la inteligencia artificial (IA), la nube y los espacios de datos, la infraestructura de comunicación cuántica, las competencias digitales avanzadas y el amplio uso de las tecnologías digitales en toda la economía y la sociedad, hasta finales de 2022.

El segundo se centra en la financiación en el ámbito de la ciberseguridad, con un presupuesto de 269 millones de euros hasta finales de 2022, mientras que el tercero pretende crear y explotar la red de centros europeos de innovación digital, con un presupuesto de 329 millones de euros hasta finales de 2023.

Según informa la Comisión, el principal programa de trabajo del programa Europa Digital abarcará inversiones como las siguientes:

❖ **Creación de espacios comunes de datos** (por ejemplo, espacios de datos para la fabricación, la movilidad y la financiación) que faciliten el intercambio transfronterizo de datos para el sector público y las empresas, incluidas las pymes y las empresas emergentes, y creación de una infraestructura y unos servicios federados de la nube/borde, esto es, una espina dorsal de soluciones digitales que garanticen la seguridad de los flujos de datos.

❖ **Creación de instalaciones de ensayo y experimentación** para soluciones basadas en inteligencia artificial con el fin de impulsar el uso de IA fiable (también por parte de las pymes y las empresas emergentes) para abordar cuestiones sociales clave, tales como el cambio climático y la asistencia sanitaria sostenible (por ejemplo, creaciones de instalaciones de ensayo de IA para la salud y ciudades y comunidades inteligentes).

❖ **Creación de una infraestructura de comunicación cuántica segura para la UE** (EuroQCI) que ofrezca una elevada resiliencia frente a los ciberataques.

❖ **Creación e impartición de cursos de máster en tecnologías digitales avanzadas** clave para impulsar las competencias digitales en Europa, por ejemplo, cursos intensivos en materia digital para las pymes, tal como se anunció en la Agenda de Capacidades de 2020 y en la estrategia para las pymes.

❖ **Creación, explotación y mantenimiento permanente y en evolución de servicios digitales** que apoyen la interoperabilidad transfronteriza de soluciones en apoyo de las administraciones públicas (por ejemplo, identidad digital europea).

El programa sobre ciberseguridad incluirá inversiones en la creación de equipos, herramientas e infraestructuras de datos avanzados en materia de ciberseguridad. Financiará el fomento y el mejor uso de los conocimientos y capacidades relacionados con la ciberseguridad, promoverá el intercambio de mejores prácticas y garantizará la amplia utilización de soluciones de ciberseguridad de última generación en toda la economía europea.

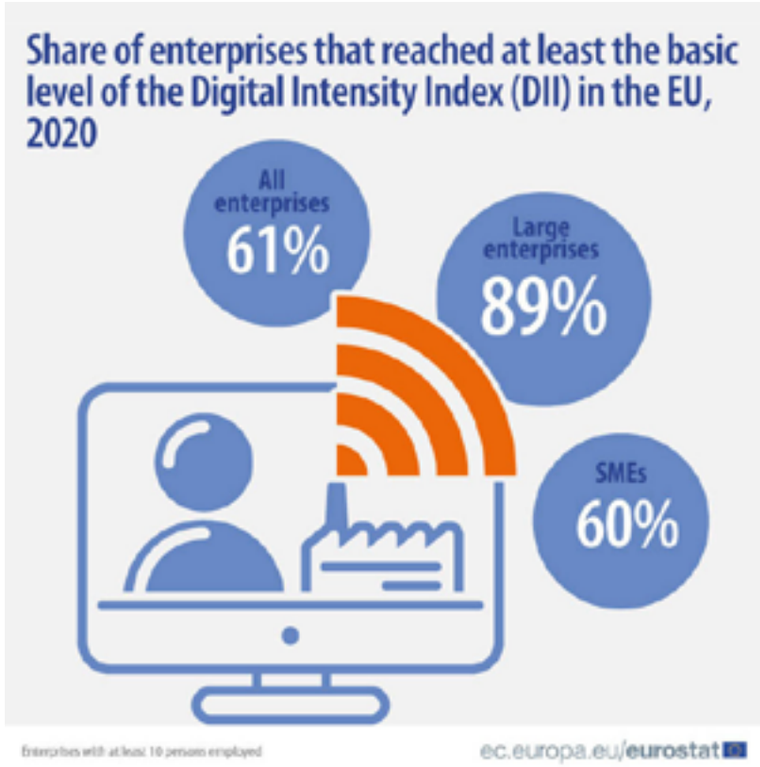
El último de ellos, será crear una red de centros europeos de innovación digital que facilite la realización de ensayos tecnológicos y sostenga la transformación digital de organizaciones públicas y privadas de toda Europa, también la de las administraciones nacional, regional o local, según proceda.

Las primeras convocatorias para el programa Europa Digital se han publicado a finales de noviembre, y en 2022 se publicarán más. Los programas de trabajo se ejecutarán principalmente mediante subvenciones y contratos públicos. ■

MÁS INFORMACIÓN

The Digital Economy and Society Index (DESI)

España en el Informe DESI 2021



Clica en la imagen para ver la infografía más grande

La documentación TIC, a un solo clic

Cómo las empresas B2B pueden diversificar sus canales de ventas digitales

Las empresas que comercializan bajo el modelo B2B han tenido que analizar la eficacia de sus canales de venta existentes y aprovechar la oportunidad para abrir otros nuevos. ¿Cuáles son los riesgos y recompensas de diversificar los canales de venta digitales? ¿Te preocupa perder tus relaciones actuales si adoptas el método digital?

La hoja de ruta de DevOps en materia de seguridad

Las compañías, buscando agilidad, flexibilidad y reducción de tiempos para llevar sus aplicaciones al mercado, han apostado por DevOps, pero ¿es esta decisión un buen paso cuando hablamos de seguridad? Este documento nos muestra que, cuando una organización gestiona bien DevOps, consigue reforzar la estrategia de seguridad en todos los aspectos.

MTWO Complete Construction Cloud

MTWO Complete Construction Cloud es una plataforma empresarial integrada de modelado de información de construcción en cinco dimensiones (BIM 5D) en la nube que permite a contratistas, propietarios de activos y desarrolladores acelerar su proceso de transformación digital.

Informe: Cloud, en busca de la agilidad

La nube se ha asentado en las organizaciones como un modelo de TI que permite ganar agilidad en las operaciones y en el despliegue de nuevos servicios. Este informe IT Trends apunta las principales tendencias en torno a la cloud en nuestro país.

Una de cada cuatro empresas tuvieron dificultad para contratar a perfiles TIC en 2020

El empleo en el sector tecnológico necesita más perfiles especializados, un dato en el que vuelve a incidir un informe del ONTSI, que analiza los indicadores sobre la situación española y europea. Además, el documento destaca la importante brecha de género existente.

El Observatorio Nacional de Tecnología y Sociedad (ONTSI) ha publicado el informe con el que pretende tomar el pulso al mercado laboral TIC en nuestro país y la UE.

El sector tecnológico ha sido tradicionalmente fuente de creación de empleo. Sin embargo, hoy el sector tiene dificultades para encontrar los perfiles adecuados a sus necesidades. Según la Comisión Europea, en 2020 hubo 341.000 puestos de trabajo vacantes para profesionales de datos en Europa, más 168.000 en la rama de ciberseguridad.

En 2020, una de cada cuatro empresas españolas y casi la mitad de las europeas que intentaron contratar profesionales especializados reconocieron que no lo tuvieron fácil. Los principales obstáculos fueron la falta de experiencia y de cualificación, la falta de solicitudes o unas expectativas salariales demasiado elevadas.

España contaba el año pasado con 727.000 especialistas TIC, el equivalente al 3,8% del empleo en todo el país, por debajo del 4,8% de la me-

¿Te avisamos del próximo IT User?

dia europea. Además, destaca que, aunque la expresión especialista TIC puede parecer poco concreta, lo cierto es que el 80% de los contratos de especialistas firmados entre enero y agosto de 2021 correspondieron a solo siete categorías profesionales: programadores informáticos (23,5%), técnicos en operaciones de sistemas informáticos (17,3%), analistas, programadores, y diseñadores Web y multimedia (12,5%), instaladores y reparadores en TIC (10,4%), analistas de sistemas (6,4%) y técnicos en asistencia al usuario de Tecnologías de la Información (5,7%).

BRECHA DE GÉNERO

El sector es claramente masculino, como muestran los datos. En 2020, había 144.000 expertas en TIC, lo que supone un 19,8 % del total. Esta proporción es ligeramente superior a la media europea, que es del 18,5 %.

Una de las razones a las que apunta el informe para explicar este desequilibrio es la falta de mujeres graduadas en STEM, las siglas en inglés que engloban los estudios sobre ciencias, tecnología, ingenierías y matemáticas. En 2018, la proporción de mujeres graduadas en estas disciplinas era de 14,3 por cada mil mujeres de entre 20 y 29 años en Europa. En España, la cifra era menor de 12,7.

OBJETIVOS

La Comisión Europea quiere que el número de especialistas TIC en la UE pase de los 8,4 millones en 2020 a 20 millones en 2030, es decir, doblar el número actual de especialistas en menos de una década. El objetivo fijado por nuestro país en la agenda España 2025 es incrementar en 20.000 el número de especialistas TIC entre 2020 y 2025, en áreas específicas como la inteligencia artificial, la ciberseguridad y análisis de datos.

SOLO EL 3,2% DE LOS PROFESIONALES CUALIFICADOS EN ESPAÑA SON EXPERTOS EN NUEVAS TECNOLOGÍAS

La importancia de la inclusión de nuevas tecnologías en la empresa es indiscutible dadas sus múltiples ventajas. En este sentido, España presenta una evolución positiva de los principales indicadores internacionales de digitalización en los últimos años pero no ha avanzado de la misma forma en la dimensión de Integración de Tecnología Digital por parte de las empresas, según el INE.

En 2020, una de cada cuatro empresas españolas y casi la mitad de las europeas que intentaron contratar profesionales especializados reconocieron que no lo tuvieron fácil

ACTUALIDAD

España necesita un mayor grado de especialización en competencias tecnológicas. Así lo evidencian los resultados de un estudio de IEBS Business School, que destaca entre sus conclusiones que, aunque las empresas están impulsando su transformación digital solo el 3,2% de los profesionales son expertos en las tecnologías que la están impulsando.

Para la escuela de negocios, la falta de formación en las nuevas tecnologías es la principal barrera que se encuentran tanto microempresas como pymes y grandes compañías a la hora de avanzar en la digitalización, por delante de los elevados costes de implementación y la ausencia de personal cualificado.

La encuesta, realizada por IEBS entre más de 1.500 profesionales españoles, indica también que hay una mayor conciencia general sobre este desconocimiento, ya que nueve de cada diez participantes han asegurado tener la intención de formarse en alguna de estas tecnologías para mejorar su recorrido profesional. Los puestos de trabajo relacionados con la tecnología, como especialistas en Big Data, análisis de datos, Ciberseguridad, Inteligencia Artificial, física, matemáticas, simulación, realidad virtual... encabezan los rankings de perfiles más demandados.

La tecnología más utilizada en la empresa es la computación en la nube como la más utilizada (69,2%) seguida de las plataformas de analítica y Business Intelligence (53,8%), la Realidad Aumentada y/o Realidad Virtual (46,2%) y la Inteligencia Artificial (30,8%). De cara al futuro, la inteligencia artificial ha sido la tecnología preferida por los encuestados, que prevén utilizarla en un futuro próximo, con un 69,2%. A esta le sigue Blockchain e Internet de las Cosas, ambas con un 38,5%.

Por otro lado, en cuanto a las tecnologías que consideran que están lo suficientemente desarrolladas y extendidas en las empresas digitales, la computación en la nube, las plataformas de analítica y Business Intelligence y la inteligencia artificial han sido las más seleccionadas, con un 69,2%, un 53,8% y un 38,5%, respectivamente. Las que menos, la Realidad Aumentada y/o Realidad Virtual, IoT y Blockchain. ■

MÁS INFORMACIÓN

- ONTSI: Indicadores sobre el empleo tecnológico en España y en la Unión Europea
- Falta de formación: principal barrera para la digitalización

it whitepapers

IT TRENDS 2021. ASIMILANDO LA ACELERACIÓN DIGITAL

¿Qué tendencias tecnológicas dominarán en el año post-pandemia? ¿En qué áreas y tendencias TI se concentrarán las inversiones de las empresas? ¿Qué corrientes se desarrollarán en los próximos meses? ¿Qué objetivos se marcan los responsables de TI de las empresas españolas para este año 2021? En este informe de IT Research desvelamos las principales claves de las estrategias TI para este 2021.

La nube pública y el segmento de IaaS impulsan el mercado de servicios cloud

Se espera que el tamaño del mercado cloud a nivel mundial crezca un 16,3% anual hasta 2026. Tecnologías emergentes, como Big Data, Inteligencia Artificial y aprendizaje automático (ML), están ganando tracción, lo que en última instancia está llevando al crecimiento del mercado de la computación en la nube.

Según un nuevo informe de investigación publicado por MarketsandMarkets, se espera que el tamaño del mercado global de cloud computing crezca de 445.300 millones de dólares en 2021 a 947.300 millones para 2026, lo que representa una tasa de crecimiento anual compuesta (CAGR) del 16,3% durante el período de pronóstico.

La flexibilidad y agilidad de los modelos basados en la nube respaldarían las necesidades de servicios de TI de las empresas. El creciente volumen de datos en sitios web y aplicaciones móviles, el creciente enfoque en la entrega de aplicaciones para impulsar la satisfacción del cliente y la creciente necesidad de controlar y reducir el gasto de capital (CAPEX) y el gasto operativo (OPEX) son algunos de los factores que impulsan el crecimiento del mercado. Además, tecnologías emergentes, como Big Data, Inteligencia Artificial (IA) y aprendizaje automático (ML), están ganando tracción, lo que en última instancia está

CONTENIDOS↓

llevando al crecimiento del mercado de la computación en la nube a nivel mundial.

El cierre repentino de oficinas, escuelas, universidades y tiendas físicas minoristas ha interrumpido masivamente las operaciones; esto ha llevado a un aumento en la demanda de herramientas y servicios digitales. Se espera que industrias como TI y telecomunicaciones, comercio minorista y online, medios de comunicación y servicios financieros, aumenten el gasto en servicios basados en la nube para mantener su negocio. También se espera que las industrias altamente reguladas muevan cargas de trabajo selectivas a entornos de nube pública.

Los costes más bajos y las crecientes capacidades de seguridad dan como resultado una creciente popularidad de la nube pública. Los servicios ofrecidos a través del modelo de implementación pública son gratuitos u ofrecidos bajo un modelo de suscripción. Las ventajas de usar la nube pública incluyen simplicidad y facilidad de implementación. Además, la inversión inicial requerida para el despliegue es mínima, y no hay responsabilidades involucradas en la gestión de la infraestructura.

El segmento de infraestructura como servicio (IaaS) registrará la tasa de crecimiento más alta durante el período de pronóstico. El entorno empresarial en constante cambio y las demandas de los clientes alientan a las empresas a aumentar su enfoque en sus operaciones de negocio principales, e IaaS permite a las

La flexibilidad y agilidad de los modelos basados en la nube respaldarían las necesidades de servicios de TI de las empresas

empresas escalar su infraestructura de TI sin hacer grandes desembolsos. IaaS proporciona flexibilidad, movilidad, acceso fácil y escalable a las aplicaciones, para ayudar a las empresas a centrarse en sus negocios principales. ■

MÁS INFORMACIÓN

- Mercado Cloud Computing 2021-2026
- Claves para una estrategia multicloud de éxito
- Guía completa sobre la economía cloud

LOS INGRESOS EN EL MERCADO DE LA NUBE AUMENTAN UN 25% EN EL PRIMER SEMESTRE DE 2021

Descarga este documento ejecutivo de IT RESEARCH

NUEVO INFORME

El 70% de las compañías españolas prevé aumentar su gasto en ciberseguridad

Más del 50% de las compañías que han participado en un estudio de PwC esperan que los ciberataques vayan a más en 2022, tras un 2021 de máximos históricos. Siete de cada diez compañías españolas prevén aumentar sus presupuestos en ciberseguridad.

2021 ha sido un año récord en el número de ataques registrados, y las empresas creen que el panorama de ciberamenazas va a seguir su escalada en 2022, según un estudio de PwC, que recoge la opinión de 3.602 responsables de seguridad, CEO y altos directivos de 66 países, entre ellos España.

De sus respuestas se desprende que esperan un nuevo incremento de los ciberataques a empresas en 2022: más del 50% de las compañías entrevistadas cree que el próximo año se superarán los niveles históricos de 2021. Esta previsión va a tener su reflejo en los presupuestos destinados a ciberseguridad. El 69% de las compañías (el 70% en España) prevé aumentar sus inversiones en ciberseguridad, frente al 55% del año pasado. Además, tanto a escala mundial como a nivel local, un 26% los incrementará un 10% o más.

LA NUEVA ERA DEL TRABAJO REMOTO EXIGE UNA MENTALIDAD DE SEGURIDAD MODERNA

ATAQUES QUE PREDOMINARÁN

Según el 57% de los encuestados, los ataques que más van a crecer el próximo año son los que tienen como objetivo los servicios en la nube y los ransomware, seguidos del malware descargado a través de las actualizaciones de software y los ataque al software de la cadena de suministro y al correo corporativo (56%). Los responsables de ciberseguridad españoles coinciden en señalar a las amenazas a los servicios en la nube como las que más se van a incrementar seguidas, en este caso, por los ataques a la cadena de suministro.

La puerta de entrada que más van a utilizar estos ciberdelincuentes serán Internet de las Cosas, los móviles, los proveedores de servicios en la nube, la ingeniería social y los proveedores, Mientras que los tres principales protagonistas de estos ciberataques serán los cibercriminales, los hackers y activistas, y los Estados nación.

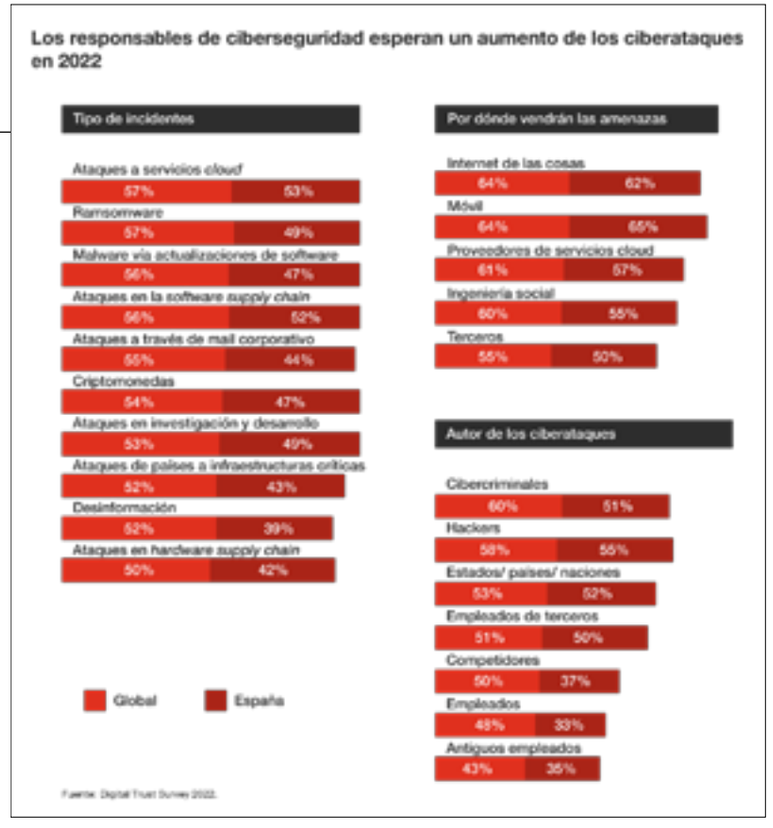
Este documento pone de relieve también que hay factores que están haciendo más difícil la protección: la falta de conocimiento de las brechas que pueden sufrir los proveedores con los que trabajan y terceras partes, y la complejidad tanto de las arquitecturas tecnológicas como de las infraestructuras de datos.

El informe pone un punto de atención especial sobre el conjunto de proveedores y terceras partes que intervienen en la operativa diaria de una compañía. Las empresas los podrían estar pasando por alto y que éstos estarían convirtiéndose en un punto ciego de entrada de los ciberataques. El 60% de los entrevistados reconoce no tener un conocimiento profundo de las brechas de seguridad asociadas con estas terceras partes y un 20% asegura tener poco o ninguno. En el caso de los encuestados en España, la situación es idéntica.

Además, las empresas se han vuelto demasiado complejas como para poder ser aseguradas en su totalidad como consecuencia del incremento exponencial de la conectividad y de la aceleración de la transformación digital en los últimos años. El 75% de encuestados afirma que sus empresas tienen un exceso de complejidad en su modelo operativo y en sus procesos que podría ser innecesario, lo que conlleva un incremento notable de los riesgos de ciberseguridad y de privacidad.

Las infraestructuras de datos de las empresas y las arquitecturas tecnológicas, con multitud de sistemas distintos, muchos de ellos heredados y difícilmente integrables, son algunos de los principales factores que más contribuyen a esta complejidad. Para los entrevistados, esta

El 69% de las compañías (el 70% en España) prevé aumentar sus inversiones en ciberseguridad, frente al 55% del año pasado. Además, tanto a escala mundial como a nivel local, un 26% los incrementará un 10% o más



Clica en la imagen para ver la infografía más grande

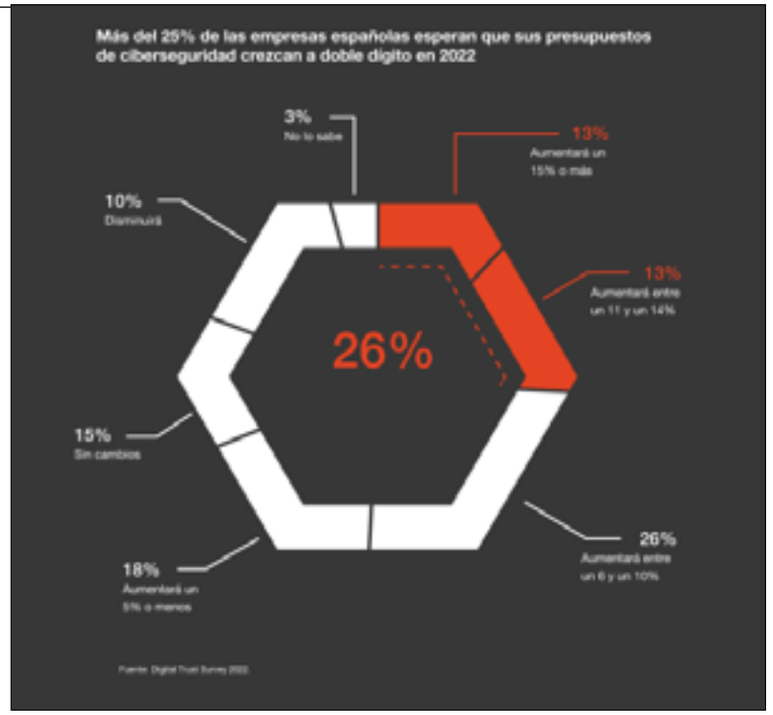
Sólo el 34% del conjunto de los participantes en el estudio -el 33% en España-, afirman haber implantado procesos formales de seguridad de los datos que incluyan su cifrado y su intercambio seguro

circunstancia se traduce en el día a día de las compañías, en pérdidas económicas, en una menor capacidad de innovación y en una menor capacidad de recuperación ante ciberataque o ante los fallos tecnológicos.

Finalmente, el estudio resalta la importancia de los datos: el activo más codiciado por los ciberdelincuentes. Un riesgo que las compañías podría minimizar protegiendo los datos contra la manipulación y el robo. Sólo el 34% del conjunto de los participantes en el estudio -el 33% en España-, afirman haber implantado procesos formales de seguridad de los datos que incluyan su cifrado y su intercambio seguro y que determine cuáles son los que deben proteger y cuáles no. ■

MÁS INFORMACIÓN

- Tendencias de ciberseguridad 2022. La ciberinteligencia entra en escena
- Global Digital Trust Insights 2022



Clica en la imagen para ver la infografía más grande

Encuentros it TRENDS

TENDENCIAS DE CIBERSEGURIDAD 2022. LA CIBERINTELIGENCIA ENTRA EN ESCENA

Los ciberataques llevan creciendo en cantidad y en sofisticación desde hace años, y nada hace pensar que el año próximo vaya a cambiar la tendencia. Los ciberdelincuentes se esmeran cada vez más, han creado un negocio extremadamente rentable y siguen estando lejos de las autoridades. Como consecuencia, las pérdidas financieras de los ciberataques se han multiplicado, así como los daños a la marca.

FORO it User TECH & BUSINESS

CONTENIDOS↓

ADMINISTRACIÓN PÚBLICA: AFRONTANDO LA DÉCADA DIGITAL

Organiza

it Digital MEDIA GROUP

Patrocinadores Platinum

CISCO

dynatrace

salesforce

Socios colaboradores

Astic

Foro CPP colaboración público-privada TECNOLOGÍA & INNOVACIÓN

Patrocinadores Gold

blueprism

f5

MicroStrategy

proofpoint

VEEAM

CONTENIDOS↓

LA BRÚJULA DIGITAL PARA 2030: LA VÍA EUROPEA DE LA DÉCADA DIGITAL, ES UNA ESTRATEGIA DE LA COMISIÓN EUROPEA DIRIGIDA A CONSEGUIR UNA TRANSFORMACIÓN DIGITAL EXITOSA, BASADA EN EL EMPODERAMIENTO DE LOS CIUDADANOS Y EL LIDERAZGO TECNOLÓGICO, CON EL OBJETIVO DE QUE SIEMBRE LAS BASES DE UNA SOCIEDAD MÁS RESILIENTE Y PRÓSPERA.

DIBUJANDO EL CAMINO HACIA LA DÉCADA DIGITAL

La Unión Europea quiere avanzar en la digitalización de la sociedad y la economía, y, para ello, la Comisión Europea presentaba el pasado mes de marzo la Brújula Digital 2030, una hoja de ruta para el desarrollo de los objetivos digitales de nuestro continente con especial interés en la capacitación de las personas, el desarrollo de las infraestructuras necesarias, la transformación de los negocios y el despliegue de unos servicios públicos plenamente digitales.

En palabras de la Presidenta de la Comisión, Ursula von der Leyen, "Europa tiene una oportunidad única de reconstruirse mejor. Mediante el nuevo presupuesto plurianual y el Mecanismo de Recuperación y Resiliencia, hemos movilizado recursos sin precedentes para invertir en la transición digital. La pandemia ha puesto de manifiesto hasta qué punto las tecnologías y capacidades digitales son cruciales para trabajar, estudiar y mantenerse en contacto, y qué aspectos deberíamos mejorar. Ahora debemos hacer de esta la Década Digital de Europa para que todos los ciudadanos y empresas puedan acceder a lo mejor que pueda ofrecer el mundo digital. La Brújula Digital de hoy nos ofrece una visión clara de la manera de conseguirlo".

BRÚJULA DIGITAL 2023: LA VÍA EUROPEA PARA LA DÉCADA DIGITAL

POBLACIÓN CON CAPACIDADES DIGITALES

Europa necesita ciudadanos con capacidades digitales, una mano de obra cualificada digitalmente y muchos más expertos en estas tecnologías que en la actualidad. Las competencias digitales básicas para todos los ciudadanos y la oportunidad de adquirir competencias especializadas en tecnologías de la información y la comunicación (TIC) para la mano de obra son un requisito previo para participar activamente en la Década Digital. Por tanto, cuando la Comisión Europea habla en su estrategia de ciudadanos con capacidades digitales y profesionales del sector digital altamente cualificados, lo que quiere conseguir es que de cara al año 2030, no menos del 80 % de los ciudadanos adultos tengan competencias digitales básicas y que, por lo menos se cuente con veinte millones de especialistas en TIC en los países de la Unión, incrementando, de forma paralela, el porcentaje de mujeres en este tipo de perfiles y puestos de trabajo.

INFRAESTRUCTURAS DIGITALES SEGURAS, EFICACES Y SOSTENIBLES

La Comisión estima que Europa sólo alcanzará el liderazgo digital si se basa en infraestructuras digitales sostenibles, seguras y eficaces para la conectividad, la microelectrónica y el procesamiento de datos. Una base sólida para la tecnología digital permitirá la innovación y apoyará la ventaja competitiva de la industria europea. Es necesario realizar importantes inversiones en todos estos ámbitos que requieren una coordinación para alcanzar la escala europea.

Todo esto se traduce en que para finales de la década, todos los hogares de la UE han de tener conectividad de Gigabit y que la cobertura de las redes 5G deba alcanzar todas las zonas pobladas, además de asegurar que la producción de semiconductores punteros y sostenibles en Europa debería representar una quinta parte de la producción mundial, el despliegue en la Unión de 10.000 nodos externos seguros y climáticamente neutros, y que Europa debería tener su primer ordenador cuántico.

TRANSFORMACIÓN DIGITAL DE LAS EMPRESAS

Para los miembros de la Comisión Europea, la verdadera Transformación Digital de las empresas dependerá de su capacidad para adoptar las nuevas tecnologías con rapidez y de forma generalizada, incluso en los ecosistemas industriales y de servicios que hasta la fecha se encuentran más retrasados en su avance. Esto permitirá un uso más eficiente de los recursos, impulsará la productividad de los materiales y reducirá la vulnerabilidad a las crisis de suministro. La PYME desempeña un papel fundamental en este proceso, no sólo porque representan el grueso de las empresas de la Unión, sino también porque son una fuente crítica de innovación. Para la Comisión, un mercado único que funcione de verdad debería crear condiciones favorables para la asimilación digital, la innovación disruptiva, el crecimiento rápido y la ampliación.

Para alcanzar esta meta, la Comisión Europea espera que en el año 2030 el 75% de las empresas estén utilizando servicios de computación en nube, macrodatos e Inteligencia Artificial, así como que nueve de cada diez pequeñas y medianas empresas cuentan con lo que denominan como nivel básico de intensidad digital, así como que el número de unicornios de la UE debería multiplicarse por dos.

DIGITALIZACIÓN DE LOS SERVICIOS PÚBLICOS

Desde la perspectiva de la Comisión, Europa debe aprovechar la digitalización para impulsar un cambio de paradigma en la forma en que los ciudadanos y las empresas interactúan con las Administraciones Públicas y las instituciones democráticas. Los servicios públicos deben ser totalmente accesibles en línea, incluso para las personas con discapacidad, y beneficiarse de herramientas fáciles de usar con al-

tos estándares de seguridad y privacidad. El gobierno como plataforma, como una nueva forma holística de construir servicios públicos digitales, debe garantizar la interoperabilidad en todos los niveles de la administración.

Así, con este punto se quiere conseguir que, para 2030, todos los servicios públicos clave sean accesibles en línea, que los ciudadanos puedan tener acceso a su historial médico electrónico y que el 80% de estos ciudadanos ya estén utilizando una solución de identificación electrónica.

PILARES DIGITALES PARA LA EUROPA DE 2030

La estrategia de digitalización europea se apoya en tres pilares básicos como garantía de que los países miembros de la Unión Europea van a aprovechar la oportunidad otorgando a los ciudadanos, las empresas y las Administraciones Públicas el control de la Transformación Digital.

El primero de estos pilares básicos es poner la tecnología al servicio de las personas, para lo que las autoridades de la Unión invertirán en competencias digitales para todos los ciudadanos y para los trabajadores del sector TIC, protegerán a las personas contra las amenazas cibernéticas, garantizarán que la IA se desarrollará de manera respetuosa con los derechos de las personas y sea confiable, acelerará el despliegue de la banda ancha ultrarrápida para hogares, escuelas y hospitales, y ampliará la capacidad de supercomputación de Europa para desarrollar soluciones innovadoras en Sanidad, Transportes y Medio Ambiente. El segundo de estos elementos básicos apunta a lo que denominan una economía digital justa y competitiva que, en opinión de los reguladores y legisladores europeos, posibilitará el acceso a la financiación y la expansión de una comunidad dinámica de empresas emergentes y pequeñas empresas innovadoras y de rápido crecimiento, reforzará la responsabilidad de las plataformas online al proponer una Ley de servicios digitales, clarificará las normas sobre servicios on-line, garantizará que las normas sean adecuadas para la economía digital, velará por unas condiciones justas de competencia y mejorará el acceso a datos de alta calidad al tiempo que se garantiza la protección de los datos personales y sensibles. Por último, la UE persigue una sociedad abierta, democrática y sostenible, o, lo que es lo mismo, que emplee la tecnología para ayudar a la Unión a ser climáticamente neutra antes de 2050, que reduzca las emisiones de carbono del sector digital, que de a los ciudadanos mayor control y protección de sus datos, que cree un espacio europeo de datos de salud que favorezca la investigación, el diagnóstico y el tratamiento específicos, y que luche contra la desinformación online y fomente la diversidad y fiabilidad de los contenidos en los medios de comunicación.

LA COMISIÓN EUROPEA HA PROPUESTO EN SU BRÚJULA DIGITAL 2030 LOS PASOS NECESARIOS PARA HACER REALIDAD LAS OBJETIVOS DIGITALES DE LA UNIÓN EUROPEA AL FINAL DE ESTA DÉCADA

POTENTES INVERSIONES PARA AVANZAR EN LA DÉCADA DIGITAL

Para hacer realidad la Década Digital, la Comisión Europea ha hecho propias tres iniciativas del programa Europa Digital, definido para reforzar la soberanía tecnológica europea y aportar soluciones digitales al mercado, que contarán con una financiación de 1.980 millones de euros.

La primera, dotada con 1.380 millones de euros, se centrará en Inteligencia Artificial, la nube y los espacios de datos, la infraestructura de comunicación cuántica, las competencias digitales avanzadas y el amplio uso de las tecnologías digitales en toda la economía y la sociedad, hasta finales de 2022. La segunda de las iniciativas se centra en el ámbito de la ciberseguridad, con un presupuesto de 269 millones de euros hasta finales de 2022, y la tercera, en la creación y explotación de la red

de centros europeos de innovación digital, con un presupuesto de 329 millones de euros hasta finales de 2023.

Para Margrethe Vestager, Vicepresidenta Ejecutiva responsable de Una Europa Adaptada a la Era Digital, "con el programa Europa Digital creamos infraestructuras digitales seguras y sostenibles. También facilitamos a las empresas tener un mejor acceso a los datos o utilizar soluciones impulsadas por la IA. El programa también invierte para velar por que los europeos puedan tener las capacidades necesarias para participar de forma activa en el mercado laboral. Se trata de que todos en Europa puedan beneficiarse de soluciones tecnológicas adaptadas al mercado". ■

SI TE HA GUSTADO ESTA REVISTA, COMPÁRTELA

CONTENIDO RELACIONADO

Brújula Digital 2030

La Comisión invertirá casi 2.000 millones de euros para avanzar en la transición digital

¿Qué es la Brújula Digital de la Comisión Europea?

La Brújula Digital de Europa

La Década Digital de Europa

España en el Informe DESI 2021

Comunicación de la Comisión al Parlamento Europeo de la Brújula Digital

Configurar el futuro digital de Europa

Informe Iria

Informe sobre Gobierno Electrónico 2021 de la Comisión Europea

Programa Europa Digital

PRIMEROS PASOS DE LA COMISIÓN

Para ir avanzando para la consecución de estos ambiciosos objetivos, la Comisión Europea va a facilitar la creación de proyectos plurinacionales que combinen inversiones con cargo al presupuesto de la UE, los estados miembros y la industria, y aprovechen el Mecanismo de Recuperación y Resiliencia y otros fondos de la UE.

Entre estos destaca la creación de una infraestructura paneuropea interconectada de tratamiento de datos; el diseño y despliegue de la próxima generación de procesadores fiables de baja potencia; y administraciones públicas conectadas.

Por otra parte, y con el objetivo de asegurar que los valores y derechos de la Unión Europea se mantienen inalterables en el espacio digital, la Comisión Europea ha propuesto la definición de un marco de principios digitales como, por ejemplo, el acceso universal a una conectividad de alta calidad, a suficientes competencias digitales, a servicios públicos y a servicios en línea equitativos y no discriminatorios.

Según el comisario de Mercado Interior, Thierry Breton, "Europa tiene que velar por que sus ciudadanos y empresas tengan acceso a un surtido de tecnologías punteras que mejoren su vida y sean más seguras e incluso más ecológicas, siempre que también tengan las capacidades necesarias para utilizarlas. En el mundo posterior a la pandemia, es así como configuraremos juntos una Europa resiliente y digitalmente soberana. Ésta es la Década Digital de Europa".

ADMINISTRACIÓN PÚBLICA: AFRONTANDO LA DÉCADA DIGITAL

LA UNIÓN EUROPEA TIENE EN MENTE SEGUIR PROFUNDIZANDO EN LA TRANSFORMACIÓN DE LOS NEGOCIOS E INSTITUCIONES, CON EL OBJETIVO DE DESARROLLAR UNA ECONOMÍA Y UNA SOCIEDAD MÁS DIGITALES, Y QUE OFREZCAN NUEVAS OPORTUNIDADES A UNOS CIUDADANOS QUE DEBERÍAN CONTAR LAS HABILIDADES NECESARIAS PARA APROVECHARLAS.

Europa quiere capacitar a las empresas y las personas para un futuro digital sostenible, más próspero y centrado en el ser humano y, con este objetivo, el pasado 9 de marzo la Comisión Europea presentó una visión y unas vías para la transformación digital de Europa de ahora a 2030. Esta Década Digital de la UE se estructura en planes y objetivos en cuatro ámbitos:

- **Infraestructuras digitales seguras y sostenibles,** con el foco puesto en la conectividad, los semiconductores, los datos en la nube y en el Edge, la seguridad, y la capacidad de supercomputación de la Unión.
- **Digitalización de los servicios públicos,** con la idea de alcanzar la disponibilidad en línea del 100% de los servicios públicos clave, así como avances en salud electrónica e identidad digital.
- **Transformación Digital de las empresas,** con las miras puestas en la innovación y los usuarios.
- **Capacitación,** pensando tanto en el incremento de especialistas TIC en el territorio europeo, con especial énfasis en reducir la brecha de género, como en las habilidades digitales del resto de los ciudadanos.

Por este motivo, el pasado 24 de noviembre, celebramos un nuevo Foro IT User que, bajo el título "Administración pública: afrontando la década digital", abordó las oportunidades que ofrecen estos cuatro puntos cardinales para el desarrollo de un sector público innovador y digital en nuestro país. Para este evento contamos con el patrocinio de Cisco, Dynatrace, Salesforce, Blueprism, F5, MicroStrategy, Veeam, y Proofpoint, así como con la participación de nuestros socios estratégicos ASTIC y el Foro de Colaboración Público-Privada.■

Si quieres repasar lo que pasó en este Foro IT User, clica en la imagen

“LA DIGITALIZACIÓN ES CLAVE PARA LA MODERNIZACIÓN DEL TEJIDO PRODUCTIVO DEL PAÍS, Y PARA ESO NECESITAMOS LA IMPLICACIÓN DE OTROS”

SALVADOR ESTEVAN, DIRECTOR GENERAL DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

El rol de la Administración Pública en la modernización del país fue el hilo conductor de la entrevista con Salvador Estevan, Director General de Digitalización e Inteligencia Artificial, que sirvió como punto de partida del Foro IT User: Administración pública, afrontando la década digital. Tal y como comentaba este responsable, “España tiene todo a favor para convertirse en una referencia mundial en una transformación exitosa y con impacto en la realidad social del país. Contamos con el talento, las infraestructuras y el firme compromiso de impulsar la Transformación Digital como un proyecto estratégico, un proceso que ya está en marcha y que tenemos que asumir como política de Estado. La Transformación Digital será fundamental para dotarnos de competitividad y de los recursos para afrontar los retos del futuro. Para ello, contamos con una hoja de ruta clara y consensuada, la Agenda España

Los planes del Gobierno en materia de digitalización y su alineamiento con los de la Comisión Europea, fueron el eje central de la entrevista a Salvador Estevan (Clica en la imagen para ver el vídeo).

Digital 2025, y cuatro planes transversales que ya están en fase de despegue: la Estrategia Nacional de Inteligencia Artificial, el Plan Nacional de Competencias Digitales, el Plan de Digitalización de PYMES, y el Plan de Digitalización de la Administración Pública".

"Tenemos los recursos", continuaba, "que vienen a ser un tercio de los fondos del Mecanismo de Recuperación y Resiliencia que ya estamos ejecutando. Y estamos poniendo en marcha una serie de medidas, en el ámbito del impulso a las nuevas tecnologías, como la Convocatoria de Emisiones de I+D en Inteligencia Artificial, dotada con 50 millones de euros, que esperamos lanzar a principios de diciembre; se ha publicado y cerrado ya la Convocatoria de Cadenas de Valor en IA; Manifestaciones de Interés en el ámbito de la Computación Cuántica, la neurotecnología y Algoritmos Verdes. Relacionado con el emprendimiento, hemos sacado adelante la línea de financiación Emprendedoras Digitales ENISA, con un presupuesto de 51 millones de euros para los próximos tres años, y estamos trabajando en la ley de startups, con el firme objetivo de facilitar y acelerar la puesta en marcha de proyectos de emprendimiento digital innovador y la atracción de talento".

"Muy importantes", añadía, "son las medidas relacionadas con la digitalización de las PYMES. Estamos en plena fase de despliegue de la red de oficinas Acelera PYME, pero, también, vamos a lanzar un programa de más de 3.000 millones de euros para digitalizar estas empresas, sobre todo las de menos de 50 trabajadores, incluyendo autónomos".

"ESPAÑA TIENE TODO A FAVOR PARA CONVERTIRSE EN UNA REFERENCIA MUNDIAL EN UNA TRANSFORMACIÓN EXITOSA Y CON IMPACTO EN LA REALIDAD SOCIAL DEL PAÍS"

Adicionalmente, "consideramos que contar con los conocimientos adecuados para afrontar la digitalización de la economía productiva del país es fundamental, porque las personas, el talento, tienen que estar en el centro del cambio, y es fundamental impulsar las competencias digitales. Para ello, hemos lanzado el Plan Nacional de Competencias Digitales, que completa una inversión de más de 3.750 millones de euros. Finalmente, hay otras iniciativas que ya hemos lanzado o que están en proceso, como la Carta de Derechos Digitales, enfocada a garantizar los derechos y valores democráticos también en el mundo digital; Manifestaciones de Interés relacionadas con la Inteligencia Artificial, Ciberseguridad, PYMES o Gaia-X. De hecho, estamos trabajando en la creación de un hub de Gaia-X. Y, por último, cabe destacar el Fondo Next Tech, una iniciativa público-privada que movilizará 4.000 millones de euros que serán invertidos en empresas innovadoras en sus primeras etapas de crecimiento, particularmente en el ámbito del Deep Tech".

ESTRATEGIA NACIONAL DE INTELIGENCIA ARTIFICIAL

Tal y como explicaba Salvador Estevan, "España está inmersa en un profundo y ambicioso plan de transformación digital, una apuesta, como país, por lo digital, como un elemento clave para la recuperación económica y social. En la modernización de este tejido productivo, la Inteligencia Artificial va a tener un papel absolutamente decisivo. Es un reto que precisa poner todo su potencial al servicio de una transformación digital, inteligente y transversal. Con este objetivo, estamos impulsando proyectos dentro de la Estrategia Nacional de Inteligencia Artificial (ENIA), uno de los ejes principales de la Agenda España Digital 2025, además de ser un elemento esencial de nuestro plan de Recuperación, Transformación y Resiliencia. A través de los proyectos contemplados en la ENIA, se van a movilizar 600 millones de euros hasta 2023, una inversión sin precedentes a la que podemos unir otras iniciativas de colaboración público-privada como el mencionado Fondo Next Tech de 4.000 millones de euros. Los principales objetivos de la ENIA son fomentar la investigación pública en excelencia en IA, promover sinergias de investigación entre las universidades y centros de investigación, así

como empresas y Administración, crear plataformas de colaboración público-privada, promover sinergias entre la investigación en IA y otras tecnología de alto impacto, o explorar mecanismos alternativos de investigación".

Respecto a las iniciativas, "hemos lanzado la Convocatoria de Emisiones de I+D, una respuesta a la medida 7 del eje 1 de la ENIA, y objetivo es la financiación de proyectos de investigación industrial o desarrollo experimental en materia de IA para abordar grandes desafíos en sectores concretos de especial relevancia y alta capacidad de disrupción e impacto, con un presupuesto de 50 millones, y apuntando a sectores como el Agroalimentario, Salud, Medio Ambiente, Empleo y Energía del siglo XXI. Por otro lado, queremos acercar la IA al día a día. Por tanto, uno de los aspectos donde la ENIA da un paso al frente es en la integración de la IA en la cadena de valor de las empresas y los negocios, y la Convocatoria de Cadena de Valor de Red.es tiene un presupuesto de 105 millones, y ya hemos recibido más de 1.200 solicitudes, más del 75% provenientes de PYMES. Además, la IA tiene su aplicación en la Administración Digital.

COLABORACIÓN PÚBLICO-PRIVADA

En palabras de Salvador Estevan, "la digitalización es clave para la modernización del tejido productivo del país, y para eso necesitamos la implicación de otros. En 2020 elaboramos el diagnóstico de la situación y diseñamos la hoja de ruta, y en 2021 hemos puesto en marcha proyectos con este objetivo y, para ello, la colaboración público-privada es esencial. Hay ejemplos como el Plan de Digitalización de las PYMES, que cuenta con una inversión pública de más de 4.600 millones de euros; el ámbito de Digitalización Básica de las PYMES, con más de 3.000 millones o el Kit Digital, que vamos a lanzar, en su primera fase, a final de año. Pero, también, tenemos el Apoyo a la Gestión del Cambio, con la formación de directivos o expertos en Transformación Digital para PYMES; Innovación Disruptiva y Emprendimiento Digital, con más de 400 millones para el apoyo a centros de innovación digital o agrupaciones empresariales innovadoras; o la digitalización en sectores clave, como el Comercio, Turismo e Industria, con más de 400 millones de euros. Adicionalmente, una línea horizontal y fundamental en el desarrollo de la digitalización es la Ciberseguridad.

PUNTOS DE MEJORA

En este punto, destacaba Salvador Estevan que el objetivo es "avanzar hacia una Administración del siglo XXI, con servicios digitales como los actuales, pero más orientada a la multicanalidad, más proactiva, más accesible y adaptada a las necesidades de los distintos colectivos. Hay varios ejes de trabajo. Primero, la transformación de la Administración General del Estado a nivel transversal, con una asignación de casi 1.000 millones de euros, con soluciones orientadas a mejorar la movilidad de los servicios públicos, mejorar los accesos de la ciudadanía a los servicios con un nuevo modelo de identidad digital más ágil y usable, hacer más eficientes y centrados en el dato los servicios públicos con medidas orientadas al impulso de tecnologías como RPA, IA o la analítica y gestión del dato, y también en infraestructuras, con la creación de un ecosistema flexible y robusto para dar respuesta a las necesidades actuales y futuras. Todo ello, sin dejar de lado la Ciberseguridad. Segundo, tenemos que poner el foco en el impulso de proyectos de alto impacto, con una inversión de más de 1.200 millones, con el foco en sectores clave como Sanidad, Justicia, Empleo, Seguridad Social o el ámbito consular. Por último, para acompasar la velocidad de transformación de las administraciones, dirigido a comunidades autónomas y entidades locales. Por último, y en paralelo a este plan, hay que recordar el Plan de Formación en Capacitaciones Digitales de la Administración Pública, que será fundamental para la absorción de las bondades de la digitalización y su capilaridad". ■

CONTENIDO RELACIONADO

Foro IT User: Administración pública, afrontando la década digital

INFRAESTRUCTURAS DIGITALES SEGURAS Y SOSTENIBLES

Participaron en esta mesa redonda el Ministerio de Asuntos Económicos y Transformación Digital, la Comisión Europea, la Secretaría de Fondos Europeos del Ministerio de Hacienda y el Ayuntamiento de Alcobendas (Clica en la imagen para ver el vídeo).

LA CONECTIVIDAD, LA CAPACIDAD PARA ANALIZAR GRANDES CANTIDADES DE DATOS Y LA SEGURIDAD SON ELEMENTOS FACILITADORES PARA LA GENERACIÓN DE SERVICIOS DIGITALES ROBUSTOS Y COMPETITIVOS. UNO DE LOS PUNTOS CLAVE DE LA COMISIÓN EUROPEA PARA LA AGENDA DE 2030 ESTÁ VINCULADO A LA CREACIÓN DE INFRAESTRUCTURAS SEGURAS Y SOSTENIBLES. ESTO, APLICADO A LA MODERNIZACIÓN DEL SECTOR PÚBLICO, IMPLICA UN DESPLIEGUE DE TECNOLOGÍA QUE PERMITA A LOS TRABAJADORES DESEMPEÑAR SU FUNCIÓN DE UNA MANERA ÁGIL Y CREAR, ADEMÁS, SERVICIOS PARA LOS CIUDADANOS ALREDEDOR DE LA CONECTIVIDAD.

La primera mesa redonda del Foro IT User: Administración pública, afrontando la década digital, estuvo centrada en cómo conseguir infraestructuras digitales seguras y sostenibles en el entorno público. Contó con la participación de José Antonio Eusamio, Vocal Asesor en el Ministerio de

Asuntos Económicos y Transformación Digital; Luis Miguel Vega, Jefe de Área en la Comisión Europea; Sergio Caballero, Director TIC del Ayuntamiento de Alcobendas; Jorge Navas, CIO de la Secretaría General de Fondos Europeos del Ministerio de Hacienda; y Xavier Massa, Director de Sector Público de Cisco España, en calidad de co-moderador.

Y el primer tema sobre la mesa es cómo se había dotado a estas instituciones de una infraestructura de TI que siga estos principios. Para José Antonio Eusamio, "desde la Secretaría General de Administración Digital, completamente alineados con los planes puestos en marcha con el Gobierno, se le ha dado mucha importancia a los servicios digitales accesibles y eficientes, como parte de los objetivos estratégicos; a una Administración guiada por los datos, para lo que se está diseñando una nueva plataforma para dar servicio a nuestra organización como al resto de administraciones, porque es un elemento fundamental; y el acceso al resto de tecnologías emergentes. Dentro del Eje 1 del Plan de Transformación, Recuperación y Resiliencia, existen una serie de medidas de actuación, unas orientadas a la ciudadanía, como la primera de ellas, la App Factory, un servicio que pretende facilitar el desarrollo de aplicaciones móviles para que el ciudadano tenga accesible la Administración en aquel dispositivo que es más fácil para él,

"LA SEGURIDAD Y LA CALIDAD SON DOS ELEMENTOS ESENCIALES, Y HAY QUE BUSCAR EL EQUILIBRIO A LA HORA DE PROPORCIONAR SERVICIOS, HACIÉNDOLOS SEGUROS, PERO SIN BLOQUEARLOS"

JOSÉ ANTONIO EUSAMIO (M. ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL)

el móvil. Se trata de un salto cualitativo muy importante, porque muchos de los trámites de la Administración Electrónica tradicional no habían terminado de arraigar. También tenemos otras medidas, como la definición e implementación de un data lake accesible para todas las Administraciones Públicas que pensamos que va a marcar la diferencia en la prestación de un servicio eficiente y de calidad al ciudadano, basado en el valor que aporta el dato y la información. En el resto de las medidas también se está haciendo un gran esfuerzo, como en las relacionadas con la seguridad, para aportar valor al ciudadano".

En palabras de Luis Miguel Vega, "la Década Digital es una iniciativa de la Comisión Europea, presentada hace un año, que pretende una verdadera Transformación Digital de la economía y la sociedad europea para el año 2030. Dentro de ella, hay un elemento clave, las infraestructuras seguras y sostenibles. Hay una idea fundamental en nuestras acciones, promover la conectividad entre territorios, posibilitar que todos los ciudadanos cuenten con conexiones de hasta 1Gbps y 5G. España, por ejemplo, ha sido uno de los grandes líderes de conectividad y durante el confinamiento no ha habido problemas con el servicio, los operadores han seguido ofreciéndolo de forma normal, incluso con el incremento de la demanda. En el caso de 5G, los servicios que se prestan son posteriores a la propia infraestructura, de ahí que tengamos que dotarnos de ella en primer lugar. Por último, hablando de las infraestructuras digitales, estamos afrontando graves problemas con la disponibilidad de equipos y dispositivos, y algo que queremos potenciar es que Europa sea cada vez más autónoma y tengamos una verdadera soberanía digital".

Para Sergio Caballero, en el Ayuntamiento de Alcobendas "desde 2012 hemos adoptado una estrategia cloud first, siempre que supusiera

para la organización unas ventas en términos económicos y de eficiencia operativa. Con los pasos que hemos ido dando, estábamos preparándonos para el momento al que estamos llegando hoy, buscábamos la necesidad de industrializar el servicio y controlar los costes, dirigido a establecer una infraestructura que nos permitiera crecer con la organización, capacitándonos para procesar grandes cantidades de datos bajo un modelo híbrido. Es un cambio de paradigma que se inició con la transformación de los servicios públicos en servicios digitales y, en el caso de algunas ciudades, en lo que se denominan Smart Cities. Esto requería un cambio de enfoque, que convivían con factores de riesgo, como la baja capacidad de inversión, por lo que recurrimos a diferentes fondos provenientes de la Unión Europea. También realizamos inversiones en seguridad, con un plan de mejora desde 2016, y obteniendo la certificación del Esquema Nacional de Seguridad en el año 2018 con el nivel medio, y haciendo la recertificación en 2020. Hemos generado nuevos puestos de trabajo en el área TI dada la necesidad de ir creciendo en todos los servicios. Asimismo, hemos invertido en la modernización de los sistemas de información, de cara a moverlos a un modelo gestionado en multi cloud, permitiéndonos mejorar la obsolescencia y mejorando el marco de cumplimiento normativo. Existía el problema

"ESTAMOS AFRONTANDO GRAVES PROBLEMAS CON LA DISPONIBILIDAD DE EQUIPOS Y DISPOSITIVOS, Y ALGO QUE QUEREMOS POTENCIAR ES QUE EUROPA SEA CADA VEZ MÁS AUTÓNOMA Y TENGAMOS UNA VERDADERA SOBERANÍA DIGITAL"

LUIS MIGUEL VEGA (COMISIÓN EUROPEA)

de una plantilla TIC escasa o dimensionada para otra época, de ahí que hayamos evolucionado de un modelo gestionado por nosotros a otro en el que nos apoyamos en proveedores, lo que hace que necesitemos nuevos perfiles, más centrados en la gestión, que nos permitan acelerar el cambio".

Finalizaba esta primera ronda de valoraciones Jorge Navas, del Ministerio de Hacienda, indicando que "en nuestro caso, todas las infraestructuras se llevan desde la Oficina de Informática Presupuestaria. Desde hace años, sabemos que las infraestructuras son vitales en la Transformación Digital, porque de nada sirve tener unas apps muy buenas si los usuarios no se pueden conectar y el soporte es malo. De ahí que la apuesta desde hace tiempo haya sido disponer de unas infraestructuras adecuadas, tanto para los usuarios internos como para los ciudadanos. Se ha montado un ecosistema de aplicaciones con un sistema de usuarios registrados que hace necesaria una identificación segura con diferentes niveles, según la aplicación y el servicio. Todo está unificado con una capa de presentación basada en navegadores web, y las identificaciones internas o de usuarios externos son independientes. Los puestos de trabajo internos están pensados también para la movilidad. Los cargos medios y altos cuentan con portátiles y estaciones de trabajo con 4G. Todos los edificios tienen WiFi y contamos con utilidades compartidas como la Impresión Segura. También ha sido importante la inversión en disponibilidad, por lo que toda la infraestructura está activa en dos centros de datos, algo a lo que obliga el Esquema Nacional de Seguridad, entre otras cosas".

TRABAJAR EN REMOTO ES YA UNA REALIDAD

Comentaba Xavier Massa que el teletrabajo al que nos hemos visto forzados en esta pandemia, y que se mantiene en muchas organiza-

ciones, ha supuesto un reto importante, sobre todo en las Administraciones Públicas. Pero ¿qué enseñanzas hemos sacado? ¿Qué se va a mantener de cara a futuro? Para Luis Miguel Vega (Comisión Europea), "es sorprendente la velocidad con la que se ha hecho, y eso ha sido gracias a la colaboración público/privada. Existía una tecnología que se ha podido implantar, una innovación que nos ha mostrado las ventajas del teletrabajo, las herramientas colaborativas, de las infraestructuras... En la Comisión, tenemos una inmensa actividad legislativa, un altísimo número de reuniones internacionales plenarias, tanto con estados miembros como con la industria y las asociaciones, y la maquinaria ha seguido funcionando. Hemos seguido trabajando y lo hemos hecho gracias al teletrabajo, que parecía algo lejano para las Administraciones Públicas, pero la tecnología estaba y la pandemia ha sido un acicate para implantar algo que es muy necesario. Nosotros estamos apostando por el teletrabajo como elemento de futuro. Estamos haciendo una racionalización de edificios y de los consumos energéticos y es una apuesta clara de futuro".

Según explicaba Sergio Caballero (Ayto. Alcobendas), "fue un reto profesional y personal para todos, tanto para los equipos de TI como para los trabajadores. Antes su uso era escaso, y la infraestructura implementada tradicionalmente no fomentaba su utilización. Pero

"DESDE 2012 HEMOS ADOPTADO UNA ESTRATEGIA CLOUD FIRST, SIEMPRE QUE SUPUSIERA PARA LA ORGANIZACIÓN UNAS VENTAS EN TÉRMINOS ECONÓMICOS Y DE EFICIENCIA OPERATIVA"

SERGIO CABALLERO (AYTO. ALCOBENDAS, MADRID)

desde 2014, la planificación nos había llevado a buscar sistemas de acceso remoto adecuados y acordes con las medidas de seguridad necesarias, bajo una política de bajo mantenimiento y reducido coste. Tras varias alternativas sin éxito, en 2019 desarrollamos una solución de escritorio remoto en cloud con un fabricante y conseguimos replicar escritorios con las compatibles con las características de rápido despliegue, con el menor coste posible y con gran flexibilidad, bajo un modelo de pago por uso predecible. En marzo de 2020 ya teníamos probado el entorno y, en pocos días, fuimos capaces de dotar de las herramientas a todos los empleados encargados de los servicios esenciales de nuestra ciudad. En pocos días tuvimos a todo el personal teletrabajando y usando la plataforma y otras soluciones de colaboración. El verdadero reto fue empezar a trabajar con soluciones existentes que no habían recibido la atención necesaria. Nos llevó de tres a cuatro semanas, formar en competencias digitales a todo el personal. Otro problema fueron los plazos de contratación y presupuestación, incompatibles con el Sector Público. Actualmente, nuestra política pasa por un modelo mixto de escritorios virtuales para aquellos puestos que no requieren un puesto de trabajo in-situ con VPN. Esto ha supuesto un claro impulso en la Administración Pública, pero, para ello, se necesita un liderazgo claro, una dotación de recursos para abordar la convergencia digital, una adaptación normativa, una mayor formación en competencias digitales entre el personal y la adopción de una nueva forma de trabajar por objetivos".

En el caso de Jorge Navas (Ministerio de Hacienda), "el inicio de la pandemia lo viví en otro ministerio, donde ya existía un sistema seguro con portátiles repartidos entre altos cargos con un acceso securizado por VPN, pero estos altos cargos no eran conscientes de que se podía trabajar a distancia con esos equipos, y solo accedían, en algunos casos, al correo electró-

nico. La pandemia ha cambiado esto. Como la infraestructura estaba, solo hubo que cambiar algunos equipos, incorporar formación y modificar algunos procedimientos, incluyendo la posibilidad de trabajar con los equipos de los propios funcionarios. Todo funcionó bastante bien. Se adquirió la tecnología necesaria, y fue un cambio radical. Con la llegada de Filomena, no hubo ningún problema, con lo que podemos decir que el cambio de mentalidad ya se ha producido. Por parte de los usuarios de TI, esto nunca ha sido un problema, el uso estaba asumido, pero el personal no TIC no estaba preparado. En una segunda fase, estaba no el trabajar a distancia, sino cómo trabajar a distancia, y ahora estamos en una situación mucho mejor que antes. Por último, uno de los aspectos a los que los usuarios son reacios es la colaboración con documentos en la nube. Hace falta evangelizar y que aprendan a trabajar con documentos compartidos en línea".

Según José Antonio Eusamio (Ministerio de Asuntos Económicos y Transformación Digital), "en 2006 ya se hizo un programa piloto de teletrabajo y no se cubrieron todas las plazas. Desde entonces, la organización se ha ido dotando de infraestructura, pero lo cierto es que faltaba un cambio en el modelo de organización. La tecnología y las infraestructuras han mejorado y estaban ahí cuando se han necesitado, pero hemos necesitado un empujón

"DEBERÍAMOS TRABAJAR EN LA MEJORA DE LA MOVILIDAD DE LAS APLICACIONES, ALGO QUE ES UNA REALIDAD EN LAS EMPRESAS PRIVADAS. Y NO SOLO PARA INFORMAR, SINO PARA REALIZAR TRÁMITES"

JORGE NAVAS (M. HACIENDA)

para salir de nuestra zona de confort. Pero la realidad es que nos hemos adaptado, hemos seguido trabajando. Es cierto que, al principio, cada usuario tuvo que usar sus propios dispositivos, pero con voluntad es posible. Y es una lección que tenemos que sacar, pero el teletrabajo tiene sus retos y hay que gestionar el espacio compartido, por ejemplo. No parece razonable que renunciemos a las cosas buenas del teletrabajo, pero hay que buscar un punto de equilibrio para conciliar la vida personal con la profesional, y la prestación de un servicio on-site y en remoto. Estamos en un punto de inflexión importante y hay que estar preparados para responder de la forma más eficiente, pero, en líneas generales, creo que la Administración ha respondido en este caso".

DEFINIR SERVICIOS SEGUROS PARA EL CIUDADANO

Otro tema de debate en esta mesa redonda fue la prestación de servicios a los ciudadanos con la seguridad adecuada, sobre todo en una realidad en la que se ha diluido el perímetro, apuntaba Xavier Massa, de Cisco. ¿Cómo se está reforzando esta seguridad? Según explicaba Sergio Caballero, "éramos conscientes de la realidad, y decidimos ofrecer acceso cloud securizado a los servicios para que nuestro legacy no fuera un vector de entrada de posibles ataques. Hemos desplegados sistemas de protección contra código dañino, en equipo de usuarios y en servidores, mediante clientes ligeros, además de antivirus reforzados con soluciones EDR y de Ataques Zero Day. Además, hicimos obligatorio el doble factor de autenticación para todos los accesos desde fuera de la institución, y estamos implementando un sistema de doble barrera perimetral. Arrancamos hacking éticos en las zonas más vulnerables para permitir su solución en caso necesario. Es muy importante, asimismo, la formación a todo el personal en los tres niveles y, sobre todo, concienciación continua. Realizamos ataques de

phishing simulados y, pese a las labores de concienciación, muchos usuarios siguen cayendo. Es importante seguir trabajando. También hemos desplegado sondas de detección y monitorización, integrándolas en un sistema SIEM, y en previsión tenemos, además del sistema de alerta temprana para los sistemas industriales, sistemas Scada para el control energético, integración de los endpoints de sistemas críticos en este SIEM. Pero, en todo caso, todo esto no podemos hacerlo a nivel interno, y necesitamos empresas externas que estén en continua adquisición de conocimientos y que se integre con nuestros equipos".

En palabras de Jorge Navas, "el perímetro no existe y hay que actuar como si el enemigo estuviera dentro. Hay que monitorizar constantemente, porque no puedes dar por seguro que nada esté libre de ataques. Esto es lo que estamos haciendo y tenemos la vista puesta en la entrada en funcionamiento del centro de servicio gestionado de la AGE. Desde el punto de vista de las redes internas, hay que fortalecer las conexiones con autenticación de dispositivo y otros mecanismos de seguridad. Con la conexión de cualquier dispositivos, chequeamos las políticas de seguridad y, si no, no permitimos el acceso hasta que se cumplan. En los dispositivos bastionados, solo tiene permisos de instalación el equipo de soporte. Las VPN están en el último estado de actualización, y hacemos auditorías instantes para conocer la realidad de la situación. Por último, la concienciación de los usuarios, que es fundamental, también, incluso, sobre las medidas más impopulares de seguridad".

Según José Antonio Eusamio, "nuestra realidad es similar a la de mis contertulios, pero hay dos elementos adicionales que son fundamentales. Por un lado, la seguridad y la calidad son dos elementos esenciales, y hay que buscar el equilibrio a la hora de proporcionar servicios, haciéndolos seguros, pero sin bloquearlos. ¿Tenemos capacidad para ser eficientes a la vez que seguros? La respuesta es sí. Por otro lado, estamos en un contexto donde los riesgos crecen, no solo por la pandemia, y van a seguir creciendo, y debemos adaptarnos a ello".

Concluía este apartado de seguridad Luis Miguel Vega, afirmando que "las medidas organizativas son muy parecidas, pero desde la Comisión Europea estamos planteando una serie de medidas políticas en el ámbito de la seguridad. Las cifras de ataques crecen, y hemos planteado un paquete de políticas públicas en relación con la seguridad. Hasta ahora, teníamos un marco legal en ciberseguridad un tanto heterogéneo y complejo, que se ha ido desarrollando según surgían las necesidades. A finales de 2020, anunciamos la Estrategia Europea de Ciberseguridad, que va a permitir abordar este tema de forma global en toda la economía, porque no afecta solo a las Administraciones Públicas. Destacan tres medidas, el Reglamento de Inteligencia Artificial, que viene a regular las medidas de ciberseguridad para tener una IA segura; el Acta Europea de Ciber-resiliencia, una normativa horizontal para que los productos y servicios sean seguros desde el principio; y el Reglamento que va a obligar

a los fabricantes de dispositivos inalámbricos instalar medidas de ciberseguridad de fábrica y certificarse si quieren poner sus productos en el mercado europeo".

TENDENCIAS TECNOLÓGICAS DE MAYOR IMPACTO EN LA ADMINISTRACIÓN PÚBLICA

Vista la realidad actual, nos preguntábamos qué tendencias tecnológicas tendrán, a partir de ahora, mayor impacto de ahora a 2030. En opinión de Jorge Navas, "deberíamos trabajar en la mejora de la movilidad de las aplicaciones, algo que es una realidad en las empresas privadas. Y no solo para informar, sino para realizar trámites. Espero que el DNI electrónico en el móvil sea el impulsor definitivo de la autenticación para mejorar esta movilidad".

En palabras de José Antonio Eusamio, "la Analítica de Negocio y la IA van a cobrar mucho protagonismo por el mejor conocimiento de las organizaciones. Además, necesitamos, para poder ofrecer servicios on-line, que la información que ya tiene la Administración esté disponible para el diseño de formularios que hagan realidad esta prestación de servicios. La tecnología está disponible, pero es necesario un cambio legal para dar validez a estos servicios. No es un cambio tecnológico, sino que se necesita un cambio conceptual para adaptarnos al tiempo en el que estamos".

Añadía Luis Miguel Vega "el factor medioambiental. Europa es pionera en este cambio, y contamos con muchas iniciativas y medidas que tienen su traslación a las infraestructuras. Las Administraciones debemos apostar por infraestructuras sostenibles y de menos consumo energético y concienciar a nuestros usuarios sobre un uso respetuoso con el medioambiente que tenemos que dar a estas infraestructuras".

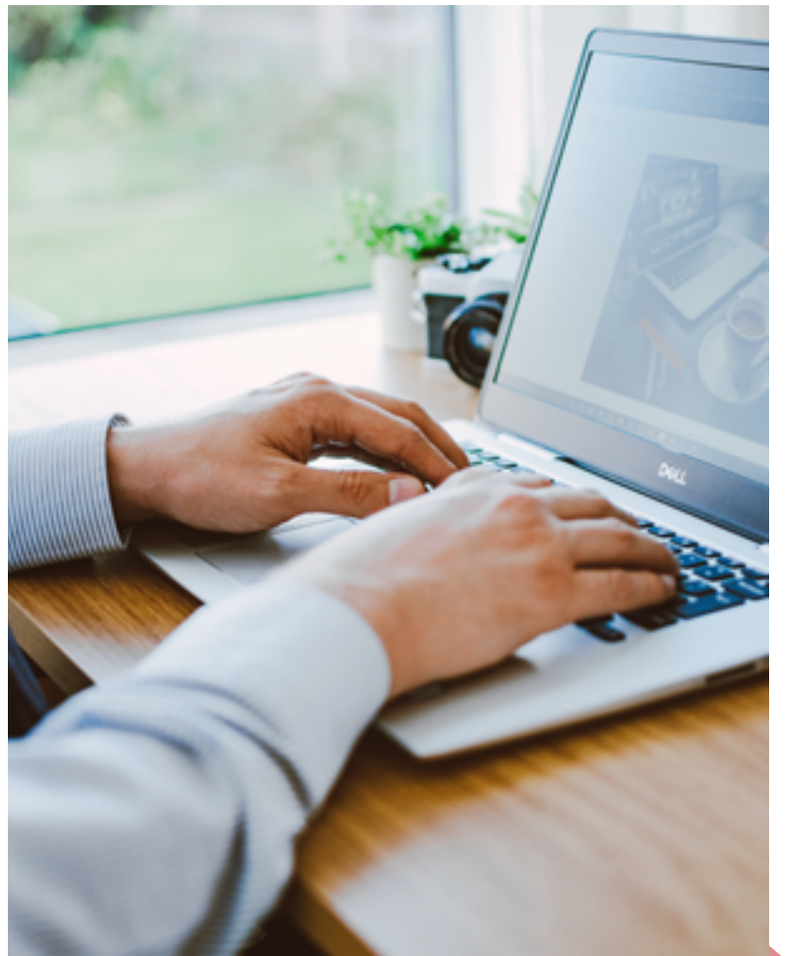
Se mostraba de acuerdo Sergio Caballero con que "lo importante no es solo la tecnología, sino que la Administración esté al servicio de la ciudadanía, aportándole todo lo que necesite. Eso está en nuestra mano, pero requiere cambios estructurales que deben apoyarse en tecnología y personas. Pero, además, hay que cambiar el modelo de gestión de recursos propios y servicios gestionados, con más foco en la gestión que en la operación; la ciberseguridad, que debe ser una prioridad, es imposible asumirla con recursos propios; hay que adoptar servicios en cloud, por la escasez de perfiles y por las inversiones; hay que apostar por puestos de trabajo móviles, seguros e inteligentes; la automatización y los procesos basados en bots o en sistemas conversacionales; y, por último, IoT, 5G y la sensorización, nos llevarán a tendencias como el Edge Computing. Eso sí, sin olvidar que necesitamos un adecuado Gobierno del Dato". ■

#FOROAAPPDIGITAL

CONTENIDO RELACIONADO

Foro IT User: Administración pública, afrontando la década digital

SI TE HA GUSTADO ESTA REVISTA, COMPÁRTELA



El software domina el mundo.
Nosotros nos aseguramos de que funcione.
A la perfección.

Acelera tu transformación
con observabilidad automática e inteligente.

Prueba nuestra plataforma >

dynatrace

@dynatrace

XAVIER MASSA, DIRECTOR DE SECTOR PÚBLICO DE CISCO ESPAÑA

“LA CLAVE PARA CONSTRUIR UNAS ADMINISTRACIONES PÚBLICAS MÁS SEGURAS, SOSTENIBLES Y ROBUSTAS, ES LA TECNOLOGÍA”

LA REALIDAD DE LOS ENTORNOS DE TRABAJO HA CAMBIADO RADICALMENTE, Y ESTO HACE IMPRESCINDIBLE QUE CAMBIEN, PARA PODER AFRONTAR LOS RETOS QUE TENEMOS POR DELANTE, LAS INFRAESTRUCTURAS DIGITALES, QUE TIENEN QUE SER SEGURAS, SOSTENIBLES Y ROBUSTAS, FACILITANDO LA MEJOR EXPERIENCIA DE USO TANTO A TRABAJADORES COMO A LOS CIUDADANOS QUE UTILIZAN LOS SERVICIOS PÚBLICOS.

En su ponencia en el Foro IT User: Administración pública, afrontando la década digital, Xavier Massa, Director de Sector Público de Cisco España, apuntó que “la clave para construir unas Administraciones Públicas más seguras, sostenibles y robustas, es la tecnología. Los cambios que estamos experimentando en nuestra forma de vivir, trabajar y relacionarnos, unos cambios que se están acelerando, nos obligan a utilizar la tecnología. Estos cambios están redefiniendo cómo trabajamos y desarrollamos nuestra actividad, y desde todos los ámbitos de la prestación de servicios a los ciudadanos, hay que adaptarse a estos cambios. La realidad está provocando impactos muy importantes en nuestras vidas en distintos ámbitos. Algunos datos que reflejan esto son el porcentaje de empresas y directivos que piensan que el trabajo no va a ser igual, o el aumento del uso de la tecnología en nuestros hábitos cotidianos, pero estos

ADMINISTRACIONES PÚBLICAS DIGITALES, SEGURAS Y SOSTENIBLES, FUE EL HILO CONDUCTOR DE LA PONENCIA DE XAVIER MASSA (clica en la imagen para ver el vídeo)

cambios están aquí para quedarse, y vamos a ver entornos más híbridos, que no van a ser como los que conocíamos. Hace año y medio, el puesto de trabajo en las administraciones públicas estaba en las oficinas, aunque los organismos estaban preparados para el trabajo en remoto, y el hecho de que la tecnología estuviera lista, permitió afrontar con garantías los efectos de la pandemia con un modelo de teletrabajo. Ahora nos movemos en un escenario híbrido, mixto, entre trabajo presencial y en remoto, que está definiendo cómo hay que evolucionar el puesto de trabajo en las empresas y organismos públicos. Las necesidades son diferentes y debemos adecuar los puestos y espacios de trabajo".

"Hemos aprendido", continuó, "que colaborando con otras personas y organismos somos capaces de hacer más cosas más rápido, y el incremento de esta colaboración está rediseñando cómo debemos definir esos entornos de trabajo, con un número mayor de salas de reuniones y con menos puestos de trabajo individuales. Hay un reto de rediseño de los espacios de trabajo, y las tecnologías deben facilitar este cambio cultural. En este nuevo enfoque intervienen muchos elementos. Van a ser puestos de trabajo más inteligentes, seguros, con acceso a múltiples aplicativos que ya no van a estar en el CPD de nuestra organización, sino en centros de datos de proveedores externos que nos dan ese servicio, con lo que tendremos un entorno multi-cloud que, además, será híbrido. En base a eso, tenemos que orquestar la seguridad y sostenibilidad de este nuevo modelo de trabajo".

CONSTRUCCIÓN DEL NUEVO PUESTO DE TRABAJO

La propuesta de Cisco para este nuevo puesto de trabajo la definía Xavier Massa apuntando que "se trata de una solución que conecte, proteja y automatice la infraestructura digital para servir a los propios empleados y poder dar unos servicios fiables y eficientes a todos los ciudadanos. Nosotros lo hacemos desde un enfoque de arquitectura. No creemos que colocar piezas inconexas sea una solución sostenible en el tiempo. Esta solución debe estar orquestada y formar parte de un diseño donde todo esté integrado y sincronizado, que, de forma innata, incorpore la seguridad y contemple la realidad de los entornos multi-cloud híbridos que tenemos que gestionar".

Cuando habla Xavier Massa de conectar, se refería a "facilitar la conexión de todas las personas, con cualquier dispositivo, a cualquier aplicación y con seguridad de protección de los datos, de forma que garanticemos una experiencia máxima del empleado y el ciudadano a la hora de acceder a los datos y servicios. Desde el punto de vista de la protección, un elemento fundamental, debemos ser capaces de proteger a cualquier usuario con cualquier dispositivo que quiera utilizar. Algunas entidades han usado los dispositivos personales de los usuarios, y eso se tiene que poder hacer de forma segura. Y debemos proteger las conexiones desde cualquier lugar. Ofrecer un acceso seguro y de confianza es crítico para que tengamos éxito en la prestación de los servicios públicos. Sin duda, tiene que ser también una solución que sea capaz de autoprotegerse, de detectar cualquier intento de amenaza y que, automáticamente, dé respuestas de protección frente a estos ataques. Finalmente, creemos que para tener soluciones sostenibles, éstas deben ser capaces de automatizar tanto los procesos de prestación de los servicios tecnológicos como los propios del organismo, facilitando esa transición a un mundo digital, con tecnologías como IA, Blockchain... embebidas en nuestras soluciones. Queremos que estas soluciones, complejas tecnológicamente, sean sencillas de utilizar, además de seguras, confiables y lo más automáticas posibles. ■

CONTENIDO RELACIONADO

Reimagina el Gobierno

Soluciones para ciudades y comunidades

DIGITALIZACIÓN DE LOS SERVICIOS: HACIA UNA OPERACIÓN INTELIGENTE

Participaron en esta mesa redonda el Ministerio de Justicia, la Diputación Provincial de Albacete, el Ministerio de Hacienda, el Ayuntamiento de Málaga, y el Servicio Público de Empleo Estatal. (Clica en la imagen para ver el vídeo).

DE AHORA A 2023, EL OBJETIVO DE LA UNIÓN EUROPEA ES GARANTIZAR QUE LA VIDA DEMOCRÁTICA Y LOS SERVICIOS PÚBLICOS EN LÍNEA SEAN PLENAMENTE ACCESIBLES PARA TODOS, PARA QUE PUEDAN BENEFICIARSE DE UN ENTORNO DIGITAL DE MÁXIMA CALIDAD QUE OFREZCA HERRAMIENTAS Y SERVICIOS FÁCILES DE UTILIZAR, EFICIENTES Y PERSONALIZADOS, Y CON ALTOS NIVELES DE SEGURIDAD Y PRIVACIDAD. PARA SOSTENER ESTOS SERVICIOS, LAS ENTIDADES PÚBLICAS ESTÁN ADOPTANDO PLATAFORMAS TECNOLÓGICAS DIGITALES QUE ESTÁN ACELERANDO SU TRANSFORMACIÓN. EN ESTE CAMINO, DEBEN BUSCARSE, ADEMÁS, ALTERNATIVAS SOSTENIBLES QUE SEAN CAPACES DE REUTILIZAR Y CONCENTRAR RECURSOS PARA LA PRESTACIÓN DE SERVICIOS COMUNES, GANANDO ASÍ EN EFICIENCIA.

MESA REDONDA

La segunda mesa redonda del Foro IT User: Administración pública, afrontando la década digital, puso el foco sobre cómo digitalizar los servicios consiguiendo una operativa inteligente. Contó con la participación de Aitor Cubo, Director General de Transformación Digital del Ministerio de Justicia; José Joaquín de Haro, Jefe del Servicio de Modernización Administrativa y Tecnologías de la Información de la Diputación Provincial de Albacete; Ángel Esteban Paúl, Inspector General del Ministerio de Hacienda; Víctor Solla Bárcena, Director General de Innovación y Digitalización Urbana del Ayuntamiento de Málaga; Angelines Turón, Subdirectora General TIC del Servicio Público de Empleo Estatal. Julia Santos, Directora de Ventas de Dynatrace, co-moderó esta sesión.

En primer lugar, quisimos saber qué rol están jugando las plataformas digitales en la creación de servicios innovadores en las Administraciones Públicas, y qué desafíos conllevan el uso de estas plataformas. Tal y como señaló Aitor Cubo (Ministerio de Justicia), "las plataformas de servicios digitales, tanto internos como externos, son uno de los pilares tecnológicos de la innovación en las Administraciones Públicas. Suponen un desafío porque a veces dependes de otros para proporcionar ese servicio. Pero el modelo en España está bastante asentado. Nosotros tenemos varias, como la de Comunicaciones Electrónicas, que emite

"LAS PLATAFORMAS DE SERVICIOS DIGITALES, TANTO INTERNOS COMO EXTERNOS, SON UNO DE LOS PILARES TECNOLÓGICOS DE LA INNOVACIÓN EN LAS ADMINISTRACIONES PÚBLICAS"

AITOR CUBO (MINISTERIO DE JUSTICIA)

8,2 millones de notificaciones todos los meses. Y nuestra idea es seguir innovando y mejorando el servicio público, incluso integrando estas plataformas. También hay que destacar el papel que han tenido las plataformas en la gestión de la crisis sanitaria que hemos vivido. El nuestro es un servicio fundamental y, sin estas plataformas, hubiera sido muy difícil que la Justicia hubiera funcionado. Más de 8.000 funcionaros trabajan ya con un modelo deslocalizado. Por último, estas plataformas deben ser seguras, y las herramientas del Estado que lo garantizan son indispensables".

Para José Joaquín de Haro (Diputación Provincial de Albacete), "tenemos un proyecto bastante interesante con una plataforma digital que hemos compartido con todos los municipios de nuestra provincia, reutilizando la plataforma para los de más de 20.000 habitantes. Desde 2018 hemos exportado un modelo de compartición de infraestructuras digitales que ya se están usando en 9 comunidades autónomas. Creemos que las plataformas de calidad que contemplen la integración, tanto interna como externa, y abiertas para conectar con el sector privado, son un elemento esencial en el camino de la Transformación Digital. Son necesarias, no son el único elemento, pero sí es un gran avance para un objetivo compartido".

Por su parte, Ángel Esteban Paúl (Ministerio de Hacienda) comentó que "entre nuestros proyectos hay uno que destaca y que consiste en la modificación del entorno informático de los tribunales económico-administrativos y Dirección General de Tributos para apoyarse en el de la Gerencia Estatal de Administraciones Públicas. Es un proyecto que recoge elementos clave para la Transformación Digital, como la mejora del servicio a los ciudadanos, automatización e IA, compartición y reutilización de infraestructuras. Con este proyecto tratamos de dar solución al mayor problema que plantean las infraestructuras: la integración".

Añadió Víctor Solla Bárcena (Ayuntamiento de Málaga) que "hoy por hoy, con el desarrollo de la normativa y la exigencia de los ciudada-

"LAS PLATAFORMAS DE CALIDAD QUE CONTEMPLEN LA INTEGRACIÓN, TANTO INTERNA COMO EXTERNA, Y ABIERTAS PARA CONECTAR CON EL SECTOR PRIVADO, SON UN ELEMENTO ESENCIAL EN EL CAMINO DE LA TRANSFORMACIÓN DIGITAL"

JOSÉ JOAQUÍN DE HARO (DIPUTACIÓN PROVINCIAL DE ALBACETE)

nos, las Administraciones no nos podemos permitir el lujo de no disponer de plataformas que resuelvan nuestros problemas. Cada organización debe tener en cuenta sus particularidades para elegir la mejor plataforma, pero es clave la integración porque son los ciudadanos los que tienen que recibir los mejores servicios. Una plataforma es necesaria, pero no suficiente, y la AGE juega en esto un papel importantísimo en el nivel de administración digital que estamos ofreciendo a los ciudadanos. Pero una plataforma no lo resuelve todo. También es necesario un cambio organizativo, que debe resolverse a la par que la implantación de la plataforma, porque, si no, tendremos una gran herramienta pero veremos reducida su eficacia".

Finalizó esta primera ronda de valoraciones Angelines Turón (Servicio Público de Empleo Estatal) indicando que "son importantes varios aspectos. Primero, el marco de referencia, el Plan de Recuperación, Transformación y Resiliencia, una apuesta muy importante para el proceso de digitalización. Nosotros estamos muy alineados con los objetivos globales y estamos siendo, incluso, pioneros en algunos. Contamos con varias plataformas digitales, como las relacionadas con el puesto de trabajo colaborativo, que han sido imprescindibles durante la época de pandemia para mantener el servicio. Pero hay más, como las herramientas de modelado para la automatización y el diseño de procesos para conseguir una mayor eficiencia y eficacia de los mismos. Pero lo cierto es que se necesitan cambios legales y organizativos, porque estas herramientas no pueden optimizarse con la forma de hacer las cosas actual. Es necesario también un mayor liderazgo en la definición de las necesidades de interoperatibilidad. Y, por último, la evolución de las infraestructuras, don-

"LA NUBE ESTÁ MÁS QUE IMPLANTADA EN LAS ADMINISTRACIONES, ASUMIDA, Y LA ÚNICA DISCUSIÓN QUE NOS QUEDA ES SI DETERMINADOS SERVICIOS Y DATOS DEBEN ESTAR EN UNA NUBE PÚBLICA O PRIVADA"

ÁNGEL ESTEBAN PAÚL (MINISTERIO DE HACIENDA)

de también necesitamos una redefinición, para dar paso a modelos híbridos o de nube pública; los procesos de autenticación y firma, que también deben evolucionar; o las herramientas de mejora de calidad del dato y la IA, que va a necesitar un replanteamiento en las estrategias de desarrollo".

SOSTENIBILIDAD Y EFICIENCIA EN LOS SERVICIOS PÚBLICOS

Son varios ámbitos donde la sostenibilidad tiene un rol importante, destacaba desde el Ministerio de Justicia Aitor Cubo, "pero si nos fijamos en el ámbito TIC, hablamos de compartir servicios y aquí es importante estable-

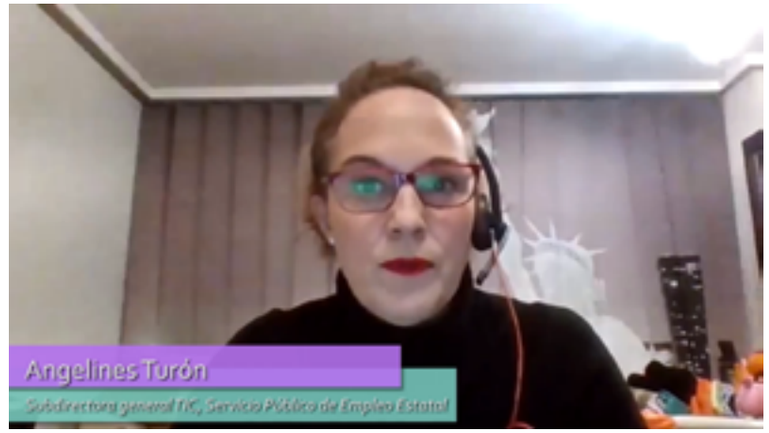
"HOY POR HOY, CON EL DESARROLLO DE LA NORMATIVA Y LA EXIGENCIA DE LOS CIUDADANOS, LAS ADMINISTRACIONES NO NOS PODEMOS PERMITIR EL LUJO DE NO DISPONER DE PLATAFORMAS QUE RESUELVAN NUESTROS PROBLEMAS"

VÍCTOR SOLLA BÁRCENA (AYUNTAMIENTO DE MÁLAGA)

cer la diferencia entre quien presta el servicio y el responsable del mismo en caso de fallo. La co-gobernanza es, por tanto, muy importante, y hay que influir en el desarrollo de la plataforma porque, si no, no la entiendes como propia y tienes un problema. Otro aspecto importante es el marco legal que, en nuestro caso, refuerza las premisas de la Administración General promoviendo la sostenibilidad con la compartición de servicios nuevos y previos, como el proyecto Clave Justicia. Es un proyecto importante para permitir la eficiencia y sostenibilidad del sistema, pero que tiene algunos retos que debemos superar, como la compartición de datos entre Administraciones. Debemos valorar, no obstante, la posibilidad de convertirlo en un proyecto tractor del ecosistema TIC de país. Si las Administraciones consiguen llevar este ecosistema de plataformas al sector privado, conseguiremos que el sistema sea más sostenible a la par que generamos mercado y especialistas TIC en el país".

En la Diputación Provincial de Albacete, explicó José Joaquín de Haro, "la sostenibilidad es un pilar básico de nuestro proyecto, que tiene un modelo de gobernanza muy claro, con una plataforma propia, que articula la sostenibilidad en dos ámbitos, la funcionalidad, que es configurada por los propias entidades que la adoptan, y la económica, con un modelo de coste que es tan sencillo como decir que se paga entre todos en cuestión de una serie de criterios previamente definidos. Por tanto, la sostenibilidad es un elemento innegociable. Ahora, con la llegada de nuevos retos, deberemos ir acomodando el modelo para alinearlas con él".

Por su parte, Ángel Esteban Paúl destacó que en el Ministerio de Hacienda "la compartición de servicios y bases es fundamental. Hay



"TENEMOS ELEMENTOS COLATERALES EN LA NUBE, PERO EN LOS SISTEMAS TRONCALES, LOS LEGACY DE TODAS LAS ADMINISTRACIONES, ES DONDE ESTÁ EL QUID DE LA CUESTIÓN"

ANGELINES TURÓN (SERVICIO PÚBLICO DE EMPLEO ESTATAL)

un centro organizativo que tiene un mayor desarrollo y no tiene sentido que el resto tenga que duplicar el trabajo. Además, estamos en el ámbito tributario, donde la protección de los datos tiene un papel enormemente relevante. El proyecto tiene ese foco previo, pero precisa de tres elementos esenciales. Cuando queremos avanzar en esa compartición de servicios es necesario realizar un análisis sectorial de integración. A esto hay que añadir una plena trazabilidad y la determinación de roles de cada jugador. Si no establecemos este esquema multiorganismo, estaríamos perdidos".

En una línea similar se expresó Víctor Solla hablando de su experiencia en el Ayuntamiento de Málaga, al afirmar que "independientemente del modelo, la sostenibilidad siempre debe estar encima de la mesa, con otros conceptos como integración o la interoperatibilidad. El objetivo de la Agenda Digital es que en 2025 el ciudadano sea el centro de las cosas. Nosotros representamos diferentes niveles de la Administración, pero el ciudadano es el mismo. Las Administraciones más pequeñas no pueden sobrevivir sin esos elementos que hacen que el ciudadano tenga un punto único de acceso a toda la información, lo que es un reto y una oportunidad. Si somos capaces de hacerlo, estaríamos consiguiendo una mejora en la calidad de vida de los ciudadanos a la vez que ahorraríamos muchos recursos. El resto es, por tanto, tener la suficiente confianza en el modelo como para subirnos a él. A la AGE le queda camino por recorrer, y el modelo debe transformarse por las nuevas tecnologías y la realidad. Hay que adaptar este modelo al momento actual, porque detrás estamos el resto de las Administraciones para poder avanzar".

Según el Servicio Público de Empleo Estatal, en palabras de Angelines Turón, "a todo lo anterior hay que añadir la posibilidad de obtener ahorros de costes por las economías de escala, y la simplificación y homogeneización de plataforma. Los ministerios vamos a tener que dejar paso a la Secretaría General de Administración Digital para que ésta asuma el liderazgo. Es el momento de trabajar en común para simplificar y homogeneizar. Esto va a tener un gran impacto y va a haber que hacer una redefinición de funciones, pero hay que abordarlos con valentía, acompasando los tiempos de los Ministerios y la SGAD. Y es importante las alianzas con el sector privado, porque las nuevas tendencias tecnológicas exigen una profunda reflexión, sin olvidar la falta de capital humano para poder abordar estos cambios y transformaciones. Se está intentando incorporar profesionales, pero estamos escasos tanto en la Administración General como en el mercado TIC en general. Por último, la simplificación de la contratación, porque sigue siendo muy complicado definir los requisitos. Esto debe cambiar de cara al futuro para que sea una commodity para nosotros".

LA NUBE Y EL SECTOR PÚBLICO

Muchos de las avances en digitalización necesitan las capacidades de la nube pero, como se indicó en la mesa redonda, todavía hay que modificar algunos aspectos de la contratación para que las Administraciones Públicas puedan aprovechar el mundo cloud en su totalidad. Para Aitor Cubo, "todos nuestros funcionarios ya trabajan en la nube, al igual que muchos procesos y servicios. Pero no solo eso, dado que toda la estrategia está planteada sobre la nube. Los servicios que da la SGAD los ofrece en modo nube. Por tanto, no es cierto que la Administración Pública no esté usando la nube. Debemos actualizar, por tanto, esta idea. La contratación pública es un problema que debemos replantearnos, pero no solo en relación con la nube, sobre todo para proyectos a corto plazo que necesitan inmediatez, pero la orientación en la nube ya tiene casos reales en la Administración".

En opinión de José Joaquín de Haro, "el mundo actual de las administraciones está bastante evolucionado y viaja en todo tipo de nubes. Además de los problemas de contratación, hasta ahora, muchos de los fondos públicos, y esperemos que con los Fondos NextGeneration no sea así, venían supeditados a infraestructuras físicas, lo que provocaba que, a la hora de reutilizar, cada administración volviera a invertir en infraestructura en la medida de sus necesidades. Esto es algo que ha ido consolidando estructuras de nube privada. Esto, unido al miedo a las cláusulas de salida de la nube, ha supuesto un freno frente a la celeridad del mundo privado. Pero creo que el uso de la nube está siendo bastante eficaz, y el problema está más en la falta de perfiles TIC en las plantillas de las Administraciones. De todas formas, somos optimistas con el desarrollo del modelo".

"Desde un punto de vista comercial", indicó Ángel Esteban, "la nube está más que implantada en las Administraciones, asumida, y la única discusión que nos queda es si determinados servicios y datos deben estar en una nube pública o privada. Pero la iniciativa en la Administración está más que asentada, así como el trabajo diario en la nube. Pero la contratación es una variable a tener en cuenta, no un problema, porque los problemas son los que tienen solución. Es una variable que debemos afrontar de forma coordinada, que es una mejor opción que tratar de resolverlo de forma individual".

Se mostraba de acuerdo Víctor Solla, que añadió que "la contratación es un freno tremendo, porque estamos trabajando en la nube para algunas cosas, pero para otras siguen siendo reacias las organizaciones. Es un cambio que los que trabajamos en el mundo TIC estamos propiciando. Pero hay algunos frenos a superar, como la falta de profesionales y la necesidad de seguridad, y eso tenerlo en nuestras plantillas es complicado. La seguridad, por tanto, va a ser un elemento tractor para pasar a la nube, porque el nivel de protección que nos va a ofrecer va a ser mayor del que podamos tener a nivel interno. Quizá no sea por ahorro de costes, porque todavía estamos amortizando inversiones previas en infraestructuras clásicas, pero debemos seguir dando pasos hacia la nube, porque es un camino que no tiene marcha atrás".

Sin embargo, para Angelines Turón "es cierto que tenemos elementos colaterales en la nube, pero en los sistemas troncales, los legacy de todas las Administraciones, es donde está el quid de la cuestión. Esto hay que evolucionarlo y no es sencillo, porque todavía estamos muy lejos en la SGAD de tener un sistema de aprovisionado rápido de infraestructura sea en la nube que sea. Falta una estrategia clara en los sistemas core, y ése es el proceso de digitalización que necesitamos. Estamos haciendo mucho, pero todavía necesitamos un plan claro y el tiempo corre en nuestra contra". ■

CONTENIDO RELACIONADO

Foro IT User: Administración pública, afrontando la década digital

SI TE HA GUSTADO ESTA REVISTA, COMPÁRTELA

JULIA SANTOS, DIRECTORA DE VENTAS DE DYNATRACE

"QUE UN SERVICIO ESTÉ DISPONIBLE EN DIGITAL NO ES GARANTÍA DE EFICIENCIA NI DE FÁCIL ACCESO"

LA UNIÓN EUROPEA Y LOS PAÍSES MIEMBROS DEBEN APROVECHAR LA DIGITALIZACIÓN PARA CAMBIAR LA FORMA EN LA QUE LOS CIUDADANOS Y LAS EMPRESAS INTERACTÚAN CON LAS ADMINISTRACIONES. Y PARA ELLO, DEBEN SACAR PARTIDO A LAS VENTAJAS QUE ESTA TRANSFORMACIÓN LES PROPORCIONA PARA MEJORAR LA OFERTA Y LA EJECUCIÓN DE LOS DIFERENTES SERVICIOS PÚBLICOS.

La operación excelente y orientada a la ciudadanía de los servicios públicos fue el hilo conductor de la intervención en el Foro IT User: Administración pública, afrontando la década digital de Julia Santos, Directora de Ventas de Dynatrace, que explicaba que "si dejamos de lado algo tan relevante como la capacitación digital, destacaría la orientación a la ciudadanía de los servicios públicos digitales, la aplicación de Inteligencia Artificial a las operaciones, y la transformación de las infraestructuras que soportan estos servicios hacia lo que denominamos infraestructuras líquidas, como los principales elementos de estos servicios digitales excelentes".

OPERACIÓN EXCELENTE Y ORIENTADA A LA CIUDADANÍA, CLAVES DE UNOS ADECUADOS SERVICIOS PÚBLICOS (Clica en la imagen para ver el vídeo).

CREACIÓN DE SERVICIOS EXCELENTES

De todas formas, para esta responsable conviene viene contextualizar, y lo hizo en base a cuatro elementos. "Primero, la influencia de la pandemia, que ha acelerado la Transformación Digital. Las organi-

zaciones se centraron en poder seguir dando servicio, moviendo a los trabajadores a sus hogares y posibilitando el trabajo en remoto, pero han pasado a una fase de redefinición del propio modelo de negocio. Y nada de esto es ajeno a las Administraciones que, además, tienen que asegurar el acceso de todos los ciudadanos. Por otro lado, todos los negocios se están convirtiendo en empresas de software, y las Administraciones, también, con el añadido de garantizar el acceso universal a los servicios públicos. Otro factor sería que España es uno de los países más avanzados en la Administración digital en Europa, pero el hecho de que un servicio esté en digital no garantiza ni su acceso, ni su sencillez de uso ni su eficacia. Por último, la UE ha habilitado unos fondos para digitalización en diferentes capítulos".

UNA NUEVA REALIDAD PARA LOS SERVICIOS PÚBLICOS

Esta realidad, explicaba Julia Santos, "va a sustentarse en tres aspectos: la inteligencia en las operaciones, aplicando IA a las operaciones TI; las infraestructuras líquidas; y poner al ciudadano en el centro".

En este momento, "tanto la Agenda Digital 2025 como el Plan de Digitalización de las Administraciones Públicas recogen iniciativas alrededor de estos aspectos tan relevantes. Hay que tener en cuenta que el hecho de que un servicio esté disponible en digital no es garantía de eficiencia. Por tanto, hay que dar un salto, y las Administraciones están yendo a modelos que colocan al ciudadano en el centro, apoyándose en conceptos como la Experiencia Digital. Una mala experiencia en una empresa privada, hace que se pierda una venta, pero una mala experiencia en un servicio público hace que falle el acceso universal al que tenemos derecho los ciudadanos. Por tanto, se trata de trasladar esta cultura del cliente en el centro a todos los canales, con servicios públicos productivos, personalizados y omnicanal. Y, en este sentido, venimos viendo la puesta en marcha de muchas iniciativas, como la capacitación digital, simplificar y ordenar el acceso a los servicios públicos, facilitar la tramitación en formato digital... complementado con plataformas de evaluación continuada para poder realizar un trabajo proactivo".

Si miramos hacia las operaciones inteligentes, "la IA es una tecnología aceleradora con muchos ámbitos de aplicación, como pueden ser las operaciones de TI. Estos servicios se basan en software y tienen que ofrecer la mejor experiencia de uso, por lo que la IA puede posibilitar mayor resiliencia y, puede hacer que los propios servicios sean operables, porque la adopción de tecnologías innovadoras va a implicar una mayor complejidad de gestión. Queremos que los servicios siempre estén funcionando y lo hagan correctamente, y para ello la IA es vital".

Y todo esto es más relevante, aseguraba Julia Santos, "cuando hablamos de infraestructuras líquidas que van a proporcionar la agilidad necesaria para la transformación, pero que necesitan una operación adecuada con unos elevados grados de automatización".

EL APORTE DE DYNATRACE

Para Julia Santos, "nuestra plataforma proporciona una observabilidad avanzada combinada con un alto grado de automatización e Inteligencia Artificial, y esto permite a las organizaciones un trabajo proactivo para evitar problemas o para reducir los tiempos de respuesta en caso de que se haya producido un incidente. Es una plataforma diseñada y pensada para entornos líquidos, que son más dinámicos y con mayores cargas de datos. Pero, como venimos de entornos legacy, nuestra soportabilidad es muy amplia". ■

CONTENIDO RELACIONADO

Modernice su entidad con observabilidad e inteligencia automática

Amazon Web Services reconoce la capacidad de Dynatrace para abordar proyectos de modernización de la Administración Pública

Unimos la administración pública con los ciudadanos.

Descubra cómo Salesforce puede acelerar su transformación digital con una visión 360° integrada y de confianza de sus ciudadanos.

AL SERVICIO DEL CIUDADANO DIGITAL

Participaron en esta mesa redonda la Seguridad Social, el Ayuntamiento de Madrid, el Ministerio de Justicia y el Ayuntamiento de Valencia (Clica en la imagen para ver el vídeo).

La última mesa redonda del Foro IT User: Administración pública, afrontando la década digital, estuvo dedicada a la creación de servicios para los ciudadanos digitales. Contó con la participación de Andrés Pastor, Gerente Adjunto de la Gerencia de Informática de la Seguridad Social; Fernando Álvarez, Subdirector de Transformación Digital de la Dirección General de la Oficina Digital del Ayuntamiento de Madrid; Nimia Rodríguez Escolar, Directora de

EL AÑO 2030 ES EL HORIZONTE QUE SE HA PROPUESTO LA COMISIÓN EUROPEA PARA LLEVAR A UN ENTORNO DIGITAL LOS SERVICIOS PÚBLICOS CLAVE, BENEFICIANDO CON ELLO A CIUDADANOS Y EMPRESAS. TAMBIÉN ES LA FECHA PARA QUE EL 80% DE ESOS CIUDADANOS UTILICEN UNA SOLUCIÓN DE IDENTIFICACIÓN DIGITAL. ABOGA EN SUS PLANES POR ESTABLECER UN GOBIERNO COMO PLATAFORMA, UNA NUEVA FORMA DE ESTABLECER ESOS SERVICIOS PÚBLICOS DIGITALES PARA FACILITAR EL ACCESO A ELLOS POR PARTE DE LA CIUDADANÍA, CON UNA INTERACCIÓN CONTINUA Y CAPACIDADES AVANZADAS CON TECNOLOGÍAS COMO LA IA O LA REALIDAD VIRTUAL. PARA APROVECHAR AL MÁXIMO ESTOS RECURSOS, LOS CIUDADANOS HAN DE TENER ACCESO UNIVERSAL A INTERNET Y UN ENTORNO ON-LINE SEGURO Y FIABLE, ADEMÁS DE CONTAR CON COMPETENCIAS PARA PODER PARTICIPAR EN ESTA SOCIEDAD DIGITAL.

la División de Tecnologías y Servicios Públicos Digitales del Ministerio de Justicia; Fernando Gallego García, Jefe de Servicio de Transparencia y Gobierno Abierto del Ayuntamiento de Valencia; y Antonio Ceño, Director de Gobierno Central de Salesforce, ejerció de co-moderador durante la sesión.

El primer tema del debate fue conocer cómo se plantean estos retos las diferentes organizaciones participantes. En el caso de la Gerencia de Informática de la Seguridad Social, en palabras de Andrés Pastor, "es cierto que el ciudadano es cada vez más digital, algo que se ha acelerado en los últimos meses. Estos objetivos han estado en la mente y en las iniciativas de las Administraciones, y todos hemos trabajado para que sean una realidad, pero lo cierto es que hemos tenido un éxito relativo. Hemos tratado de tener en nuestra web versiones digitales de todos los servicios, pero no es un tema de cantidad, sino de calidad. No queremos obligar a los ciudadanos a acceder a los servicios digitales, sino que quieran acceder, que sea su medio preferente, y, para eso, necesitamos mejorar la experiencia de uso. Tenemos que atacar el problema desde el punto de vista de la tecnología pero también desde la experiencia del usuario. Lo que estamos haciendo es incorporar la web del ciudadano en el diseño de los servicios públicos y rompiendo esa barrera de acceso a los mismos que es

"NO EXISTE UNA SOLA TECNOLOGÍA QUE DINAMICE LA RELACIÓN CON LOS CIUDADANOS, SINO UN CONJUNTO DE ELLAS QUE SE INTEGRAN EN UN PLAN DE DIGITALIZACIÓN MUY AMBICIOSO QUE PRETENDE CAMBIAR RADICALMENTE LA ORGANIZACIÓN"

ANDRÉS PASTOR (GERENCIA DE INFORMÁTICA DE LA SEGURIDAD SOCIAL)

la identificación digital. Pero tenemos que seguir trabajando en la simplificación del acceso de los ciudadanos a los servicios públicos".

Para Fernando Álvarez (Ayuntamiento de Madrid), "los dos últimos años ha sido un período de aceleración y cambio profundo en los servicios. Nos hemos incorporado a Cl@ve, para la identificación de usuarios, y en los últimos 18 meses se ha reforzado la gestión digital de todos los procesos de los servicios públicos municipales. Por ejemplo, la firma digital se ha incrementado considerablemente, mientras que a nivel presencial a menos de un 40%. El plan de choque puesto en marcha hace unos años se ha visto agudizado por la pandemia. Además, nos hemos integrado con DEHú, lo que ha supuesto el envío de 125.000 notificaciones electrónicas y un ahorro de 525.000 euros. Y también empezamos con los primeros pasos de la automatización".

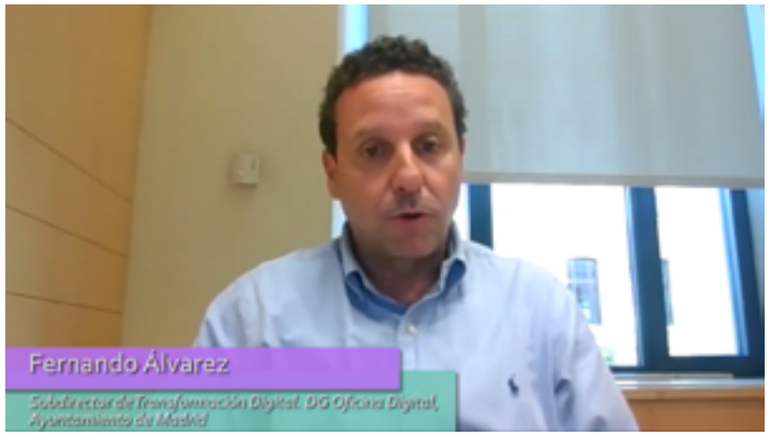
Nimia Rodríguez Escolar explicaba que en el Ministerio de Justicia "la apuesta es clara, pero hemos ido un paso más allá, para personalizar la relación electrónica. Habíamos trabajado en ello antes de la pandemia, pero se ha visto reforzada la necesidad, por los actores con los que nos relacionamos, de tener esas herramientas personalizadas de forma electrónica. Para ello, uno de los grandes proyectos es el de Identificación Digital y Servicios No Presenciales que va más allá de una simple videoconferencia, porque había que dotarlo de la seguridad jurídica exigida por los organismos judiciales. Fue un reto el cambio del modelo de identificación telemática por medio de esa videoconferencia. Hemos tenido que hacer un gran esfuerzo formativo, si bien los ciudadanos y las instituciones ya estaban acostumbrados a realizar videoconferencias, por lo que la formación no está tanto sobre la tecnología sino sobre su uso para que tuviera esas garantías cubiertas. Para ello, hemos lanzado varias campañas sobre los

servicios y sobre cómo usarlos. Ya estábamos, entonces, inmersos en el proceso de ayudar al ciudadano. Todo esto, por supuesto, de acuerdo con el marco legal para dar soporte y garantías en todos los pasos".

Según Fernando Gallego García, del Ayuntamiento de Valencia, "en nuestro caso, todavía estamos en proceso de digitalización de muchos de los servicios. Estos tienen un diseño vertical, por departamentos, y necesitamos una visión más horizontal. No se trataba, por tanto, solo de implantar tecnología, sino de hacer una revisión de los servicios y de la organización de las entidades. No tenemos un problema de tecnología, ni de formación de los ciudadanos, pero necesitamos servicios más usables y entendibles por su parte. Estamos trabajando precisamente en esta línea, con el fin de ofrecer una atención integral, de ahí que sea importante tener una visión holística. Durante la pandemia, las interacciones digitales han superado a las presenciales, pero eso no quiere decir que sea fácil para los ciudadanos ni que sean expertos en cuestiones administrativas. Queremos potenciar, por tanto, que los servicios sean entendibles".

RETOS A SUPERAR PARA CONSTRUIR SERVICIOS INNOVADORES

Al igual que las compañías en el sector privado, las Administraciones Públicas deberían ser capaces de crear servicios innovadores para los ciudadanos, si bien se enfrentan a una serie de reto. En el caso del Ayuntamiento de Madrid, detallaba Fernando Álvarez, "uno de ellos es la necesidad de reducir la heterogeneidad de las posibilidades de acceder a los servicios digitales. Es una oportunidad y una debilidad. Los líderes digitales de determinadas áreas deben impulsar el desarrollo en otras áreas. Otro reto es la adaptación continua a las tecnologías emergentes, y esto no es sencillo por los modelos que tenemos de gobernanza de las TIC. Otro aspecto es la cultura digital del personal. Hemos superado la primera fase, porque sí hemos digitalizado, pero hay que avanzar hacia trabajar con estructuras de datos, diseñar los procesos con la aplicación intensiva de la tecnología y desarrollar el trabajo colaborativo, integrando a las personas en los procesos de diseño para que los servicios sean más usables. Pero también hay retos externos, porque la sociedad es diferente y la Administración debe ser capaz de responder a esas demandas, sobre todo las de las nuevas generaciones, más proactivas en el consumo de este tipo de servicios. Además, empezamos a tener competencia en determinados servicios públicos, como puede ser el de la movilidad, y tenemos que aprender a trabajar con ellos para mejorar la calidad de vida de las personas, que es el objetivo final".



"LA PRIVACIDAD ES, SIN DUDA, UNA OPORTUNIDAD PARA REFORZAR LA CONFIANZA DE LOS CIUDADANOS EN EL BUEN USO DE LOS DATOS"

FERNANDO ÁLVAREZ (DIRECCIÓN GENERAL DE LA OFICINA DIGITAL DEL AYUNTAMIENTO DE MADRID)

Por su parte, en el Ministerio de Justicia, "el mayor reto ha sido implantar estas soluciones en un brevísimo lapso, porque con la pandemia no se podía hacer nada. Nosotros no ofrecemos una tramitación normal y poner en marcha un sistema con garantías procesales para todos los intervinientes, fue el mayor reto. No la aceptación de la gente, que ya lo tiene asumido, sino asegurar que se cumplían los mismos requisitos de seguridad que en el modelo presencial. La Administración de Justicia no podía parar, y teníamos que ser capaces de convencer de la idoneidad de un nuevo modelo de relación electrónica, y explicarles cuál es el procedimiento adecuado para aprovechar la tecnología. Y otro punto importante era el relativo a la co-gobernanza, para que todas las

entidades y administraciones pudieran avanzar al mismo ritmo y nadie se quedase fuera".

En el Ayuntamiento de Valencia, nos comentaba Fernando Gallego, que "desde el punto de vista externo, el reto es acercarse al lenguaje de la ciudadanía. Además, hay que hacerles entender la necesidad de los sistemas de identificación digital, así como mostrarles la confiabilidad de los sistemas, con los elementos básicos de ciberseguridad. Desde el punto de vista interno, hay varios retos, pero uno destaca por encima del resto: conseguir gobernanza de los datos en la organización. La datificación es algo que nos demanda la sociedad. No solo tener la información de un documento digital, sino que detrás de él haya datos que nos permitan explotar esa información. Pero es importante el cambio cultural a este respecto. Si ahora se habla de un plan nacional de IA y de proyectos de IoT, si no datificamos la información no tendremos la gasolina que necesitan los motores de la Inteligencia Artificial. Necesitamos modelizar y automatizar, con el objetivo de avanzar en la compartición de la información. Necesitamos una visión general en la organización que se cumpla en todos los departamentos, porque es la única forma de desarrollar cuadros de mando que podamos aprovechar. Además, con los Fondos Next Generation necesitaremos analizar y cruzar información para ofrecer las métricas que nos van a demandar".

"LA APUESTA POR LOS SERVICIOS PÚBLICOS DIGITALES ES CLARA, PERO HEMOS IDO UN PASO MÁS ALLÁ, PARA PERSONALIZAR LA RELACIÓN ELECTRÓNICA"

NIMIA RODRÍGUEZ ESCOLAR (MINISTERIO DE JUSTICIA)

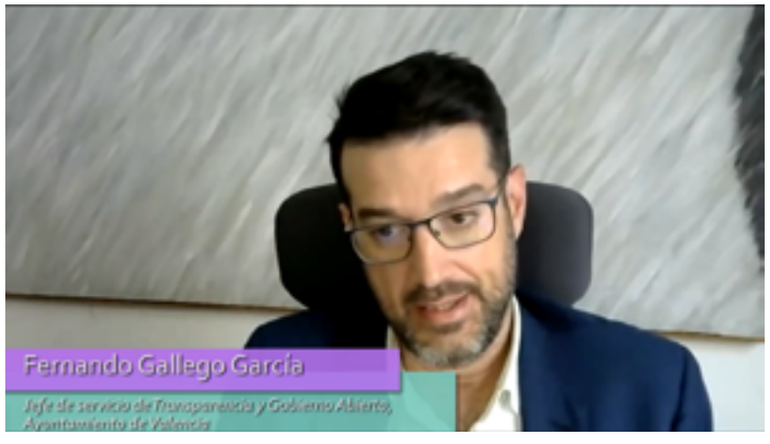
Concluyó esta ronda de valoraciones Andrés Pastor, asegurando que, en la Seguridad Social, comparten "muchos de estos retos. Pero tenemos una dificultad inherente, y es que no somos una entidad de servicios de consumo recurrente, lo que complica la implicación de los usuarios con estos servicios. Otro aspecto en el que tenemos que innovar en que los ciudadanos puedan romper la barrera de la identificación. Llevamos tiempo con certificados digitales, el DNI electrónico e, incluso, con Cl@ve, que son medios necesarios pero insuficientes, porque muchos ciudadanos no son capaces de acceder a los servicios digitales, algo que se ha intensificado con la pandemia. Experimentamos, en pandemia, eliminar la barrera de identificación y facilitarlo solo con una dirección de correo electrónico, y hemos comprobado que prácticamente todo el mundo, con un móvil, era capaz de acceder a los servicios, incluso los más complejos. Tenemos que romper esta barrera, y hemos optado por modificaciones, incluso a nivel jurídico, para facilitar el acceso de los ciudadanos, y ese es un camino en el que hemos de avanzar. Porque una vez que acceden a los servicios, puedes ofrecerles más opciones, pero no si no consiguen hacerlo. Por otra parte, la Administración tiene que abrirse a la innovación rompiendo esquemas culturales, y lo importante es que esta innovación surge en la parte analógica, las personas".

TECNOLOGÍAS Y PROYECTOS DINAMIZADORES

Comentaba Nimia Rodríguez que en el Ministerio de Justicia "es fundamental que la relación presencial fuera una relación electrónica personalizada. Por eso, las tecnologías en las que más nos hemos apoyado son los sistemas de videoconferencia, pero integradas con otras tecnologías para generar un escritorio virtual de integración digital, para que se pudiera firmar por videoconferencia con las garantías judiciales necesarias, además de poder ser guardado, posteriormente, como un expediente judicial electrónico. Todo esto tenía que

ir muy ligado a instalar el sistema de cita previa, tan extendido en otras administraciones. En estos meses se han dado más de 250.000 citas previas para la tramitación en los juzgados, y se han realizado casi unas 600.000 vistas telemáticas, por lo que esperamos que todo esto se mantenga, sobre todo porque se están cambiando las normativas para poder adaptar la Justicia a las nuevas tendencias".

Para Fernando Gallego, en el Ayuntamiento de Valencia, "se están llevando a cabo diferentes proyectos, desde la potenciación y rediseño de la Sede Electrónica, una nueva aplicación de contabilidad, iniciativas de IoT, modernización de aplicaciones... También vamos a realizar una inversión fuerte en seguridad y servidores, y estamos trabajando en un proyecto de atención ciudadana transversal. Queremos contar con una plataforma unificada para poder explotar la información en diferentes servicios, además de ofrecer una cara más amable para la ciudadanía, con información más accesible e, incluso, de manera proactiva, y sistemas de chatbot para poder ofrecer respuestas de manera automática. Desde el punto de vista del ámbito del gobierno y los datos abiertos, queremos implementar un repositorio municipal de datos para poder someterlos a explotación tanto interna como externa. Es un proceso que se está licitando en este momento y será importante en el próximo ejercicio".



"QUEREMOS CONTAR CON UNA PLATAFORMA UNIFICADA PARA PODER EXPLOTAR LA INFORMACIÓN EN DIFERENTES SERVICIOS, ADEMÁS DE OFRECER UNA CARA MÁS AMABLE PARA LA CIUDADANÍA"

FERNANDO GALLEGO GARCÍA (AYUNTAMIENTO DE VALENCIA)

En el caso de la Seguridad Social, explicaba Andrés Pastor, "no existe una sola tecnología que dinamice la relación con los ciudadanos, sino un conjunto de ellas que se integran en un plan de digitalización muy ambicioso que pretende cambiar radicalmente la organización. A nivel tecnológico, contamos con unos sistemas muy robustos pero que no son los más adecuados para integrar nuevas tecnologías. Por eso, estamos inmersos en una redefinición de la arquitectura, así como en un rediseño de los procesos más adecuado al lenguaje de los ciudadanos, con una experiencia de uso optimizada para ellos. Últimamente, hemos apostado por tecnologías en la nube, que son dinamizadoras de la transformación porque, por una parte, facilitan la puesta en marcha iniciativas de manera rápida, como ha sido la gestión del Ingreso Mínimo Vital, algo que no iba a ser posible con nuestras arquitecturas anteriores. Además, nos facilitaban cambios muy rápidos en función de cómo se comportaba el propio sistema. Asimismo, todo lo relacionado con IA y chatbots nos ha permitido mantener la comunicación con los ciudadanos en un canal que sustituyó al presencial".

En palabras de Fernando Álvarez del Ayuntamiento de Madrid, "estamos diseñando una gran estrategia de Transformación Digital con la que intentamos dar respuesta a todos los retos que estamos detectando, identificando las mejores prácticas en ciudades similares a la nuestra. Al hilo de esta gran estrategia, estamos trabajando en cinco programas operativos. Uno para la IA, con pilotos a realizar a corto plazo en algunos casos; un segundo para el desarrollo de apps; un tercero centrado en la gobernanza del dato, con un cuadro de mando operativo de los distintos servicios municipales; el cuarto es sobre 5G, que estamos desarrollando con las operadoras y el Colegio de Ingenieros de Madrid, y con el que estamos definiendo pilotos; y, el último, la ciberseguridad. Por otra parte, estamos

impulsando la figura del Delegado Digital en todas las áreas municipales para tener un interlocutor con inquietudes en todas las tendencias y que conozca la realidad de las diferentes áreas. Y, en el día a día, tenemos un plan de choque para la implantación efectiva de los instrumentos de administración digital junto con un esfuerzo importante de capacitación del personal para seguir mejorando en la prestación de los servicios".

PRIVACIDAD Y CONFIANZA

El manejo de datos por parte de la Administración Pública es todo un desafío. Fernando Gallego, así lo constató: "es una de las preocupaciones que tenemos, y el presupuesto de ciberseguridad se ha incrementado. Pero tenemos mucho por avanzar en la confianza de la ciudadanía, porque no creo que los servicios públicos sean menos seguros que los privados, y los ciudadanos acceden a ellos sin reparos, pero les cuesta más dar la información a una entidad pública. Choca bastante la imagen de exposición de la privacidad por parte de la Administración, así que tenemos una tarea importante para transmitir confianza, además de las medidas de seguridad que tenemos que poner en marcha. Y hemos de avanzar en seguir desarrollando la cultura digital de los ciudadanos".

Para Andrés Pastor, "el cumplimiento de una privacidad razonable, limita la rapidez con la que se pueden poner en marcha las iniciativas. Tenemos que ser cuidadosos con la normativa y transmitir a los ciudadanos las garantías reales, pero también las aparentes, de que estamos haciendo las cosas bien. Es necesario que lo que hagamos esté suficientemente protegido, pero no se nos trata igual que a las empresas privadas, que pueden tener más información de los ciudadanos pero que son medidas con otro baremo. Por otra parte, hemos que reforzar la toma de decisiones en cuanto algoritmos para que, además de hacer cosas eficaces y eficientes, pensemos en el impacto que pueden tener. Aquí nos queda mucho por hacer, sobre todo ahora que estamos potenciando su uso a todos los niveles".

Señalaba por su parte Fernando Álvarez que "la privacidad es, sin duda, una oportunidad para reforzar la confianza en el buen uso de los datos, pero también a la hora de generar grupos de trabajo multidisciplinares, que deben enriquecerse con perfiles de protección de datos, haciendo partícipes también a colectivos que usan estos servicios, para que vean el rigor con el que se desarrollan. Estos grupos multidisciplinares nos ayudan en el propio rediseño del proceso y esto nos hace valorar diferentes alternativas y soluciones. Esto demora los plazos de los proyectos, pero incrementa la calidad de los mismos, porque la información es de la persona y diseñamos servicios para la persona".

De acuerdo se mostró Nimia Rodríguez añadiendo que "el dato es un bien público que debe protegerse, manejarse y reutilizarse, poniéndolo en valor para que todas las Administraciones nos pongamos de acuerdo. Prueba de ello es el programa de Justicia orientada al Dato, donde se cambia todo el paradigma tradicional de la orientación al documento por uno de orientación al dato. Antes, por ejemplo, un nacimiento era un número en un tomo, mientras que ahora pasará a ser un dato de una persona, y esto implica un cambio muy importante. Esto permitirá reutilizar la información y mejorar la definición de las políticas públicas que quiera hacer cualquier administración. Para nosotros, es la piedra angular de toda nuestra transformación y va a ayudar a incrementar la confianza del ciudadano en lo que estamos haciendo". ■

CONTENIDO RELACIONADO

Foro IT User: Administración pública, afrontando la década digital

SI TE HA GUSTADO ESTA REVISTA, COMPÁRTELA

ANTONIO CEÑO, DIRECTOR DE GOBIERNO CENTRAL DE SALESFORCE

“QUEREMOS OFRECER UNA EXPERIENCIA INTEGRADA DE LA INFORMACIÓN, CON UNA VISIÓN COMPLETA DEL CIUDADANO”

DENTRO DE LOS AVANCES DE DIGITALIZACIÓN EN LAS ADMINISTRACIONES PÚBLICAS, UN ELEMENTO ESENCIAL ES REFORZAR LAS RELACIONES DE ÉSTAS CON LOS CIUDADANOS, PARA LO QUE ES NECESARIO EL DESARROLLO DE SERVICIOS INNOVADORES Y PERSONALIZADOS. Y LA CLAVE PARA ESTOS SERVICIOS ES COLOCAR A LOS CIUDADANOS EN EL CENTRO DE LA ESTRATEGIA.

Antonio Ceño, Director de Gobierno Central de Salesforce, en su intervención en el Foro IT User: Administración pública, afrontando la década digital recordó la necesidad de colocar al ciudadano en el centro como elemento básico en los procesos de transformación de la Administración Pública. Para este responsable, “nos encontramos en un momento histórico. Venimos de una pandemia que ha afectado fuertemente a España con una contracción de dos dígitos, pero se ha trabajado en un plan para recuperar esa economía y es importantísimo poder aprovecharlo bien. Estas inversiones nos obligan a trabajar en cosas productivas que mejoren la vida del ciudadano y la realidad del país, para aprovechar la oportunidad. Somos uno de los países que vamos a recibir más fondos, con un 30% dirigido a la Transformación Digital, lo que abre una

LA CLAVE DE LA TRANSFORMACIÓN DIGITAL DEL SECTOR PÚBLICO PASA POR SITUAR A LOS CIUDADANOS EN EL CENTRO DE LA ECUACIÓN (Clica para ver el vídeo).

puerta a hacer cambios que, hasta la fecha, no se han podido afrontar".

RETOS SIGNIFICATIVOS A AFRONTAR

En palabras de Antonio Ceño, "existen unos retos para digitalizar la Administración Pública y ponerla más cerca de los ciudadanos. El primero de ellos es la atención a la propia ciudadanía, porque las personas están acostumbradas a interactuar con organismos de forma omnicanal, y esto es algo que demanda a las Administraciones. El segundo es que la relación sea personalizada y proactiva, aprovechando todos los datos que disponen de cada uno. Durante años, las compañías han perdido oportunidades por tener la información en silos, y esto es algo que también afecta a las Administraciones Públicas. Otro reto es la propia gestión de los datos, porque hay veces que están en sistemas diferentes y se pierden oportunidades para aprovecharlos y dar valor a la ciudadanía".

Desde Salesforce "pensamos que somos la compañía adecuada para afrontar estos retos, porque ya lo hemos ido haciendo en el sector privado e, incluso, en la propia Administración, donde estamos creciendo más que nuestra competencia en el segmento CRM, por ejemplo, por nuestra especialización y capacidad. Además, somos una compañía que invierte en la sociedad y con unos valores muy fuertes, incluida la innovación. Asimismo, generamos muchos puestos de trabajo. En España, unos 50.000 entre todo nuestro ecosistema".

"NOSOTROS TRABAJAMOS POR LA ADMINISTRACIÓN DEL FUTURO, CON MUCHOS SERVICIOS PARA EL CIUDADANO, A TRAVÉS DE CUALQUIER CANAL, Y CON TODA LA INFORMACIÓN COMPARTIDA ENTRE LOS DIFERENTES ORGANISMOS"

OMNICANALIDAD PARA LA ATENCIÓN AL CIUDADANO

La Administración Pública ha contado, desde siempre, "con muchos procesos distintos en áreas diferentes. Esto es complejo para el ciudadano, que no tiene el conocimiento de estos procesos realmente, lo que genera procesos lentos. Nosotros trabajamos por la Administración del futuro, con muchos servicios para el ciudadano, a través de cualquier canal, y con toda la información compartida entre los diferentes organismos. Esto mejorará la relación con ciudadanos y empresas. Queremos ofrecer una experiencia integrada de la información, con una visión completa del ciudadano, una visión de 360 grados. Para ello, ofrecemos diferentes soluciones tecnológicas que abarcan toda las áreas de la transformación para responder a los retos que se plantean. Queremos que la relación con los ciudadanos sea sencilla, ágil, eficiente y, sobre todo, que se rompan los silos de la información para poder ofrecer esa visión que comentábamos".

Salesforce "ayuda en esta transformación sin romper lo que hay en la estructura. Las Administraciones tienen sistemas legacy y desarrollos a medida, y transformar esto lleva mucho esfuerzo y problemas. Salesforce pone una capa para poder interactuar con los ciudadanos, aprovechando la información, sin tener que cambiar los sistemas core, que se irán reemplazando con el tiempo. Es necesario dar una respuesta rápida y ágil a los ciudadanos". ■

CONTENIDO RELACIONADO

Crea un Sector público digital y moderno

¿Qué es Salesforce for Government?

“LOS EQUIPOS DE GOBIERNO DE LOS AYUNTAMIENTOS DEBEN SER LOS PRIMEROS IMPULSORES DEL CAMBIO”

JOSÉ LUIS GARROTE, SUBDIRECTOR DE MODERNIZACIÓN ADMINISTRATIVA DE LA FEDERACIÓN ESPAÑOLA DE MUNICIPIOS Y PROVINCIAS

La modernización y transformación de la Administración Pública es una de las principales líneas del plan España Digital 2025, y de las iniciativas que dispone la Brújula Digital 2030 que propone la Comisión Europea. Y esto tiene especial importancia para las Administraciones de menor tamaño y más cercanas a los ciudadanos, como son los ayuntamientos.

En su intervención en el Foro IT User: Administración pública, afrontando la década digital, José Luis Garrote, Subdirector de Modernización Administrativa de la Federación Española de Municipios y Provincias, destacó que “venimos de un escenario complicado en la administración local, sobre todo a nivel de recursos humanos y económicos. En este contexto, intentamos atacar tres frentes. El primero son los recursos humanos de la administración local, con una mejora de la cualificación porque vivi-

El papel de los ayuntamientos en la digitalización de la Administración y las necesidades especiales que estos presentan fue el hilo conductor de la intervención de la FEMP en este Foro (Clica en la imagen para ver el vídeo).

mos en una realidad con nativos digitales y nativos analógicos. Desde hace tiempo se están abordando planes para mejorar esta cualificación y estamos trabajando también en que las cargas de trabajo sean asumibles. Otro elemento clave son los recursos tecnológicos. Se han ido poniendo medios, haciendo inversiones, pero la realidad municipal es muy compleja, con ayuntamientos grandes y otros más pequeños que dependen mucho de las diputaciones. Y no podemos olvidarnos de un tercer apartado, la ciudadanía. La cultura digital de la ciudadanía es muy importante para entender lo que estamos haciendo y cuáles son las necesidades para abordar el cambio".

ELEMENTOS IMPULSORES PARA EL CAMBIO

Para llevar a cabo esta modernización, los factores decisivos, en opinión de José Luis Garrote, serían "el primero, un liderazgo político importante. Los equipos de gobierno de los ayuntamientos deben ser los primeros impulsores. Cuando esto se produce, y cuenta con los recursos, el avance es más sencillo, implicando también a los trabajadores, aunque no siempre se consigue. Si, además, existe consenso de los diferentes implicados, porque esto no es algo de una única legislatura, el proyecto no se parará aunque haya cambio de gobierno. Una vez que se produce este paso, lo importante es crear equipos internos, a ser posible, multidisciplinares. No hablamos de un cambio tecnológico, pero hablamos de un cambio de cultura, de procesos. Antiguamente, existía la tendencia de trasladar los procesos de un formato tradicional a uno electrónico, pero no es la filosofía que nos guía ahora. Lo importante es que el cambio se produzca desde una revisión completa del funcionamiento del ayuntamiento, con nuevos servicios que, hasta la fecha, nadie pensaba que pudieran ofrecerse".

Los planes, tanto el de la UE como el del Gobierno de España, ponen sobre la mesa unos plazos de tiempo relativamente cortos. Para José Luis Garrote, "son tiempos factibles, pero esperamos que estas iniciativas no se acaben en 2025 o en 2030, porque hablamos de un cambio cultural para una modernización constante y permanente. Los fondos son una oportunidad única, pero no solo debemos poner el foco en servicios para hoy, sino establecer los funcionamientos internos para ser un motor permanente de cambio y transformación, tanto para la Administración como para la sociedad. Ahora tenemos por delante un esfuerzo muy importante y hay que adecuarse a los plazos, y creo que en un porcentaje muy alto llegaremos a cumplir con los proyectos que se están planteando".

UN TRABAJO EN DIFERENTES VÍAS

Desde la FEMP, explicó José Luis Garrote, "nuestra misión es representar a los ayuntamientos ante el Gobierno, y éste nos utiliza para conocer las necesidades y demandas de los ayuntamientos para poder matizar y ajustar sus políticas en relación con estos. Estamos integrados en diferentes conferencias y consejos para poder desarrollar unas políticas coordinadas. Estamos trabajando en órganos internos con técnicos municipales para conocer de primera mano las necesidades de los municipios para poder abordar iniciativas que plantear al Ministerio. Estamos elaborando propuestas con un componente técnico, con un componente importante de replicación de casos de éxito, y otras para concienciación de cargos electos, porque es muy importante que los responsables elector sean partícipes e impulsores de estas cuestiones". ■

CONTENIDO RELACIONADO

Foro IT User: Administración pública, afrontando la década digital

e-Iris: combatir la brecha digital desde la biblioteca municipal

AUTOMATIZACIÓN INTELIGENTE

Ayudando a las Administraciones Públicas a promover y acelerar sus proyectos de automatización

blueprism®

www.blueprism.com

DAVID GÓMEZ, SALES DIRECTOR PARA IBERIA DE BLUE PRISM

"LA AUTOMATIZACIÓN INTELIGENTE DE PROCESOS SE ESTÁ CONVIRTIENDO EN UNA PALANCA CLAVE PARA CONSEGUIR MAYORES EFICIENCIAS Y AGILIDAD"

LA ADMINISTRACIÓN PÚBLICA NECESITA AVANZAR EN LA CREACIÓN DE SERVICIOS ÁGILES PARA EL CIUDADANO, Y, PARA ELLO, NADA MEJOR QUE APROVECHARSE DE LAS POSIBILIDADES QUE LA AUTOMATIZACIÓN INTELIGENTE DE PROCESOS PUEDE PROPORCIONAR.

En su ponencia en el Foro IT User: Administración pública, afrontando la década digital David Gómez, Sales Director para Iberia de Blue Prism, explicó que "la realidad a la que se enfrenta la Administración Pública es de una auténtica presión para utilizar los recursos limitados en tiempo para implantar toda una batería de tecnologías que se encuentran encima de la mesa. Esta presión requiere el aprovechamiento al máximo de los recursos que tiene la Administración, tanto de personas como de tiempo. Para ello, la automatización inteligente de procesos se está convirtiendo en una palanca clave para conseguir mayores eficiencias y agilidad en la implantación".

Este tipo de tecnologías buscan "que las habilidades humanas, como la creatividad, la innovación o el trato a las personas sean las que distingan

LA AUTOMATIZACIÓN INTELIGENTE DE PROCESOS PUEDE APORTAR VALOR A LAS ADMINISTRACIONES PÚBLICAS (Clica en la imagen para ver el vídeo).

un mejor servicio al ciudadano y una mayor calidad de trabajo para el funcionario".

AUTOMATIZACIÓN INTELIGENTE DE PROCESOS

Tal y como explicaba Gómez, "las motivaciones para la digitalización de la Administración están enmarcadas en la Agenda 2030, e incluyen una serie de medidas para la automatización de procesos que tienen como objetivos un mejor servicio al ciudadano, una mayor calidad de trabajo del funcionario, cumplimiento normativo y la seguridad de los datos de los ciudadanos. La adopción de estas tecnologías de automatización ya está presente en la Administración española. Según un informe de HFS Research, dos tercios de los organismos públicos están empezando a pilotar proyectos de automatización o ya los tienen en marcha desde hace tiempo".

"Nosotros", añadió, "tenemos un papel muy relevante en estos proyectos de automatización. Nuestra tecnología busca las eficiencias operativas y el incremento de la agilidad organizacional, a través de un cambio en la forma en que los trabajadores ejecutan sus acciones del día a día, eliminando las tareas repetitivas y liberando horas de su trabajo para sus organizaciones. Cualquier empresa puede empezar estos pilotos y obtener el ROI de manera inmediata".

ALGUNOS CASOS DE USO

En los últimos dos años, Blue Prism ha llevado a cabo proyectos con diferentes entidades públicas, que David Gómez quiso repasar, empezando por el llevado a cabo en la Secretaría General de Administración Digital, "con la adjudicación de una licitación a Telefónica para la puesta en marcha de un servicio de automatización inteligente. Durante los próximos 4 años, se prestará un servicio de automatización a aquellos departamentos que así lo requieran. Otro ejemplo es el del Ministerio de Justicia, donde un proceso como el de la cancelación de antecedentes penales antes requería la ejecución y revisión de unos 2.000 expedientes a la semana, ahora es capaz de absorber hasta 140.000 revisiones diarias. Un tercer ejemplo es el de la Junta de Andalucía, que, gracias a la automatización de procesos, ha conseguido gestionar las ayudas para ciudadanos y empresas a cuenta de los Fondos COVID. Han sido capaces de absorber todas las solicitudes en tres meses, una carga de trabajo que en ocasiones anteriores no habían sido capaces de absorber en dos años. Por último, está el ejemplo de Renfe, con casos de uso en todas las áreas de su organización, como el pago de facturas a proveedores, donde han conseguido reducir el tiempo de 96 a solo 12 horas. Además, con los Centros de Competencias Digitales puestos en marcha, van a ser capaces de ofrecer servicios de automatización a cualquier entidad que lo necesite".

Pensando en las Administraciones Públicas interesadas en la automatización inteligente, David Gómez explicó que su compañía tiene disponibles "una serie de recursos gratuitos. Primeros, recursos formativos, con un catálogo de formaciones gratuitas, incluyendo cursos completos relativos a automatización e Inteligencia Artificial. Por otra parte, también ofrecen recursos desde el punto de vista del licenciamiento, con posibilidad de acceso gratuito para realizar las primeras pruebas y pilotos para poder evaluar los resultados obtenidos. En tercer lugar, ofrecemos un equipo local de recursos y de expertos consultores, rodeados de socios integradores de nuestra tecnología, que pueden ayudar a los interesados en las primeras experiencias". ■

CONTENIDO RELACIONADO

Canal de YouTube de Blue Prism

Enfoque hacia la modernización y mejore la calidad y velocidad de sus servicios de atención al ciudadano con Blue Prism

VÍCTOR PÉREZ DE MINGO, SENIOR SYSTEMS ENGINEER DE VEEAM

“LOS GRANDES RETOS A AFRONTAR EN 2020 HICIERON QUE SE DESCUIDARA LA PROTECCIÓN DE LOS DATOS”

LA ADMINISTRACIÓN PÚBLICA ES UNA GRAN CONSUMIDORA DE DATOS, UNOS DATOS QUE SE ENFRENTAN A NUMEROSOS DESAFÍOS Y, ENTRE ELLOS, SU PROTECCIÓN. SE TRATA DE TODO UN RETO, SOBRE TODO PENSANDO EN LA GRAN CANTIDAD DE INFORMACIÓN DISPONIBLE Y EN LA NECESIDAD DE QUE ESTÉ AL ALCANCE DE NUMEROSOS SERVICIOS, APLICACIONES Y USUARIOS.

Víctor Pérez de Mingo, Senior Systems Engineer de Veeam para España y Portugal, explicó durante su intervención en el Foro IT User: Administración pública, afrontando la década digital que “los retos son muchos y variados. En 2020, nos encontramos de la noche a la mañana con una presión que no habíamos vivido nunca en los departamentos de TI. El impacto forzó a todas las organizaciones a pensar maneras distintas de hacer las cosas, lo que se tradujo en una aceleración enorme del consumo de algún tipo de servicio cloud y un aumento elevado de los ataques por ransomware. Y los grandes retos a afrontar hicieron que se descuidara un poco la protección de los datos, lo que provocó que cerca del 98% de los datos perdidos que intentaron ser recuperados, no pudieran serlo”.

Estos desafíos “han cambiado mucho la forma de trabajar de los departamentos de TI. Hemos visto

LAS NUEVAS AMENAZAS REQUIEREN DE UNA APROXIMACIÓN A LA PROTECCIÓN DE DATOS MODERNA (Clica en la imagen para ver el vídeo).

un crecimiento enorme de los servicios cloud, más de un 60%; también el uso de soluciones SaaS, un 48%; y en los ciberataques, más de un 715%. Esto ha generado nuevos retos alrededor de la protección de los datos. Hemos visto décadas de Transformación Digital en apenas un año. Se ha creado una nueva ola de servicios. Y hablar de servicios y de Transformación Digital es hablar de datos".

La cara oculta de este proceso de ultra-transformación acelerada "ha generado que la gran mayoría de las organizaciones no pueden hacer que sus sistemas de protección del dato sigan el ritmo de crecimiento de adopción de servicios cloud y de flexibilizar datos que están viviendo. Según nuestro informe anual de protección de datos, cerca del 23% de los servidores van a tener, al menos, una parada no planificada al año. Si a esto le sumamos el hecho de que el 37% de los trabajos de backup fallan, igual que el 34% de los trabajos de recuperación, tenemos que el 58% de las veces que tratamos de recuperar algo no podemos hacerlo. Las organizaciones no pueden permitirse no poder recuperar lo que necesitan seis de cada diez veces. Si añadimos el incremento de los ataques de ransomware, el efecto es devastador".

Según este responsable, "debemos tener en cuenta que vamos a sufrir un ataque, y que el coste de estos ataques se ha duplicado en un año, y no por el pago del rescate, sino por el tiempo de parada, la pérdida de negocio, los costes de reparación... Incluso pagando el rescate, de media, la pérdida de datos es del 35%".

PROTECCIÓN MODERNA DEL DATO

En palabras de Víctor Pérez de Mingo, "la única forma de enfocar la protección del dato es tener una protección de datos moderna. Con ello, las organizaciones tendrán cuatro resultados, modernizar los sistemas de backup y restauración, cumpliendo con los RPO y los RTO de las soluciones más críticas, mientras nos ayuda a reducir costes y la complejidad tradicional. En segundo lugar, nos puede ayudar a acelerar la adopción de servicios cloud (SaaS). Externalizar un servicio o llevarlo a la nube pública, no significa que mi dato esté protegido, y necesito tener un backup que me permita proteger ese dato esté donde esté. El tercer punto es tener una protección infalible contra el ransomware y la seguridad de que los datos que voy a restaurar están limpios antes de ponerlos de nuevo en producción. Y, en cuarto lugar, proporcionar la agilidad que necesitan las aplicaciones desplegadas en contenedores, con capacidades de migración nativa, backup y restauración en ese entorno".

Se mostraba satisfecho Víctor Pérez de Mingo por los resultados del último año, en España y en EMEA, y por el reconocimiento de las consultoras, algo que achacaba a "nuestra estrategia, basada en cuatro pilares: simplicidad, con una única protección para todo el entorno; flexibilidad, porque somos una solución definida con software sin ataduras con la infraestructura; fiabilidad, porque un backup no es fiable si no es recuperable; y potencia, porque nuestra solución nos ayuda a cumplir con los requisitos más exigentes en todas las soluciones".

Y recordaba que migrar a una solución como la de Veeam, "nos va a permitir reducir los costes de backup y recuperación en más de un 50%, tener un 83% menos de pérdida de disponibilidad, ayudar a contener los costes del almacenamiento, disminuir de la ventana de backup de forma considerable, o tener la garantía de que el 95% de nuestros clientes que han sido objetos de un ataque de ransomware han salido de él con coste cero." ■

CONTENIDO RELACIONADO

El Ayuntamiento de Vilafranca del Penedès impulsa la disponibilidad de servicios públicos clave con Veeam

El INTA amplía los límites de la investigación científica en los sectores aeroespacial, de seguridad y defensa, permitiendo el acceso ininterrumpido a los datos

JUAN RODRÍGUEZ, DIRECTOR GENERAL PARA ESPAÑA Y PORTUGAL DE F5

“LAS APLICACIONES Y EL DATO SON LOS PRINCIPALES ACELERADORES DE LA TRANSFORMACIÓN DIGITAL”

HACER QUE LA ADMINISTRACIÓN DIGITAL SEA MÁS ÁGIL Y CERCANA PARA LOS CIUDADANOS Y LOS FUNCIONARIOS, DEPENDE, EN GRAN MEDIDA, DE LAS APLICACIONES; HERRAMIENTAS QUE SE HAN CONVERTIDO EN HABITUALES PARA GESTIONAR DATOS E INTERACCIONES. PERO LA TRANSFORMACIÓN VA MÁS ALLÁ DE ESAS APLICACIONES.

“La Transformación Digital lleva ya tiempo en marcha, pero la era post-COVID ha acelerado muchas de las tendencias y de las necesidades que están sufriendo los clientes”, aseveró en su tiempo durante el Foro IT User: Administración pública, afrontando la década digital, Juan Rodríguez, Director General para España y Portugal de F5. “Ha habido muchos más servicios on-line y el tráfico digital se ha disparado, al igual que el uso del móvil para todo tipo de interacciones y acceso a servicios. Todas las empresas y los usuarios están inmersos en esta transformación, que no solo se apoya en la movilidad, sino que busca ofrecer una experiencia omnicanal, ofreciendo la misma calidad de uso independientemente de la plataforma y el dispositivo. Las aplicaciones y el dato son los principales aceleradores de la Transformación Digital”.

Un claro ejemplo de estas tendencias es que los consumidores “quieren una experiencia única de

LA TRANSFORMACIÓN DIGITAL ES ALGO MÁS QUE LA MODERNIZACIÓN DE LAS APLICACIONES, COMO EXPLICA EN ESTA PONENCIA JUAN RODRÍGUEZ (Clica en la imagen para ver el vídeo).

aplicación o de servicio, ya sea en su trabajo o en su vida personal, ya sea con un ordenador, un móvil o una tableta. El usuario busca esa experiencia omnicanal, ya sea en una interacción personal o digital. Por tanto, es esta tendencia la que está acelerando la Transformación".

LAS APLICACIONES SON CRÍTICAS PARA EL NEGOCIO

Según los datos que maneja F5, "un 98% de las organizaciones indica que las aplicaciones son críticas para su negocio, para su evolución y para la Transformación Digital. Pero sigue habiendo muchos retos, y este año hemos detectado que se ha incrementado la complejidad de la gestión de las aplicaciones en los clientes. Muchos de ellos no saben ni cuántas tienen ni qué problemas les están generando, porque su número está creciendo de forma desmesurada. Por otro lado, los ciberataques, o los acosos que se están produciendo a los datos, los usuarios o los accesos ha crecido más de un 300% en los últimos años. Además, no tienen suficiente visibilidad sobre los procesos ni la seguridad de los datos. En un entorno on-premise está todo más controlado, pero cuando empezamos a mover cargas a la nube la situación cambia, y la empresa debe asegurarse de contar con la seguridad necesaria. Por tanto, existen algunas lagunas que hay que solucionar".

Otra realidad que viven las empresas es "la convivencia de aplicaciones legacy con las nuevas aplicaciones ágiles que, normalmente, están en fuentes dispares, como el centro de datos tradicional, cargas de trabajo en la nube pública, y últimamente se apoyan en el extremo, en el Edge. Hablamos, por tanto, de un entorno multicanal y multicloud. Y todo esto, con arquitecturas que deben ser adaptativas, para poder construir aplicaciones más resilientes; y con la Inteligencia Artificial jugando un papel muy destacado en la ciberseguridad".

La estrategia "se ha acelerado con la pandemia, y los mecanismos y los procesos se están implementando de forma más rápida. Pero necesitamos disponer una capa de servicios de aplicación, independientemente de dónde resisa ésta, que permita mover la carga".

EL ROL DE LA IA

La Inteligencia Artificial, apuntó Juan Rodríguez, "es clave para la ciberseguridad. Tenemos que ser capaces de encontrar el equilibrio entre seguridad y experiencia de usuario. Las aplicaciones tienen que aprender a protegerse por sí mismas. Deben implementarse con el mínimo esfuerzo de operación, independientemente de dónde estén alojadas. Y, sobre todo, debe mantenerse a largo plazo. La seguridad debe estar totalmente unida al despliegue de la aplicación, y debe ir más allá de cerrar las típicas vulnerabilidades".

Desde F5, "proponemos una evolución en las aplicaciones, con seguridad desde el inicio, para poder implementarlas, con totales garantías, donde más me convenga. Con los mismos niveles de protección, ya sea en la nube pública o privada. Pero una arquitectura distribuida requiere una cloud distribuida, y necesitamos una herramienta que me permita abordar la gestión de la nube de forma más trasparente. Abogamos por la automatización en el despliegue de la aplicación, independientemente de dónde se alojen; acelerar las aplicaciones nativas en modo API; extender la seguridad al máximo al extremo; y tener una información perimetral para poder ser más predictivo y para permitir que la aplicación aprenda. Para todo esto, disponemos de una plataforma, Volterra, que, independientemente de dónde tenga el dato, qué tipo de aplicación utilice o qué tipo de despliegue haga, ofrece todos los mecanismos de seguridad desde el código hasta el usuario, mejorando la experiencia de uso en cualquier plataforma". ■

CONTENIDO RELACIONADO

Retos y prioridades del Sector Público en España ante la llegada de los fondos Next Generation EU

Soluciones de F5 para sector público

NUEVO

Kit de prevención de ransomware

Descubra cómo evitar, detectar y recuperar tras un ataque de ransomware.

- **White paper exclusivo**
- **Webinar de análisis en profundidad**
- **Versión de evaluación de 30 días gratuita**

http://vee.am/RansomwareES

SEVERINO GALA, DIRECTOR GENERAL DE MICROSTRATEGY PARA ESPAÑA Y PORTUGAL

"LAS ADMINISTRACIONES SE HAN ESFORZADO PARA CREAR DATA LAKES Y PONER CIERTO ORDEN Y CONCIERTO. LA SEGUNDA FASE ES LLEVAR ESE DATO A UN ENTORNO TOTALMENTE HETEROGÉNEO Y AMPLIO"

TANTO EN LA EMPRESA PRIVADA COMO EN EL SECTOR PÚBLICO, DISPONER DE INFORMACIÓN ES FUNDAMENTAL PARA LA TOMA DE DECISIONES, DE AHÍ QUE SEA ESENCIAL DEMOCRATIZAR EL ACCESO A LOS DATOS EN LAS ORGANIZACIONES PARA POTENCIAR SU VALOR EN LA TRANSFORMACIÓN DE LOS NEGOCIOS.

En su intervención en el Foro IT User: Administración pública, afrontando la década digital, Severino Gala, Director General de MicroStrategy para España y Portugal, repasó algunos de los datos del Informe DESI 2021, que analiza las capacidades digitales de todos los países miembros de la Unión Europea. En la edición de este año, indicaba, "España está situada en la parte alta de la tabla, tenemos buena nota. Se trata de un informe que tiene cuatro componentes principales: conectividad, donde nos sitúa en la tercera posición, porque el trabajo realizado por las operadoras y las empresas de telecomunicaciones ha sido muy potente y durante la pandemia lo hemos notado; también salimos bien parados en los servicios digitales, porque la Administración Pública ha hecho una buena labor; en el área del capital humano nos baja la calificación, al igual que en la integración de las tecnologías digitales dentro de

EL ACCESO A LA INFORMACIÓN ES EL PILAR FUNDAMENTAL DE LA TRANSFORMACIÓN DIGITAL, EXPLICÓ SEVERINO GALA EN SU PONENCIA (Clica para ver el vídeo).

este entorno. Y los que trabajamos en este sector vemos que los puntos donde fallamos son muy evidentes, porque, por ejemplo, nos cuesta muchísimo contratar a personas para todo el entorno del dato, analítica e inteligencia de negocio, y, por otro lado, la integración de la tecnología no es igual en todas las empresas y, dentro de éstas, el nivel de adaptación varía muchísimo. Y este es uno de los objetivos que tenemos que cubrir".

POTENCIAR LOS OBJETIVOS DE DIGITALIZACIÓN

Para Severino Gala, "el concepto de digitalización es tan sencillo como definir cómo somos capaces de llevar el dato desde la fuente a convertirlo en un valor operativo que alguien use y le saque rendimiento. Pero en su aplicación no es tan sencillo, y en el caso de la Administración Pública se complica más, porque el volumen de fuentes de datos es enorme. Las Administraciones han hecho mucho esfuerzo, y están trabajando en la creación de data lakes o data wharehouses para poner cierto orden y concierto en el dato que debe estar preparado para poder usarlo. Pero eso es solo la base. La segunda fase es llevar ese dato a un entorno totalmente heterogéneo y amplio, que, en el caso de la Administración Pública, hablamos de empleados públicos y ciudadanos, con lo que eso significa. En este punto, la tecnología tiene la misión de automatizar todos los procesos y el resto es cómo ser capaces de poner ese engranaje a funcionar, porque si una pieza falla, todo deja de funcionar. Y debe funcionar manteniendo las directrices de partida: el dato debe ser de calidad, estar verificado y ser válido. Y hay que tener en cuenta que ese uso operativo del dato va a depender mucho de la organización a la que se lo presentemos, el momento y el canal, y en todo ese entorno es donde la tecnología tiene un valor importante. El reto, por tanto, es ser capaces de combinar las piezas, simplificando en la medida de lo posible los procesos que hacen posible la digitalización".

EL VALOR DE LA TECNOLOGÍA

En el caso de MicroStrategy, "desde el origen nos dedicamos a convertir el dato en información útil, y planteamos el tratamiento del dato desde un punto de vista centralizado, o, lo que es lo mismo, combinar en un punto único las relaciones que definen cómo se van a organizar los datos, los usuarios y los canales. Esto aporta muchas ventajas: hacer definiciones únicas para toda la organización, y permite establecer de forma coordinada la seguridad y los niveles de acceso. Hay otro componente, más asociado a la arquitectura de la solución, ser capaz de funcionar de manera híbrida, manejando el dato en memoria y accediendo, a la vez, a la base de datos, lo que supone que la variedad de casos de uso es muy amplia y la escalabilidad, tanto a nivel de usuario como a nivel de dato es incremental y, además, permite optimizar y simplificar la infraestructura necesaria para cubrir una amplia variedad de datos.".

En este tiempo, comentó Severino Gala, "hemos sido pioneros a la hora de llevar la inteligencia de negocio a los móviles de manera nativa, lo que incrementó la digitalización, porque cubríamos casos de uso nuevo con usuarios que antes no tenían acceso".

De cara al futuro, este responsable apuntó que "si no innovas, estás muerto, y nuestro objetivo es ir cubriendo las necesidades que tienen nuestros clientes. Hemos visto también el gran trabajo de las Administraciones, y, en línea con este avance, hemos puesto sobre la mesa HyperIntelligence, que permite llevar información al entorno de trabajo desde cualquier fuente del dato, reduciendo los tiempos de acceso a la información, favorece la productividad y el grado de adopción es muy rápido". ■

CONTENIDO RELACIONADO

Hiperinteligencia: Tome decisiones más inteligentes y rápidas inyectando conocimientos en cada aplicación

Pasar de hiperinteligente a hiperproductivo

PEDRO ÁLAMO DE LA GALA, SENIOR NAMED ACCOUNT MANAGER DE PROOFPOINT

“TODAS LAS AMENAZAS SE DIRIGEN A LAS PERSONAS Y NECESITAN LA INTERVENCIÓN HUMANA. ES FUNDAMENTAL LA CONCIENCIACIÓN”

UN VECTOR DE ATAQUE QUE SUFREN LAS ORGANIZACIONES, YA SEAN DEL SECTOR PRIVADO O DE LA ADMINISTRACIÓN PÚBLICA, ES EL CORREO ELECTRÓNICO. DE HECHO, SEGÚN LOS DATOS QUE MANEJA PROOFPOINT, EL 94 POR CIENTO DE LAS AMENAZAS LLEGAN A LAS ENTIDADES A TRAVÉS DE ESTA VÍA. SIN EMBARGO, EL PORCENTAJE DEL PRESUPUESTO DE SEGURIDAD DEDICADO A ATAJAR ESTE PROBLEMA SIGUE SIENDO ESCASO.

La reducción de riesgos con seguridad centrada en personas fue el tema que abordó Pedro Álamo de la Gala, Senior Named Account Manager de Proofpoint, en el Foro IT User: Administración pública, afrontando la década digital. La compañía analiza desde sus sistemas la quinta parte del correo mundial al día: “Lo que estamos viendo es que todas las amenazas se dirigen a las personas y necesitan la intervención humana. El actor malicioso es una organización que busca una recompensa, normalmente financiera, y están viendo cómo comprometer nuestras cuentas y, a partir de ahí, nuestras organizaciones, pero muchas de estas están viendo la seguridad desde un punto de vista estratégico de la infraestructura. Viendo cómo proteger las aplicaciones y los servidores, pero se olvidan de hacerlo con las personas”.

LA PONENCIA DE PROOFPOINT SE CENTRÓ EN LA REDUCCIÓN DE RIESGOS CON SEGURIDAD CENTRADA EN LAS PERSONAS (Clica en la imagen para ver el vídeo).

Con datos de las consultoras en la mano, Álamo explicó que “el 94% de las brechas de seguridad de los clientes provienen del correo electrónico, pero apenas se dedica un 10% del presupuesto de seguridad a protegerlo, y ésta es una vulnerabilidad que los actores maliciosos están atacando. Y lo están haciendo con dos herramientas, fundamentalmente, las de suplantación de identidad, ya sea mediante la suplantación de dominio o bien cambiando el nombre del usuario, o aquellas que aspiran a convertirse en el usuario, ya sea por ataques de contraseña, phishing, malware, para infectar una cuenta y moverse de forma lateral por las organizaciones”.

PROTECCIÓN DEL CORREO...

La propuesta de Proofpoint para atajar estos problemas pasa por “la protección del correo y la concienciación. Hablando de la primera, se entiende en tres fases: primero, prevención, mediante la solución de Email Protection; segundo, detección, mediante nuestra solución Targeted Attack Protection (TAP), que analizará los archivos y URL maliciosas y cuenta con herramientas de detección de ataques; y, tercero, remediación, con la solución TRAP, con la que vamos a ayudar a los SOC a optimizar su tiempo y emplearlo en labores a las que deberían dedicarlo. A una solución de correo, desde el punto de vista de Proofpoint, le pedimos que sea efectiva y que nos proporcione visibilidad. Si hablamos de efectividad, lo mejor es hacer una auditoría de la realidad del cliente, y si ponemos un ejemplo de un caso real, de un cliente cuyo firewall de correo dejaba pasar 16,3 millones de mensajes, nuestra solución de prevención bloqueó más del 50% de los mensajes por reputación del dominio y otros 500.000 por contenido; nuestra solución de amenazas avanzadas detectó 1.200 amenazas en archivos adjuntos y 6.000 escondidas en URLs, con lo que paramos casi el 60% del correo que nuestra competencia ha entregado. Mientras, si hablamos de visibilidad, nuestras herramientas permiten definir quiénes son los usuarios más atacados en base al número de ataques, los privilegios que tengan y las vulnerabilidades que detectemos. Esta información nos permite tener una visión clara para poder definir las estrategias de seguridad para un usuario o para toda la organización”.

...Y CONCIENCIACIÓN

Destacó Pedro Álamo de la Gala que “los ataques necesitan la activación humana, y por eso es fundamental la concienciación. Si tenemos a nuestros usuarios formados e informados, y saben discernir cuándo un mensaje es malicioso, serán menores las posibilidades de que nuestras organizaciones se vean comprometidas. De ahí, nuestras soluciones de concienciación. Es importante definir quién recibe qué información y cuándo. Hablamos de soluciones formativas de menos de diez minutos para que el usuario se sienta cómodo con ellas. Nuestra metodología se basa en tres fases: identificación del riesgo del usuario, asignación de los módulos correspondientes a los usuarios que hayan caído en una vulnerabilidad, y hacerles partícipes de la seguridad de la organización mediante el botón de phishing alarm, un plug-in en su correo. Se trata de formar y educar a los usuarios para evitar que caigan en las amenazas”.

SUPLANTACIÓN DE DOMINIOS

Una amenaza que está de moda es la suplantación de dominios. Este responsable aseguró que “muchos usuarios caen en estas estafas, porque las entidades supuestamente emisoras de los correos no tienen implementados los protocolos adecuados. Desde Proofpoint facilitamos gran parte de este trabajo de implantación de DMARC de forma automática para facilitar la labor de los responsables”. ■

JUAN FERNANDO MUÑOZ, SECRETARIO GENERAL DE SALUD DIGITAL

“LA TRANSFORMACIÓN DIGITAL DEL SECTOR SANITARIO NO DEBE SER UNA MERA CUESTIÓN DE CAMBIO TECNOLÓGICO”

SEGÚN LA BRÚJULA DIGITAL, QUE ESTÁ MARCANDO EL RUMBO DE LA DIGITALIZACIÓN EN LA UNIÓN EUROPEA, PARA 2030, TODOS LOS SERVICIOS PÚBLICOS CLAVE DEBERÍAN ESTAR DISPONIBLES EN LÍNEA Y, ADEMÁS, TODOS LOS CIUDADANOS DEBERÍAN PODER ACCEDER A SU HISTORIAL MÉDICO DE MANERA ELECTRÓNICA.

Juan Fernando Muñoz, Secretario General de Salud Digital, habló de las iniciativas de Transformación Digital en el ámbito de la Sanidad que se están llevando a cabo, en el Foro IT User: Administración pública, afrontando la década digital. Tal y como explicó, “estamos trabajando en la Estrategia de Salud Digital. Centramos ahí todos nuestros esfuerzos. Para nosotros, la digitalización es algo transversal, y su capacidad de transformación en cualquier sector concreto es incremental por su ubicuidad e inmediatez y la posibilidad de prestar servicio desde dispositivos comunes como los teléfonos o las tabletas. La Sanidad es, sin duda, uno de los sectores con mayor capacidad de mejora con la incorporación de las tecnologías digitales, como señalan desde hace años la OMS, la OCDE o la Unión Europea”.

Al hablar de la transformación digital “estamos hablando de un cambio fundamental en las organizaciones, de una renovación de los métodos de trabajo

JUAN FERNANDO MUÑOZ EXPUSO LAS CLAVES DE LA ESTRATEGIA NACIONAL DE SANIDAD DIGITAL (Clica en la imagen para ver el vídeo).

y de una evolución en los modelos de relación internos y externos gracias a la implementación de las nuevas tecnologías. Esto supone variar el enfoque, porque la tecnología no es un mero facilitador sin plantearnos qué, cómo y para qué hacemos las cosas, o incluso si es necesario seguir haciéndolo. La tecnología, por sí, sola, no produce una transformación digital. Hay que reorientar la organización para aprovechar el potencial de las tecnologías, y esto sí es lo que producirá esta transformación. Por eso, todos los componentes de la organización deben ser conscientes de los retos planteados, que en el caso de la Sanidad son muchos".

La pandemia, apuntó Juan Fernando Muñoz, "ha puesto de manifiesto la necesidad de cambiar muchos elementos para estar en condiciones de afrontar situaciones como las que hemos vivido. En especial, la necesidad de reforzar la atención primaria, como núcleo de los sistemas sanitarios; el carácter crítico de la información y los datos; así como la importancia de incrementar la sostenibilidad, la resiliencia y la equidad del conjunto, como garantía de la salud de todas las personas".

PALANCAS PARA EL CAMBIO

Para este responsable, "las tecnologías digitales son una de las palancas más potentes para contribuir a alcanzar estos resultados, pero su aplicación en el conjunto del Sistema Nacional de Salud requiere una estrategia de alcance nacional. La transformación digital del sector sanitario no debe ser una mera cuestión de cambio tecnológico, sino que ha de incorporar un cambio adaptativo en las actitudes y habilidades humanas, así como en los marcos legales, la organización del trabajo asistencial y de gestión, para dar respuesta a los retos que enfrentan los sistemas sanitarios".

"LA TECNOLOGÍA, POR SÍ, SOLA, NO PRODUCE UNA TRANSFORMACIÓN DIGITAL. HAY QUE REORIENTAR LA ORGANIZACIÓN PARA APROVECHAR EL POTENCIAL DE LAS TECNOLOGÍAS, Y ESTO SÍ ES LO QUE PRODUCIRÁ ESTA TRANSFORMACIÓN"

Es por esto por lo que desde el Ministerio de Sanidad "hemos trabajado con todas las comunidades autónomas en el desarrollo de esta Estrategia Nacional de Salud. Esta estrategia busca alinear las iniciativas de transformación digital de todo el país con la propia sanidad. Aborda la estrategia de transformación del Sistema Nacional de Salud como un paso fundamental para alcanzar una atención preventiva, diagnóstica y terapéutica centrada en el paciente, y que contribuya al objetivo esencial: la salud de las personas".

Esta estrategia parte de alinear "con las que ya habían sido publicadas, como la Estrategia de España Digital, la de Inteligencia Artificial, la de Política Industrial, la de Medicina Personalizada y la Estrategia Española de Ciencia, Tecnología e Innovación, además de los programas europeos Digital Europe for Health y Horizonte Europa. A partir de ahí, con diferentes grupos de trabajo, creamos un borrador, que es el que llevamos a aprobación".

El objetivo de esta estrategia es, en palabras del Director de Salud Digital, "ser un espacio común donde desarrollar estas iniciativas de transformación digital sobre el sector de salud, y para ello, se basa en unos principios rectores, los del propio Sistema Nacional de Salud, autonomía de los pacientes, desarrollo de los profesionales y la transformación digital de forma sistémica. Buscamos capacitar e implicar a las personas en el estado de su salud; hacer más eficientes y mejores los procesos e instrumentos que les damos a los profesionales sanitarios; adecuar el progreso del sistema sanitario a la sociedad, que tiene un gran foco en la innovación y en la denominada Medicina 5P (Poblacional, Preventiva, Predictiva, Participativa y Personalizada); y contar con información de calidad e interoperable mediante la creación de un espacio de datos de salud, para generar el conocimiento clínico y científico y la evaluación y mejora de los servicios médicos. Todo ello apoyado en tres líneas transversales que deben estar presentes en todos los proyectos,

como son el impulso de la analítica avanzada de datos, el refuerzo de la interoperabilidad de la información sanitaria a nivel nacional e internacional, y el desarrollo de los servicios sanitarios digitales e inteligentes".

MODELOS ORGANIZATIVOS Y DESARROLLO DE PROYECTOS

Esta estrategia busca alinear la transformación con el resto de actuaciones "y esto es así porque en nuestra organización, en materia de competencias, la estrategia debe definir los modelos organizativos que permitan el desarrollo de los proyectos de la manera más adecuada. En este caso, teniendo en cuenta el esquema competencial en España, tenemos tres modelos de ejecución en función de las áreas que se han identificado con los diferentes agentes. Los modelos donde aplicaremos los fondos son, por una parte, aquellos en los que ya veníamos trabajando con las comunidades, y en los que el Ministerio asume la ejecución con la participación de las comunidades, algunos mediante la compartición de información y otros porque no se pueden crear, como la receta electrónica interoperables. Estas iniciativas nos permiten obtener el máximo beneficio para todo el Sistema Nacional de Salud y para la sociedad en su conjunto. El segundo modelo es la ejecución colaborativa con las comunidades lideradas o coordinadas por el Ministerio, con lo que buscamos convertir la fragmentación del sistema en una ventaja, aprovechando lo mejor de cada una para llevarlo al resto. Y, finalmente, una serie de proyectos con una competencia conjunta que no se pueden hacer de otra manera, como puede ser la vigilancia epidemiológica. Es en estas tres áreas donde la combinación de presupuestos del Ministerio de Sanidad y los fondos europeos, nos permitirán empezar a trabajar en proyectos que consideramos más prioritarios, donde destacan los relacionados con el refuerzo del Sistema Nacional de Salud, incluyendo ese espacio de datos del Sistema Nacional de Salud, la historia clínica interoperable, o la receta electrónica interoperable que permitió, durante el período más duro del confinamiento, a más de 200.000 personas recibir su medicación fuera de la comunidad autónoma de su residencia habitual. Asimismo, también los proyectos destinados a impulsar los centros sanitarios digitales y la atención personalizada a colectivos específicos, como pacientes crónicos, pluripatológicos o residentes en áreas remotas. Por último, el desarrollo de un nuevo sistema de vigilancia de amenazas sanitarias con el que estamos plenamente comprometidos".

Todas estas actuaciones se articulan en torno a un conjunto "de reformas e instrumentos de colaboración para transformar la cadena de valor del sector. En concreto, recientemente se ha publicado el anteproyecto de ley por el que se modifican ciertas normas para consolidar la equidad, universalidad y cohesión del Sistema Nacional de Salud como un instrumento fundamental de estas reformas a las que la tecnología debe dar soporte, así como el PERTE de Salud en Vanguardia del que somos co-ponentes como uno de estos elementos fundamentales. En todos estos proyectos, la participación e implicación del personal TIC es clave en el éxito. Debemos ser catalizadores en la incorporación de estas tecnologías al servicio de la salud de las personas y facilitadores del uso de las mismas por parte de los profesionales y de los pacientes. Podemos y debemos aspirar a que las mejoras que la tecnología puede aportar lleguen a todas las personas, reforzando la sostenibilidad, equidad y cohesión, que son señas de identidad de nuestro Sistema Nacional de Salud, garantizando, a la vez, la privacidad de los pacientes y el uso seguro y ético de los datos, en beneficio de toda la sociedad. Debemos aspirar a que nuestro trabajo contribuya a transformar el Sistema Nacional de Salud, incrementando la calidad de la atención sanitaria, porque eso supondrá aumentar la calidad de vida de todos los ciudadanos". ■

CONTENIDO RELACIONADO

Foro IT User: Administración pública, afrontando la década digital

Retos y Prioridades del Sector Publico

ante la llegada de los Fondos NextGen EU

DESCARGAR INFORME →

LEONOR TORRES MORENO, VICEPRESIDENTA DE ASTIC

“ES MUY IMPORTANTE CONTAR CON UN DIRECTIVO PÚBLICO CON CAPACIDADES DIGITALES”

EUROPA NECESITA CIUDADANOS EMPODERADOS Y CAPACITADOS DIGITALMENTE, UNA FUERZA DE TRABAJO CON MÁS HABILIDADES DIGITALES Y UN MAYOR NÚMERO DE EXPERTOS TIC. CONTAR CON ESTAS CAPACIDADES DIGITALES EN FUNDAMENTAL PARA CONECTAR CON LA SOCIEDAD ACTUAL. POR ESO, LA COMISIÓN EUROPEA SE HA PROPUESTO DOS OBJETIVOS PARA 2023: QUE EL 80% DE LOS ADULTOS EUROPEOS CUENTEN CON ESAS HABILIDADES Y QUE AL MENOS HAYA 20 MILLONES DE EXPERTOS TIC CONTRATADOS EN LA UE ENTRE HOMBRES Y MUJERES.

En su ponencia en el Foro IT User: Administración pública, afrontando la década digital Leonor Torres Moreno, Vicepresidenta de ASTIC, explicaba que la pandemia “ha mostrado la necesidad de estar conectados con la tecnología, y ha evidenciado la brecha digital que tenemos que afrontar. La capacitación digital es un factor clave que debemos aprovechar para transformarnos y hacer que nuestro país progrese económicamente, seamos más productivos y limitemos las desigualdades. Esta capacitación es una prioridad clave del Plan de Recuperación, Transformación y Resiliencia”.

LA SITUACIÓN ACTUAL

Pese a que es un reto por afrontar, lo cierto es que no partimos de cero. Tal y como explicaba Leonor Torres, “hasta la fecha hemos conseguido ciertos logros. En

LEONOR TORRES MORENO EXPLICA LOS LOGROS Y RETOS DE LA CAPACITACIÓN DIGITAL EN EL ENTORNO PÚBLICO (Clica en la imagen para ver el vídeo).

plena pandemia, fuimos capaces de absorber todo el incremento que hubo de servicios digitales, ya sea de acceso a la carpeta ciudadana o autenticaciones y firmas. Pero no solo eso. España está a la cabeza del mundo en ciberseguridad, con el cuarto puesto a nivel mundial y el segundo a nivel europeo. En el Informe DESI 2021 hemos mejorado, pasando del puesto 11 en 2020 al puesto 9, por encima de la media del resto de países de la Unión Europea. En conectividad hemos mejorado, pasando de un puesto 5 al tercer lugar, pese a que no somos un país pequeño ni de orografía homogénea. En cuanto a la integración de tecnología digital, estamos en el puesto 16, justo en la media. Es verdad que nuestras PYMES han hecho un esfuerzo importante, pero necesitan incorporar nuevas tecnologías para ser más productivos. En lo referente a servicios públicos digitales, tenemos la séptima posición, muy por encima de la media. Somos también el segundo puesto del ranking en Europa en datos abiertos. Y, por último, en el índice de capital humano, estamos en el puesto 12, pero tenemos margen de mejora tanto en especialistas TIC como en mujeres especialistas TIC. En el ranking de la UE de mujeres en el mundo digital, ocupamos la octava posición, por encima de la media, y, si vemos áreas de mejora, vemos graduados STEM y especialistas TIC, donde nos alejamos de la media de Europa y de las cifras de nuestros colegas varones. Es verdad que Europa tiene que hacer un esfuerzo por mejorar, y lleva tiempo haciéndolo".

Si ponemos el foco en los datos de la AGE, Leonor Torres indicaba que "la plantilla es bastante numerosa, pero los TIC son una minoría y la carga de trabajo es muy alta. También se pone de manifiesto la brecha de género. Si lo comparamos con otros cuerpos, en concreto, el cuerpo TAC, vemos que sí se han incorporado mujeres, pero en los TIC sigue existiendo una brecha de género. La diferencia es notoria en todos los niveles".

UNA GRAN OPORTUNIDAD

Los planes de digitalización actuales suponen "una gran oportunidad. Entre ellos, destaca el Plan Nacional de Competencias Digitales, muy completo y multidisciplinar, que abarca todos los aspectos de las competencias digitales, incluyendo a los empleados. Dispone de una línea transversal para luchar contra la brecha de género, porque las matriculadas en carreras tecnológicas descendieron un 3% entre 2013 y 2017, y más de la mitad de ellas no se gradúan, lo que provoca que hay muy pocas especialistas TIC que apenas llegan a altos cargos en las empresas. También hay que recordar que los empleos más amenazados por la automatización son los ocupados por mujeres, por lo que hay que hacer un esfuerzo para integrar a las mujeres en este mundo TIC, porque algunos informes estiman que incorporar este talento femenino podría incrementar el PIB español en 200.000 millones de euros".

Si hablamos de las personas a servicio de las Administraciones Públicas, "tenemos mucha experiencia, pero han surgido nuevas competencias que hay que incorporar, además del envejecimiento del colectivo, porque más de la mitad se habrá jubilado en 10 años, lo que sería una gran pérdida de conocimiento".

Cuando Leonor Torres hablaba de especialistas digitales, destacaba que hay "un número insuficiente de ellos. Es necesario que se adapten los planes de estudio con los nuevos perfiles y tecnologías. Es curioso que también hay cierto envejecimiento en este nivel y sigue creciendo la demanda de estos perfiles en las empresas, de ahí la importancia de la colaboración público-privada en este terreno".

Las competencias digitales "se han estandarizado en el Marco Europeo, lo que nos ayuda a identificar los componentes de estas competencias para integrarlo en el currículo". ■

CONTENIDO RELACIONADO

ASTIC

Informe DESI (Economía y Sociedad Digital) España 2021

JOSÉ MIGUEL MUÑOZ, DIRECTOR DEL FORO DE COLABORACIÓN PÚBLICO-PRIVADA

FONDOS EUROPEOS: SISTEMA DE GESTIÓN Y CONTROL DE LOS FONDOS DEL PLAN DE RECUPERACIÓN Y RESILIENCIA

LA FINANCIACIÓN NECESARIA PARA AVANZAR EN EL CAMINO DE LA DIGITALIZACIÓN Y LA TRANSFORMACIÓN DE LAS ADMINISTRACIONES PÚBLICAS SE VA A VER INCREMENTADA CON LOS FONDOS NEXT GENERATION PROVENIENTES DE EUROPA, DE LOS QUE SEGUIMOS CONOCIENDO NOVEDADES.

En su ponencia en el Foro IT User: Administración pública, afrontando la década digital José Miguel Muñoz, Director del Foro de Colaboración Público-Privada (Foro CPP), repasó las novedades surgidas de la última Orden Ministerial, lanzada a finales de septiembre, para la regulación, por parte de las Administraciones Públicas, de la gestión de los fondos económicos que van a llegar. En palabras de este responsable, "el objeto de esta orden es configurar y desarrollar un sistema de gestión que ayude a las Administraciones Públicas decisoras y ejecutoras en todo lo relacionado con la gestión del Plan de Recuperación, Transformación y Resiliencia, y su ámbito de actuación incluye a todas las entidades del sector público".

La orden, según detalló el Director del Foro CPP, "habla de cuatro conceptos importantes: Entidad Decisora, aquella que decide y tiene un papel menos ejecutor; Entidad Ejecutora, que tiene un rol

DESDE EL FORO DE COLABORACIÓN PÚBLICO-PRIVADA EXPLICARON EL SISTEMA DE GESTIÓN Y CONTROL DE LOS FONDOS DEL PLAN DE RECUPERACIÓN Y RESILIENCIA (Clica en la imagen para ver el vídeo).

más táctico a la hora de actuar directamente sobre los fondos; Órgano Responsable, con la responsabilidad de vigilar la correcta ejecución de los fondos; y Órgano Gestor; con el papel de gestionar la ejecución. Por tanto, hay una autoridad responsable de los fondos, la Secretaría General de Fondos Europeos; unas entidades decisoras, principalmente los departamentos ministeriales; y dos órganos de gestión que tienen diferentes funciones dependiendo de cuál sea cada uno".

PRINCIPIOS DE OBLIGADA EJECUCIÓN

La citada Orden Ministerial marca 7 principios que son de obligada ejecución. En palabras de José Miguel Muñoz, "en primer lugar, tenemos el concepto de hito y objetivo. Es importante diferenciar que siendo Entidad Decisora o Entidad Ejecutora existen diferentes hitos y objetivos, pero es necesario, para asegurar la correcta ejecución del plan y poder hacer seguimiento de las actuaciones del mismo, definirse, a cualquier nivel, hitos de gestión, hitos críticos e hitos no críticos. Los críticos vienen relacionados con las decisiones e indicaciones del Consejo de Europa, mientras que los no críticos están más asociados a actuaciones más tácticas y operativas. Las entidades tienen la capacidad de definir hitos, validar que se están cumpliendo y reportar el cumplimiento de los mismos. Tendrá que haber un sistema informático para que todos los participantes incluyan toda la información relacionada con la ejecución y gestión de los fondos".

El segundo concepto de la Orden es "la necesidad de definir el grado de etiquetado verde y etiquetado digital. El tercer aspecto es el Análisis de Riesgo Negativo Significativo en el Medio Ambiente, DNSH por su denominación en inglés. La Orden incorpora un test de autoevaluación de impacto medioambiental y referencias para que las entidades puedan medir el impacto a nivel de proyecto o subproyecto. Asimismo, incorpora un anexo para que sea firmado por los adjudicatarios de las ejecuciones".

Continuó José Miguel Muñoz con el cuarto punto de la Orden, "el que más dudas está generando, que es la necesidad de disponer de un mecanismo de medidas antifraude. Se trata de un plan obligatorio que debe contener cuatro aspectos que marca la Orden: prevención, detección, corrección y persecución. Tienen que definir las maneras de actual y todo lo relacionado con conflictos de interesas y gestión del fraude. El plan debe, por tanto, ser propio de cada entidad, definir el punto de partida, definir los roles de los actores que van a participar, y cumplir con los cuatro aspectos señalados en la orden, que da 90 días de plazo desde la emisión de la propia orden o desde que la entidad sea consciente de que va a recibir los fondos. Ahora mismo hay mucha incertidumbre que puede impactar en la planificación de los fondos, con lo que serían de agradecer unas directrices básicas para estos planes".

Otro aspecto que incluye la orden es "la compatibilidad con el régimen de ayudas del Estado, algo más conocido por las diferentes entidades. Sin embargo, el sexto aspecto vuelve a ser un punto complejo, la necesidad de recoger por parte de las entidades hasta el más mínimo nivel de quiénes van a ser los beneficiarios últimos de los fondos, incluyendo los proyectos que ya se estaban ejecutando antes de la propia Orden. Y, por último, el punto relacionado con la comunicación". ■

CONTENIDO RELACIONADO

Foro IT User: Administración pública, afrontando la década digital

Foro de Colaboración Público – Privada. Grupo en LinkedIn

Fondos europeos: sistema de gestión y control de los fondos del Plan de Recuperación y Resiliencia

OPINIÓN

LOS EQUIPOS DE TI TRABAJAN BAJO PRESIÓN FRENTE A LA BATALLA CONTRA LA AVALANCHA DE ALERTAS CONTINUAS

JOSÉ MATIAS

REGIONAL DIRECTOR PARA IBERIA DE DYNATRACE

Las organizaciones de todo el mundo están en pleno proceso de transformación digital y trabajando para ofrecer experiencias más satisfactorias a los clientes. Para ello, necesitan llevar a cabo innovaciones constantes y de forma rápida para satisfacer sus expectativas.

Conseguir este objetivo requiere migrar cada vez más servicios a entornos híbridos nativos de la nube. Estos ecosistemas dinámicos brindan un nivel notable de agilidad a las organizaciones, pero también introducen niveles de complejidad sin precedentes. De hecho, investigaciones recientes demuestran que administrar toda esta complejidad supera las capacidades humanas.

Los equipos de TI reciben un constante bombardeo de alertas de rendimiento y disponibilidad que deben de investigar para identificar y resolver posibles problemas antes de que afecten el rendimiento de los servicios y reduzcan la satisfacción de los usuarios y clientes. Ante un volumen tan alto de alertas, los equipos de TI invierten un promedio del 15% de su tiempo tratando de identificar en cuáles deben centrarse. Esto les cuesta a las organizaciones una media anual de 1.5 millones de dólares, incluso antes de ponerse a resolver el problema.

UN FUTURO COMPLEJO

Gran parte del desafío al que se enfrentan los actuales equipos de TI radica en el hecho de que las aplicaciones que se ejecutan en los ecosistemas de nube empresariales son enormemente complejas, con cientos de tecnologías, millones de líneas de código y miles de millones de dependencias entre ellas. Todo esto está produciendo un volumen, velocidad y variedad de datos de monitorización y alertas de rendimiento sin antecedentes y los métodos tradicionales de monitorización de aplicaciones ya no son suficientes para dar sentido al volumen de datos y proporcionar el nivel de observabilidad que los equipos de TI necesitan para administrar el rendimiento del servicio de manera efectiva.

En gran parte, este desafío se debe al hecho de que los sistemas de monitorización tradicionales generalmente operan de manera aislada. El resultado es que envían miles de alertas individuales que carecen del contexto más amplio de lo que está ocurriendo en todo el stack. Por lo tanto, los equipos de TI reciben un gran número de falsos positivos y alertas duplicadas que deben ser analizadas antes de poder continuar con el trabajo de resolver problemas.

Los equipos de TI, enfrentados a este constante aluvión de datos e incapaz de enfocarse de inmediato en problemas de rendimiento genuinos, dedican cada vez más tiempo a determinar hacia dónde deben dirigir sus esfuerzos y esta tarea se vuelve aún más engorrosa por el hecho de que la mayoría de las alertas son irrelevantes, tan sólo el 26% de estas requiere acción según afirman los propios responsables de estos departamentos.

AHOGARSE EN TORMENTAS DE ALERTA

Ordenar los falsos positivos, los duplicados y las alertas de baja prioridad de los problemas genuinos es un proceso lento y propenso a errores. Esto significa que los equipos de TI tienen menos tiempo para tareas más importantes, como identificar la causa raíz de los problemas de rendimiento y solucionarlos antes de que los clientes o usuarios finales sufran interrupciones en el servicio. En la era actual del cliente, donde tenemos muchas opciones y oportunidades para cambiar a un servicio alternativo en un abrir y cerrar de ojos, esto puede conducir a una pérdida de ingresos y perjudicar el resultado final para las organizaciones. Los usuarios esperan una experiencia digital perfecta y, para poder ofrecerla, los equipos de TI deben poder mantener la capacidad de observación de extremo a extremo. Sólo así podrán gestionar eficazmente sus entornos de TI cada vez más complejos, con la capacidad de identificar y resolver problemas de rendimiento antes de que se vea afectada la calidad del servicio.

Claramente, el estatus quo es insostenible, y se necesita un cambio radical para aliviar la presión sobre los equipos de TI. Los recursos críticos que los equipos están actualmente desperdiciando en la clasificación de miles de alertas de rendimiento deben ser redirigidos hacia una gestión de rendimiento efectiva y para impulsar experiencias digitales sin interrupciones. Algunas organizaciones están intentando resolver el problema actualizando sus herramientas, pero es una opción limitada ya que estas herramientas no se crearon para la naturaleza dinámica de los entornos de nubes múltiples. Domar la complejidad de estos ecosistemas requiere un cambio que va más allá de confiar sólo en las capacidades humanas.

OPERACIONES IMPULSADAS POR IA

Las organizaciones necesitan hacer la transición de operaciones a la nube impulsadas por la inteligencia artificial para controlar sus entornos complejos y seguir teniendo éxito en un mundo centrado en la experiencia del usuario. La combinación de esto con un enfoque global de datos comunes que rompe los silos entre los datos de monitorización ofrecien-

“LAS EMPRESAS DE HOY NECESITAN HACER UN CAMBIO DECISIVO HACIA LAS OPERACIONES EN LA NUBE IMPULSADAS POR IA QUE BRINDAN INFORMACIÓN PROCESABLE SOBRE EL RENDIMIENTO DE SUS APLICACIONES Y EL IMPACTO EN EL USUARIO FINAL”

do un soporte mucho mejor para los equipos de TI, brindándoles respuestas precisas y totalmente contextualizadas a los problemas de rendimiento, en lugar de más datos y alertas. Esto allanará el camino hacia aplicaciones de auto reparación automática mediante la automatización de la entrega continua de actualizaciones y los procesos operativos.

En última instancia, los líderes de TI y de empresas deben abordar la insuficiencia de los sistemas de monitorización tradicionales que están ahogando a los departamentos de TI en alertas implacables. Las empresas de hoy necesitan hacer un cambio decisivo hacia las operaciones en la nube impulsadas por IA que brindan información procesable sobre el rendimiento de sus aplicaciones y el impacto en el usuario final. Sólo así podrán ofrecer experiencias digitales sin problemas en medio de la complejidad de la nube empresarial y seguir siendo competitivos en un mundo centrado en el cliente. ■

SI TE HA GUSTADO ESTA REVISTA, COMPÁRTELA

HYPERINTELLIGENCE®

Las respuestas
le encontrarán

MicroStrategy®
Intelligence Everywhere

CLAVES TECNOLÓGICAS PARA LA GESTIÓN DE LOS PLANES DE RECUPERACIÓN

JESÚS GALINDO

VICEPRESIDENTE
DE SECTOR PÚBLICO DE
SALESFORCE IBERIA

La crisis económica derivada de la crisis sanitaria de Covid-19 ha llevado a la creación de un plan de recuperación europeo sin precedentes (NextGenerationEU), que cuenta con un presupuesto de más de 800.000 millones de euros. En cada país de la Unión Europea, los gobiernos están diseñando sus estrategias para aprovechar estos fondos, que en España se articulan a través del Plan de Recuperación, Transformación y Resiliencia.

Además de los planes nacionales que se sustentan sobre la estrategia europea, las administraciones públicas de todos los niveles (estatal, autonómico y municipal) están desarrollando planes para fomentar su propia digitalización y ayudar a la digitalización de las empresas.

Para desplegar con éxito estos planes excepcionales de recuperación, las administraciones públicas deben contar con las herramientas tecnológicas adecuadas que les permitan simplificar los procesos complejos y garantizar la coordinación a gran escala de los actores implicados. De lo contrario, las estrategias podrían no dar los frutos deseados, embarrancando en un mar de trámites y burocracia o resultando en financiación de proyectos que realmente no impulsen la recuperación. Veamos con más detalle algunos factores clave del éxito.

CONTROLAR LA COMPLEJIDAD

Casi todos los actores públicos y privados están preocupados por esta necesidad de recuperación y transformación, ya sean proveedores de ayuda u organizaciones con derecho a recibirla. Dominar la complejidad resultante de la gestión y la coordinación es en sí mismo un gran desafío.

El éxito depende de la claridad de la financiación, las responsabilidades y las condiciones. Por eso es importante comunicar y ofrecer una experiencia fluida a los usuarios que deseen solicitar y recibir la aprobación de la financiación. Una buena financiación es una financiación utilizada y, desgraciadamente, hay precedentes en muchos países europeos de fondos que no han sido adecuadamente asignados o simplemente no han sido utilizados.

En este caso concreto, es importante entender que los destinatarios de los fondos son, en muchos casos, gestores y directivos de pequeñas y medianas empresas que no pueden dedicar muchos recursos ni tiempo de trabajo de sus empleados a completar complejos formularios o entender detalles técnicos de los procesos. El diseño de todo el sistema debe estar centrado en las necesidades y nivel de conocimiento de estas organizaciones y ciudadanos, es decir, es necesario un diseño sencillo que no implique un amplio conocimiento de procesos y normativas por parte de los ciudadanos.

GESTIÓN DE TODOS LOS ASPECTOS DEL PLAN DE RECUPERACIÓN

Para gestionar este gigantesco sistema, es necesario prever una gobernanza que permita la coordinación entre los actores nacionales y locales, y entre los actores públicos y privados. Los indicadores deben garantizar el

seguimiento de las medidas: su buen destino, su impacto a largo plazo, el retorno de la inversión, sus efectos en la contratación... El objetivo es controlar el buen uso de los fondos públicos.

Como en la mayoría de los casos de uso digital de hoy en día, y en particular en el sector público, es muy recomendable apostar por tecnologías que permitan un rápido despliegue a gran escala. Es indudable que las soluciones en la nube son preferibles a la hora de realizar estos nuevos despliegues, sobre todo teniendo en cuenta que es perfectamente viable, mediante conectores y reglas basadas en API, integrar esta capa de soluciones en la nube –que funcionaría como el front-end de cara a los ciudadanos- con los sistemas existentes donde residen los datos y las aplicaciones back-end de las administraciones públicas.

Desde las empresas tecnológicas estamos ofreciendo incluso a las administraciones públicas soluciones concretas para la gestión de ayudas y subvenciones. En el caso de Salesforce, nuestra solución, desarrollada a nivel mundial durante la crisis internacional, consiste en una completa plataforma de gestión de los procesos de solicitud de fondos y distribución de ayuda. Esta solución se basa en un motor de reglas que es esencial en un mundo tan complejo como el de la financiación pública. También incluye instrumentos de colaboración entre los distintos participantes en los procedimientos y los indicadores de rendimiento y ejecución necesarios. Por último, y siempre con el objetivo de dar a conocer todas estas medidas a los posibles beneficiarios, la plataforma cuenta con una capa de funciones para promocionar ampliamente los planes de ayuda entre los destinatarios.

“PARA DESPLEGAR CON ÉXITO ESTOS PLANES EXCEPCIONALES DE RECUPERACIÓN, LAS ADMINISTRACIONES PÚBLICAS DEBEN CONTAR CON LAS HERRAMIENTAS TECNOLÓGICAS ADECUADAS QUE LES PERMITAN SIMPLIFICAR LOS PROCESOS COMPLEJOS Y GARANTIZAR LA COORDINACIÓN A GRAN ESCALA DE LOS ACTORES IMPLICADOS”

FAVORECER LAS SOLUCIONES SÓLIDAS QUE YA HAN SIDO PROBADAS

Al elegir una herramienta tecnológica existente en lugar de intentar crear una nueva solución, las autoridades pueden dedicar su energía al desarrollo estratégico del plan de recuperación y a su vertiente más humana: el impacto social, la comunicación, la educación, la gestión del cambio y la gestión de equipos.

Para que la recuperación sea una realidad, es crucial que las organizaciones públicas trabajen al mismo ritmo que las empresas privadas, con repositorios informáticos compatibles y abiertos. La plataforma segura de Salesforce y su oferta de “Gestión de ayudas” es un puente entre los financiadores públicos y privados, los gestores y los beneficiarios. ■

SI TE HA GUSTADO ESTA REVISTA, COMPÁRTELA

IMPULSO A LA IMPARABLE TRANSFORMACIÓN DIGITAL DEL SECTOR PÚBLICO

DAVID GÓMEZ

SALES DIRECTOR IBERIA, BLUE PRISM

Si bien la digitalización ya era una prioridad estratégica tanto para las empresas como para el Sector Público, la pandemia del Covid-19 ha acelerado la transformación en marcha. En España, en el centro del proceso de transformación del Sector Público se encuentra el Plan de Digitalización de las Administraciones Públicas, que cuenta con una inversión de los fondos europeos Next Generation de al menos 2.600 millones de euros para los próximos tres años. En este escenario de transformación digital, la automatización tiene, y ha de tener, un papel fundamental. Consciente de esto, la Administración Pública ha entendido que, para lograr la recuperación y reforzar la economía, es necesario acelerar la transformación y dar ejemplo desde las instituciones, dando un paso adelante en la adopción de la automatización inteligente. El objetivo es mejorar la calidad, cantidad y eficiencia de los servicios y procesos de gestión y tramitación de la Administración.

No es de extrañar que el primer paso para ello haya sido diseñar e implantar una plataforma que permita la automatización de las actuaciones administrativas y tareas de los distintos departamentos ministeriales. Los procedimientos que se pretenden automatizar son tanto los de compra pública, desarrollando soluciones que permitan digitalizar la tramitación de los expedientes de contratación de forma más ágil y eficiente, como la gestión de ayudas y subvenciones, mediante una solución que permita configurar de forma sencilla los procesos de baremo y concesión, así como la prevención del fraude. En resumen, se trata de mejorar el servicio al ciudadano y mejorar las condiciones de trabajo de los propios funcionarios.

En base a este plan, la SGAD (Secretaría General de Administración Digital), órgano responsable de dirigir, coordinar y ejecutar la Medida 5 del Plan (el Servicio de Automatización Inteligente), ha realizado una licitación adjudicando el proyecto a Telefónica, con tecnología de Blue Prism. Ante la cuestión de por qué se ha valorado Blue Prism como la mejor opción para llevar a cabo este ambicioso proyecto, la clave está en las características de su tecnología: auditoría inmutable, cumplimiento de los más altos estándares de seguridad y solvencia ante la necesidad de escalabilidad futura.

Gracias a estas características, las soluciones de Blue Prism se han convertido en el estándar tecnológico para la automatización en Administraciones Públicas. Más allá de la teoría, esta tecnología ofrece beneficios contrastados, ya sea en otras administraciones como las de Reino Unido o Estados Unidos, donde la tecnología de Blue Prism ha llevado a cabo con éxito procesos de automatización inteligente de organismos públicos, como en España, cuyos beneficios ya conocen la Junta de Andalucía, Renfe-LogiRAIL, el Ministerio de Justicia o el Ministerio de Trabajo. ■

SI TE HA GUSTADO ESTA REVISTA, COMPÁRTELA

EL ACCESO A LA INFORMACIÓN COMO PILAR PARA LA TRANSFORMACIÓN DIGITAL

SEVERINO GALA

DIRECTOR GENERAL DE MICROSTRATEGY

La evolución de la digitalización en la sociedad actual es un hecho indiscutible e imparable que, además, se ha visto potenciado en el último año y medio con la pandemia, donde muchas de las compras, tareas cotidianas... se han visto obligadas a realizarse a través de portales y medios digitales.

Si hablamos de la digitalización en la Administración Pública Española, el punto de partida es increíblemente bueno: España está el 2º en el ranking en la digitalización de los procesos y gestiones administrativas. Pero a pesar de que ambos componentes de la ecuación se encuentren en un buen punto de partida, la combinación de ambos no tiene el resultado esperado, puesto que existe una barrera, tanto tecnológica como de complejidad, idioma y conocimiento en determinados sectores y rangos de edad, que dificulta ese acceso digital a la administración pública.

Es por eso por lo que esta transformación digital debe ir encaminada en facilitar el acceso del empleado y ciudadano a la información más relevante, un acceso rápido y sencillo; un acceso intuitivo que rompa esa brecha digital y un acceso, digamos, omnicanal, que sea único y homogéneo, accedamos por el canal que accedamos, ya sea portal web, aplicación móvil o incluso con la ayuda de chatbots.

La transformación digital no es solo un proceso puramente tecnológico, es un proceso de cómo se accede e interactúa con la información. Se deben trabajar ambos aspectos para alcanzar el objetivo.

Desde MicroStrategy llevamos años trabajando para ayudar a las organizaciones en ambos aspectos. Por un lado, hemos trabajado en una solución flexible, con el uso de API Rest, que permita interactuar con las diferentes piezas tecnológicas existentes, conectando y combinando diferentes fuentes de datos y aplicativos, proporcionando gobierno del dato y una visión única a lo largo de la organización, acceda desde donde se acceda, una visión única y omnicanal de la información. Esto simplifica mucho el aspecto tecnológico de la transformación digital.

Y, por otro lado, MicroStrategy ha desarrollado una tecnología innovadora que permite al consumidor de información un acceso intuitivo, rápido y sencillo a la información más relevante. Es la información la que viene a ti en vez de ir a buscarla. Se llama HyperIntelligence y se trata de información contextual, que aparecerá automáticamente aportando la información más relevante y los links necesarios para ayudar al empleado y ciudadano a visualizar los datos necesarios y disponer de los vínculos para poder realizar la gestión si fuera necesario, de esta manera no solo se muestran los datos, si no que se genera un flujo de trabajo. Es una tecnología que dada su sencillez y rapidez ayuda a reducir, sino eliminar, la brecha digital existente tanto internamente como con el ciudadano. Además, es una tecnología cuya puesta en marcha es extremadamente rápida.

La visión de MicroStrategy es facilitar el acceso a las personas a la información desde cualquier dispositivo y en cualquier momento. Ayudar a las organizaciones y personas a convertir el dato en información y acceder a él de manera sencilla y rápida para ayudar tanto a los empleados en la toma de decisiones basadas en datos como al ciudadano en visualizar de manera simple los datos y vínculos necesarios para realizar su gestión. ■

GRABACIÓN DISPONIBLE

Administración pública:

afrontando la década digital

> PLAY

Organiza

it Digital MEDIA GROUP

Patrocinadores Platinum

CISCO

dynatrace

salesforce

Socios colaboradores

Astic

Foro CPP colaboración público-privada TECNOLOGÍA & INNOVACIÓN

Patrocinadores Gold

blueprism

f5

MicroStrategy

proofpoint

VEEAM

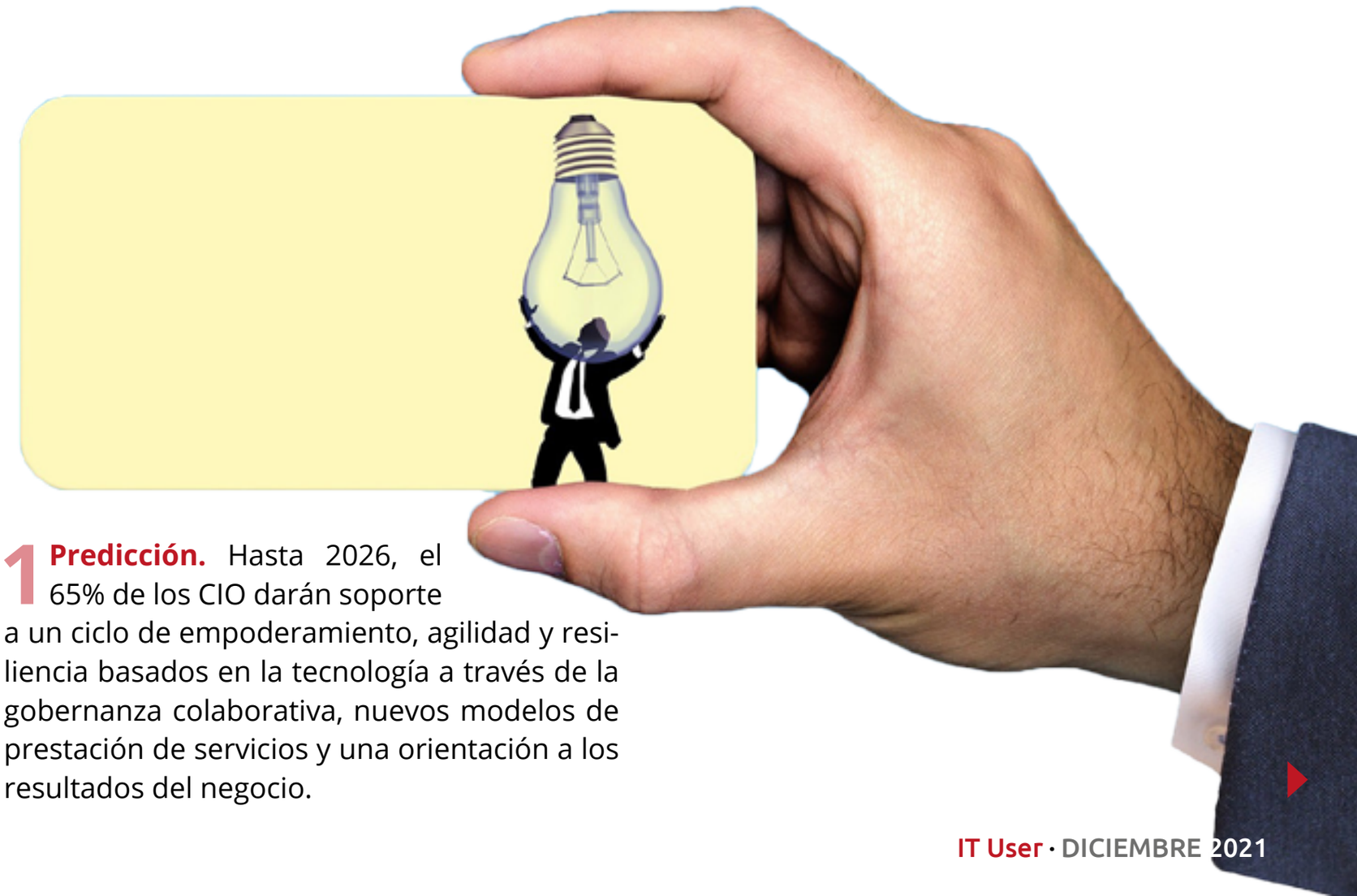
FORO it User TECH & BUSINESS

10 claves que los CIO deberán tener en su agenda en los próximos cinco años

El imperativo digital coloca a los CIO de todo el mundo ante el reto de crear y afianzar una base tecnológica que facilite la flexibilidad, agilidad y resiliencia necesaria para los procesos y modelos de negocio de sus organizaciones. Basándose en esta premisa, IDC ha elaborado las predicciones que marcarán su agenda entre 2022 y 2026.

En un contexto de digitalización acelerada, los CIO tendrán que orientar sus estrategia para ayudar a sus organizaciones a habilitar nuevos ecosistemas, procesos y modelos de negocio, que sean flexibles, ágiles y resilientes. Esto marcará sus agendas en los próximos cinco años, y se complementa con otro de sus informes, prácticamente coincidente en el tiempo sobre sus expectativas de evolución para las inversiones en transformación digital que, según sus estimaciones, supondrán más de la mitad del gasto en TIC en 2024.

Al igual que Gartner, que desveló las doce tendencias que generarán disrupciones y oportunidades significativas en el horizonte de cinco a diez años, IDC pone el acento en que los próximos años serán claves para crear bases técnicas escalables y resilientes que impulsen la ruta digital. Estas son las diez predicciones de la consultora:



1 Predicción. Hasta 2026, el 65% de los CIO darán soporte a un ciclo de empoderamiento, agilidad y resiliencia basados en la tecnología a través de la gobernanza colaborativa, nuevos modelos de prestación de servicios y una orientación a los resultados del negocio.

2 Predicción. En 2023, el trabajo de seis de cada diez CIO se medirá principalmente por su capacidad para cocrear nuevos modelos de negocio y de los resultados que obtenga mediante una amplia colaboración en toda la empresa y el ecosistema.

3 Predicción. En 2025, el 75% de los CIO y CFO tendrán que acelerar o tener prácticas formales de gestión de la deuda técnica generada por los retrasos o fracasos de los proyectos causados.

4 Predicción. Ante el auge de los entornos de trabajo híbrido y la evolución hacia puestos de trabajo inteligentes, en 2024, el 60% de los CIO habrá reimaginado el soporte al usuario y creará equipos basados en centros de excelencia (COE) para llevar a cabo las inversiones necesarias en tecnología y procesos.

5 Predicción. En 2026, el 85% de las organizaciones cuyas prácticas de datos limitan sus estrategias empresariales y operativas, darán luz verde a los responsables de TI para que lideren las inversiones en gobierno, calidad y cumplimiento de datos.

6 Predicción. En 2024, cuatro de cada diez CIO no habrán logrado evolucionar eficazmente la capacidad de TI para ofrecer infraestructuras digitales modernas, proporcionar un gobierno tecnológico del ecosistema y dar soporte a los resultados empresariales, impulsados por la arquitectura.

7 Predicción. Debido la presión de los inversores para minimizar los gastos operativos fijos, en 2024, el 40% de las organizaciones trasladará al menos el 25% del gasto en TI a costes directos, alineándolos con productos y servicios específicos de sus líneas de negocio.

8 Predicción. El 60% de los directores de tecnología adoptará la autenticación multifactor en todo el ecosistema, por su eficacia para contrarrestar las crecientes amenazas de ciberseguridad en 2022. Tendrán que obviar su coste y la fricción que puede suponer, ya que se vuelve esencial.

9 Predicción. En 2025, seis de cada diez CIO colaborarán para aprovechar las capacidades del ecosistema de su sector como fuente crítica de innovación, intercambio de

¿CÓMO SER UN CIO MÁS DIVERSO?

datos, diferenciación y gestión de riesgos de ciberseguridad.

10 Predicción. En 2023, las compañías requerirán que el 55% de los directivos de TI de las 2.000 principales empresas privadas, agrupadas en la lista G2000 de Forbes, implementen una estrategia de TI sostenible, incorporando prácticas medioambientales, sociales y de gobierno en el ciclo de vida de la tecnología.

LOS CIO GANAN INFLUENCIA EN SUS ORGANIZACIONES POR EL PAPEL DE LA TECNOLOGÍA TRAS LA PANDEMIA

La influencia de los directores de TI va a más en paralelo a la urgencia que la transformación digital tiene en la recuperación y en la nueva economía que se está fraguando. Así lo concluye un nuevo estudio, llevado a cabo por el IBV en colaboración con Oxford Economics, que se basa en una encuesta en la que han participado 2.500 CIO de 29 sectores, y que también incluye la visión de los CEO.

Cuando se les preguntó a los primeros ejecutivos quiénes serán más críticos en los próximos años, los encuestados nombraron a sus jefes de tecnología (CIO y CTO) más del doble de las veces que a los directivos de marketing, recursos humanos o cualquier otra posición, a excepción a los directivos de las áreas de finanzas y operaciones.

El informe constata, por tanto, que las necesidades tecnológicas tras la pandemia impulsa el papel influenciador de los CIO en las estrategias corporativas.

Resultados en España

Los CIO españoles creen que la tecnología tendrá un gran impacto en la experiencia de empleado en los próximos tres años. Según el estudio, casi la mitad de ellos consideran que el área de experiencia de empleado será en la que tendrá mayor impacto la tecnología en los próximos tres años seguida de los nuevos tipos de trabajo y habilidades (38%).

A pesar de que el 93% de los encuestados asegura que su empresa ha realizado una estrategia para trabajar en remoto, solo el 23% cree que se pueda gestionar de manera únicamente virtual.

Por último, el 71% de los CIO encuestados considera que la mayor inversión tecnológica que se realizará en sus empresas en los próximos tres años será en IoT, seguido de 5G y automatización (62%) e inteligencia artificial (57%).

TENDENCIAS

Los CIO encuestados lideran la transformación digital centrándose en la IA, la nube híbrida y la sostenibilidad. Aunque siguen prestando los servicios de TI que necesitan las operaciones empresariales, muchas veces también se espera que ayuden a impulsar la innovación y el crecimiento empresarial.

Muchos de ellos destacaron la importancia de los datos y la automatización para acabar con los silos y crear nuevos flujos de valor. El número de CIO encuestados que informaron de una alta madurez en los flujos de trabajo habilitados por la inteligencia aumentó un 560% en comparación con hace dos años y, el 37% citaron la automatización de procesos como la principal oportunidad de impacto positivo dentro de sus organizaciones. Los participantes indicaron que el mayor uso de la automatización se da en TI, finanzas y producción, con cargas de trabajo de un 40%, 35% y 35%, respectivamente.

La nube híbrida es un pilar clave para los flujos de trabajo inteligentes impulsados por la IA. El número de directores que mencionan una alta madurez en sus operaciones de nube híbrida aumentó un 700% en comparación con 2019.

A su vez, muchos CIO también buscan emplear la tecnología para potenciar el desarrollo de los objetivos corporativos, como la sostenibilidad. El 42% espera que la tecnología tenga un impacto significativo en la sostenibilidad en los próximos tres años, el mayor de todos los ámbitos de impacto.

ENTORNOS HÍBRIDOS

Los CIO encuestados pueden estar subestimando el reto que supone el lugar de trabajo híbrido actual. El 83% de los sondeados afirmaron haber implementado estrategias de trabajo a distancia, pero sólo el 23% espera que los cambios sean permanentes. Por el contrario, casi dos de cada tres (65%) empleados encuestados afirman que preferirían trabajar exclusivamente a distancia o en un modelo híbrido, si se les diera la opción. ■

MÁS INFORMACIÓN

- Predicciones tecnológicas 2022 (IDC)
- Tendencias tecnológicas dominantes en 2022 (Forbes)
- Predicciones TI para 2022 y más allá (Gartner)

it whitepapers

ESPAÑA EN LA ERA POST-COVID: TI para transformar el negocio

La COVID-19 ha trastocado la vida de empresas y ciudadanos que ven con incertidumbre el futuro. A la preocupación sanitaria se le unen unas previsiones económicas, y de desempleo, nada esperanzadoras. Descubre en este IT Research cuáles son las principales previsiones para España y cuál es el papel que va a jugar la tecnología en la recuperación a través de más de 40 gráficos, divididos en seis bloques (Perspectivas Económicas para España, Evolución del Empleo, Situación de las Empresas Españolas, La Transformación Digital en España, la I+D, y la Importancia de los Fondos Europeos), y las opiniones de diversos analistas del sector.

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!!!

Las empresas seguirán aumentando el gasto en transformación digital

En los próximos años las organizaciones van a seguir incrementando el gasto en digitalización para desarrollar una estrategia digital que abarque a las personas, los procesos, la tecnología, los datos y la gobernanza. Según IDC, la inversión aumentará de forma constante hasta 2025, duplicando la cifra registrada en 2020, cuando se aceleró la adopción de nuevas tecnologías para superar la crisis.

Alcanzar la madurez digital se ha convertido en una prioridad para muchas empresas, que tras el bache sufrido a consecuencia de la pandemia se han dado cuenta de la necesidad de adoptar una estrategia digital más amplia y transversal que permita competir en la era digital. El año pasado se vieron obligadas a implementar nuevas herramientas y tecnologías digitales de forma más o menos improvisada para salir del paso, pero ahora el objetivo es una digitalización mejor planificada y con un mayor alcance dentro de la organización, que establezca una base para el futuro.

La última Guía de gasto mundial en transformación digital de IDC muestra que las empresas van a aumentar la inversión en digitalización a una tasa interanual compuesta del 16,4% hasta el año 2025, para cuando el gasto alcanzará los 2,8 trillones de dólares, duplicando el presupuesto de DX de 2020. En este pe-

ríodo tratará de adoptar lo que los expertos consideran una estrategia digital holística, que contemple tanto las personas como los procesos, la tecnología, los datos y la gobernanza.

Como explica Craig Simpson, gerente sénior de investigación del Customer Insights and Analysis Group de IDC, esta es la primera vez que han pronosticado que el gasto en digitalización superará los 10 trillones de dólares en un período de 5 años. Y dice que "si bien la mayoría de los proyectos de DX se mantuvieron en marcha en 2020 y en 2021 durante la pandemia, IDC prevé que las inversiones en tecnología de DX se acelerarán en 2022, con un impulso renovado hacia objetivos digitales estratégicos a más largo plazo". Comenta que uno de los focos más importantes de esta inversión estará en la experiencia del cliente, especialmente en las industrias orientadas al consumidor, como las de valores y servicios de inversión, la banca y el comercio minorista.

En estos años las prioridades de inversión en DX de las empresas estarán orientadas a más largo plazo, buscando consolidar el uso de la tecnología en toda la organización y vinculando los cambios a una serie de objetivos operativos más claros. Por ejemplo, el soporte administrativo y la infraestructura para funciones comer-

Más de la mitad de la inversión TI irá a transformación digital en 2024

Según el nuevo informe de IDC, las inversiones directas en transformación digital se acelerarán a una tasa de crecimiento anual compuesta (CAGR) del 16,5% entre 2022 y 2024, frente al ratio del 15,4% en 2019-2024. A esta velocidad, el 55% de la inversión en tecnología y comunicaciones se destinará a transformación digital al final del período. Esta es la primera de las predicciones que la consultora realiza en su informe. La segunda, que es una consecuencia lógica, es que la digitalización tendrá más peso en el PIB mundial y, en este sentido, en 2022 más de la mitad de la economía estará basada o influenciada por lo digital.

Su siguiente predicción es que, para 2023, el 90% de las organizaciones en todo el mundo priorizarán las inversiones en herramientas digitales para hacer crecer sus activos y espacios físicos con experiencias digitales.

En cuarto lugar, calcula que, para 2025, el 60% de las compañías capitalizarán un enfoque de automatización de toda la empresa y su ecosistema, aprovechándose los conceptos empresariales basados ??en modelos, los centros de excelencia (COE) y las plataformas de código de bajo código o sin código.

Por otro lado, sostiene que, en 2026, un 54% de los CIO impulsará la transformación de sus empresas, promoviendo la creación de organizaciones digitalmente resilientes a través de hojas de ruta estratégicas. Habrá un rediseño de plataformas para impulsar plantillas que trabajen de forma colaborativa, basándose en datos.

El uso de herramientas sin código o de bajo código y la capacidad de utilizar datos dará lugar a que los empleados lideren la transformación e integren la resiliencia digital en sus puestos. Esto ocurrirá en seis de cada compañías en el horizonte de 2024.

Enlazando con lo anterior, la séptima predicción está dedicada a la resiliencia digital. Para 2022, el 55% de las empresas habrán ampliado sus planes de resiliencia para preparar su negocio para el futuro, para mejorar la rentabilidad, el nivel de innovación y la rentabilidad en más del 20% en comparación con las que no lo hagan.

Por otro lado, para 2023, la mitad de las organizaciones generarán más del 40% de sus ingresos a partir de productos y servicios digitales, en comparación con una de cada tres que lo hacía en 2020.

IDC también habla de que, en 2025, las empresas que apuesten por un liderazgo multifuncional, innovarán más rápido, ganarán más cuota de mercado y lograrán más eficiencias operacionales que sus competidores.

Cierra sus predicciones recordando que las iniciativas de descarbonización son un objetivo clave de las transformaciones digitales. Menos del 10% de las empresas dicen que no son aplicables o que no están implementando objetivos para reducir el carbono para fines de 2023.

ciales principales, como son la contabilidad y las finanzas, los recursos humanos, el departamento legal, la seguridad y riesgo y la TI empresarial.

Además, la necesidad de innovar, escalar y operar estará vinculada a un área más amplia que abarcará operaciones a gran escala como las actividades de fabricación, construcción y diseño. También funciones comerciales centrales como la gestión de la cadena de suministro, la ingeniería, el diseño y la investigación, las operaciones y las operaciones de las plantas de fabricación.

El último punto importante que destacan los investigadores de IDC es que la inversión en DX para mejorar la experiencia del cliente cubrirá todo aquello relacionado con las funciones relacionadas con el cliente, en las áreas de servicio al cliente, marketing y ventas. Aunque el gasto en soporte e infraestructura de back office y las prioridades de innovación, escala y operación sumarán la mayor parte de las inversiones en este campo, el gasto en mejora de la experiencia del cliente verá un crecimiento mucho más rápido en estos años.

Analizando los casos de uso de transformación digital, IDC pronostica que el mayor gasto se distribuirá en tres áreas principales, que serán la inversión en fabricación robótica (120.600 millones en 2025), operaciones autónomas y clientes 360o (90.900 millones), y gestión de clientes (74.700 millones). Los casos de uso que verán un crecimiento del gasto más pronunciado serán los de espacios de trabajo de estudiantes virtualizados (43,8% CAGR), asistencia en operaciones mineras

(39,1% CAGR) y gestión del diseño aumentada (34,5% CAGR).

Y las industrias que más invertirán en transformación digital en estos años serán la fabricación discreta y de procesos, los servicios profesionales y el comercio minorista. Y solo las dos industrias manufactureras sumarán más de 816.000 millones de dólares en 2025. El crecimiento más rápido del gasto en DX hasta 2025 se producirá en la industria de construcción (21% CAGR), los servicios de valores e inversión (19,2% CAGR) y la banca (10% CAGR).

En términos geográficos, Estados Unidos seguirá liderando el gasto en transformación digital, acaparando alrededor de un tercio de la inversión mundial. Le seguirá Europa Occidental y, muy de cerca, China. Y será precisamente este país asiático el que más rápido aumentará la inversión en digitalización, con una tasa interanual compuesta del 18,4% entre 2021 y 2025. Por detrás se situará Latinoamérica, que verá un aumento del gasto del 17,5% (CAGR).

Angela Vacca, directora de investigación sénior de Soluciones Industriales Europeas y Perspectivas y Análisis de Clientes, en IDC, concluye su informe diciendo que "para 2025, el gasto en DX en Europa alcanzará los 653.000 millones de dólares, más del doble de la cantidad gastada en 2020. Además, en 2023, el gasto en DX superará a los gastos que no son de DX, lo que confirma el fuerte compromiso de las empresas europeas con la transformación digital".

Además, especifica que "las empresas europeas de finanzas, atención médica y servicios profesionales aumentarán su gasto en DX con fuertes variaciones en los casos de uso, ya que las prioridades siguen cambiando a medida que avanza la recuperación". Afirma que "las empresas, en consecuencia, se alejan de las necesidades de emergencia para pasar a ser más estratégicas y a realizar apuestas a más largo plazo". ■

MÁS INFORMACIÓN

- Guía de gasto mundial en transformación digital de IDC
- Predicciones para el futuro de la innovación (IDC)

3 claves para competir en la economía de los datos

Según las previsiones de IDC, los datos que creamos, capturamos, replicamos y consumimos alcanzarán los 175 zettabytes y alrededor del 75% de la población mundial interactuará con ellos todos los días para 2025. Sin gestionarlos de la forma adecuada, es imposible extraer su auténtico valor y convertirlos en conocimiento para tomar decisiones y que se traduzcan en acciones. Éstas son las claves para lograrlo.

Los expertos de la consultora tecnológica Entelgy han identificado los pasos que deben seguir las empresas puedan transformar los datos que genera en información de utilidad:

INGESTA DE DATOS E INGENIERÍA

La primera fase de este recorrido hacia la información consiste en la ingesta, es decir, la forma en la que obtener e importar los datos, ya sea para su uso inmediato en tiempo real o para ser almacenados y analizados más tarde. Son muchos los datos que se generan día a día en cualquier negocio y su relación con el cliente mediante inventarios, órdenes de pedido, nóminas, partes de alta de empleados, ventas o consultas de clientes podemos extraer datos muy valiosos.

Una vez se tiene la información es el momento de comenzar a organizarla. La gran variedad de fuentes desde las que la empresa puede recopilar datos supone, en consecuencia, una gran variedad de formatos. Ahora los datos recopilados deben ser limpiados, cumplimentados y verificados para lograr una identidad única de cada dato y poder así tener una visión 360º de la información con la que contamos y comenzar el proceso de análisis.

CIENCIA Y EXPLOTACIÓN

Los datos son como un diamante en bruto. Tras recopilar y unificar hay que pulirlos, extraer el valor que encierran y así poder utilizarlos para tomar decisiones de negocio. En primer lugar, para poder extraer valor de estos datos debemos aplicar técnicas de analítica avanzada mediante la implementación de modelos probabilísticos, predictivos y prescriptivos. También existen modelos basados en machine learning, o aplicando deep learning para el análisis de datos no estructurados como vídeos, imáge-

nes o audios, mediante procesamiento de lenguaje natural.

Estos modelos son los que alimentarán las herramientas de explotación que protagonizan el siguiente paso del recorrido. Es el momento de aplicar técnicas de Data Discovery, cuya máxima es el autoservicio, permitiendo que todos los profesionales de la compañía puedan conocer y analizar, de forma rápida y sencilla, los datos que precisan. Por ejemplo, un Gerente de Ventas podría obtener información de manera directa de quiénes son los clientes y productos más rentables del último mes, sin tener que recurrir al departamento de TI permitiendo así, reducir tiempos y aumentar la productividad del negocio.

EVOLUCIÓN DEL CONOCIMIENTO

El último paso en el camino es la fase en la que realmente esa información de valor se convierte en conocimiento para no solo optimizar e incrementar el negocio actual de una compañía, sino también para poder predecir sus próximas decisiones. A través de modelos predictivos, la organización adquiere capacidades para proyectar aquellas variables que impactan de manera directa en el negocio, ayudando en la gestión proactiva de la compañía. En este estadio somos capaces de dar respuesta a preguntas sobre el futuro, y la tecnología propondrá acciones ayudándonos así a la toma de decisiones. ■

Los datos recopilados deben ser limpiados, cumplimentados y verificados para lograr una identidad única de cada dato y poder así tener una visión 360º de la información con la que contamos y comenzar el proceso de análisis

MÁS INFORMACIÓN

Empresas Data-Driven. Estrategias de datos para marcar la diferencia

La gestión del dato en las empresas

El papel de una visión empresarial global en la creación de una organización basada en los datos

Los responsables de la arquitectura empresarial y de la innovación tecnológica pueden desempeñar un papel clave en la creación de una organización basada en los datos si proporcionan una visión empresarial de las necesidades de datos en relación con los profesionales estratégicos del negocio.

Las demandas organizativas de los análisis de datos están creciendo, pero muchos líderes de la arquitectura empresarial y TI siguen centrados en programas de gestión de datos que no están vinculados a los profesionales del negocio. En cambio, deberían aprovechar su visión única de la empresa para garantizar que los responsables de la toma de decisiones tengan los datos que necesitan para impulsar los resultados empresariales.

Según una investigación reciente de Gartner, el 58% de los CIO está aumentando la inversión en inteligencia empresarial (BI) y las iniciativas de D&A en 2021, con lo que, en opinión de la consultora, hay una oportunidad para que los líderes de EA proporcionen una visión empresarial contra la cual se toman cientos de decisiones que comprenden iniciativas de datos.

Los responsables de las arquitecturas empresariales pueden identificar y capturar oportunidades para las capacidades de datos y analítica de alta demanda y alto potencial si aprovechan las ventajas que están naturalmente vinculadas a su papel. Por ejemplo, estos responsables están en una posición única para:

➤ Identificar oportunidades de datos empresariales que las personas que trabajan en silos no pueden.

➤ Comprender los flujos de datos de principio a fin para garantizar la optimización.

➤ Garantizar que las estrategias digitales y empresariales estén alineadas para satisfacer las necesidades de datos del presente y del futuro.

➤ Estas ventajas pueden traducirse en aplicaciones prácticas que son fundamentales para las aspiraciones de analítica de una organización y pueden elevar su valor empresarial.

CONSTRUIR UNA ORGANIZACIÓN MÁS ORIENTADA A LOS DATOS

Estos responsables pueden aprovechar su visión empresarial única para ayudar a construir una organización más orientada a los datos de cuatro maneras:

❖ **Proporcionar una visión empresarial del panorama de los datos.** La arquitectura empresarial mira a través de los silos para abordar las necesidades de integración de datos interfuncionales que identifica un mapa de viaje de extremo a extremo. Una mala integración de los datos en los sistemas puede conducir a la redundancia de datos, y los mapas de viaje son más que útiles para señalar estos problemas. Pueden garantizar que una organización vea el panorama completo de las oportunidades de mejora de los datos.

❖ **Mejorar y ampliar el proceso de análisis de datos.** Optimizar las prácticas de gestión de datos no es suficiente si el análisis de datos y la toma de decisiones siguen siendo engorrosos. La calidad de los datos por sí sola no puede aumentar los ingresos, reducir los costes y mejorar la agilidad.

❖ **Definir las funciones y responsabilidades para la mejora de los datos.** Aunque las respon-

Las demandas organizativas de los análisis de datos están creciendo, pero muchos líderes de la arquitectura empresarial y TI siguen centrados en programas de gestión de datos que no están vinculados a los profesionales del negocio

sabilidades de los equipos de arquitecturas empresarial y analítica dependen del modelo de negocio, es esencial definir claramente las funciones y responsabilidades de todos y, al mismo tiempo, centrarse en los resultados compartidos y las medidas de éxito para una mejor toma de decisiones. Esto puede fomentar la colaboración y evitar el solapamiento de responsabilidades. Por ejemplo, además de ser responsables de la arquitectura de la información, los arquitectos de la información pueden colaborar con los equipos de entrega de TI en áreas como la integración y la funcionalidad del sistema. Del mismo modo, el personal de ciencia de los datos puede ser propietario de los modelos de análisis de datos, pero puede colaborar con los líderes empresariales para identificar las preguntas críticas a las que pueden responder esos modelos. También puede colaborar con los arquitectos de la información para garantizar que los datos correctos estén en el lugar adecuado.

❖ **Facilitar los análisis relevantes para el negocio.** Los problemas empresariales requieren conocimientos cuantificables, contextuales y procesables que proporcionen suficiente valor para justificar una inversión. Además de reimaginar las capacidades de analítica, es necesario combinar la experiencia analítica con la perspicacia empresarial para obtener lo mejor de ambos mundos. Los grupos de arquitectura empresarial pueden asociarse con los equipos de análisis y los líderes empresariales para identificar las preguntas críticas a las que los datos pueden responder y discernir la información necesaria y disponible para responder a las preguntas. Durante estas conversaciones, los líderes de arquitecturas empresariales pueden abordar tanto las cuestiones estándar de calidad de los datos (como la precisión, la puntualidad...) como las no obvias. Por ejemplo, los datos son de buena calidad, pero no se utilizan tan bien como podrían. De este modo, pueden ser colaboradores clave para impulsar continuamente una organización hacia la toma de decisiones basada en datos. ■

MÁS INFORMACIÓN

- Foro IT User Empresas Data Driven, estrategias de datos para marcar la diferencia
- Cinco tendencias que se integran en compañías data driven
- ¿Qué tienen en común las organizaciones data driven?
- El papel de las arquitecturas empresariales en las empresas data driven

it whitepapers

INFORME: HACIA LA EMPRESA HIPERINTELIGENTE

IT Research ha realizado para MicroStrategy un estudio acerca de la toma de decisiones en la empresa y las herramientas utilizadas. Según el informe, un 86% de los consultados afirma que la información interviene en más del 40% de las decisiones que se toman en su organización. Además, un 71% considera que en su compañía estas decisiones se llevan a cabo con la información lo más actualizada posible; un 29% cuestiona esta posición. Descárgalo ahora para conocer otros datos.

Estas son las ventajas que las empresas perciben cuando utilizan la Inteligencia Artificial

Boston Consulting Group (BCG) y MIT Sloan Management Review (MIT SMR) han presentado los resultados de un estudio que indaga en las mejoras que consiguen las empresas cuando utilizan la Inteligencia Artificial. Tres de cada cuatro directivos destacan las que tienen que ver con la eficiencia y la forma de trabajar de los equipos.

Más del 75% de los directivos de empresas que han integrado la Inteligencia Artificial (IA) en sus procesos, afirman que la tecnología mejora la toma de decisiones y la eficiencia de los equipos, y también aprecian cambios positivos en el aprendizaje empresarial (87%), la moral de los trabajadores (79%) y la colaboración entre compañeros (78%), según 'The Cultural Benefits of Artificial Intelligence in the Enterprise', un nuevo informe global publicado la consultora estratégica Boston Consulting Group (BCG) y MIT Sloan Management Review (MIT SMR).

El informe resalta que "los beneficios culturales y económicos relacionados con la IA se complementan entre sí". En este sentido, su uso ayuda a que las empresas reevalúen lo que significa ser eficaz en sus procesos y formas de trabajar. Por ejemplo, el informe se-

ñala que el 64% de las empresas que utilizan la Inteligencia Artificial reevalúan la forma de medir su rendimiento y ajustan sus KPI.

Además, la encuesta indica que las organizaciones que aprecian beneficios económicos significativos derivados de su uso son 10 veces más propensas a cambiar su forma de medición. En este punto, el informe añade que el 66% de los directivos que coinciden en que la IA ha modificado sus KPI aprecian una cultura de trabajo más colaborativa.

De acuerdo con la encuesta, el 59% de las empresas que utilizan la IA para explorar nuevas formas de crear valor coinciden en que su uso las ayuda a diferenciarse de los competidores. Además, favorece la captura de oportunidades de negocio en sectores adyacentes.

FRENOS A SU ADOPCIÓN

La desconfianza en la tecnología puede perjudicar su adopción, y esta tiene una variedad de causas, según los encuestados. Al respecto, casi la mitad de las empresas creen que la desconfianza en la IA se debe a la falta de comprensión (49%) o de formación (46%), pero también esgrimen otras razones que pueden erosionar la confianza como no proporcionar el suficiente contexto sobre por qué se toman las decisiones (34%) o suministrar demasiada información (17%) puede erosionar la confianza.

También puede generar desconfianza la calidad insuficiente de los datos (31%), el incumplimiento de las expectativas (20%) o la implementación de soluciones incorrectas (14%).

Otra cuestión que aborda el estudio es que la IA, que es eficaz a nivel de equipo, no siempre produce un éxito económico a nivel organizativo.

El 58% de los directivos a nivel mundial coinciden en que su equipos han mejorado tanto la eficiencia como la calidad de las decisiones desde la implementación de estas soluciones. Sin embargo, solo el 11% ha visto beneficios significativos a nivel organizativo. Este dato indica que es posible que todavía sean pocas las empresas que estén implantando la IA a una escala suficiente para poder generar beneficios sustanciales.

En su quinta edición, la investigación de BCG y MIT SMR se ha basado en una encuesta a 2.197 directivos de 106 países de 28 sectores de actividad. ■

MÁS INFORMACIÓN

www The Cultural Benefits of Artificial Intelligence in the Enterprise

DESCUBRE LAS **TENDENCIAS** QUE DEFINEN EL **FUTURO DIGITAL**

it TRENDS

Claves de usabilidad web para no dañar la experiencia del cliente

La usabilidad de una página web, app o producto digital es un elemento clave para determinar su éxito o su fracaso. Lo ha recordado IEBS Business School, coincidiendo con la celebración del Día Mundial de la Usabilidad. Sus expertos han reunido ocho aspectos que hay que considerar para garantizarla.

Desde 2005 se celebra el segundo jueves de diciembre el Día Mundial de la Usabilidad, que este año se centra en el diseño del mundo online con confianza, ética e integridad. Para acercar este concepto a los usuarios, IEBS Business School ha identificado las claves para una buena usabilidad web:

❖ **Simplicidad:** es un equilibrio entre lo funcional y lo entendible. Menos es más. No importa cuán inteligente sea una página web, si los usuarios no la entienden o les frustra, se vuelve inútil. Por eso, debe evitarse la complejidad innecesaria y ofrecer un producto fácil de entender y de usar. La mayor parte de los visitantes no entran en una web para evaluar el diseño, sino para encontrar información concreta o para realizar alguna acción. Por eso, a veces añadir elementos innecesarios puede dificultar que los usuarios consigan hacer lo que quieran.

❖ **Accesibilidad:** desde hace años los smartphones son los dispositivos más utilizados por los usuarios para acceder a Internet con un 93,1%, según Statista, seguido por los ordenadores, la tablet, la TV y los asistentes virtuales. Por eso, hay que tener en cuenta todos estos dispositivos a la hora de proporcionar una buena experiencia de usuario. La página web debe ser Mobile-First. Es decir, primero se diseña para móviles y después se adapta a la gran pantalla.

❖ **Diseño limpio y atractivo:** un buen diseño visual aumenta la expectativa de uso del producto, aumenta el valor final de lo que el usuario está dispuesto a pagar

por él y comunica la esencia de la marca. Hacer un buen uso de imágenes, colores, formas y tipografía impactará directamente en la experiencia del usuario. La primera impresión es clave. En un mundo donde el usuario puede encontrar millones de productos similares, los detalles son los que marcan la diferencia.

❖ **Enfoque en el usuario:** en la línea de los puntos anteriores, la intuitividad debe reinar a la hora de tomar decisiones sobre diseño web. Para ganar en eficiencia, reducir el número de clics que debe hacer el usuario en la interfaz es un buen principio. Es importante minimizar el tiempo que tarda un visitante en completar sus necesidades o sus tareas. Para mejorar este aspecto, lo mejor es realizar pruebas de usuario, mapas de calor, mapas de desplazamiento o focus group.

❖ **Jerarquía visual:** la página web debe estar diseñada de tal forma que los usuarios puedan navegar con ella de forma natural y ágil. Una persona debe poder escanear de un vistazo la web e identificar los contenidos que le interesan de forma fluida. En este sentido, la jerarquización de contenidos ayuda a detectarlos más rápidamente y en gran parte dependen de su ubicación. Los contenidos más importantes deberán estar ubicados en aquellas zonas que retienen más la atención del usuario, las llamadas "zonas calientes".

❖ **Buena velocidad de carga:** si una web tarda en cargarse más de cuatro segundos lo

La mayor parte de los visitantes no entran en una web para evaluar el diseño, sino para encontrar información concreta o para realizar alguna acción

más probable es que la mayoría de usuarios la abandonen sin ni siquiera haber accedido. Hay que cuidar los tiempos a la hora de hacer clic en cualquier enlace, cuando se interactúa con la página o cuánto tarda en descargarse un documento. Para ello, se recomienda optimizar todos los formatos un poco pesados como las imágenes o los vídeos, comprimir código de programación de lenguajes, evitar aquellas páginas de bienvenida que se descargan antes de entrar en la página de inicio, tecnología AMP, hacer copias de caché de las páginas que no se modifican para los visitantes recurrentes...

❖ **Menús cuidados:** igual que las indicaciones a la hora de conducir, los menús de navegación son la puerta de entrada a un grupo de contenido. Por eso, describir y etiquetar de forma breve, clara y sencilla las diferentes pestañas evitando la jerga corporativa y centrándonos en la del usuario. En los menús debe mostrarse siempre texto, a no ser que se pueda añadir un icono o símbolo mundialmente reconocido, como podría ser un carrito de compra.

❖ **Diseño rompedor pero tradicional:** a pesar de que la creatividad en el diseño está bien aplicada, hay ciertos aspectos a los que los usuarios están acostumbrados. Por ejemplo, el logo de la empresa siempre se ubica en la parte superior izquierda en todas las páginas y al hacer clic en el logo debe redirigir a la página de inicio, los enlaces deben estar subrayados, aparecer en color azul y cambiar de color cuando ya se ha hecho clic en él, buscador visible en la parte superior derecha de la web, carrito de compra en la página de inicio... Cambiar este tipo de aspectos podría ser negativo para la usabilidad ya que podría confundir al usuario. ■

MÁS INFORMACIÓN

Claves para la usabilidad web

Los Retos de la Industria 4.0

Patrocinadores: Check Point SOFTWARE TECHNOLOGIES LTD. · ESET · kaspersky · SAMSUNG · STORMSHIELD · TREND MICRO

Los Retos de la Industria 4.0

La cuarta revolución industrial ya es toda una realidad. Ante la evolución de la industria de servicios, se crearon sistemas de producción inteligentes que han traído más eficiencia y un aumento de la productividad, debido al seguimiento y análisis de datos en tiempo real, la virtualización (monitorización remota de los procesos de producción), la descentralización de la toma de decisiones y la modularización. La característica más llamativa de esta Industria 4.0 es la digitalización de la información, así como la demanda de investigación y desarrollo que ofrecen oportunidades para profesionales técnicamente cualificados, con formación multidisciplinar para entender y trabajar con una gran variedad de tecnologías disruptivas.

LOS RETOS DE LA INDUSTRIA 4.0

La Industria 4.0 se considera la cuarta revolución industrial, ya que implica todo un cambio en el modelo de producción hacia una realidad más digital. Según el informe Forces of change: Industry 4.0 de Deloitte, esta revolución combina técnicas avanzadas de producción y operaciones con tecnologías inteligentes que se integrarán en las organizaciones, las personas y los activos.

La base de esta cuarta revolución industrial es la transformación digital. La Edición 2020 del informe Global Conectedness Index que publica DHL señala que España se encuentra en el puesto 27 de los países más conectados, mientras que BBVA Research en su informe DiGiX 2020 nos sitúa en la posición número 35 a la hora de estudiar el grado de digitalización del país. Estos datos indican que todavía falta mucho camino por recorrer.

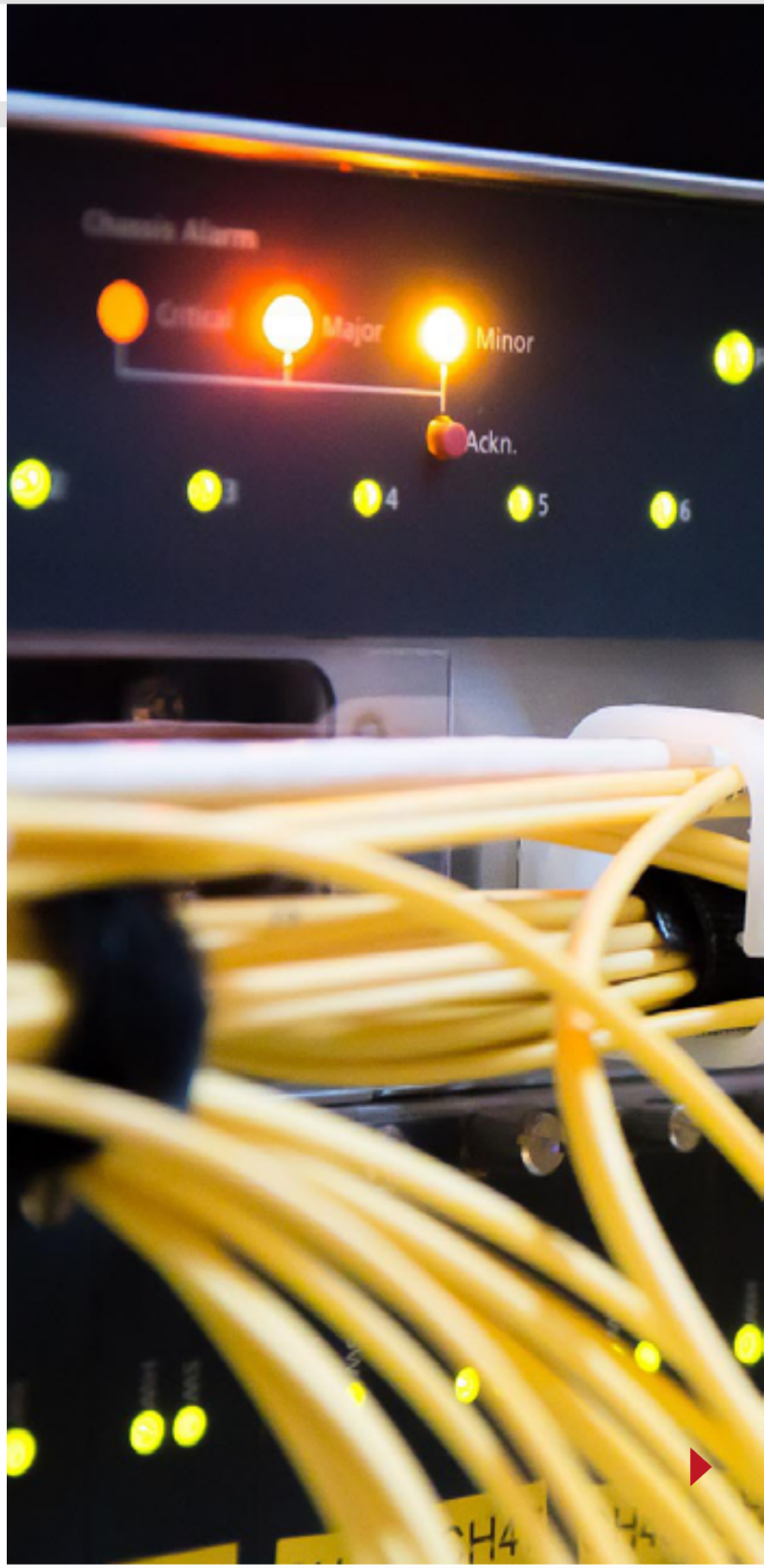
PLAN PARA LA RECUPERACIÓN DE LA INDUSTRIA

El impacto de la COVID-19 también fue muy grande en el sector industrial español. Es por ello que el Plan de Recuperación, Transformación y Resiliencia que ha puesto en marcha el Gobierno de España para canalizar los fondos proporcionados por Europa con el fin de reparar los daños provocados por la crisis derivada de la pandemia del coronavirus recoge en su quinta palanca, entre otros aspectos, la modernización y digitalización del tejido industrial y de la pyme, centrando sus planes para el sector industrial en el componente número 12, titulado Política Industrial España 2030.

El objetivo de este plan es impulsar la modernización y la productividad del ecosistema español de industria-servicios, mediante la digitalización de la cadena de valor, el impulso de la productividad, la competitividad y la mejora de la eficiencia energética de los sectores estratégicos claves en la transición ecológica y la transformación digital. Este informe indica que la industria manufacturera (sin contar el sector energético) representa un 12.3% del Valor Añadido Bruto de la economía española, porcentaje inferior al resto de países que nos rodean. La crisis del coronavirus ha puesto en jaque a la industria española, sector que representa un 83% de la exportación total del país. Así, este plan prevé la puesta en marcha de Proyectos Estratégicos para la Recuperación y la Transformación Económica (PERTEs), los cuales engloban la cadena de valor en un ámbito estratégico.

UNA PRIORIDAD

Deloitte ha realizado una encuesta global a más de 350 ejecutivos en 11 países de América, Asia y Europa, cuyas conclusiones ha destacado el su informe The Industry 4.0 paradox en el que resalta que esta necesidad de abordar una transformación digital en el tejido industrial ya es una prioridad estratégica para el 94% de los encuestados. A pesar de ello, esto no quiere decir que esta transformación se vaya a completar de la



noche a la mañana, como indican los datos del informe a la hora de hablar de presupuestos destinados a la digitalización: de media las empresas planean invertir en ella el 30% de su presupuesto destinado a TI, mientras que del presupuesto destinado a I+D, solo el 11% iría para trabajar en la digitalización de la compañía.

Everis (ahora NTT Data) habla en su informe Smart Industry 4.0 en España de que la digitalización de la industria se debe tener en cuenta en cuatro áreas: cadena de suministro, fabricación, productos digitales y la propia transformación digital de la empresa. Este estudio resalta que las grandes carencias a la hora de hablar de la cadena de suministro son que no hay una monitorización centralizada y acusan una falta de flujo de información entre proveedores y línea de producción. En cuanto a la fabricación, sería necesario abordar áreas como la secuenciación de la producción, la logística interna y la identificación de los materiales a lo largo de los procesos de la planta. A la hora de hablar de los productos digitales, esta necesidad se observa en la inversión planeada para este objetivo: el estudio revela que la mitad de las empresas tenían la previsión de invertir en procesos de creación de productos digitales el año siguiente, mientras que solo un 14% había descartado invertir en el futuro. Asimismo, la industria española está convencida de la necesidad de ir hacia esa digitalización, como indica que solo el 4% había decidido no ponerla en marcha.

La característica más llamativa de esta Industria 4.0 es la digitalización de la información, así como la demanda de investigación y desarrollo que ofrecen oportunidades para profesionales técnicamente cualificados

NUEVAS TECNOLOGÍAS PARA UNA NUEVA REALIDAD INDUSTRIAL

Para hacer realidad esta transformación digital en el sector industrial es necesario apoyarse en una serie de tecnologías que van a apoyar esta digitalización de procesos. El Informe de Tecnologías Disruptivas 2021 de IEBS señalaba que las tecnologías que más se van a utilizar en el futuro serían la inteligencia artificial, el Blockchain y el Internet de las Cosas (IoT). Pero no serán solo esas las herramientas que van a construir el futuro de la industria, ya que otras como el Big Data, la ciberseguridad o el cloud computing serán fundamentales a la hora de abordar este cambio. En este sentido, los analistas de Marketsandmarkets han estimado que el mercado de soluciones para la Industria 4.0 crecerá por encima del 20% anual hasta 2026.

INTELIGENCIA ARTIFICIAL Y ROBÓTICA

Según el estudio La carrera mundial por la IA de IBM, el 82% de las empresas españolas ya está implantando o explorando la incorporación de tecnologías de inteligencia artificial a sus procesos. Esta tecnología permite a las plantas de fabricación escalar en sus modelos de producción sin perjudicar la calidad de los procesos. Los principales ámbitos de uso de la Inteligencia Artificial se podrán observar en la automatización de los procesos industriales, la mejora de las capacidades de la mano de obra y el desarrollo de nuevos productos. Íntimamente ligado a este concepto hallamos la robótica, campo que Gartner espera que crezca en un 19,5% este 2021, hasta llegar a alcanzar los 1.890 miles de millones de dólares.

BLOCKCHAIN

La cadena de bloques o Blockchain también es uno de los elementos que marcarán esta cuarta revolución industrial, ya que permite optimizar los procesos industriales, haciendo que estos sean más flexibles, eficientes y seguros. En concreto, las áreas en las que más impacto puede tener esta tecnología, de acuerdo al informe Tecnologías clave para una Industria 4.0 de DigitalES, son la logística y sus procesos asociados, la seguridad y la trazabilidad, la reducción del fraude y el seguimiento en el comercio

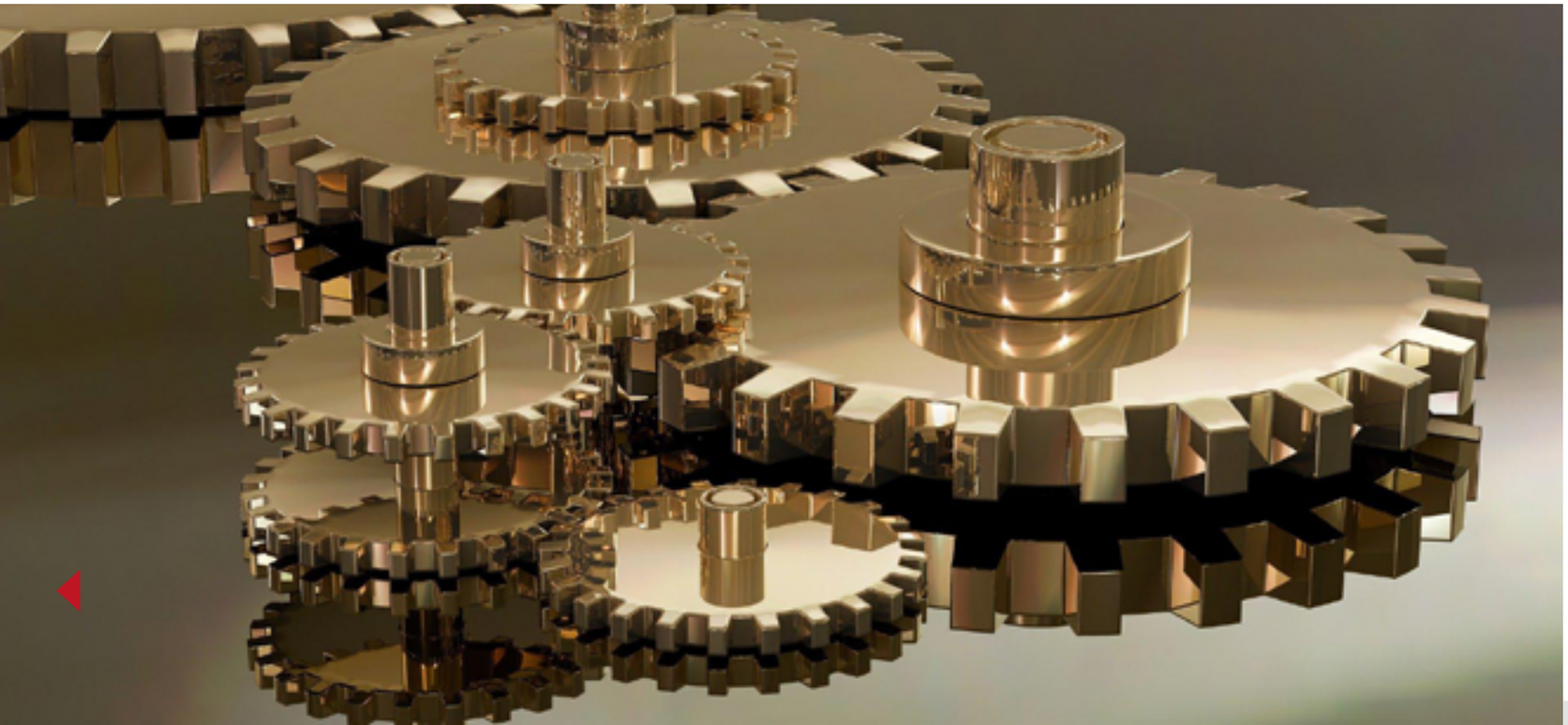
internacional. IDC estima que el gasto global en 'blockchain' alcanzará los 14.400 millones de dólares en 2023.

INTERNET OF THINGS

El Internet de las cosas va a ser un factor fundamental en la transformación digital del tejido industrial. Se trata de un ecosistema de sensores, ordenadores integrados y dispositivos inteligentes que se comunican entre sí con el objetivo de recoger y analizar datos del entorno de fabricación. De nuevo el estudio Tecnologías clave para una Industria 4.0 de DigitalES señala que las principales aplicaciones de esta tecnología irían hacia el mantenimiento predictivo, la optimización de la producción, la gestión del inventario, así como la gestión de flotas. Los datos de IOT Analytics revelan que el gasto global en IoT va a crecer en un 24% en este 2021.

BIG DATA

Todo lo relacionado con la analítica de datos se va a convertir, si no lo es ya, en una pieza clave de la Industria 4.0. Esta datificación va a impactar en todos los demás elementos tecnológicos que forman parte de esta transformación digital, desde favorecer la automatización hasta optimizar procesos y mejorar la toma de decisiones en base a datos completamente fiables. Los datos se han convertido en el petróleo de hoy, por lo que la gestión y análisis de gran cantidad de estos se ha vuelto clave para poder entender la realidad del negocio. Statista señala las cifras que envuelven a esta tecnología, estimando que el mercado global del Big Data alcanzará los 103.000 millones de dólares en el año 2027.



CIBERSEGURIDAD

La transformación digital no tiene sentido si no se toman las medidas necesarias para proteger los activos ante el gran abanico de amenazas que se abren al interconectar todos los sistemas de la empresa y la proliferación del Internet de las Cosas. Además, el sector industrial siempre ha sido un blanco muy apetecible para los ciberdelincuentes, como demuestran los datos de Positive Technologies en un estudio sobre la evolución de las ciberamenazas en 2020, el cual revela que los ataques a empresas industriales aumentaron un 91% entre 2019 y 2020. Es por ello que la filosofía Zero Trust se está imponiendo en el modelo de ciberseguridad actual, por la cual es necesario desconfiar por defecto de cualquier tipo de acceso a la red para mantenerla segura. INCIBE-CERT, en sus predicciones de seguridad industrial 2020-2029 señala varios factores a tener en cuenta, entre los que destacan que crecerá el interés de los ciberdelincuentes por este tipo de entornos, aumentará la superficie de ataque y como consecuencia proliferarán las herramientas para la explotación de vulnerabilidades en entornos industriales.

CLOUD COMPUTING

La nube es uno de los factores clave de toda transformación digital. Según el Enterprise

LOS RETOS DE LA INDUSTRIA 4.0

Cloud Index Report de Nutanix, el 75% del sector industrial y de fabricación señala que la crisis del coronavirus ha provocado que aumenten considerablemente sus inversiones en el cloud. Esta tecnología se podrá poner en marcha a través de diferentes modelos, principalmente IaaS (Infraestructura como servicio), PaaS (Plataforma como servicio) y SaaS (Software como servicio). INCIBE-CERT señala que la nube híbrida será fundamental para el sector industrial, ya que permite mayor interoperabilidad, escalabilidad, seguridad y una mejor administración y gestión de los activos. En cuanto al crecimiento de este segmento, IDC considera que el gasto global superará el billón de dólares en 2025.

IMPRESIÓN 3D

De acuerdo con un estudio desarrollado por HP y 3dbpm Research, el 75% de los fabricantes españoles espera un fuerte crecimiento de la fabricación aditiva. El mismo estudio revela que el 96% está de acuerdo en que este modelo les va a ayudar a la hora de que sus productos lleguen más rápidamente al mercado y 3 de cada 4 considera que la impresión 3D es útil para ayudar a superar los retos de producción, como la satisfacción de la demanda de nuevos productos y una mayor flexibilidad. Estos datos demuestran que la impresión 3D ha abierto un gran abanico de posibilidades que podrá aprovechar el sector de fabricación, ya que implica un menor coste por pieza, favoreciendo así la posibilidad de realizar tiradas cortas y permitiendo implementar mayor personalización. Además, la fabricación se vuelve mucho más veloz, ya que es posible pasar del diseño a la producción en pocas horas. Por otro lado, la impresión 3D implica también una reducción en las cadenas de suministro y en muchos casos elimina la necesidad de realizar transporte de mercancías físicas y de mantener inventarios, al poder fabricar las piezas necesarias directamente y en poco tiempo.

REALIDAD AUMENTADA

La realidad aumentada permite incorporar elementos visuales a la propia realidad y visualizarlos a través de dispositivos como gafas inteligentes o un smartphone. Para Oasys, esta tecnología va a permitir desarrollar distintas funcionalidades como prototipado, mantenimiento y reparación, transmisión en video, muestra de datos en vivo e integración con el resto de sistemas. Además implica una serie de beneficios para el sector, como facilitar la formación de nuevos profesionales, previsualizar las funcionalidades de cualquier herramienta facilitando su uso, un etiquetado de los sistemas para identificarlos en cualquier momento y facilitan la accesibilidad. Según Research and Markets, el mercado global de realidad aumentada llegará hasta los 88.400 millones de dólares en 2026.

Además, otras tecnologías como la simulación, los sistemas de Integración vertical y horizontal, el gemelo digital o los drones también van a colaborar a la hora de hacer realidad la transformación digital en el sector industrial.

LOS RETOS DE LA INDUSTRIA 4.0

DEMANDA DE PROFESIONALES CUALIFICADOS

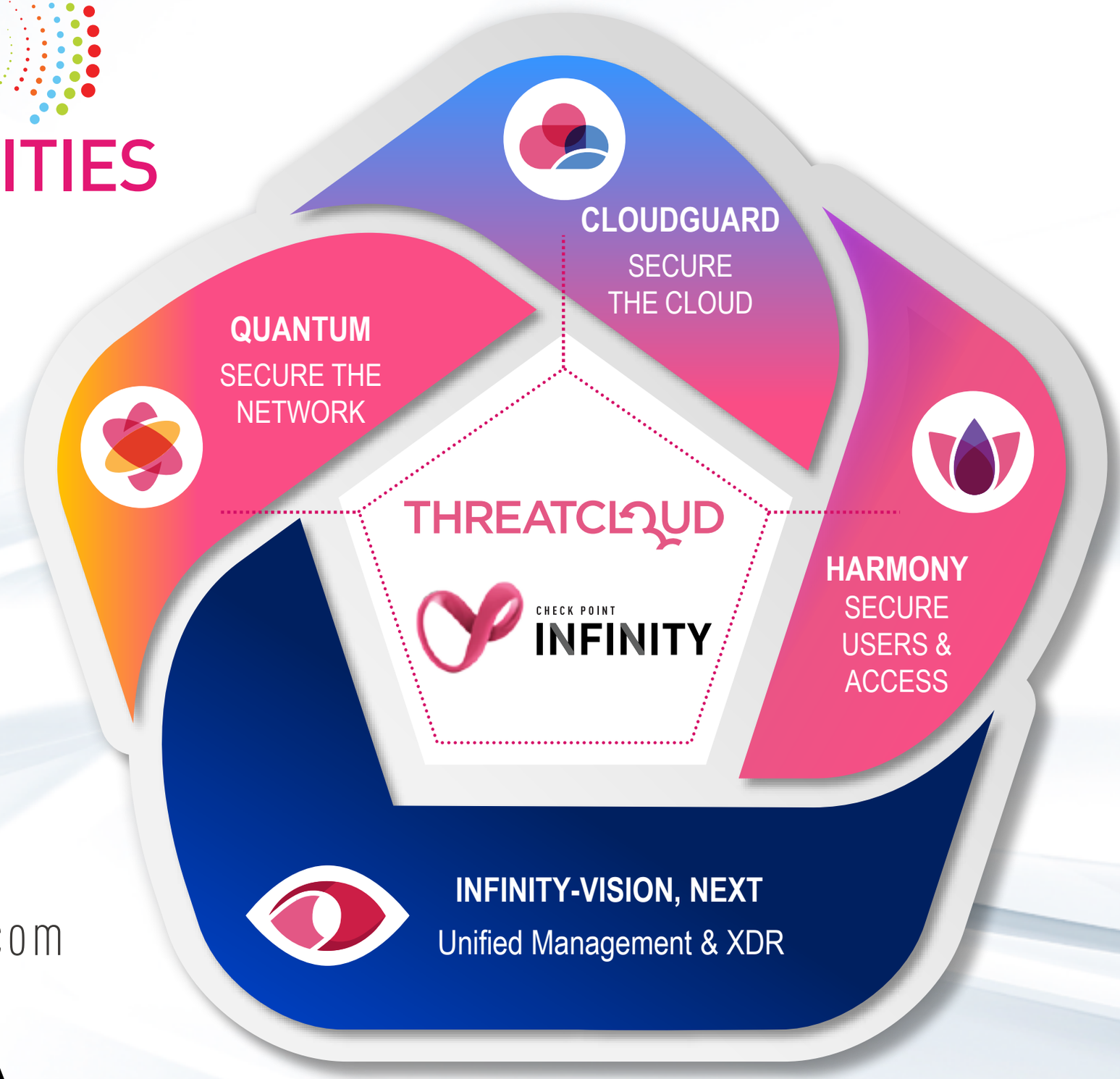
La implementación de todas estas novedades va a requerir de profesionales cualificados que sean capaces de manejar todos estos nuevos procesos, y que cuenten con una formación multidisciplinar para entender y trabajar con toda esta gran variedad de nuevas tecnologías. Según los datos del Informe de Tecnologías Disruptivas 2021 de IEBS, solo el 3,2% de los profesionales cualificados son expertos en estas nuevas tecnologías, lo que implica grandes oportunidades laborales en estos sectores. De hecho, el informe de IEBS también señala que 9 de cada 10 profesionales encuestados tiene la intención de formarse en alguna de estas tecnologías para mejorar su recorrido profesional. Sin duda, tanto las necesidades en el sector industrial como las tecnologías para solventarlas ya están sobre la mesa, ahora lo necesario es contar con profesionales técnicamente cualificados que sean capaces de hacer realidad esta transformación digital en el sector industrial. ■

MÁS INFORMACIÓN

- Informe Forces of change: Industry 4.0 de Deloitte
- Informe Global Conectedness Index de DHL
- Informe DiGiX 2020 de BBVA Research
- Plan de Recuperación, Transformación y Resiliencia del Gobierno de España
- Política Industrial España 2030 del Gobierno de España
- Informe The Industry 4.0 paradox de Deloitte
- Informe Smart Industry 4.0 en España de Everis (ahora NTT Data)
- Informe de Tecnologías Disruptivas 2021 de IEBS
- Informe sobre la evolución del mercado de tecnología para Industria 4.0 de Marketsandmarkets
- Estudio La carrera mundial por la IA de IBM
- Datos sobre ingresos mundiales del software de automatización de procesos robóticos (RPA) de Gartner
- Informe Tecnologías clave para una Industria 4.0 de DigitalES
- Datos sobre gasto global en Blockchain de IDC
- Datos sobre inversión en IoT de IOT Analytics
- Previsión de ingresos en el mercado global de Big Data de 2011 a 2027 de Statista
- Estudio sobre la evolución de las ciberamenazas en 2020 de Positive Technologies
- Predicciones de seguridad industrial 2020-2029 de INCIBE-CERT
- Enterprise Cloud Index Report de Nutanix
- Tecnología cloud en entornos industriales de INCIBE-CERT
- Datos de gasto global en cloud computing de IDC
- Estudio sobre fabricación aditiva de HP y 3dbpm Research
- Realidad aumentada en la industria. Funciones y beneficios. Oasys
- Global Augmented Reality Market Report 2021 de Research and Markets

Check Point®
SOFTWARE TECHNOLOGIES LTD

NEW WORLD
NEW OPPORTUNITIES
2021



MÁS INFORMACIÓN:

www.checkpoint.com/es

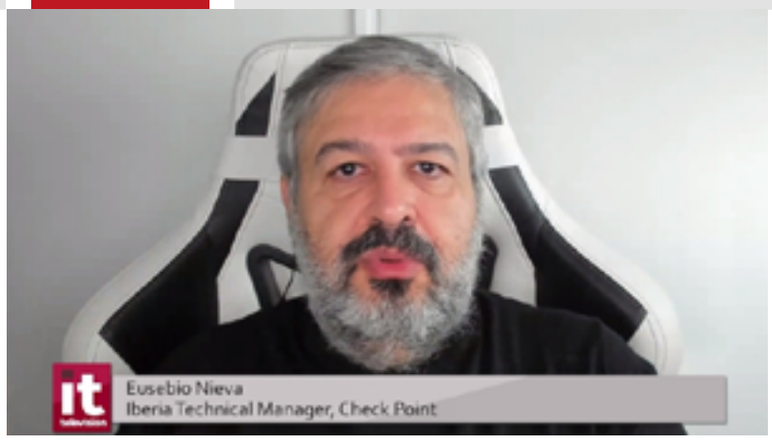
info_iberia@checkpoint.com

Los retos de la Industria 4.0

La cuarta revolución industrial, también llamada Industria 4.0, ha supuesto un gran avance para el sector, que gracias a las nuevas tecnologías y a la conectividad va a ser capaz de recoger datos con los que realizar una gran optimización de procesos e implantar soluciones y herramientas que mejoren sus rendimientos a todos los niveles. Pero el sector no debe olvidar un aspecto fundamental: la seguridad. Esta conectividad amplía enormemente el perímetro de la red, y con él las amenazas a las que se enfrenta.

La relevancia de las tecnologías IoT, así como las ventajas que ofrecen en nuestro día a día, es una realidad. Sin embargo también presentan varios inconvenientes que hay que tener en cuenta. La información que manejan estos dispositivos es cada vez más sensible o relevante, por lo que mantenerlos seguros resulta de vital importancia. Además, el crecimiento exponencial del número de estos dispositivos supone un incremento en el número de nuevas vulnerabilidades que les afectan. Por ello, ¿cuáles son los principales retos a los que se debe enfrentar el sector de la industria y la fabricación en esta cuarta revolución industrial? Para analizar el papel de la seguridad como elemento habilitador para que la industria 4.0 sea operativa; cuáles son los principales aspectos referentes a la ciberseguridad que hay que tener en cuenta en los entornos IoT e industria 4.0; cuáles son los principales tipos de ataque a los que se enfrenta este sector; cuáles son las principales medidas de prevención y cuáles son las principa-

MESA REDONDA IT: Los retos de la Industria 4.0



“Nadie se debería plantear exponer datos internos o de sus usuarios, sin dotarlos del apropiado nivel de seguridad”

EUSEBIO NIEVA

les áreas de mejora, hemos contado en esta Mesa Redonda IT con la participación de Eusebio Nieva, Iberia Technical Manager de Check Point; Carlos Tortosa, Director de Grandes Cuentas de Eset; Pedro Viana, Presales Manager Iberia de Kaspersky; Enrique Martín, Head of Business Development & Innovation Iberia de Samsung; Borja Pérez, Iberia Country Manager de Stormshield; y Jesús Gayoso, System Engineer de Trend Micro.

SEGURIDAD COMO HABILITADOR DE LA INDUSTRA 4.0

Cualquier tipo de negocio que esté conectado a internet tiene que pasar obligatoriamente por un filtro de seguridad. Para Eusebio Nieva a día de hoy ya nadie debería plantearse hacer negocios en internet sin seguridad por la gran cantidad de amenazas que existen, la dinamicidad de esas amenazas y porque precisamente la seguridad es un habilitador para que esos negocios se puedan realizar de manera correcta. “De la misma forma que ningún banco se plantea tener oficinas sin tener cierto nivel de seguridad, nadie se debería plantear exponer datos internos o de sus usuarios, servicios internos y servicios de sus usuarios en internet sin dotarlos del apropiado nivel de seguridad”.

De la misma forma opina Pedro Viana cuando indica que la ciberseguridad en la industria 4.0 es habilitadora. Para el portavoz en la industria 4.0 siempre estaremos hablando de información, hiperconvergencia y seguridad, no solamente a nivel de dispositivo, sino que como indica también “es necesario garantizar que esa información que está almacenada para la toma de decisiones y también para el correcto funcionamiento del proceso productivo esté lo más garantizada posible”.

También de acuerdo se muestra Borja Pérez, señalando que hasta ahora la disponibilidad ha sido fundamental en el diseño de las redes OT. “Ha habido ciertos momentos donde los responsables de procesos, los responsables de redes operacionales veían con cierto resquemor la ciberseguridad, porque veían un punto de posibles fallos de disponibilidad. Esto está cambiando. Ya la percepción es que sin esa ciberseguridad es

“El especialista en ciberseguridad debería participar desde el diseño de la arquitectura hasta situaciones donde nos encontramos con plantas industriales realmente con recursos muy limitados”

CARLOS TORTOSA

posible o es muy probable que se puedan tener problemas de disponibilidad”.

ASPECTOS A TENER EN CUENTA EN CUANTO A CIBERSEGURIDAD

A la hora de hablar de ciberseguridad en la industria 4.0 hay que tener en cuenta ciertos aspectos importantes, tanto al hablar de su funcionamiento como en sus comunicaciones.

Teniendo en cuenta que cualquier tecnología ha de considerar en el propio diseño los aspectos fundamentales de la ciberseguridad, Carlos Tortosa

“Es necesario que la información almacenada para la toma de decisiones y el correcto funcionamiento del proceso productivo esté lo más garantizada posible”

PEDRO VIANA

indica que se han de aplicar también estos criterios cuando hablamos de entornos industriales. “Es necesario proteger las conexiones internas, tanto para evitar posibles ataques externos como para evitar que los dispositivos dentro de la planta industrial sean la puerta de entrada de los atacantes para después acceder a dispositivos con información privilegiada, con una mayor capacidad de almacenamiento, para poder llegar a la información que el atacante está buscando. También se ha de proteger en la medida de lo posible la apertura de procesos que sean sospechosos y que puedan convertirse finalmente en una amenaza real”.

Para Enrique Martín, desde el punto de vista del dispositivo hay una serie de consideraciones importantes. “Al fin y al cabo el dispositivo almacena información, desde la información que pueda tener un directivo en un smartphone hasta un elemento conectado que tenga la cadena de producción que tenga cierta información. Al final cada uno tiene distinta información pero seguramente en gran parte de ellos es importante que esa información esté securizada, cifrada y que sea complicado acceder a ella”. También es necesario tener en cuenta la seguridad de las comunicaciones a través de mecanismos de cifrado y de securización. Además, dado que lo normal es que las empresas cada vez se dirijan más hacia el cloud, es importante la autenticación. Por último, es necesario que el software esté actualizado.

Por su parte, Jesús Gayoso indica que lo primordial es tener visibilidad para tener un control de qué es lo que está pasando en la planta, cómo está llevándose a cabo ese proceso de producción. “Hay que tener un control de la ejecución de los procesos de un servidor o de un HMI o de un controlador en cuanto a qué se puede ejecutar en esa máquina”. A nivel de comunicaciones es muy importante tener segmentación y tener un control del protocolo. Es muy importante tener control de que se estén ejecutando los procesos adecuadamente, tanto a nivel de sistemas como a nivel de comunicaciones.

“En un mundo en el que cada día aparecen nuevas funcionalidades, es fundamental tener capacidad de evolucionar”

ENRIQUE MARTÍN

PRINCIPALES TIPOS DE ATAQUE

No cabe duda de que el auge de los dispositivos IoT y su interconexión les convierte en un objetivo perfecto y diario para los ciberdelincuentes. ¿Cuáles son los principales tipos de ataque a los que se enfrenta este sector? ¿Tienen particularidades respecto a otros sectores?

En la opinión de Pedro Viana, los principales tipos de ataques dentro de la vertiente del IoT casi siempre suelen ser ataques de fuerza bruta contra dispositivos que están directamente conectados a internet, que no tienen ningún tipo de supervisión o de protección a nivel perimetral. “Por supuesto son software y dispositivos que tienen una capacidad muy limitada, consecuentemente el proceso de actualización de ese firmware o de ese sistema operativo no sigue un patrón o no si-

“Ha habido momentos donde los responsables de redes operacionales, veían con resquemor la ciberseguridad, porque veían un punto de posibles fallos de disponibilidad”

BORJA PÉREZ

gue un ritmo adecuado”. Además, los ciberdelincuentes a través de estos ataques pueden utilizar estos dispositivos para realizar ataques a otras corporaciones, o para tener acceso a cualquier red dentro de la infraestructura.

Jesús Gayoso señala que es muy importante disponer de dispositivos IPS, de sondas de red que tengan análisis de comportamiento y ver las anomalías que ese están produciendo a nivel de red en cuanto a ejecución de protocolos, a una explotación de una vulnerabilidad y una propagación en la misma red. “Yo me he llegado a encontrar en varias plantas Windows NT o Windows 2000, que ya es todavía más obsoleto. Es bastante más difícil de proteger un sistema legacy llegado a ese punto, porque ni siquiera la arquitectura del sistema operativo es la misma que en la que trabajamos a día de hoy”, comenta a la hora de hablar de la importancia de contar con sistemas actualizados. El portavoz incide en que es muy importante tener visibilidad a nivel de red, porque en cuanto exista un compromiso en una de las máquinas, en cuanto vaya a haber una propagación, se va a detectar y a partir de ahí se va a poder actuar en consecuencia.

Por su parte, Eusebio Nieva subraya que cualquiera de estas empresas es susceptible de sufrir un ataque a través de los métodos tradicionales y además por métodos más específicos en cualquier entorno industrial. “Tienen un espectro de vulnerabilidades mucho mayor precisamente porque tienen una peculiaridad. Y además, como se están moviendo muy deprisa hacia una transformación digital en la cual los dispositivos están cambiando, la forma de utilizarlos, la conectividad, dónde residen los servicios…”. En su opinión todo esto está exponiendo de manera mucho más importante a estas empresas precisamente porque tienen las mismas amenazas que cualquier empresa tradicional y además un riesgo adicional por sus propias características. Por ello tienen que abordar la seguridad desde esos dos puntos de vista.

“La mayoría tienen poca visibilidad, poca concienciación, mucha heterogeneidad en cuanto a sistemas, no tienen un control de la red, no están segmentadas las redes…”

JESÚS GAYOSO

En el resumen que hace Carlos Tortosa parte de la base de “los ataques de fuerza bruta, de la denegación de servicio, control y mando de los dispositivos, y que esto se convierte en una puerta de acceso para poder ir a parar a cualquier otro dispositivo dentro de la red”. Para él lo que se puede hacer es proteger usuarios, proteger accesos, tener visibilidad de los procesos y poner en marcha procesos de actualización. En cuanto a la concienciación, recalca que hay que tener clarísimo que desde la base de la educación de los niños más pequeños hasta situaciones como estas donde el entorno industrial tiene mucha complejidad y tiene una serie de puertas abiertas donde

el atacante puede elegir por dónde quiere entrar, es necesario concienciar al usuario e intentar que se tomen las medidas oportunas.

MEDIDAS DE PREVENCIÓN

Como se ha ido comentando, la prevención es fundamental en el entorno de la industria 4.0, pero, ¿cuáles son las principales medidas de prevención? ¿Estas medidas tienen que tener algún aspecto diferencial respecto a otros entornos?

En este sentido, Enrique Martín destaca que es necesario disponer de equipamiento y tecnología actualizada. "En un mundo en el que cada día aparecen nuevas funcionalidades es fundamental tener el software y los sistemas con capacidad de evolucionar". Esos equipos almacenan cada vez más información, por lo que hay que tener capacidad de poder cifrarla y tenerla securizada.

Al hablar del tema de las actualizaciones, Borja Pérez apunta que no es algo tan sencillo. "Las medidas tienen que ser distintas porque lo que prima en la industria es la disponibilidad". Es importante entender cuáles son los procesos industriales y cuándo se puede parar una planta, por mantenimiento, para hacer actualizaciones, etc., ya que suele ser una ventana muy estrecha en un momento muy determinado del año.

Para Carlos Tortosa no hay que olvidar el factor conocimiento. "Hay que poner en valor también el valor del profesional, en este caso el especialista en ciberseguridad, que debería participar desde el diseño de la arquitectura hasta en situaciones donde nos encontramos con plantas industriales realmente con recursos muy limitados, obsoletos y demás, y que además buscan una interconexión".

Por su parte, Pedro Viana hace hincapié en la curva de madurez del cliente. "Hay clientes que todavía están en un proceso de transferencia de conocimiento de ciberseguridad de la parte de IT, que está más que consolidado, traspasar eso a la parte de OT". Además de la prevención, es necesario señalar la importancia de la reacción, que la industria sepa qué hacer cuando ocurre un incidente. ■

Áreas de mejora

Es evidente que aún queda mucho por hacer. ¿Cuáles son las principales áreas de mejora que se deben abordar para cerrar ese gap existente? ¿Sigue siendo necesaria en estos entornos la sensibilización y la concienciación?

Como indica Borja Pérez, la sensibilización y la concienciación son claves. "Lo que vemos es que se ha avanzado un montón, en poco tiempo hay un aumento de la concienciación importante". Se ven más consultorías y más auditorías de red para saber qué se está haciendo bien o qué se debe mejorar, pero aún queda camino por recorrer.

Según Jesús Gayoso, "la mayoría de entornos pecan de lo mismo, tienen poca visibilidad, poca concienciación, mucha heterogeneidad en cuanto a sistemas, no tienen un control de la red, no están segmentadas las redes…". Son todos estos los factores que se deben abordar, a través de por ejemplo análisis de telemetría multivector.

Eusebio Nieva se muestra de acuerdo al señalar que aún queda mucho por avanzar en algunos aspectos. Pero gracias a las nuevas normativas y a los ataques que cada vez más se están produciendo "cada día hay más concienciación, cada día hay más percepción de que la seguridad tiene que ser tomada como algo fundamental".

Para finalizar, Enrique Martín comenta que "ha tenido que venir la pandemia para que todos nos sensibilicemos con la seguridad". El portavoz comenta que sigue siendo necesario seguir concienciando y seguir trabajando, porque aún quedan empresas que no son conscientes de la importancia que tiene la seguridad en su negocio.

MÁS INFORMACIÓN

Mesa redonda IT- Industria 4.0

ÓSCAR LAGE, HEAD OF CYBER SECURITY & BLOCKCHAIN
@ TECNALIA RESEARCH & INNOVATION

“La gran asignatura pendiente es poder compartir y explotar de forma segura el dato industrial”

La relevancia de las tecnologías IoT, así como las ventajas que ofrecen en nuestro día a día, es una realidad. Sin embargo, también presentan varios inconvenientes a tener en cuenta. Con Óscar Lage, Head of Cyber Security & Blockchain @ TECNALIA Research & Innovation, repasamos algunos de ellos.

La información que manejan estos dispositivos es cada vez más sensible o relevante, por lo que mantenerlos seguros resulta de vital importancia. ¿En qué estadio nos encontramos hoy en día?

La IoT industrial, o Industrial Internet of Things (IIoT), hablando de la Industria 4.0, es capaz de capturar una grandísima cantidad de información de los procesos industriales, pero a día de hoy mucha de esa información todavía no está siendo almacenada y explotada. En muchos casos, la falta de explotación de dicha información se debe precisamente al miedo a que dicha información sensible para el negocio pueda ser filtrada a otras empresas competidoras.

Nos podemos encontrar con diferentes niveles de madurez digital en la empresa industrial, desde la que ya ha adoptado IoT pero que no está almacenando ni explotando dicha información, hasta las empresas que están capturando toda la información disponible, subiéndola a cloud, y explotando dicha información con técnicas de inteligencia artificial.

Pero la gran asignatura pendiente es poder compartir y explotar de forma segura el dato industrial con terceros de cara a poder exprimir el potencial de la Inteligencia Artificial en la Industria. Las empresas conocen el potencial de este tipo de acciones, pero, a pesar de ello, todavía no existe un marco de confianza para compartir los datos

con terceros. Esperamos que los últimos avances que está realizando la comunidad científica en técnicas como criptografía homomórfica o computación multiparte, permitan generar la confianza necesaria para la creación de los tan ansiados espacios de datos industriales promovidos por iniciativas como GAIA-X o IDSA.

La tendencia de crecimiento de los dispositivos IoT es exponencial y se estima que en 2025 estos sean más de 21.000 millones. El crecimiento de estos dispositivos supone también un incremento en el número de nuevas vulnerabilidades que les afectan. ¿Cuáles son en su opinión?

La principal problemática de IoT en general es precisamente el no contemplar la ciberseguridad desde el diseño. Es muy habitual diseñar, pilotar, y comenzar la explotación de un proyecto industrial, sin que nadie se haya preguntado por los requisitos y necesidades de ciberseguridad del proyecto. Debemos de implantar una cultura de seguridad desde el diseño tanto en los fabricantes de equipamiento IoT, como en los proyectos de despliegue de infraestructura.

A pesar de que poco a poco la seguridad va cobrando una mayor relevancia en el ámbito industrial, todavía hoy en día su protagonismo es insuficiente. Muchísimos dispositivos industriales han sido diseñados únicamente bajo requisitos funcionales, incluso en muchos casos la digitalización de un equipamiento industrial se ha focalizado en "digitalizar" los protocolos analógicos con los que

"La gran asignatura pendiente es poder compartir y explotar de forma segura el dato industrial con terceros de cara a poder exprimir el potencial de la Inteligencia Artificial en la Industria"

funcionaban estos dispositivos, pasando a Ethernet comunicaciones de tipo serie diseñadas en los ochenta sin tener en cuenta las implicaciones de ciberseguridad. La Industria 4.0 ha traído la conexión de estos sistemas industriales de forma masiva, y como resultado podemos ver en rastreadores como shodan.io cómo cada vez hay más dispositivos IoT conectados directamente a internet, con protocolos no seguros y/o sin configurar ningún tipo de ciberseguridad en sus despliegues.

El auge de los dispositivos IoT y su gran interconexión les convierte en el objetivo perfecto para los ciberdelincuentes. ¿Cuáles son los principales vectores de ataque?

Podríamos decir que en la última década la tendencia ha sido maximizar la conectividad de dichos dispositivos para la explotación de datos, sin preocuparse por la seguridad, o sin un conocimiento sobre los riesgos de estas conductas. Esto desafortunadamente va cambiando por culpa de los sustos que las empresas industriales están sufriendo en los últimos años debido en parte a estas conductas.

Esta situación se ve agravada debido a que la mayoría de los dispositivos industriales no han sido diseñados para convivir con la infraestructura TI (Tecnologías de la Información), por lo que un simple escaneo de puertos, que es muy habitual en una red TI, puede suponer una parada en la red industrial.

Los protocolos de las redes industriales, además, pueden no incorporar ningún tipo de ciberseguridad. En el mejor de los casos estos dispositivos admiten las versiones más novedosas de esos protocolos industriales que incorporan protecciones específicas de ciberseguridad, pero desafortunadamente es habitual que éstas no se hayan activado para maximizar la "compatibilidad" con equipamiento legado existente en la red, o simplemente para "facilitar" el despliegue.

En muchos casos estas redes de operaciones, además, no están segmentadas ni cuentan con elementos de protección suficientes, con lo que es habitual que cualquier malware pueda propagarse de forma rápida por toda la infraestructura.

Por si fuera poco, es habitual que los dispositivos industriales estén operados por ordenadores que no han sido actualizados en muchos meses o años, y, por lo tanto, pueden existir diferentes vulnerabilidades conocidas para su sistema operativo que no han sido parcheadas. Estas situaciones

a veces son provocadas por falta de actualizaciones del fabricante, y en otros muchos casos por parte del propio operador de la infraestructura cuyo objetivo principal es maximizar la disponibilidad de la red y que ve en estas actualizaciones un riesgo de disponibilidad. Todo ello nos lleva a un riesgo menos inmediato, pero con efectos desastrosos, como es operar una red con dispositivos industriales que muestran decenas de vulnerabilidades conocidas.

Esta situación, en muchos casos, se está aprovechando por operadores de botnets que comprometen cada vez más dispositivos IoT conectados para ponerlos a su servicio.

Los nuevos procesos en la Industria 4.0 solo pueden materializarse aprovechando las oportunidades que brindan las nuevas tecnologías. Se introducen las arquitecturas en la nube, IA, Big Data o la virtualización. ¿Qué nivel de implantación tienen ya estas tecnologías y cómo complican la seguridad?

Existe hoy en día una gran adopción en las grandes y medianas empresas, que están viendo el potencial de la explotación del dato, así como la flexibilidad que les ofrece la nube o la virtualización. El peligro de la adopción de estas tecnologías es que, en muchos casos, tal y como advertíamos, es una adopción centrada exclusivamente en el ámbito funcional, sin tener en cuenta la ciberseguridad.

En la mayoría de los casos en los que no se tiene en cuenta la ciberseguridad en el despliegue de un proyecto de transformación digital, nos encontramos como consecuencia decenas o centenares de equipamientos industriales de una empresa visibles a través de internet, con los riesgos que ello supone.

La situación provocada por la COVID-19 ha originado un incremento importante del número de ataques a empresas, y los modelos Industria 4.0, no han sido ajenos a ello. ¿Cuáles has sido los sectores más afectados y de qué manera?

Indudablemente el foco durante la pandemia se ha centrado en la industria farmacéutica debido al gran valor de sus activos, las vacunas COVID-19. A nivel general lo que se ha visto es un gran incremento del phishing y ransomware, aprovechando el teletrabajo de muchos de los profesionales del sector industrial. No obstante, la industria, en general, no ha sido un ámbito en el que el teletrabajo haya sido masivo debido a las restricciones físicas y la naturaleza del sector, por lo que tampoco diría que estos ataques hayan tenido una efectividad mucho mayor que en la época pre-COVID.

¿Hacia dónde debe evolucionar la Industria 4.0 y cuáles son los aspectos más críticos de mejora desde el punto de vista de la Ciberseguridad?

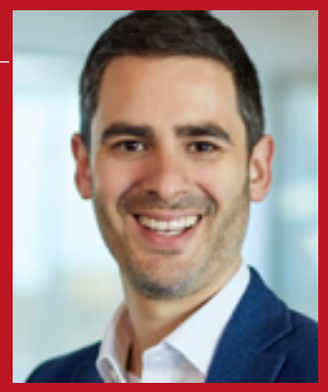
La industria debe adoptar la seguridad por diseño tanto en la fabricación de equipamiento industrial como en los despliegues de infraestructura. Es donde creo que se debería poner el foco durante los próximos años.

Precisamente si queremos maximizar la resiliencia de la industria, uno de los tres pilares fundamentales del nuevo paradigma de la Industria 5.0, debemos adoptar tanto patrones de Security by Design, como medidas de seguridad en la cadena de suministro.

Por otro lado, debemos de hacer un especial hincapié en los robots industriales, que ya están saliendo de las jaulas en las que los hemos contemplado durante los últimos años por motivos de seguridad física (safety). Estos robots van a trabajar y cooperar directamente con humanos en entornos de coworking, lo que supone un riesgo aun mayor ya que estos dispositivos en caso de fallo podrán causar daños personales a los trabajadores. ■

OSCAR LAGE

es Responsable de Ciberseguridad de Tecnalia, conferenciante, profesor y líder del primer laboratorio industrial de blockchain de Europa.



Ciberseguridad orientada al futuro

Kaspersky
Industrial
CyberSecurity

kaspersky BRING ON THE FUTURE

www.kaspersky.es

Avanzar en la digitalización de una forma segura, el mayor reto para la Industria 4.0

DAVID GALDRÁN,
Security Engineer Team Leader, Major Accounts, Check Point Software

Este año 2021 la industria ha "comenzado la vuelta a la normalidad" tras un 2020 en el que, debido a la pandemia, muchas plantas y empresas se han visto obligadas a parar su producción. La situación ha sido complicada para todo el sector y, aun ahora, están comenzando a levantar cabeza. Desde el punto de vista de la ciberseguridad, la situación vivida los últimos meses ha causado que los proyectos asociados a la misma se hayan visto paralizados durante todo el 2020 para relanzarse en 2021 lo que, aunque en un principio ha retasado un poco las cosas, actualmente está suponiendo un avance en ese proceso de digitalización e hiperconectividad que va de la mano del paradigma Industria 4.0.

A pesar de los distintos avances y puestas a punto de este sector, aún quedan bastantes puntos a desarrollar en todo lo relacionado con la ciberseguridad, que sigue sin formar parte de su ADN corporativo. Todos ellos son tremendamente relevantes para realizar una digitalización y transición al modelo Industria 4.0 de forma segura. Aunque se está haciendo un esfuerzo titánico en la creación de grupos de trabajo y se ha avanzado mucho en la innovación de planes de ciberseguridad industrial, nos seguimos encontrando, aunque cada vez menos, con escollos debidos a la falta de concienciación en el campo de la ciberseguridad OT.

Industria 4.0 es sinónimo de Transformación Digital de la cadena de producción, lo que implica que las amenazas más comunes que afectan a este sector tienen relación con el equipamiento productivo, ya que no está pensado para que la comunicación IP tenga que enviar información a sistemas que, a veces, se encuentran en zonas con conexión a internet (eso sino se comunica el equipo directamente con un activo que esté presente en internet o similar...). Por ello, en muchas ocasiones se ha dado visibilidad a la cadena de producción en el exterior lo que ha hecho que amenazas como el ransomware estén cada vez más presentes en el mundo industrial. Derivado de esta nueva situación, se puede dar el caso de que algún ciberdelincuente llegue a secuestrar una cadena de producción y pedir dinero a cambio de la liberación, o el robo de la propiedad intelectual como, por ejemplo, la fórmula de un químico para hacer un producto igual a menor precio.

LA AUSENCIA DE UNA ÚNICA NORMA DE CIBERSEGURIDAD INDUSTRIAL ES UNO DE LOS PRINCIPALES PROBLEMAS PARA LA INDUSTRIA 4.0.

Por el lado contrario, nos encontramos con que los sectores de la Industria 4.0 más protegidos son las denominadas Infraestructuras Críticas. Seguramente, debido a la presión que ha ejercido la administración y la Unión Europea para el establecimiento de un plan de ciberseguridad, los operadores críticos ya cuentan con un uno para el ámbito industrial y están actualmente implantando medidas de control. Está claro que aquellos sectores que cuentan con operadores críticos entre sus filas son los más avanzados. En cambio, hay otros, como por ejemplo las utilities, que hoy en día aún

están diseñando un plan de ciberseguridad industrial a la vez que avanza la digitalización. Lo que hay que tener claro es que, dentro del mismo sector, nos podemos encontrar con empresas con un nivel de madurez muy alto, mientras otras apenas han comenzado su transformación.

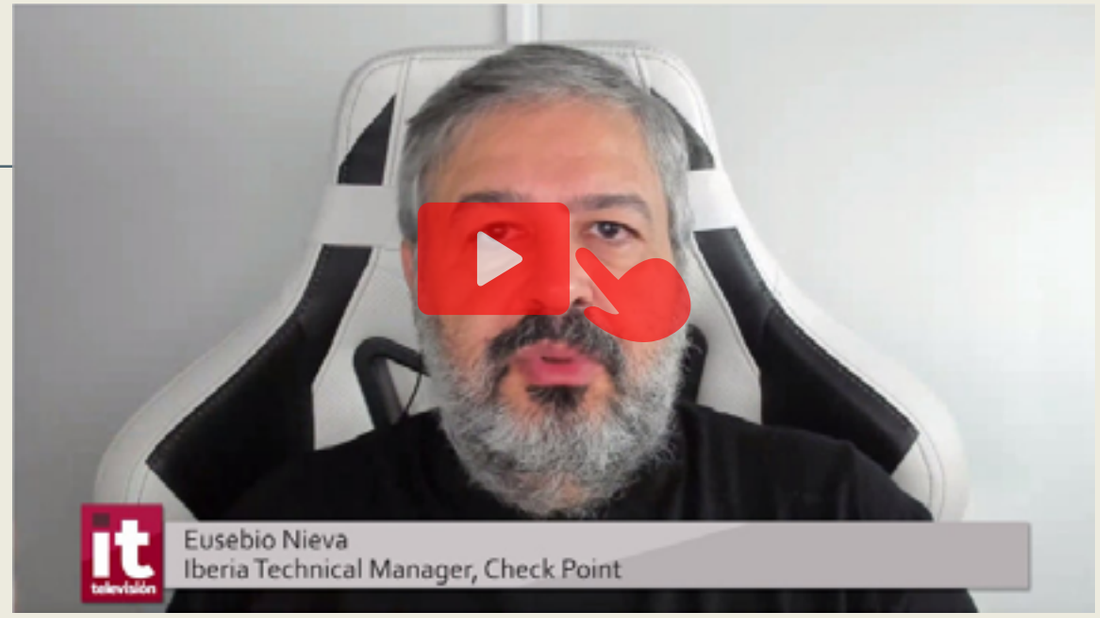
La ausencia de una única norma de ciberseguridad que se pueda llegar a aplicar a toda la industria no ayuda en esta tarea. Esta falta de estandarización es la que está haciendo que, determinadas secciones industriales que tienen presencia "mundial" tengan que definir su propia norma como una mezcla de ambas.

A lo largo del próximo 2022 los ataques de ransomware y robo de información a las empresas de la Industria 4.0 van a crecer exponencialmente acompañados de la evolución y avance de la transformación digital de sus distintos sectores. Los problemas que puede conllevar el no instalar las medidas necesarias de protección de software en los sistemas OT pueden ir mucho más allá de lo que las empresas puedan llegar a imaginar. La medida de solventar un ataque siempre va a estar ahí, pero la mejor estrategia, sin duda, pasa por implementar un plan de prevención para evitar cualquier tipo de riesgo antes de que suceda. Para ello, es imprescindible avanzar en la digitalización de una forma segura con el objetivo de evitar estar expuestos a las cada vez más recurrentes amenazas. ■

EUSEBIO NIEVA, IBERIA TECHNICAL MANAGER DE CHECK POINT

Adaptar la seguridad a los peligros de hoy

Desde que el uso de los dispositivos IoT en el mundo de la industria 4.0 se ha extendido y su despliegue cada vez es mayor, este sector se ha convertido en un objetivo para los ciberdelincuentes. Por ello es necesario contar con un plan de acción en materia de seguridad.



En el sector industrial existen muchas compañías a las que aún les falta mucho camino por recorrer a la hora de abordar la seguridad de sus activos tecnológicos. Para Eusebio Nieva, Iberia Technical Manager de Check Point, hay que contar siempre con una seguridad adaptada a los peligros que pueden venir, con enfoques novedosos como pueda ser el Zero Trust.

Entre los principales retos a los que se enfrenta la seguridad en entornos industriales, hay que tener en cuenta primero a nivel interno que se trata de un sector resistente al cambio y con una metodología muy establecida, por lo que abordar esa transformación digital y envolverla de una capa de seguridad no debe interferir con el propio funcionamiento de la compañía. Por otra parte, no hay que olvidar todas las amenazas que pudieran provenir de una conexión con el exterior. Por todo ello, lo fundamental es establecer una estrategia flexible que marque cómo se ha de abordar la securización de este nuevo paradigma.

La ciberseguridad en las empresas 4.0 no es una opción,

sino una herramienta esencial para garantizar el éxito

CARLOS TORTOSA,
Director de Grandes Cuentas de ESET

Vivimos en un mundo cada vez más interconectado a través de Internet y el mundo empresarial no es una excepción. Esta interconexión necesaria surgida en los últimos años, por ejemplo, ha motivado que las instalaciones tipo SCADA, DSS o PLC, que tienen en su arquitectura una amplia intervención del propio fabricante del dispositivo, tuvieran que conectarse con el resto de la red para recopilar información necesaria a nivel organizativo.

Esta situación ha supuesto que instalaciones tipo "caja negra" donde no existía ninguna opción de acceder de manera remota al dispositivo de control industrial asumieran el riesgo de estar conectadas a redes de amplio rango de acceso a Internet y, por lo tanto, expuestas a los mismos riesgos que el resto de dispositivos con acceso a cualquier tipo de aplicativo que requiera de acceso externo.

Ante este panorama tan dependiente de Internet no todas las áreas industriales han tenido opción de afrontar el riesgo con la misma eficacia, y como consecuencia se han ido abriendo claras brechas de seguridad en entornos donde, incluso con intención de hacerlo, resulta sumamente complicado poder aplicar soluciones de seguridad.

Precisamente, llegado a este punto cabe preguntarse cuáles son las principales vulnerabilidades que podrían afectar al mando y control de los propios dispositivos, es decir que un atacante tenga capacidad de acceder a estos y modificar el comportamiento, bloquear el acceso a promover actuaciones fuera de toda norma, como podría ser el acceso a dispositivos IoT que tengan que ver con infraestructuras críticas. De hecho, mucho se ha hablado de un posible ataque que podría producirse en plantas potabilizadoras de agua y el efecto que este podría tener o el control de plantas de generación eléctrica, ahora que está tan de moda el posible "apagón general".

Igualmente, otro de los riesgos que pueden tener es que este acceso permita a los atacantes llegar a otro tipo de dispositivo interconectado con estos IoT posibilitando así que con una "puerta trasera" el riesgo se trasladara a equipos supuestamente bien protegidos dentro de la red corporativa y que el IoT fuera únicamente el vehículo de acceso a otros dispositivos.

Por otro lado, se hace inevitable al hablar de la industria 4.0 destacar el avance tecnológico que supondrá el 5G para ella, puesto que conllevará que el acceso a la información sea mucho más rápido fiable y aplicado y esto supondrá una mejora tanto en los procesos como en los productos que serán más rentables, eficientes y seguros.

Si bien es cierto que la mejora será importante, se debe tener en cuenta, también, un importante escollo con el que la industria se va a encontrar y es la actualización de los sistemas que funcionan en los entornos industriales ya que estos suelen resultar sumamente complejos y en ocasiones prácticamente inasumibles, es decir, que en muchas instalaciones industriales será todo un reto acondicionar la infraestructura para que estos dispositivos puedan funcionar de manera conveniente con tecnología 5G, que es más eficiente y supuestamente más segura.

Sin embargo, una vez salvado este inconveniente, evidentemente este avance tecnológico es muy positivo para el entorno empresarial.

Por último, es importante subrayar que lo primero que deben considerar las empresas a la hora de diseñar una estrategia de ciberseguridad es tener en cuenta todos los aspectos que puedan suponer un posible inconveniente a largo plazo. También es importante la información relativa al consumo de energía, niveles de productividad, la interacción con el sistema de control general de las plantas de producción... Y es igualmente esencial saber qué dispositivos requieren de interconexión con otros y asegurarse que estos dispositivos tengan aplicada una política de ciberseguridad desde el propio diseño, que permita actualizaciones del sistema, así como el despliegue de parches o el mando desde el centro de control de ciberseguridad que el cliente tenga implementado en el resto de la red. Es decir, que se tenga en cuenta que el ciclo de vida de la instalación ha de contemplar la posibilidad de aplicar mejoras a nivel de ciberseguridad tan necesarias hoy en día. ■

CARLOS TORTOSA, DIRECTOR DE GRANDES CUENTAS DE ESET

"Hay que pensar en la protección desde el diseño"

Los entornos industriales de tipo SCADA se han visto abocados a tener que interconectarse con el resto de dispositivos de una red corporativa, a pesar de que no estaban diseñados para ello. Esto ha supuesto una serie de vulnerabilidades que se han convertido en todo un reto para la seguridad.

La necesidad de interconectar dispositivos que no estaban preparados ha abierto la puerta a que algún atacante pueda acceder a los mismos. Carlos Tortosa, Director de Grandes Cuentas de Eset, señala dos peligros fundamentales: que un acceso exterior pueda obtener el control de estos dispositivos, con lo que todo ello pudiera conllevar por ejemplo a la hora de hablar de infraestructuras críticas, o que a través de esta vía de entrada pueda irrumpir en otras partes de la red corporativa.

Por ello la compañía recomienda que a partir del propio diseño o definición de la estructura se tenga en cuenta que tiene que ser protegida. Asimismo, es necesario tener en cuenta la necesidad de actualización de esos sistemas, por lo que habrá que hacerlos accesibles a través de algún entorno tipo consola de administración que permita este acceso a la hora de actualizar el sistema sin necesidad de parar el proceso productivo.

Avanzando hacia la industria 4.0 con seguridad

ALFONSO RAMÍREZ,
director general
Kaspersky Iberia

Históricamente, las empresas industriales de todo el mundo han abordado la ciberseguridad en sus redes de TI y OT (tecnología operativa) de manera diferente. De hecho, la mayoría de las empresas ya cuentan con medidas maduras de detección de infracciones y respuesta a incidentes en su infraestructura corporativa, pero cuando se trata de la tecnología operativa este enfoque suele encontrarse bastante desfasado.

Sin embargo, la creciente tendencia de Industria 4.0, también llamada industria inteligente o cuarta revolución industrial, busca transformar a la empresa en una organización inteligente para conseguir los mejores resultados de negocio.

Términos como fabricación aditiva, robótica colaborativa, herramientas de planificación de la producción, visión artificial, realidad virtual, gamificación, simulación de procesos, inteligencia operacional o IoT, entre otras, suponen que las empresas industriales sean cada vez más "digitales", incrementen constantemente su inversión en tecnología inteligente y, en consecuencia, se desdibuje la frontera tradicional entre los entornos de TI y OT, por lo que las ciberamenazas pueden llegar con mayor frecuencia a los sistemas de control industrial. De hecho, según un reciente informe de Kaspersky ICS CERT, en el primer semestre de 2021 el porcentaje de ordenadores industriales en los que se detectaron objetos maliciosos alcanzó el 33,8%.

INTERNET, CORREO ELECTRÓNICO Y DISPOSITIVOS EXTRAÍBLES: ORIGEN DE LAS AMENAZAS

Las amenazas provenientes de Internet crecieron en este semestre un 1,5% y fueron detectados en el 18,2% de los equipos industriales. Las amenazas que llegan a través de conexiones de medios extraíbles se bloquearon en el 5,2% de los ordenadores ICS, lo que supone un descenso del 0,2 % respecto del semestre anterior y confirma la tendencia a la baja iniciada en el segundo semestre de 2019.

Por último, los archivos adjuntos maliciosos del correo electrónico se bloquearon en el 3,4% de los ordenadores industriales, lo que supone un descenso del 0,6% respecto al semestre anterior. Los países del sur de Europa (Italia, España, Grecia y Portugal) destacan en el Top 15 como los más afectados por este tipo de ataques. En concreto en nuestro país se bloqueó un 5,7% de este tipo de amenazas provenientes de adjuntos al correo electrónico.

Vistas las cifras, el riesgo de infección es claro. De hecho, no siempre es necesario que la empresa industrial sea el objetivo, también existe el riesgo de infección accidental por malware convencional: una simple unidad flash o un mensaje de correo electrónico de tipo phishing con un troyano bancario o ransomware introducido involuntariamente en el entorno ICS puede afectar seriamente a la actividad principal de una empresa. Incluso si las infecciones accidentales no se producen con demasiada frecuencia, es evidente que un hacker motivado también puede penetrar en las redes de OT y causar daños considerables a la producción o en equipos de gran valor, o bien robar información valiosa.

Tampoco se puede olvidar que más del 80% de los ciber-incidentes en las empresas se deben a errores humanos y la mejor manera de afrontarlos es la formación. Ya existen en el mercado

soluciones de formación gamificada online que utilizan las técnicas más modernas de aprendizaje y abordan todos los niveles de la estructura empresarial. Este tipo de soluciones brinda a las organizaciones una serie de resultados muy alentadores, ya que consiguen hasta un 90% de reducción en el número total de incidentes y un 50% de reducción en el impacto económico de los incidentes.

Por ello, para que las empresas industriales puedan avanzar seguras en la digitalización es importante que tengan en cuenta unas medidas básicas de ciberseguridad:

- Protección de los endpoints industriales para prevenir las infecciones accidentales y dificultar las intrusiones motivadas.
- Supervisión de la red de OT y detección de anomalías para identificar acciones maliciosas en el nivel PLC.
- Programas de formación para los empleados con el fin de reducir los accidentes y minimizar el factor humano.
- Servicios de expertos dedicados a investigar la infraestructura, llevar a cabo análisis de expertos o mitigar el impacto de un incidente. ■

MÁS INFORMACIÓN

Ciberseguridad orientada al futuro

Kaspersky Industrial Cybersecurity

PEDRO VIANA, PRESALES MANAGER IBERIA DE KASPERSKY

"La visibilidad es la clave"

A pesar de que el nivel de la ciberseguridad en el sector industrial español está mejorando, aún queda mucho camino por recorrer. Amenazas como los ataques dirigidos o el ransomware pueden poner en jaque a las infraestructuras críticas del país. La monitorización es fundamental para poder reaccionar a tiempo ante cualquier tipo de problema.

Aún queda mucho margen de mejora a la hora de analizar la ciberseguridad en el sector industrial. Así lo señala Pedro Viana, Presales Manager Iberia de Kaspersky, que menciona varios verticales que están recibiendo un mayor número de amenazas dentro del sector industrial: la inmótica, la cadena de suministro, Oil&Gas, energía y la industria automovilística. Entre los riesgos que más pueden afectar al sector industrial destacan los ataques dirigidos, las URLs maliciosas y los scripts, el compromiso de los sistemas para el minado de criptomonedas y el ransomware, amenaza que cada vez va a más. Por ello, para la compañía de seguridad la monitorización de los sistemas es clave para poder generar una respuesta de la forma más adecuada posible en caso de incidente, de tal forma que no tenga impacto en el proceso productivo.

ESET BUSINESS SOLUTIONS

BLINDA TU EMPRESA CON LA COMODIDAD DE LA NUBE

Gestiona toda la ciberseguridad de tu empresa estés donde estés.

PREDICCIÓN	PREVENCIÓN
ESET Threat Intelligence ESET Virus Radar WeLive Security	Endpoint Protection Platform ESET Mail Security ESET Sharepoint Security ESET Secure Authentication ESET Endpoint Encryption ESET PROTECT
ESET Enterprise Inspector ESET Dynamic Threat Defense ESET PROTECT	Endpoint Protection Platform ESET Dynamic Threat Defense ESET Enterprise Inspector ESET Mail Security ESET Secure SharePoint Server ESET Secure Authentication ESET Endpoint Encryption ESET PROTECT
RESPUESTA	DETECCIÓN

CYBERSECURITY EXPERTS ON YOUR SIDE

PROVEEDOR Nº 1 DE LA UNIÓN EUROPEA EN CIBERSEGURIDAD EMPRESARIAL

MADE IN EU

La seguridad móvil
un factor clave para la nueva Industria 4.0

ENRIQUE MARTÍN,
Head of Business Development & Innovation Iberia

Uno de los principales objetivos de los Fondos Europeos de Recuperación es que los países miembros refuercen su economía. Para ello, la Unión Europea está decidida a digitalizar la industria para proporcionar productos y procesos de mayor valor, con el fin de ser más competitivos. Para llevar a cabo esta transformación, será muy necesario apoyarse en las nuevas tecnologías de conectividad, como 5G, y en aquellos dispositivos que nos permiten ganar productividad y eficiencia en todo tipo de escenarios. Pero lo más importante, será la seguridad, que habilitará redes y puntos de acceso a la información fiables, en un nuevo mundo hiperconectado que sentará las bases de la Industria 4.0.

En Samsung estamos preparados para proporcionar la tecnología y los dispositivos necesarios para abordar con éxito la transformación de procesos y de los negocios en la industria 4.0. En nuestro caso, el ecosistema Galaxy cada vez es mayor, con las máximas prestaciones y las ultimas innovaciones en conectividad 5G y Wifi 6E. La productividad en el puesto de trabajo es otro de nuestros focos, los dispositivos móviles disponen de la potencia y funcionalidades necesarias para que seamos efectivos y eficientes en nuestro trabajo, por ejemplo, gracias a Samsung DeX (que permite usar un terminal móvil como un portátil, transformando la interfaz de usuario en una experiencia similar a la de un PC) y a las funciones multitarea en los plegables serie Z (con la opción de utilizar S Pen para tomar notas) podemos gestionar procesos y realizar tareas en cualquier lugar y momento. También llevamos la eficiencia más allá de la oficina a empleados con trabajos en movilidad (personal en tiendas, sucursales, restaurantes, fabricas, agricultura, construcción, salud, logística, seguridad, instaladores) gracias a la familia de equipos rugerizados para profesionales que trabajan en entornos exigentes, con humedad y temperaturas extremas.

Y, por supuesto, otro factor clave: la seguridad. Somos el único fabricante de dispositivos que adopta una estrategia tan amplia e integral para garantizar la seguridad de la información. Empezamos con el diseño y la fabricación de los componentes de hardware en nuestras propias fábricas, y durante ese proceso incorporamos la plataforma de seguridad Knox en el hardware y el sistema operativo, para asegurar la integridad del dispositivo en todo momento. Así, desde su iniciación hasta la ejecución de tareas, nuestros clientes –sean consumidores o empresas–pueden confiar siempre en su dispositivo, y en las aplicaciones o datos que se encuentre en él. Además, Knox es una plataforma abierta, lo que supone que

todas las mejoras y capacidades están a disposición de la industria, para que puedan utilizarlo en sus soluciones y estas sean más seguras y flexibles.

También ofrecemos un grado de compromiso con la seguridad, ya que la mayoría de los productos Galaxy lanzados desde 2019, incluidas las series Z, S, Note, A, XCover y Tab, ahora recibirán al menos cuatro años de actualizaciones. Por último, nuestros dispositivos son los únicos que están probados y certificados por el CCN, aptos para ser utilizados en despliegues ENS Alto, y colaboramos con el INCIBE en España para mejorar la seguridad de nuestras empresas, lo que demuestra que también otros actores de la industria avalan nuestra estrategia de seguridad móvil. En definitiva, ponemos nuestra experiencia, innovación y capacidad de respuesta al servicio de la Industria 4.0 y de la movilidad. De esta manera ayudamos a que las empresas puedan desarrollar todo su potencial con seguridad y garantías, lo que les facilitará afrontar la transformación digital con éxito. ■

ENRIQUE MARTÍN, HEAD OF BUSINESS DEVELOPMENT & INNOVATION IBERIA DE SAMSUNG

"Hay que apostar por la innovación y la seguridad"

El perímetro se ha convertido en algo muy difícil de controlar, debido a la gran cantidad de dispositivos y otros elementos que han comenzado a conectarse entre sí en esta nueva revolución industrial. Por ello es necesario concienciar a las compañías de que la ciberseguridad de este nuevo entorno 4.0 es muy importante.

La digitalización y la movilidad permiten acceder a información en cualquier lugar y en cualquier momento, además de poder aportar información a los procesos industriales. Para Enrique Martín, Head of Business Development & Innovation Iberia de Samsung, esta es una de las grandes ventajas que permite la movilidad dentro del entorno industrial, haciendo que los procesos cada vez sean más automatizados y más inteligentes, de manera que la empresa sea mucho más eficiente y productiva. El 5G va a traer mejoras tanto en conectividad, como en velocidad, calidad y retardo. La seguridad de este nuevo entorno debe incidir mucho en el dispositivo, tanto a la hora de proteger lo que contiene como las conexiones que va a realizar, a través de métodos de autenticación robusta. Además, no hay que olvidar la importancia de tener la capacidad de actualizar y tener el software actualizado en todos los sistemas de la compañía.

Hacia un mundo OT eficiente y seguro:

la ciberseguridad industrial a examen

BORJA PÉREZ,
Iberia Country Manager de Stormshield

Los ciberataques contra la industria se están diversificando. Empresas energéticas, manufactureras, de distribución o transporte y movilidad están sufriendo importantes episodios de ransomware, con un impacto directo en sus cuestiones operativas. El ansia de ciberdelincuentes por infiltrarse y aprovechar las conexiones entre OT e IT para obtener acceso a las capas inferiores industriales, es una cuestión crucial que toda industria debe abordar.

En la ciberseguridad de los sistemas industriales existen tres puntos débiles que deben ser abordados con la máxima celeridad. Así, la gestión de un extenso conjunto de recursos industriales (a través de una arquitectura distribuida), con fábricas cada vez más interconectadas, supone un importante riesgo de propagación de ataques. Lo mismo ocurre con la creciente permeabilidad entre los sistemas industriales y los sistemas de información, al abrir nuevas superficies de ataque; o con el cibergobierno, un reto para los departamentos de IT y OT. El ERP (en el lado de IT) y el MES (en el lado de OT) están cada vez más interconectados, intercambiando más y más datos, por lo que cualquier ataque contra IT afectaría también a OT, como ha ocurrido recientemente a varios actores industriales (Trigano, Tata Steel u Honda, entre otros).

SEGMENTAR PARA PROTEGER

Para evitar incidentes de este tipo, y garantizar que cualquier ataque se detenga y se contenga en un único lugar, realizar una segmentación para aislar los distintos sistemas (producción, calidad y seguridad) ayudará a minimizar los ataques de rebote.

No obstante, estas medidas de protección digital, que son esenciales y sientan las bases de la seguridad global, requieren la adopción de tres pasos esenciales de seguridad: mantener la barrera entre IT y OT, lo que supone segmentar los sistemas de información y las fábricas entre sí, la red de la oficina y el sistema industrial, el sistema industrial e internet... en definitiva, garantizar que haya un nivel básico de seguridad entre las fábricas y todo lo demás. El segundo paso consiste en segmentar la red industrial, para evitar que, en caso de ataque, este se extienda por toda la planta. La introducción de la segmentación permite asegurar ciertas zonas, frenar el ataque y contenerlo. Por último, la tercera etapa consiste en acercarse lo más posible a los controladores industriales y asegurar las comunicaciones entre ellos. Como ocurre con la IT tradicional, la IT industrial necesita controlar sus comunicaciones utilizando los cortafuegos adecuados. Y esto es así incluso en la nube.

ASEGURANDO LO QUE ESTÁ EN LA NUBE

Por su creciente importancia, la nube se está convirtiendo en un nuevo factor a tener en cuenta en la estrategia global de seguridad. En este sentido y por estar directamente conectada al sistema industrial, su uso conlleva nuevos retos de seguridad, que evidencian la necesidad de proteger los datos subidos a la nube, instalando cortafuegos

en la nube para lograr que las comunicaciones entre el sistema industrial y la nube sean seguras, y salvaguardar su infraestructura, para evitar que cualquier problema pueda ser transmitido al sistema industrial.

Una última cuestión importante es el mantenimiento remoto. ¿Quién dice que no sea más peligroso el uso negligente de una llave USB que un ataque desde el sistema informático? Cada vez que alguien se conecta a distancia a la red de la empresa para recuperar datos de un servidor, expone un punto débil entre el servidor y el mundo exterior. Por tanto, es imperativo que el túnel de comunicación sea seguro: que el usuario pueda autenticarse adecuadamente y que los intercambios estén cifrados.

LA MEJOR PROTECCIÓN

Dado que las organizaciones industriales se enfrentan a los mismos riegos que las tradicionales, adoptar un enfoque de protección basado en la segmentación de la red, el uso seguro de la nube y el mantenimiento de las mejores prácticas digitales se convierte en la medida más eficaz para contener las ciberamenazas y evitar que el malware se propague dentro de una infraestructura de IT u OT. De igual modo, y para las necesidades específicas del mundo industrial, una oferta compuesta por cortafuegos industriales y un agente de seguridad para endpoint permite abordar la industria del futuro con total tranquilidad cibernética. ■

BORJA PÉREZ, IBERIA COUNTRY MANAGER DE STORMSHIELD

“Un entorno industrial es más vulnerable que un entorno TI”

Las empresas industriales están evolucionando muy rápidamente hacia la Industria 4.0 por todas las ventajas que les aporta. A pesar de ello, se está dejando un poco de lado la ciberseguridad. Hoy por hoy, estas organizaciones están expuestas a los mismos peligros que las redes IT pero aún les falta concienciación en seguridad.

El sector industrial es un entorno muy heterogéneo, con lo cual es posible encontrar realidades muy diversas. Según Borja Pérez, Iberia Country Manager de Stormshield, en general son redes u organizaciones que han pasado de estar desconectadas a estar completamente conectadas, aumentando la superficie de ataque en gran medida, por lo que se trata de un entorno más vulnerable que el entorno IT y menos acostumbrado a lidiar con estos riesgos. Las grandes barreras que se dan en este sector son que existe una separación entre el mundo de procesos y el de IT, así como el miedo a que la introducción de cualquier elemento vaya a tener un impacto en la disponibilidad de la planta. Por ello, a la hora de implantar un sistema de ciberseguridad es necesario primero hacer una auditoría para comprobar la composición de la red y chequear qué procesos deben comunicarse entre sí para poder realizar una segmentación adecuada.

Endpoints de ICS: bajo la lupa de las ciberamenazas

RAÚL NÚÑEZ HERRERO,
sales engineer y experto en ciberseguridad, Trend Micro Iberia

La seguridad de los Sistemas de Control Industrial (ICS) ha pasado a un primer plano debido a la mayor exposición de los entornos industriales por la creciente interconexión entre el proceso empresarial TI y el proceso OT. Aunque esta interconexión mejora la visibilidad, la eficiencia y la velocidad de información, también expone al entorno ICS a las amenazas que han estado afectando a las redes de TI durante décadas.

La relevancia o importancia que tiene este tipo de redes motiva aún más a los atacantes ya que pueden adquirir mayor notoriedad o lograr un mayor beneficio económico gracias a la criticidad de las redes ICS.

El malware introducido en una red ICS puede proporcionar información sobre el entorno de la red afectada, esta información es utilizada directamente por el software malicioso para hacerse con persistencia en la red gracias a la explotación de vulnerabilidades encontradas dentro del entorno ICS.

Ante este escenario, la visibilidad, conocimiento y protección de los endpoints permite evitar tiempos de inactividad involuntarios y pérdida de control del entorno ICS.

Los métodos utilizados en los ataques actuales combinan tanto técnicas modernas como malware persistente antiguo que permite hacerse con el control de las máquinas de una manera silenciosa.

La presencia cada vez mayor de ransomware en los entornos ICS, indica que los atacantes están empezando a reconocer estos sistemas y atacándolos más activamente. Esto significa que se debe dar un mayor peso a la seguridad antes de interconectar la red TI con la red OT.

Una de las claves principales es que el personal de seguridad de TI aborde la seguridad hablando previamente con el personal de sistemas del entorno OT para que puedan comprender y abordar la seguridad con herramientas focalizadas a las necesidades de dicho entorno. Es necesario abordar la compatibilidad del sistema operativo y los requisitos de tiempo de actividad, y aprender el proceso y las prácticas operativas para llegar a una estrategia de ciberseguridad adecuada para proteger correctamente estos sistemas críticos.

RECOMENDACIONES

Éstas son algunas recomendaciones para asegurar los endpoints de ICS:

❖ Aplicar parches con prontitud es vital. Si esto no es posible, considere la posibilidad de aplicar una correcta política de parcheo virtual tanto a nivel de red como a nivel de host gracias a las soluciones de Trend Micro.

❖ Utilice herramientas de reconocimiento y control de aplicativos para hacer un correcto bastionado de los host.

❖ Utilice herramientas de detección y respuesta a amenazas que permitan barrer las redes en busca de IoC.

❖ Restrinja los recursos compartidos de la red y aplique combinaciones sólidas de nombre de usuario y contraseña para evitar el acceso no autorizado a través de la fuerza bruta de credenciales.

❖ Utilice un IDS o IPS para establecer una línea de base del comportamiento normal de la red y así detectar mejor la actividad sospechosa.

❖ Escanee los endpoints de ICS en entornos cerrados con herramientas independientes.

❖ Aplicar el principio del mínimo privilegio a los administradores y operadores de redes OT. ■

JESÚS GAYOSO, SYSTEM ENGINEER DE TREND MICRO

"Las redes industriales están más expuestas, y hay que tener mayor control sobre ellas"

Cada día las redes están más interconectadas. Antiguamente hablábamos de plantas industriales completamente aisladas y controladas, a día de hoy cada vez hay más conectividad. Para contar con unos sistemas completamente seguros es necesario tener el control de todos los procesos que se definen en una planta.

Cada vez hay mayor concienciación, pero las plantas industriales deben de acelerar los conceptos básicos como visibilidad, concienciación de los usuarios, segmentación de las redes y control de lo que está ocurriendo en una planta. Jesús Gayoso, System Engineer de Trend Micro, señala que las redes están más expuestas y hay que tener un mayor control sobre ellas, sobre todo a causa de sistemas operativos obsoletos, que no pueden parchearse, que son más vulnerables y los ataques cada vez son más sofisticados. La industria 4.0 se basa en recoger datos y en que las máquinas puedan tomar decisiones por sí mismas, por lo que hay que tener muy controlado el entorno y la planta industrial. Lo primordial es tener una segmentación y una visibilidad de la red, sobre todo segmentar esas redes críticas en cuanto a nivel de operación y producción.

SAMSUNG

Tu “Todo en uno”

Mitad smartphone. Mitad tablet. Galaxy Z Fold3 es resistente al agua, compacto y puede ejecutar varias aplicaciones a la vez. ¡Ideal para trabajar sobre la marcha!

Galaxy Z Fold3

Soluciones específicas para cada necesidad

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". Por ello, abordan las necesidades de ciberseguridad más inminentes de las organizaciones basándose en tres principios básicos. Estos principios son:

- **Enfoque de prevención:** implementar protecciones de usuario preventivas para eliminar las amenazas antes de que lleguen a los usuarios.
- **Gestión Gold Standard:** panel único para gestionar todo el patrimonio de seguridad.
- **Solución consolidada:** protección preventiva completa contra las amenazas más avanzadas mientras se logra una mejor eficiencia operativa.

SECURE YOUR EVERYTHING CON CHECK POINT INFINITY

En esta nueva normalidad, los clientes merecen 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 esta visión, en 2021 han recalibrado su oferta de productos Infinity para enfocarse en 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 el acceso remoto más fácil y seguro (basado en la adquisición de Odo), navegación segura por Internet, punto final y seguridad móvil 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 las 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 establece el estándar de oro para proteger 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, continúan aprovechando Maestro, su solución de rendimiento escalable. Acelerarán la innovación en el firewall del centro de datos con la introducción de un gateway de firewall 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 la 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 seguridad 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 son los mejores para prevenir la quinta generación de ciberataques. Además, lanzan una nueva serie de dispositivos para sucursales y oficinas dirigidos a las pequeñas y medianas empresas: Quantum SPARK.

INFINITY VISION, GESTIÓN UNIFICADA Y XDR

Alcance una gestión de seguridad unificada y un 100% de prevención de brechas de seguridad. Administre todo su 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

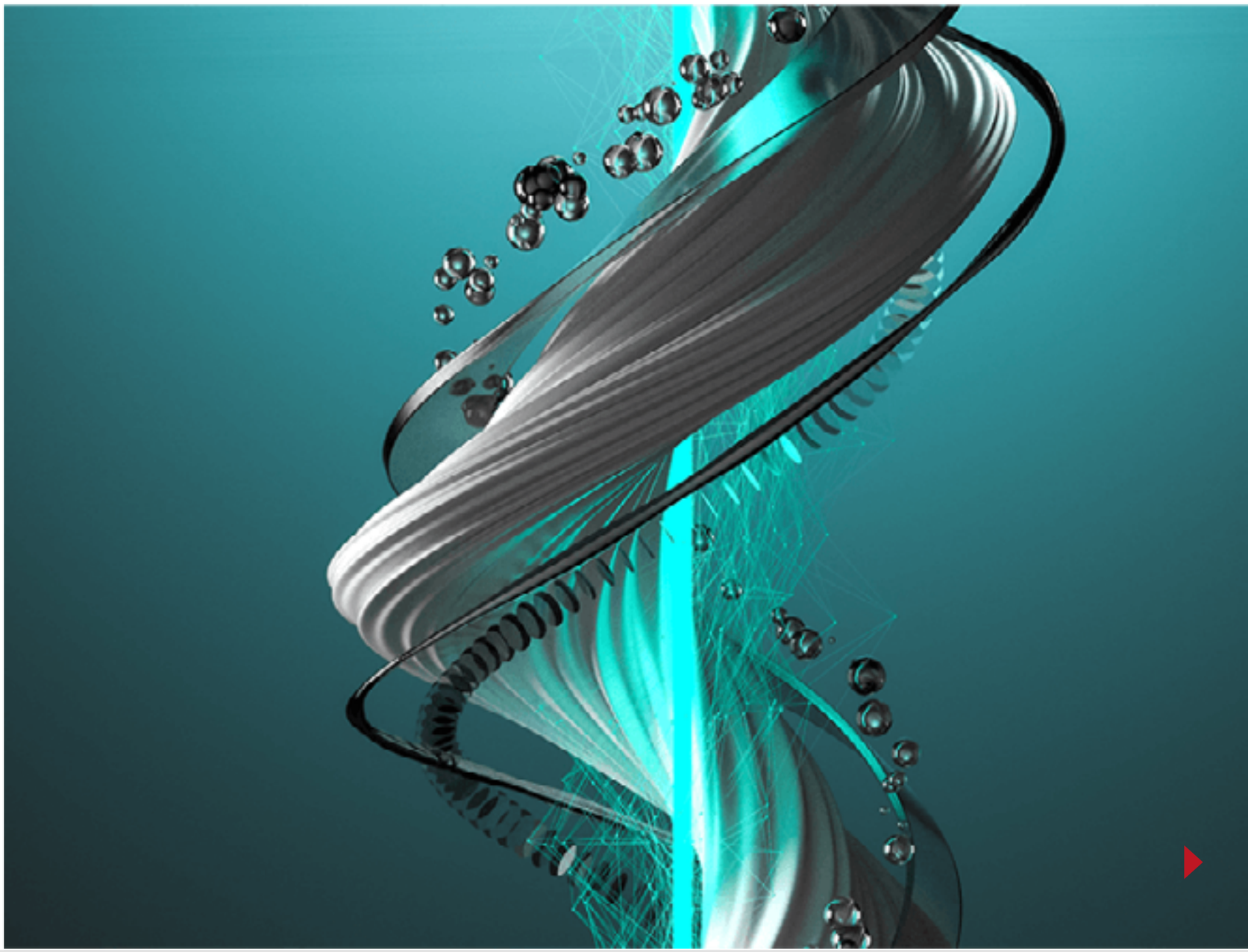
- Guide for delivering IoT Security
- Check Point IoT Protect Solution Brief
- IoT Security for Networks and Devices
- IoT Security for Enterprise, Industrial and Healthcare
- CloudGuard for Cloud Native Security

La propuesta de seguridad de ESET apuesta por ofrecer soluciones específicas para necesidades específicas

Una solución para cada necesidad

❖ **ESET PROTECT ADVANCED**, es una solución para un nivel de ciberseguridad empresarial más avanzado con administración basada en la nube. Proporciona protección a su red de equipos y servidores de archivos contra ransomware, amenazas avanzadas y amenazas zero-day. Asegure sus datos con el cifrado completo del disco y administre todo desde la consola en la nube ESET PROTECT. Está orientado a la protección de servidores, ordenadores de sobremesa, portátiles y dispositivos móviles.

❖ **ESET PROTECT COMPLETE** es una solución de protección completa para empresa que además mantiene seguras las aplicaciones de Microsoft 365 con administración basada en la nube. Proporciona protección para su red de equipos, servidores, correo electrónico no deseado, de las aplicaciones de la empresa en la nube, contra todo tipo de amenazas: ransomware, avanzadas, día cero y malware, también protege sus datos con el cifrado de disco completo y todo administrado desde la consola de administración en la nube ESET PROTECT. Está diseñado para la protección de aplicaciones, al-



macenamiento y comunicaciones de Microsoft 365, servidores de archivo, servidores de correo, ordenadores de sobremesa, portátiles y dispositivos móviles.

❖ **ESET PROTECT MAIL PLUS**, solución que protege las comunicaciones por correo electrónico con espacio seguro basado en la nube. Protege su empresa de los ataques de red y ofrece protección directamente a través del servidor antes de llegar a las cuentas de correo de los usuarios, filtra los mensajes de correo no deseado con casi el 100% de precisión además de brindar seguridad frente a las amenazas persistentes avanzadas y amenazas día cero. Todo administrado desde la consola en la nube ESET PROTECT. Orientado a la protección del servidor de correo electrónico, el vector de ataque más común.

❖ **ESET CLOUD OFFICE SECURITY**, una solución de protección avanzada para el correo, sharepoint y almacenamiento de Microsoft 365. Su combinación de filtrado spam, antimalware, antiphishing, escaneo y detección de páginas fraudulentas ayuda a proteger la comunicación, las aplicaciones y almacenamiento de la empresa en la nube además puede inspeccionar los objetos que están en cuarentena. Protege la comunicación de la empresa y el almacenamiento en la nube para las aplicaciones de Microsoft 365.

❖ **ESET PROTECT ENTERPRISE ON-PREM**, solución para grandes empresas que incorpora una potente capa de protección EDR: identificación de comportamientos anómalos, fugas de información, análisis de riesgos... Proporciona máxima protección para su red de equipos y servidores de archivo contra ransomware, amenazas persistentes avanzadas (APT), amenazas día cero y malware sin archivo. Protege sus datos con el cifrado de disco completo y además incrementa su seguridad con la protección EDR más avanzada por su detección y respuestas de amenazas en equipos. Todo gestionado fácilmente desde la consola de administración local ESET PROTECT. Protege servidores de archivo, ordenadores de sobremesa, portátiles y dispositivos móviles.

❖ **ESET PROTECT COMPLETE ON-PREM**, una solución de protección completa para empresa que, además, mantiene seguras las aplicaciones de Microsoft 365. Proporciona protección para su red de equipos, servidores, correo electrónico no deseado, contra todo tipo de amenazas: ransomware, avanzadas, día cero y malware, también protege sus datos con el cifrado de disco completo y todo administrado desde la consola local ESET PROTECT. Protege aplicaciones, almacenamiento y comunicaciones de Microsoft 365, servidores de archivo, servidores de correo, ordenadores de sobremesa, portátiles y dispositivos móviles. ■

La propuesta de seguridad de ESET apuesta por ofrecer soluciones específicas para necesidades específicas

MÁS INFORMACIÓN

- Tendencias en Ciberseguridad 2021
- Informe sectorial sobre los gobiernos 2021
- Protección de end point
- Dynamic Threat Defense

TREND MICRO™

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

Movilidad segura en Industria 4.0

La movilidad es uno de los elementos destacados en el avance de la Industria 4.0. Pero como ocurre en todos los segmentos del negocio, esta movilidad debe ser segura y eficiente.

Los entornos industriales también necesitan dispositivos para trabajar en movilidad, y, sobre todo, para hacerlo de forma segura. La propuesta de Samsung en este terreno para por los dispositivos, pero no se detiene ahí.

❖ **Galaxy Z Fold3.** Posee una pantalla Infinity Flex de 7,6 pulgadas, y cuenta con una mayor área visible para que los usuarios obtengan un fondo ininterrumpido para ver sus aplicaciones favoritas. Con la nueva tecnología de pantalla Eco, la pantalla es un 29% más brillante y consume menos energía. Gracias a la tasa de refresco adaptable Super Smooth de 120 Hz, se puede experimentar un deslizamiento por la pantalla aún más suave y una rápida interacción con el dispositivo, tanto en la pantalla principal como en la de la cubierta frontal.

Por primera vez en la serie Galaxy Z, Samsung incorpora la funcionalidad de S Pen. Ahora es más sencillo tomar notas durante una videollamada o revisar una lista de tareas mientras se leen correos electrónicos. Los usuarios de Z Fold3 pueden escoger entre dos opciones: S Pen Fold Edition y S Pen Pro. Ambos cuentan con una punta retráctil especialmente diseñada con un límite de fuerza para proteger la pantalla principal de Z Fold3 5G; con una latencia aún más baja.

El modo Flex de Z Fold3 5G permite hacer más cosas a la vez como, por ejemplo, unirse a una videollamada en la pantalla superior del dispositivo mientras se consultan las notas de la reunión en la inferior. Con la función Multi-Active Window es más fácil organizar una presentación y redactar un mensaje de texto mientras se consulta el calendario; todo desde

la pantalla grande del dispositivo. Además, en Z Fold3 5G, los usuarios pueden crear un acceso directo y volver a abrir las aplicaciones más tarde en la misma posición, gracias a App Pair. También pueden utilizar la nueva barra de tareas para cambiar rápidamente de aplicación sin tener que volver a la pantalla de inicio.

❖ **Galaxy Tab S7 FE.** Con un diseño minimalista y ligero, Galaxy Tab S7 FE luce un cuerpo metálico elegante de 6,3 mm y 608 g de peso, lo que lo convierte en un dispositivo fácil de llevar a cualquier parte. Además, cuenta con una potente batería de hasta 13 horas, y es compatible con carga súper rápida de 45W.

Galaxy Tab S7 FE está pensado para hacer más trabajo en menos tiempo. Incluye S Pen en la caja para hacer todo tipo de tareas más rápido, y, con Samsung Notes, se puede convertir las notas escritas a mano en texto. Con Multi Active-Window se pueden abrir hasta tres aplicaciones a la vez, y con Grupo de Apps, se puede guardar e iniciar rápidamente varias aplicaciones

Además, gracias a Samsung DeX y a una funda teclado, el usuario puede utilizar la tablet como un portátil, transformando la interfaz de usuario en una experiencia similar a la de un PC. Y con la opción de Segunda Pantalla, Galaxy Tab S7 FE se puede convertir en una pantalla adicional para el PC y así maximizar la productividad en un tiempo menor.

❖ **Samsung Knox Vault.** Desde su presentación en 2013, Samsung Knox ha evolucionado hasta convertirse en una plataforma de gestión de seguridad integral, que protege los dispositivos móviles de millones de usuarios y empresas en todo el mundo frente a las amenazas más sofisticadas. Samsung Knox Vault es la evolución natural de la plataforma de seguridad de Samsung, que proporciona un entorno aislado e integrado en el hardware, para mantener los datos protegidos. Knox Vault aísla la información más crítica del terminal, como claves y certificados digitales, para que no permanezcan vulnerables ante un acceso no autorizado. Este nuevo protocolo permite separar los datos confidenciales del sistema operativo, para evitar brechas de seguridad como el malware. Se incluye en todos los dispositivos de la serie Galaxy S21 y en los plegables Galaxy Z, con el fin de protegerlos ante ataques físicos y ciberataques.

❖ **Samsung DEX.** DeX convierte cualquier lugar en un puesto de trabajo al conectar un smartphone Galaxy compatible, un monitor y un teclado. Proporciona a los usuarios una experiencia de escritorio segura y productiva que permite editar documentos, ver presentaciones en pantalla completa y realizar tareas de ordenador, entre otras funciones, con solo conectar el smartphone a la base. Además, el nuevo dispositivo aprovecha la Pantalla Infinita del terminal como un panel táctil para controlar el cursor. ■

MÁS INFORMACIÓN

- El 5G abre un mundo de oportunidades de negocio
- ¿De qué está hecho un móvil todoterreno para resistir tanto?
- Firmas legales con S-Pen, el secreto de Samsung Galaxy Note
- Siete pasos para asegurar tu dispositivo móvil

Soluciones de seguridad para la empresa

Stormshield pone sobre la mesa diferentes soluciones tecnológicas para garantizar la seguridad de las empresas según las distintas necesidades que éstas tengan.

❖ **SNi20**, un firewall a medida para entornos industriales. Perfectamente adaptado a su entorno operativo, el firewall industrial SNi20 ofrece una integración de red única y completa (enrutamiento y NAT) y seguridad avanzada. Asimismo, proporciona una inspección profunda de paquetes (análisis basado en el contexto), permitiéndole proteger sus protocolos de comunicación industrial. El firewall garantiza la confiabilidad operativa de su infraestructura y una continuidad de negocio óptima en todo momento, incluso en caso de avería, gracias al sistema de alta disponibilidad y modo de seguridad de la red operativa. El SNi20 le asegura ciberserenidad industrial.

El cortafuegos industrial SNi20 ha sido diseñado para cumplir con los estándares de certificación más estrictos del mercado. Es por eso que las organizaciones con las necesidades de seguridad más críticas confían en Stormshield: organizaciones de defensa, organismos públicos y gubernamentales e infraestructuras críticas.

❖ **SNi40**, firewall para sistemas industriales. El cortafuegos industrial SNi40 está especial-

mente diseñado para proteger PLC (controladores lógicos programables) y ofrece una amplia gama de funciones: segmentación de red, control de acceso por filtrado de direcciones IP o MAC, análisis contextual de paquetes, control de mensajes operativos y cumplimiento de protocolos (IPS), comunicaciones seguras de mantenimiento remoto (VPN). Además, este equipo se puede integrar fácilmente en su entorno industrial, especialmente en sus armarios de control (sobre rieles DIN), gracias a un sencillo procedimiento de puesta en marcha.

El SNi40 garantiza la continuidad de la actividad gracias, en particular, a su sistema de alta disponibilidad y al modo de seguridad de la red operativa, que mantiene sus sistemas de producción funcionando sin interrupción incluso en caso de fallo.

El SNi40 es un cortafuegos industrial certificado al más alto nivel europeo. Ha recibido la certificación y calificación CSPN a nivel elemental, emitida por ANSSI. Por ello, si elige esta solución de Stormshield Network Security, puede estar seguro de que su infraestructura industrial estará cubierta por la mejor protección posible.

❖ **Stormshield Endpoint Solution (SES)**. A menudo considerados como los eslabones más débiles en la seguridad de TI, los terminales incluyen todos los dispositivos que se conectan a la red central de una empresa: ordenadores de escritorio y portátiles, tabletas, teléfonos inteligentes, impresoras y todos los demás dispositivos (inteligentes o no) que se nos requiera conectar a la red interna. Sin embargo, todos estos terminales podrían ser secuestrados y utilizados por los ciberdelincuentes como un punto de entrada para penetrar en su sistema informático con el fin de instalar malware u obtener acceso a sus datos. Desde ellos, pueden saltar a la red OT provocando graves daños.

SES tiene características que lo hacen especialmente adecuado para el entorno industrial: protege sistemas operativos obsoletos que siguen operando en redes OT como puede ser Windows XP. Por otra parte, SES no está basado en firmas ni necesita conexiones al exterior para su correcto funcionamiento. Por último, hay que destacar sus capacidades de creación de listas blancas, que no son manejables en el mundo IT pero sí en el OT, donde las aplicaciones necesarias para los puestos son mínimas y estables.

SES también controla qué dispositivos y a qué redes puede conectarse cada puesto de trabajo, bloqueando, por ejemplo, el uso no deseado de dispositivos USB. ■

MÁS INFORMACIÓN

- Ciberseguridad en entornos sensibles: inmersión en la industria del agua
- From 2015 to tomorrow: cyberintrusions in electrical grids
- Sistemas DPI y seguridad de red : la tecnología IPS Stateful DPI en entornos de TO

A menudo considerados como los eslabones más débiles en la seguridad de TI, los terminales incluyen todos los dispositivos que se conectan a la red central de una empresa

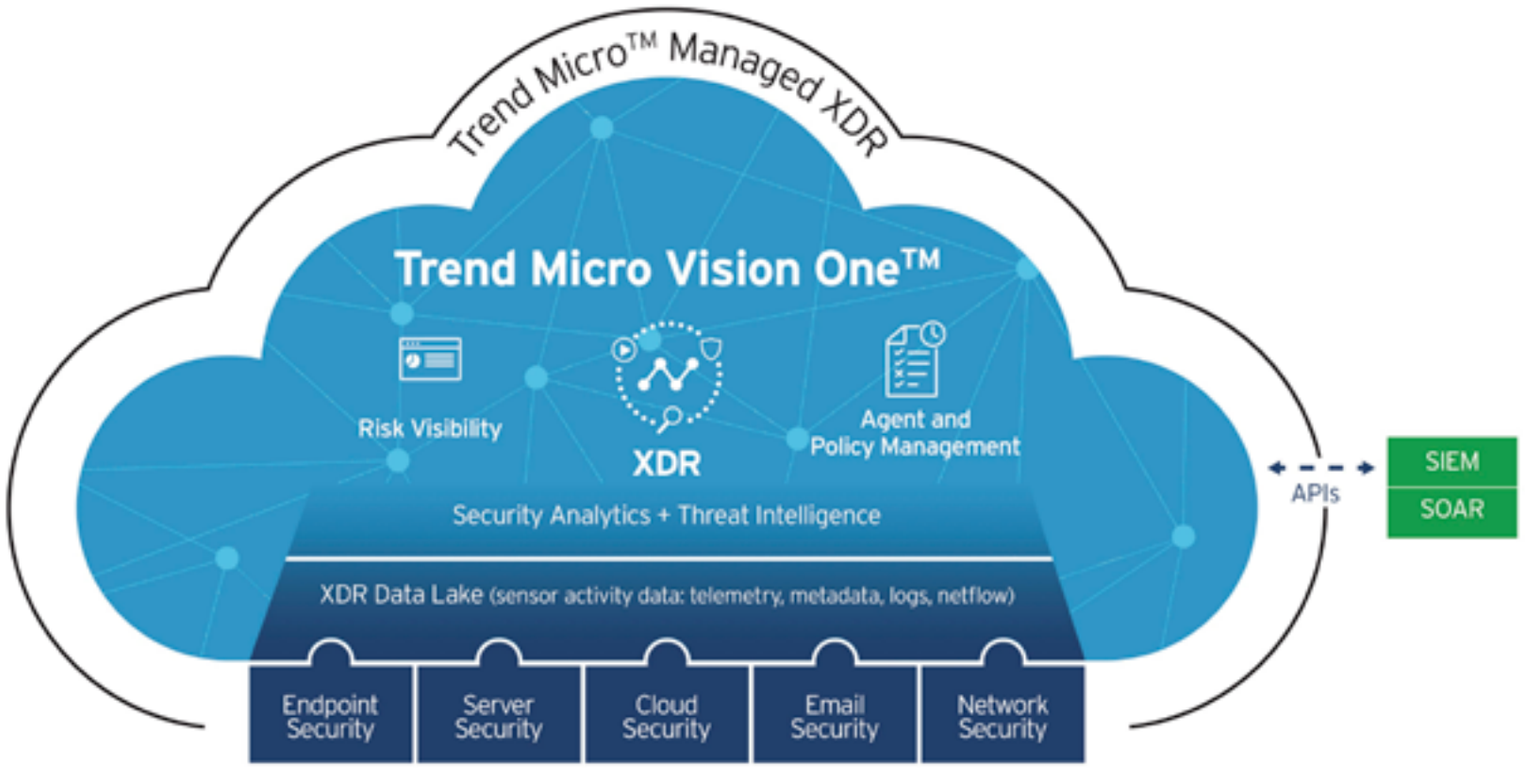
Una propuesta más allá de la seguridad tradicional para afrontar desafíos complejos

En el ámbito industrial, al igual que en otros, Trend Micro escucha las necesidades tanto de principales fabricantes como de operadores de infraestructuras críticas y luego recopila la mejor propiedad intelectual existente en las empresas asociadas.

El resultado es una respuesta personalizada que va más allá de las herramientas de seguridad tradicionales para mitigar los desafíos complejos. Y eso se materializa en una propuesta como la de Trend Micro TXOne.

❖ **Txone Networks Portable Security v3.** Se trata de una herramienta de escaneo y limpieza de malware para sistemas con conexión aislada y ordenadores autónomos. Portable Security facilita a los propietarios y operadores de ICS el escaneo de malware y la recopilación de información de activos en ordenadores autónomos y en sistemas aislados. A diferencia del software antivirus tradicional, Portable Security escanea y limpia el malware sin necesidad de instalar software de escaneo, mostrando el estado con una pantalla LED fácil de entender. Durante el escaneo, Portable Security 3 también recopila información sobre los activos, lo que ayuda a mejorar la visibilidad de la OT y a eliminar el shadow OT.

❖ **TXOne StellarEnforce.** Es un software de bloqueo de sistemas para dispositivos de misión crítica. Los sistemas de control industrial (ICS), los activos industriales de IoT y los dispositivos integrados esenciales para las operaciones diarias se enfrentan a un riesgo cada vez mayor. Los activos críticos que dependen de sistemas operativos antiguos son especialmente vulnerables, ya que es probable que sean difíciles o imposibles de parchear, funcionando con vulnerabilidades que los atacantes pueden explotar fácilmente. TXOne StellarEnforce bloquea los activos sensibles, limita el acceso y preserva los recursos del sistema con su sencilla y fiable tecnología de listas de confianza. Desplegada, esta solución solo permite la



ejecución de aplicaciones aprobadas y necesarias para las operaciones diarias, impidiendo la propagación y ejecución de malware sin depender de los archivos de patrones u otros recursos.

❖ **TXOne StellarProtect.** Hablamos de seguridad de endpoint profesional y de última generación para los ICS. La protección de los endpoints de ICS debe tener en cuenta diferentes prioridades, pues el antivirus tradicional ya no es suficiente. Así, las soluciones elegidas deben garantizar que los procesos de trabajo diarios nunca se vean comprometidos, que los cálculos nunca se ralenticen y que las decisiones de producción nunca se retrasen. TXOne StellarProtect es la primera solución de este tipo: protección de endpoints todoterreno, una solución defensiva diseñada a medida para la tecnología operativa. Su escaneo avanzado de amenazas hace frente a los ataques conocidos mientras que su motor de machine learning de última generación bloquea las amenazas desconocidas, sin necesidad de acceso a Internet. El filtrado ICS de StellarProtect, basado en un inventario de aplicaciones y certificados, elimina la sobrecarga innecesaria para permitir el funcionamiento más ligero posible.

❖ **TXOne Networks EdgeFire.** Se trata de detección eficiente en línea que respalda las operaciones continuas de los lugares de trabajo. EdgeFire, es un firewall de nueva generación que permite la segmentación y segregación de la red para dividirla en diferentes zonas de control, incluso hasta el nivel de célula.

❖ **TXOne Networks EdgeIPS.** IPS industrial de próxima generación que protege los activos de misión crítica. EdgeIPS protege de forma transparente activos individuales y pequeñas zonas de producción, al tiempo que proporciona una visibilidad fiable de OT, filtrado de protocolos de OT y funcionalidad en línea o fuera de línea, todo ello diseñado específicamente para adaptarse a su red sin alterar sus configuraciones preexistentes.

❖ **TXOne Networks IPSPro.** Matriz de IPS industrial inteligente basado en propósito para operaciones a gran escala. El dispositivo de seguridad industrial transparente y multisegmento protege las máquinas críticas y apoya el funcionamiento continuo de la línea de producción. La segmentación de red basada en la intención es la base de una seguridad de red ICS cómoda, conveniente y fiable, eliminando las superficies de ciberataque y reduciendo el impacto de cualquier incidente de seguridad.

❖ **Trend Micro Deep Security Virtual Patching.** Módulo Virtual Patching de la plataforma Deep Security ofrece protección frente a las vulnerabilidades de sistemas críticos hasta que haya disponible un parche que se pueda implementar, o bien como alternativa al parche en el caso de que este nunca se publique. El parcheo virtual funciona implementando capas de políticas y reglas de seguridad que impiden e interceptan que un exploit tome las rutas de red hacia y desde una vulnerabilidad. Una buena solución de parcheo virtual debe ser multicapa. Esto incluye capacidades que inspeccionan y bloquean la actividad maliciosa del tráfico crítico para el negocio; detectan y previenen las intrusiones; frustran los ataques a las aplicaciones orientadas a la web; y se despliegan de forma adaptable en entornos físicos, virtuales o en la nube. ■

MÁS INFORMACIÓN

- Trend Micro Industrial Network Security
- Lost in Translation – When industrial protocol translation goes wrong
- Secure manufacturing on Cloud, Edge and 5G
- Seguridad de endpoint para los ICS con Trend Micro StellarProtec
- TXone Networks
- Industrial Endpoint Security

STORMSHIELD

La opción europea en ciberseguridad

El partner de confianza
para
securizar sus
infraestructuras operacionales y sensibles

www.stormshield.com

Una IA en mi empresa:

dónde está y dónde debería

La inteligencia artificial es un campo en auge de descubrimientos científicos e implementaciones prácticas. Después de haber sido un área de estudio académica, la IA del siglo XXI permite un espectro de tecnologías convencionales que están teniendo un impacto sustancial en la vida cotidiana. En muchos casos, la IA está en nuestras tareas diarias y en nuestra vida profesional. En el futuro, no solo remodelará los negocios, la administración pública, la atención médica, las finanzas o la educación, sino que también puede contribuir a resolver grandes desafíos de civilización como el cambio climático, el hambre o la desigualdad. De lo que no hay duda es de que esa fase en la que la IA transformará masivamente la sociedad, la economía y la política ya ha comenzado.

El desarrollo de la inteligencia artificial se remonta a los años cuarenta y cincuenta. Desde sus inicios, la tasa de progreso en la inteligencia artificial ha sido irregular e impredecible. Su historia es bastante larga e incluye tanto períodos de abundante financiamiento e interés vital (muchas veces denominados como los "veranos de IA") y períodos de decepción y falta general de inversiones (conocidos como "inviernos de IA"). Muchos de los inventos en IA que el público en general percibe como completamente nuevos también se remontan a hace algunas décadas. Un buen ejemplo aquí son las redes neuronales artificiales que se han desarrollado conceptualmente primero en los años 40 del siglo XX, más tarde en los 80 y actualmente resurgieron y se están convirtiendo en el paradigma más importante dentro de la inteligencia artificial per se.

Hoy en día, los sistemas basados en inteligencia artificial se pueden encontrar en una variedad de aplicaciones, desde teléfonos inteligentes hasta sistemas CRM y bolsas de valores. La amplia gama de aplicaciones comerciales de IA abarca, entre otros, la evaluación de riesgos financieros, la optimización de precios, la focalización de clientes y la personalización del servicio, el diagnóstico médico, los sistemas de recomendación y los asistentes virtuales. En lo que respecta a la disciplina más aplicada dentro de la IA, el aprendizaje automático, podemos distinguir 3 pilares: aprendizaje supervisado, aprendizaje no supervisado y aprendizaje reforzado. El aprendizaje supervisado consiste en métodos como la regresión, que se utilizan con frecuencia en la predicción del crecimiento de la población o en la estimación de la esperanza de vida y clasificación, utilizados, entre otros, en la detección de fraudes de identidad. El aprendizaje no supervisado consiste en la reducción de la dimensionalidad que permite la visuali-

EL IMPACTO DE LA INTELIGENCIA ARTIFICIAL Y LA ANALÍTICA EN LAS ORGANIZACIONES, A DEBATE

¿Te avisamos del próximo IT User?

zación de big data y la agrupación en clústeres, que las empresas utilizan con frecuencia en la segmentación de clientes. El aprendizaje por refuerzo se utiliza en la navegación de robots, la adquisición de habilidades de robots y la IA de juegos (juegos de IA, incluidos ajedrez, Go o videojuegos).

DE QUÉ HABLAMOS CUANDO DECIMOS IA

Sin embargo, una de las primeras cosas que debemos acotar es de qué hablamos cuando lo hacemos de Inteligencia Artificial, un término muy difícil de definir. Con frecuencia, la gente lo usa para referirse a cosas que son difíciles de hacer para los ordenadores (como comprender el lenguaje natural) en contraposición a cosas que sabemos que manejan bastante bien (como contabilidad).

Así pues, y estableciendo primero una definición muy simple, podemos decir que la IA son máquinas que actúan de formas que parecen inteligentes. Sin embargo, esta definición es, a todas luces, insuficiente. Por lo tanto, es más adecuado decir que la inteligencia artificial es inteligencia demostrada por máquinas, en contraste con la inteligencia natural mostrada por humanos y animales. También se podría afirmar que la inteligencia artificial es un término general que abarca la visión por ordenador (máquina), el procesamiento del lenguaje natural, los asistentes virtuales y bots, la automatización de procesos robóticos, el aprendizaje automático (incluidas las técnicas más avanzadas como el aprendizaje profundo) y los procesos cognitivos en las organizaciones. Además, la inteligencia artificial es una rama de la ciencia y, como tal, puede definirse como un conjunto de tecnologías computacionales que se inspiran en las formas en que las personas usan sus sistemas nerviosos y cuerpos para sentir, aprender, razonar y actuar.

Así pues, la pregunta es si todo lo que decimos que es IA es, en realidad, IA o si hay inteligencia artificial en cosas, aunque no seamos consciente de ellos.

En este sentido. Nacho Fernández, Business Development Manager de Arsys, explica que dado que la IA es la ciencia de hacer máquinas inteligentes, "la idea subyacente es la creación de programas de cómputo capaces de imitar las funciones cognitivas humanas apoyándose en algoritmos. En ocasiones se le atribuyen muchos «súper poderes» que, en realidad, están lejos de hacerse realidad. También hay muchos procesos "que se venden como IA" pero que en realidad responden a la combinación de sistemas matemáticos y estadísticos con una capacidad de cómputo que antes no teníamos, pero

> "Todo el mundo debe estar concienciado de la importancia de los datos en la compañía. Y para ello hace falta contar con personal especializado y una cultura del dato que aún no está suficientemente generalizada"
>
> NACHO FERNÁNDEZ, BUSINESS DEVELOPMENT MANAGER DE ARSYS

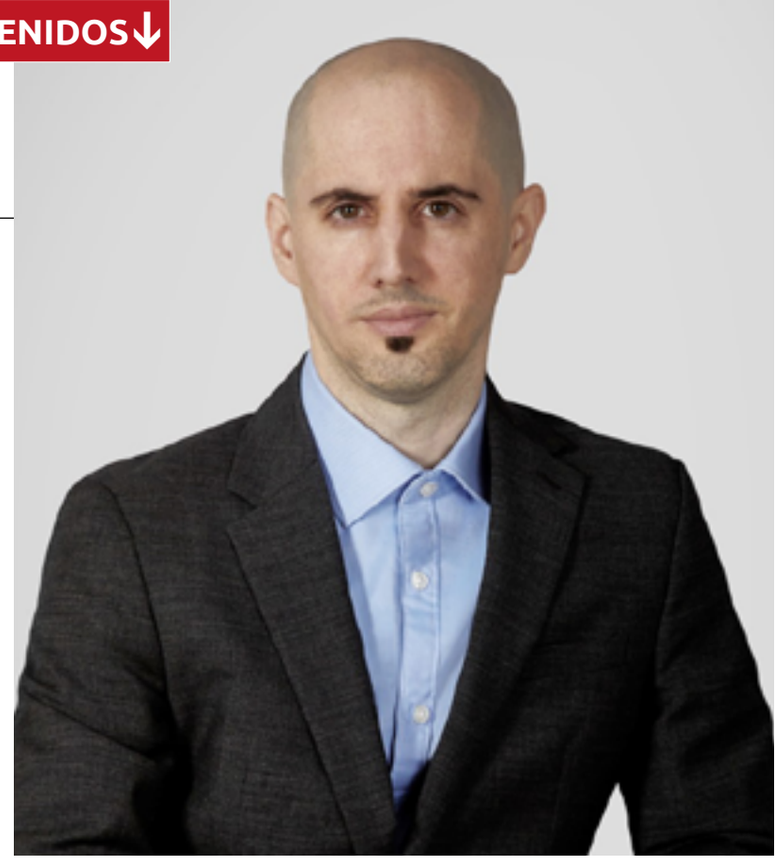
donde no existe el ingrediente de aprendizaje y evolución que sí serían propio de la IA".

Para David Mosen, Chief Data Scientist de Crayon Group, Todo depende del contexto. "La IA hoy en día son modelos matemáticos complejos; la cuestión es cómo de complejos tienen que ser para considerarse IA y no un modelo estadístico o una fórmula matemática". Para entenderlo un poco mejor, pone un ejemplo. "Un científico de datos diría que un modelo de regresión lineal no es IA, sin embargo vemos cómo en el mundo de los negocios se están presentando ciertas soluciones que se denominan IA y responden a modelos simples", explica. En todo caso, "ya sea desde el punto de vista técnico o de negocio la intención es la misma: explorar un problema desde su nivel más básico viendo qué nivel de complejidad IA es necesaria abordar para su resolución".

Javier González Alonso, Senior Solutions Architect de Dell Technologies, asegura que aunque todo lo que llamamos IA puedan no serlo en realidad, no tiene "ninguna duda de que cada vez más tareas cotidianas serán resueltas utilizando IA". "El presente de la IA es impresionante y me atrevería a decir que en un corto plazo la adopción de la IA se va a democratizar porque la tecnología ya permite poder llevar la IA al Edge, con lo que los casos de uso se van a multiplicar cada año. Muchos sectores empresariales ya están inmersos en su utilización y el resto de ellos están comenzando a explorar sus posibilidades, ahora mismo la imaginación es el límite".

Por su parte, Alberto Pinedo, National Technology Officer de Microsoft en España, asegura que explicar el concepto de Inteligencia Artificial con una sola definición "no es sencillo. Con el incremento de potencia de los ordenadores, de la cantidad de datos procesables y las técnicas de análisis, entrenamiento y procesamiento, ha evolucionado mucho". Además, avanza que el campo de la IA "tiene un gran recorrido por delante y sus aplicaciones, así como su diversidad en función del grado de complejidad de sus algoritmos son prácticamente ilimitadas. Para ayudar a los altos ejecutivos con perfiles no técnicos a introducirse en el mundo de la Inteligencia Artificial y tener una visión de cómo puede ayudar a sus organizaciones, en Microsoft hemos creado la AI Business School, un programa formativo gratuito que aporta gran valor para mirar al futuro".

Mientras, Manel Picallò, Consulting Systems Engineer en NetApp España, considera que la IA pasa "con frecuencia desapercibida" en la mayoría de los productos donde se aplica. Algo que se debe, en su opinión, a que es "una herramienta previa más para la prestación de un servicio posterior o en la elaboración de un producto, pero incluso en aquellos donde existe la presencia propia de la IA durante la prestación del servicio o en el producto final, muchas veces el usuario no es consciente realmente de ello, nos acostumbramos rápido a tener mejores productos a nuestro servicio y no nos paramos a analizar la complejidad de algunas de las mejoras que se nos ofrecen".



"Su peso va a ser tan determinante que los CEO de grandes empresas provendrán del ámbito de la ciencia de datos y la IA. Las empresas que ahora cuentan con una buena estrategia de datos estarán sacando ya fruto de soluciones de IA asentadas en plataformas de datos robustas"

DAVID MOSEN, CHIEF DATA SCIENTIST DE CRAYON GROUP

¿Te avisamos del próximo IT User?

QUÉ DEBEN TENER PARA SER IA

Visto, pues, que definir y acotar qué es Inteligencia Artificial es algo complejo incluso de definir, hemos preguntado a los expertos cuáles son aquellas características básicas que debe tener para poder ser considerado como inteligencia de máquinas.

A este respecto, José Luis Flórez, director de Plaiground, la unidad de negocio especializada en inteligencia artificial de Minsait (Indra), explica que "debe tener la capacidad de imitar capacidades cognitivas humanas: percibir el entorno, identificar patrones y relaciones causa-efecto, tomar decisiones y dar lugar a un proceso de aprendizaje al evaluar su impacto. Si no se relaciona con el entorno y no aprende, no puede ser entendido como Inteligencia Artificial".

Una definición en la que coincide Alberto Calvo, Territory Manager de Omega Peripherals, para quien la IA "básicamente debe intentar imitar la parte cognitiva humana, y desde ahí crecer, toda vez que debe tratar de evitar tareas totalmente repetitivas sin valor".

Violeta Gallego, Líder de la práctica de Analytics en SAS Consulting España, detalla que "si nos atenemos a la definición, la inteligencia artificial es la ciencia de entrenar máquinas para desarrollar tareas humanas. Por tanto, para poder desarrollar completamente un modelo de IA necesitaremos definir un volumen adecuado de datos y diversidad en estos para que nuestro modelo puede aprender correctamente y actualizarse". Sin embargo, y aunque reconoce que no estaría dentro de la definición, Gallego cree que un punto importante para desarrollar IA también es "la disponibilidad de un servidor y un software con una potencia suficiente para realizar el análisis de toda la información de la manera más optimizada posible. En mi opinión, quienes cumplan esto pueden ser catalogados como IA". David Sanz, Solution Consulting Senior Manager para Iberia e Israel de ServiceNow, considera que para poder sr llamado IA "deben ser soluciones tecnológicas lo suficientemente flexibles para adaptarse a cada situación en función de los datos que reciban, a partir de los que "aprenden" a funcionar mejor (esto es, a dar más valor en la situación concreta en la que operan)".

Como concluye Iván Gento, Marketing Executive de Synology para España, para que un programa sea considerado IA "es necesario que el programa sea capaz de gestionar una gran cantidad de datos ofreciendo un procesamiento relativamente rápido y algoritmos inteligentes, lo que permite que el software aprenda automáticamente de patrones o características en los datos".

"El presente de la IA es impresionante y me atrevería a decir que en un corto plazo su adopción se va a democratizar porque la tecnología ya permite poder llevarla al Edge, con lo que los casos de uso se van a multiplicar cada año"

JAVIER GONZÁLEZ ALONSO,
SENIOR SOLUTIONS ARCHITECT DE DELL TECHNOLOGIES

LO QUE APORTA Y MEJORA LA IA

¿Cómo se traslada toda esta capacidad y potencia en resultados para las empresas que implementan la IA en sus herramientas tecnológicas?

Gento detalla que la IA puede producir "grandes mejoras en diversas áreas de una empresa y en el día a día en organizaciones, aunque dependerá sobre que aplicaciones la IA se aplica para conocer sus ventajas especificas dentro de una organización". Así, "mejora la eficiencia y productividad, ya que esta tecnología permite realizar un gran volumen de tareas repetitivas eficientemente lo que permitirá que los trabajadores tengan una dedicación en tareas de mayor rango. Al poder gestionar y analizar un gran volumen de datos, las empresas tienen la oportunidad de encontrar nuevas oportunidades de negocio y adaptarse fácilmente a situaciones inesperadas", explica, para añadir que otra de las áreas que mejora "dada la capacidad basta del procesamiento de datos es el sistema de monitoreo y alertas como puede ser, predecir errores antes de que ocurra en un datacenter, o detectar análisis de entrada y salida de u edificio con cámaras de vigilancia, incluso en detectar y proteger de ataques ransomware antes de que ocurran. Esto puede prevenir errores hu-

"Debe tener la capacidad de imitar capacidades cognitivas humanas: percibir el entorno, identificar patrones y relaciones causa-efecto, tomar decisiones y dar lugar a un proceso de aprendizaje al evaluar su impacto. Si no se relaciona con el entorno y no aprende, no puede ser entendido como Inteligencia Artificial"

JOSÉ LUIS FLÓREZ, DIRECTOR DE PLAIGROUND, LA UNIDAD DE NEGOCIO ESPECIALIZADA EN INTELIGENCIA ARTIFICIAL DE MINSAIT (INDRA)

PASADO, PRESENTE Y FUTURO DE LA IA

manos o grandes costes, reparaciones o ataques malintencionados".

Para David Sanz, son "innumerables" las mejoras que aporta la IA. "Cuando eres capaz como empresa de entender el flujo de tus procesos, puedes empezar a automatizar acciones, con lo cual reduces tiempos y costes mientras aumentas la productividad. Además, eso redunda en una mayor satisfacción tanto de empleados (con lo que los ratios de atracción y retención de talento mejoran) como de clientes, y esto está directamente relacionado con los ingresos y la posición de mercado de una compañía.

Si además aplicas la IA a asistentes virtuales, redoblas los beneficios al aumentar los ratios de autorresolución de problemas. Y si lo haces en las operaciones de TI, puedes prevenir (y por lo tanto reducir) paradas de sistema y como consecuencia mejorar el rendimiento de tu negocio", pone como algunos de los ejemplos. "La IA se está convirtiendo en una ventaja competitiva y vemos que no solo es importante ser rápidos y ágiles encontrando casos de uso: la ventaja de los early adopters es muchas veces definitiva. Es decir, cuando antes se empiece a buscar áreas donde experimentar con la IA, mejor", sentencia.

Mientras, Violeta Gallego expone que el uso de la IA produce ventajas competitivas tanto "optimizando los procesos y las decisiones que se toman en las organizaciones, como a nivel cliente mejorando la satisfacción y conexión con la empresa". Esta experta cree que en función del tipo de sector en el que estemos esto se traducirá en distintos usos. "Por ejemplo, en el industrial se está utilizando en la mejora de toda la cadena de abastecimiento, con un foco importante en la predicción de la demanda y en el mantenimiento predictivo de las fábricas analizando los datos de IoT. Si nos centramos en el sector de la salud, la IA tiene un gran potencial en el análisis de imágenes, con aplicación en la mejora de la detección de tumores con tomografías computarizadas gracias a las capacidades de extracción de información que tienen las redes convolucionales. También, por ejemplo, en la mejora en el ajuste de las dosis farmacológicas a los enfermos a través de modelos que aprenden de otros pacientes con las mismas características", explica. "De manera

"Las condiciones necesarias para que una empresa sea capaz de sacar todo el potencial de la IA son: tener una estrategia bien definida y consistente con los principios de la compañía o sector de actividad; cambiar la cultura empresarial y liderazgo para asumir esta apuesta por la innovación; ser capaz de buscar socios innovadores como Microsoft y sus partners que permitan eliminar las barreras tecnológicas; y, ganar confianza para la adopción de esta tecnología"

ALBERTO PINEDO, NATIONAL TECHNOLOGY OFFICER DE MICROSOFT EN ESPAÑA

transversal a muchos sectores se está implantando la IA para mejorar la precisión de modelos que anteriormente ya se realizaban. Estos casos irían desde la detección del fraude, a la propensión a la compra que permite que las campañas de marketing que recibimos sean las que más ajustadas a nuestras preferencias", añade para determinar que una de las grandes ventajas de la IA es que se puede aplicar en sectores diferentes y dentro de muy variados departamentos. "Anteriormente se pensaba que la IA tenía sentido únicamente en departamentos analíticos de cliente, pero actualmente se utiliza incluso en departamentos legales para ayudar con el análisis de texto en el análisis de los contratos".

Por su parte, el Territory Manager de Omega Peripherals, lo resume en que "en vez de saber de qué te has muerto que es lo que aportaría el Business Intelligence, la IA te van dando diagnósticos cada vez más precisos basados en información y algoritmos que mejoran incluso el pensamiento humano".

STATE OF THE ART

Aunque nadie duda de las capacidades que tiene la IA, la gran pregunta es si las organizaciones que la están usando ya están siendo capaces de de sacar todo el partido que esta tecnología ofrece o si, como en muchos de los programas y aplicaciones que usamos en nuestro día a día, tienen tantas funciones que muchas de ellas no son totalmente desconocidas.

En este sentido, Manel Picalló cree que, sobre todo cuando se quiere una solución de AI propia para la empresa, lo más complejo es "establecer las bases previas de recursos para ello, desde las necesidades de computación hasta lo más importante: la cantidad, calidad y formato de los datos que se necesitan para tener una red neuronal lo suficientemente entrenada como para obtener resultados que sean realmente útiles". Teniendo en cuenta lo anterior, este responsable cree que lo primero que hay que hacer es "analizar las necesidades empresariales y elegir el mejor caso de uso para que cada organización lo aborde. Muchos equipos empiezan por un caso de uso frecuente en su sector, particularmente si es su primer proyecto de IA", añade.

"Puede ser útil considerar una estrategia de "aterrizaje y expansión", donde se escoge un caso de uso que tenga una buena oportunidad de producir resultados en un período relativamente corto y luego expandir ese caso de uso a otras áreas del negocio. Por ejemplo, Liberty Mutual Insurance comenzó con un asistente digital (o bot de chat) para sus empleados internos, un caso de uso relativamente seguro y sin exposición directa al cliente. Los buenos resultados permitieron a Liberty Mutual pilotar un enfoque tecnológico similar en su centro de atención al cliente y también comercializar el software a través de su filial Workgrid Software", determina.

"Es un proceso que implica innovación y, por tanto, ensayo y error, también disrupción, hay pione-

"El primer paso de cualquier proyecto de IA es analizar las necesidades empresariales y elegir el mejor caso de uso para que cada organización lo aborde. Muchos equipos empiezan por un caso de uso frecuente en su sector, particularmente si es su primer proyecto de IA"

MANEL PICALLÒ, CONSULTING SYSTEMS ENGINEER EN NETAPP ESPAÑA

ros, seguidores y otros que van más retrasados, pero corresponde al patrón de cualquier cambio profundo. El potencial que aporta la IA está lejos de los límites de nuestra propia imaginación. Esto solo está comenzando", reflexiona en este sentido José Luis Flórez.

Mientras, el National Technology Officer de Microsoft en España cree que es importante tener en cuenta que las condiciones necesarias para que una empresa sea capaz de sacar todo el potencial de la IA. En su opinión, estas condiciones pasan por "tener una estrategia bien definida y consistente con los principios de la compañía o sector de actividad; cambiar la cultura empresarial y liderazgo para asumir esta apuesta por la innovación; ser capaz de buscar socios innovadores como Microsoft y sus partners que permitan eliminar las barreras tecnológicas; y, ganar confianza para la adopción de esta tecnología". Es más, según diversos estudios de Microsoft, "la implantación de tecnologías de Inteligencia Artificial (IA) junto a una apuesta por la capacitación digital del capital humano son claves para hacer que las empresas públicas y privadas sean más competitivas. Los profesionales encuestados ven un vínculo claro entre el nivel de madurez en el uso de la Inteligencia Artificial y el valor que estas tecnologías aportan a su estrategia de negocio".

Por lo tanto, Pinedo asegura que "con la implicación y conocimiento necesarios, las empresas así son capaces de sacar todo el potencial de la IA. Al fin y al cabo, sabemos que la demanda de profesionales especializados en IA seguirá creciendo. De hecho, se prevé que para 2025, el 61% de los trabajadores deberá tener conocimientos de estas tecnologías. En este sentido, ya en España, el 54% de las organizaciones líderes en la adopción de IA está reclutando activamente profesionales con conocimientos en Inteligencia Artificial y el 36% de los directivos cree que las personas con conocimientos en IA pueden optar a salarios más altos y acceder con facilidad a mejores puestos".

Sin embargo, Nacho Fernández cree que no siempre las empresas sacan partido de todas estas posibilidades que brinda la IA. "La energía fundamental de la que se alimenta la IA son los datos. Para poner en marcha sistemas de IA hacen falta grandes cantidades de datos y, tan importante como lo anterior, que sean datos de calidad. Esto no es fácil si tenemos en cuenta que los datos, por su propia naturaleza, son heterogéneos, proceden de fuentes muy diversas, tienen formatos distintos, llegan de forma irregular y no siempre está clara su autenticidad. Todo el mundo debe estar concienciado de la importancia de los datos en la compañía. Y para ello hace falta contar con personal especializado y una cultura del dato que aún no está suficientemente generalizada. Que una empresa se base en los datos significa que ha emprendido la transformación digital y considera a esos datos como una fuente impagable de información sobre su actividad, sus clientes y

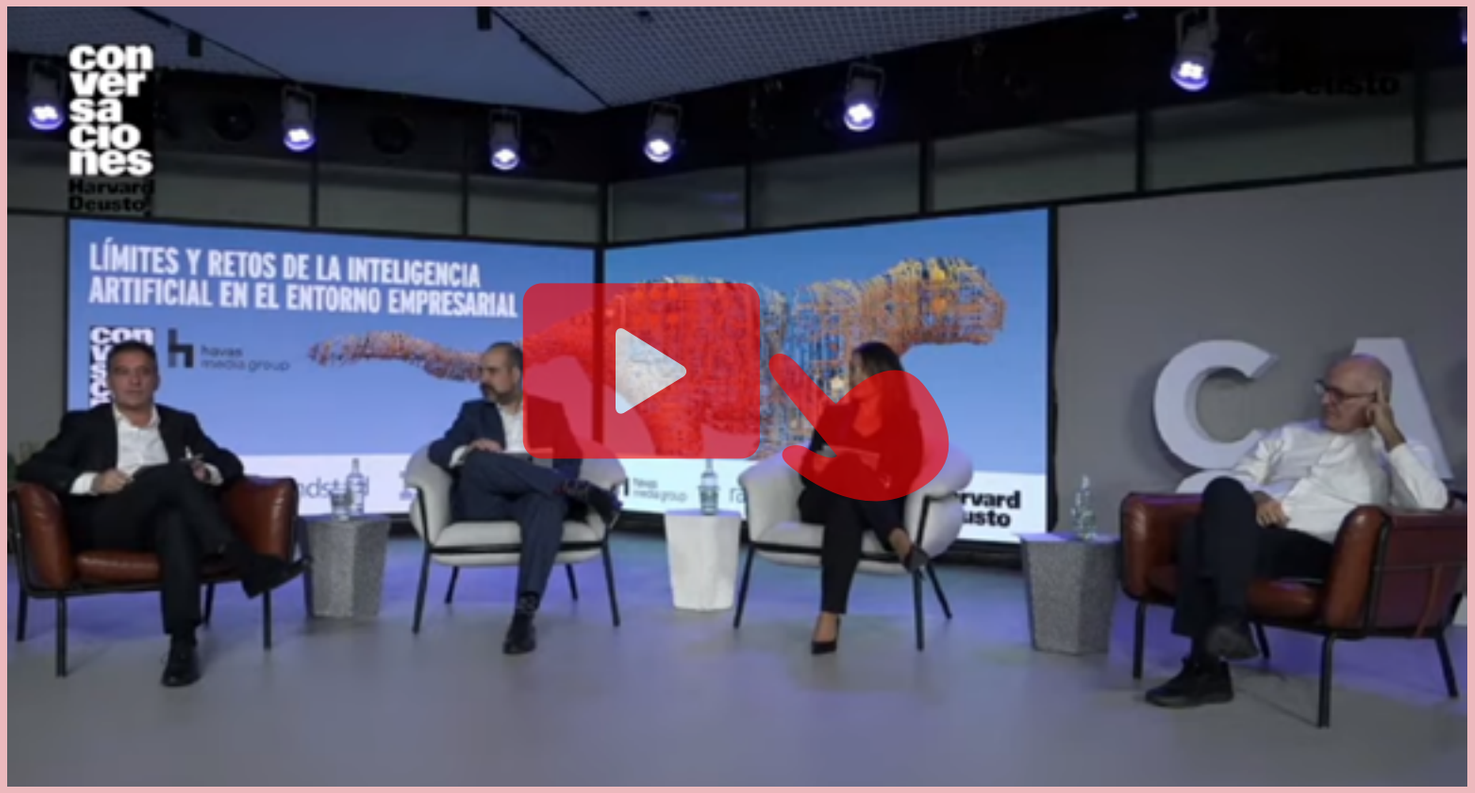
sus relaciones. Luego se necesita hardware y software especializados y profesionales expertos en esta materia", razona.

En este punto, David Mosen expone que "es fácil ver las mejoras en distintos sectores y procesos de negocio", como el despliegue de chatbots en las empresas que ofrecen servicios de Call Center, que "permite reducir costes porque limita la intervención humana que siempre incurre en gastos". Algo (reducir costes) en lo que la IA es "una gran aliada en cualquier sector y negocio facilitando mantenimientos predictivos".

Otra de las áreas en las que se está usando ya la IA es a la hora de ofrecer recomendaciones de upselling en eCommerce. "Respecto a las mejoras en los procesos, su uso en el sector de la fabricación y la energía es crítico para optimizar la gestión y el procesamiento de materiales, consiguiendo menos desperdicios y una mayor calidad, que se traducen también en ahorro de costes y aumento de beneficios", incide Mosen, para quien "la mejora en la toma de decisiones se constata fácilmente, por ejemplo, al realizar proyecciones de demanda apoyadas en IA. La siempre valiosa opinión de los

"En vez de saber de qué te has muerto que es lo que aportaría el Business Intelligence, la IA te van dando diagnósticos cada vez más precisos basados en información y algoritmos que mejoran incluso el pensamiento humano"

ALBERTO CALVO, TERRITORY MANAGER DE OMEGA PERIPHERALS



LÍMITES Y RETOS DE LA INTELIGENCIA ARTIFICIAL EN EL ENTORNO EMPRESARIAL

¿Te avisamos del próximo IT User?

expertos se refuerza con IA que está basada al 100% en datos reales".

Javier González Alonso también añade que son muchas las empresas que ya están utilizando con éxito la IA: "sectores como Telco y Banca suelen ser los líderes en cuanto a adopción de nuevas tecnologías, pero es destacable que la Industria ya está utilizando la inteligencia artificial en bastantes ámbitos como el mantenimiento predictivo y el I+D", detalla. Así, el Centro Tecnológico del Calzado de La Rioja es "un ejemplo muy interesante para ver como la IA artificial está ayudando a un sector tan tradicional: utilizan la IA para crear modelos tridimensionales a partir de un conjunto de fotografías (fotogrametría), lo que se conoce como Gemelos Digitales. Estos modelos 3D son manipulables pudiendo diseñar a partir de ellos representaciones virtuales de nuevos productos, esta gran ventaja se interrelaciona y vincula con la operativa de la propia fábrica en sí, pues permite variaciones casi instantáneas de los productos a fabricar, antes de una producción en cadena. En este caso, se pueden reducir los costes de probar nuevos materiales o diseños sin tener que incurrir en costosos prototipos, mejorando además la calidad final y pudiendo simular muchas más situaciones de estrés que las que podrían emularse en un laboratorio".

OBSTÁCULOS EN EL CAMINO

Sin embargo, y pese al creciente número de aplicaciones de la IA en los últimos años, los impactos del desarrollo de la IA no se limitan al desarrollo empresarial e industrial. También tienen una importante dimensión jurídica, social y ética. Si bien, por un lado, la IA ofrece un enorme potencial, al mismo tiempo nos enfrentamos al desafío de volver a capacitarse, dilemas legales, éticos y legales con respecto a la implementación de la toma de decisiones algorítmicas y problemas relacionados con la explicabilidad general del sistema, particularmente visibles en el aprendizaje profundo.

Entre algunos de los desafíos más importantes relacionados con la IA, cabe mencionar:

- **Interacción** junto con problemas relacionados con la asignación de roles sociales a otros, encontrando patrones de (des) éxito.
- **Accesibilidad e integridad:** los sistemas de inteligencia artificial se utilizarán cada vez más en contextos importantes, si no críticos.
- **Privacidad y seguridad:** las preocupaciones por la privacidad son un problema relevante para el funcionamiento de los sistemas basados en IA.
- **Abordar el sesgo algorítmico:** dicho sesgo se puede encontrar en todas las plataformas, incluidos, entre otros, los resultados de los motores

"Cuando eres capaz como empresa de entender el flujo de tus procesos, puedes empezar a automatizar acciones, con lo cual reduces tiempos y costes mientras aumentas la productividad. Además, eso redunda en una mayor satisfacción tanto de empleados como de clientes"

DAVID SANZ,
SOLUTION CONSULTING SENIOR MANAGER PARA IBERIA E ISRAEL DE SERVICENOW

CONTENIDOS↓

de búsqueda y las plataformas de redes sociales. Ocurre cuando un sistema informático refleja los valores implícitos de los humanos que participan en la codificación, recopilación, selección o uso de datos para entrenar el algoritmo. El sesgo puede tener impactos que van desde violaciones involuntarias de la privacidad hasta el refuerzo de los prejuicios sociales de raza, etnia, sexualidad o género.

❖ **La explicabilidad y la transparencia** se refieren al tipo de IA cuyas acciones pueden ser fácilmente entendidas por los humanos. Contrasta con el concepto de "caja negra" en el aprendizaje profundo, ("interpretabilidad" de los trabajos de algoritmos complejos, donde incluso sus diseñadores no pueden explicar por qué la IA llega a los datos de decisión específica).

Para Iván Gento, Marketing Executive de Synology para España, uno de los principales obstáculos que nos encontramos es "el lento proceso de digitalización. A pesar de que la pandemia a favorecido un proceso profundo de digitalización de forma transversal, todavía nos encontramos avanzando sobre la punta del iceberg", reflexiona. Además, alude a la falta de "conocimiento a nivel organizativo del potencial del IA. Como resultado nos encontramos con que el IA no se plantea a nivel estratégico por lo que resulta difícil que encaje en los planes de crecimiento y de desarrollo empresarial". Finalmente, "otro de los problemas que nos encontramos frecuentemente es de la falta de talento capaz de llevar a cabo estas implementaciones. Ya nos encontramos con este problema cuando se trata de adoptar un modelo de transformación digital basado en la gestión de datos. Nos encontramos en muchos casos que ante la falta de datos almacenados y profesionales en el sector tecnológicos resulta muy complejo implementar todos los cambios que requiere la infraestructura y organización".

Mientras, la líder de la práctica de Analytics en SAS Consulting España alude como uno de los principales problemas a la disponibilidad de datos. "No siempre se dispone de la información histórica adecuada para poder crear un algoritmo que tome decisiones en base a lo aprendido. Muchas veces lo adecuado es definir un plan de recopilación de información de los datos nuevos y la realización de un roadmap analítico. Esto nos permitirá ir obteniendo insights de los datos que disponemos, a la vez que vamos evolucionando en la madurez analítica para ese determinado caso", expone. Además, cree que otro de los problemas es la operacionalización de la IA. "Muchas veces encontramos equipos que han desarrollado correctamente modelos de inteligencia artificial, pero que desconocen cómo llegar al Last Mile de analytics que implica ponerlos en producción y disponibles para que no se queden en desarrollos y obtener así el valor esperado. Actualmente conocemos que más del 50% de los modelos que se construyen nunca se ponen en producción".

A este respecto, David Sanz cree que es posible que "la implantación global de tecnologías basadas en IA implique todavía unos costes elevados y sea difícil calcular el retorno de una inversión tan grande" y asegura que ellos apuestan por "ayudar a nuestros clientes en el cálculo de esos retornos, y cuando lo hacemos, el caso de negocio sale muy rápido".

Como incide José Luis Flórez, "no me centraría en los obstáculos porque pienso que la adopción está sucediendo a un ritmo extraordinario, pero si tuviera que citar un aspecto crítico sería la propia comprensión de lo que es la IA, sus posibilidades

CONTENIDOS↓

y limitaciones, por parte del personal directivo. Falta formación básica en la capa ejecutiva de gestión". En cuanto al mayor obstáculo de la IA en su desarrollo, este experto considera que "para aprender necesita una enorme cantidad de ejemplos. En comparación, un ser humano es capaz de generalizar o descubrir patrones a través de un proceso de aprendizaje que es mucho más eficiente. Uno de los principales retos de la IA consiste en alcanzar una eficiencia energética más cercana a la del cerebro humano para aprender".

Alberto Calvo añade que en su implantación, la IA se enfrenta a "perfiles muy diferentes a nivel generacional; infraestructuras no preparadas y que todavía se ve como gasto y no inversión", mientras que en su desarrollo cree que está avanzando mucho a nivel mundial, España incluida. "Solo que no se está convirtiendo en Commodity, pero cada vez hay más empresas implantando modelos predictivos y convirtiendo a los antiguos analistas de datos en artistas del dato".

"El uso de la IA produce ventajas competitivas tanto optimizando los procesos y las decisiones que se toman en las organizaciones, como a nivel cliente mejorando la satisfacción y conexión con la empresa"

VIOLETA GALLEGO,
LÍDER DE LA PRÁCTICA DE ANALYTICS
EN SAS CONSULTING ESPAÑA

¿INVIERNO O VERANO? LA IA EN 2026

Como veíamos antes, los periodos en los que la IA ha sufrido grandes avances y desarrollos se han considera los veranos de la IA. Por el contrario, las épocas más oscuras, en las que los avances apenas han sido constatables y dignos de mención, son catalogados como los inviernos. Incluso cuando hablamos de Inteligencia Artificial es difícil hacer predicciones sobre el futuro pero, ¿dónde estará esta tecnología dentro de cinco años?

Javier González Alonso, Senior Solutions Architect de Dell Technologies, cree que la IA "estará presente ayudándonos en la mayoría de nuestras tareas cotidianas. Cada día aparecen nuevas aplicaciones de la IA que no se habían tenido en cuenta hasta ahora, así que como decía antes, la tecnología no nos pone límites, solo nuestra imaginación los pone".

Mientras, Alberto Pinedo, National Technology Officer de Microsoft en España, alude a que en tanto los investigadores de Microsoft como los de otras empresas especializadas "están progresando en el desarrollo de sistemas de IA que puedan aprender información de una forma más sofisticada. Por ejemplo, muchos apuntan hacia el aprendizaje no supervisado o autosupervisado, un método en el que los sistemas de IA buscan patrones en los datos que no están etiquetados, en lugar de simplemente ser alimentados con datos que han sido etiquetados previamente". Además, "somos conscientes de que la IA seguirá creciendo y, nosotros creemos que puede ser fundamental en el uso de modelos de lenguaje natural muy grandes, ayudando con una variedad de tareas, como parafrasear un discurso o sugerir mejores respuestas a los correos electrónicos". Pero, yendo más allá, asegura que "las soluciones más novedosas incidirían en la Inteligencia Artificial Fuerte para crear sistemas que funcionen

más como creemos que funcionan los cerebros de las personas. Eso sí, los expertos dicen que, para hacer que los sistemas de IA emulen a los cerebros de las personas, necesitamos obtener una comprensión más profunda de cómo funcionan estos". Eso sí, teniendo en cuenta los desafíos, considera que "las tecnologías que utilizan la IA deben desarrollarse de manera responsable y de una manera que fomente la confianza y mantenga las protecciones de privacidad. Pero somos optimistas sobre su futuro y creemos que los avances resolverán muchos más desafíos de los que presentan". "Al final, para nosotros la tecnología es un facilitador y nuestro enfoque sobre el futuro de la IA es consistente con la misión de la empresa: ayudar a cada persona y organización del planeta a seguir creciendo de forma segura y responsable", concluye.

Por su parte, Nacho Fernández, Business Development Manager de Arsys, asegura que no se atreve a hablar de años o plazos de tiempo, pero sí que "tendrá un impacto directo en todos los aspectos de nuestras vidas. Especialmente en el mercado de trabajo, haciendo que desapa-

"Para que un programa sea considerado IA es necesario que el programa sea capaz de gestionar una gran cantidad de datos ofreciendo un procesamiento relativamente rápido y algoritmos inteligentes, lo que permite que el software aprenda automáticamente de patrones o características en los datos"

IVÁN GENTO, MARKETING EXECUTIVE DE SYNOLOGY PARA ESPAÑA

LA INTELIGENCIA ARTIFICIAL EN LOS NEGOCIOS

rezcan determinadas posiciones y dando lugar a otras nuevas. Pero vamos a ver sus huellas en los coches autónomos, el transporte, la robótica, logística, la medicina, el ocio e incluso en nuestra vida doméstica. Estamos rodeados de todo tipo de dispositivos (smartphones, relojes inteligentes, electrodomésticos, asistentes de voz, sistemas médicos) capaces de provocar una verdadera explosión de datos y que, más pronto que tarde, empezarán a entenderse entre sí e intentarán actuar en función de nuestros comportamientos".

Lo que parece claro, al menos a ojos de Manel Picallò, Consulting Systems Engineer en NetApp España, es que la IA se está convirtiendo en una tecnología fundamental con beneficios para todos los sectores. "Está transformando ámbitos tales como la agricultura, la fabricación, la automoción y los servicios financieros. En muchos de ellos, el Machine Learning y el Deep Learning son ya esenciales para la competitividad y la viabilidad a largo plazo". Además, añade que en el sector salud está siendo una "gran revolución que nos permitirá tener un sistema sanitario mucho más eficiente en todos los aspectos, en calidad y en sostenibilidad económica. Pero existen otros sectores en auge, como el control y gestión de procesos: análisis inteligentes, determinación de objetivos, etc. En la fabricación también vamos a ver una notoria influencia, desde el diseño, gestión de proyectos, planificación, monitorización y mejora de la robótica industrial".

Violeta Gallego, Líder de la práctica de Analytics en SAS Consulting España, detalla que la IA está en constante actualización, por lo que "conocer lo que está por venir es complicado. Su propio uso abrirá nuevos caminos que ahora mismo no somos capaces de visualizar. Para mí el factor clave será mantenerse actualizados, ya que no hay duda de que la inversión en IA repercute en beneficios para la empresa. ¿Próximas tendencias? Entre otras áreas en SAS seguiremos apostando por la democratización de la IA para acercar su uso a todos los perfiles de la manera más sencilla y ágil posible, usando algoritmos de última generación", detalla.

Mientras, Iván Gento, Marketing Executive de Synology para España, considera que "debemos esperar un crecimiento masivo de la inteligencia artificial. Dentro de la gestión del dato, la IA es el foco tecnológico más atractivo, y la innovación se acelera junto con el crecimiento de los datos. Una encuesta reciente revela que el 43% de las empresas esperan ejecutar modelos de inteligencia artificial en los próximos tres años, en comparación con solo el 28% que lo están haciendo en la actualidad. También vemos un cambio en el pensamiento sobre cómo lidiar con las enormes

cantidades de datos que se generan fuera de las cuatro paredes del centro de datos, y la viabilidad de ejecutar casos de uso de IA".

Para David Mosen, Chief Data Scientist de Crayon Group, "disfrutaremos de una IA multimodal que se alimenta de múltiples tipos de datos: imagen, texto y sonido. En el entorno laboral, la IA se encargará de todos los trabajos con tareas repetitivas, el ser humano solo se centrará en tomar decisiones de alto nivel. Con ella, y gracias a nuevos desarrollos en robótica y tecnología inalámbrica, el teletrabajo transcenderá lo que conocemos ahora. Así, por ejemplo, una sola persona podrá supervisar de forma remota máquinas diversas, como camiones, carretillas elevadoras, robots quirúrgicos, maquinaria agrícola, equipos de fábrica, etc. La IA se utilizará cada vez más como un asistente avanzado que aumenta las capacidades humanas, por ejemplo a la hora de conducir o de incorporar inmediatamente datos en tiempo real en áreas como el marketing. Donde también será imprescindible es en el campo de la biología molecular, especialmente en virología y en el desarrollo de medicamentos. Y, sin duda, pocos juegos habrá en los que la IA no supere a cualquier humano". Además, considera que "su peso va a ser tan determinante que CEO de grandes empresas provendrán del ámbito de la ciencia de datos y la IA. Y sin duda, las empresas que ahora cuentan con una buena estrategia de datos estarán sacando ya fruto de soluciones de IA asentadas en plataformas de datos robustas. Otra certeza es que China será el origen de la mayor parte de investigación avanzada en IA y que todos los desarrollos que se hagan utilizarán, al menos parciamente, herramientas de los grandes proveedores de la nube".

David Sanz, Solution Consulting Senior Manager para Iberia e Israel de ServiceNow, reconoce que, "efectivamente, predecir el futuro nunca es fácil y como ocurre con la gran mayoría de los avances tecnológicos, delinear el desarrollo de la IA es complejo" pero explica que la visión a futuro de ServiceNow es que "la IA empezará cada vez más a usarse para conectar diferentes procesos empresariales de forma más eficiente, y es algo que ya estamos viendo: nuestra plataforma es capaz de ingestar datos de sensores IoT, por ejemplo, detectar anomalías en los mismos y lanzar automáticamente una tarea asignada al empleado más preparado y más cercano al problema para una resolución ágil. El resultado es una operativa mejor; por detrás hay una compleja tecnología que usa IA, pero lo mejor es que ni el cliente, ni el técnico que ha resuelto el problema ni el gestor del servicio perciben esa complejidad. Las cosas simplemente ocurren de manera más rápida y mejor, y ese es el futuro: la eficiencia máxima de los procesos, que en esos cinco años estarán con gran probabilidad basados en su mayoría en tecnologías digitales".

Mientras, Alberto Calvo, Territory Manager de Omega Peripherals, alude a que estaremos en META, en un mundo virtual. "Creo que sinceramente estará siendo explotada en ese nuevo mundo virtual, donde se podrá perfeccionar los avatares en base incluso a estados de ánimo y donde con el IoT habrá información precisa y adaptada".

José Luis Flórez, director de Plaiground, la unidad de negocio especializada en inteligencia artificial de Minsait (Indra), concluye asegurando que "estará cada vez más integrada tanto en los procesos de negocio de las organizaciones como en nuestra propia vida, incluso en nuestro propio cuerpo, donde ya el móvil es un apéndice imprescindible en nuestra anatomía, un complemento que nos aporta capacidades sobrehumanas". ■

MÁS INFORMACIÓN

- 5G Edge Automation and Intelligence
- IA y su aplicación en los Servicios Públicos
- Indicadores de uso de la IA en las empresas españolas
- Guía empresarial sobre Inteligencia Artificial

¿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 IT User

Tecnología para tu Empresa

Con la colaboración de:

NFON
Cloud Telephone System

NO SOLO it

PANEL DE EXPERTOS

TALENTO

Formación digital: de ser una ventaja a una necesidad

Óscar Fuente,
Director y fundador
de IEBS Business School

REFLEXIONES éTICas

¿Naciste allá por el año 1971?

Màrius Albert Gómez,
Experto en digitalización
e Innovación y humanista
por convicción

CIBERSEGURIDAD 4.0

El Amanecer de la Humanidad Digital VI: ¿cómo serán los nuevos Jueces Digitales?

Mario Velarde Bleichner,
Gurú en CiberSeguridad

Formación digital:
de ser una ventaja a una necesidad

La situación derivada de la pandemia ha obligado a las empresas a sumarse a la digitalización para poder seguir adelante. Sin embargo, los grandes avances conseguidos en cuanto a transformación digital no han ido de la mano del nivel de conocimientos ni habilidades digitales de los empleados, ni de la población en general. Esto supone una barrera en el avance y el desarrollo de las organizaciones, que ven la falta de profesionales digitales formados como un freno en su crecimiento.

Según el INE, España presenta una evolución positiva de los principales indicadores internacionales de digitalización en los últimos años

Óscar Fuente

Director y fundador de IEBS Business School

Óscar Fuente es el fundador de IEBS Business School. Anteriormente creó otras empresas como Área de Ventas, la Agencia Digital Área Interactiva, Diverbium o el portal Iberestudios. Ha participado como inversor y/o Business Angel en startups de éxito como Glovo, Coverfy, Chicfy, Wazypark o Hannun, entre otras. También ejerce como Mentor en la aceleradora Seedorocket.

pero no ha avanzado de la misma forma en la dimensión de Integración de Tecnología Digital por parte de las empresas. De hecho, España está situada en el número 13 en el ranking europeo entre los 28 países

Por otro lado, un estudio realizado por la escuela digital IEBS revela que, a pesar de los grandes avances tecnológicos, solo el 3,2% de los profesionales son expertos en estas tecnologías, lo que significa que se necesita un mayor grado de especialización para cubrir la creciente demanda. Esto deja entrever que la formación digital no ha crecido a la par que el desarrollo del sector, existiendo un retraso generalizado entre los profesionales. De hecho, como curiosidad, este mismo informe señala que, mirando a futuro, la inteligencia artificial es la tecnología preferida de los profesionales, los cuales prevén utilizarla en un futuro próximo, con un 69,2%. A esta le sigue el Blockchain, con un 38,5%, e Internet of Things, con un 38,5%.

Hace unos meses la Secretaria de Estado de Digitalización, Carmen Artigas, dijo que, en la actualidad, "el 43% de la población no tiene competencias básicas, es decir, son analfabetos digitales". Una cifra muy preocupante teniendo en cuenta que la mayor parte de empleos (de ahora y del futuro) se basarán en esas habilidades. Lo cierto es que la oferta formativa de las universidades y los colegios tradicionales no se adecúa a la alta demanda de competencias digitales, por lo que la brecha digital no deja de aumentar.

A pesar de todo, parece que enfrentamos este reto con positividad ya que, según la encuesta de IEBS, 9 de cada 10 profesionales tiene la intención de formarse en alguna de estas tecnologías para mejorar su recorrido profesional. Tiene sentido ya que los puestos de trabajo relacionados con la tecnología, como expertos en Big Data, Realidad Virtual o Inteligencia Artificial encabezan las listas de perfiles más demandados por las empresas.

Para que nos hagamos una idea del impacto que las nuevas tecnologías tienen y tendrán en el empleo, según diversos estudios, actualmente el 40% del PIB de la Unión Europea procede de actividades que se desarrollan en un entorno digital. Además, los pronósticos apuntan a que se crearán cuatro empleos digitales por cada cinco tradicionales. No sólo aquellos puestos de trabajo como los mencionados anteriormente, sino también aquellos que implican tendencias mundialmente implantadas que han venido para quedarse, como el teletrabajo, el comercio electrónico, la telemedicina o la formación online.

Por todo esto, la formación en competencias digitales no es solo una buena opción para aquellos que quieran prosperar en su empresa o crecer profesionalmente, sino prácticamente una necesidad. El mundo en el que vivimos actualmente es digital y formarse en el ámbito nos proporciona un mayor abanico de posibilidades en muchos sentidos. Sabemos que todo seguirá evolucionando y hay que prepararse para ello, tanto empresas como profesionales.

La transformación digital en las organizaciones es un proceso lento y complicado, pero fundamental si queremos asegurarnos de la supervivencia de nuestra empresa en un futuro. No solo implica la implementación de plataformas y herramientas, sino que engloba el desarrollo de toda una cultura empresarial más datificada y ágil. Sin duda, se trata de una realidad ineludible que no solo afecta a las multinacionales, sino a todo tipo de negocios. Su irrupción ha hecho que los clientes sean cada vez más digitales, un cambio mucho más profundo que simplemente el auge de las compras online. Las empresas han tenido que adaptarse a las preferencias y nuevos hábitos de los clientes, en un contexto de comunicación global y multicanal impulsando la creación de relaciones directas y duraderas. ■

MÁS INFORMACIÓN

www Solo tres de cada 10 profesionales son expertos en nuevas tecologías

CONTENIDOS↓

¿Naciste allá por el año 1971?

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".

Si naciste allá por el año 1971, naciste al amparo del Imaginar de John Lenon en un año que ha sido considerado probablemente el mejor año de la historia del Rock'n'Roll y del Rythm & Blues. Seguramente pudiste vivir la explosión de las videoconsolas y el amanecer de la computación personal con tu Commodore, MSX o Spectrum mientras se enviaba ya por entonces el primer e-mail. Mientras tanto, Estados Unidos rompía el patrón oro-dólar generando probablemente un punto de inflexión en el comportamiento de los indicadores macroeconómicos y sociales, y España se avecinaba a sus democráticas nuevas puertas mientras disfrutaba de veinte poemas y una canción desesperada de un premiado Neruda.

Si naciste en el año 1971, bien unos cuantos antes, bien unos cuantos después, generacionalmente seguro que compartes más o menos dichas experiencias, junto con muchos otros eventos propios y remarcables que se evocarán a tu mente. Aun así, es bastante más que probable que quizás no se evoque el hecho más decisivo de esos años y que marcaría "inconscientemente" tu vida como profesional de las TIC. Ese año tiene lugar el simposio "71' ACM SIGACT Symposium on the Theory of Computing", donde un señor llamado Stephen A. Cook publica un artículo llamado "The Complexity of Theorem Proving Procedures" dando pie a la consolidación de uno de los problemas más famosos del mundo de la computación cuya resolución se premia con un millón de dólares (Problemas del Milenio del Instituto Clay de Matemáticas). Hablamos de "P vs NP", relativo a lo que se puede resolver computacionalmente en un tiempo eficiente polinómico o no (el lector

entienda a modo Stephen A. Cook, antes de que se apague nuestro Sol). Aprendimos sobre la indecidibilidad (¿existe solución?) de algunos problemas, así como sobre la intratabilidad de algunos otros (¡tiempo necesario de resolución!). En los tipos de problemas NP descansa precisamente la "bondad" de un problema que es la base de nuestros actuales sistemas criptográficos y de seguridad (por ejemplo para la compra "segura" por Internet), así como también los "retos" para muchos otros ámbitos de problemas diarios de carácter práctico y de investigación, y que normalmente requerirían de métodos de fuerza "bruta", esto es, capacidad de computación.

La capacidad de computación resulta ser pues, inherente a nuestro afán de comprensión de todo aquello especialmente complejo que nos rodea. Desde el estudio del clima y la predicción de sus potenciales cambios, al propio estudio, observación y comprensión del universo, o bien el estudio de análisis genómicos o la predictibilidad y personalización de medicamentos. También de multitud de problemas complejos del mundo de la empresa, en la energía, en la movilidad inteligente y autónoma... Una capacidad de computación que ya actualmente nos permite viajar desde los teraflops y petaflops, hacia el nuevo "universo" de la computación a exaescala (exaflop o 1018 FLOPS) o bien avanzar en nuevos esquemas especializados como pueden ser el desarrollo de la computación cuántica o neuromórfica. Un viaje hacia potenciales disruptores del orden de magnitud de los problemas que hoy en día podemos resolver con los supercomputadores más avanzados que tenemos, no exento de grandes retos como puede ser el consumo energético en la exaescala o la propia escalabilidad de los qubits.

Quiero creer que, como ingenieros, el contexto que se nos originó desde su formulación la indecidibilidad P vs NP representó en buena medida, una motivación clave de superación profesional no sólo ya en el diseño y desarrollo de mejores capacidades computacionales como la exascala o el quantum, sino también en nuestro afán personal de mejor comprensión de los problemas que nos rodean y en esa búsqueda continua de soluciones y estrategias "útiles" que, si bien no puedan confirmar un resultado, resulten la mejor aproximación disponible para los mismos.

Seguramente, dicho contexto representa como colectivo TIC, nuestra base fundamental de creación de conocimientos y para la investigación científica. De cómo proyectamos el futuro. En ese pensamiento tal vez filosófico que trata de vislumbrar lo posible a partir de lo real y potencial, para el conocimiento y transformación de nuestra sociedad con las TIC. La trascendencia de ese pensamiento supera los vagos planteamientos utilitarios de las tecnologías, para ponerlas al servicio del humanismo, como profesionales, como managers, como investigadores.

En 1971, cuando nací, no me di cuenta, pero representa que el destino nos condujo a muchos al mundo de las TIC, permitiéndonos poder contribuir profesionalmente a su desarrollo, poder ejercer personalmente como pensadores y humanistas TIC, y en todo caso, poder combinar como managers ambos mundos. Nos quedaría pendiente a algunos en dicha combinación, poder soportar con mucha más intensidad las propias actividades de investigación y transferencia tecnológica empresarial y social. Nos faltaría reforzar ahí el nivel de esfuerzo y de inversión. Pero firmemente creo, que la combinación final de todo ello, no supone un problema ni indecidible, ni intratable. Eso sí, seguramente sí debería de ir acompañado de altas dosis de Rock'n'Roll de los 70. ■

MÁS INFORMACIÓN

- The European High Performance Computing Joint Undertaking, EuroHPC
- El BSC inaugura su nueva sede para los superordenadores MareNostrum del futuro
- P VS NP Problem, Clay Mathematics Institute

El Amanecer de la Humanidad Digital VI: ¿cómo serán los nuevos Jueces Digitales?

La Justicia también tendrá su Disrupción en este amanecer de la nueva Humanidad Digital. Es inimaginable que cuando la Humanidad esté compuesta por una mayoría de Nativos Digitales o como de forma natural lleguen a ser todos los humanos vivos Nativos Digitales la justicia continúe siendo como lo es en la actualidad, que, con sus defectos y carencias, ha sido muy útil en estos dos siglos previos para solucionar los conflictos de los ciudadanos.

El Poder Judicial, como una de las tres patas de los estados democráticos modernos, tendrá

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.

que evolucionar para prestar el servicio adecuado a sus nuevos Ciudadanos Digitales conforme a los cambios que produzca en ellos la gran disrupción digital en curso.

Como es natural, los Ciudadanos Digitales esperan que los servicios sean inmediatos o, al menos, ágiles, eficientes y eficaces, con procesos digitalizados y apoyo de las nuevas tecnologías como, por ejemplo, la Inteligencia Artificial y el "Deep Learning".

Un buena tarea para los responsables del Poder Judicial, además de las habituales, será ir evolucionando los procesos judiciales introduciendo nuevas tecnologías de apoyo a jueces y funcionarios, digitalizando procesos para hacerlos más eficientes y eficaces, estableciendo procesos formativos adicionales en nuevas tecnologías digitales para jueces, abogados y funcionarios y personal de apoyo, creando las infraestructuras de información y datos para los futuros procesos automatizados de soporte a todo el sistema judicial.

Las Universidades deberían haber iniciado ya la inclusión de formación de nuevas tecnologías digitales en los planes de estudios de la carrera de Derecho para que todos los nuevos abogados estén a la altura de su generación digital, no solo para sustituir el papel por un PC para realizar sus escritos, conseguido ya como primer paso de la digitalización.

Deberían tener los nuevos abogados al terminar su carrera un conocimiento práctico de cómo los sistemas de Inteligencia Artificial, usando inmensas bases de datos de sentencias, les podrán ayudar a obtener información para la elaboración de sus casos.

Creo que vienen tiempos apasionantes, no solo para los responsables actuales del Poder Judicial que tienen el deber de ir cambiando la Justicia a una nueva estructura digital que sea más ligera, eficaz y eficiente para que las nuevas generaciones digitales de abogados, jueces, fiscales y personal de apoyo judicial estén a la altura de los cambios que llegan con las nuevas generaciones de Nativos Digitales que conformaran en dos o tres generaciones la nueva Humanidad Digital.

También vienen tiempos apasionantes para los Nativos Digitales que elijan la carrera de Derecho. Son ellos los que tendrán que convivir con los modelos y procesos antiguos para

La Disrupción Digital no es la destrucción de la Justicia como la conocemos, más bien será la evolución de todo lo bueno que tienen los sistemas judiciales que, mediante la utilización de las tecnologías digitales, mejorarán radicalmente sus procedimientos

crear y establecer la nueva Justicia Digital para cuando todos los humanos no digitales seamos parte de la historia.

Los nuevos Jueces Digitales necesitarán un cambio de paradigma del Poder Legislativo que anteponga la necesidad de adecuar las leyes a los nuevos tiempos digitales y use solamente un mínimo de tiempo para la confrontación política. El ciudadano actual está cansado de ver como se pierde el tiempo en los Parlamentos en discusiones políticas estériles en vez de aportar el trabajo de actualizar las leyes conforme al cambio tecnológico que la Digitalización de la sociedad está trayendo a la vida diaria de los ciudadanos.

Las tres patas de la Disrupción Digital de la Justicia son, primero, el cambio de procedimientos para mejorar radicalmente los tiempos de la Justicia utilizando las nuevas herramientas digitales, como, por ejemplo, la Inteligencia artificial; segundo, la adecuación de las leyes a los nuevos retos a los que se tendrá que enfrentar la sociedad en la que le toque vivir a la Humanidad Digital; y tercero, la capacitación de las personas que, como ahora, se ocupen de la Justicia empezando por los jueces, fiscales, abogados y, por supuesto, todo el personal auxiliar.

Por supuesto, esta Disrupción Digital de la Justicia cuenta y contará con detractores que, en nombre de un falso sentido de la conservación de las tradiciones, intentarán boicotear los cambios que son imprescindibles, tal vez solo por mantener ventajas de las que han estado disfrutando durante ya varios siglos en las llamadas democracias modernas.

La Disrupción Digital no es la destrucción de la Justicia como la conocemos, más bien será la evolución de todo lo bueno que tienen los sistemas judiciales que, mediante la utilización de las tecnologías digitales, mejoren radicalmente procedimientos obsoletos que, aunque fueron útiles en siglos pasados, no lo serán para la nueva sociedad de la Humanidad Digital.

El resultado de la Disrupción Digital de la Justicia será un servicio casi inmediato, eficaz y eficiente que estará a la misma altura de las mejoras de las nuevas generaciones digitales en todos los servicios públicos o privados cundo en dos o tres generaciones la gran Disrupción Digital Global haya surtido sus efectos beneficiosos.

Así pues, y espero no equivocarme, los Jueces Digitales que impartirán justicia en la Humanidad Digital serán personas de una gran capacitación jurídica pero también de una gran capacitación tecnológica para, conforme al gran avance de la humanidad, realizar su importante cometido en la sociedad con los mismos criterios de inmediatez, eficacia y eficiencia que el resto de la sociedad del futuro. ■

MÁS INFORMACIÓN

Transformación Digital del Poder Judicial

it Reseller
TECH&CONSULTING

Cada mes en la revista,
cada día en la web.