it Digital Security

La publicación electrónica sobre Seguridad Digital que necesitas

Junio 2022 - nº 53

Empleado formado, empresa segura

‘La inspección de tráfico de red en tiempo real es fundamental’ Jesús M. Doña, EMASA

‘Los clientes lo tiene difícil a la hora de decidir qué servicios quieren’ Rosa Ortuño, OptimumTIC

‘Tecnológicamente hablando es un momento realmente emocionante’ Iker del Fresno, Aruba

Foro IT User AAPP. Tecnologías habilitadoras para un Gobierno abierto

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

Digital Security

Directora Rosalía Arroyo, rosalia.arroyo@itdmgroup.es
Colaboradores Hilda Gómez, Arantxa Herranz, Reyes Alonso, Ricardo Gómez
Diseño revistas digitales Contracorriente
Producción audiovisual Miss Wallace, Alberto Varet
Fotografía Ania Lewandowska

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

Empleado formado, empresa segura

Modernizar su lugar de trabajo mediante la adopción de tecnologías móviles y en la nube puede ser una experiencia liberadora tanto para los profesionales de TI como para los empleados. Sin embargo, a medida que la empresa adopta esta libertad sin ataduras, aumenta su superficie de ataque y debe asegurarse de salvaguardar la información, los procedimientos y, por supuesto, a los trabajadores. ¿Cómo? La respuesta puede parecer sencilla, aunque esto no significa que sea fácil, como ponemos de manifiesto en el tema de portada de #ITDSJunio.

En este número de la revista contamos además con varios protagonistas. El primero es Jesús M. Doña, responsable de infraestructura, soporte y ciberseguridad en el Departamento IT de EMASA, quien asegura, entre otras muchas cosas, que no puede vivir sin un SOC y que la inspección de tráfico de red en tiempo real es fundamental.

Rosa Ortuño, CEO de OptimumTIC, y una mujer de reconocido prestigio en el mercado de ciberseguridad, nos cuenta que los clientes lo tienen difícil a la hora de decidir qué servicios quieren o necesitan, mientras Iker del Fresno, country manager de Aruba Networks desde hace unos meses habla del "emocionante" momento que se está viviendo en el mercado de TI; y Fabio Cichero, Yubico Channel Sales Manager Southern Europe de Yubico, habla del passwordless como un objetivo a perseguir.

En la actualidad os resumimos la ponencia del Dr. Tom Leighton, CEO y cofundador de Akamai, durante el Cybersecurity Summit celebrado por la compañía a finales de mayo; y os hablamos de Maltiverse, una empresa española que nació como un hobby y hoy cuenta con decenas de miles de usuarios únicos.

¿Te interesa la seguridad? Entonces seguro que te gusta este número de IT Digital Security.

Empleado formado, empresa segura

Índice de anunciantes

ESET Bitdefender Stormshield WatchGuard Aruba

SonicWall Citrix IT AAPP IT User IT Reseller

itds

Sumario

Actualidad

Akamai propone ZTNA y microsegmentación como la nueva aproximación a la ciberseguridad

Maltiverse, el Threat Intelligence sencillo que nació como un hobby y hoy tiene 85.000 usuarios únicos

Entrevistas

'La inspección de tráfico de red en tiempo real es fundamental'
Jesús M. Doña, EMASA

'Los clientes lo tiene difícil a la hora de decidir qué servicios quieren o necesitan'
Rosa Ortuño, OptimumTIC

'Tecnológicamente hablando es un momento realmente emocionante'
Iker del Fresno, Aruba

'El passwordless es donde queremos llegar'
Fabio Cichero, Yubico

No solo IT

El Amanecer de la Humanidad Digital IX: Los Ciudadanos Digitales no superaron la oscura década de los 20
Mario Velarde Bleichner

Revista Digital

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**

Digital Security
Progress. Protected.

PROVEEDOR Nº 1 DE LA UNIÓN EUROPEA EN CIBERSEGURIDAD EMPRESARIAL

MADE IN EU

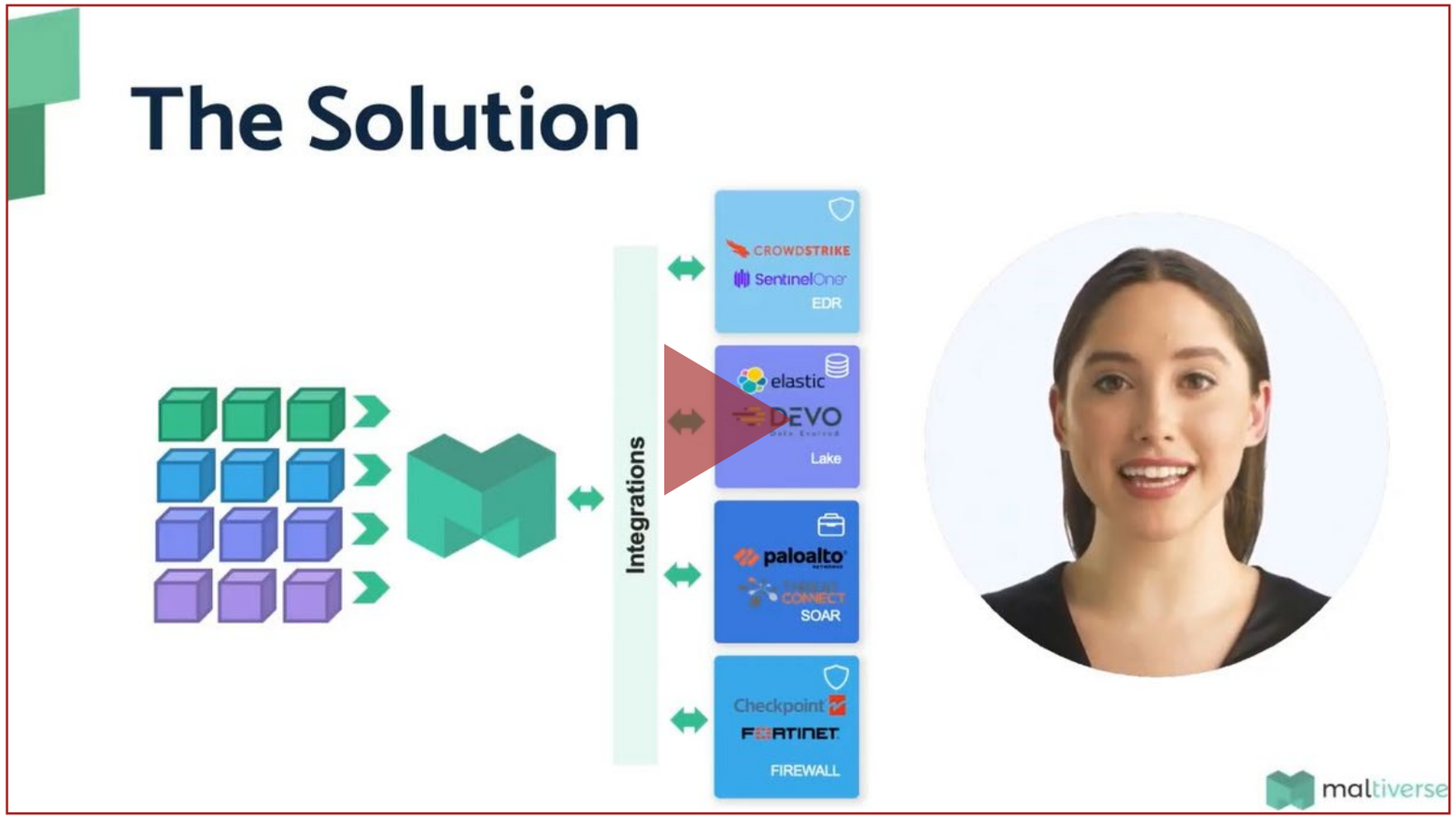
Maltiverse,

el Threat Intelligence sencillo que nació como un hobby y hoy tiene 85.000 usuarios únicos

Los equipos pequeños y medianos de SecOps no pueden invertir tanto tiempo y esfuerzo para incorporar decenas de fuentes de Threat Intelligence, seleccionarlas y mantenerlas. Maltiverse automatiza este arduo trabajo y proporciona un servicio de inteligencia de amenazas eficaz

Maltiverse se creó como un servicio dirigido a analistas de ciberseguridad para el análisis avanzado de indicadores de compromiso. El germen fue el Sistema de Alerta Temprana del CCN-CERT en el que trabajaba Hesaul Sánchez Raya, uno de los fundadores de Maltiverse, quien en una reunión mantenida con IT Digital Security nos explica que “de ese proyecto vimos que hay ciertos patrones de ataque que tienden a repetirse mucho. Si aprendes del primer ataque y haces análisis, esa información la puedes extrapolar a los sistema de defensa y así puedes prevenir los ataques”.

Con la filosofía de intentar compartir la información de las amenazas se inició Maltiverse, un proyecto con tecnología moderna, montado en big data, cloud computing, inteligencia artificial,



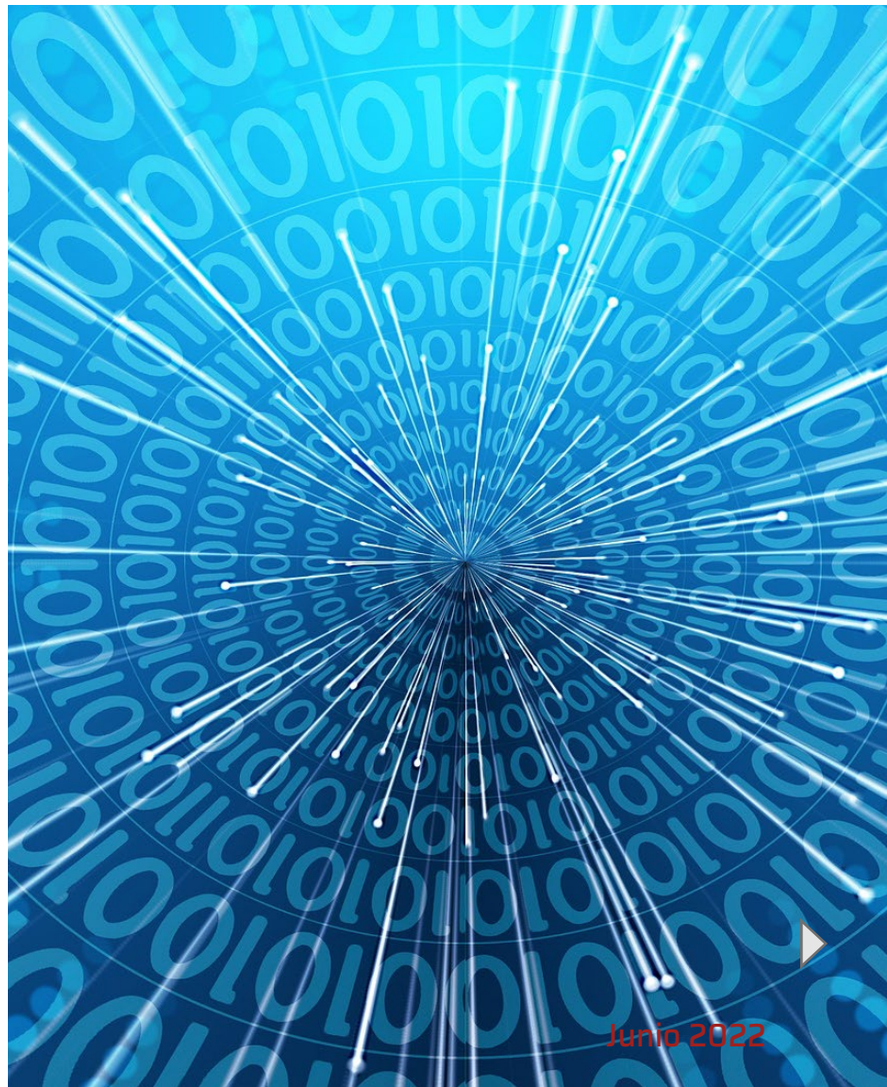
WHAT IS MALTIVERSE **CLICAR PARA VER EL VÍDEO**

machine learning… que hace más de tres años se publicó en Internet y que ya recibe más de cuatro millones de visitas al mes y tiene unos 85.000 usuarios únicos, cifras significativas “para ser algo tan de nicho”, explica Hesaul.

En los últimos años se ha constatado que las campañas de malware tienen una vida útil cada vez más corta. Esto significa que, ante un incidente de seguridad real, es muy probable que los Indicadores de Compromiso, IOC, sean desconocidos. Maltiverse analiza todas las dimensiones posibles del conjunto IOC conocido almacenado para compararlas con indicadores desconocidos.

En sus comienzos plataforma de Maltiverse era de acceso gratuito, “pero tuvimos que poner límites porque empezamos a ver empresas de Estados Unidos, la India o China que nos hacían miles de consultas al día. De alguna manera esas empresas se estaban lucrando con nuestro servicio, por lo que

El 98% de los ataques son predecibles, y teniendo los indicadores de compromiso cargados correctamente te puedes proteger contra ellos de una manera sencilla



"Lo nuestro va de trabajar muy poco, que todo sea automático"

Hesaul Sánchez, Cofundador, Maltiverse

decidimos tener una opción de pago que nos ayudara a seguir desarrollando".

Se empezaron a definir servicios, aunque "muchas veces eran los mismo clientes quienes definían los servicios que querían, como el integrar la información de Maltiverse en un firewall de determinada manera, de integrarlo en un ordenador para poder hacer consultas… El hobby de Hesaul Sánchez y Antonio Gómez Martín, co-fundadores de Maltiverse estaba solucionando un problema que existía en el mercado, un problema al que estos profesionales se enfrentaban en su quehacer diario: no tener una base de datos centralizada con toda la información de los ataques.

Explica Hesaul Sánchez que cada vez que se identificaba un ataque, había que investigar con qué estaba relacionado, mirando en un montón de fuentes, y todo ese conocimiento adquirido no se estaba aprovechando para distribuirlo al resto de miembros del equipo. Con Maltiverse "podemos tener centralizada la información y la podemos compartir y distribuir. Ahora tenemos una comunidad de 70 equipos de investigadores que suben indicadores a la plataforma enriqueciendo el sistema". Añade que también las búsquedas, que ya suman más

Respaldo de la industria

Maltiverse nació hace algo más de tres años gracias al esfuerzo de Hesaul Sánchez, y Antonio Gómez Martín, quienes actualmente ocupan los cargos de CEO y CPO respectivamente.

Socios en el proyecto son David Gil y Jorge López Zarza, quien es el responsable de la plataforma.

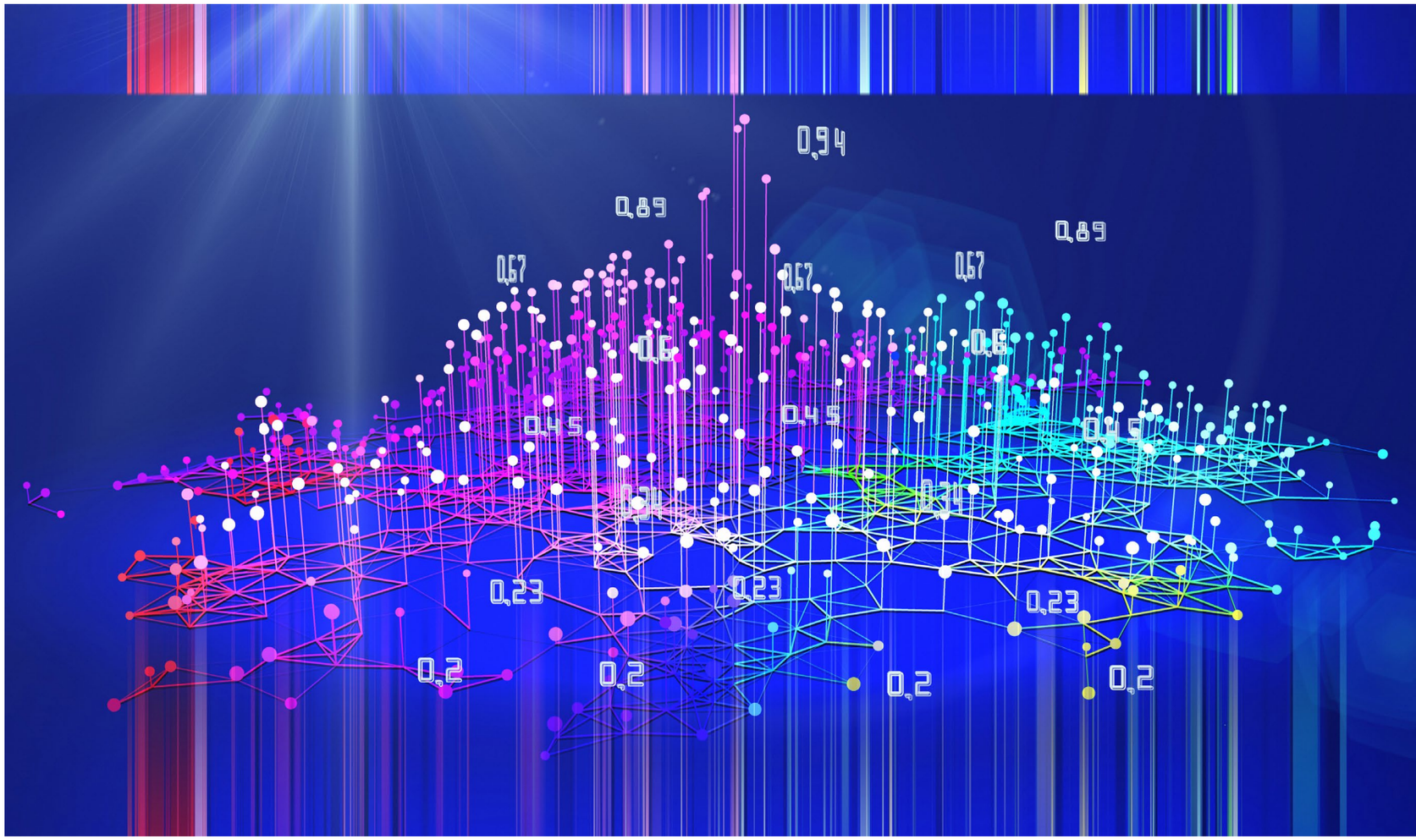
Una de las últimas incorporaciones al accionariado es Pedro Tortosa, quien, como fundador y CEO de Peak Thomas, se define como ingeniero, inversionista, emprendedor y evangelista tecnológico con experiencia en la creación y liderazgo de nuevas empresas tecnológicas desde cero y su crecimiento hasta lograr una tracción efectiva en el mercado.

También recientemente se ha incorporado al accionariado Pedro Gálatas, un ejecutivo con más de 25 años de experiencia que además es el fundador, CEO, consejero/asesor independiente y EVP en empresas y organizaciones sin fines de lucro que operan en todo el mundo.

Ovane Mikhaylov, otro gran conocido, está a cargo, desde hace unos meses, del desarrollo de negocio internacional.

Marc Legido, CTO de la compañía, y Joaquín Ramos, son también parte de Maltiverse, una empresa española que compite con Recorded Future y Anomali. Hasta ser comprada por Insight Partner en mayo de 2019 por 780 millones de dólares, Recorded Future había recaudado casi 58 millones de dólares en seis rondas de financiación. En cuanto a Anomali, desde su fundación en 2013 la compañía ha recaudado 96,3 millones de dólares en seis rondas de financiación, según datos de Crunchbase.

Maltiverse cuenta con una comunidad de 70 equipos de investigadores que suben indicadores a la plataforma, enriqueciendo el sistema



de cuatro millones, enriquecen, “porque si alguien está buscando un indicador y nosotros no lo tenemos categorizado, automáticamente lo guardamos como sospechoso y lanzamos una serie de procesos en background para intentar identificar cómo de malo puede ser y categorizarlo, por lo que tenemos información viva y dinámica”.

Con mucha experiencia en el mercado de respuesta ante incidentes asegura Hesaul Sánchez que, en la práctica, el 98% de los ataques son predecibles, y teniendo los indicadores de compromiso cargados correctamente te puedes proteger contra ellos de una manera sencilla. Reconoce que Maltiverse ayuda cuando ya se tiene un cierto grado de madurez, “porque no podemos aportar mucho a un cliente que no tenga un SIEM”, por ejemplo, y que los principales clientes de la plataforma son los MSSP.

A los clientes se les trata con un extremo cuidado, configurando la plataforma “en función de tu contexto, tu geografía, tu necesidades, en qué dispositivo vamos a integrarlo… Nosotros ayudamos a perfilar muy bien cuáles son los datos más relevantes para el dispositivo concreto de ese cliente; si es un dispositivo perimetral tiene cierto sentido tener cierta información y en un endpoint son otro tipo de indicadores los que tienen más sentido”.

“Lo nuestro va de trabajar muy poco, que todo sea automático”, asegura Hesaul Sánchez añadiendo que los que trabajan en Maltiverse vienen de hacer frente a situaciones con 50 incidentes al mismo tiempo y no saber por dónde empezar; “nosotros intentamos poner luz en saber qué es lo más crítico y lo más relevante”.

Modelo de negocio

Hay varias opciones de consumo de Maltiverse. El plan Community, gratuito, te permite hacer poco más que cien consultas diarias. Hay una modalidad Lite, de pago, en la que “nosotros hacemos búsquedas, selecciones muy concretas de la información

relevante para el cliente y que pueda integrarlo automáticamente su dispositivo". Por otra parte, si se quiere ir más allá hay un modo Enterprise.

La mayor parte del negocio de Maltiverse se genera fuera de España, donde además entienden la oferta mucho más rápido. Estados Unidos, China, India, Latinoamérica, norte de Europa son mercados en los que la compañía se mueve con ligereza. En cuanto a los verticales, se trabaja mucho con el de banca, sector farmacéutico e industria.

¿Cuál es el mensaje que quieres lanzar al mercado? "Aprovechemos la información que hay; no gastéis esfuerzos en lo que ya hemos hecho nosotros; dadnos feedback para seguir mejorando y que tengamos algo muy bueno", responde el directivo recordando que llevan cuatro años con este proyecto en el que ya trabajan unas diez personas.

Enlaces de interés...

- Muy pocas empresas aprovechan las ventajas de la Inteligencia ante Ciberamenazas
- W 2021 SANS Cyber Threat Intelligence Survey

En los últimos años se ha constatado que las campañas de malware tienen una vida útil cada vez más corta

Compartir en RRSS

Bitdefender®

BUILT FOR RESILIENCE

Protegemos tu negocio
Protegemos a tus clientes

- eXtended Endpoint Detection and Response (XEDR)
- Managed Detection and Response (MDR)
- Cloud Workload Security (CWS)

www.bitdefender.es/business

Akamai Cybersecurity Summit

Akamai propone ZTNA y microsegmentación como la nueva aproximación a la ciberseguridad

Hay una ciberguerra y nuestra misión es mantener a las empresas y los usuarios a salvo de los ciberataques. Lo decía el Dr. Tom Leighton, CEO y cofundador de Akamai, durante un evento celebrado de manera simultánea en varias ciudades europeas con responsables locales pero que conectaba en directo con Londres, donde se encontraba Leighton.

El Akamai Cybersecurity Summit servía para hablar de la situación a la que se enfrenta el mercado, de tendencias y de propuestas. Explicaba Leighton que la oferta de la compañía en materia de ciberseguridad se organizaba en tres categorías, la primera es la Seguridad de la Infraestructura para hacer frente a los ataques DDoS y contra el DNS; “muchos de los grandes colapsos en Internet han sido el resultado de situaciones o ataques de DNS”, recordaba el Dr. Tom Leighton.

Un gráfico mostraba cómo hay un incremento de los ataques de DDoS, en número e intensidad, en los últimos años. No es una sorpresa, apuntaba el

"Cuando surge una vulnerabilidad el parcheo de la misma no es el problema, sino encontrar todas las instancias del software vulnerable"

Dr. Tom Leighton, CEO y cofundador, Akamai

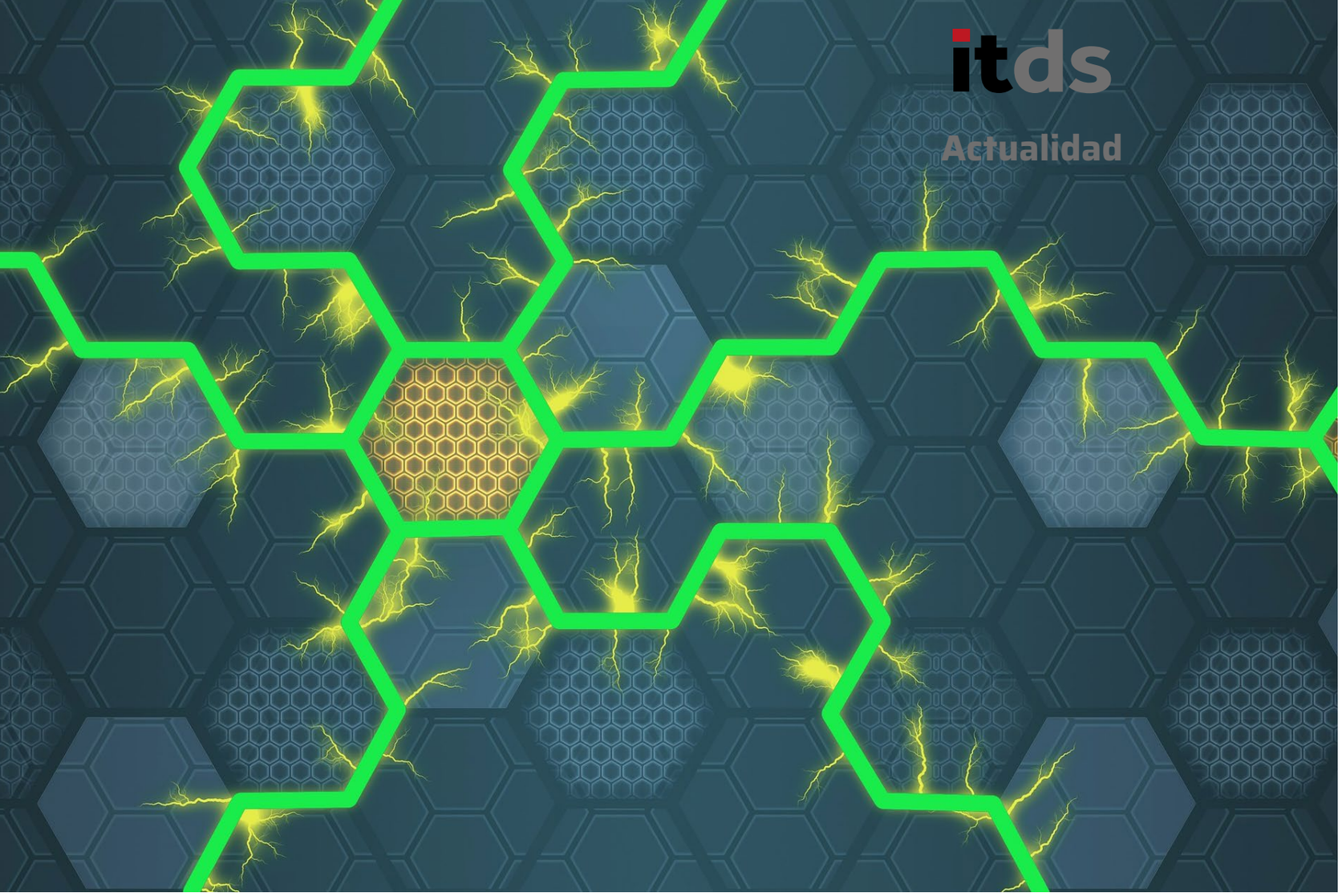
CEO de Akamai, que “últimamente se vean grandes ataques contra empresas de servicios financieros”, para después comentar que en Europa los ataques DDoS se han triplicado en el primer trimestre y que durante el periodo “es la primer vez que hemos visto peores ataques en EMEA que en Norteamérica”.

Mencionaba también el directivo cómo muchas empresas están recibiendo amenazas de sufrir ataques DDoS a menos que se pague un rescate, nada menos que 20 bitcoins; “tenemos muchos clientes que reciben cartas como esta y se lo toman muy en serio. Y aquí es donde tenemos capacidades que pueden evitar que tengas que pagar 20 bitcoins y mantenerte a salvo cuando lanzan los ataques”, aseguraba el Dr. Tom Leighton.

Junto a la Seguridad de las Infraestructuras, mencionaba el directivo la Seguridad de las Aplicaciones y las API como la segunda categoría en la que se organiza la oferta de ciberseguridad de la compañía. Los ataques contra aplicaciones y APIS se han disparado, decía el directivo, añadiendo que “la base para la protección de aplicaciones y API es un firewall de aplicaciones web, o WAF”, un área en la que la compañía ha realizado una gran inversión y que puede suponer “una gran diferencia”. Mencionando ataques a la cadena de suministro como Log4G, aseguraba el directivo que cuando surge una vulnerabilidad el parcheo de la misma no es el problema, sino “encontrar todas las instancias del software vulnerable. Y tener el firewall de Akamai actualizado con las reglas significa que puedes dejar de ser vulnerable en menos tiempo”. Definía el CEO de Akamai este problema como uno de los tendones de Aquiles de Internet porque “todos usamos código de terceros, código de fuente abierta que no está bien mantenido y ni siquiera sabes que lo tienes. Los malos están encontrando vulnerabilidades en él y explotándolo, y eso hace que sea difícil de defender”.

La guerra de los Bots

“No todos los bots son malos”, aseguraba durante su intervención Tom Leighton, al tiempo que aseguraba que su gestión, junto con la protección de las cuentas de usuario son un problema. Hay muchos tipos de bots, y aunque la



"Muchos de los grandes colapsos en Internet han sido el resultado de situaciones o ataques de DNS"

Dr. Tom Leighton, CEO y cofundador, Akamai

primera reacción sea la de bloquearlos a todos, "dependiendo del tipo de bot necesitas responder frente a él de manera diferente". Se ha llegado a un punto en el que los gestores de bots son tan buenos que los ciberdelincuentes están contratando humanos para probar credenciales robadas "porque si es un bot, lo sabemos y no lo dejamos entrar; y si es un humano, debemos verificar si es el humano correcto". La solución es Account Protector que, obviamente, es muy importante en los sitios de comercio electrónico y banca.

Habló también el cofundador de Akamai de los scripts para presentar una herramienta, inventada en Londres por uno de los empleados de la compañía, que está diseñada para mostrar lo que está pasando en la página web de una empresa y evitar la inyección de código malicioso. Page Integrity Manager, que es como se llama la solución, es clave si tenemos en cuenta que el estándar PCI fue modificado hace unos meses y exige contar con un método que verifique todos los scripts de terceros para asegurarse de que no estén haciendo nada malicioso. "Page Integrity Manager verifica y funciona al hacer que insertemos nuestro propio script a medida que entregamos la página al navegador. Nuestro script está mirando lo que están haciendo todos los otros scripts. Y si ve uno de los otros scripts accediendo a lo que nos parece una tarjeta de crédito, eso no es bueno y lo bloqueamos", explicaba el Dr. Tom Leighton

Microsegmentación

La tercer área en la que Akamai tiene soluciones de seguridad tiene que ver con la protección de las aplicaciones empresariales y datos. Empezaba señalando el CEO de Akamai que las soluciones tradicionales para la seguridad empresarial no están evitando que los ciberdelincuentes hagan un montón de daño y que se necesita una aproximación diferente; "necesitas la arquitectura Zero Trust y una red perimetral real como primera línea de defensa", aseguraba, añadiendo que la micro segmentación se ha convertido en un elemento de defensa dentro

"La microsegmentación se convierte en algo crítico para los permisos de confianza cero"

Pavel Gurvich, co-founder, de Guardicore

de las organizaciones y dando paso a Pavel Gurvich, co-founder de Guardicore, la compañía que Akamai compró en septiembre del año pasado por 600 millones de dólares.

Pavel Gurvich empezó su intervención hablando de brechas de seguridad, cada vez más numerosas, y cómo un 25% de las mismas tiene como origen un empleado o partner de confianza; recordó además cómo se han detectado grupos de ciberdelincuentes que detectan empleados a los que pagan para dejarles entrar en las redes empresariales y aplicaciones críticas, desde donde pueden extenderse por toda la organización. Asegurando que es un problema realmente difícil de afrontar, aseguraba Gurvich que el enfoque correcto pasa por ZTNA y microsegmentación; lo primero limita el acceso completo a las redes y recursos, y lo segundo garantiza que cada aplicación está aislada de las demás. De forma que "la microsegmentación se convierte en algo crítico para los permisos de confianza cero". La ventaja de Guardicore, es que supieron simplificar el proceso, hacerlo fácil e "introdujimos una capacidad de visibilidad muy fuerte" que permite ver cómo se comporta una red, cómo se comunican las aplicaciones entre sí, cómo hablan los usuarios con estas aplicaciones y qué sucede realmente.

La solución de Guardicore, "funciona en todos los sistemas operativos. Se ejecuta en casi cualquier entorno de nube y, debido a que tenemos esta visibilidad en la red, también podemos mirar e identificar si algo malo está pasando aquí". Destacaba también Pavel Gurvich que la identidad también es fundamental, "así que aquí tenemos una solución MFA que se implementa sin ningún hardware. Y además tenemos un servicio de centro de amenazas avanzado que monitoriza la combinación de algoritmos y personas de la red que pueden identificar muy rápidamente una brecha".

Enlaces de interés...

- 'Guardicore es una empresa dedicada principalmente a proteger internamente el datacenter' (Domingo Téllez)
- Akamai compra Guardicore, una compañía experta en microsegmentación

Compartir en RRSS

STORMSHIELD

La opción europea en ciberseguridad

El partner de confianza
para
securizar sus
infraestructuras operacionales y sensibles

www.stormshield.com

Fuente RRPP

‘La inspección de tráfico de red en tiempo real es fundamental’

(Jesús M. Doña, EMASA)

Asegura que sin el SOC no podría vivir; que tener un buen corazón, capaz de aguantar emociones fuertes, es una de las necesidades de un CISO, además de tener tiempo y capacidad de análisis; que la inteligencia artificial está funcionando muy bien en la generación de ransomware y ataques vía phishing, y que la concienciación del usuario es algo que está en el ADN del EMASA, donde ejerce como responsable deinfraestructura, soporte y ciberseguridad en el Departamento IT. Hablamos con Jesús M. Doña.

Rosalía Arroyo

Jesus M. Doña Fernández es el Responsable de infraestructuras, soporte y ciberseguridad del Departamento de Tecnologías de la Información de EMASA, Empresa Municipal Agua de Málaga. Nos cuenta que llega al mundo de la seguridad “como una evolución natural dentro de la responsabilidad en la administración de sistemas”. Inicia el camino en el Servicio Andaluz de Salud, como responsable provincial de sistemas, “donde la preocupación inicial es que todo funcione. Y llega un momento en el que te das cuenta de que de nada sierve toda la infraestructura que estás montando si no tienes en cuenta la seguridad”. Añade que a partir de ahí se va tomando conciencia y que hay que darle un giro a la situación, tanto a nivel de formación como a nivel de responsabilidades, “y te estoy hablando

de hace 15-20 años, cuando aún no se hablaba del CISO; fue entonces cuando los que trabajábamos en administración de sistemas empezamos a preocuparnos por la seguridad".

Se empezó pensando en la disponibilidad, "en contar con un sistema que fuera tolerante a fallos; luego en la recuperación ante desastres, y en las copias de seguridad. Pero empiezan a surgir eventos que generar interrupciones de servicio y ya se habla de la seguridad como protagonista. Y esa necesidad a mí me cautivó". Así se introdujo en el mundo de la seguridad este Doctor Ingeniero en Informática con más de 20 años de experiencia en el sector TI que además tiene tiempo para la investigación en Inteligencia Artificial, Sistemas de Apoyo a la Decisión, Ciberseguridad y BigData, junto con docencia universitaria a través de la UNED.

Preguntamos a Jesús M. Doña si el CISO, después de una evolución que en muchos casos ha llevado a que su voz sea escuchada en los consejos de dirección, tiene el peso que debe tener dentro de las compañías. "Yo te diría rotundamente que no. Básicamente porque la seguridad sí tiene peso generalmente dentro de las empresas, pero la ciberseguridad como tal está todavía muy alejada de la alta dirección, y cuando no eres consciente de que la ciberseguridad te puede parar el negocio, no das importancia a la figura que la gestiona". Opina el Responsable de Infraestructuras, soporte y ciberseguridad de EMASA que, en España, y a nivel de Administración Pública falta hacer crecer, e incluso al definir la figura del CISO".

"La elección de un sistema es por benchmark que puedas encontrar, experiencia previa de otros usuarios que te hablan de la herramienta y por POCs"

Uniendo TI y TO

Hablando de los retos de ciberseguridad a los que se enfrenta Jesús M. Doña, responde que el mayor es la concienciación de la organización en lo que se refiere a la ciberseguridad. Explica que el CISO de EMASA está muy vinculado al Departamento de Tecnologías de Información, "con lo cual nosotros somos rápidos ejecutores de las necesidades que parten de la ciberseguridad, pero en lo que es la organización todavía es complicado crear esa

"Puedes tener todas las tecnologías que quieras, si un usuario pincha un USB que ha traído de su casa o te deshabilita el antivirus, ya ha acabado contigo"

Fuente RRPP

conciencia de ciberseguridad; el que sean capaces de tomar en cuenta la ciberseguridad como punto clave que no puede faltar en ningún proyecto".

Destaca el responsable que en la compañía se está apostando porque la tecnología de la operación adquiera la madurez en ciberseguridad que tiene el equipo de TI. Explica que, sobre todo en industria, la parte de TI suele estar muy concienciada y trabajando mucho en ciberseguridad mientras que a la parte de TO, de Tecnologías de la Operación, que además suele ser generalmente el core del negocio, les cuesta más centrarse en ciberseguridad, "y ahora estamos trabajando mucho en equiparar lo que son los sistemas de TO en ciberseguridad a los sistemas de TI, y vamos consiguiendo que haya una sinergia a partir de la ciberseguridad, que es algo que nos compete a todos. Estamos consiguiendo resultados muy interesante, ya no solo a título de proyecto que podemos realizar, sino a colaboraciones, formación o compartición de intereses a la hora de implantar tecnologías".

Ser responsable de ciberseguridad día a día

¿Qué cualidades debe tener un buen CISO? "Debe tener buen corazón. Y no me refiero a que sea buena persona, sino a que sea capaz de aguantar emociones fuertes, porque el CISO es una responsabilidad que la llevas 24/7", responde Jesús M. Doña. Añade que el tema de la ciberseguridad no entiende de jornadas, no entiende los festivos, y te involucra a todos en todo momento; "siempre está preocupado y es importante el poder hacer una gestión del estrés grande".

Además de tener el corazón en forma, añade el responsable de EMASA que un buen CISO también debe tener la capacidad de dedicar tiempo "a analizar cosas: analizar la tecnología, analizar los riesgos, poder estar continuamente bebiendo de fuentes de información para no solo saber lo que está pasando en el día a día, sino el conocer tendencias… ser muy esponja". Añade: "Te tiene que

gustar. Si no te gusta la ciberseguridad no puedes ser CISO".

¿De dónde sacáis esa información? "Nosotros tenemos varias fuentes que son muy interesantes. Nos llega mucha información a través de CCN-CERT; también tenemos mucha información de Seguridad Digital de Andalucía; de INCIBE; Foros especializados y, a través de distintos proveedores de ciberseguridad estamos asociados a la serie de boletines".

Sobre los servicios de seguridad gestionados, que es hacia donde se está dirigiendo el mercado, asegura Jesús el responsable ciberseguridad de EMASA que "han venido para quedarse", y una de las razones es porque las empresas no tienen capacidad económica ni humana para generar lo que se necesita en ciberseguridad. Por otra parte, hay que tener en cuenta, los servicios gestionados son rentables porque dan servicio a varios clientes, lo que hace que "el servicio no sea todo lo todo lo personal o directo que te gustaría".

Tecnologías imprescindibles

Preguntado por las tecnologías de seguridad que considera imprescindibles, asegura que sin el SOC no podría vivir; "a mí me quitas el SOC y me quitas una herramienta clave para el funcionamiento de la ciberseguridad. Y es una herramienta que no puedo suplir con personal mío".

El antivirus en el puesto de trabajo es una de las tecnologías que Jesús M. Doña considera imprescindibles. Habla de un "muy buen antivirus que sea capaz de cortar antes de que ocurra la acción".
Por concretar preguntamos si se refiere a antivirus o al EDR, la respuesta no deja dudas: "Ahora el antivirus es el EDR. Ya no se concibe un antivirus como tal si no tiene su módulo de inteligencia

"El ransomware es una amenaza muy peligrosa porque te puede hacer muchísimo daño, pero al mismo tiempo te entra por lo más simple"

Fuente RRPP

artificial", apunta, añadiendo que la analítica del tráfico de red también se ha convertido en algo esencial.

Sobre las nuevas tendencias del mercado que llegan imparables, como SASE, Zero Trust, SSE, Cybersecurity Mesh, que en ocasiones llegan rodeadas de marketing, dice que es habitual tener reuniones y realizar auditorías de calidad periódicas para conocer más cosas. Menciona el Zero Trust más como un objetivo que como una realidad y nos cuenta que uno de los aspectos que se están revisando son los accesos adoptando la política de menor privilegio.

¿Todo es tecnología? ¿Qué papel juega la concienciación del empleado? la respuesta es clara: "puedes tener todas las tecnologías que quieras, si un usuario pincha un USB que ha traído de su casa o te deshabilita el antivirus, ya ha acabado contigo". Por eso la concienciación del usuario es algo que está en el ADN del EMASA, donde se realizan campañas de phishing dirigidas a toda la organización, además de compartirse noticias para fomentar la cultura de seguridad.

El balance de estas campañas de concienciación en bueno. Entre otras cosas, se han multiplicado las incidencias de usuarios que avisan de correos sospechosos, "y eso antes era impensable. Hemos conseguido que un porcentaje muy grande de la organización tenga ya una conciencia de ciberseguridad importante".

Mencionamos la Inteligencia Artificial como una de las tecnologías que serán imprescindibles en el futuro. Como gran experto, ya que es Doctor en Informática especializado en Inteligencia Artificial, nos asegura Jesús M. Doña que todas las IA son inteligentes realmente, pero que "hay sistemas que dicen que tienen inteligencia artificial y no la tienen". Advierte además que en lo que ahora mismo está funcionando muy bien la IA "es en la generación de ransomware y ataques vía phishing". Teniendo en cuenta que la respuesta frente a esos ataques también tiene que integrar inteligencia y que tratamos con un experto, ¿llegas a escoger una solución de seguridad en función de cuán inteligente es? "No. Al final la elección de un sistema es por benchmark que puedas encontrar, experiencia previa de otros usuarios que te hablan de la herramienta y por POCs".

Fuente
RRPP

"Cuando no eres consciente de que la ciberseguridad te puede parar el negocio, no das importancia a la figura que la gestiona"

Entre las tecnologías de seguridad que serán necesarias en el futuro la primera que menciona Jesús M. Doña es "la inspección de tráfico en tiempo real" Dice que es una tecnología que se utiliza mucho, sobre todo en los entornos de Tecnologías de la Operación ante la dificulta de poner agentes en los puntos finales "y lo que se hace es analizar continuamente el tráfico de red que se produce y si encuentran patrones de tráfico de red que coinciden con lo que sería un tráfico de un malware, por ejemplo, aíslan ese elemento de la red. Esto no te impide la infección, pero sí la transmisión de la infección".

La segunda tecnología que menciona es la gestión y seguridad de los accesos a los entornos, ya sean en nube o en local para evitar el acceso no deseado.

Explica el responsable de ciberseguridad de EMASA que está muy interesado "con el análisis de tráfico, de red, el uso de IRM (Information Rights Management), DLP, control de cuentas privilegiadas (PAM)… Todo este análisis hay que hacerlo para evitar los ataques dirigidos. Yo al que más temo es el ataque dirigido".

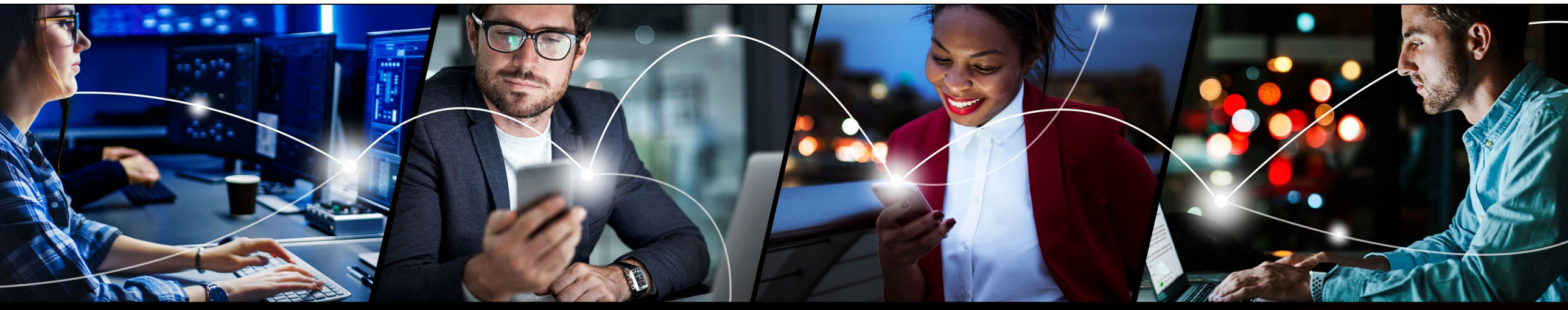
Y ya que hablamos de ataques, ¿el ransomware es tan indetectable, imparable y súper sofisticado o es que las empresas están mal preparadas? "El ransomware es una amenaza muy peligrosa porque te puede hacer muchísimo daño, pero al mismo tiempo te entra por lo más simple, que es hacer doble clic en un enlace; hay una interacción por parte del usuario que con concienciación y elementos de IA que detectan que están cifrando pueden parar rápidamente la amenaza", responde Jesús M. Doña, insistiendo en que lo que más le preocupa es un ataque dirigido que entra en tu sistema porque está analizando por dónde puede entrarte y no es un correo electrónico sino que está atacando la vulnerabilidad de los servicios expuestos en internet y que una vez que entran se quedan en el sistema y hacen lo que quieren.

Enlaces de interés...

- 'La seguridad se convertirá en una ventaja competitiva de las empresas' (Pablo Masaguer, CISO, Sociedad Textil Lonia)
- 'Lo importante, y más en el ámbito de la seguridad, no es tanto la solución o producto que vayas a seleccionar, sino el proveedor' (Roberto González, Grupo Primavera)
- "Resisten los que se adaptan" (Belén Pérez, CISO, Grupo Nueva Pescanova)
- 'Identificar los roles críticos en la organización, que no necesariamente son los del comité de dirección, es fundamental' (Gabriel Moliné, Leroy Merlín)
- 'En los próximos años la tendencia en ciberseguridad será el análisis de comportamiento' (Mario Andrés, Mercadona)

Compartir en RRSS

Seguridad unificada para un mundo RECONECTADO



SEGURIDAD DE RED

AUTENTICACIÓN MULTIFACTOR

NUBE SEGURA WI-FI

SEGURIDAD ENDPOINT

Unified Security Platform™

CLARIDAD Y CONTROL | **SEGURIDAD INTEGRAL** | **CONOCIMIENTO COMPARTIDO** | **ALINEACIÓN OPERATIVA** | **AUTOMATIZACIÓN**

Contacto: +34 917 932 531

Email: spain@watchguard.com

www.watchguard.com

‘Tecnológicamente hablando es un momento realmente emocionante’

(Iker del Fresno, Aruba)

La evolución e innovación de una compañía que este año cumple 20 en el mercado queda reflejada en conceptos que han ido apareciendo en el mercado bautizados por consultoras de renombre. Hablamos con Iker del Fresno, country Manager de Aruba para España Y Portugal, quien, entre otras muchas cosas, asegura que no hay que hablar tanto de la explosión del IoT, sino darle sentido.

Rosalía Arroyo

Con una trayectoria de más de 18 años en el ámbito TI, Iker del Fresno se unió a Aruba en 2016 para liderar el negocio de la compañía en el norte de España. En 2019 fue nombrado director de ventas para España, puesto que ha ocupado hasta su nombramiento como country manager de la compañía en España y Portugal hace algo más de seis meses. “Todo lo que me planteé de cara a este fiscal year 2022, que en nuestro

"Somos el fabricante con mayor número de sedes SD-WAN conectadas en España"

caso empieza en noviembre y que es cuando empecé yo, ha sido posible realizarlo gracias a que ya había unas buenas bases", dice Iker del Fresno cuando le pedimos que haga balance del tiempo que lleva liderando la compañía en nuestro país. Entre los retos, la transformación del canal hacia un modelo de servicios gestionados apoyado por nuevas incorporaciones al departamento de canal, que ha permitido "transformar el negocio, el servicio gestionado que queremos, que ya funciona muy bien".

"Es un momento realmente emocionante tecnológicamente hablando", responde Iker del Fresno cuando preguntamos por la situación del mercado. Habla de una trasformación tremenda, primero porque la situación post pandemia ha acelerado que se acabe el perímetro como tal, por la flexibilidad en el trabajo, la explosión de soluciones en software-as-a-service, así como la explosión del cloud… "todo esto es disrruptivo para los responsables de IT, que tienen más herramientas para mejorar su negocio, pero también tienen un montón de riesgos".

Añade el directivo de Aruba que si a toda la explosión del Cloud y de IoT, y la parte de seguridad que necesitas en ese contexto "le añades cómo utilizo el Big Data y la Inteligencia Artificial con toda la información que soy capaz de recoger para que mejore mi proceso, el reto que tiene el responsable de IT es apasionante".

Desde Aruba lo tienen claro, asegura Iker del Fresno, explicando que lo que propone la compañía es una plataforma unificada para poder gestionar el IoT, las soluciones SaaS, la conectividad, la seguridad "y que sea capaz de automatizar procesos para reducir aquellas tareas más repetitivas y con menos valor para centrarse en la gestión del proyecto y de cómo mejorar su poder productivo, flexibilizando el modelo de consumo para que la gente pueda seguir

"Edge to Cloud es la historia de Aruba desde 2002"

invirtiendo en tecnología en un modelo de servicio y pago por uso que les permita ser ágiles en esa transición".

SASE

Conocida inicialmente como Aruba Wireless Networks, Aruba Networks es una empresa que nace proporcionando servicios de acceso a red. La evolución de la compañía ha hecho que además de catalogarla como una empresa de redes, también se la considere como una empresa de seguridad. Tengamos en cuenta que modelos como SASE (Secure Acces Service Edge) están validando esta evolución. Le preguntamos a Iker del Fresno qué pesa más en las cuentas de la compañía, si la oferta de redes o la de seguridad. "No existe seguridad sin red ni red sin seguridad", responde, añadiendo que no es un mensaje novedoso que se lance ahora.

Aruba cumple 20 años. Nació en 2002 "con el Wireless como bandera, cuando no había tantos dispositivos en movilidad, y en 2004 la compañía ya tenía un firewall de Capa 7 embebido en la

it whitepapers

LA SEGURIDAD
EN LA NUEVA ERA DE SD-WAN

Considerado como un elemento clave en cualquier proceso de transformación digital, SD-WAN mejora el rendimiento de las aplicaciones empresariales, optimizando la experiencia de usuario y simplificando las operaciones; todo ello de la mano de nuevos modelos de consumo como SaaS o NaaS.

No hay que hablar tanto de la explosión del Iot sino darle sentido a ese

solución, con lo cual ya entendía perfectamente la necesidad de la seguridad en la red. Pero es que, además, ClearPass, que es la solución de pre y post autenticación de Aruba, es una solución de Zero Trust que llegó en 2010, hace doce años, lo que nos convierte en líderes del mercado en el control de acceso a la red".

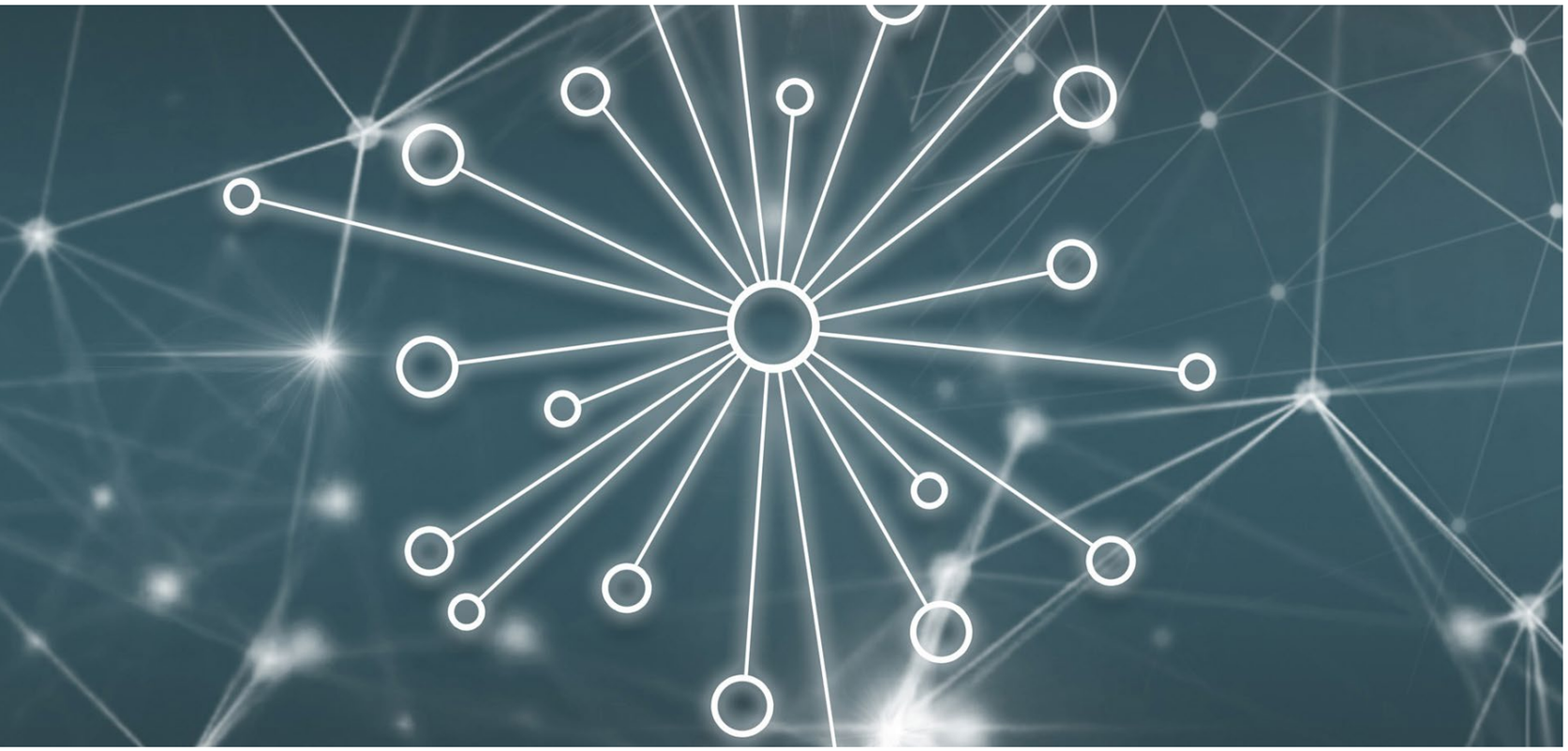
Añade además que Aruba lanzó los primeros switches en los que podías llevar el firewall de capa 7 a cada uno de los puertos hace diez años, para terminar comentando que el modelo SASE "ha venido a recoger el éxito de la innovación de Aruba. Y esto es algo fantástico".

Sobre SSE, convertido en la evolución de SASE, dice Iker del Fresno que viene a reflejar quién es el mejor en cada parte, "y nosotros tenemos una alianza con aquellos que son los mejores en la parte de Cloud Security", proponiendo una solución que permita gestionarlo todo, con la heterogeneidad de fabricantes que cada empresa decida que son los mejores.

SD-WAN

El primer punto de crecimiento de la compañía es SD-WAN, nos confirma Iker del Fresno. La tecnología, de la que se lleva hablando desde hace más de cuatro años "acaba de explotar en el mercado, así que hemos vivido un final de 2021 y un principio de 2022 con un montón de proyectos de SD-WAN. Nuestra estrategia de SD-WAN Fabric está funcionando muy bien y somos el fabricante con mayor número de sedes SD-WAN conectadas en España, con mucha diferencia".

Respecto al cliente tipo de una propuesta de SD-WAN, nos cuenta Iker del Fresno que cuando se comenzó hace cuatro años a hablar de esta tecnología, Aruba optó por hablar de SD-Branch "entendiendo que el primer interesado, donde más iba a triunfar el negocio eran en negocios masivos y distribuidos". El retail, que es el ejemplo perfecto, se iba a convertir en el motor que impulsara esa transformación, "y efectivamente, en los primeros años fue así. Pero ahora ha habido un cambio, de tal manera que tenemos proyectos de seis sedes unidas por SD-WAN".



ClearPass, que es la solución de pre y post autenticación de Aruba, es una solución de Zero Trust que llegó en 2010, hace doce años

Explica el directivo de Aruba que el motor del cambio no es exclusivamente un motor económico de reducción de costes del operador, que lo es, sino la oportunidad de automatizar procesos, de reducir personal, de la orquestación desde una única plataforma. “Tenemos soluciones de seis sedes, cuatro, siete… Honestamente cuando empezamos a hablar de SD-WAN hace cuatro años, no me lo esperaba”.

Ahora Aruba SD-WAN tiene referencias en gobiernos autonómicos, ayuntamientos, universidades con seis campus… que han universalizado la solución SD-WAN independientemente del tamaño y el tipo de negocio.

Hablando del papel del Service Provider, del operador, en la expansión de SD-WAN, o en la ralentización de su adopción teniendo en cuenta que la tecnología impactaba en su cuenta de resultados, dice Iker del Fresno que es habitual que haya una resistencia a la transformación, pero que el negocio de SD-WAN también ha provocado una transformación en el negocio del Service Provider, “de entender que el negocio tradicional había cambiado y que ellos tenían que incorporar el SD-WAN como una oferta de servicios gestionados dentro de su propuesta. Lo que hemos hecho es enriquecer las propuestas a los clientes”. El mercado se ha vuelto a impulsar cuando el operador ha incorporado dentro de su oferta el SD-WAN definido por software.

Estrategia Edge to Cloud

Preguntamos también a Iker del Fresno por la estrategia Edge to Cloud de Aruba. Lo primero que nos dice es que una vez más, las consultoras recogen la visión e innovación de la compañía ante una situación en la que la conectividad en el extremo crece brutalmente.

“Edge to Cloud es la historia de Aruba desde 2002”, asegura Iker del Fresno, explicando que todo empieza en el Edge, a media que se conecta, genera tráfico, genera datos, algunos de los cuales se procesan en local y otros en la nube… Edge to cloud, añade, “define muy bien las necesidades de cualquier cliente, de cualquier empresa española”; una empresa que no tiene por qué ser grande, aunque la mayor parte del negocio de Aruba esté en el segmento Enterprise.

"Los responsable de IT tienen más herramientas para mejorar su negocio, pero también tienen un montón de riesgos"

Diferencial

Sobre el valor diferencial del Aruba destaca en primer lugar Iker del Fresno el ser "un refugio de soluciones de seguridad y comunicaciones desde el año 2002". Añade la capacidad que ha tenido la compañía de flexibilizar el modelo de consumo, que permite acercar "la tecnología de alto nivel a cualquier cliente, desde más pequeño hasta más grande".

No se olvida de mencionar la capacidad "de tener una gestión unificada de toda la tecnología que decidas implementar en tu empresa. Que sea la misma plataforma de Aruba la que te orqueste todo, y no sólo lo de Aruba".

Y, por último, "sin duda la capacidad de reducir tiempos de trabajo recurrentes" y la capacidad de las soluciones "de autorregularse o autocorregirse".

IoT

La proliferación del IoT es innegable. Se ha dejado de hablar de cifras, pero cada vez hay más dispositivos conectados, cada vez son más inteligentes y procesan en el extremo, una realidad que no hace sino refrendar la estrategia Edge to Cloud de Aruba; "en ese Edge debes tener securización del puerto, securización de los accesos, ese Zero Trust y ese perfilado avanzado de quién se está conectando, además de ese scoring del endpoint antes de que se conecte".

Asegura también el directivo que ya no hay que hablar tanto de la explosión del Iot sino del para qué tanto IoT, darle sentido a esto. "Estamos viendo un montón de proyectos relativos al Smart buildings", asegura Iker del Fresno, explicando que algunos buscan una mejora de la experiencia, y es donde entran las soluciones con tags y beacons de la compañía que explotan la información y ayudan a las empresas a mejorar esa experiencia; y también otro tipo de empresas que explotan el IoT para una mejora interna porque "en esta vuelta paulatina de los empleados a las oficinas, buscan cómo reducir consumos a través de la sensorización, hasta que los empleados tengan una concepción clara de cuáles son espacios que están ocupados y cuales no, de qué manera que puede utilizar diferente la oficina".

Enlaces de interés...

- Iker del Fresno, nuevo Country Manager de Aruba en España
- 'NaaS es una tendencia muy sólida para los próximos dos años' (José Tormo, Aruba) - 15 MAR 2022

Compartir en RRSS

aruba
a Hewlett Packard
Enterprise company

LLEVE LA SEGURIDAD AL EDGE

Proteja su entorno de trabajo híbrido

‘Los clientes lo tienen difícil a la hora de decidir qué servicios quieren o necesitan’

(Rosa Ortuño, OptimumTIC)

Tiene claro Rosa Ortuño que la figura del CISO no ha evolucionado lo suficiente como para cubrir completamente las necesidades de las organizaciones; que la tecnología siempre debe ir acompañada de unas medidas legales; que los EDRs son herramientas imprescindibles o que los CASB o las soluciones DLP lo serán en el futuro cercano.

Fundada en 2009, OptimumTIC es una empresa de gestión integral de la ciberseguridad que, desde sus inicios, apostó por los servicios transversales, incluyendo aspectos técnicos, organizativos y legales. La compañía ofrece soluciones de calidad adaptadas a las necesidades de cada cliente, acompañándolos en su estrategia de seguridad y en la implementación y gestión de las soluciones más potentes y óptimas del mercado, gracias al partnership de soluciones líderes en ciberseguridad.

"Apostamos por soluciones comprometidas en conseguir solucionar los problemas de ciberseguridad que se plantean en las juntas directivas"

ROSA ORTUÑO:
CEO A OPTIMUMTIC - CIBERSEGURETAT

CLICAR PARA VER EL VÍDEO

Los servicios de la compañía se centran en tres ramas diferenciadas: Ciberseguridad, Systems & Infrastructure y Compliance IT, que se trabajan de manera transversal para establecer la estrategia de ciberseguridad de los clientes. Rosa Ortuño, CEO de OptimumTIC responde a nuestras preguntas.

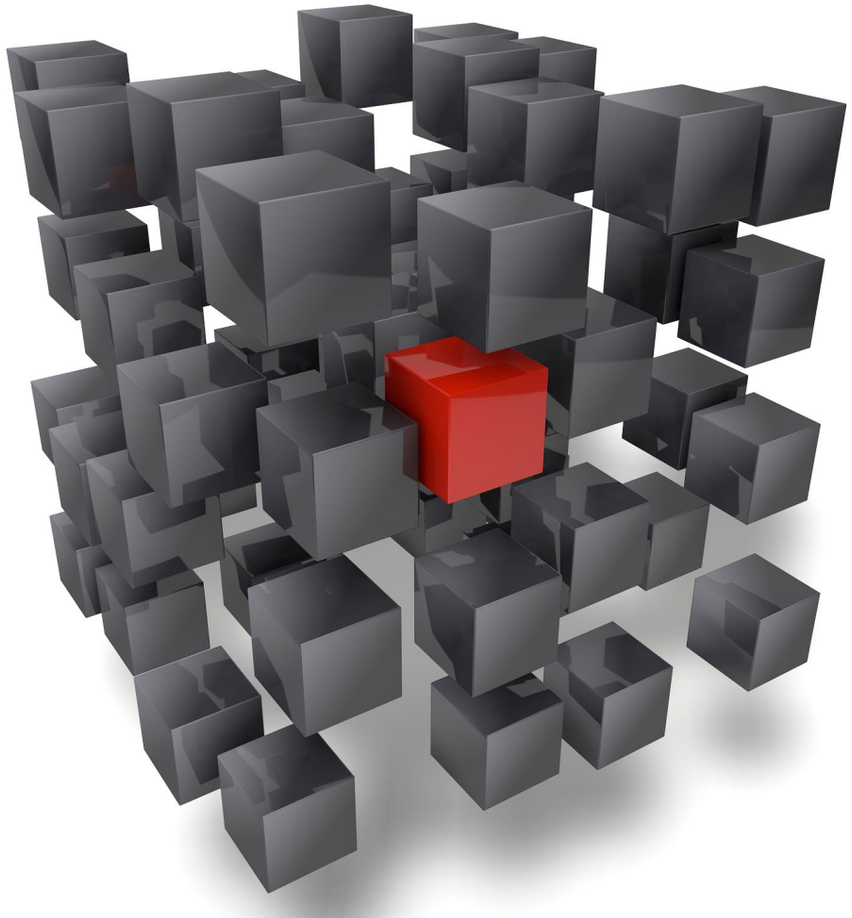
¿Cómo ha evolucionado el mercado de ciberseguridad?

El sector de la ciberseguridad es un mercado que históricamente, siempre ha evolucionado de manera progresiva. OptimumTIC se fundó en 2009, en este momento existía una notable falta de madurez del sector y de las organizaciones en materia de ciberseguridad, esto hizo que el crecimiento de OptimumTIC se produjera de manera progresiva, hasta que, en el año 2020, debido a la pandemia, las organizaciones tuvieron la necesidad de adaptar su metodología de trabajo, revelando así la importancia que tenía y tiene la ciberseguridad, dando un giro de 360 grados al sector y haciendo que como expertos en ciberseguridad creciéramos de manera muy rápida en muy poco tiempo.

Dentro de vuestra oferta, ¿qué servicio está creciendo más?

Actualmente, el servicio que está creciendo más es el acompañamiento y asesoría en certificaciones de seguridad de la información como la ISO 27001. La certificación ISO 27001 es un estándar internacional de Gestión de la Seguridad de la Información y Datos de la organización.

En la actualidad, el cumplimiento con el marco normativo recogido en el Reglamento General de Protección de Datos no es certificable y las empresas muchas veces necesitan demostrar su cumplimiento y buenas prácticas ante proveedores y clientes, contar con certificaciones como la ISO 27001,



"Los trabajadores de las organizaciones son y seguirán siendo una de las vulnerabilidades más importantes"

no sólo aporta un valor añadido a la organización si no que les ayuda a cumplir con los requisitos demandados por terceros.

¿Cómo cree que ha evolucionado la figura del CISO en los últimos años?

Es importante que todas las organizaciones cuenten con una figura interna o externa que vele por la seguridad de la información de la organización. En los últimos años, la figura del CISO ha sido y es un perfil muy dual, donde hemos encontrado tanto CISO con un perfil totalmente técnico como CISO con un perfil normativo y de cumplimiento. En los últimos años la figura del CISO no ha evolucionado lo suficiente como para cubrir completamente las necesidades de las organizaciones, en esta línea, los CISO deberían ir hacia un perfil mucho más híbrido y transversal que plantee los retos de seguridad desde las tres perspectivas en las que se basa la ciberseguridad, las medidas técnicas, organizativas y legales, y es por ello la importancia de tener un asesoramiento externo u oficina de seguridad como realizamos nosotros con varios clientes y empresas.

¿Qué es lo que están demandando los clientes?

Realmente los clientes lo tienen difícil, a la hora de decidir qué servicios quieren o necesitan. El gran abanico de soluciones que existen en el mercado hace que en muchas ocasiones los equipos de seguridad de las organizaciones vayan perdidos y no pongan foco en las verdaderas vulnerabilidades y riesgos de sus sistemas, hay cada vez más oferta y no todos ofrecen ciberseguridad, aunque digan que la ofrecen.

Para poder conocer tus necesidades, o tus puntos débiles, todas las organizaciones deberían comenzar realizando una Auditoría de Seguridad o Análisis de vulnerabilidades y/o Riesgos, con el fin de conocer los puntos débiles de la organización y aprender sobre la situación de los recursos IT, permitiéndoles describir el escenario en el que se encuentra la organización en materia de ciberseguridad e ir creciendo en madurez, la ciberseguridad no es un proyecto cerrado que empiezas y finalizas en un tiempo, sino que es un ciclo de gestión continua y mejorando día a día. De esta manera, mediante el análisis de las vulnerabilidades las organizaciones pueden; conocer el estado de salud de aquello que les identifica, conocer el nivel de seguridad del tráfico y conocer la seguridad de código que es muy importante y no siempre se afronta conforme el riesgo que llega a ser en todas las organizaciones.

En un mercado saturado de fabricantes, soluciones y propuestas, ¿cómo escoger?

Es importante apostar por empresas de ciberseguridad que lleven tiempo en el mercado, que adapten las soluciones y proyectos a las necesidades de cada cliente y que acompañen en la gestión e implementación de estos, basando su trabajo en la mejora continua, tal y como hacemos desde OptimumTIC. Como empresa de gestión de la ciberseguridad no sólo vendemos e implementamos, sino que acompañamos y gestionamos todos los proyectos tanto desde la dirección como desde todo el equipo y siempre bajo las best practices que marca cada fabricante, ya que nos certificamos en todo lo que ofrecemos, y luego nuestra gran trayectoria y experiencia nos hace abordar los proyectos de una forma muy optimizada dando resultados en poco tiempo.

En seguridad, ¿todo es tecnología?
No, la seguridad es transversal y se articula bajo las medidas técnicas, organizativas y legales. Es decir, la tecnología siempre debe ir acompañada de unas medidas legales, que aseguren los máximos estándares de cumplimiento en las normativas de protección de datos vigentes en cada momento, como el Reglamento General de Protección de Datos a nivel europeo y de unas medidas organizativas, que permitan integrar todos los elementos en la estrategia de ciberseguridad bajo los máximos estándares de seguridad de la información.

Algunos de los fabricantes con los que trabajáis son bien conocidos y otros no tanto, ¿qué comparten? ¿Qué buscáis a la hora de escoger un cliente? (¿Fabricante?)
Desde OptimumTIC siempre hemos apostado por aquellas compañías enfocadas plenamente en la ciberseguridad, y que a la vez inviertan en I+D, en la evolución de los comportamientos de los usuarios, etc.

Apostamos por soluciones comprometidas en conseguir solucionar los problemas de ciberseguridad que se plantean en las juntas directivas de las organizaciones desarrollando tecnologías pioneras en el ámbito y que al mismo tiempo no solo aporten una medida técnica, sino que cumplan en Compliance, ubicación de datos, decomisado, registro de eventos, certificaciones PCI, ley de ciberseguridad, etc.

Además, otro aspecto importante es que el fabricante cuente con unos requerimientos a la hora de establecer un partnership, como, por ejemplo, la certificación de parte del equipo. Esto demuestra que el fabricante cuenta con unos niveles de calidad establecidos en el servicio y que asegura la gestión e implementación siempre bajo unas best practices.

"La ciberseguridad no es un proyecto cerrado que empiezas y finalizas en un tiempo, sino que es un ciclo de gestión continua y mejorando día a día"

¿Qué tecnologías de seguridad cree que son imprescindibles en cualquier empresa?
Con el fin de establecer unas mínimas medidas de ciberseguridad es imprescindible proteger, por un lado, una de las vías de entrada más utilizada por los ciber atacantes, el correo electrónico. Los ciber atacantes emplean campañas de ingeniería social (como el phishing) para engañar a los usuarios por carreo electrónico. Para protegernos de estos ataques, las herramientas de protección del correo, mediante la aplicación de unas políticas y medidas de seguridad concretas, consiguen que esos mensajes de phishing no lleguen a las bandejas de entrada de los usuarios, por lo tanto, paramos cualquier tipo de intento de engaño.

"Hay cada vez más oferta y no todos ofrecen ciberseguridad, aunque digan que la ofrecen"

Por otro lado, son importante las herramientas de EDR (Endpoint Detection and Response), que monitorean los dispositivos (endpoints) para mitigar las amenazas cibernéticas, es decir, son herramientas de detección y respuesta de amenazas. Esta tecnología integra de forma nativa los datos de la red, los endpoints y la nube para detener los ataques sofisticados.

Desde OptimumTIC somos partners de dos de las herramientas líderes del mercado en protección de correo y en tecnología EDR. Por un lado, somos partners de Proofpoint, líderes en protección de correo que además cuentan con una de las plataformas de formación de equipos en materia de ciberseguridad más potentes del mercado, PSAT. Por otro lado, como herramienta de EDR para equipos y servidores, somos Partner de Cortex de Palo Alto Networks, la organización estadounidense más potente del mercado de la ciberseguridad y de SentinelOne como únicos fabricantes que recomendamos y a nivel de protección móvil solo recomendamos JAMF- Wandera que implementamos en protección completa de movilidad desde 2018.

¿Qué tecnologías de seguridad cree que serán fundamental?

La protección de todos tus dispositivos, las empresas compran soluciones para dispositivos de trabajo olvidando el dispositivo móvil, cuando a veces trabajas más con el móvil que con un equipo informático, la facilidad de infección, spyware en el móvil, geolocalización y vulnerabilidad de tu privacidad, etc. Está en auge en los ciberataques, ya que llegan a una persona por el móvil y pueden interactuar

"Todas las organizaciones deberían comenzar realizando una Auditoría de Seguridad o Análisis de vulnerabilidades y/o Riesgos, con el fin de conocer los puntos débiles de la organización"

Enlaces de interés...

- El mercado de detección y respuesta gestionada doblará su tamaño en cinco años
- Los CISO españoles sienten ahora que tienen más control sobre su entorno

con tus datos y por tanto alcanzar a tu red. Es muy importante que se tenga en cuenta la protección en este dispositivo.

El futuro se encuentra en el cloud, la acelerada digitalización está llevando a las empresas de entornos on-premise a entornos 100% cloud. Para poder proteger esta nueva metodología de trabajo, una de las soluciones que serán fundamentales en el futuro y que llevamos ya tiempo certificados, será la tecnología CASB (Cloud Access Security Broker), tecnología que permite monitorear toda la actividad en el cloud y conocer todo lo que las organizaciones tienen fuera de su entorno para proteger todo el entorno cloud.

Otra de las soluciones fundamentales en un futuro serán las soluciones DLP (Data Loss Prevention). Los trabajadores de las organizaciones son y seguirán siendo una de las vulnerabilidades más importantes, en muchas ocasiones las fugas de datos se producen debido a malas prácticas realizadas intencionada o des intencionadamente por los propios usuarios de las tecnologías de las organizaciones. Las soluciones DLP son softwares de prevención de pérdida de datos que tienen como finalidad prevenir las fugas de información, una vez que detectan una posible fuga, alertan al usuario para que sea consciente de que la acción que está realizando atenta contra la confidencialidad de la empresa o contra una política de seguridad. Las soluciones DLP, además de monitorear los datos tanto de la red interna de la organización como de los dispositivos, actúan como medida de concienciación.

2021

SONICWALL®

INFORME DE CIBERAMENAZAS

SONICWALL.COM | @SONICWALLSPAIN

A medida que las situaciones de trabajo evolucionaron en 2021, también lo hicieron los **métodos de los actores de las amenazas y los perpetradores motivados**.

En la **actualización semestral del Informe de Ciberamenazas 2021 de SonicWall**, se analiza cómo los actores de las amenazas utilizan cualquier medio necesario (**controles de seguridad laxos, vulnerabilidades sin parches, ataques de día cero y debilidades en la cadena de suministro**) para obtener beneficios maliciosos y provocar disturbios a nivel mundial.

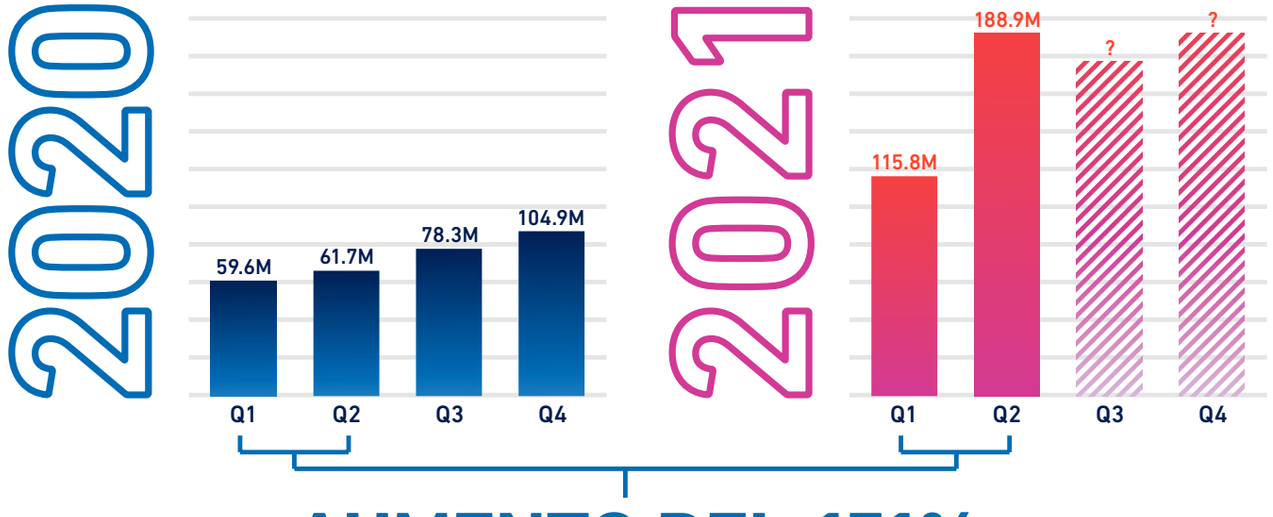
OBTENGA EL INFORME COMPLETO

sonicwall.com/threatreport

EL RANSOMWARE ALCANZA SU MÁXIMO HISTÓRICO

Los ataques de ransomware en el primer semestre de 2021 ya han eclipsado todo el volumen total de 2020: **un aumento del 151% en lo que va de año.**

En los primeros seis meses de 2021, el volumen mundial de ransomware alcanzó la cifra sin precedentes de **304,7 millones** de intentos de ataque.



TENDENCIAS MUNDIALES DE LOS CIBERATAQUES

-22%
2.5 billones
ATAQUES DE MALWARE

+151%
304.7 millones
ATAQUES DE RANSOMWARE

+59%
32.2 millones
ATAQUES DE IoT

+26%
2.1 millones
AMENAZAS CIFRADAS

+23%
51.1 millones
ATAQUES DE CRYPTOJACKING

+9%
2.5 trillones
INTENTOS DE INTRUSIÓN

it Digital Security

Entrevista

‘El passwordless es donde queremos llegar’

(Fabio Cichero, Yubico)

“El vector número uno de ataque sigue siendo el de robo de credenciales, y estamos viendo un mayor interés por robustecer estos sistemas”. Así comienza una charla con Fabio Cichero, Channel Sales Manager Southern Europe de Yubico, una empresa proveedora de llaves de autenticación por hardware.

Rosalía Arroyo

El mercado está tardando en reaccionar. El doble factor de autenticación se extiende, pero lentamente. Asegura el directivo de Yubico que en los más de dos años que lleva trabajando el mercado del sur de Europa ha constatado que sigue habiendo una infraestructura legacy importante, aunque la modernización se está acelerando.

Cuando le preguntamos por lo que está impulsando el mercado de autenticación, menciona Fabio Cichero el cumplimiento; “estamos viendo cómo se pone foco en tener tecnologías que sean resistentes al phishing”. También menciona “una situación geopolítica que está causando que las amenazas y la cantidad de ataques contra la administración pública está creciendo mucho, lo que hace que el tema de la autenticación sea más relevante”.

Parece claro que el uso de contraseñas como única medida para autenticar a un usuario no es un método con las suficientes garantías de seguridad. Grandes organizaciones como Google, Mozilla o Microsoft están llevando el control de accesos a un nuevo paradigma denominado passwordless que reemplazará el uso de contraseñas por alternativas más seguras y amigables para el usuario. Pero este reemplazo no está cerca de producirse porque “sigue habiendo una gran cantidad de

FIDO2, WebAuthn y FIDO Universal 2nd Factor

■ FIDO2 es la última especificación de la Alianza FIDO (Fast Identity Online), fundada en 2012 por PayPal, Lenovo, Nok Labs, Validity Sensors, Infineon y Agnitio, y a la que un año después se sumarían Google, Yubico y NXP.

El objetivo de la alianza fue el de desarrollar estándares abiertos y sin licencia para una autenticación mundial segura en la web. Después de FIDO Universal Second Factor (FIDO U2F) y FIDO Universal Authentication Framework (FIDO UAF), FIDO2 fue el tercer estándar que surge del trabajo de la Alianza.

FIDO2 ofrece la opción de disponer de una autenticación de dos factores, en la que el nombre de usuario y la contraseña habitual de inicio de sesión se complementan con una encriptación con claves FIDO2, así como un token FIDO2 adicional (hardware), o una autenticación completamente libre de contraseña. El hecho de que FIDO2 sea un estándar abierto facilita a los desarrolladores de software y hardware la implementación del procedimiento en sus propios productos para ofrecer a los usuarios este método seguro de acceso.

■ WebAuthn es un estándar que también utiliza criptografía de clave pública, aunque, entre otras mejoras, permite acceder a una aplicación o dispositivo sin utilizar contraseñas (Passwordless).

WebAuthn supone un gran avance no solo en seguridad, sino también en rapidez de acceso, mejorando la experiencia de usuario y reduciendo costes en las empresas. Este estándar va más allá de ser un simple (o múltiple) factor de autenticación, ya que es un estándar que gestiona la autenticación con criptografía de clave pública más un factor adicional como biometría o un PIN.

■ En cuanto a FIDO U2F (UNIVERSAL 2ND FACTOR) es un estándar que utiliza criptografía de clave pública como segundo factor de autenticación. Para ello se utiliza una llave física compatible. El usuario debe tener la llave conectada al dispositivo y, tras introducir sus credenciales, simplemente debe dar un toque a la llave.

Por lo tanto, el factor es doble en sí mismo: primero, es algo que el usuario tiene, la llave con un certificado de clave pública. Este método es resistente al phishing, ataques MiTM, malware y cualquiera de las ciberamenazas más comunes.

"Nuestro día a día es concienciar al mercado y destacar la importancia y lo seguro que es el passwordless"

empresas del sector privado que siguen dependiendo de aplicaciones, sistemas e infraestructura legacy". Asegura Fabio Cichero que "el passwordless es donde queremos llegar. Siendo uno de los miembros fundadores de la Alianza FIDO apostamos por FIDO 2 y WebAuthm, que es lo que te permite hacer el passwordless, así como el FIDO Universal 2nd Factor (FIDO 2F), y nuestro día a día es concienciar al mercado y destacar la importancia y lo seguro que es el passwordless".

Añade Fabio Cichero que hay un 80% de las empresas con las que Yubico está haciendo negocio cuya infraestructura on-prem no permite hacer passwordless, pero que en los próximos 24 meses se verá un cambio que llevará a que el 60% de los clientes estarán preparados para dar el paso hacia el passwordless. La YubiKey es una propuesta de la compañía que permite a los clientes empezar a usarla en una infraestructura legacy, "y poder utilizar el mismo token el día de mañana, cuando tu empresa tenga toda una infraestructura basada en nube".

MEET YUBICO!

CLICAR PARA VER EL VÍDEO

Oferta

"Yo le vendo a los partners el hardware y después les educo para poder prestar servicios", explica el directivo cuando le preguntamos por la oferta de la compañía. La propuesta llega al mercado a través de dos tipos de partners: transaccionales, que venden solamente el hardware, "y lo que nosotros llamamos partners de valor añadido (RAD – Reseller Add Value), que son los que están ofreciendo los servicios".

El producto estrella es la YubiKey Serie 5, una propuesta multiprotocolo que te permite poder aplicarla a los servicios legacy "y el día de mañana modernizar la autenticación de tu empresa".

También cuenta la compañía con un YubiHSM, una propuesta con un HSM incluido para cifrado que ya utilizan algunos clientes de la compañía en Europa, y que se empezará a potenciar en la región de la que Fabio Cichero es responsable de canal.

A finales del año pasado la compañía presentaba serie YubiKey Bio. Creada para la autenticación biométrica en ordenadores de sobremesa, esta serie es compatible con los modernos protocolos FIDO2/WebAuthm y U2F, en factores de forma USB-A y USB-C.

"Sigue habiendo una gran cantidad de empresas del sector privado que siguen dependiendo de aplicaciones, sistemas e infraestructura legacy"

Yubico España

Dos años después de la apertura de una oficina en España, preguntamos a Cichero por la evolución de la compañía en nuestro país. Menciona la firma del acuerdo con Ingecom, así como

"Estamos viendo cómo se pone foco en tener tecnologías que sean resistentes al phishing"

Enlaces de interés...

- Guía de factores de autenticación
- Yubico reimagina la autenticación biométrica por hardware
- Se dispara la adopción de tecnologías de autenticación sin contraseña

el negocio de DotForce, quien distribuye los productos de Yubico desde hace cinco años, como impulsores de un incremento del negocio "muy importante". Asegura además el directivo que el potencial que ven en el mercado, comparado con el previsto hace doce meses, es muy bueno.

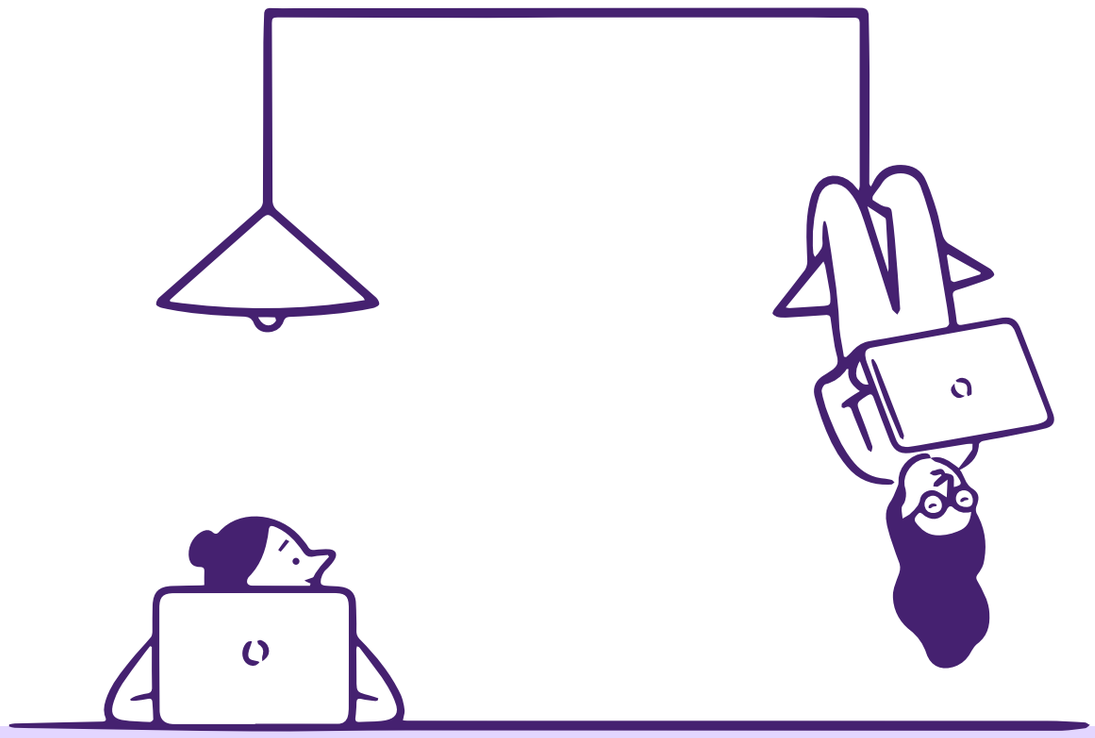
En cuanto a la tipología de cliente, "está cambiando un poco". Cuando la compañía comenzó a operar en España a través de DotForce hace cinco años se trabajaba con empresas pequeñas y medianas, de hasta 500 usuarios; "después empezamos a hacer un ejercicio grande para entrar en grandes cuentas y ahora, con la incorporación de Ingecom y la ayuda de DotForce estamos empezando a penetrar ese mercado". Añade además Cichero que se empieza a tratar con la Administración Pública que "empieza a ser muy relevante en nuestro pipeline".

El mercado de gestión de accesos e identidades, que es el proceso que sigue después de una autenticación, está en pleno proceso de consolidación. ¿Tiene planes Yubico de adentrarse en ese mercado? "No, no está en el roadmap hacer eso. Nuestro core business y nuestro expertise está en el hardware, en la autenticación robusta con tecnología resistente al phishing como la Yubikey, pero sí trabajamos con grandes empresas de ese sector".

¿Cuándo hablas de autenticación robusta resistente al phishing significa que ya no necesito una solución de protección del email? Responde Fabio Cichero diciendo que depende de la tecnología que tenga la llave, y que una de las ventajas de proteger el protocolo WebAuthm es eliminar completamente el factor humano". Añade que hay otras tecnologías que son muy útiles, pero "lo que puedo decir de la Yubikey es que utilizando WebAuthm te detecta si la URL es maligna y la llave no te deja hacer la autenticación. De forma que si la llave se utiliza correctamente es completamente resistente al phishing".

Compartir en RRSS

Tus empleados
se merecen una
tecnología tan
única como ellos.



citrix™

FORO ADMINISTRACIÓN PÚBLICA

itUser

TECNOLOGÍAS HABILITADORAS DE UN GOBIERNO ABIERTO

Organiza

itDigital MEDIA GROUP

Socios estratégicos

Astic

Foro CPP colaboración público-privada TECNOLOGÍA & INNOVACIÓN

Colaboradores

PENTEO

DOUBLETRADE SPAIN Inteligencia comercial para su negocio

NEOKNOW Gestión del Conocimiento

Patrocinadores Platino

MicroStrategy

dynatrace

salesforce

Patrocinadores Oro

veeAM

Mitel

WatchGuard | CYTOMIC

eset

logitech

Patrocinador Silver

INGRAM MICRO

EN BUSCA DEL GOBIERNO ABIERTO

A nivel global, la ciudadanía exige una mayor transparencia y rendición de cuentas de sus gobiernos, y estos han dado un paso adelante para escuchar y atender esta demanda. Los funcionarios están haciendo públicos los datos para permitir una mejor supervisión pública de sus actividades, pero ¿por dónde empezar? ¿Qué pasos hay que dar para conseguir un Gobierno Abierto? ¿Qué elementos y aspectos definen este concepto? ¿Puede existir un Gobierno Abierto sin una adecuada estrategia de Datos Abiertos? ¿Qué supone esto para las Administraciones Públicas y para sus departamentos de TI?

GOBIERNO ABIERTO: ORIGEN Y OBJETIVOS

La Organización para la Cooperación y el Desarrollo Económicos (OCDE) define el Gobierno

#FOROAAPPDIGITAL

Abierto como la apertura de procesos, procedimientos, documentos y datos gubernamentales para el escrutinio y la participación pública. En 2007, 30 defensores de este concepto se reunieron en Sebastopol (California, Estados Unidos) para desarrollar un conjunto de principios para el Gobierno Abierto, y determinaron que hay ocho principios que deben guiar estas iniciativas:

❖ Todos los datos públicos deben estar disponibles. Los datos "públicos" se refieren a información que no está sujeta a limitaciones válidas de privacidad, seguridad o privilegios.

❖ Los datos se recopilan en su fuente principal y no se modifican ni se presentan en conjunto.

❖ Los datos están disponibles de manera oportuna para que sean valiosos y útiles.

❖ Los datos son accesibles para el mayor número de usuarios y para la más amplia gama de propósitos.

❖ Los datos están estructurados para que puedan ser procesados por una máquina.

❖ Los datos están disponibles para cualquier persona, y nadie necesita registrarse para acceder a ellos.

❖ Los datos están disponibles en un formato no propietario: nadie tiene control exclusivo sobre ellos.

❖ Los datos están libres de licencia y no están sujetos a ninguna regulación de derechos de autor, patentes, marcas o secretos comerciales. Sin embargo, las restricciones razonables de privacidad, seguridad y privilegios son aceptables.

EL CONCEPTO DE GOBIERNO ABIERTO SE SUSTENTA EN TRES PILARES BÁSICOS: LA TRANSPARENCIA, LA COLABORACIÓN Y LA PARTICIPACIÓN

Por su parte, OpenGovData.org sugiere siete principios adicionales:

➤ Los datos deben ser gratuitos y deben estar disponibles en línea.

➤ Los datos deben estar disponibles en una ubicación estable de Internet durante un período de tiempo indefinido, y deben permanecer en un formato de datos estable durante el mayor tiempo posible.

➤ Los datos deben ser confiables. Con ese fin, deben estar firmados digitalmente o incluir una certificación de la fecha de publicación / creación, su autenticidad y su integridad.

➤ Debe haber una presunción de apertura. Es decir, el gobierno debe ser proactivo para hacer que la información sea pública y esté disponible.

➤ El gobierno debe proporcionar a los usuarios suficiente información para que puedan determinar si la información es precisa y actual.

➤ Los datos deben ser seguros de abrir, sin contenido ejecutable que pueda transmitir gusanos, virus y malware.

➤ El gobierno debe implementar sugerencias del público sobre cómo difundir información.

Más allá de estos principios, hay dos razones fundamentales para abrir el gobierno: el impacto positivo que tendrá en los ciudadanos (que incluye una mayor conciencia de lo que hace el gobierno, el conocimiento de cómo se gastan sus impuestos y una mejor participación cívica) y los beneficios que los gobiernos pueden obtener (como una mayor confianza cívica en el gobierno, una mayor eficiencia y una mejor prestación de servicios o funciones de sistemas).

GOBIERNO ABIERTO EN ESPAÑA

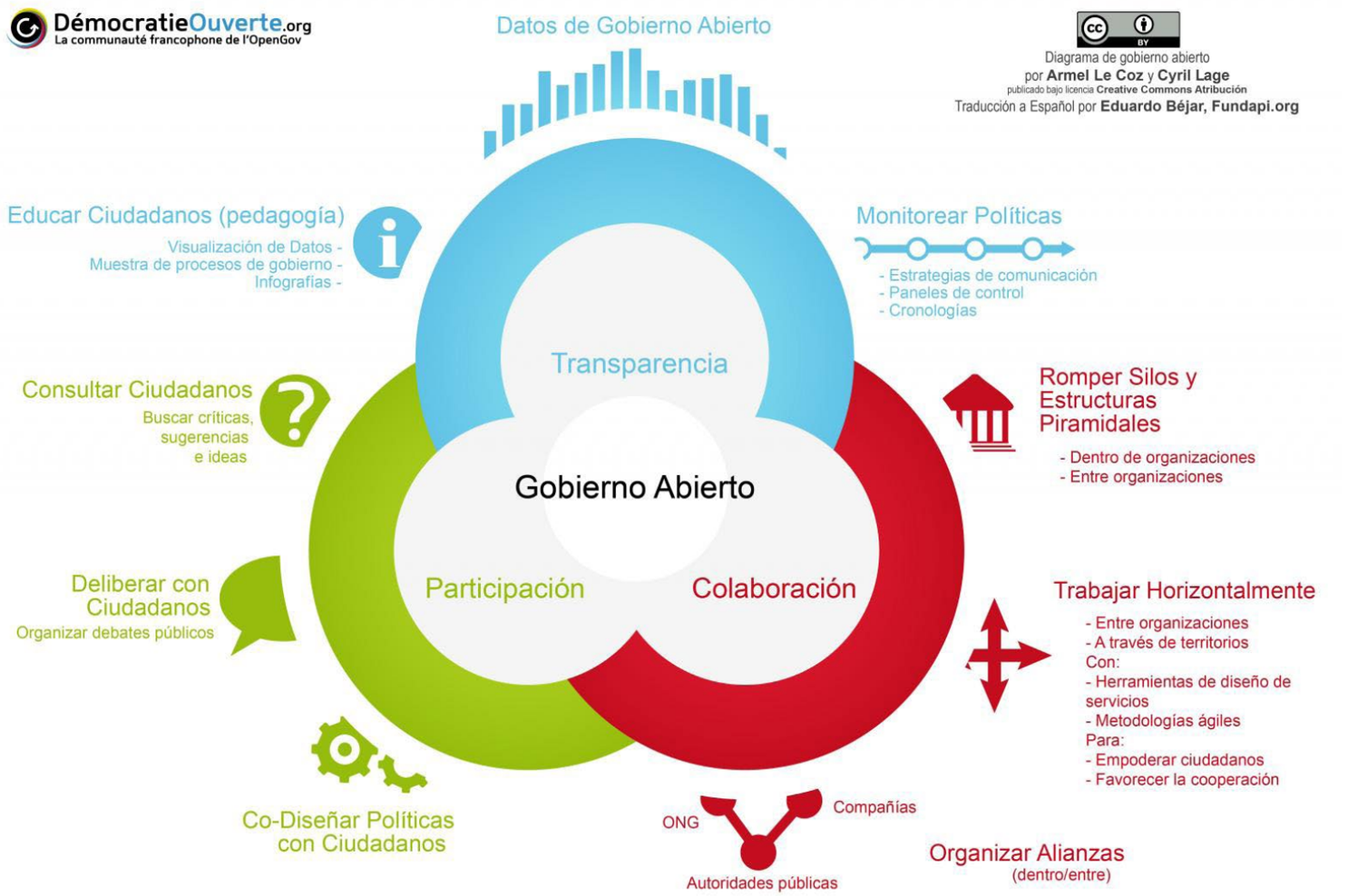
Tal y como se indica en el Portal de Administración Electrónica del Gobierno de España, el Gobierno Abierto tiene como objetivo que los ciudadanos colaboren en la creación y la mejora de los servicios públicos y en el robustecimiento de la transparencia y la rendición de cuentas. El concepto de Gobierno Abierto se sustenta en tres pilares básicos: la Transparencia, la Colaboración, la Participación, y, en el caso de nuestro país, estos

principios se ponen de manifiesto en diferentes actuaciones llevadas a cabo desde las Administraciones Públicas:

✪ **Transparencia, acceso a la información pública y Buen Gobierno.** Los responsables públicos deben velar por la transparencia de la actividad pública, el derecho de acceso a la información y cumplir las obligaciones de buen gobierno.

✪ **Reutilización de la información del Sector Público.** La reutilización de la información del Sector Público consiste en el uso por parte de personas físicas o jurídicas, de información generada o custodiada por organismos del Sector Público, con fines comerciales o no.

✪ **La Administración General del Estado en los medios sociales.** Los medios y redes sociales son un lugar de encuentro, en el que los usuarios de Internet consumen un tiempo cada vez mayor. Los organismos y ministerios han iniciado un acercamiento a los mismos, saliendo al encuentro de los ciudadanos.



TRANSPARENCIA Y BUEN GOBIERNO

La Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno, tiene por objeto ampliar y reforzar la transparencia de la actividad pública, regular y garantizar el derecho de acceso a la información relativa a aquella actividad y establecer las obligaciones de buen gobierno que deben cumplir los responsables públicos. Se trata de una norma que se aplica a todas las Administraciones Públicas y a todo el Sector Público estatal, así como a otras instituciones, como son la Casa de Su Majestad el Rey, el Consejo General del Poder Judicial, el Tribunal Constitucional, el Congreso de los Diputados, el Senado, el Banco de España, el Defensor del Pueblo, el Tribunal de Cuentas, el Consejo Económico y Social y las instituciones autonómicas análogas, en relación con las actividades sujetas a Derecho Administrativo.

REUTILIZACIÓN DE LA INFORMACIÓN DEL SECTOR PÚBLICO

La reutilización de la información del Sector Público consiste, como indicábamos anteriormente, en el uso por parte de personas físicas o jurídicas, de los datos generados y custodiados por los organismos del sector público, con fines comerciales o no.

Bajo este marco, en el año 2009 nace el Proyecto Aporta con el objetivo de fomentar la cultura de la reutilización de la información del Sector Público y difundir su valor social y económico.

La esta reutilización presenta un considerable potencial económico, ya que permite desarrollar nuevos productos, servicios y mercados. Fomenta el desarrollo económico y la creación de puestos de trabajo en la industria de contenidos digitales. Adicionalmente, la puesta a disposición de la información pública por parte de las Administraciones incrementa la transparencia administrativa, teniendo un efecto de refuerzo de los valores democráticos y habilitando la participación ciudadana en las políticas públicas.

La web datos.gob.es es el portal de carácter nacional que gestiona el Catálogo de Información Pública del Sector Público. Constituye un punto único de acceso a los datos que la Administración española pone a disposición para su reutilización. Se trata de una plataforma que alberga más de 25.000 conjuntos de datos de 300 organismos de la administración central, autonómica y local; ofreciendo herramientas que permiten la federación y sincronización efectiva de otros catálogos open data existentes en España.

ES NECESARIO QUE LAS ENTIDADES PÚBLICAS UTILICEN DE FORMA INTERACTIVA LAS TIC PARA QUE LA PARTICIPACIÓN Y LA RELACIÓN CON LOS CIUDADANOS SE VEA FACILITADA

LA ADMINISTRACIÓN GENERAL DEL ESTADO EN LOS MEDIOS SOCIALES

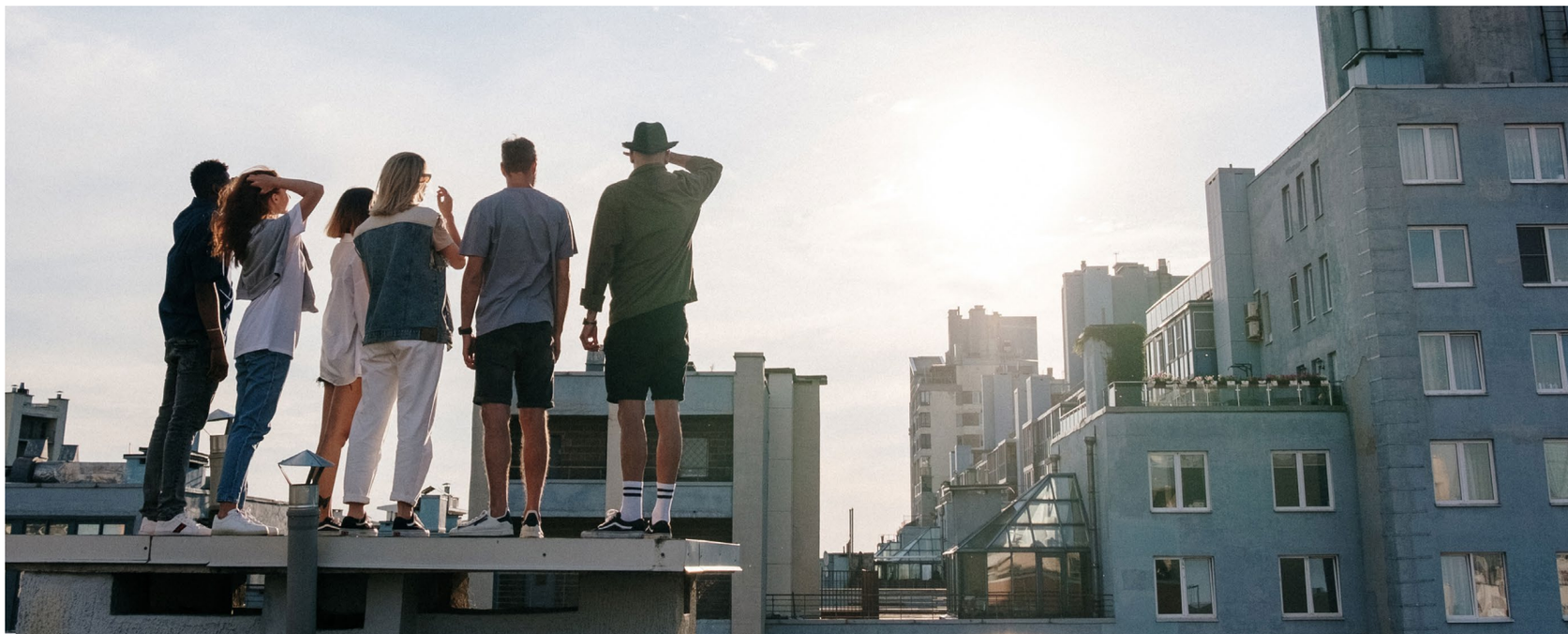
Los medios y redes sociales son un paso más en la estrategia de la Administración para acercarse a los ciudadanos.

Así, el Observatorio de Administración Electrónica de la Administración General del Estado, encargado del seguimiento de la información relacionada con los servicios públicos electrónicos y sus indicadores, difunde la actualidad sobre Administración Electrónica en su cuenta de Twitter.

DIGITALIZACIÓN Y GOBIERNO ABIERTO

La digitalización, implantada ya en muchos organismos e instituciones, también ha llegado a la gestión pública y entidades locales para asentar políticas de Gobierno Abierto.

Esta digitalización, por tanto, es clave para lograr las metas del Gobierno Abierto y se traducirá en una mayor transparencia e integridad en la gestión pública ya sea local, autonómica o central, pero, para alcanzar los



objetivos pretendidos es necesario implementar una estrategia sobre los siguientes factores: mayor transparencia de los datos, mejora de la participación abierta, y mejora de la colaboración abierta. En esta línea, es necesario que las entidades públicas utilicen de forma interactiva las Tecnologías de la Información y Comunicación para que la participación y la relación con los ciudadanos se vea facilitada, y algunas de estas herramientas pueden ser útiles en este sentido:

- **Redes sociales,** como canal de comunicación para sugerencias, reclamaciones, o incidencias de servicio.
- **Portal de Transparencia,** como centro de toda la información de la Administración.
- **Open data,** apertura de datos públicos para generar valor, con los objetivos de pasar de una gestión reactiva a una proactiva, convertirse en una herramienta a disposición de la generación de valor, y como elemento para mejorar el seguimiento y la evaluación de la gestión pública.
- **Omnicanalidad,** con el uso coordinado de los diferentes canales electrónicos, telefónico y presencial.
- **Empleados públicos,** porque son un elemento clave para la Transformación Digital, y será necesario formarlos en habilidades digitales y competencias sociales para mejorar la atención ciudadana.

LA DIGITALIZACIÓN EN EL MARCO DE GOBIERNO ABIERTO PUEDE AYUDAR A MEJORAR LA TRANSPARENCIA, LA PARTICIPACIÓN, LA COLABORACIÓN, Y A GENERAR CONFIANZA EN LAS INSTITUCIONES POR PARTE DE LA CIUDADANÍA

- **Sociedad Civil/Asociaciones** como vehículo para la implantación y desarrollo de políticas de gobierno abierto.

En definitiva, la digitalización en el marco de Gobierno Abierto puede ayudar a mejorar la transparencia, la participación, la colaboración y a generar confianza en las instituciones por parte de la ciudadanía.

DATOS ABIERTOS COMO BASE DEL GOBIERNO ABIERTO

Para que un Gobierno Abierto funcione es necesario que los ciudadanos tengan acceso a información fácil de comprender, pero también fácil de reutilizar. Los Datos Abiertos no solo tienen que ser accesibles, sino que, a través de su reutilización, también tienen que dar la posibilidad a los ciudadanos y empresas de ser parte activa de la comunidad, generando nuevos productos y servicios que puedan ayudar al conjunto de la sociedad. Con estos Datos Abiertos se busca:

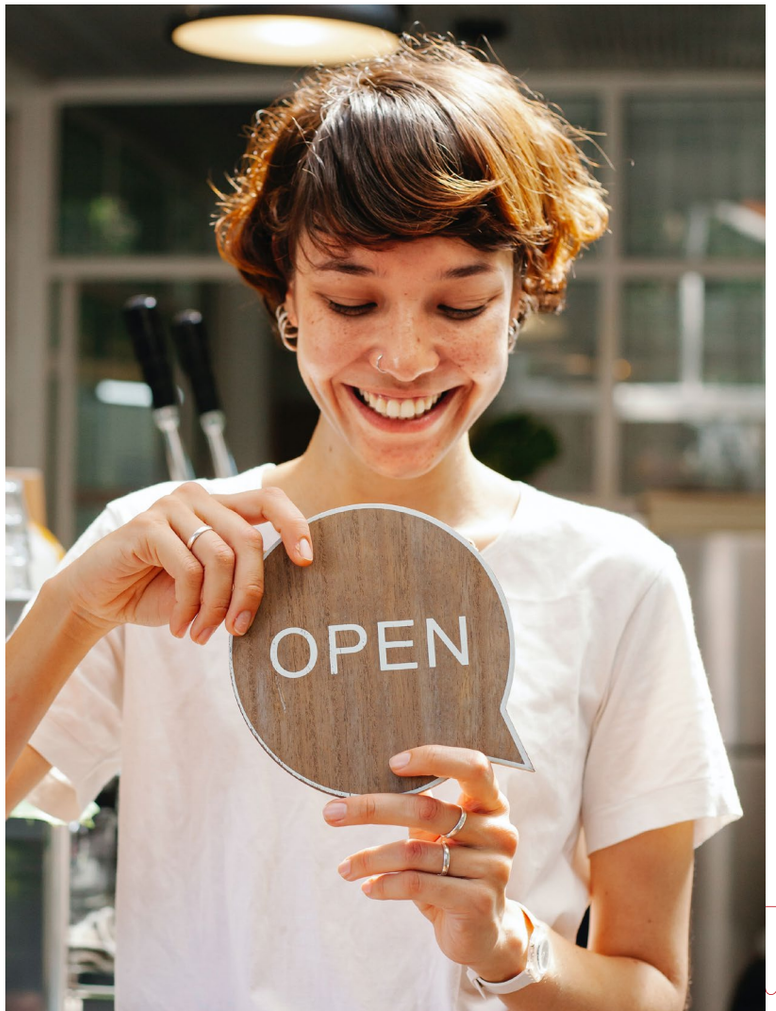
- El acceso a la información pública busca empoderar a los ciudadanos, facilitando que puedan conocer qué acciones se están llevando a cabo.
- La reutilización de la información pública tiene como objetivo que los ciudadanos o empresas la utilicen para crear nuevos servicios y productos que aporten valor a la sociedad, lo cual también repercute en la mejora de la actividad económica.

Pero, aunque ambos conceptos están relacionados, cada uno de ellos es regulado por una norma diferente. Así, en España, el acceso a la información está regulado por la Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobier-

no, que establece una serie de obligaciones referentes a la publicación de información pública que permita a los ciudadanos conocer cómo se toman las decisiones que les afectan. Entre la información que se debe compartir está la distribución de fondos públicos, las funciones de los distintos órganos o los criterios de actuación de las diversas instituciones. Esta información debe ser compartida de la forma más comprensible posible: a través de datos de calidad, claros y sencillos, que se actualizan periódicamente y que son accesibles universalmente, entre otras características.

Sin embargo, la reutilización de información pública está regulada por la Ley 37/2007, de 16 de noviembre, sobre Reutilización de la Información del Sector Público, que fue adaptada por la Ley 18/2015, de 9 de julio, por la que se modifica la Ley 37/2007, de 16 de noviembre, sobre Reutilización de la Información del Sector Público, para incluir los cambios normativos de la Unión Europea (Directiva 2013/37/UE). En esta ley se consigna la necesidad de procesar y publicar la información con unas condiciones que faciliten su reutilización: formatos estructurados, abiertos e interoperables, que garanticen la seguridad, así como la propiedad intelectual e industrial. Es importante que los datos estén completos, y que sean fiables y de calidad.

La información que comparten los organismos públicos para ser reutilizada es de naturaleza muy diversa, y va desde los datos de carácter social o económico hasta información geográfica o estadística. Estos datos pueden ser utilizados para crear, por ejemplo, aplicaciones, ya sea con fines comerciales o no, que ayuden a los doctores a tratar a sus pacientes, a los agricultores a gestionar con eficacia sus explotaciones agrícolas o a los ciudadanos a conocer dónde están los puntos de acceso libre a internet. ■



CONTENIDO RELACIONADO

Informe Global del Gobierno Abierto

Resumen ejecutivo del Informe global del Gobierno Abierto

Gobierno Abierto. Ayuntamiento de Madrid

Catálogo de datos de información Pública del Gobierno de España

Portal de Administración Electrónica del Gobierno de España

Consejo de Transparencia. Gobierno de España

Portal de Transparencia del Gobierno de España

Una introducción al Gobierno Abierto

SI TE HA GUSTADO ESTA REVISTA, COMPÁRTELA

NOEMÍ CÍVICOS, DIRECTORA GENERAL DE SALUD DIGITAL Y SISTEMAS DE INFORMACIÓN DEL SISTEMA NACIONAL DE SALUD DEL MINISTERIO DE SANIDAD

"LAS INICIATIVAS DE GOBIERNO ABIERTO DEBEN SER GARANTES DE LA EVOLUCIÓN DE UNOS SERVICIOS PÚBLICOS PARTICIPATIVOS, EFICIENTES Y RESILIENTES"

Según la OCDE, un Gobierno Abierto es una cultura de gobernanza que promueve los principios de Transparencia, Integridad, Rendición de cuentas y Participación de las partes interesadas, en apoyo, principalmente, de la Democracia y el crecimiento inclusivo.

Por este motivo, "la OCDE trabaja con los empleados públicos y representantes de la Sociedad Civil para la identificación de políticas integradoras que avancen en este enfoque de apertura de las AAPP, y abarca áreas muy diversas, como la coordinación gubernamental, el compromiso cívico y el acceso a la información, la transparencia presupuestaria, la integridad y la lucha contra la corrupción, el uso de las TIC, redes sociales y datos abiertos, y el desarrollo local", tal y como explicaba Noemí Cívicos, Directora General de

Noemí Cívicos repasó en la ponencia inaugural de este Foro IT User, las iniciativas del Ministerio de Sanidad alrededor del Gobierno Abierto. Clica en la imagen para ver el vídeo.

Salud Digital y Sistemas de Información del Sistema Nacional de Salud del Ministerio de Sanidad, en el Foro IT User Administración Digital: "Tecnologías habilitadoras de un Gobierno Abierto", que comentaba además que "el Gobierno Abierto se encuentra presente en los Objetivos de Desarrollo Sostenible de la Agenda 2030, a través del Objetivo 16, que se denomina Paz, Justicia e Instituciones Sólidas, y constituye un acelerador para el resto de estos objetivos".

El Gobierno de España, añadía Noemí Cívicos, "aprobó el Plan de Acción para la implementación de la Agenda 2030, donde los planes de Gobierno Abierto se consideran políticas palanca de toda esta Agenda 2030. Además, las TIC actúan como catalizador de la Transparencia e Información y como elementos clave del Gobierno Abierto. Los profesionales que nos dedicamos a ello en la AGE debemos velar por que así sea desde cada uno de los organismos en los que prestamos servicio, con la ayuda de nuestros colaboradores del sector privado".

DATOS SIGNIFICATIVOS EN EL ENTORNO DE LA SALUD

En concreto, "en la Sede Electrónica del Ministerio de Sanidad, en la página de Datos Abiertos y en nuestra web ministerial, se pueden consultar catálogos de datos significativos relacionados con la gestión propia del Sistema Nacional de Salud".

Uno de los servicios públicos mejor valorados por los ciudadanos, nos explicaba, "incluso, en tiempos difíciles como los de la pandemia, debe contribuir a la trasparencia de las actuaciones de las Administraciones Públicas en la Salud. En concreto, el Sistema de Información Sanitaria garantiza la disponibilidad de la información y la comunicación recíproca entre las administraciones sanitarias. Tiene como objetivo responder a las necesidades de distintos colectivos, como las propias autoridades sanitarias, los profesionales, las asociaciones de este ámbito y los ciudadanos. Se ofrece información sobre sus derechos y deberes o sobre los riesgos para la salud, facilita la toma de decisiones sobre su estilo de vida, fomenta las prácticas de autocuidado y la utilización de los servicios sanitarios, y ofrece la posibilidad de efectuar sugerencias sobre estos aspectos. Contiene también informaciones sobre las prestaciones y la cartera de servicios, e incorpora como datos básicos los relativos a población protegida, recursos humanos y materiales, actividad desarrollada, farmacia y productos sanitarios, financiación y resultados obtenidos, así como las expectativas y opinión de los ciudadanos".

En cuanto al Consejo Interterritorial del Sistema Nacional de Salud, "se pueden consultar las órdenes del día y los acuerdos adoptados en su seno".

DATOS SENSIBLES

En el caso de los datos de Salud, apuntaba Noemí Cívicos, "hemos de tener en cuenta que están especialmente protegidos por la legislación, algo de especial relevancia ahora que se quiere crear un espacio de datos del Sistema Nacional de Salud, alineado con el europeo, una de las diez líneas de actuación definidas en la Estrategia de Salud Digital. Aquí es fundamental distinguir entre el uso primario y secundario de los datos. Será esencial contar con un organismo, que forme parte de la estructura del Ministerio, que regule y administre el acceso a estos, junto con un modelo de gobernanza adecuado y alineado con el Reglamento Europeo de Espacio de Datos". ■

CONTENIDO RELACIONADO

Foro IT User Administración Digital: "Tecnologías habilitadoras de un Gobierno Abierto"

SI TE HA GUSTADO ESTA REVISTA, COMPÁRTELA

HYPERINTELLIGENCE®

Las respuestas
le encontrarán

MicroStrategy®
Intelligence Everywhere

ESPAÑA AVANZA EN LA EJECUCIÓN DEL IV PLAN DE GOBIERNO ABIERTO

EL IV PLAN DE GOBIERNO ABIERTO SE ENCUENTRA EN PLENO PROCESO DE DESPLIEGUE, QUE ESTÁ PREVISTO ENTRE 2020 Y 2024, Y ESTÁ DISEÑADO PARA POTENCIAR LA PARTICIPACIÓN CIUDADANA EN LA ADMINISTRACIÓN, Y, COMO EN OTROS SEGMENTOS, LA TECNOLOGÍA TIENE UN PAPEL FUNDAMENTAL EN LA CONSECUCIÓN DE SUS OBJETIVOS.

Carmen Cabanillas intervino en el Foro para hablar sobre el IV Plan de Gobierno Abierto. Clica en la imagen para ver el vídeo.

Debido a la importancia de los profesionales en los procesos de Transformación Digital de la Administración Pública y en los avances hacia un Gobierno Abierto, la Asociación Profesional de Cuerpos Superiores de Sistemas y Tecnologías de la Información de las Administraciones Públicas (ASTIC) participó en el Foro IT User Administración Digital: "Tecnologías habilitadoras de un Gobierno Abierto". Así, en el evento intervinieron Carmen Cabanillas, Subdirectora General de Gobernanza de los Registros en Dirección General de Gobernanza Pública y Presidenta de ASTIC, y Leonor Torres, Directora de Informática del Ayuntamiento de Alcobendas y Vicepresidenta de ASTIC.

IV PLAN DE GOBIERNO ABIERTO

Carmen Cabanillas nos explicó en qué consiste este IV Plan de Gobierno Abierto y qué papel juegan las TIC en la consecución de los objetivos

#FOROAAPPDIGITAL

marcados. Para esta responsable, “el Gobierno Abierto plantea un nuevo modelo de colaboración, más cercano a la sociedad, dando a conocer qué hace la Administración y fomentando la participación activa de los agentes sociales para mejorar las políticas públicas. Por eso se centra en la transparencia, el acceso a la información pública y la rendición de cuentas, y se apoya en proyectos de colaboración ciudadana e innovación utilizando las tecnologías y en los Datos Abiertos. Está muy relacionado con los Objetivos de Desarrollo Sostenible”.

Para calibrar el papel de la tecnología, “empleamos el modelo del profesor Criado, que coloca en el centro los datos que vamos a explotar con la tecnología, buscando aproximarnos a la necesidad ciudadana con un modelo de tres V: Visión, Administraciones más transparentes e íntegras; Voz, a los ciudadanos y las empresas para que aporten valor con su conocimiento; y Valor, gracias a la colaboración y la co-producción. España pertenece a la Alianza para el Gobierno Abierto desde 2011, y busca promover un modelo de gobernanza más transparente, participativo, inclusivo y responsable. Y somos el único país, de los 78 integrantes, que participa con las tres administraciones: central, autonómica y local”.

En el IV Plan de Gobierno Abierto “se incluyen 10 compromisos y se pone el foco en la mejora del Portal de Transparencia para incrementar la participación ciudadana, y se están integrando tecnologías disruptivas, como la IA, mientras seguimos insistiendo en el valor que aportan los datos para la ciudadanía. El Plan se estructura en 5 ejes: transparencia y rendición de cuentas, participación, integridad, sensibilidad y formación, y compromiso en los ámbitos autonómico y local. Se establecen los mencionados 10 compromisos y, para ello, se plantearon 110 iniciativas a las que se han unido dos más, una en el ámbito académico, con la Red Universitaria, y otra relacionada con la reutilización de datos, con Asedie, que ha logrado que todas las comunidades autónomas se pongan de acuerdo para compartir tres conjuntos de datos de alto valor”.

Leonor Torres centró su presentación en algunas iniciativas de Gobierno Abierto puestas en marcha. Clica en la imagen para ver el vídeo.

De momento, se han conseguido hitos interesantes en este Plan, “como la trasposición de la directiva de Datos Abiertos y la reutilización de la información, y seguimos avanzando en mejorar el uso de tecnologías como la IA, con la involucración de actores importantes para analizar las cuestiones éticas y la definición de los algoritmos”.

NECESIDADES Y TECNOLOGÍA

Por su parte, Leonor Torres indicaba que el concepto de Gobierno Abierto no es nuevo,

pero recibió un importante impulso en la administración de Barack Obama. Tal y como nos comentaba, "el funcionario TIC tiene una labor muy amplia, porque tiene que participar desde diferentes roles para liderar e implementar el Gobierno Abierto. La tecnología es fundamental para llevarlo a cabo".

Para esta responsable, en la espiral de valor de este concepto, "el punto de partida es la gran cantidad de datos que genera la Administración Pública, y nosotros debemos tratarlos y hacerlos accesibles. Y, para ello, nos apoyamos en la transparencia, que nos va a permitir abrir los datos a los ciudadanos, para que vean lo que se está haciendo y de qué manera. A partir de ahí, hemos de rendir cuentas ante los ciudadanos, lo que les permitirá participar y dotar de más integridad a los datos, y esto va a generar un cambio cultural como origen de un cambio social".

Si nos fijamos en los factores clave de este concepto, nos enumeraba Leonor Torres que son "la proactividad, la claridad, la accesibilidad, la reutilización y la sencillez, y esto provocará la conversión de información en conocimiento, que es lo que pretendemos. Pero, para asegurar esto, la información debe ser completa, los datos deben ser primarios, extraerse con la frecuencia suficiente para mantener su valor, garantizarse la accesibilidad, y estar apoyados en formatos abiertos".

Pero ¿qué tecnología se necesita? Para Leonor Torres, "es muy variada. Necesitamos extraer, clasificar, catalogar, y almacenar datos de muchas fuentes. Para ello, vamos a emplear tecnologías Cloud o de Big Data. A esto hay que añadir diferentes técnicas de IA para poder automatizar para poder tomar decisiones de forma más sencilla, y ofrecer los datos de forma más cercana al usuario".

ALGUNOS PASOS YA DADOS

Tal y como apuntaba Leonor Torres, "en los últimos años hemos trabajado en el desarrollo de los diferentes portales de transparencia, ofreciendo los datos para que puedan ser consultados; hemos desarrollado plataformas de participación, incluso con presupuestos participativos; y trabajado en la creación de catálogos de Datos Abiertos, cuyo uso por parte de los ciudadanos nos van a ayudar en futuras catalogaciones".

Mención especial recibieron las "Ciudades Abiertas, una iniciativa liderada por A Coruña, Madrid, Santiago de Compostela y Zaragoza, que busca generar una plataforma de Gobierno Abierto, participativo e interoperable, y ha diseñado una serie de vocabularios de datos que se emplean en los diferentes negocios de las ciudades".

También se está trabajando, añadía Leonor Torres, en el Gobierno del Dato, "una estrategia que viene marcada por la Unión Europea. Se trabaja en iniciativas como la Ley del Dato o la Ley de Gobernanza de Datos. Se busca generar servicios y productos y tener una estrategia mucho más competitiva a nivel económico. Y también se están creando oficinas del dato, tanto en el entorno central como en otras administraciones. Todo ello nos va a permitir la creación de un Mercado Único del Dato, con espacios europeos de datos comunes".

Y no podemos olvidar que el Plan España 2025 "creó la Oficina del Dato, que busca la compartición de datos entre ciudadanos, Administración y empresas privadas, con el objetivo de crear valor y mejorar la economía de nuestro país". ■

CONTENIDO RELACIONADO

Foro IT User Administración Digital: "Tecnologías habilitadoras de un Gobierno Abierto"

SI TE HA GUSTADO ESTA REVISTA, COMPÁRTELA

MARC ISERN, ANALISTA SÉNIOR DE PENTEO

"PARA TENER ÉXITO A LARGO PLAZO HAY QUE INVERTIR EN EL ECOSISTEMA QUE NOS RODEA PARA IR UN PASO POR DELANTE"

¿QUÉ TENDENCIAS TECNOLÓGICAS VAN A MARCAR LA INVERSIÓN PARA FACILITAR UN GOBIERNO ABIERTO? SON DIFERENTES LAS TECNOLOGÍAS QUE ESTÁN IMPACTANDO EN LA SOCIEDAD Y A LAS QUE EL SECTOR PÚBLICO DEBE PRESTAR ESPECIAL ATENCIÓN.

Para conocer cuáles son estas tendencias, participó en el Foro IT User Administración Digital: "Tecnologías habilitadoras de un Gobierno Abierto", Marc Isern, Analista Sénior de Penteo, que explicaba que "son cinco macrotendencias las que están impactando. Actualmente, estamos cerca de la Inteligencia Artificial y la Robótica avanzada, desarrollando la Web 3.0, y viendo como convergen una serie de tecnologías que nos provocan cierta incertidumbre, pero que pueden agruparse en cinco grandes grupos".

Marc Isern mostró en su participación en este Foro IT User las principales tendencias que están impactando en el Sector Público. Clica en la imagen para ver el vídeo.

1. ARQUITECTURA DIGITAL COMPUESTA

La primera es la Arquitectura Digital Compuesta, "una respuesta a las necesidades cambiantes de las organizaciones en su intento por adaptarse a los clientes, a los ciudadanos, de forma ágil y elástica. Las empresas unificarán la experiencia empresarial y la tecnológica para rediseñar la toma de decisiones y establecerán las políticas y estructuras de las propias organizaciones, pasando de un enfoque de eficiencia basado en la estabilidad a uno dinámico basado en la agilidad y el cambio continuo. Tecnologías que componen esta tendencia incluyen la cloud distribuida, Data Fabric y las aplicaciones compuestas, aunque otras colaboran, como los servicios en cloud o las arquitecturas basadas en microservicios, Edge Computing..."

2. HIPER-AUTOMATIZACIÓN

Actualmente "estamos en camino de la Automatización con tecnologías comercializadas como RPA, plataformas Low-Code, chatbots... y en los próximos años, esta Automatización se sofisticará, y las empresas deberán replantearse parte de sus fuerzas de trabajo. Esta tendencia podría llevar a una empresa autónoma guiada por la estrategia de negocio y sus resultados comerciales, pero la máxima eficiencia debería conseguirse con la integración de la eficiencia de la tecnología y la creatividad humana. Hablando de tecnologías, lo hacemos de IA Generativa, vehículos autónomos, o el Software 2.0".

3. CONFIANZA ALGORÍTMICA

Con la digitalización del mundo, "la seguridad ha adquirido una mayor importancia. Todo forma parte de un gran sistema de información, lo que provoca una mayor exposición de los datos. Las organizaciones necesitan potenciar la confianza, tanto en los organismos reguladores como con mecanismos y procesos automatizados basados en algoritmos descentralizados. Hablamos de tecnologías como Blockchain, pero, como hay que asegurar la autenticidad de la información original, entran en escena técnicas de Procedencia Autentificada o de IA Explicable, o la Anonimización Dinámica".

4. NUEVA COMPUTACIÓN

Tal y como apuntaba Marc Isern, "los sistemas tradicionales no son capaces de resolver determinados problemas computacionales, y esto ha llevado a la evolución de las formas de computación con el objetivo de romper el modelo clásico. Encontramos aquí la Computación Neuromórfica, la Computación Cuántica o la Computación Biológica".

5. INTERACCIÓN AUMENTADA

En palabras de Marc Isern, "cada nueva innovación nos aporta nuevos canales de comunicación, y modifica la interacción persona/máquina. La Interacción Aumentada contiene todas las formas de tecnología perceptiva e interactiva. Un paradigma que ahora está de moda en este sentido es el Metaverso, pero también estamos incorporando dispositivos integrados o superpuestos a nuestro cuerpo, como gafas de RV o exoesqueletos. Otro ejemplo es NeuraLink, para tratar ciertos trastornos neurológicos".

En resumen, "todas estas tendencias van a seguir provocando cambios a una velocidad mayor, y no podemos esperar para empezar a funcionar con ellas. Para tener éxito a largo plazo, hay que invertir en el ecosistema que nos rodea, modelando la infraestructura de la propia empresa, para ir un paso por delante". ■

CONTENIDO RELACIONADO

Foro IT User Administración Digital: "Tecnologías habilitadoras de un Gobierno Abierto"

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

DATOS ABIERTOS, LA BASE DE LA TRANSFORMACIÓN DE LA ADMINISTRACIÓN PÚBLICA DIGITAL

Participaron en esta mesa, patrocinada por MicroStrategy, el Ministerio de Asuntos Económicos y Transformación Digital, el Ayuntamiento de Madrid, el Ministerio de Justicia, INAP, y el Ministerio de la Presidencia. Clica en la imagen para ver el vídeo.

EL DATO ES UN ELEMENTO CLAVE EN LA TRANSFORMACIÓN DIGITAL. CONFIABLE Y DE CALIDAD, ES LA BASE DE TODO, DESDE LAS PRINCIPALES DECISIONES ESTRATÉGICAS HASTA EL PROCESO OPERATIVO DE UNA RUTINA. ES FUNDAMENTAL PARA EL DESARROLLO DE SOLUCIONES DISRUPTIVAS LIGADAS A ÁMBITOS COMO LA INTELIGENCIA ARTIFICIAL O BIG DATA. SU CORRECTA GESTIÓN Y GOBIERNO SE HA CONVERTIDO EN UNA ACTIVIDAD ESTRATÉGICA PARA TODO TIPO DE ORGANIZACIONES, YA SEAN PÚBLICAS O PRIVADAS.

La primera mesa redonda del Foro IT User Administración Digital: "Tecnologías habilitadoras de un Gobierno Abierto" se centró en los Datos Abiertos y su gobierno, y contó con la participación de Carlos Alonso, Director

“LOS ESPACIOS DE DATOS DEBEN CONSTRUIRSE SOBRE LOS VALORES EUROPEOS DE TRANSPARENCIA, SOBERANÍA, APERTURA, DESCENTRALIZACIÓN E INTEROPERABILIDAD”

CARLOS ALONSO (MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL)

de la División de la Oficina del Dato del Ministerio de Asuntos Económicos y Transformación Digital; Antonio de la Paz, Secretaría General de Estrategia del Dato del Ayuntamiento de Madrid; Nimia Rodríguez Escolar, Directora de la División de Tecnologías y Servicios Públicos Digitales del Ministerio de Justicia; Manuel Gómez Vaz, Responsable TIC en INAP; y Julián Hernández Vigliano, Subdirector General TIC del Ministerio de la Presidencia, co-moderados por Fernando Gutiérrez Cabello, Responsable de Sector Público de MicroStrategy.

ESTRATEGIAS DE DATOS ABIERTOS

Como primer punto del debate se situaron las diferentes estrategias de datos abiertos. En este sentido, Carlos Alonso señalaba que “la Oficina del Dato está trabajando en el diseño de una estrategia del dato de las Administraciones Públicas, donde se incluye la potenciación del uso de los Datos Abiertos, para lo que queremos escuchar a los implicados en lo que se ha venido a llamar la Tercera Ola de los Datos Abiertos”.

Para Antonio de la Paz, “en el Ayuntamiento de Madrid estamos definiendo la hoja de ruta que vamos a seguir. Hemos trabajado ya mucho en la consolidación y en la visualización de datos, porque no solo basta con poner los datos, sino que hay que presentarlos para su consumo de forma sencilla, rápida y automatizada. Además, estamos tratando de diseñar una estrategia global para todos los pasos, desde la generación hasta el consumo de la información, pasando por la concienciación de todos los implicados”.

Apuntaba Nimia Rodríguez que en el Ministerio de Justicia buscan emplear “datos confiables, de calidad, disponibles e interoperables. Con estos pilares, estamos trabajando en la estrategia de Justicia basada en datos, que incluye el Portal de la Justicia, un proyecto que nace del marco de co-gobernanza con todas las entidades que conforman la Justicia. Es la base sobre la que pivota toda la estrategia, a partir de la transparencia, la reutilización y la compartición y la comunicación de los datos, para lo que hemos creado grupos multidisciplinares que han incluido a los usuarios implicados”.

“HAY QUE ELEVAR A LA GLOBALIDAD LOS ESFUERZOS QUE SE HAN IDO HACIENDO PARA COMPARTIR DATOS, PENSANDO EN SU CONSUMO, NO DÓNDE SE CREÓ O CÓMO SE DEFINIÓ EN ORIGEN”

ANTONIO DE LA PAZ (AYUNTAMIENTO DE MADRID)

En el caso de Manuel Gómez, explicaba que, a día de hoy, “el INAP no comparte información pública y solo aporta cinco de todos los catálogos de la Oficina del Dato. En los últimos años, nuestros esfuerzos han ido dirigidos a ofrecer servicios a los usuarios, pero no disponemos de

plataformas de consolidación y análisis de datos, aunque no podemos olvidar que la mayoría de la información que manejamos es relativa a datos personales, y que, aunque debe ser publicada por razones de transparencia, no es susceptible de ser reutilizada de forma inmediata y directa, por las implicaciones legales".

Finalizaba esta primera ronda de opiniones Julián Hernández Vigliano, que argumentaba que "el Ministerio de la Presidencia tiene una labor más interna dentro de la propia Administración, y, por eso, nuestro foco está muy dirigido a la AGE. Nuestros datos están muy enfocados a la actividad política de alto nivel; no tienen un gran volumen, pero sí son relevantes a nivel de imagen".

DESAFÍOS A ENFRENTAR ALREDEDOR DE LOS DATOS ABIERTOS

Las diferentes entidades deben afrontar una serie de desafíos, tanto tecnológicos como de otra índole. En este sentido, Antonio de la Paz apuntaba que "contamos con tecnologías y herramientas, pero lo complejo es lo relativo a la organización. Es necesario perder el miedo y publicar la información. Además, es necesario que el dato sea de calidad, y contar con unas reglas que aseguren esta calidad del dato en el origen para que la información que se publique no genere conclusiones erróneas, Y, quizá, por último, el problema de cómo se adquiere esa tecnología que podemos necesitar, porque esta tecnología debe ser una palanca facilitadora, no una complicación".

"ES FUNDAMENTAL CONSEGUIR LA IMPLICACIÓN DE LA ALTA DIRECCIÓN, Y LA MEJOR FORMA ES VIENDO CASOS DE USO SENCILLOS, CONCRETOS Y QUE LES APORTEN VALOR"

NIMIA RODRÍGUEZ ESCOLAR (MINISTERIO DE JUSTICIA)

En palabras de Nimia Rodríguez, "tenemos varios retos, tanto no tecnológicos como alrededor de la tecnología. Dentro de los primeros, el fundamental es cambiar el paradigma de expediente judicial al dato, un cambio importante, porque hay que entender que el dato es importante, no el documento. Por otra parte, la normalización del dato con todas las Administraciones. Si no entendemos todos lo mismo, no vamos a poder compartir. Por último, necesitamos saber priorizar lo importante. En cuanto a los tecnológicos, hay que exprimir la potencia del dato, y necesitamos para ello herramientas predictivas que nos permitan tomar decisiones y crear las políticas públicas. Estamos trabajando en identificar estas tecnologías para maximizar los resultados".

Para Manuel Gómez, "podría pensarse que los principales retos pasan por ofrecer información de calidad o minimizar el posible impacto de los riesgos de seguridad, pero la verdad es que los retos no tecnológicos son igual de importantes. Quisiera poner el foco en la cultura que existe en muchas unidades sobre el concepto de propiedad de su información. Es bastante habitual que las diferentes unidades gestionen y analicen sus datos de manera aislada. No tienen la práctica de compartir información no ya con otros organismos dentro de la AGE, sino dentro de la propia entidad. Sería muy importante cambiar esta cultura y pensar en compartir la información, sin olvidar otros desafíos como el equilibrio que necesitamos entre la disponibilidad y la seguridad".

Añadía Julian Hernández que, "por nuestra naturaleza, nuestro enfoque es a compartir datos más interna que externamente. Pero para todos es básica la calidad del dato, lo que

requiere unas plataformas con el mayor nivel de Automatización e inteligencia posible para proporcionar un set de datos que minimice la intervención manual. Es la clave para ofrecer la información adecuada. Además, necesitamos establecer una plataforma para poder enfocarnos en la calidad del dato y no tanto en el cómo. Debe ser flexible para poder centrarnos en el valor añadido a partir del dato. Por otra parte, tendemos a ver el mundo desde nuestra posición, y tenemos que ser conscientes de que para el ciudadano eso es secundario. No podemos forzarle a entender cómo funcionamos y luego buscar el dato. Debemos centrarnos en el valor final a empresas y ciudadanos, no es nuestra organización".

Concluía Carlos Alonso explicando que "hay que diferenciar entre la estrategia de Datos Abiertos y el Gobierno del Dato. La tecnología está disponible, hay que determinar cuál es mejor para cada caso, pero hay retos no culturales importantes. Si hablamos de los Datos Abiertos, hay que dejar hueco a los principales usuarios de estos datos. Por otra parte, deberíamos apostar por la homogenización y por dar herramientas para el correcto consumo de los datos. Asimismo, hay que poner el foco en la calidad, pero también en la semántica de esos datos, y creo que la existencia de repositorios de datos públicos para poder reutilizar la información es fundamental. Con la vista puesta en una estrategia del dato, hay que romper los silos de información con la creación de espacios de datos, para que uniendo los datos seamos capaces de extraer inteligencia".

"LA INNOVACIÓN Y EL CRECIMIENTO BASADO EN DATOS PUEDE APORTAR BENEFICIOS A LAS EMPRESAS Y A LA CIUDADANÍA"

MANUEL GÓMEZ VAZ (INAP)

EL ROL DE LOS DATOS NACIONALES EN EL ESPACIO ABIERTO DE DATOS EUROPEOS

Señalaba Nimia Rodríguez desde el Ministerio de Justicia que "Europa está impulsando la Estrategia de Datos para convertirlo en un motor de innovación, y para ello es fundamental la implicación de los diferentes países miembros. Igual que nosotros debemos colaborar con las diferentes instituciones, en la UE los datos deben fluir entre los estados miembros para generar beneficios, conocimientos, nuevos servicios... y para ello es básico que nuestros espacios de datos se pongan en común con el resto de países. Pero esto impone un reto mayor, porque ya no es lo que entendemos en España, sino que la información debe generar un conocimiento real para que Europa se consolide como una sociedad impulsada por los datos".

Para Manuel Gómez, desde INAP, "los espacios de datos van a definir la estrategia europea. Serán las herramientas que facilitarán la disponibilidad y compartición de los datos de forma confiable y segura. Por eso es importante la unificación de la información y que las reglas del juego sean comunes para poder desarrollar otros servicios e innovación. Hay que ver cómo definir los servicios de intercambios de datos y cómo implantar un sistema de gobernanza de datos compatible con la legislación europea. La innovación y el crecimiento basado en datos puede aportar beneficios a las empresas y a la ciudadanía. Pero todavía estamos en una fase incipiente".

Desde el Ministerio de Presidencia, Julián Hernández comentaba que "nuestra participación es limitada, pero sí lo hacemos en el marco del último Plan de Gobierno Abierto en lo referido a la huella normativa, en la interoperabilidad de las herramientas de legislación, concretamente en la herramienta LEOS, que estamos aterrizando en el marco normativo

español. El objetivo es elaborar una normativa ágil e integrada a nivel europeo. Herramientas como esta permiten agilizar la elaboración normativa y, a nivel europeo, alinear los datos".

Indicaba Carlos Alonso, del Ministerio de Asuntos Económicos y Transformación Digital, "que la palabra clave es interoperatibilidad. Los espacios deben ser interoperables. Alrededor del 12% del valor de la Economía del Dato provienen de los Datos Abiertos. Estos espacios deberían construirse sobre los valores europeos de transparencia, soberanía, apertura, descentralización e interoperabilidad".

Finalizaba esta ronda con la valoración de Antonio de la Paz, del Ayuntamiento de Madrid, que señalaba que "apostamos por los Datos Abiertos, y la demanda cada vez es más grande por parte de los ciudadanos. Hay que elevar a la globalidad los esfuerzos que se han ido haciendo para compartir datos, pensando en su consumo, no dónde se creó o cómo se definió en origen. Debemos consumirlo para poder aportar valor, y la normativa debe facilitarlo. Por supuesto, respetando los conceptos básicos de protección de datos y privacidad".

MEJORES PRÁCTICAS

Cómo se lleva esta teoría a la práctica. Tal y como explicaba Julián Hernández, "hay que aprovechar el esfuerzo del Plan de Recuperación, Transformación y Resiliencia, poniendo en valor las unidades TIC de los ministerios, porque somos los que podemos aunar el conocimiento del negocio con la tecnología que permite ofrecer al ciudadano el valor a partir de los datos. Porque el valor añadido de los datos debe primar sobre la tecnología".

"EL VALOR AÑADIDO DE LOS DATOS DEBE PRIMAR SOBRE LA TECNOLOGÍA"

JULIÁN HERNÁNDEZ VIGLIANO, (MINISTERIO DE LA PRESIDENCIA)

Para Carlos Alonso, "si hablamos de una Administración orientada al dato, la clave es la interoperabilidad, para poder sacar partido a toda la información, y para ello es clave conseguir el apoyo de la dirección. Es fundamental en este avance, el foco basado en casos claros de uso".

Añadía Antonio de la Paz, "los responsables deben creerse este esfuerzo para que tenga sentido, y son básicos esos ejemplos palanca para poder seguir avanzando y generar sinergias necesarias con otros departamentos, unidades o instituciones".

En palabras de Nimia Rodríguez, "conseguir una organización orientada al dato no es sencillo, y desde TI debemos sensibilizar a los poseedores de los datos del valor de estos. Es fundamental conseguir la implicación de la alta dirección, y la mejor forma es viendo casos de uso sencillos, concretos y que les aporten valor".

Concluía Manuel Gómez señalando que "es fundamental la capacidad de decisión de los CIO en las unidades administrativas. La tecnología es el elemento más destacado, pero en la AGE la figura del CIO no ha conseguido alcanzar la importancia que debería, porque muchas decisiones se toman en espacios donde no participan. Y estas decisiones deberían apoyarse en el conocimiento y en las herramientas adecuadas". ■

CONTENIDO RELACIONADO

Foro IT User Administración Digital: "Tecnologías habilitadoras de un Gobierno Abierto"

SI TE HA GUSTADO ESTA REVISTA, COMPÁRTELA

FERNANDO GUTIÉRREZ CABELLO, RESPONSABLE DE SECTOR PÚBLICO DE MICROSTRATEGY

"QUEREMOS UNA ADMINISTRACIÓN PÚBLICA DIRIGIDA POR EL DATO"

LA BASE DE LA TRANSFORMACIÓN DIGITAL DE LAS ADMINISTRACIONES PÚBLICAS Y DE LOS AVANCES EN BUSCA DE UN GOBIERNO ABIERTO ES PODER ACCEDER A LOS DATOS, PORQUE LA INFORMACIÓN GENERADA A PARTIR DE ELLOS PUEDE AYUDAR A REDISEÑAR DE LA MANERA MÁS ÁGIL Y EFICIENTE LOS DIFERENTES SERVICIOS PÚBLICOS DIGITALES.

Con el objetivo de analizar cuáles son las claves para que las instituciones puedan acceder de manera adecuada a los datos, en el Foro IT User Administración Digital: "Tecnologías habilitadoras de un Gobierno Abierto" participó Fernando Gutiérrez Cabello, Responsable de Sector Público de MicroStrategy, que explicaba que "puede haber mucha tecnología, pero lo fundamental es compartir ese dato con el ciudadano de manera intuitiva y rápida.

Fernando Gutiérrez Cabello habló sobre la aplicación de la Hiperinteligencia para la gestión de datos en el Sector Público. Clica en la imagen para ver el vídeo.

#FOROAAPPDIGITAL

Cuando hablamos de Gobierno Abierto, conviene destacar tres elementos, transparencia, colaboración y participación".

LOS RETOS A ABORDAR

Tal y como señalaba Fernando Gutiérrez, "los retos incluyen los múltiples sistemas heredados, y, derivado de él, ser capaces de tener una visión única y un Gobierno del Dato. El tercer problema es el tamaño y la dispersión territorial de la Administración, igual que el hecho de tener que ofrecer un servicio a un público heterogéneo. Por último, hablando de datos, un reto importante es la seguridad".

Frente a estos retos, MicroStrategy planea soluciones como "la flexibilidad con conectores para poder conectarnos e interoperar, herramientas de Gobierno del Dato de visión única, capacidades de escalar datos a nivel local y global, facilitar el acceso a la información de forma rápida e intuitiva a través de HyperCards y portales, y una seguridad única y robusta". A la vista de estos puntos, Gutiérrez apuntaba que "nuestra misión es poder ver el dato en cualquier lugar. Queremos que la Administración sea también una entidad dirigida por el dato".

SOLUCIONES PARA AFRONTAR LOS RETOS

En palabras de Fernando Gutiérrez, "la primera propuesta es ser flexibles, contar con los suficientes conectores y RestAPI que nos permitan integrarnos con la tecnología existente y ser flexibles para añadir otros elementos. Esto nos va a ayudar a la interoperabilidad con otros sistemas y otras instituciones. La segunda, es ser un hub de datos conectado a diferentes fuentes para trabajarlas como si fueran una con seguridad y capacidad para explotarlos".

Para dar respuesta a la visión única y el Gobierno del Dato, la propuesta de MicroStrategy pasa por "intentar concentrar todos los datos en un único lugar donde definiremos los diferentes conceptos de negocio, pero, a partir de ahí, hay que explotarlo de forma organizada para evitar el desgobierno. Ahí hacemos mucho foco en cómo explotar la información gobernada. En este sentido, proponemos una metadata única y común para toda la organización. Esto se traduce en una reducción del tiempo, el coste y el riesgo".

Para paliar el problema de la heterogeneidad de los ciudadanos, el Responsable de Sector Público de MicroStrategy ponía el foco en "romper la brecha digital, aumentar la productividad del ciudadano y del empleado público, acceso multicanal con la misma experiencia, o la HyperInteligencia. Cuando trabajamos con portales, lo que hacemos en embeber MicroStrategy dentro del portal, no hace falta crear uno nuevo, ofreciendo imágenes, información o, incluso, cuadros de mano que se comuniquen con el portal. Esto se apoya en la HyperInteligencia, que indexa en el navegador información de diverses fuentes para, en cuanto reconoce una palabra, subrayarla y ofrecer información contextual. Estas tarjetas permiten la consolidación de datos en un único lugar, y permiten la inclusión de enlaces para otras aplicaciones, procesos o herramientas".

Por último, una pincelada sobre la seguridad que debe ser "única, sencilla y robusta". ■

CONTENIDO RELACIONADO

Foro IT User Administración Digital: "Tecnologías habilitadoras de un Gobierno Abierto"

HiperInteligencia

De la HiperInteligencia a la HiperProductividad

Business Intelligence

SI TE HA GUSTADO ESTA REVISTA, COMPÁRTELA

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.

APLICAR LA INTELIGENCIA PARA LA CREACIÓN DE MEJORES SERVICIOS PÚBLICOS DIGITALES

UNO DE LOS PRINCIPIOS DEL GOBIERNO ABIERTO ES LA PARTICIPACIÓN CIUDADANA. EL SECTOR PÚBLICO TIENE QUE POTENCIAR ESA RELACIÓN CON LA CIUDADANÍA CON UNOS SERVICIOS QUE SEAN ÁGILES EN SU CONSTRUCCIÓN Y TAMBIÉN EN SU RESPUESTA. LA IA Y LAS TECNOLOGÍAS DE AUTOMATIZACIÓN INTELIGENTE CONSTITUYEN UN POTENCIAL ALIADO DE LAS ENTIDADES PARA LOGRAR ESTOS OBJETIVOS.

La segunda mesa redonda del Foro IT User Administración Digital: "Tecnologías habilitadoras de un Gobierno Abierto" se centró en la creación de servicios centrados en la ciudadanía y apoyados en la Inteligencia Artificial, y en ella participaron Carlos Maza, Subdirector TIC del Tribunal de Cuentas; Jorge Navas Elorza,

Esta mesa redonda, patrocinada por Dynatrace, contó con la participación del Tribunal de Cuentas, el Ministerio de Hacienda y Función Pública, el Ministerio de Agricultura, Pesca y Alimentación, el Gobierno de Cantabria y el Ministerio de Asuntos Económicos y Transformación Digital. Clica en la imagen para ver el vídeo.

Responsable TIC de la Secretaría General de Fondos Europeos del Ministerio de Hacienda y Función Pública; Faustino Sánchez, Responsable del Área de Analítica de Datos del Ministerio de Agricultura, Pesca y Alimentación (MAPA); Rocío Montalbán, Secretaria General de Transformación Digital y Relaciones con los Usuarios de la Consejería de Sanidad del Gobierno de Cantabria; Montaña Merchán, Coordinadora de tecnologías habilitadoras del Ministerio de Asuntos Económicos y Transformación Digital; co-moderados por Julia Santos, Directora de Ventas de Dynatrace.

TECNOLOGÍAS INTELIGENTES Y SERVICIOS PARA EL CIUDADANO

Tal y como señalaba Carlos Maza, “algunas tecnologías, como RPA, están ya implantadas en el mercado y son estándares. También está bastante extendido el Procesamiento de Lenguaje Natural, y la que es más incipiente en este momento es la Inteligencia Artificial, porque hace falta que haya suficientes datos de calidad, con series históricas. Tenemos la suerte de contar con una Estrategia Nacional de Inteligencia Artificial, un marco donde se fijan prioridades y se destacan áreas de implementación, y tenemos los PERTES, como el puesto en marcha alrededor del leguaje español. En el

“TENEMOS UNA BUENA BASE PARA IMPLEMENTAR LA IA, PORQUE SOMOS USUARIOS AVANZADOS DE BI, Y CONTAMOS CON UNA FUERTE FORMACIÓN DEL PERSONAL EN CUESTIONES TI Y UNA BASE ALGORÍTMICA MUY AMPLIA”

CARLOS MAZA (TRIBUNAL DE CUENTAS)

Sector Público lo iremos absorbiendo poco a poco según avance su implantación”.

Para Jorge Navas, “aunque llevamos mucho tiempo con grandes expectativas, es ahora cuando la IA se está empezando a usar en la Administración. Un ejemplo son las herramientas de guiado o navegación. Si lo mezclamos con IoT, el potencial es enorme, como las posibles aplicaciones en las Ciudades Inteligentes. Esto está aportando una gran dinamización. Otras tecnologías implantadas ya son la de Reconocimiento de Voz o el Aprendizaje Automático, de las que podemos ya ver casos de uso cotidianos, pero la tecnología más destacada ahora es RPA”.

En opinión de Faustino Sánchez, “la Inteligencia Artificial está en auge ahora por el hardware que permite procesar más datos, por la propia disponibilidad de datos para realizar análisis y la existencia de librerías abiertas para que los desarrolladores puedan crear sus sistemas de IA y aplicarlos. Hay que distinguir entre una aplicación indirecta de la IA, embebida en otros sistemas, como los de RPA, que no precisa un conocimiento profundo ni cambiar tus procesos; pero la aplicación directa sí necesita abordar la IA con una forma de trabajo diferente, con soluciones más disruptivas”.

Apuntaba Rocío Montalbán, que “en el mundo sanitario estas tecnologías tienen un nivel de madurez importante, y todos hemos visto cómo han ayudado en la reciente crisis. Pero en un punto más cercano a los ciudadanos, el Procesamiento del Lenguaje Natural está ayudando a procesar muchos datos médicos para permitir que el trato de los profesionales sea más huma-

“HAY QUE TRATAR DE AUTOMATIZAR PROCESOS CON TAREAS REPETITIVAS QUE NO REQUIERAN LA VALORACIÓN DE UN EXPERTO”

JORGE NAVAS ELORZA

(MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA)

no y la información pueda tratarse y aportar valor. Otra tecnología muy desarrollada es Machine Learning para el despliegue de la medicina personalizada o de precisión, que trata de adaptar los protocolos sanitarios a la circunstancias del propio paciente. Otro uso muy generalizado es el análisis de imágenes médicas”.

Finalizaba la primera ronda de opiniones Montaña Merchán, que comentaba que “estamos en un momento disruptivo de la IA, sobre todo cuando aparece la palabra aprendizaje. Esto es algo que, con la capacidad de proceso, da un impulso enorme a la IA. El Sector Público va incorporando estas tecnologías, aunque sea algo más lento. Ha avanzado también mucho el Procesamiento de Lenguaje Natural. Y otro caso es la automatización en las inspecciones del Ministerio de Trabajo, que aporta un elemento interesante: si el sistema puede abrir un expediente sancionador sin la intervención de un inspector. Es un salto importante ligado a la responsabilidad de estos sistemas”.

ÁREAS DE APLICACIÓN CONCRETA DE ESTAS TECNOLOGÍAS

En el Ministerio de Hacienda y Función Pública, Jorge Navas señalaba que “hay que tratar de automatizar procesos con tareas repetitivas que no requieran la valoración de un experto. Áreas con gran volumen de usuarios y expedientes, o en aquellas con dificultad para integrar múltiples plataformas, algo que puede solventarse con RPA. Además, otras áreas de aplicación son aquellas con personal menguante y necesidad de incrementar la eficiencia. En nuestro caso hemos arrancado algunos pilotos en departamentos concretos. Si hablamos de Machine Learning, es muy

“HACE TRES AÑOS NOS PLANTEAMOS HACER ESTE TIPO DE PROYECTOS, Y HEMOS TENIDO QUE HACER CAMBIOS CULTURALES, ORGANIZATIVOS Y TECNOLÓGICOS”

FAUSTINO SÁNCHEZ

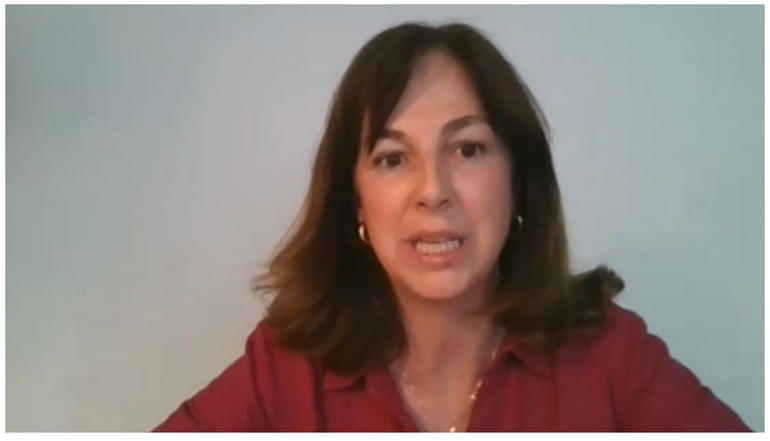
(MINISTERIO DE AGRICULTURA, PESCA Y ALIMENTACIÓN)

útil para áreas de inspección, por ejemplo. El problema es que necesitamos miles de expedientes para alimentar el modelo de referencia”.

Para Faustino Sánchez, en el Ministerio de Agricultura, Pesca y Alimentación, “de manera indirecta, aplicamos la IA en sistemas como la Ciberseguridad y no somos conscientes de ello. No necesitamos, en

ese caso, un experto en Inteligencia Artificial, sino un experto en Ciberseguridad. Pero si hablamos de aplicación directa, nosotros lo hemos aplicado a la Analítica predictiva. Hemos tenido que adaptar el Machine Learning a la naturaleza de los datos que necesitamos. Por ejemplo, lo estamos usando para detección de incendios forestales, integrando el histórico de datos y datos públicos de terceros para generar patrones que se aplican al día a día. También lo estamos aplicando para predicción de cosechas".

En el Gobierno de Cantabria, Rocío Montalbán apuntaba hacia "tres áreas de actuación. Primero, el diagnóstico clínico y la investigación; segundo, la telemedicina; y la gestión de los centros sanitarios. En el primer grupo, hay un campo de acción importante en la prevención, para lo que es necesario un gran volumen de datos históricos y periódicos, y ahí podemos usar el Aprendizaje Automático. En teleasistencia, el incremento de la esperanza de vida aumenta la necesidad de tratamientos crónicos, con un fuerte impacto en el consumo de recursos. Utilizando dispositivos en el domicilio del paciente podemos facilitar el trabajo del profesional sanitario. Por último, en la gestión de los centros, podemos mejorar el manejo con



"EN EL MUNDO SANITARIO ESTAS TECNOLOGÍAS TIENEN UN NIVEL DE MADUREZ IMPORTANTE, Y TODOS HEMOS VISTO CÓMO HAN AYUDADO EN LA RECIENTE CRISIS"

ROCÍO MONTALBÁN (GOBIERNO DE CANTABRIA)

este tipo de tecnologías, como es el caso de los chatbots".

En palabras de Montaña Merchán, en el Ministerio de Asuntos Económicos y Transformación Digital "podemos mencionar el proyecto de la SGAD (Secretaría General de Administración Digital), que tiene como objetivo ofrecer servicios comunes en base a Automatización Inteligente. Se ha empezado con una plataforma de RPA para que el resto de organismos puedan llevar a cabo sus propios proyectos de Automatización. Posteriormente, se ofrecerán otros desarrollos basados en IA, porque la integración de ambas tecnologías tiene un gran potencial en muchos procesos de la Administración".

Concluía esta segunda ronda, desde el Tribunal de Cuentas, Carlos Maza, que añadía "el suyo es un órgano muy especializado, pero muy favorable para la implementación de la IA, porque nuestra principal función es la fiscalización. Recibimos las cuentas y los contratos de todo el Sector Público, esto es, instituciones, empresas y fundaciones de todos los tamaños, tanto en forma de información estructurada como desestructurada, y con una gran variedad de contratantes. Tenemos unos altísimos volúmenes de información, difícil de procesar, y una buena base para implementar la IA, porque somos usuarios avanzados de BI, tenemos una fuerte formación del personal en cuestiones TI, así como una base algorítmica muy amplia. Sobre ello, vemos varios usos directos de estas tecnologías en el Tribunal, ya sea para el Procesamiento del Leguaje Natural, la traducción automatizada, o los análisis para luchar contra el fraude. Estamos en una institución donde la dirección está apoyando la implementación de la IA".

RETOS A LOS QUE ENFRENTARSE

Para Faustino Sánchez, “hace tres años nos planteamos hacer este tipo de proyectos, y hemos tenido que hacer cambios culturales, organizativos y tecnológicos. Decidimos orientaros a casos de uso concretos, y vimos que nos enfrentábamos a retos tecnológicos, porque necesitábamos una agilidad y flexibilidad que no nos ofrecía la tecnología on-premise, así que nos fuimos a la nube. Necesitábamos un cambio de metodologías e incrementar los niveles de colaboración entre los agentes. Así que tuvimos que cambiar la filosofía de los propios grupos de trabajo para el desarrollo de estos proyectos, con la formación adecuada a cada uno de los perfiles, ya sean de tecnología como de negocio para interpretar los propios datos”.

En opinión de Rocío Montalbán, “nos enfrentamos a un reto considerable de anonimización de los datos. Se requiere compartir información entre distintas organizaciones, y, para ello, tenemos que entendernos, y es otra dificultad añadida. Esto nos ha provocado el viaje a cloud como vía inexcusable. Asimismo, necesitamos que los ratos sean de calidad para que las decisiones no sean erróneas. Además, estamos hablando de un entorno que es foco de ciberataques. A favor, tenemos que tec-

“LA INTEGRACIÓN DE RPA E INTELIGENCIA ARTIFICIAL Y MACHINE LEARNING TIENE UN GRAN POTENCIAL EN MUCHOS PROCESOS DE LA ADMINISTRACIÓN”

MONTAÑA MERCHÁN (MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL)

nología y Sanidad han ido de la mano desde el principio, y los profesionales están muy acostumbrados al cambio continuo. En este momento, estamos enfocados, de forma conjunta, a encontrar la aplicación de los datos como solución a muchos de los problemas de salud”.

Según Montaña Merchán, “uno de los retos del uso de la IA a las Administraciones es que adoptemos la innovación como una forma de diseñar servicios. Pero esto sin datos no es posible. La Administración debe estudiar, analizar y limpiar estos datos, porque los algoritmos no son sesgados, pero sí los datos, y hay que aprender a limpiarlos, aunque sea complicado hacerlo. Por tanto, la responsabilidad de las Administraciones es un reto, igual que la capacitación y formación del empleado público. El análisis de los datos es muy importante, tanto a nivel técnico como a nivel funcional”.

Añadía Carlos Maza que “el primer reto es el mercado, porque estas tecnologías todavía están menos maduras que otras. Por otra parte, nos encontramos con el Modelo de Gobernanza de estos proyectos, porque necesitan una implicación transversal que implique a todas las partes y la involucración de la dirección”.

Ponía el punto final a estas opiniones Jorge Navas, que apuntaba que “en la Administración los retos son jurídicos, organizativos y técnicos, porque si algo no está regulado no se puede poner en marcha, aunque esté muy avanzado. Necesitamos equipos multidisciplinares que interactúen en todo el proceso. La Administración Pública va a transformarse por completo, y hasta 800.000 empleados públicos podrían dejar de hacer las funciones que están realizando a día de hoy”.

MEJORES PRÁCTICAS

Para Rocío Montalbán, “hay que valorar en estos proyectos la calidad de los datos, la formación de los profesionales que participan en los grupos de trabajo, la colaboración de las diferentes perspectivas para generar mayor valor, y pensar en el objetivo a alcanzar para no tener experiencias frustradas. Además, en nuestro caso, la legislación y los protocolos son muy importantes”.

En palabras de Montaña Merchán, “hay que determinar los objetivos y los resultados a conseguir, para, a partir de ahí, puedes empezar con un piloto o con la aplicación de un proceso. Necesitas suficiente datos de calidad y relevantes, y esto es lo más importante, porque de ellos dependerá el éxito del proceso. Y, por último, aplicar una metodología adecuada”.

Según Carlos Maza, “lo importante es abrir camino presupuestario, igual que ya se piensa en ciberseguridad, por ejemplo, a la hora de planificar las inversiones. Todos los años tiene que haber una partida y la dirección tiene que ser consciente de que la IA es algo tan propio de las TIC como una base de datos”.

Apuntaba Jorge Navas que “es importante crear un grupo estratégico multidisciplinar para definir el proyecto piloto asegurando la cobertura necesaria. Pero no todo se puede hacer, y hay que centrarse en lo importante, lo necesario o lo que no se pueda hacer de otra manera, e implicar a la dirección. Además, hay que elegir una plataforma que te permita realizar la Automatización asistida”.

Y finalizaba Faustino Sánchez, “son proyectos que tienen una gran incertidumbre, pero es en estos contextos donde mejor funcionan. Por eso hay que definirlos bien desde el principio y no perdernos en los conceptos de moda, sino en lo que funcionar realmente. Y, por último, evitar que se instrumentalicen los algoritmos”. ■

CONTENIDO RELACIONADO

Foro IT User Administración Digital: “Tecnologías habilitadoras de un Gobierno Abierto”

SI TE HA GUSTADO ESTA REVISTA, COMPÁRTELA

JULIA SANTOS, DIRECTORA DE VENTAS DE DYNATRACE

"LAS TECNOLOGÍAS TRANSFORMADORAS MODIFICAN LOS MODELOS DE SERVICIO Y ACELERAN EL CAMBIO"

HAY NUMEROSOS EJEMPLOS DE CÓMO SE ESTÁ APLICANDO LA AUTOMATIZACIÓN Y DEL USO DE LA INTELIGENCIA ARTIFICIAL EN LA ADMINISTRACIÓN PÚBLICA, PERO AMBAS LÍNEAS DE DESARROLLO SE ENFRENTAN A SIGNIFICATIVOS DESAFÍOS PARA SEGUIR AVANZANDO EN LA CREACIÓN DE SERVICIOS ÁGILES PARA LOS CIUDADANOS.

Para hablar de tendencias como la IA y la Automatización en el Sector Público, en el Foro IT User Administración Digital: "Tecnologías habilitadoras de un Gobierno Abierto" intervino Julia Santos, Directora de Ventas de Dynatrace, que nos explicaba que "hay dos ámbitos que son muy interesantes, como son la creación de infraestructuras y servicios digitales líquidos y una administración orientada a la ciudadanía".

Julia Santos centró su intervención en la evolución de la automatización en el Sector Público. Clica en la imagen para ver el vídeo.

ÁREAS DE IMPLEMENTACIÓN

En el primero de los casos, comentaba Julia Santos, "el Plan se refiere a la adopción de modelos cloud, a la potenciación de la nube SARA, pero es trasladable al esto de administraciones. Ahí vemos una aplicabilidad muy importante, porque estas tecnologías transformadoras modifican los modelos de servicio y aceleran el cambio, pero deben acompañarse de otras medidas, como aplicar la IA a las operaciones".

Por otra parte, "cuando hablamos de administración orientada a la ciudadanía, se están adoptando medidas para poner al ciudadano y al empleado público en el centro, con acciones como los chatbots o los asistentes digitales, o simplemente el rediseño de lo que se muestra en la web. Pero es interesante que estas medidas se puedan medir, empleando la IA, para poder tener un proceso real de mejora continua".

DESAFÍOS A SUPERAR

En este camino, las Administraciones Públicas se enfrentan a una serie de desafíos. Como resumía Julia Santos, "muchas de las organizaciones se han encontrado con que las herramientas que tienen de medición de estas iniciativas, generalmente, están en silos. Las diferentes partes de las instituciones miden con distintas herramientas, con lo que las personas de cada área hablan un lenguaje diferente, y el reto es encontrar plataformas que unifiquen los datos para que todos naveguen en la misma dirección. Nos encontramos muchos proyectos de transformación de la observabilidad, es decir, la capacidad de una organización para conocer los elementos que sustentan un servicio digital y cómo se relacionan entre sí, algo importante para detectar problemas antes de que impacten al ciudadano o, en el caso de impacto, el tiempo de recuperación sea lo más rápido posible. A estos proyectos, ligados a otros más transformadores, hay que pedirles un alto grado de automatización, la aplicación de la IA para controlar y manejar la información, y contextualización de la información con el contexto y la realidad del servicio".

ALGUNOS CASOS DE ÉXITO

Para aterrizar estos conceptos en la realidad, Julia Santos recordaba algunos de los casos de éxito que tiene Dynatrace en el Sector Público. "Podemos mencionar", apuntaba, "el caso del Ayuntamiento de Baracaldo, que puso en marcha una iniciativa para que los canales digitales pudieran ser utilizados por toda la población. Otro proyecto es el de la Secretaría General de Administración Digital, que ha puesto en marcha un proceso de transformación de la observabilidad para coordinar las acciones, reducir los incidentes y poder ofrecer un servicio más proactivo".

Estos ejemplos se apoyan en tecnología de Dynatrace, "una plataforma de observabilidad para monitorizar infraestructuras, aplicaciones, servicios, negocio, experiencia digital y seguridad, en base a tecnología de Inteligencia Artificial, que, en nuestro caso, llamamos Davis, embebida en el corazón de la solución, que tiene un alto grado de automatización tanto para la recogida de información como para la interrelación de los diferentes componentes de una aplicación o servicio. Con esto, detectamos problemas antes de que impacten en el usuario o el empleado, además de detectar la causa real o reducir el tiempo de respuesta en caso de impacto". ■

CONTENIDO RELACIONADO

Foro IT User Administración Digital: "Tecnologías habilitadoras de un Gobierno Abierto"

SI TE HA GUSTADO ESTA REVISTA, COMPÁRTELA

Modern Data Protection

Own, control, backup and recover your data anywhere in the hybrid cloud. Ensure business resilience, protect your data from malicious actors and eliminate data loss and downtime. Confidently move to the cloud, avoiding lock-in with cloud mobility.

Ransomware Protection

Cloud Acceleration

Backup Modernization

APROVECHANDO LA INFORMACIÓN PARA DESARROLLAR UNA ADMINISTRACIÓN PROACTIVA

En esta mesa redonda, patrocinada por Salesforce, participaron el Principado de Asturias, la Generalitat Valenciana, la Comunidad de Madrid, el Gobierno de Canarias, el Gobierno de La Rioja y el Ayuntamiento de Alcobendas. Clica en la imagen para ver el vídeo.

MEJORAR LA CALIDAD DE LA DEMOCRACIA MEDIANTE SERVICIOS PÚBLICOS DIGITALES, ÁGILES Y ÚTILES, Y LA IMAGEN QUE LA CIUDADANÍA TIENE DE SU ADMINISTRACIÓN, EXIGE ELEVAR LA RELACIÓN QUE CUALQUIERA DE SUS GOBIERNOS, INDEPENDIENTEMENTE DE SU NIVEL, TENGAN CON LOS CIUDADANOS. ¿CÓMO SE PUEDE GENERAR UNA ADMINISTRACIÓN PROACTIVA QUE LLEVE AL SIGUIENTE NIVEL LA RELACIÓN ENTRE GOBIERNO Y CIUDADANOS?

En la tercera mesa redonda del Foro IT User Administración Digital: "Tecnologías habilitadoras de un Gobierno Abierto", centrada en la potenciación de una Administración proactiva, participaron José Antonio Garmón, Director General de Gobernanza Pública, Transparencia, Participa-

ción Ciudadana y Agenda 2030 del Principado de Asturias; Andrés Gomis Fons, Director General de Transparencia, Atención a la Ciudadanía y Buen Gobierno de la Generalitat Valenciana; Pablo García-Valdecasas, Director General de Transparencia y Atención al Ciudadano de la Comunidad de Madrid; Marta Saavedra, Directora General de Transparencia y Participación Ciudadana del Gobierno de Canarias; Axier Amo, Director General de Transparencia y Buen Gobierno del Gobierno de La Rioja; y Roberto Magro, Jefe de Servicios Interactivos del Ayuntamiento de Alcobendas; co-moderados por Julia Molina, Directora de Estrategia y Desarrollo de Negocio en Sector Público de Salesforce.

LA REALIDAD DE LA ADMINISTRACIÓN PROACTIVA

Una Administración proactiva es aquella que inicia la comunicación con los ciudadanos, se adelanta a los acontecimientos problemáticos, utiliza herramientas de análisis, toma decisiones innovadoras y planifica con antelación. ¿En qué punto se encuentran las entidades invitadas a esta mesa redonda?

Explicaba para comenzar Axier Amo que "estamos apostando por el uso de la tecnología y por favorecer la predicción para adelantarnos en la respuesta a las demandas de la ciudadanía. El ciudadano es cada vez más exigente, y la tecnología nos ayuda. Tenemos que acostumbrarnos a ello, aunque no todo lo que es tecnología realmente ayuda, pero la proactividad debe permitirnos adelantarnos a las exigencias de la ciudadanía aportando soluciones. Un ejemplo de esto se ha visto en los hospitales de La Rioja, durante la Covid, para adelantarnos a la posible necesidad de camas por parte de los enfermos. Y ahí hemos visto lo que puede aportar la tecnología y la proactividad a la Administración".

"TENEMOS MUCHOS DATOS DE LA CIUDADANÍA, PERO HAY QUE GESTIONARLOS MEJOR PARA QUE SEAN REALMENTE ÚTILES PARA ELLOS"

JOSÉ ANTONIO GARMÓN (PRINCIPADO DE ASTURIAS)

En palabras de Marta Saavedra, "la proactividad en la Administración la entendemos desde la perspectiva en la que nos manejamos del Gobierno Abierto. Cuando los gestores políticos llegamos al puesto al principio de la legislatura, tenemos un encontronazo con la realidad. Es muy importante el análisis previo de los servicios y la disponibilidad para trabajar de forma proactiva. A veces nos encontramos con ciertas reticencias, y hay que ver cómo está el nivel de los procedimientos. Pero sabiendo que el Gobierno Abierto es una declaración de intenciones para ir mejorando en la relación con la ciudadanía, establecimos un plan con medidores de avance y metas alineadas con los objetivos. Resumiendo, hemos sido capaces de implementar una dirección por objetivos, estableciendo indicadores y líneas de trabajo, y hemos creado un cuadro de mandos para evaluar el avance y seguir tomando decisiones, así que estamos satisfechos, por el momento".

Añadía Pablo García-Valdecasas, "estamos en el camino de lograr esa cercanía con el usuario. La tecnología ha venido para quedarse, y hemos visto un salto importante como consecuencia de la pandemia, pero la legislación viene estando preparada desde hace tiempo, y la proactividad es mayor porque a la intención se unen ahora las he-

rramientas para ayudarnos a hacerlo. Que se recoja en la normativa de 2015, por ejemplo, el formulario autocompletado, nos permite adelantarnos a lo que va a demandar el usuario. En la Comunidad de Madrid estamos viendo cómo podemos aprovechar la información que ya tenemos de los ciudadanos, cumpliendo con los requisitos de protección de datos, con las finalidades, usos y tratamientos, para avanzar en la proactividad. Hemos tenido dos casos de uso claros en este sentido, la oficina que se instaló para atender a los refugiados de Ucrania y, por otra parte, la Cuenta Digital, un expediente de datos interconectados de cada ciudadano".

Apuntaba José Antonio Garmón, que "la Administración es, en esencia, una prestadora de servicios, en muchos casos en régimen de monopolio con una clientela, los ciudadanos, que es cautiva, y de la que salen los propios empleados. Es una realidad diferente a la de la empresa privada. Con todo esto, se podría pensar en un cierto nivel de complacencia, pero no podemos quedarnos al margen de las demandas de los ciudadanos, pese a que el nivel de complejidad es mucho mayor que en el sector privado. Hablamos de centenares de procedimientos, y hemos avanzado mucho, aunque todavía tengamos camino por recorrer

"NO SE TRATA DE UNA MEDIDA O POLÍTICA CONCRETA, SINO DE QUE ESTA VISIÓN ESTÉ PRESENTE EN TODA LA ORGANIZACIÓN"

ANDRÉS GOMIS FONS (GENERALITAT VALENCIANA)

en la parte de análisis de la información. Es esfuerzo está siendo muy importante para mejorar la asistencia a los ciudadanos".

Por su parte, Andrés Gomis indicaba que "una Administración proactiva coincide en mucho con lo que podría ser un Gobierno inteligente. Tenemos mucho camino por recorrer, porque estamos poniendo las bases para estar más cerca del ciudadano. Hemos empezado con las políticas de Gobierno Abierto, aprovechando las TIC para democratizar las instituciones. Estamos en un momento importante porque estamos desarrollando nuevos sistemas de información más modernos y potentes, impulsando herramientas y cuadros de mando más potentes e impulsando un modelo de gobernanza del dato orientado a crear un sistema público de gestión de datos, que es la clave para ser más eficientes y proactivos. Es fundamental gestionar bien los datos de los ciudadanos. Esto será la base para el desarrollo de nuevos canales y herramientas".

Finalizaba esta primera ronda de valoraciones Roberto Magro, comentando que "tengo el sueño de que, a partir de los datos que el ayuntamiento tiene de mí, sea capaz de ofrecerme un servicio que me beneficie sin que yo lo solicite. Eso es realmente una Administración proactiva, y espero que pronto podamos conseguirlo, pero, para eso es necesaria la tecnología, una buena gobernanza del dato, personal preparado, unas normas que nos lo permitan... y el foco hay que ponerlo en las personas, y, aprovechando las experiencias vividas, estamos desarrollando un Plan Estratégico de cara a 2030. Ahí es clave cómo queremos relacionarnos con nuestro ayuntamiento, porque la tecnología es un medio para conseguir un fin. Estamos poniendo las bases de lo que queremos que sea el futuro".

UN CIUDADANO HIPERCONECTADO QUE QUIERE UN TRATO HUMANIZADO

La clave de todos estos retos está en el conocimiento del ciudadano. En este sentido, desde el Ayuntamiento de Alcobendas, Roberto Magro continuaba señalando que "es básico que el ciudadano se considere el centro, y tenemos que trabajar para que así sea. El Gobierno Abierto rompe moldes antiguos e integra las demandas de los ciudadanos, que quieren participar cuando ven que se atienden sus problemas en el entorno más cercano. Si nos alejamos del ciudadano, la participación disminuye. Tenemos que mejorar en el uso de la tecnología, pero no todos los ciudadanos son expertos, por lo que hay que mantener un mix analógico/digital en esta relación. E igual de importante es una adecuada gobernanza del datos. Pero es el momento de hacer, y, si, además les hacemos partícipes, es el ideal".

En el caso de la Generalitat Valenciana, comentaba Andrés Gomis que "no se trata de una medida o política concreta, sino de que esta visión esté presente en toda la organización, Y esto nos lleva a uno de los principales desafíos, la transversalidad y la integración entre el front-office y los servicios que hay tras ello. Para poder atender mejor a la ciudadanía, lo que hay que hacer es preguntarle y adaptarnos a los diferentes colectivos de ciudadanos. Pero la idea general debe ser acompañarlos en todo el proceso y tener en cuenta sus necesidades. Además, hay que aprovechar las posibilidades de la tecnología para conocer al ciudadano e ir más allá, pero es una visión global de la Administración, más allá de la tecnología".

"LA TECNOLOGÍA ES EL MEDIO PARA CUMPLIR UN FIN, PERO ES ESENCIAL EL CAMBIO CULTURAL EN EL QUE TENEMOS QUE TRABAJAR"

PABLO GARCÍA-VALDECASAS (COMUNIDAD DE MADRID)

Desde el Principado de Asturias apuntaba José Antonio Garmón que "nuestra experiencia es que la tecnología abre grandes oportunidades, pero es solo una herramienta para una visión de cómo debe ser esta relación. A día de hoy, hay departamentos que tienen este tipo de relación, pero son casos concretos que, además de las personas y las herramientas, tienen el compromiso con una forma de atender a la ciudadanía. No se trata de hablar de participación, sino de establecer los mecanismos para favorecerla y para realizar una escucha activa de lo que necesitan, que en el fondo es lo que tiene que hacer la Administración, resolver sus problemas".

En palabras de Pablo García-Valdecasas, de la Comunidad de Madrid, "es necesario tener una visión 360 transversal a toda la organización para ser capaz de trabajar de manera proactiva y, empleando tecnología, adelantarte a las necesidades que la ciudadanía va a tener. Por eso pusimos en marcha hace unos meses la Oficina 360 para ofrecer al ciudadano tantos canales como el usuario necesite. Pero no se trata solo de poner recursos, sino de actuar de forma proactiva para mejorar el servicio. Es la misma filosofía que queremos emplear en el nuevo servicio 012 de Atención al Ciudadano".

Para el Gobierno de Canarias, en la persona de Marta Saavedra, "hablamos de conceptos muy amplios, pero si recordamos la situación generada hace unos meses por el volcán en Canarias, vemos lo que supone montar una oficina de atención al ciudada-

“LA TECNOLOGÍA ESTÁ SIENDO UNO DE LOS ELEMENTOS QUE SUSTENTA EL TRABAJO DIARIO DEL GOBIERNO ABIERTO”

MARTA SAAVEDRA (GOBIERNO DE CANARIAS)

no integrando a diversas instituciones. Se puso en marcha en 40 días y atiende todo tipo de necesidades y ayudas. Esto nos ha enseñado que tenemos la capacidad para coordinarnos y solventar soluciones complejas. Pero hay otros ejemplos en marcha en nuestra comunidad. El concepto de la ciudadanía 360 pone a la persona en el centro, pero no sólo como receptor del servicio, sino como participante activo para ayudar en el diseño de estos servicios. Tenemos que avanzar en el desarrollo del gobierno fácil, porque es la forma de estar cerca de los ciudadanos”.

Y, desde el Gobierno de La Rioja, concluía esta ronda Axier Amo, que destacaba que “no pensamos solo en el Objetivo 16, sino también en el Objetivo 17, la creación de alianzas, para lo que es fundamental la cercanía y la confianza. La tecnología no es un objetivo, es un medio, y debe ser ágil, útil y fiable. Tenemos que pensar que sigue habiendo una brecha entre la ciudadanía y la Administración. Lo vemos como un reto vivo que tiene que dinamizar nuestras políticas. Pero el ciudadano de hoy no es el mismo de ayer ni será el de mañana, y la brecha también surge dependiendo del territorio. Estamos en el buen camino, pero hay que seguir trabajando”.

TECNOLOGÍA PARA APOYAR LA INNOVACIÓN

Indicaba Andrés Gomis que la tecnología no es lo esencial, “pero ofrece muchas más posibilidades de interactuación con la ciudadanía, para recopilar y organizar los datos, y para dotarnos de herramientas de analíticas y cuadros de mando que nos permitan tener un seguimiento constante de los comportamientos y hábitos de los ciudadanos, a la ver que mejora la rendición de cuentas. Además, nos facilita la automatización y la simplificación de algunas tareas”.

“SIGUE HABIENDO UNA BRECHA ENTRE LA CIUDADANÍA Y LA ADMINISTRACIÓN, Y HEMOS DE VERLO COMO UN RETO VIVO QUE TIENE QUE DINAMIZAR NUESTRAS POLÍTICAS”

AXIER AMO (GOBIERNO DE LA RIOJA)

Para Marta Saavedra, “la tecnología está siendo uno de los elementos que sustenta el trabajo diario del Gobierno Abierto. Se han modernizado mucho los portales, y lo hemos hecho pensando ya en el acceso desde el móvil. La usabilidad tiene que ser la clave. Así como la transparencia, que se ha consolidado con uno de los referentes del uso de la tecnología”.

Según explicaba Pablo García-Valdecasas, “la tecnología es fundamental, pero no debemos implementar todo lo que aparece nuevo, porque la interoperabilidad es y debe

ser la clave. Es una necesidad, pero no siempre se cumple. La tecnología es el medio para cumplir un fin, sin embargo es esencial el cambio cultural en el que tenemos que trabajar. Tenemos una ley preparada para mucho, pero no siempre un cumplimiento de todo lo que deberíamos. El problema no es solo de la tecnología, porque las empresas sí consiguen ser interoperables".

En palabras de Roberto Magro, "que la tecnología nos ofrezca la posibilidad de saber lo que el ciudadano hace cuando navega por la web, nos permite mejorar la toma de decisiones y mejorar el servicio. Pero los ciudadanos utilizan todos los canales, por lo que tenemos que poner el foco en responder a sus necesidades".

Añadía Asier Amo que "tenemos que mejorar la comunicación con la ciudadanía para entender exactamente cuáles son sus necesidades, para que el avance sea conjunto, no de cada uno por su lado o a diferentes velocidades".

Para cerrar esta ronda, José Antonio Garmón apuntaba que "tenemos muchos datos de la ciudadanía, pero hay que gestionarlos mejor para que sean realmente de utilidad para ellos. Esta información, además, nos puede ayudar a gestionar nuestra propia labor y recursos, lo que redunda en una mayor calidad del servicio que se proporciona. La tecnología nos ayudará mucho, pero sigue existiendo una brecha para muchos usuarios que, posiblemente, nunca acabará de cerrarse del todo, y esas personas no pueden quedar al margen del sistema, porque seguramente son las que mayor ayuda necesiten".

MEJORES PRÁCTICAS RECOMENDADAS

Desde la experiencia, Axier Amo destacaba que el ciudadano debe ver la transparencia "como una ventana de oportunidad", mientras que Roberto Magro añadía que "es el momento de rendir cuentas y debemos dar a conocer al ciudadano que tiene derecho a conocer y a pedir información".

Pablo García-Valdecasas apostaba por "la colaboración público-privada y la apuesta por la flexibilidad y la adaptación, y ofrecer al ciudadano el servicio antes de que nos lo pida", a lo que Marta Saavedra añadía "buena organización interna y creencia en los empleados públicos para poder transmitirla a la ciudadanía".

Finalizaban Andrés Gomis apostando por la "transversalidad y la idea de digitalización inclusiva", a lo que José Antonio Garmón sumaba "empatía con la ciudadanía, una nueva cultura que tenga en cuenta al ciudadano y le ofrezca participación en la toma de decisiones". ■

"TENEMOS QUE MEJORAR EN EL USO DE LA TECNOLOGÍA, PERO NO TODOS LOS CIUDADANOS SON EXPERTOS, POR LO QUE HAY QUE MANTENER UN MIX ANALÓGICO/ DIGITAL EN ESTA RELACIÓN"

ROBERTO MAGRO (AYUNTAMIENTO DE ALCOBENDAS)

CONTENIDO RELACIONADO

Foro IT User Administración Digital: "Tecnologías habilitadoras de un Gobierno Abierto"

SI TE HA GUSTADO ESTA REVISTA, COMPÁRTELA

SOLEDAD CAMACHO, DIRECTORA DE VENTAS DE SECTOR PÚBLICO DE SALESFORCE

"EL CIUDADANO DEMANDA DE LAS ADMINISTRACIONES INMEDIATEZ Y EFICACIA"

CUANDO HABLAMOS DE UNA ADMINISTRACIÓN PROACTIVA, LO HACEMOS DE CÓMO SE RELACIONA CON LOS CIUDADANOS Y DE CÓMO ES LA EXPERIENCIA DE ESTOS AL HACER USO DE LOS SERVICIOS PÚBLICOS DIGITALES, ADEMÁS DE LOS PASOS QUE SE TIENEN QUE IR DANDO PARA INCREMENTAR ESTE NIVEL DE PROACTIVIDAD.

Soledad Camacho habló en su intervención sobre la creación de un Sector Público digital y moderno. Clica en la imagen para ver el vídeo.

Y para hablar de esta proactividad de la Administración, en el Foro IT User Administración Digital: "Tecnologías habilitadoras de un Gobierno Abierto" contamos con la participación de Soledad Camacho, Directora de Ventas de Sector Público de Salesforce, que señalaba que el mundo "ha cambiado, acelerado por la pandemia, y creemos que no hay una vuelta atrás", y que nos encontramos en un momento en que "los ciudadanos nos hemos

distanciado de la clase política, la Unión Europea ha adquirido un mayor protagonismo, y, como ciudadanos, hemos cambiado nuestra percepción de determinados servicios públicos, y la comodidad es mucho más importante para todos que hace un tiempo".

DIVERSAS FORMAS DE RELACIONARSE CON LAS AAPP

En este momento, "conviven cinco generaciones digitales diferentes, lo que implica una relación diferente con la Administración y con las empresas privadas. E, incluso, aunque se relaciones digitalmente, utilizan herramientas diferentes para hacerlo. Por tanto, la Administración debe dar soporte a todas estas generaciones y a la forma en que quieren relacionarse con ella".

Salesforce ha hecho un estudio con Censuswide sobre el uso de la administración digital de la ciudadanía, y algunas de las conclusiones son "el incremento del uso, que los servicios no cumplen con las expectativas de los ciudadanos, y una peor valoración para la Administración más cercana al ciudadano y la Salud".

Según indicaba Soledad Camacho, "el 54% de los encuestados han usado al menos una vez los servicios digitales, principalmente en la franja de entre 45 y 54 años, pero solo un tercio encuentra esta experiencia satisfactoria".

INMEDIATEZ, EFICACIA, SENCILLEZ Y PERSONALIZACIÓN

En resumen, "el ciudadano demanda de las Administraciones inmediatez y eficacia, la digitalización es clave para ofrecer unos servicios públicos de calidad, y el futuro del Sector Publico es omnicanal y multicanal. Queremos que sea simple, predecible y confiable, pero la experiencia está fragmentada porque hay muchos silos de información. Cada interacción genera un nuevo silo, lo que genera una relación impersonal con el ciudadano, con lo que no se recoge información de ella ni se utiliza, lo que nos lleva a perder un conocimiento fundamental para tener una Administración más proactiva".

Por otra parte, "no existe conexión entre el mundo on-line y el mundo off-line, con lo que no hay una experiencia única y compartida entre todos los canales. Y falta proactividad por parte de la Administración en su relación con los ciudadanos".

Frente a esto, Salesforce apuesta "por una plataforma multicanal que convierte cualquier evento en información relevante para el ciudadano, independientemente del canal en que se produzca. Esto permite a la Administración tener una comunicación personalizada y proactiva con cada ciudadano, así como otras a grandes segmentos de población afectados por algún evento, o la posibilidad de ofrecer servicios o información necesaria para el ciudadano, antes incluso de que ése sepa que puede solicitarla".

Salesforce Citizen 360 "es una plataforma para conectar instituciones, empresas, ciudadanos y empleados, de una forma ágil, rápida y flexible, cubriendo áreas como el CRM, la atención al ciudadano, la comunicación digital con herramientas de automatización, comercio electrónico, analítica embebida, integración con los sistemas actuales, seguridad de la plataforma y de cualquier desarrollo... con herramientas que te permite sacar partido de datos alojados fuera de la nube de Salesforce. Creamos una vista de 360 grados de toda la información del ciudadano, con una interacción en tiempo real, sobre una plataforma ágil, flexible y extensible a nuevas funcionalidades. Y todo ello, con los niveles de protección adecuados". ■

CONTENIDO RELACIONADO

Foro IT User Administración Digital: "Tecnologías habilitadoras de un Gobierno Abierto"

SI TE HA GUSTADO ESTA REVISTA, COMPÁRTELA

WatchGuard | CYTOMIC

WatchGuard for SOC – Eficiencia y proactividad

Anticípate a las ciberamenazas en constante evolución

Threat Hunting

Ciber Resiliencia

Detección, investigación y respuesta

WatchGuard for SOC se basa en la combinación de soluciones de seguridad avanzada y plataforma de threat hunting para buscar, detectar y responder de manera eficiente a amenazas que hayan logrado evadir otras protecciones en endpoints, servidores, entornos virtuales y dispositivos móviles.

SEGURIDAD ENDPOINT AVANZADA

AUTENTIFICACIÓN MULTIFACTOR

NUBE SEGURA WI-FI

SEGURIDAD DE RED

Contacto: **900 840 407** **strategic.accounts@watchguard.com** **www.watchguard.com**

JOSÉ LUIS GARCÍA DÍAZ, RESPONSABLE DE SECTOR PÚBLICO DE VEEAM

"ASOCIADO AL DESPLIEGUE DE UN GOBIERNO ABIERTO, LO MÁS RELEVANTE ES EL DATO"

LA PRESTACIÓN DE SERVICIOS DE VALOR DENTRO DEL MARCO DE UN GOBIERNO ABIERTO TIENE ALGUNOS RETOS Y DESAFÍOS, COMO ES GARANTIZAR LA DISPONIBILIDAD DE ESOS DATOS ABIERTOS CON LOS QUE SE CONSTITUYEN LAS ESTRATEGIAS DE LAS DIFERENTES ADMINISTRACIONES.

Para hablar de estos retos, en el Foro IT User Administración Digital: "Tecnologías habilitadoras de un Gobierno Abierto" contamos con la intervención de José Luis García Díaz, Responsable de Sector Público de Veeam, que nos explicaba cómo dar la continuidad necesaria a los servicios basados en datos cuando surge algún incidente. En palabras de este portavoz, "asociado al despliegue de un Gobierno Abierto, es muy relevante el dato, porque este concepto no

José Luis García Díaz centró su presentación en los retos en la prestación de valor del Gobierno Abierto. Clica en la imagen para ver el vídeo.

es sencillo de implantar. Con la aceleración de la Transformación Digital, ahora estamos más cerca, pero no podemos olvidar que la principal moneda de cambio es el dato".

Si fijamos la vista en 2021, José Luis García Díaz apuntaba que "ha seguido creciendo la incertidumbre económica, si bien lo que más nos preocupa es lo que ha acontecido alrededor de la seguridad, y que nos muestra un 700% de crecimiento en los ataques de ransomware, y, asociado a ello, lo relacionado con la recuperación del dato. A esto se añade que mover cargas a la nube ya es una realidad madura, y esto es un apoyo para afrontar estos retos".

UNA MAYOR EXPOSICIÓN

Para el responsable de Sector Público de Veeam, "la arquitectura de los entornos que dan soporte a la prestación de valor se está complicando. La hibridación es una realidad, y cada vez más entidades consumen sus datos fuera de sus CPD, por lo que el perímetro a proteger es mayor. Con los datos del Data Protection Report que realizamos todos los años en la mano, empieza a haber un mayor número de caídas y de paradas de servicio, lo que en la práctica supone una mayor complicación para recuperar el servicio y la información. Como conclusiones de este informe, las migraciones de cargas a la nube y la apuesta por SaaS son tendencias importantes".

Si hablamos de la recuperación del servicio después de estos ataques y caídas, "vemos que un tercio de los servidores tienen caídas no planificadas, lo que implica fallos en el backup y la recuperación, porcentaje que se eleva a los dos tercios en este último caso. Si bien los sistemas y las cargas sí están migrándose a la nube, las plataformas de protección de datos no siguen el mismo ritmo, porque los sistemas legacy no facilitan abrazar estas nuevas tecnologías y entornos para mejorar la prestación de valor y de servicio".

RETOS A ASUMIR

Tal y como señalaba José Luis García Díaz, "los retos que tienen que asumir, tanto las entidades públicas como las empresas privadas, a la hora de aumentar la prestación del servicio y garantizar el negocio y, por tanto, el retorno en valor, son la seguridad, que es lo que más les preocupa; modernizar las estructuras de nuestro centro de datos para que los entornos legacy no sean un freno a la innovación; y seguir apoyándonos en la nube, dada la madurez en la propuesta y en la accesibilidad a los servicios".

En cualquier caso, las caídas de servicio, según los datos que maneja Veeam, se deben a múltiples razones, si bien la principal es, tal y como nos comenta, "la ciberseguridad, pero también hay errores de hardware, de software, de parcheado, de sistema operativo... Un dato significativo: la brecha de realidad. Es decir, ¿puede permitirse mi organización un retraso o pérdida de información en caso de caída? Son muy pocos gestores de TI que piensan que su brecha de realidad es pequeña, y el 90% piensa que es necesario hacer un esfuerzo para mejorar la plataforma de backup y restauración para garantizar unos tiempos y volúmenes de información acordes con las líneas de negocio". ■

CONTENIDO RELACIONADO

Foro IT User Administración Digital: "Tecnologías habilitadoras de un Gobierno Abierto"

SI TE HA GUSTADO ESTA REVISTA, COMPÁRTELA

MIGUEL CARRERO, VICE PRESIDENT,

SECURITY SERVICE PROVIDERS & STRATEGIC ACCOUNTS DE WATCHGUARD-CYTOMIC

"NO PUEDE HABER UN GOBIERNO ABIERTO SI NO HAY UN GOBIERNO SEGURO"

MUCHOS SON LOS FACTORES QUE INFLUYEN EN LA GENERACIÓN DE UNA ADMINISTRACIÓN ABIERTA Y MODERNA. ENTRE OTROS, UN MODELO DE TRABAJO FLEXIBLE, ADAPTADO A LA ACELERACIÓN DE LOS SERVICIOS CLOUD Y SEGURO PARA SU INTERACCIÓN CON LOS CIUDADANOS.

Para conocer más de cerca las posibilidades que ofrece este puesto de trabajo flexible, en el Foro IT User Administración Digital: "Tecnologías habilitadoras de un Gobierno Abierto" contamos con la participación de Miguel Carrero, Vice President, Security Service Providers & Strategic Accounts de WatchGuard-Cytomic, que nos explicaba que el objetivo de un Gobierno Abierto es que "los ciudadanos colaboren en la creación y mejora de unos servicios públicos que queremos consumir de una

Miguel Carrero explicó en su ponencia que una Administración abierta empieza por su modelo de trabajo y se apoya en una adecuada seguridad. Clica en la imagen para ver el vídeo.

manera lo más flexible y adecuada posible, desde cualquier elemento físico o digital".

Para este responsable, "no puede haber un Gobierno Abierto si no hay un gobierno seguro. Y debemos entender este gobierno como toda la Administración Pública que, con sus distintas piezas, ejerce esa función, y que, a la vez, está tremendamente interconectada con ciertos elementos del sector privado, sobre todo en instituciones con infraestructuras críticas".

GOBIERNO SEGURO

Las instituciones están haciendo un trabajo robusto en un escenario complejo con "el Esquema Nacional de Seguridad. Esto ofrece un marco de actuación a organismos públicos y empresas privadas, y es algo absolutamente crítico. En él se reflejan los elementos de ciberseguridad que deben ser tenidos en cuenta, y cómo se monta una seguridad racionada y efectiva. Además, hace especial hincapié en elementos como la consistencia o la interoperatibilidad entre los diferentes entornos, lo que es fundamental para los elementos de especialización y la compartición de inteligencia para una respuesta efectiva ante incidencias. Asimismo, la seguridad se consume como servicio, y esto es algo que aplica también a la Administración, como se incorpora en el Esquema".

"La seguridad", resumía Miguel Carrero, "está en la intersección entre las personas, las tecnologías y los procesos", y añadía que "quizá hemos tenido una fragmentación excesiva de la ejecución de la seguridad en las Administraciones, y no todas las instituciones tienen la masa crítica para tener las inversiones en tecnologías o la capacidad de atraer al talento. Por eso estamos convencidos de la necesidad de una red nacional de SOC federados, integrados y que comparten entre ellos, que darán servicios de seguridad a todas las instituciones. Hay que interiorizar la necesidad de la seguridad como servicio".

SEGURIDAD ADAPTADA A LA REALIDAD

Más allá de la teoría, la seguridad debe plasmarse en la realidad, y Miguel Carrero exponía un caso de éxito con la Conselleria de Sanidad de la Generalitat Valenciana, "que se vio en una situación específica cuando en 2020, de improviso, tuvieron que empezar a trabajar en un modo distribuido y heterogéneo, aunque ya sea una realidad que se mantiene como parte de ese Gobierno Abierto. Se trató de un cambio para el que no estaban preparados, con un entorno heterogéneo, poco controlado e, incluso, con equipos personales de los funcionarios. Pero, más allá de la tecnología, estuvo el factor humano y, por suerte, las personas son el elemento definitorio". En ese momento, "hubo que ver cuáles eran las necesidades básicas de seguridad para el trabajo en remoto. Y, en el caso que nos ocupa, hablamos de 24 departamentos, 29 hospitales, 37 centros de datos, 1.100 servidores y 35.000 equipos de usuarios... un entorno complejo que contaba con una seguridad que funcionaba hasta ese momento, pero que ya no servía para dar respuesta a la nueva necesidad. Hablamos de un momento en que había más de 50.000 alertas de seguridad, casi 1.500 ataques de malware, un 23,4% de equipos atacados activamente... y tener una solución para controlar esos ataques en una semana, es algo de lo que nos sentimos muy orgullosos". ■

CONTENIDO RELACIONADO

Foro IT User Administración Digital: "Tecnologías habilitadoras de un Gobierno Abierto"

SI TE HA GUSTADO ESTA REVISTA, COMPÁRTELA

ANTONIO SANTOFIMIA, DIRECTOR COMERCIAL DE MITEL

"LA SEGURIDAD GENERA CONFIANZA, Y, SIN ELLA, LAS MEDIDAS PARA ESTABLECER UNA RELACIÓN DIGITAL CON EL CIUDADANO PIERDEN EFICACIA"

LAS COMUNICACIONES SON FUNDAMENTALES PARA CONSTRUIR UN GOBIERNO ABIERTO Y SUSTENTAR PILARES COMO EL DE LA COLABORACIÓN. PERO ¿CÓMO ESTÁN EVOLUCIONANDO Y, CON ELLO, ACOMPAÑANDO LA PROPIA TRANSFORMACIÓN DIGITAL DE LAS ADMINISTRACIONES PÚBLICAS?

Para conocer en profundidad la realidad de las comunicaciones en el Sector Público, en el Foro IT User Administración Digital: "Tecnologías habilitadoras de un Gobierno Abierto", conversamos con Antonio Santofimia, Director Comercial de Mitel, que explicaba que ven cuatro retos. "Partimos de entornos complejos y diversificados, y el reto es que cada día sea más sencillo; vemos también un reto en el cambio de filosofía, porque, como con-

Antonio Santofimia explicó durante su intervención cómo tener unas comunicaciones modernas potencia el Gobierno Abierto. Clica en la imagen para ver el vídeo.

secuencia de los cambios de arquitectura que toma la Administración Pública para pasar de entornos distribuidos a entornos centralizados, se está dando entrada a soluciones tipo Cloud y se está produciendo un retraso en la toma de decisiones; un tercer reto es el presupuesto, que son limitados, lo que no quita que quieran hacer muchas cosas, lo que para nosotros, como proveedores, es un desafío importante; y el cuarto es la diferente velocidad del ciudadano digital, dado que nos encontramos con nativos digitales que demandan servicios avanzados a la Administración, mientras que existen otros usuarios que no se sienten cómodos en ese entorno, lo que implica mantener una doble velocidad para no dejar de lado a una parte importante de la población".

ARQUITECTURAS DE COMUNICACIONES MÁS DEMANDADAS

Ante esta realidad, apuntaba el Director Comercial de Mitel, "es necesario homogeneizar las soluciones. Desde un punto de vista de arquitectura, se pasa de modelos distribuidos a sistemas concentrados en uno o varios CPD. Básicamente, vemos modelos con infraestructura propia de la Administración o basados en proveedores de servicio. Hablamos de cloud que, mayoritariamente, es privado, aunque ya vemos soluciones de cloud público. En cualquiera de los casos, lo que quiere la Administración es que sea un despliegue seguro, con una posibilidad de retroceso sencilla, lo que provoca una gran demanda de servicios profesionales de alto valor".

Para Antonio Santofimia, "estamos viendo una apuesta por la Automatización y las soluciones Como Servicio. El objetivo es que el ciudadano sea capaz de iniciar y finalizar un proceso dentro de la Administración sin la intervención de un funcionario, siempre que la naturaleza del trámite lo permita. Otras de las exigencias del ciudadano son la inmediatez y la seguridad, porque sin confianza no se fortalece esta relación".

SEGURIDAD, UNA PRIORIDAD

"Más que una cortapisa, la seguridad es una prioridad", recalca Antonio Santofimia, "y lo demuestra el nuevo Esquema Nacional de Seguridad. Todos los proveedores debemos cumplir con esta normativa. Nosotros tenemos la certificación de máximo nivel, que se consigue con un elevado compromiso con la seguridad de los datos y de los procesos de los clientes. La seguridad genera confianza, y, sin ella, las medidas para establecer una relación digital con el ciudadano pierden eficacia".

Sin embargo, "lo que buscamos es que cada día sea más sencillo. Eliminar la complejidad".

Desde su punto de vista, "vemos una gran demanda de servicios profesionales, no solo en la puesta en marcha, sino en toda la vigencia del producto. Además, es fundamental la personalización, porque cada cliente tiene unas necesidades propias. Por último, es esencial la integración. El cliente no admite que un proveedor no se entienda con otros, con lo que la integración es un modo de asegurar la inversión realizada". ■

CONTENIDO RELACIONADO

Foro IT User Administración Digital: "Tecnologías habilitadoras de un Gobierno Abierto"

SI TE HA GUSTADO ESTA REVISTA, COMPÁRTELA

Comunicaciones y colaboración para la Administración Pública

EFICIENTES Y SEGURAS

Mitel apoya y personaliza la transformación tecnológica del sector público mientras protege sus sistemas heredados.

Mitel®
Powering connections

EDUARDO CARCEDO, RESPONSABLE DE ADMINISTRACIÓN PÚBLICA DE LOGITECH

"ES FUNDAMENTAL ESCUCHAR AL USUARIO PARA HACERLE PARTÍCIPE DEL USO DE LAS HERRAMIENTAS DE COLABORACIÓN"

LAS FORMAS DE COMUNICACIÓN Y COLABORACIÓN HAN CAMBIADO RADICALMENTE EN LOS ÚLTIMOS TIEMPOS. LA VIDEOLLAMADA SE HA CONVERTIDO EN UN MEDIO HABITUAL TANTO EN EL ÁMBITO EMPRESARIAL COMO EN EL SECTOR PÚBLICO, PARA RELACIONARSE CON EL CIUDADANO Y POTENCIAR SU PARTICIPACIÓN EN LOS SERVICIOS DIGITALES, O PARA ESTRECHAR LA RELACIÓN ENTRE FUNCIONARIOS.

En su exposición, Eduardo Carcedo mostró cómo la democratización de la videocolaboración puede hacer evolucionar a las Administraciones. Clica en la imagen para ver el vídeo.

Eduardo Carcedo, Responsable de Administración Pública de Logitech, explicaba en el Foro IT User Administración Digital: "Tecnologías habilitadoras de un Gobierno Abierto" que, con la pandemia, "tanto empresas como las instituciones tomaron decisiones para poder salir del paso y dar continuidad a la activi-

dad en la medida de lo posible. Esta situación inédita, dejó clara la falta de recursos y la necesidad de acelerar la Transformación Digital en el puesto de trabajo. Ahora, podemos ver más claramente los cambios en los entornos laborales, y es necesario analizarlos para tomar decisiones a futuro. Existen escenarios que plantean retos a las instituciones, y el desafío es que TI tome la decisión de implementar soluciones tecnológicas abordando la modernización de la Administración desde las necesidades y experiencias de los usuarios finales".

RESPUESTAS A ESTA PROBLEMÁTICA

En palabras de Eduardo Carcedo, "igual que las Administraciones invierten en plataformas de videocolaboración en la nube, deben acompañarlas con herramientas y soluciones que incrementen la usabilidad, haciendo al usuario partícipe de esa colaboración de forma sencilla. Es primordial la escucha de este usuario para no crear rechazo en ellos a la hora de emplear estas plataformas de colaboración".

Tras la experiencia vivida, y con la vista puesta en el futuro, señalaba Eduardo Carcedo que el puesto de trabajo digital debe "apoyarse en el análisis de todos los cambios que se han asentado en el entorno laboral tras la pandemia para acometer una verdadera transformación. Debemos atender diferentes requerimientos que permitan a las Administraciones Públicas ofrecer sus servicios de la mejor forma posible, adaptándose a las necesitades tanto del trabajador como del ciudadano solicitante de los mismos, tanto de forma remota como híbrida, y hacerlo de forma sencilla desde cualquier ubicación y dispositivo. Además, la seguridad debe ser un punto clave debido al manejo continuo de datos e información sensible".

SEGURIDAD REFORZADA EN EL PUESTO DE TRABAJO REMOTO

Según nos recordaba este responsable, "los ciudadanos estamos acostumbrados a utilizar múltiples plataformas sin el control por parte de TI, y es muy importante que dejemos de hacerlo y usemos estas soluciones con el mismo nivel de seguridad en el puesto remoto, la sala de reuniones, el dispositivo del individuo o una herramienta colectiva. Tendríamos que usar estos medios totalmente controlados bajo los parámetros de TI, y no cualquier al que pueda tener acceso el usuario. Hay que ofrecer a los usuarios las mejores y más amplias prestaciones, pero siempre con la seguridad en mente. Nosotros, por ejemplo, tenemos soluciones sobre Windows o sobre Android 10 con un nivel de seguridad que no permiten al usuario añadir elementos sin control del departamento de TI. Hay que delimitar estos equipamientos para la función que han sido creados, para asegurar la protección de los usuarios".

ESCRITORIO COMO SERVICIO

Para Logitech, "el escritorio es un elemento muy importante, porque el usuario quiere tener en casa lo mismo que en la oficina, pero cuando llegamos a esta, el ámbito es distinto. Queremos mantener la facilidad de uso para el usuario esté donde esté. Una forma puede ser la inclusión de auriculares con cancelación de ruido o de eco, o la posibilidad de evitar que se escuchen las conversaciones, al tiempo que generamos una imagen adecuada, y, a veces, las condiciones ambientales no son las más adecuadas. Sin las herramientas adecuadas, puede estar poniendo en riesgo la llamada o la información. La comunicación debe fluir sin alteraciones en el puesto de trabajo". ■

CONTENIDO RELACIONADO

Foro IT User Administración Digital: "Tecnologías habilitadoras de un Gobierno Abierto"

SI TE HA GUSTADO ESTA REVISTA, COMPÁRTELA

CARLOS TORTOSA, RESPONSABLE DE GRANDES CUENTAS DE ESET

"LA ADMINISTRACIÓN NECESITA UNA SOLUCIÓN ADECUADA PARA CUALQUIER TIPO DE AMENAZA"

LA CONFIANZA DEL CIUDADANO EN LAS INSTITUCIONES ESTÁ ESTRECHAMENTE LIGADA A LA SEGURIDAD DE LOS SERVICIOS DIGITALES QUE OFRECEN, Y CUANTO MAYOR ES ESTA, MÁS AMPLIA ES LA PARTICIPACIÓN Y EL NIVEL DE USO DE ESTOS SERVICIOS, CLAVES PARA LA TRANSFORMACIÓN DE LA ADMINISTRACIÓN PÚBLICA. PERO ¿CÓMO DEBE SER SU APROXIMACIÓN A ESTA SEGURIDAD? ¿QUÉ TIPO DE SOLUCIONES NECESITAN?

Carlos Tortosa centró su participación en el cambio necesario que debe producirse en las Administraciones. Clica en la imagen para ver el vídeo.

Con la vista puesta en la confianza, intervino en el Foro IT User Administración Digital: "Tecnologías habilitadoras de un Gobierno Abierto" Carlos Tortosa, Responsable de grandes cuentas de ESET, que explicaba que la "Administración Pública abierta tiene

una serie de implicaciones de seguridad, porque almacena y accede a datos personales de los ciudadanos, genera información sensible y de interés general, tiene obligaciones de cumplimiento normativo, y es objetivo de los ciberdelincuentes en todas sus modalidades".

RESPONDER A LAS AMENAZAS

Para mitigar todas estas amenazas, señalaba Carlos Tortosa que existen una serie de soluciones "como los Endpoint Protection Platform (EPP), Endpoint Detection and Response (EDR), Extended Detection and Response (XDR), Endpoint Detection and Response Maganed (MDR) o Sandbox personalizadas. Tenemos que pensar que toda esta tipología de ataques debe tener una solución adecuada a la que la Administración debe poder acceder".

En este sentido, "la Administración Pública necesita tener acceso a la mejor tecnología del mercado, debe utilizar soluciones certificadas, es necesaria una visión de 360 grados de todo lo que ocurre en la red y soluciones multicapa, la actualización de la tecnología debe ser constante, ofrecer servicios de calidad y ofrecer formación constante para los usuarios, no solo para el personal técnico, sino cualquier empleado público para que tenga unos conocimientos básicos para enfrentarse a posibles amenazas".

LA SEGURIDAD EN LA PRÁCTICA

Quiso Carlos Tortosa poner el foco en un caso práctico al que se enfrentaron en los meses de la pandemia en una entidad pública de un gobierno autonómico. "Este cliente tiene 8 sedes con unos 3.000 dispositivos administrados, pero no siempre el acceso era sencillo. Existían plataformas y tecnologías, y se necesitaba cubrir todo con una única solución que sustituyera a la que estaba instalada, y es un cambio que no hay que tener miedo a llevar a cabo. El cliente necesitaba elevar el nivel de protección, mejorar el rendimiento de equipos obsoletos, protección de dispositivos móviles, definir políticas de seguridad en base a diferentes criterios... y todo con un tiempo limitado para el despliegue que no podía superar las 4 semanas. Además, necesitaban una plataforma unificada y la formación de todo el personal técnico para adaptarse a la nueva solución".

Frente a esta realidad, la propuesta de ESET pasaba por "una solución unificada de Endpoint Protection Platform más un EDR, basada en módulos, en protección por comportamientos y en la nube. Hablamos de una de las soluciones certificadas que menos recursos de los dispositivos, que permite centralizar los dispositivos móviles y aplicar diferentes políticas desde una consola central unificada. Como el despliegue fue realizado por nuestros técnicos, no hubo problemas a la hora de cumplir los plazos exigidos, y se garantizó la formación del personal técnico del cliente".

A nivel de producto, "incorporamos ESET Protect para poder gestionar todas las herramientas integradas. Unas primeras herramientas fueron ESET Endpoint Security, para dispositivos, y ESET Server Security. Además, añadimos ESET Liveguard Advanced, nuestra herramienta sandbox que analiza cualquier archivo sospechoso antes de su entrada en nuestra red; y ESET Inspect, el EDR basado en procesos que nos ofrece visibilidad completa de todos los procesos que se detectan en cualquier equipo dentro del parque. Asimismo, añadimos el elemento de la gestión humana, convirtiendo este EDR en un MDR". ■

CONTENIDO RELACIONADO

Foro IT User Administración Digital: "Tecnologías habilitadoras de un Gobierno Abierto"

SI TE HA GUSTADO ESTA REVISTA, COMPÁRTELA

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

"ECHAMOS EN FALTA UNA MAYOR PARTICIPACIÓN DE LA SOCIEDAD EN LA DEFINICIÓN DE LAS ACCIONES INCLUIDAS EN EL PLAN DE RECUPERACIÓN"

LA PRINCIPAL HERRAMIENTA PARA AYUDAR A LAS ADMINISTRACIONES PÚBLICAS EN SU PROCESO DE TRANSFORMACIÓN DIGITAL Y EN SU CAMINO HACIA LOS OBJETIVOS DE UN GOBIERNO ABIERTO DEBERÍAN SER LOS FONDOS NEXTGENERATION, QUE DEBERÍAN SUPONER UN FUERTE EMPUJÓN PARA LAS INICIATIVAS QUE APORTAN AGILIDAD, FLEXIBILIDAD Y UBICUIDAD A LOS SERVICIOS PÚBLICOS DIGITALES.

José Miguel Muñoz comentó cómo los fondos NextGeneration deberían impactar en el Gobierno Abierto. Clica en la imagen para ver el vídeo.

Con la vista puesta en esta inyección económica, participó en el Foro IT User Administración Digital: "Tecnologías habilitadoras de un Gobierno Abierto" José Miguel Muñoz, Director del Foro de Colaboración Público-Privada, que nos explicaba que "los elementos que definen un Gobierno Abierto son

#FOROAAPPDIGITAL

la transparencia, la rendición de cuentas, la participación ciudadana, la integridad pública y a colaboración. El IV Plan de Gobierno Abierto 2020-2024 recoge mejoras y compromisos en todas las áreas mencionadas, y la situación actual de despliegue de este plan es que aproximadamente un 30% de las iniciativas están finalizadas, un 30% no se han arrancado y un 39% están parcialmente ejecutadas".

Además, teniendo en cuenta las conclusiones del Grupo de Estados Contra la Corrupción, GRECO, "de las 19 recomendaciones que el grupo hizo a nuestro país, ninguna de ellas fue satisfecha. Algunas de ellas contaban con soluciones o medidas parciales, pero en otras no se había hecho nada. Hay algunos avances, según el informe, y tenemos una nueva oportunidad con la nueva revisión, prevista para marzo de 2023. Greco reconoce las difíciles circunstancias, pero estiman que no son suficientes las medidas puestas en marcha".

MEDIDAS EN DIFERENTES ÁMBITOS

Apuntaba José Miguel Muñoz que, en el ámbito de la transparencia, "ni en el Portal de Transparencia ni en las indicaciones del Consejo de Transparencia, se recoge ninguna mención a los Fondos NextGeneration. Este Consejo de Transparencia, en septiembre de 2021, pidió que se diera más visibilidad a las acciones relacionadas con el Plan de Recuperación. En esa línea, el Gobierno ha empezado a publicar en la web oficial bastante información, actualizada periódicamente, sobre cómo se están repartiendo los fondos, o información somera sobre cómo se están ejecutando estos fondos. Hay cada vez más información, y esperamos que siga aumentando".

Hablando de la integridad pública, "el año pasado se publicó una orden que hacían especial hincapié en las medidas de detección y acciones contra el fraude, como la necesidad de que todas las entidades decisoras y ejecutoras de los fondos tengan un plan anti-fraude que vigile el ciclo completo y el impacto de las acciones, que implemente medidas para proteger al denunciante o las actuaciones que van a llevarse a cabo en caso de fraude. Otro aspecto destacado se refiere a disponer de una base de datos de beneficiarios de las ayudas que llegue al nivel de subcontratista. Sin embargo, a estas alturas no sabemos cómo está esta iniciativa".

Al poner el foco en la rendición de cuentas, comentaba José Miguel Muñoz, "se debe ir más allá de ofrecer un recuento de cómo se ha gastado el dinero, y analizar si las medidas han tenido los resultados y el impacto esperado en todos los aspectos importantes".

Asimismo, cuando nos centramos en la participación ciudadana, indicaba José Miguel Muñoz que "echamos en falta una mayor participación de la sociedad en la definición de las acciones incluidas en el Plan de Recuperación. Las manifestaciones de interés de los diferentes ministerios es lo más cercano a la colaboración ciudadana".

Por último, la colaboración, que, en opinión del Director del Foro de Colaboración Público-Privada, "debemos resaltar que el 50% de los presupuestos, aproximadamente, son destinados a comunidades autónomas y entidades locales, si bien están sujetos a las líneas maestras que marca el plan del Gobierno. Los PERTES sí buscan una colaboración público-privada, pero queriendo que sean las empresas las que financien estas acciones". ■

CONTENIDO RELACIONADO

Foro IT User Administración Digital: "Tecnologías habilitadoras de un Gobierno Abierto"

SI TE HA GUSTADO ESTA REVISTA, COMPÁRTELA

SOLUCIONES DE **VIDEOCOLABORACIÓN**

Las soluciones avanzadas de videocolaboración de Logitech permiten a los equipos mantenerse en contacto, trabajen desde donde trabajen.

SALVADOR ALARCÓN, DIRECTOR COMERCIAL DE SERVICIOS DE DOUBLETRADE

"LAS ADMINISTRACIONES NECESITAN CONTAR CON LOS MEJORES PROVEEDORES DE TI Y CONOCER TODOS LOS DETALLES DE INTERÉS A LA HORA DE LICITAR"

LAS INICIATIVAS DE GOBIERNO ABIERTO, LAS ESTRATEGIAS DIGITALES Y LOS PROYECTOS ALREDEDOR DEL DATO, SE APOYAN EN LA TECNOLOGÍA. EL MERCADO TI OFRECE MÚLTIPLES OPCIONES, Y LAS ADMINISTRACIONES NECESITAN INFORMACIÓN DETALLADA SOBRE LOS PROVEEDORES DE LOS DIFERENTES PROYECTOS PARA GENERAR LAS LICITACIONES.

Para hablar sobre la inteligencia comercial en el Sector Público, participó en el Foro IT User Administración Digital: "Tecnologías habilitadoras de un Gobierno Abierto", Salvador Alarcón, Director Comercial de Servicios de Doubletrade, que explicaba que el trabajo de su empresa consiste en "ayudar a las entidades a crecer mediante el uso de los datos", y añadía

Salvador Alarcón centró su ponencia en la inteligencia comercial en el Sector Público, y las ventajas del análisis de datos clave. Clica en la imagen para ver el vídeo.

que solo en seis meses, “hasta el pasado 30 de abril, han salido a licitación 4.500 millones de euros en el sector TI en 10.000 concursos. Esta es una de las ventajas del Sector Público, la cantidad de información que genera. Con este volumen de licitaciones, a veces puede ser un problema, sobre todo si no somos capaces de lidiar con todos estos datos. Pero, si conseguimos aprovecharlos, tendremos una gran ventaja competitiva, tanto como empresa licitadora como Administración Pública”.

“Los organismos”, continuaba, “necesitan hacer la mejor puntuación de proveedores, identificar las empresas que mejor pueda responder a las necesidades de sus convocatorias de licitación, así como conocer las iniciativas que se están llevando a cabo por otras Administraciones, y los precios de adjudicación y bajas para las categorías de servicio y productos de su interés. Definir la estrategia de compras ya no es una opción, pasa a ser una obligación para controlar las inversiones de la mejor manera posible”.

MONITORIZAR EL SECTOR PÚBLICO

Doubletrade tiene una visión acerca de “cómo monitorizar el Sector Público, generando KPI y definiendo vistas de la información con todos los datos claves de la licitación pública”, y, a modo de ejemplo, Salvador Alarcón repasó las licitaciones habidas alrededor de dispositivos de impresión.

En este sentido, “lo primero que podemos conocer es la evolución del volumen de licitaciones, así como la evolución de los CPV, o qué zonas tienen más concursos o licitaciones, así como ver la información exacta de una zona geográfica concreta. En un segundo paso, se puede analizar la baja media, tanto para todas las Administraciones como para un organismo específico. Asimismo, se puede conocer qué proveedores son los que están usando las Administraciones en un determinado tipo de producto, o ver todos los concursos que ha realizado un organismo en especial. Igualmente, podemos conocer el perfil de adjudicatarios de los diferentes CPV, tanto por ubicación como por número de empleados o cualquier otra segmentación, lo que nos permite tener una visión clara del tipo de beneficiarios de las licitaciones de un determinado producto de una determinada Administración”.

TOMAR VENTAJA DEL ANÁLISIS DE LA INFORMACIÓN

Otro aspecto interesante es conocer “la previsión del vencimiento de los contratos. Es importante tener una vista clara de los vencimientos y de las posibles prórrogas. Toda esta información viene de una base de datos para la que es muy importante investigar, capturar y mantener los datos del Sector Público, así como contar con la tecnología para centralizar, analizar y dar sentido a los datos”.

En definitiva, “las Administraciones necesitan contar con los mejores proveedores de TI, evitar los concursos desiertos, y conocer todos los detalles de interés a la hora de licitar, teniendo una visión clara de los proveedores y de lo que están haciendo otras administraciones. Es muy importante tomas decisiones basadas en datos, no en intuiciones”. ■

CONTENIDO RELACIONADO

Foro IT User Administración Digital: “Tecnologías habilitadoras de un Gobierno Abierto”

SI TE HA GUSTADO ESTA REVISTA, COMPÁRTELA

RAFAEL AYALA, EXPERTO EN GOBIERNO ABIERTO E INNOVACIÓN DE NEOKNOW, GESTIÓN DEL CONOCIMIENTO

"PODEMOS VER MUCHOS PROYECTOS INNOVADORES APOYADOS EN LA TECNOLOGÍA"

SON DIFERENTES LAS INICIATIVAS DE GOBIERNO ABIERTO QUE ESTÁN EJECUTÁNDOSE EN ESPAÑA EN LAS DIFERENTES ADMINISTRACIONES, Y CONVIENE TENER EN CUENTA LAS DIVERSAS TENDENCIAS QUE SE ESTÁN DIBUJANDO EN ESTE TERRENO EN NUESTRO PAÍS.

Rafael Ayala participó en el evento hablando sobre las tendencias de Administración abierta en España.

Para hablar de estas tendencias, participó en el Foro IT User Administración Digital: "Tecnologías habilitadoras de un Gobierno Abierto" Rafael Ayala, Experto en Gobierno Abierto e Innovación de NeoKnow, Gestión del Conocimiento, quien comentaba que "los numerosos ejemplos de prácticas de Gobierno Abierto en España son una oportunidad, desde el punto de vista de la tecnología. Durante la pandemia, hemos visto que vivimos una crisis de confianza que afecta a la ciudadanía

y al Sector Público. Como consecuencia de esta crisis, ha emergido una ciudadanía digital, también en nuestra relación con la Administración; existe una crisis económica y hay que ver cómo podemos aprovechar la oportunidad con la solidaridad y lo colaborativo, y el elemento digital va a ayudarnos".

Comentaba Rafael Ayala que en estos años "hemos visto que muchos de nuestras administraciones han sembrado iniciativas de Gobierno Abierto. Un ecosistema de gobierno sólido y pujante, que ha contado con la sociedad civil y el sector empresarial. Y, en este entorno, caminamos no solo hacia un Gobierno Abierto, sino hacia un Estado Abierto".

ELEMENTOS DEL GOBIERNO ABIERTO

Si repasamos los diferentes elementos del Gobierno Abierto, el primero es, tal y como apuntaba Rafael Ayala, la transparencia. Algunos ejemplos en este sentido serían "el portal de Gobierno Abierto y Comunicación de Castilla y León o el Govern Obert de la Generalitat de Cataluña, al igual que el Portal de Transparencia del Gobierno de España, o el Comisionado de Transparencia de Canarias, que ha incrementado la transparencia también para las entidades privadas. Pero también vemos otros casos en ayuntamientos pequeños, como el de Riba-Roja del Turia, con un portal de licitaciones muy innovador".

El segundo elemento, la participación, "se ha visto claramente durante la pandemia. Dos ejemplos claros son Decidim, con una gran evolución del software libre para la generación de herramientas de votaciones seguras, o el proyecto Madrid Sale al balcón. Otros proyectos interesantes son el Cliente Misterioso de la Diputación de Castellón, que ha aplicado la innovación para mejorar los servicios públicos, el de participación ciudadana del Ayuntamiento de Baracaldo realizado por Ibatuz, o el de la Comunidad de Murcia para promover la participación de niños y niñas".

Un tercer pilar de estas iniciativas es, nos recordaba Rafael Ayala, "la innovación abierta. Dentro de los laboratorios destaca el proyecto del Lab de Aragón (LAMB) con el modelo HIP, que abre la puerta a la posibilidad de colaboración del sector privado. Un claro ejemplo de este modelo es Frena la curva, que agrupó la participación de la Administración, de entidades privadas y del Tercer Sector, y se puso en marcha en tiempo récord".

En el caso de los Datos Abiertos, "ponemos el foco en la creatividad, porque alrededor suyo surgen una gran cantidad de iniciativas creativas que cada vez generan valor de forma más profesionalizada. Podemos hablar de los concursos de Datos Abiertos de la Junta de Castilla y León o de Euskadi, pero también de Asedie, como ejemplo de colaboración público-privada".

Si hablamos de colaboración, "además de la iniciativa Frena la curva ya mencionada, podemos mencionar The Participatory Group en Madrid, que es una forma de repensar la Administración y de atraer a otros agentes de la participación ciudadana", y si lo hacemos de Integridad, "no podemos olvidarnos de los tres grandes agentes, las agencias antifraude de Cataluña, Baleares y la Comunidad Valenciana, que son muy innovadoras en comunicación, formación y herramientas".

El gran reto es "la rendición de cuentas. Aquí encontramos el VisualGob del Gobierno de Aragón, uno de los ejes del Plan de Gobierno Abierto, que une esta rendición de cuentas a objetivos de desarrollo sostenible". ■

CONTENIDO RELACIONADO

Foro IT User Administración Digital: "Tecnologías habilitadoras de un Gobierno Abierto"

SI TE HA GUSTADO ESTA REVISTA, COMPÁRTELA

JAVIER FERNÁNDEZ RODRÍGUEZ,

DIRECTOR GENERAL DE SEGURIDAD Y ESTRATEGIA DIGITAL DEL GOBIERNO DEL PRINCIPADO DE ASTURIAS

"LA INNOVACIÓN TIENE QUE SER UN OBJETIVO EN SÍ MISMO, PORQUE LA ADMINISTRACIÓN DEBE SER UN ELEMENTO TRACTOR"

LAS DIFERENTES INICIATIVAS PUESTAS EN MARCHA PARA FAVORECER Y FACILITAR UN GOBIERNO ABIERTO TIENEN UN IMPACTO DEFINITIVO SOBRE LA CIUDADANÍA Y SOBRE CÓMO ÉSTA SE RELACIONA CON LA ADMINISTRACIÓN. UNO DE LOS EJEMPLOS DE TRANSFORMACIÓN QUE TENEMOS EN NUESTRO PAÍS ESTÁ EN EL PRINCIPADO DE ASTURIAS, QUE, RECIENTEMENTE, APROBABA SU ESTRATEGIA DIGITAL.

Con el fin de conocer los pilares de esta estrategia, quisimos contar en el Foro IT User Administración Digital: "Tecnologías habilitadoras de un Gobierno Abierto" con Javier Fernández Rodríguez, Director General de Seguridad y Estrategia Digital del Gobierno del Principado de Asturias, para poner el broche

Javier Fernández Rodríguez nos habló sobre la estrategia digital del Principado de Asturias y sobre los retos y desafíos que tienen que superar. Clica en la imagen.

#FOROAAPPDIGITAL

a este evento y que nos explicara que recientemente han aprobado una estrategia "que se apoya en 5 pilares fundamentales. Primero, la proactividad y la personalización de los servicios; segundo, la excelencia operativa; tercero, poner la innovación como un objetivo en sí mismo, no como una herramienta, porque la Administración debe ser un elemento tractor para la región; cuarto, basar estos servicios en la confianza, la seguridad y la robustez de la plataforma; y, quinto, la gestión del dato, eliminando los silos preexistentes y apostando por un dato único que podamos explotar para conseguir el resto de objetivos".

Esta estrategia apoya, tal y como nos explicaba Javier Fernández, "un Gobierno Abierto. Forma parte de una línea de confianza, que va por la seguridad, pero, también, para que los ciudadanos vean para qué se utilizan los datos. Los datos son de la ciudadanía, y deben ser susceptibles de generar información de lo que está realizando la Administración con una gestión transparente, y, además, ser aprovechados para otros proyectos".

TECNOLOGÍAS PARA SUSTENTAR ESTA ESTRATEGIA

Hablando de tecnología, "una parte fundamental es la Analítica de Datos. Primero, el ordenamiento, normalización y análisis de esos datos. A medida que pones en marcha procesos basados en esta información, llegas a Big Data, Machine Learning, a herramientas predictivas... pero necesitas entender por qué han pasado las cosas, para poder tomar decisiones, antes de poder predecir que va a pasar para tomarlas de cara al futuro. Todo lo que son herramientas de explotación de datos son fundamentales en esta dinámica".

Por otra parte, "para alcanzar la excelencia operativa y llegar a esa proactividad y a ofrecer una respuesta más ágil a las necesidades de la ciudadanía, entramos en la Automatización de procesos para interactuar con otros sistemas de la propia Administración o de otras entidades. De hecho, tenemos en marcha algunos pilotos para interactuar, en base a Blockchain, con otros sistemas. Asimismo, la Inteligencia Artificial es algo que ya está formando parte de las soluciones tecnológicas".

DESAFÍOS A AFRONTAR

Tal y como explicaba Javier Fernández, "el primer desafío que tenemos es que el proyecto que implantamos alcance todo el valor que pueda aportar porque lo utilicemos bien. De poco vale hacer una gran inversión en herramientas y aplicaciones si no ayudamos a quien tiene que utilizarlas a sacarles todo el provecho. Por tanto, la capacitación de los empleados públicos y de la ciudadanía es algo básico. Por otra parte, hablamos mucho de fondos, que ayudan a la puesta en marcha de iniciativas y proyectos, pero tenemos que construir proyectos sostenibles en el tiempo y que generen un valor que les permitan mantenerse".

Partiendo de su experiencia, Javier Fernández explicaba que "hemos intentado pensar los servicios en función de los objetivos que queremos alcanzar. En base a eso, construimos nuestra estrategia. A veces hay incertidumbres presupuestarias, y por eso hay que tener claro dónde quieres llegar, porque la financiación ayudará, pero no debe definir tu estrategia. Asimismo, es muy importante la constancia. Estar cerca de las áreas funcionales, para ayudar a transformar y optimizar estos servicios desde el conocimiento de ellos". ■

CONTENIDO RELACIONADO

Foro IT User Administración Digital: "Tecnologías habilitadoras de un Gobierno Abierto"

SI TE HA GUSTADO ESTA REVISTA, COMPÁRTELA

ALBERTO PASCUAL, DIRECTOR EJECUTIVO DE INGRAM MICRO ESPAÑA

"LA MEJORA DE LA EXPERIENCIA REQUIERE UNA GRAN INVERSIÓN EN TECNOLOGÍA Y SERVICIOS"

LA ADQUISICIÓN DE BIENES POR PARTE DE LA ADMINISTRACIÓN PÚBLICA SE AGILIZA MEDIANTE LOS ACUERDOS MARCO, QUE FIJAN UNA SERIE DE CONDICIONES O TÉRMINOS COMUNES PARA LA CONTRATACIÓN. DE ESTA FORMA, SE SIMPLIFICA LA GESTIÓN DE LOS CONTRATOS Y SE FACILITA LA ADHESIÓN DE ENTIDADES AUTÓNOMAS Y COMUNIDADES LOCALES.

La oportunidad que supone la venta de tecnología al Sector Público tuvo su protagonismo en el Foro IT User Administración Digital: "Tecnologías habilitadoras de un Gobierno Abierto" con la entrevista a Alberto Pascual, director ejecutivo de Ingram Micro España, que explicaba que el rol de su compañía es doble. Por un lado, somos un conector entre demanda y oferta, identificando todas las

Alberto Pascual explicaba las oportunidades que ofrece la venta de tecnología al Sector Público a través del Acuerdo Marco 13. Clica en la imagen para ver el vídeo.

oportunidades, haciéndolas especialmente visibles a los miembros de nuestro ecosistema de partners. Además, somos un agregador de soluciones, sumando las capacidades de nuestros resellers, las de nuestra comunidad de fabricantes, y complementándolas con las nuestras". En procesos de transformación tan complejos como los que enfrentamos, tanto desde el punto de vista tecnológico como administrativo, simplificar es esencial. Conseguir una interlocución única para el cliente, movilizando un complejo ecosistema, acelera la transformación".

Tal y como nos comentaba, "siendo la aceleración digital, una de las palancas clave para nuestra competitividad y cambio de modelo económico de país, el canal TI cobra un protagonismo esencial. El reto es de tal magnitud que difícilmente será abordable por una compañía en solitario. Hay que movilizar ecosistemas, y dotarles de recursos aprovechando nuestro tamaño, en aquellas capacidades para las que las economías de escala sean imprescindibles. Aportamos al canal conocimiento especializado tanto en áreas tecnológicas emergentes como en aquellas otras más tradicionales, donde los recursos de nuestro canal puedan verse desbordados. Ofrecer productos y servicios en pagos mensualizados es indispensable, y nuestro equipo de Financial Solutions lo hace simple".

Para el director ejecutivo de Ingram Micro España, "experiencias pasadas nos han enseñado que el tipo de estímulos económicos ofrecidos por NextGenerationEU se desaprovechan por dos razones: desconocimiento y complejidad en la gestión. Atacar ambos frentes constituye el pilar de nuestro Centro de Recursos Next Gen. Máxima visibilidad y proactividad en la comunicación de los fondos disponibles en cada iniciativa que se activa, buscador inteligente de ayudas, herramienta de diagnóstico digital comparado, habilitación de agentes digitalizadores y, sobre todo, centralización de todo el proceso de gestión, desde la solicitud hasta el cobro efectivo de la subvención".

"Para el Sector Público", añadía, "identificamos una necesidad adicional. El último Acuerdo Marco 13 presentaba unas exigencias de solvencia técnica y económica que excluían a figuras que aportaban gran valor a la Administración Pública y a la comunidad de fabricantes. Para hacer, además, más sencillos los procesos administrativos y de gestión del cobro, nos homologamos para ser agregadores de las soluciones y servicios construidos por nuestro canal".

PROXIMIDAD AL CLIENTE

La aportación del canal, "por su proximidad al usuario, es esencial en la comprensión de las necesidades reales de negocio de los clientes, en la prescripción de las soluciones más competitivas, y en el acompañamiento durante todo el proceso. La capilaridad que proporciona nuestra red de partners es la que garantiza un despliegue amplio y homogéneo de la transformación que se persigue, especialmente en un entorno tan atomizado como el de la PYME".

Los resellers que quieran aprovechar esta oportunidad, deben "no perder la perspectiva de la tecnología como un habilitador de los modelos de negocio de los clientes. La Transformación Digital es mucho más que tecnología. Supone nuevos modelos de negocio, nuevos modelos financieros y gestión del cambio. En estos aspectos deben formarse y diferenciarse nuestros partners, porque en esas áreas reside el verdadero valor, y la rentabilidad. ■

CONTENIDO RELACIONADO

Foro IT User Administración Digital: "Tecnologías habilitadoras de un Gobierno Abierto"

SI TE HA GUSTADO ESTA REVISTA, COMPÁRTELA

HIPERINTELIGENCIA PARA LA GESTIÓN DE DATOS EN EL SECTOR PÚBLICO

FERNANDO GUTIÉRREZ

ACCOUNT EXECUTIVE

DE MICROSTRATEGY

Algunos de los objetivos del Gobierno Abierto son incrementar la transparencia, colaboración y aumentar la participación de la ciudadanía; datos abiertos que redunden en el beneficio del ciudadano; y la recopilación de datos de diferentes zonas, entidades y organismos que facilitará y mejorará los modelos de Inteligencia Artificial que pretenden crearse para potenciar la experiencia y los beneficios que el ciudadano podrá obtener de los datos abiertos.

Para que esto suceda, es necesaria la interoperabilidad entre las diferentes Comunidades Autónomas y Organismos. Existen desafíos no tecnológicos, como la cultura del dato y la concienciación de la importancia que este dato tiene. Y, por otro lado, existen desafíos tecnológicos como son:

- Una visión única, un único diccionario para todo el mundo que facilite la interoperabilidad.
- Flexibilidad para facilitar la interoperabilidad y federar el dato.
- Puesto que el objetivo final es incrementar el beneficio que el ciudadano obtiene del dato abierto, la tecnología debe facilitar el acceso y el consumo de ese dato de manera sencilla, intuitiva y rápida.
- Por último, abrir el dato debe ir acompañado también de criterios de seguridad robusta.

Desde MicroStrategy trabajamos en múltiples referencias del Sector Público en solucionar esos 4 desafíos técnicos.

"MICROSTRATEGY HA DESARROLLADO UNA TECNOLOGÍA INNOVADORA LLAMADA HYPERINTELLIGENCE, QUE AYUDA A LOS ORGANISMOS PÚBLICOS A ALCANZAR EL OBJETIVO DE FACILITAR EL ACCESO A LOS CIUDADANOS AL DATO, CREANDO UNA VÍA SENCILLA, SEGURA, ESCALABLE Y RAPIDA"

¿CÓMO LO HACEMOS?

MicroStrategy es una arquitectura orientada a objetos, dispone de una verdadera metadata única, donde se define ese diccionario, catálogo de conceptos de negocio de manera única para todos los usuarios, asegurando una misma visión y definición. Esto favorece también el gobierno del dato y la reutilización a lo largo de las diferentes necesidades de negocio.

Para solucionar la interoperabilidad y esa flexibilidad necesaria para poder interoperar con otros sistemas de otros organismos, MicroStrategy, además de un gran número de conectores, ha apificado todo el producto, lo que permite que se pueda interaccionar con MicroStrategy desde aplicaciones de terceros y sistemas variados.

Además, con la capacidad anteriormente mencionada de un diccionario único, junto con la capacidad de ser un proveedor de datos de aplicaciones de terceros, MicroStrategy se

convierte en un hub de datos, que permite la federación del dato y ser consumido por diferentes canales y sistemas.

MicroStrategy ha desarrollado una tecnología innovadora llamada HyperIntelligence, que ayuda a los organismos públicos a alcanzar el objetivo de facilitar el acceso a los ciudadanos al dato, creando una vía sencilla, segura, escalable y rápida. No requiere de integraciones técnicas, y su despliegue es cuestión de 1-3 semanas.

Consiste en una o varias tarjetas que consolidan información de una o más fuentes, y aparece con tan solo pasar el ratón por encima de aquellos conceptos relevantes para el ciudadano, como, por ejemplo, datos tributarios, sanitarios, procesos judiciales... en cualquier aplicación que corra en un navegador o móvil. Asimismo, permite enriquecer otros aplicativos con datos que provienen de otras aplicaciones sin ningún desarrollo.

Otra manera en la que MicroStrategy ha colaborado con organismos públicos para facilitar el acceso al dato por parte del personal interno y del ciudadano, es con la capacidad de insertar datos en los portales existentes. Existen también casos en los que lo que se ofrece son ficheros en formato csv, Excel, PDF, e, incluso, JSON, para acelerar la creación de portales con datos abiertos y transparencias.

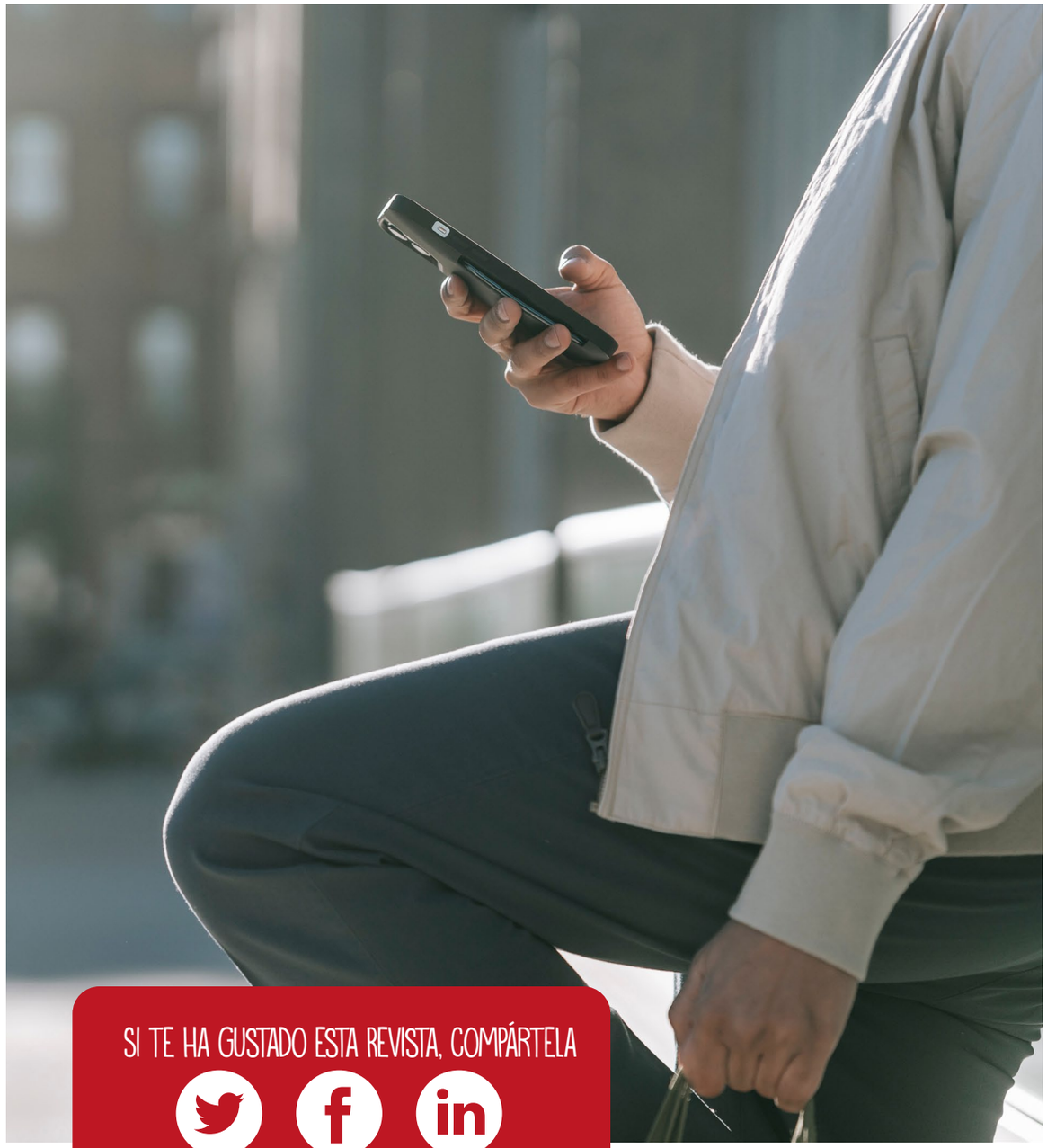
Por último, y no menos importante, la seguridad robusta, única y flexible que permite MicroStrategy para favorecer el acceso a los datos de manera segura. ■

CONTENIDO RELACIONADO

HyperIntelligence

De la HiperInteligencia a la HiperProductividad

Business Intelligence



SI TE HA GUSTADO ESTA REVISTA, COMPÁRTELA

EL USO DE SOFTWARE INTELIGENTE PERMITE ACELERAR EL ÉXITO DIGITAL

JOSÉ MATÍAS

DIRECTOR GENERAL
PARA ESPAÑA Y PORTUGAL
DE DYNATRACE

Resulta innegable que la demanda de servicios digitales se está disparando al mismo tiempo que los usuarios aumentan sus expectativas sobre ellos. De hecho, y según un informe de statista.com, está previsto que las organizaciones incrementen su inversión en transformación digital más de un 25% en sólo dos años, pasando de 1,3 mil millones de dólares de 2020 a 1,7 mil en 2022 para satisfacer la demanda de consumidores que buscan experiencias digitales eficaces y cada vez más satisfactorias.

Este ritmo acelerado de transformación ejerce una presión cada vez mayor sobre los equipos de DevOps que han de actuar con rapidez sin comprometer la calidad. Si hace pocos años su cometido era lanzar una gran actualización trimestral de software, ahora la expectativa es que cada día tengan disponibles varias actualizaciones con pequeñas mejoras. Esta presión es insostenible incluso para grandes corporaciones que representan los más altos estándares de experiencia digital.

La caída de Facebook el pasado octubre, que dejó a los usuarios sin acceso a sus servicios durante seis horas, es un ejemplo de cómo, incluso, un pequeño cambio en la configuración de la infraestructura digital genera el caos. Para que las organizaciones innoven sin perjudicar la experiencia del usuario, necesitan contar con soluciones modernas e inteligentes de desarrollo y actualización. Esto reduciría el riesgo de errores inesperados mejorando la calidad del código y aliviando la presión sobre los equipos de DevOps.

COMPROMETER LA CALIDAD POR LA VELOCIDAD

Los ciclos de innovación se han acelerado, de hecho, una investigación reciente de Dynatrace señala que las organizaciones esperan que la frecuencia de sus lanzamientos de software aumente un 58% en 2023. Pero a muchos les resultará difícil seguir este ritmo, ya que los equipos de DevOps han de seguir luchando también con las cargas de trabajo existentes, invirtiendo innumerables horas en el desarrollo de actualizaciones para cientos de variaciones en dispositivos, aplicaciones y sistemas operativos. Y a medida que crece la complejidad de los entornos de TI, la demanda de tiempo a los equipos de DevOps aumentará aún más.

Aun así, escribir código es solo la mitad del problema, ya que hemos de pensar también el tiempo necesario para hacer pruebas manuales consumen mucho tiempo y el necesario para gestionar un creciente número de herramientas cada vez más fragmentadas y la explosión de datos como resultado del cambio a la nube. Todos estos factores actúan contra el proceso de desarrollo. Con tanto que hacer y sin recursos adicionales, la presión sobre los equipos de DevOps puede poner en riesgo la calidad del código, incrementándose la probabilidad de que los errores de código se filtren a través de la red y poniendo en peligro los servicios digitales y las experiencias de los usuarios.

LOS PEQUEÑOS CAMBIOS TAMBIÉN IMPLICAN RIESGOS

Puede resultar difícil de comprender el verdadero impacto de una nueva versión de software hasta que se pone en marcha. Incluso, a menudo, es difícil revertir el cambio en caso de que cree un problema y volver a una versión anterior de la aplicación que haya demostrado su estabilidad.

Gran parte de este desafío se debe a la complejidad de los entornos multinube actuales. Los servicios digitales están compuestos por cientos de millones de líneas de código y miles de millones de dependencias, que abarcan múltiples plataformas y diferentes tipos de infraestructura. Esta interconexión dificulta que los equipos de DevOps comprendan las consecuencias de los cambios que realizan, por pequeños que parezcan. También se ha creado una sobrecarga de alertas, ya que las herramientas de monitorización en la nube capturan a alta velocidad un volumen y variedad de datos que va más allá de la capacidad humana de administrar. A menudo, es imposible para los equipos de DevOps encontrar rápidamente la única línea de código que ha desencadenado un problema.

UN ENFOQUE MÁS AUTOMATIZADO

Ante este panorama, las organizaciones necesitan incorporar inteligencia en el desarrollo de software si quieren evitar que el código de baja calidad llegue a la producción y garantizar así experiencias de usuario perfectas.

Deben comenzar por aplicar automatización continua en tareas repetitivas, lo que libera a los equipos de DevOps y les permite trabajar en actividades de mayor valor. En primer lugar, las organizaciones deben establecer niveles mínimos de calidad automatizados que midan los nuevos desarrollos en relación con los objetivos de nivel de servicio (SLO) para los indicadores clave de rendimiento. Esto significa que los nuevos cambios de código no pueden activarse a menos que cumplan con los mínimos requisitos para la experiencia de usuario, evitando un inesperado impacto negativo.

En caso de que algo salga mal, las organizaciones pueden mejorar el tiempo de resolución aprovechando las capacidades unificadas de observabilidad de principio a fin. Este nivel de seguimiento brinda a los equipos de DevOps información a nivel de código sobre todas las compilaciones de software, aplicaciones y servicios en cualquier plataforma en la nube, tanto si están en desarrollo o implementados.

La combinación de la observabilidad con AIOps y el uso de IA en las operaciones puede llevar los conocimientos un paso más allá, al priorizar automáticamente los problemas de acuerdo con su impacto comercial. Ello permite que los equipos de DevOps identifiquen rápidamente las alertas más urgentes y las resuelvan antes de que los usuarios experimenten un problema.

ALIVIAR LA PRESIÓN Y LOGRAR EL ÉXITO

Mejorar las prácticas de desarrollo a través de AIOps, la automatización y la observabilidad reducen significativamente la presión sobre los equipos de DevOps y les ayuda a seguir el ritmo de la transformación digital. A medida que las organizaciones continúan lanzando versiones de software cada vez más rápidamente, es vital integrar información de forma continua y automática en todo su entorno de servicios digitales para acelerar la transformación y ofrecer experiencias de software más fluidas. ■

SI TE HA GUSTADO ESTA REVISTA, COMPÁRTELA

LA EFICACIA Y SIMPLICIDAD QUE DEMANDA EL CIUDADANO LLEGARÁ SI LA ADMINISTRACIÓN DA UN PASO AL FRENTE EN TECNOLOGÍA

JESÚS GALINDO

AREA VICE PRESIDENT
SECTOR PÚBLICO
DE SALESFORCE

Uno de los problemas endémicos de la Administración Pública, no solo en España, sino en toda Europa, es que estas organizaciones funcionan con infraestructuras tradicionales, con información en silos y con un servicio al ciudadano que no es el que está demandando.

El ciudadano se ha acostumbrado a la inmediatez y a la eficacia de las empresas privadas a través de cualquier canal y busca lo mismo a la hora de realizar sus trámites con la administración. Lo cierto es que no está encontrando esa calidad en el servicio en su ayuntamiento, comunidad autónoma u organismo de ámbito estatal.

Si bien el 54% de la población afirma haber utilizado algún tipo de servicio digital de la Administración Pública, sólo el 29% siente que los servicios públicos digitales son de calidad. Por contra, el 35% afirma que los servicios digitales ofrecidos por la Administración son demasiado complicados y, casi un 9% sentencia que no sabe encontrar lo que necesita. Estas cifras fueron reveladas por un estudio realizado por la compañía de investigación Censuswide para Salesforce en el que participaron más de 2.000 personas de toda España.

Acabar con la complejidad y lograr que la Administración sea accesible para todos, salvando barreras de edad y residencia geográfica, debería ser un objetivo prioritario para el Sector Público. A tenor del estudio, el grupo de entre 25 y 34 años es el que mejor opinión tiene de la administración pública digital (32%) pero, aun así, por debajo de los que opinan que los trámites son demasiado complicados (35%). Los mayores de 55 años son los que peor opinión tienen de los servicios digitales en la administración, ya que, en este grupo de edad, los que consideran los trámites demasiado complejos ascienden a un 40%.

UNA ADMINISTRACIÓN MOBILE-FIRST

El futuro del Sector Público deberá ser omnicanal, con prioridad para los dispositivos móviles, que son utilizados principalmente por el 49% de los ciudadanos para realizar trámites con las entidades públicas. Al igual que ocurre en el sector privado, la posibilidad de ofrecer experiencias digitales conectadas, la unificación de los canales y la garantía del flujo de trabajo en todas las organizaciones de la Administración son cuestiones prioritarias. Se ha avanzado mucho en los últimos años en cuanto a nivel de atención, pero la Administración debe ser proactiva en su relación con el ciudadano, ofrecerle los servicios de forma personalizada y sacar el máximo partido del marketing digital.

La digitalización es fundamental para mantener unos servicios públicos de calidad. La tecnología se ha convertido en el aliado perfecto para un momento tan trascendente como el que afronta la Administración Pú-

blica. Ofrecer experiencias digitales conectadas, la unificación de los canales y la garantía del flujo de trabajo en los organismos que pagamos todos son cuestiones prioritarias.

Tanto si se trata de la tramitación de solicitudes de permisos de conducir como de urbanismo, los ciudadanos deben poder dirigirse a la Administración a través de una sola fuente, sin necesidad de navegar por varios departamentos y sistemas. Esto es posible utilizando una plataforma de participación flexible y escalable que ponga al ciudadano en el centro.

Además de dar prioridad a lo digital, una de las tareas principales de los gobiernos será ayudar a sus ciudadanos a convertirse en nativos digitales para que puedan aprovechar estas nuevas tecnologías y prosperar en la economía digital. En los próximos años se espera un aumento de la inversión en la mejora y el refuerzo de las competencias digitales de toda la sociedad. En 2022 muchas empresas se podrán aprovechar del Programa Kit Digital, impulsado por el Gobierno de España, por el que se regulan las ayudas para la digitalización de las pymes, con una dotación de hasta 3.000 millones de euros

AMPLIO MARGEN DE MEJORA

La progresiva adopción de tecnologías que faciliten las relaciones con el ciudadano acabará con la brecha actual detectada por el estudio que he citado anteriormente. La consultora preguntaba específicamente por las áreas de Salud, Agencia Tributaria y Educación para conocer la opinión de la población acerca de la digitalización de cada una de ellas. Según los resultados, los ciudadanos consideran que el área que más mejoras necesita es Salud (62%), seguida de la Agencia Tributaria (54%) y Educación (47%).

Respecto a los servicios que los usuarios mejorarían de la administración pública digital, simplificar los procesos para encontrar la información que se necesita es lo más deseado para un 46%. De hecho, preguntados sobre qué les gustaría poder hacer de forma más sencilla, rápida y segura en sus gestiones con la administración, los participantes mencionaron como primera opción la localización y descarga de documentos (52%) seguida de agendar citas para trámites (50%) y de tener todo en un único espacio virtual (44%).

Con el objetivo de lograr esa ansiada simplificación de los procesos, es importante aplicar una estrategia que permita a los empleados públicos acceder fácilmente a las aplicaciones y a los datos que necesitan para realizar su trabajo de la forma más eficaz, desde cualquier lugar. Para ello son vitales las herramientas de comuni-

“UNA DE LAS TAREAS PRINCIPALES DE LOS GOBIERNOS SERÁ AYUDAR A SUS CIUDADANOS A CONVERTIRSE EN NATIVOS DIGITALES PARA QUE PUEDAN APROVECHAR ESTAS NUEVAS TECNOLOGÍAS Y PROSPERAR EN LA ECONOMÍA DIGITAL”

cación, como el chat en directo y los servicios de asistencia digital. Con una plataforma segura y unificada, el flujo de trabajo adecuado y la hiper automatización, los organismos públicos mejorarán la experiencia de los empleados y de los ciudadanos.

Uno de los handicaps de las entidades públicas es el peso que en sus infraestructuras de TI tienen los sistemas heredados, que no están alojados en la nube. Sin embargo, tampoco esto es un problema porque existen tecnologías de integración como Mulesoft, que conectan los sistemas on-premise con capas de tecnología más user friendly, gracias a las API. Las innovaciones de MuleSoft y Salesforce están ayudando a los clientes a integrar y crear experiencias conectadas tres veces más rápido. Se trata de una oportunidad magnífica para que estas organizaciones modernicen las infraestructuras heredadas, lanzando nuevos canales digitales y creando entornos de API para ofrecer al ciudadano una visión de 360°.

TRANSPARENCIA Y SOSTENIBILIDAD

Los ciudadanos confían en el tratamiento seguro de sus datos por parte de los organismos públicos. Esta percepción la manifiesta un 77% de participantes en el estudio, frente a un exiguo 3% que no observa los servicios digitales como seguros. Por tanto, el Sector Público continuará apostando por la transparencia como una prioridad, ya que va íntimamente relacionada con la confianza que depositan los ciudadanos.

Durante la pandemia, las Administraciones que han contado con modelos de datos abiertos han demostrado ser las más ágiles y, por otra parte, los ciudadanos son más proclives a compartir más datos con la administración y a ser más abiertos. El uso eficaz de sus datos es esencial para crear una experiencia personalizada, pero también para ganar confianza, mejorar el compromiso y obtener los resultados de las políticas que se desean.

No es una cuestión desdeñable la ciberseguridad, ya que una pérdida de datos confidenciales podría lastrar para siempre la reputación de un organismo público. Una de las conclusiones del estudio de Censuswide es que el riesgo de ciberataques hacia la Administración Pública supone intranquilidad para el 66% de los encuestados, aunque sólo un 24% manifiesta sentir una “alta preocupación”. Por el contrario, un 3,5% de los participantes afirma no sentirse para nada preocupado por esta amenaza.

Para concluir, quiero aprovechar este espacio para poner de relieve que la Transformación Digital de la Administración tiene que estar conducida por un objetivo: la sostenibilidad. La sostenibilidad y el cuidado del medio ambiente son prioridades para Salesforce, que desde septiembre de 2021 es una empresa Net Zero (cero emisiones) en toda su cadena de valor, habiendo conseguido abastecerse en un 100% de energía renovable en todas sus operaciones.

Queremos ayudar a que el Sector Público en España logre también sus metas en este ámbito, gracias a Net Zero Cloud, una herramienta que permite a las organizaciones identificar las oportunidades más significativas para reducir su huella de carbono. ■

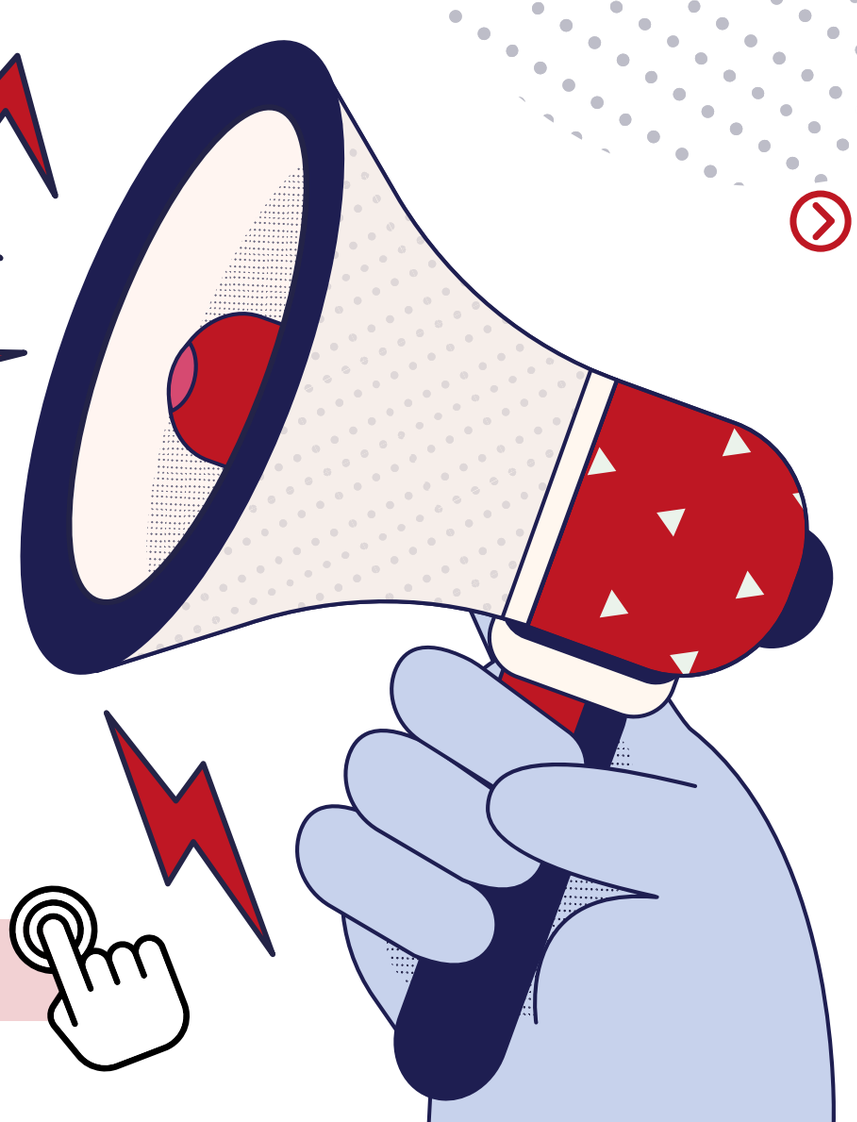
SI TE HA GUSTADO ESTA REVISTA, COMPÁRTELA

Administración Pública Digital

NUEVA WEB

¡VISÍTANOS!

www.administracionpublicadigital.es



¿A QUÉ RETOS SE ENFRENTAN LOS SOC EN CIBERSEGURIDAD EN LOS PRÓXIMOS MESES?

IRATXE VÁZQUEZ

SENIOR PRODUCT MARKETING MANAGER DE WATCHGUARD TECHNOLOGIES

Los SOC deben adelantarse a las amenazas sofisticadas y desconocidas. Su trabajo consiste en detectar y correlacionar comportamientos anómalos que identifiquen claramente un incidente de seguridad y responder lo antes posible.

El Centro de Operaciones de Seguridad (Security Operations Center - SOC) es el equipo de seguridad centralizado que emplea las herramientas necesarias para monitorizar y mejorar continuamente la postura de seguridad de una organización mientras previene, detecta, analiza y responde a alertas de seguridad. En este sentido, el SOC actúa como el "comando central" de la seguridad de la organización, de manera que aglutina toda su infraestructura de TI, incluidas sus redes, dispositivos o datos de la compañía, ya sean dentro del perímetro de lo que es la propia compañía como fuera de ella.

En los últimos años, los SOC han adquirido una enorme importancia, ya que las empresas -no importa el tamaño, el vertical en el que desempeñen su actividad o la geolocalización- se enfrentan a mayores riesgos de seguridad, debido al incremento del volumen y sofisticación de las ciberamenazas: ahora son capaces de eludir los más sofisticados controles de seguridad automatizados. Además, hay añadir la complejidad de la infraestructura a proteger, ya que se extiende la superficie de ataque exponencialmente, el volumen de alertas de seguridad a gestionar, la escasez de recursos con experiencia, cóctel que se ve agravado con la falta de presupuestos. Todo ello hace que la capacidad de defender a las organizaciones se vea negativamente afectada. Hasta tal punto es así la situación que, por ejemplo, Gartner ha pronosticado que para 2025 los ciberatacantes ya dispondrán de suficientes capacidades para afectar a las infraestructuras críticas hasta el punto de poder poner en peligro la vida de seres humanos.

En este sentido, los SOC deben ser capaces de adelantarse a las amenazas más sofisticadas y desconocidas que acechan a las organizaciones. De esta manera, son capaces de detectar y correlacionar comportamientos anómalos que identifiquen con claridad un incidente de seguridad y así pueden responder cuanto antes.

Sin embargo, las amenazas son cada vez más complejas y no todas las herramientas y soluciones para facilitar las tareas de los SOC son capaces de hacer frente a esta situación. A pesar de ser y estar diseñadas para esto, la avalancha de alertas que reciben los equipos obliga a que tengan que determinar si son reales o no. Esto da lugar a situaciones de fatiga de alerta por parte de los profesionales, que además de tener un coste operativo, pueden suponer fallos como dejar escapar amenazas o errores de diagnóstico. Por si esto fuera poco, también hay que sumarle la falta de talento cualificado y formación en ciberseguridad para poder gestionar este tipo de ataques.

Para hacer frente a estos retos, es imprescindible que los SOC cuenten con herramientas de ciberseguridad que les permitan ser lo más eficientes en su misión de defender a las organizaciones. Todos sabemos que, aunque las soluciones tradicionales de seguridad son necesarias, también somos conscientes de que por si solas son insuficientes. En primer lugar, porque sus alertas se basan en las amenazadas conocidas, por lo que pueden no tener en cuenta procesos sospechosos que no estén contemplados en sus registros y, por tanto, no detectar amenazas desconocidas. Y, en segundo lugar, tienen un enfoque reactivo con respecto a esos registros y no hacen búsquedas autónomas de otros posibles indicadores de ataque que permitan adelantarlos al incidente.

Es por esto por lo que los SOC deben complementar sus soluciones de ciberseguridad con herramientas avanzadas basadas en un enfoque proactivo, donde haya una búsqueda constante y automatizada de amenazas tanto conocidas como desconocidas, basadas en el threat hunting, la detección proactiva y la respuesta en las fases tempranas del ataque.

En el contexto actual, la propuesta de valor de WatchGuard for SOC se basa en esa combinación de soluciones de seguridad avanzadas y servicios gestionados proactivos para cazar, detectar y responder eficazmente a las amenazas que han podido evadir otras protecciones en ordenadores, servidores, entornos en la nube o dispositivos móviles. De esta forma pueden hacer frente a la fatiga de alertas, el crecimiento de la superficie expuesta a ataques, la complejidad del panorama de amenazas y los desafíos de la escasez de talento. De esta manera, se optimizan de la mejor forma posible las operaciones de seguridad de las compañías. ■

CONTENIDO RELACIONADO

WatchGuard for SOC

Threat Hunting

"LOS SOC DEBEN COMPLEMENTAR SUS SOLUCIONES DE CIBERSEGURIDAD CON HERRAMIENTAS AVANZADAS BASADAS EN UN ENFOQUE PROACTIVO, DONDE HAYA UNA BÚSQUEDA CONSTANTE Y AUTOMATIZADA DE AMENAZAS TANTO CONOCIDAS COMO DESCONOCIDAS"

SI TE HA GUSTADO ESTA REVISTA, COMPÁRTELA

ARISTÓTELES Y EL FALSO DILEMA DE CLOUD O NO CLOUD

ANTONIO SANTOFIMIA

DIRECTOR COMERCIAL
DE MITEL SPAIN

Dos conceptos tan dispares y lejanos en el tiempo como Aristóteles y la cloud - no hacen falta las presentaciones – pueden tener, sin embargo, muchos nexos dada sus naturalezas incontenibles, trascendentales y universales. La contribución del filósofo y científico griego es vastísima en áreas como la ética, la lógica, la retórica o la biología, pero yo querría fijarme hoy, y a riesgo de parecer reduccionista, en uno solo de sus principios: el del tercero excluido.

Vivimos en un mundo que ya ha empezado a rechazar el antiguo patrón de pensamiento dicotómico, sobre todo en el plano personal y en cómo nos definimos los seres humanos. En las esferas laboral, educativa y cultural, y tras la catarsis que ha supuesto la pandemia, la dualidad presencial-virtual ya se está difuminando, dando paso a lo que conocemos hoy como espacios y experiencias híbridos.

Sin embargo, cuando hablamos de cloud – una de las innovaciones más transformadoras de los últimos 25 años – pareciera que la elección se limita a cloud o no cloud. En el ámbito de las comunicaciones unificadas, da la sensación de que se ha asumido de forma generalizada que: uno, solo se puede escoger entre un modelo on-premise tradicional o la transición completa a cloud; dos, los modelos de comunicaciones on-premise están obsoletos y tres, y recurriendo de nuevo a Aristóteles, esto nos dejaría como única opción viable la de cloud.

Sin embargo, la opción de implementación en la nube, entendida como la nube pública, no es válida para todos. Es cierto que cloud es el principal habilitador de transformación por su rapidez y escalabilidad y que brinda muchas ventajas: reducción de costes, nula o mínima inversión inicial, pago por lo que se usa, se necesitan menos recursos para su gestión... Igual de cierto es que una solución cloud al uso no brinda mucha capacidad de personalizar las funcionalidades de modo que se adapten a las necesidades únicas de cada negocio, que se pierde el control sobre las evoluciones tecnológicas de una plataforma, que puede que no haya costes de inversión o de puesta en marcha pero que, a medio/largo plazo, surgen muchas dudas sobre si el coste es menor que en un modelo OPEX...

Muchas organizaciones van a seguir modernizando las soluciones de UC on-premise y demandando soporte continuo durante muchos años. Pero, para muchos clientes, a medio y largo plazo, la nube pública puede no ser una opción factible por razones de seguridad, supervivencia, soberanía de datos, conformidad normativa y otras leyes o normas específicas de cada país. Esto es especialmente relevante en sectores altamente regulados como pueden ser las Administraciones Públicas.
Por lo tanto, cuando nos alejamos un poco del foco y se amplía la perspectiva, es notorio que la flexibilidad y capacidad de elección es lo que debe predominar.

EL FALSO DILEMA

¿Por qué tengo que elegir entre cloud o no cloud? ¿Por qué no que-

darse con lo mejor de los dos mundos? Citando de nuevo a Aristóteles, ¿por qué no buscar la virtud en un punto intermedio? En este contexto, el punto medio podría ser, por ejemplo, un modelo de cloud privado que proporcione un entorno seguro y redundando, ya sea en las instalaciones de un proveedor de servicios especializado o en nuestra propia casa, pero gestionado por partners de confianza. Un despliegue de estas características va a implicar un menor coste de recursos técnicos/humanos, pero al tiempo supondrá una menor pérdida del control ya que cedemos la gestión de nuestra plataforma, pero no la capacidad de decidir qué y cuándo evolucionar. En términos económicos, el cloud privado proporciona, además, un equilibrio ideal entre la compra de un bien y la inversión en un servicio a través de la adquisición en un modelo de suscripción.

Hoy en día, cuando las organizaciones evalúan sus necesidades de infraestructura de comunicaciones, lo que realmente importa, más allá del tipo de despliegue, es centrarse en aumentar la eficiencia, mejorar la capacidad de gestión, cumplir con los requerimientos en materia de seguridad y normativa y considerar las inversiones existentes. Y, todo ello, diseñado para para respaldar a los empleados en cualquier tipo de entorno de trabajo.

En Mitel tenemos la misión de ofrecer soluciones de comunicaciones flexibles y preparadas para el futuro que apoyen las necesidades de cada cliente. Un tipo de solución, o un solo sabor de nube, no sirve para todos y Mitel tiene un firme compromiso de apoyar a los clientes a lo largo del ciclo de vida de sus comunicaciones ofreciendo la máxima flexibilidad y elección. Para ello, el catálogo de soluciones de Mitel está disponible de la forma en que los clientes prefieran adquirirlas, sin obligar a rupturas tecnológicas al tiempo que protege los sistemas heredados: opciones de CAPEX, opciones de suscripción y una gama completa de opciones de implementación privadas, híbridas y on-premise.

“LAS EMPRESAS FLEXIBLES SUELEN ADAPTARSE A LAS CONDICIONES CAMBIANTES DEL MERCADO DE FORMA RÁPIDA Y SENCILLA, Y LA CAPACIDAD DE ADAPTARSE A MENUDO PUEDE SER LA CLAVE DEL ÉXITO A LARGO PLAZO”

En los negocios, la flexibilidad es importante. Las empresas flexibles suelen adaptarse a las condiciones cambiantes del mercado de forma rápida y sencilla. Y la capacidad de adaptarse a menudo puede ser la clave del éxito a largo plazo. La pandemia fue un duro recordatorio de esta realidad. ■

SI TE HA GUSTADO ESTA REVISTA, COMPÁRTELA

VIDEOCOLABORACIÓN, CLAVE PARA LA MODERNIZACIÓN DE LAS ADMINISTRACIONES PÚBLICAS

EDUARDO CARCEDO

RESPONSABLE DE ADMINISTRACIÓN PÚBLICA DE LOGITECH VÍDEO COLABORACIÓN

La crisis sociosanitaria trajo consigo obstáculos inesperados para el grueso de la sociedad. Administraciones y organizaciones de todo tipo se lanzaron a tomar decisiones aceleradas sin una estrategia planificada, para poder salir del paso y, por tanto, dar continuidad a la actividad en la medida de lo posible de forma telemática o bajo modelos de trabajo híbridos.

Una situación inédita que dejó clara la falta de recursos y la necesidad de acelerar el proceso de transformación digital en los puestos de trabajo. En este marco y con la perspectiva de lo vivido durante estos últimos años, podemos ver más claramente los cambios que la Covid-19 ha ocasionado en entornos laborales y en las necesidades de la Administración Pública.

Ahora, ha llegado el momento de analizar los cambios y tomar decisiones con una visión de futuro que permita modernizar el ecosistema de trabajo de las Administraciones Públicas. Todo ello, con la premisa de ofrecer servicios, tanto en remoto como en formato híbrido, de forma sencilla y desde cualquier ubicación y dispositivo. Pero, además, fomentando la productividad y sin olvidar la securización de todo el entorno de trabajo. Este último, un punto indispensable, teniendo en cuenta el manejo continuo de datos sensibles.

Esta metamorfosis de las Administraciones Públicas plantea retos y problemas. Para minimizarlos, es necesario que los departamentos de TI encabecen la toma de decisiones a la hora de implementar soluciones y herramientas tecnológicas, abordando la modernización de la Administración Pública desde las necesidades y experiencias reales de los usuarios finales.

La clave está en implementar soluciones y herramientas que permiten a cualquier empleado o equipo de trabajo colaborar a distancia, con compañeros y equipos de la misma empresa, o terceros, desde la sencillez y compatibilidad con otros dispositivos y plataformas, con flexibilidad e interoperabilidad, para adaptarse a todas las necesidades, y accesibles a cualquier presupuesto.

Herramientas como webcams y auriculares profesionales para equipar el espacio de trabajo personal, especialmente relevantes en modelos de trabajo híbrido o remoto; como es el caso de webcams como Logitech Brio o auriculares empresariales como los Zone Wireless; pasando por Logi Dock, una estación todo en uno con altavoz integrado para videollamadas, que reduce la acumulación cables en el escritorio y contribuye a la productividad de quienes trabajan remotamente; hasta avanzadas soluciones de videocolaboración para salas, tales como Rally Bar, nuestra más moderna barra de video todo en uno; que facilitan el acercamiento de equipos que están en diferentes sedes, con el fin de reducir el número de viajes para el seguimiento de los proyectos.

Toda una serie de soluciones que están resolviendo muchos retos de transformación que afrontan hoy en día las Administraciones Públicas, con necesidades y perfiles de uso muy distintos, que pueden encontrar, gracias al desarrollo de esta industria, la alternativa más indicada para cada uno de ellos consolidando, a su vez, la transformación del entorno de trabajo de las Administraciones hacia una visión de futuro que ya es del presente. ■

Tecnologías habilitadoras de un Gobierno Abierto

VER

ORGANIZA

FORO ADMINISTRACIÓN PÚBLICA

it User

SOCIOS ESTRATÉGICOS

Foro CPP colaboración público-privada TECNOLOGÍA & INNOVACIÓN

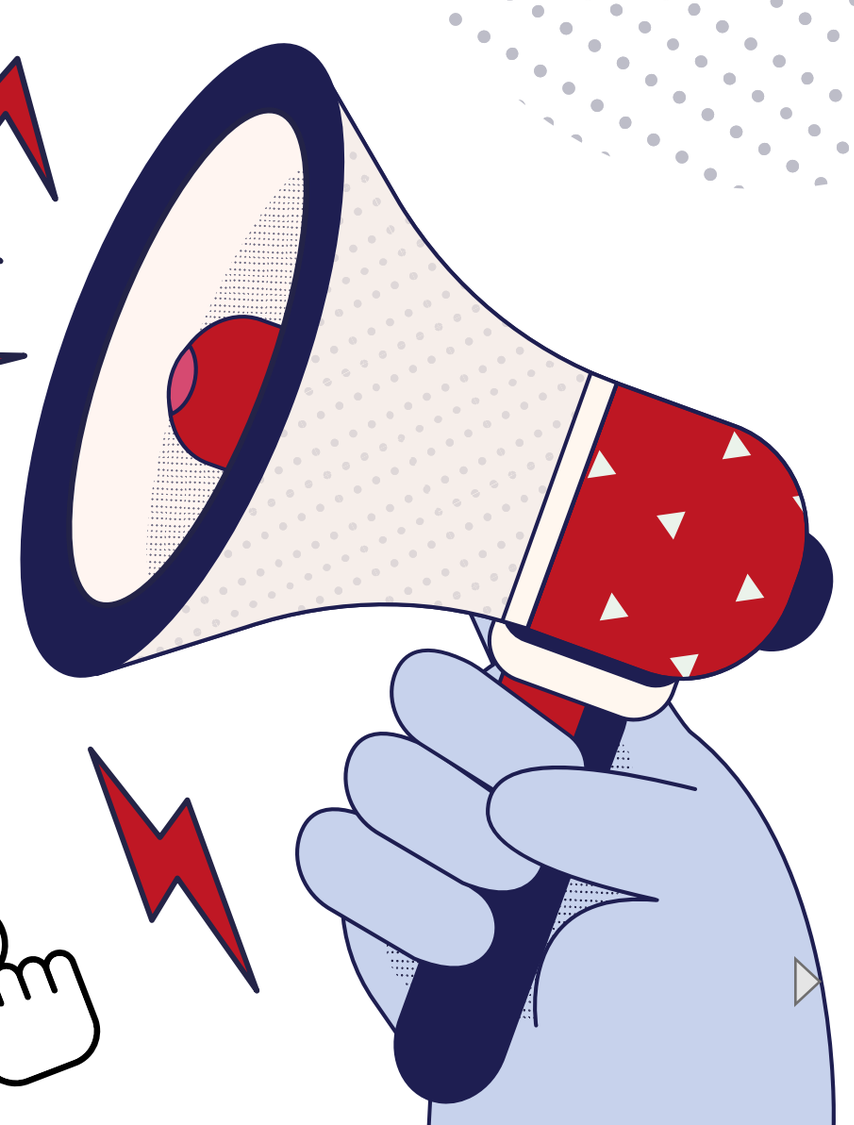
Astic

Administración Pública Digital

NUEVA WEB

¡VISÍTANOS!

www.administracionpublicadigital.es



Empleado formado, empresa segura

E. Frechoso Muñoz

Al hablar de empoderamiento empresarial se hace referencia a las nuevas corrientes de negocio en las que se aplican estrategias de gestión laboral que conceden una gran autonomía a los empleados para conseguir mayores niveles de compromiso, motivación y satisfacción, factores que redundan en una mayor productividad. Es una tendencia que se está imponiendo, pero ¿qué consecuencias tiene esto para la organización desde el punto de vista de la ciberseguridad? ¿Se puede hablar de empleados empoderados realmente? Y lo más importante ¿cómo se empodera a las plantillas en entornos de trabajo híbridos y ante un panorama de amenazas descontrolado? La clave puede estar en la formación. Permitamos que los empleados detecten las amenazas y protejan a la organización.

Modernizar su lugar de trabajo mediante la adopción de tecnologías móviles y en la nube puede ser una experiencia liberadora tanto para los profesionales de TI como para los empleados. Sin embargo, a medida que la empresa adopta esta libertad sin ataduras, aumenta su superficie de ataque y debe asegurarse de salvaguardar la información, los procedimientos y, por supuesto, a los trabajadores. ¿Cómo? La respuesta puede parecer sencilla, aunque esto no significa que sea fácil.

Establecer una estrategia de ciberseguridad que contemple el despliegue de soluciones que cubran todo el espectro de la infraestructura de TI de la compañía, contar con el apoyo de expertos en la materia y apostar por la formación y concienciación para empoderar al empleado, deben ser los ingredientes principales en esta receta. Es cierto que hay muchos otros elementos a tener en cuenta, pero nos centraremos a continuación en el último de ellos, la formación, pues es uno de los pilares fundamentales para combatir las amenazas y erradicar malas praxis entre todos los integrantes de la empresa, sea cual sea su responsabilidad.

¿Sabía que uno de los mayores agujeros de seguridad tiene que ver con la falta de conocimiento no técnico? No todos los empleados de una organización tienen que ser expertos en TI. Pérdida de información confidencial, fugas de datos, robo de credenciales, infecciones provocadas por distintos tipos de malware, errores en el uso del correo electrónico o las redes sociales, exposición de información por no contar con políticas de mínimos privilegios, daños económicos y de reputación, son solo algunos de los riesgos a los que se enfrentan los negocios en el día a día.

Está claro que un parte importante de los problemas de ciberseguridad de una organización no existirían si su plantilla tuviera interiorizados hábitos de trabajo diario seguros, especialmente en los entornos laborales híbridos actuales, y contaran con nociones básicas de las amenazas existentes para saber cómo identificar a algunas de ellas y reaccionar ante situaciones que podrían evitar consecuencias nefastas para el negocio. Los empleados son el motor de las organizaciones, los que hacen posible su funcionamiento y a diario se enfrentan a un entorno de trabajo cada vez más digitalizado. De ahí que sea clave conocer las

COMPARATIVA DE EMPRESAS SOBRE LA CONCIENCIACIÓN EN CIBERSEGURIDAD

CLICAR PARA VER EL VÍDEO

En el mundo interconectado actual, ignorar la ciberseguridad ya no es una opción viable ni para para los empleados ni para las organizaciones

situaciones más comunes que se dan en la empresa, relacionadas con la seguridad del entorno de trabajo de los empleados para poder así minimizar el riesgo de amenazas para la organización y preservar la protección de los datos cumpliendo con las diferentes normativas.

El empleado o el mito del eslabón más débil

Proteger de las ciberamenazas se ha convertido en un juego de locos. Los equipos de TI y seguridad no solo tienen que mantener una vigilancia constante de sus ciberdefensas, sino que también tienen que comunicar estos riesgos a los directivos para asegurar presupuestos suficientes, y ponerse en la piel del departamento de Recursos Humanos para buscar los conjuntos de habilidades necesarias. El papel del CISO se complica cada vez más y la demanda de soluciones de seguridad nunca ha sido tan alta, pero también de los programas de formación en ciberseguridad para ayudar a las empresas a proteger a sus plantillas y a sí mismas de las últimas ciberamenazas.

"Una organización es tan vulnerable como el más vulnerable de sus empleados. Más allá de concienciar a los trabajadores de que son el factor más débil, también es interesante hacerles saber que pueden actuar como guardianes de la seguridad de su compañía", apunta Chester Wisniewski, investigador principal de Sophos. "1.000 empleados pueden ser percibidos como 1.000 objetivos para los atacantes, pero también pueden ser utilizados como sensores remotos desplegados que pueden ser indicadores tempranos de cualquier compromiso en la red".

Si bien es cierto que los usuarios todavía no están lo suficientemente capacitados para su papel en la ciberdefensa, su concienciación en materia de seguridad va en aumento, tal y como se extrae del informe Voice of the CISO de Proofpoint, que revela que el 53% de los CISO españoles cree que los empleados entienden su papel en la protección

"1.000 empleados pueden ser percibidos como 1.000 objetivos para los atacantes, pero también pueden ser utilizados como indicadores tempranos de cualquier compromiso en la red"

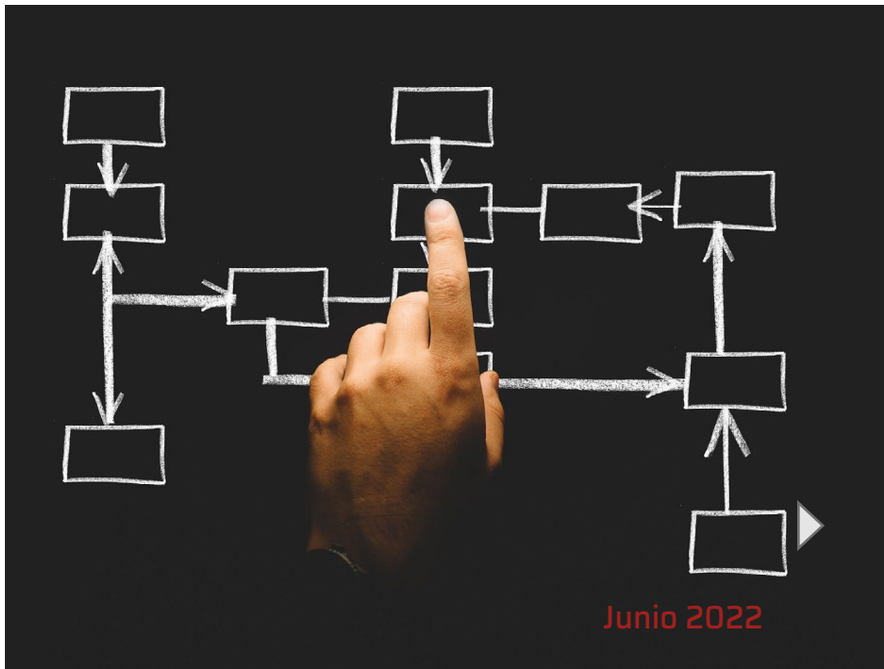
Chester Wisniewski, investigador principal de Sophos

de su organización frente a las ciberamenazas, y solo el 48% de ellos considera que el error humano es la mayor vulnerabilidad de su organización. "Consecuentemente, el 50% de las organizaciones aumentó la frecuencia de sus programas de formación y concienciación en ciberseguridad", explica Nuria Andrés, estratega de ciberseguridad para España de la compañía.

Con la evolución de las nuevas tecnologías, los usuarios han llegado a un punto en que se han visto cada vez más expuestos tanto a nivel personal como profesional, e incluso forzados a un cambio que en ocasiones crea más incertidumbre que confianza. En este sentido, Estefanía Macías, la responsable de Secure&Academy, el Centro Avanzado de Formación en Ciberseguridad de Secure&IT, dice que "los usuarios son cada vez más conscientes de que depende de ellos no permitir ser engañados y poner obstáculos a los ciberdelincuentes, como por ejemplo, utilizando contraseñas más seguras para dificultar el acceso a los sistemas o la información. Es más, tras acciones formativas y auditorías de seguridad y hacking ético se percibe que los usuarios que participan son los más entregados en comunicar la menor sospecha de ciberataque al departamento de TI para evitar un incidente de seguridad mayor".

En la misma línea se muestra Carlos Becerra, socio fundador de CB Universal y Cyber Security Speed, que opina que "los empleados se dan cuenta cada vez más de que representan una gran superficie de ataque y que son uno de los principales vectores de ataque y, por tanto, son más conscientes de que tienen que seguir formándose y desconfían más de cualquier email que reciben consultando con TI/Seguridad con más frecuencia que antes".

Mientras, desde Kaspersky señalan que no siempre el empleado es consciente de que es uno de los principales vectores de ataque, ya sea por desconocimiento o porque confían en las medidas de ciberseguridad implementadas por su empresa. "Hay veces que sentirse respaldado o protegido



por los sistemas de ciberseguridad de las empresas puede dar lugar a descuidos. Por esto es tan importante recurrir a las herramientas de concienciación y hacer un llamamiento a los empleados para que sean prudentes de los ataques de los que pueden ser víctimas", comenta Alfonso Ramírez, director general para Iberia de la compañía.

Evidentemente, todas las empresas hoy en día son susceptibles de caer ante los correos electrónicos de phishing con ingeniería social o ataques BEC que pueden causar graves daños económicos y de reputación, pero hay buenas prácticas muy sencillas, a la vez que efectivas, como comprobar siempre las direcciones online de los mensajes desconocidos o inesperados para asegurarse de que sean auténticas y de que el enlace del mensaje no oculte otro hipervínculo, por ejemplo. Esto tipo de cosas deben tenerse interiorizadas por cualquier usuario y, por supuesto, ante cualquier duda, es mejor consultar.

Cuestión de efectivad

Hasta aquí, todos de acuerdo en que la formación es necesaria, pero ¿son realmente efectivos los programas de concienciación o terminan cansando?

Debemos tener presentes las diferencias individuales que hay entre la fuerza laboral: valores de cada empleado, responsabilidad dentro de la organización, así como aspectos de su personalidad, todos son factores importantes e impulsan el comportamiento de las personas. Para desarrollar una capacitación y prácticas más eficaces en materia de ciberseguridad, se debe prestar más atención a estos factores, según explica la Dra. Linda K. Kaye, académica de ciberpsicología de la Universidad de Edge Hill, en el informe Heads in the cloud de Trend Micro. Esto, a su vez, puede ayudar a las organizaciones a adoptar una formación en materia de ciberseguridad más adaptada o personalizada con sus empleados, lo que puede ser más efectivo.

Los programas de concienciación y las acciones formativas han de ir adaptándose a las nuevas circunstancias y el contexto de la organización, a los objetivos de su estrategia, así como a su evaluación de riesgos y propensión al mismo. "No se puede impartir solo una charla o una formación

Xxxxxx

El informe State of the Phish, de Proofpoint, revela qeu los trabajadores españoles son los más propensos a compartir los dispositivos de la empresa con sus familiares y amigos. El 69% permite que personas externas accedan a estos dispositivos, lo que supone casi un 25% más que la media mundial y un notable aumento respecto al año pasado (45%).

Al utilizar múltiples dispositivos para acceder a información sensible y confidencial definitivamente los riesgos aumentan, pero un usuario se conecta desde cualquier dispositivo y red a un servicio en Internet, por ejemplo, a un banco, y se produce un incidente de seguridad, no se le puede echar toda la culpa al usuario ya que "por desconocimiento, tendemos a hacer uso de forma generalizada de cualquier dispositivo sin protección e incluso desde cualquier red abierta y sin encriptar, lo que supone un enorme riesgo de compromiso de contraseñas y de los datos que se transmiten por la red. La concienciación de los usuarios en ciberseguridad ha aumentado, pero aún no es suficiente para prevenir todos los riesgos tales como la conexión a redes Wi-Fi abiertas sin ninguna clave", señala Carlos Becerra, de Cyber Security Speed.

Por otro lado, se está produciendo un cambio de mentalidad, según indican desde Secure&IT, pues cada vez más los usuarios están pidiendo responsabilidades a las entidades cuyas plataformas no están adecuadamente securizadas.

"Los usuarios son cada vez más conscientes de que depende de ellos no permitir ser engañados y poner obstáculos a los ciberdelincuentes".

Estefanía Macías, responsable de Secure&Academy, el Centro Avanzado de Formación en Ciberseguridad de Secure&IT

aislada y pretender que sirva para el medio-largo plazo. Por mucho que tengamos aprobadas políticas y procedimientos que garanticen un nivel adecuado de seguridad, las personas tendemos a simplificarlas en nuestro día a día o acabar adoptando malas prácticas heredadas", subraya Macías. Por lo tanto, apostar por la continuidad es otra de las claves, dado que sirve como recordatorio de aspectos esenciales a tener en cuenta a diario.

El resto de participantes opina lo mismo. Todo buen programa de formación que se precie debe ser algo vivo y estar adaptado a las necesidades de cada empresa y trabajador, "pero al mismo tiempo, seguir siendo sencillo y entretenido", apuntan desde Proofpoint. "Además, son realmente efectivos cuando se adecuan las necesidades de los usuarios y reflejan de forma fiel el panorama de amenazas al que se enfrentan, utilizando ejemplos reales que les permiten aplicar en su día a día los conocimientos adquiridos en la formación". Aspecto en el que también insiste Wisniewski, que dice que los programas de concienciación deben ir acompañados de otros recursos para ayudar a los empleados. "Si una empresa proporciona al personal herramientas de gestión de contraseñas y consejos como parte de la formación, podrá ver cómo aumenta el cumplimiento. Combinar soluciones

con casos reales han de ser actividades complementarias".

Al igual que ocurre en la enseñanza general, la idea de que cuanto más interesantes y dinámicos sean los procesos de aprendizaje, mayor será su efectividad y más atención captarán, es una realidad. En este sentido, "la gamificación es muy útil para hacer más amena la formación. Los empleados la afrontan con mayor disposición y retienen mejor los mensajes. Y es que, en muchas ocasiones, los programas de formación son vistos por los empleados como aburridos y poco estimulantes", apostilla Ramírez, que añade que según informes de Kaspersky el 80% de los CIOs afirma no estar contento con los programas de formación.

Tampoco hay que olvidar que las ciberamenazas van cambiando, de ahí que para que el programa

"Para conseguir una efectividad máxima, la formación debe estar guiada y adaptada a los diferentes perfiles profesionales y necesidades".

Nuria Andrés, Estratega de ciberseguridad de Proofpoint para España

de concienciación sea efectivo, debe proporcionar un contenido actualizado basado en los riesgos actuales de la industria, debe causar impacto, retener a la audiencia y mantenerla activa durante el entrenamiento, contener tests a lo largo del mismo para probar la atención de los usuarios y, además, debe poder medir el progreso y la eficacia del programa mediante métricas accionables, según explican desde Cyber Security Speed.

"Los sistemas humanos y de seguridad deben ir de la mano, ninguno funciona bien sin el otro", apunta el investigador de Sophos. Es cierto que los humanos son propensos a caer en ataques de phishing y otras amenazas de ingeniería social, por eso, "las soluciones tecnológicas deben proteger contra esas amenazas permitiendo la monitorización para detectar patrones inusuales de actividad que indican posibles actividades anómalas".

A pesar de esto, muchas de estas soluciones son también supervisadas por otras personas que pueden ayudar a mejorar los sistemas para detectar los matices necesarios que permitan distinguir lo bueno de lo malo. Precisamente las iniciativas de formación permiten ampliar conocimientos y contribuyen al establecimiento de nuevos patrones de comportamiento. Al final, lo que se busca es cambiar hábitos y crear una cultura de ciberseguridad que motive a los empleados a continuar con las prácticas seguras.

Otro factor que suma a la hora de que un programa sea efectivo es la adaptación del contenido a cada sector concreto de actividad en el que la empresa opera, pues aunque hay muchas amenazas comunes, no todas se dan de la misma manera en los diferentes ámbitos. Esta adaptación ha de ser extensiva a los diferentes departamentos y perfiles profesionales dentro de la organización.

"Igualmente, para que el usuario entienda e interiorice el contenido tan importante es la visión teórica y las herramientas tecnológicas, como el contar con expertos en ciberseguridad, abogados de Derecho TIC, peritos informáticos judiciales y formadores que aporten la experiencia del día a día en el uso de nuevas tecnologías y, especialmente, su visión de cómo enfrentarse a los riesgos de que determinados ciberataques se materialicen e impacten personal y profesionalmente", añade la responsable de Secure&IT.

Ojo con los descuidos

Pero errar es de humanos y por eso se dice que aún queda camino por recorrer en lo que a empoderamiento de los empleados se refiere. La creencia de que los empleados son el eslabón más débil de cualquier sistema de seguridad corporativa está instalada entre nosotros y, si se consulta a las personas que se ocupan de proteger los sistemas TI y los datos, lo corroborarán. Y es que no importa

"Es clave recurrir a las herramientas de concienciación y hacer un llamamiento a los empleados para que sean prudentes de los ataques de los que pueden ser víctimas"

Alfonso Ramírez, director general de Kaspersky para Iberia

Todos de acuerdo en que la formación es necesaria, pero ¿son realmente efectivos los programas de concienciación o terminan cansando?

lo avanzada que sea una tecnología de seguridad, pues un pequeño despiste de un empleado puede poner en riesgo la infraestructura de la empresa.

"Por lo general, se trata de situaciones producto de descuidos y falta de atención, y sobre todo, de falta de programas de formación efectivos que ayuden a los trabajadores a estar prevenidos ante este tipo de ataques", indica Ramírez. De ahí que para saber con certeza si una brecha de seguridad ha sido fruto de un descuido o no, las organizaciones deben contar con mecanismos y estrategias de seguridad adecuadas que les permitan determinar dónde está el origen del ataque. "La experiencia y el conocimiento en materia de ciberseguridad también son un valor añadido a la hora de saber cómo ha entrado el malware y establecer los mecanismos oportunos para evitar que la situación se repita el futuro", dice el directivo.

"En la mayoría de los casos podemos determinar si fue un descuido de empleado o no apoyándonos también de aplicaciones de detección y respuesta en endpoints (soluciones EDR) y sistemas de monitorización (SIEM)", añade Becerra.

Junto a las herramientas de seguridad y a los planes de contingencia, "es importante activar protocolos de emergencia, crear comités de seguridad en los que estén presentes la alta dirección y responsables de la compañía, y que expertos de ciberseguridad y privacidad lleven a cabo una pericial informática para conocer "qué", "quién", "cómo" y "por qué" ha fallado nuestra seguridad", explica Macías.

Pero la ciberseguridad es responsabilidad de todos los miembros de una organización, no solo de los empleados, tal y como señalan los expertos que participan en el reportaje. Según un reciente informe de Proofpoint, el 91% de los trabajadores españoles afirma haber recibido al menos una comunicación sospechosa en 2021. Y lo que es más preocupante, el 59% piensa que todos los emails internos son seguros y el 57% cree que su organización bloqueará automáticamente todo el correo electrónico malicioso.

Estos datos hacen saltar las alarmas y "muestran cómo la ciberseguridad de una empresa depende de todos y cada uno de sus empleados, pero eso no significa que tenga que recaer sobre ellos toda la responsabilidad. De ahí que las organizaciones deban darse cuenta de lo esencial que es la concienciación en materia de seguridad y ofrecer las herramientas y la formación necesarias a sus trabajadores", recalca Andrés.

La mayoría de las veces se trata más de una mala gestión y supervisión que de un error humano directo. Investigaciones de Sophos han revelado que la mayoría de las brechas de seguridad comienzan con compromisos por no haber parcheado los sistemas vulnerables con la suficiente rapidez o por el robo de credenciales en otras brechas de seguridad. Los ciberdelincuentes suelen permanecer dentro de una red comprometida durante más de dos semanas antes de activar un

"No es el empleado el único responsable de saber cómo actuar sino también los líderes de la empresa y el equipo de seguridad TI a la hora de formar sobre los riesgos"

Carlos Becerra, Socio Fundador de CB Universal y Cyber Security Speed

ataque. Por tanto, "a menos que el empleado lo haga de forma consciente para dañar a la empresa, o bien que, aun conociendo las buenas prácticas conformadas por políticas y procedimientos de seguridad, actúe de forma omisiva o negligente, en cuyo caso se podrían llegar a aplicar medidas disciplinarias laborales o estatutarias y exigir responsabilidades civiles y penales en función del impacto, el empleado no sería el único responsable", aclaran desde Secure&IT.

El teletrabajo marca el punto de inflexión

Como en todo, la pandemia ha supuesto un antes y un después, especialmente en cuestión de ciberseguridad. Al adoptarse ampliamente el trabajo remoto, muchas empresas han tenido que enfrentarse a este reto y como los riesgos se han incrementado, por lo general también lo han hecho los programas y planes de concienciación y las herramientas de formación para prevenir riesgos. Así, existe la idea generalizada de que los usuarios cada vez son más conscientes de los daños que pueden desencadenar en las empresas por un ataque.

También el teletrabajo ha acarreado que muchas empresas deban enfrentarse al problema del "shadow IT", o TI en la sombra, algo que siempre ha preocupado a los equipos de TI y seguridad de las empresas. Como remedio, "muchas empresas han desplegado arquitecturas Zero Trust para reducir el riesgo de posibles dispositivos conectados que estén comprometidos o mal configurados. Otras impiden también la instalación de software no autorizado en los equipos corporativos y piden a los empleados que utilicen sus teléfonos móviles personales para cualquier aplicación de chat u otro software que no sea de uso oficial de la empresa", aclara Wisniewski.

Sin embargo, cabe destacar que desde que comenzó el teletrabajo, solo un tercio (32%) de las empresas proporcionó a sus empleados una solución de seguridad para usar en dispositivos personales con fines laborales, según arroja una encuentra global de Kaspersky, que también revela que solo el 53% de los empleados usaba una VPN para conectarse a las redes corporativas.

Por tanto, como ocurre en otras tantas áreas, es posible hablar de mayor concienciación de los usuarios y empresas, lo cual ha puesto en marcha una mayor demanda de programas de formación y de herramientas de concienciación, pero aún queda trabajo por hacer, pues todos los expertos no se cansan de señalar que los planes de concienciación deben ser periódicos y estar adaptados a cada momento.

El lado menos positivo: las limitaciones

En la actualidad, las personas son el principal objetivo de ataque de los ciberdelincuentes. La mayoría de los ataques se dirigen directamente a los empleados, intentando que hagan clic en un

enlace malicioso, revelen sus credenciales de acceso, abran un archivo adjunto o que simplemente paguen una factura falsa, por lo tanto, la creación de una cultura de seguridad sólida es imprescindible. Ahora bien, también hay que preguntarse por cómo perciben y afectan a los trabajadores en su día a día las nuevas normas y los cambios en los procedimientos que se aplican en pro de la ciberseguridad. Si bien algunos usuarios pueden verlo como una limitación y una imposición, en general, estos cambios suelen terminar aceptándose.

"Es cierto que todos somos bastante escépticos a la hora de aceptar limitaciones que puedan impedir hacer más ágil y productivo nuestro trabajo, pero los empleados se están dando cuenta cada vez más de que a veces dichas limitaciones no representan un impedimento para su día a día, o un bloqueo de su productividad, sino un vehículo para proteger los sistemas e infraestructura de potenciales actividades maliciosas", señala Becerra.

"En el fondo los usuarios saben que dichas limitaciones son importantes para salvaguardar la seguridad tanto de su propia empresa como la información de sus clientes, así como la suya propia", dice Alfonso Ramírez. "Además, teniendo en cuenta que la mayoría de las personas utilizan dispositivos electrónicos en su día a día, son ellos mismos los que muchas veces toman conciencia de que deben protegerse más ante posibles ataques".

Todo buen programa de formación que se precie debe ser algo vivo y estar adaptado a las necesidades de cada empresa y trabajador

Algo similar opina Estefanía Macías, que comenta: "El paradigma actual ha cambiado. Ya no es la empresa o entidad la que impone el cumplimiento de medidas de seguridad técnicas y organizativas, sino que ya es el propio usuario que tanto a nivel personal como profesional el exige que se refuerce la seguridad y privacidad de los datos tratados".

La seguridad no es algo que haga el departamento de TI o el equipo de seguridad, es un esfuerzo de toda la empresa. El equipo de seguridad debe colaborar estrechamente con todos los departamentos para identificar los riesgos y aplicar planes para que esos departamentos contribuyan a reducirlos. "Trabajar con toda la organización ayuda a identificar las prioridades más importantes y, a menudo, la colaboración puede generar soluciones mejores que aumentan la eficiencia en lugar de impedirla", apunta el portavoz de Sophos.

Conseguir que los empleados interioricen la importancia de estas limitaciones es un proceso que empieza por promover mensajes para una

Enlaces de interés...

- Proofpoint obtiene la cualificación del CCN para su solución de formación en seguridad
- Microsoft formará y certificará gratis en ciberseguridad a más de 10.000 personas en España
- Predicciones de seguridad para 2022: un año de cambios y concienciación
- BBVA abre su formación en ciberseguridad a través de la plataforma Coursera

Si bien es cierto que los usuarios todavía no están lo suficientemente capacitados para su papel en la ciberdefensa, su concienciación en materia de seguridad va en aumento

concienciación básica, pero no termina ahí, se necesita llegar a cambiar su comportamiento. “Los empleados tienen que entender el porqué de estas medidas, y las consecuencias de no cumplirlas para que se creen unas expectativas comunes de lo que es un comportamiento aceptable. De esta manera las limitaciones no serán solo algo que impone el CISO, sino que, al crearse cierta presión del entorno, no cumplir las normas estará “mal visto””, comenta Andrés.

Por tanto, los usuarios terminan aceptando las políticas y procedimientos en ciberseguridad y privacidad de las empresas y el nivel de concienciación ha aumentado, pero no significa que sea suficiente.

En el mundo interconectado actual, ignorar la ciberseguridad ya no es una opción viable ni para para los empleados ni para las organizaciones. Es alentador ver que cada vez son más los que se toman en serio los consejos de los equipos de TI corporativos y aplican los aprendizajes de los programas de concienciación y formación de sus compañías. Sin embargo, siempre existen “versos libres” que no contemplan las buenas prácticas por distintas razones, de ahí que diseñar planes a medida y personalizados para atender a los diferentes perfiles de usuarios debería ser la tendencia a seguir para lograr a empoderar a los empleados.

Compartir en RRSS

it User
TECH & BUSINESS

Cada mes en la revista, cada día en la web.

MARIO VELARDE BLEICHNER

GURÚ EN CIBERSEGURIDAD

Con más de 20 años en el sector de la CiberSeguridad, Mario Velarde Bleichner, Licenciado en Ciencias Físicas con especialidad en Calculo Automático y PDG por el IESE, ha participado en el desarrollo de esta industria desde la época del antivirus y el firewall como paradigma de la Seguridad IT, dirigiendo empresas como Trend Micro, Ironport, Websense, la división de Seguridad de Cisco Sur de Europa y la división Internacional de Panda Software.

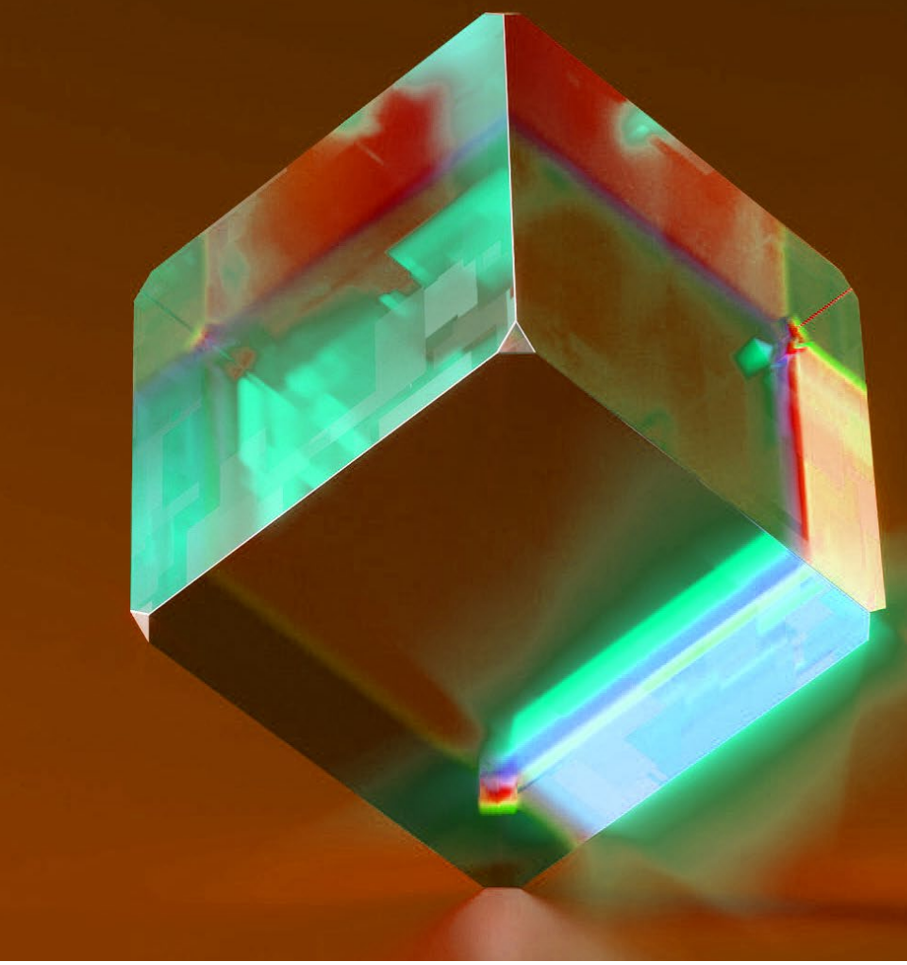
El Amanecer de la Humanidad Digital IX: Los Ciudadanos Digitales no superaron la oscura década de los 20

Los dos primeros años de la década de los años 20 del siglo XXI fueron los de la primera pandemia de la era digital, la llamada Covid-19, que afectó al vibrante avance de la Globalización Digital de las dos primeras décadas del siglo XXI de una manera brutal e inesperada, y que en los tres primeros meses del año 2020 produjo una prácticamente total paralización de la economía en todo el planeta y a toda la humanidad.

El tercer año de esa década dio inicio la primera guerra entre la Autocracia Rusa y las democracias americanas, europeas e incluso asiáticas. Los países neutrales y/o no alineados fueron forzados a tomar parte en el conflicto.

¿Cuáles fueron las consecuencias de estos acontecimientos y cómo afectaron al nacimiento de la Nueva Humanidad Digital? Vamos a ver algunos escenarios partiendo del peor posible hasta llegar al mejor y que no impactaría el amanecer de La Humanidad Digital.

Compartir en RRSS



La Covid-19 ha afectado al vibrante avance de la Globalización Digital de las dos primeras décadas del siglo XXI de una manera inesperada

■ **Primer Escenario.** La guerra, que estaba inicialmente localizada en un único país, fue gradualmente expandiéndose a los países vecinos y agravándose por la intensidad creciente de armamento cada vez más destructivo, llevando a la humanidad al Holocausto Nuclear Global, cuyas consecuencias, además de la barbarie en términos de aniquilación de la población, llevaron a la práctica desaparición de la civilización tal y como la conocemos.

En el peor caso de este escenario hay que contemplar la extinción de la especie humana, digital o no digital. Podría ser que quedaran pequeños grupos aislados de seres humanos que pasarían a vivir en condiciones similares a la humanidad de hace 15.000 años y es una pura especulación qué evolución tendrían estos supervivientes y sus descendientes. No conozco yo ningún plan para recuperar la civilización en un período corto después del escenario que se conoce como MAD (LOCO) Mutual Assured Destruction o Destrucción Mutua Asegurada.

Así pues, este primer escenario tendría como consecuencia que la Humanidad Digital no tendría un Amanecer.

■ **Segundo Escenario.** La guerra termina en menos de un año con la dominación del país invadido por las tropas de la Autocracia Rusa y la imposición de las condiciones del ganador. Ese mismo día empieza la expansión del nuevo Imperio Nacionalista Ruso del siglo XXI, que durará varias décadas, y que anexará a los países europeos a través de movimientos políticos con el triunfo en elecciones democráticas de los extremismos nacionalistas, tanto de extrema derecha como de extrema izquierda, o incluso de coaliciones de dichos extremismos de izquierda y derecha. Aquellos países que se resistan democráticamente a este tipo de anexión serán amenazados militarmente con el ejemplo de las atrocidades cometidas en la guerra de 2022 para finalmente sucumbir a formar parte del nuevo imperio Nacionalista Ruso que será regido por un emperador/zar de toda Europa.

La Unión Europea quedara reducida a pequeños territorios en el sur de Europa y conjuntamente con Gran Bretaña serán la retaguardia de lo que quede de la OTAN y como punta de lanza del Imperio Americano, que se retirará hacia sus territorios al otro lado del Atlántico.

El conflicto entre los tres Imperios, Nacionalista Ruso, Neocomunista Chino y Democrático Americano, que se repartirán el resto de los territorios del planeta, empezará un largo período de Guerra Fría y consolidación de los Imperios, que fácilmente durará todo el siglo XXI.

La evolución de estos tres imperios en conflicto permanente hará que el amanecer de la Humanidad Digital se retrase sine die y, a pesar de que el avance de las tecnologías digitales se reanude, su aplicación será eminentemente militar con el ánimo

El primer escenario tendría como consecuencia que la Humanidad Digital no tendría un Amanecer

imponerse a los otros dos imperios. Es casi imposible imaginar cual será el futuro que le espera a la humanidad si este modelo de tres imperios en conflicto se establece en nuestra bella Tierra

- **Tercer Escenario.** La guerra se estanca sin un vencedor claro ni cese de hostilidades en un largo plazo, provocando una catástrofe económica a nivel global provocando hambrunas en los países más pobres, desabastecimientos y una caída generalizada del nivel de vida en todo el planeta.

Esta situación propicia disturbios, altercados, saqueos y, en algunos países, situaciones tan caóticas que propician el resurgimiento de gobiernos autocráticos y nacionalistas que, con la excusa de mantener el orden, hacen retroceder las democracias a situaciones de hace más de un siglo.

Con esta situación, la economía global se deteriorará más aun y los avances de la economía digital se retrasarán en consecuencia. Por cada año que se prolongue esta situación de guerra estancada, el avance de la humanidad digital se retrasará una década.

Peor aún, los gobiernos autocráticos surgidos por esta situación controlarán a su población como las dictaduras digitales de la actualidad entorpeciendo todavía más la evolución hacia una Humanidad Digital. Probablemente, hasta la desaparición de los gobiernos autocráticos que habitualmente hacen todo lo posible por perpetuarse y esto podría durar décadas, no se podrá reanudar la evolución de la especie hacia la Humanidad Digital

Este escenario podría hacer que el siglo XXI sea un siglo convulso, caótico, autoritario… que haga retroceder a la humanidad y evite el amanecer de la Humanidad Digital hasta por lo menos mitad del siglo XXII.

- **Cuarto Escenario.** La guerra se detiene porque el avance de las tropas del Nacionalismo Ruso se estanca ante las defensas del país invadido.

Se inicia el contrataque del país invadido que va lentamente recuperando los territorios ocupados, haciendo prisioneros a un gran número de soldados invasores y capturando grandes cantidades de armamento abandonado en su huida por las tropas invasoras. Cuando se completa la recuperación de los territorios invadidos se producen fuertes disturbios en la capital y las principales ciudades del país invasor que culminan con la toma del poder por los generales del ejército invasor y la deposición del líder y su camarilla, acusados entonces de traición a la patria por haber iniciado una guerra sin sentido.

El nuevo poder militar decide mantener el statu quo anterior a la guerra para recuperar la situación económica a niveles iguales a los de antes del inicio

Enlaces de interés...

- La guerra entre Rusia y Ucrania impacta en las redes sociales

> Por cada año que se prolongue esta situación de guerra estancada, el avance de la humanidad digital se retrasará una década

de 2022. Este proceso llevará, al menos, una década, durante la cual los derechos del pueblo ruso quedarán en suspenso en tanto en cuanto su economía mejore y las heridas económicas y políticas, así como las grandes pérdidas de vidas humanas de la guerra, vayan cicatrizando.

El nuevo poder militar puede intentar perpetuarse e ir creando una nueva oligarquía que intente nuevamente llevar a Rusia hacia un nacionalismo desmedido y nuevas aventuras imperialista y militaristas, pero unas décadas después del fin de la guerra el pueblo ruso volverá a conseguir que su voluntad sea conocida al manifestarse para que se convoquen elecciones libres en las que se pueda conocer la voluntad real del pueblo.

Por primera vez, los rusos pueden elegir su futuro tras más de 100 años de líderes iluminados y sectarios que solo imponían sus opiniones políticas por el terror y el sometimiento de la población. Si se llega a esta situación, toda persona de bien desearía que así fuera, Rusia podría convertirse en una gran nación neutral y amiga de todos sus vecinos y del resto del mundo y ser el contrapeso de los dos imperios, el Neocomunismo Chino y la Democracia Americana, que sin duda lucharan por la hegemonía mundial en el siglo XXI.

También podríamos pensar que esta nueva Rusia democrática podría unirse a la Unión Europea y hacerla más fuerte e independiente de los dos Imperios ya consolidados en el década de los años 20 del siglo XXI.

Este cuarto escenario, en cualquiera de las dos evoluciones de Rusia, lamentablemente también produciría un retraso en el amanecer de la Humanidad Digital, aunque tal vez solo de unas cuantas décadas.

- **Quinto Escenario.** El optimismo nos debe acompañar y pensar que los dos años de pandemia y solo unos meses de guerra no interferirán con el gran avance de la especie hacia una Humanidad Digital global que se acelerará en la década de los años 30, y los seres humanos disfrutaran del amanecer de la Humanidad Digital antes de que acabe el siglo XXI.

it Reseller
TECH&CONSULTING

Radiografía del
partner tecnológico
en España

Cada mes en la revista,
cada día en la web.