it Digital Security

La publicación electrónica sobre Seguridad Digital que necesitas

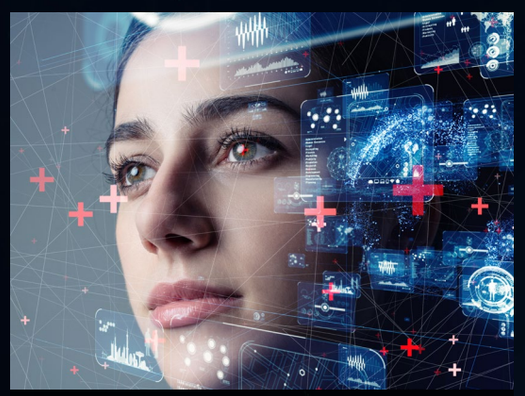
Septiembre 2022 - nº 55

Cifrado post-cuántico.

La ciberseguridad llama a la puerta

‘La concienciación del usuario es un pilar básico de una buena estrategia integral de seguridad’
Roberto Alunda, Mediapro

‘Seguimos trabajando con passwords, y esto en algún momento se tendrá que acabar’
Enrique Solís, Aguas de Añarbe



Gestión de Identidades y accesos, un mercado en auge

Revista IT Trends. La digitalización de la pyme, alimentando la productividad de nuestro tejido empresarial

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

it 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

it Digital MEDIA GROUP

Director General Juan Ramón Melara	juanramon.melara@itdmgroup.es
Director de Contenidos Miguel Ángel Gómez	miguelangel.gomez@itdmgroup.es
Directora IT Televisión y Lead Gen Arancha Asenjo	arancha.asenjo@itdmgroup.es
Directora División Web Bárbara Madariaga	barbara.madariaga@itdmgroup.es

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

Cifrado post-cuántico. La ciberseguridad llama a la puerta

La computación cuántica puede parecer ciencia ficción, pero la realidad es todo lo contrario. En los últimos años esta disciplina ha sumado notables avances y son cada vez más las compañías que se suben al tren del I+D+i en esta materia. De hecho, los investigadores anticipan que el mercado de la criptografía cuántica alcanzará un valor de 291,9 millones de dólares en 2026 a medida que más organizaciones busquen o inviertan para protegerse contra futuras amenazas cuánticas. Pero ¿qué implicaciones tiene esto para la seguridad? Desvelamos todos los secretos del cifrado post cuántico en el tema de portada de este número de IT Digital Security.

En ITDS Septiembre hablamos con Enrique Solís, CIO y CISO de Aguas de Añarbe, para quien no existe una solución de ciberseguridad milagrosa; y con Roberto Alunda, CISO Global de Mediapro, a quien le preocupa más el phishing que el ransomware. También abordamos la seguridad con Javier Gallego, Sales Director de Data Center Compute Solutions de Dell Technologies, que asegura que su compañía la aborda de una manera holística.

La gestión de identidades y accesos, y todo lo que le rodea, desde el control de las identidades privilegiadas, la autenticación de los usuarios o la vigilancia de las máquinas, centra uno de los temas de actualidad. Hablamos también de Olvido, la nueva herramienta de authUSB para borrar sin dejar rastro, que permite crear algoritmos de borrado personalizados, aunque ya se incluyen por defecto los más conocidos como Gutman, USAF 5020, German VSITR, así como dos algoritmos definidos por en CCN para sistemas que manejan información clasificada y bajo el alcance del ENS.

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

En Portada

Cifrado post-cuántico. La ciberseguridad llama a la puerta

itds

Sumario

Entrevistas

Actualidad

No solo IT

Índice de anunciantes

Revista IT Trends

STORMSHIELD

La opción europea en ciberseguridad

El partner de confianza
para
securizar sus
infraestructuras operacionales y sensibles

www.stormshield.com

Gestión de Identidades y accesos, un mercado en auge

El mercado de gestión de identidades y accesos, o IAM (Identity and Access Management), crece con salud desde hace ya unos años. La nube y el trabajo remoto han sido algunos de sus aceleradores más destacados, apuntalado por el famoso Zero Trust que promueve la validación continua de valores de confianza, como es la identidad de usuarios, y de las máquinas. Dentro de mercado de seguridad es uno de los segmentos que más se ha consolidado en los últimos años, con acuerdos tan destacados como la unión de Thycotic y Centrify, convertidos en Delinea, o la compra, por la misma fecha de Auth0 por parte de Okta.

Recientemente, la firma de inversión Thoma Bravo, ha adquirido, con meses de diferencia, dos empresas expertas en gestión de identidades: Sailpoint y Ping Identity. Y es bien seguro que el mercado seguirá evolucionando hacia la consolidación de un mercado que Fortune Business Insights calcula que alcanzará los 34.520 millones de dólares en 2028, con un crecimiento medio anual del 14,5% desde 2021.

Gartner define IAM como "la disciplina que permite a las personas adecuadas acceder a los recursos adecuados en el momento adecuado por las razones adecuadas"

Además de la consolidación, de la que hablaremos más adelante los estudios destacan que para 2025, las plataformas de IAM convergentes serán el método de adopción preferido para la gestión de accesos, la IGA (Identity Governance and Administration) y PAM (Privileged Access Management) en más del 70 % de las nuevas implementaciones.

Hablemos de IAM

Gartner define IAM como “la disciplina que permite a las personas adecuadas acceder a los recursos adecuados en el momento adecuado por las razones adecuadas”. Esto significa que entre las capacidades que debe ofrecer un proveedor de este mercado deben incluirse la sincronización de identidades; la gestión de contraseñas; el uso de diferentes métodos de autenticación, como MFA o SSO (Single Sign On); soporte para diferentes métodos de autenticación, incluido FIDO; control de acceso y autenticación de las API, así como de la identidad de las máquinas, lo que requiere un férreo control de los certificados; no cabe duda de que debe tener funciones básicas de gobierno y administración de identidades (IGA), como gestión del ciclo de vida de las mismas, aprovisionamiento de usuarios, solicitudes de acceso con aprobaciones y certificaciones de acceso; o capacidades de agregación e integración con plataformas externas, como las de analíticas de clientes o CRMs.

La transformación digital y la consecuente adopción de la nube ha provocados que empleados y usuarios puedan iniciar sesión en aplicaciones comerciales críticas desde cualquier lugar, en cualquier momento y con cualquier dispositivo, lo que ha aumentado el riesgo y la necesidad de comprobar que quien accede es quien dice ser y sólo accede a lo que debe. No es una tarea baladí si tenemos en cuenta el dinamismo del mercado y que ese derecho de acceso tiene que acompañar a la identidad a lo largo del ciclo de vida de la misma, bien

Consolidación del mercado IAM

Estas son algunas de las fusiones y adquisiciones destacadas de los últimos años en el mercado IAM

- **2022. Agosto.** Thoma Bravo compra SailPoint por 6.900 millones de dólares en efectivo; 2022. Junio. Entrust adquiere Evidos, compañía experta en soluciones de verificación de identidad.
- **2022. Abril.** OneIDLab se fusiona con Tozny
- **2022. Abril.** Thoma Bravo compra SailPoint.
- **2022. Abril.** Avast compra SecureKey sin que los detalles financieros hayan trascendido.
- **2022. Marzo.** SentinelOne coomrpa Attivo Networks por 616 millones de dólares.
- **2022. Enero.** VectraAI compra Siriux Security, proveedor de seguridad de identidad y gestión de postura en la nube.
- **2021. Octubre.** One Identity compra OpneLogin para reforzar sus capacidades de autenticación multifactor y la gestión de acceso e identidad del cliente (CIAM).
- **2021. Septiembre.** Ping Identity compra Singular Key, cuya tecnología facilita la integración de verificación de identidad, fraude, riesgo, gestión de acceso, acceso privilegiado y gobierno de identidad.
- **2021. Agosto.** Okta compra atSpoke para reforzar su estrategia de gobierno de la identidad.
- **2021. Junio.** Ping Identity compra SecuredTouch para mejorar la protección de cuentas y detección de bots.
- **2021. Marzo.** Centrify y Thycotic se fusionan y surge Delinea.
- **2021. Mayo.** Okta compra AuthO por 6.500 millones de dólares
- **2020. Mayo.** CyberArk compra Idaptive por 70 millones de dólares.
- **2019. Octubre.** Atos adquiere IDnomic.
- **2019. Julio.** Wallix compra la española Simarks, especializada en esoluciones PEDM (Privilege Elevation and Delegation Management), que son las que permiten implementar reglas de seguridad que limitan las acciones de usuarios y administradores.
- **2018.** Fue un año revolucionario para el mercado de gestión de acceso privilegiado. Bomgar adquirió Lieberman, Avecto y BeyondTrust. La empresa resultantes, que mantendría el nombre de BeyondTrust, fue comprada por Francisco Partners antes de que acabara el año.

sea la de un empleado que lleve años en el mismo puesto y accediendo a los mismos directorios, como el partner que accede de manera puntual a determinados servicios.

Y el asunto se complica si, como es necesario, incluimos en la ecuación las identidades de las máquinas. Forrester estima que las identidades no humanas (bots asistidos y no asistidos, cuentas de servicio, automatización en la nube y API, dispositivos de Internet de las cosas (IoT) y robots) están creciendo a más del doble de la tasa de identidades humanas en muchas organizaciones. El acceso de los bots también debe administrarse y hay un factor importante a tener en cuenta: es necesario controlar cómo se administran las credenciales de un bot y quién tiene acceso para modificar o ejecutar bots.

Además de la Transformación Digital, la tendencia hacia el passwordless, o el fin de las contraseñas, está también impulsando la adopción de tecnologías IAM. No es una nueva tendencia, pero parece que su realidad está más cerca. Es

el siguiente paso a la autenticación multifactor, y la basada en los estándares FIDO parece ser la preferida.

Consolidación

Como comentábamos al inicio del artículo, recientemente se han producido dos acuerdos de compra por valor de varios miles de dólares, con la firma de capital privado Thoma Bravo como protagonista, y en el mercado de gestión de identidades y accesos. Se anunciaba hace unas semanas la compra de SailPoint por 6.900 millones de dólares en efectivo; esta compra seguía la de Ping Identity por 2.800 millones de dólares. Según los analistas, Thoma Bravo habría pagado más que el valor de mercado en cada caso: un 31% más en el de SailPoint y un 63% más en el de Ping Identity, lo que no deja lugar a dudas sobre el potencial que tiene el mercado de gestión de identidades y accesos, así como todas las tecnologías que lo rodean, desde las relacionadas con el onboarding digital, a relativas a la autenticación, protección del directorio activo o el tratamiento de las identidades privilegiadas.

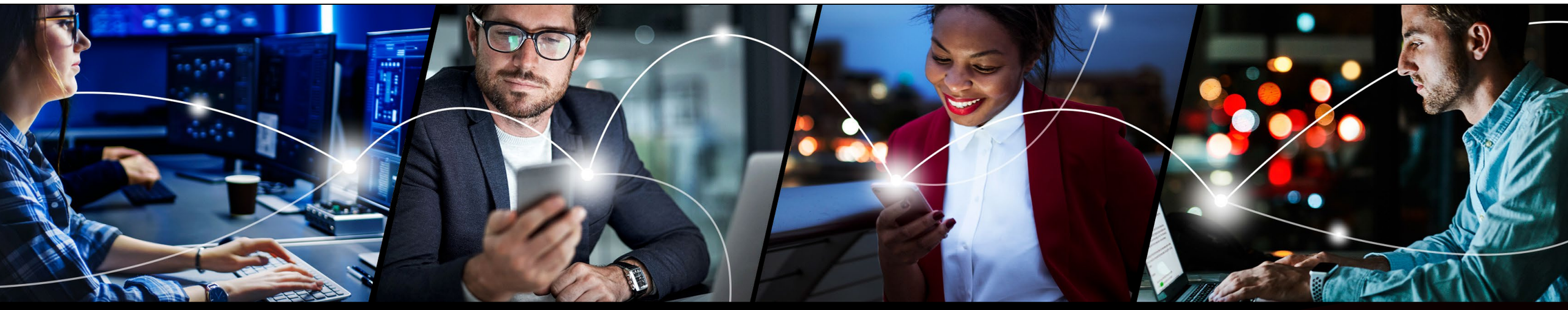
Respecto a Thoma Bravo destacar que en los últimos años ha reforzado su apuesta por el mercado de ciberseguridad con las adquisiciones de Proofpoint, McAfee, LogRhythm, Imperva, Sophos o Veracode.

Enlaces de interés...

- Solo el 16% de las empresas tiene una estrategia de IAM completamente madura
- PAM, PIM e IAM: ¿qué son y cómo ayudan a proteger los accesos críticos en las empresas?
- Tendencias clave en el diseño de soluciones de CIAM

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

Olvido,
la nueva herramienta de authUSB para borrar sin dejar rastro

AuthUSB estrena la vuelta al cole con una nueva herramienta, Olvido, que ofrece al usuario la posibilidad de borrar de forma segura distintos elementos guardados en los dispositivos de almacenamiento, bien sea en ficheros y carpetas, espacio libre, fragmentos del clúster no utilizados o discos y volúmenes.

Olvido, que realiza tareas de sobreescritura y borrado, dispone de un módulo de planificación con el que el usuario podrá programar la ejecución de las tareas de borrado. La herramienta basa el borrado de información en la sobreescritura de los datos existentes, y tanto los patrones con los que realiza la sobreescritura como el número de pases a realizar se definen en los algoritmos de borrado.

La herramienta incorpora un editor que permite crear nuestros propios algoritmos personalizados, aunque ya se incluyen por defecto los más conocidos como Gutman, USAF 5020, German VSITR, así como dos algoritmos definidos por en CCN para sistemas que manejan información clasificada y bajo el alcance del ENS

Enlaces de interés...

- Guía sobre borrado seguro de la información - INCIBE
- El 90% de las empresas españolas no realiza el borrado de datos que impone el ENS

Olvido permite también la integración con un servidor Syslog para el envío de registros de actividad

Olvido permite también la integración con un servidor Syslog para el envío de registros de actividad y estado de las tareas de borrado realizadas.

Olvido ha recibido la Categoría ALTA en el Esquema Nacional de Seguridad, ENS, y está disponible desde Septiembre para Windows 10, Windows Server 2016. En un futuro se estudiará portar la herramienta a Mac y Linux.

Preguntados sobre el tipo de cliente al que va dirigida la herramienta, responden desde authUSB que “principalmente el ámbito de defensa, administraciones públicas, infraestructuras críticas y, en general, cualquier organización que maneje información sensible y necesite garantizar la destrucción de estos datos de forma que no sean recuperables”. La herramienta es gratuita para la administración pública, mientras que para el sector privado se ofrece con un modelo de licenciamiento anual.

Entre los casos de uso más habituales identificados por la compañía, destacan “la selección manual de archivos y/o carpetas e invocar la herramienta desde el menú contextual, o la planificación de tareas de limpieza automáticas como borrado periódico de espacio libre, carpetas temporales, papelera de reciclaje o archivos de paginación”, así como el borrado de particiones o discos completos para su reutilización por otros usuarios.

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.

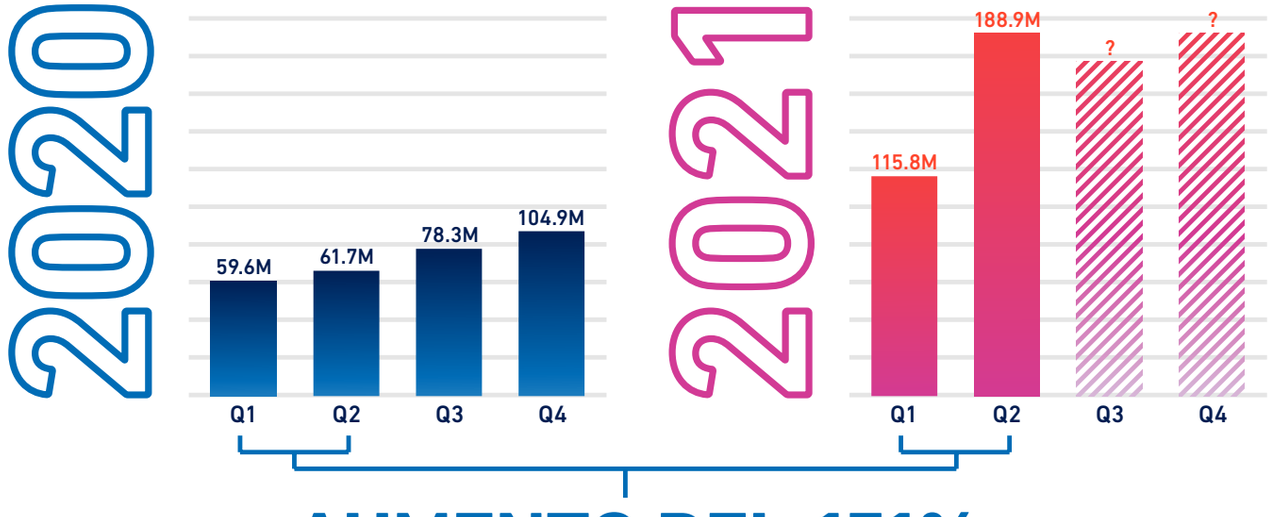
OBTENGA EL INFORME COMPLETO

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

Ser buen comunicador y gustarte mucho tu trabajo, que no acaba cuando sales de la oficina, son algunas de las cualidades que debe tener un buen CISO; apostando por una cultura de ciberseguridad, dice también Enrique Solís, CIO y CISO de Aguas de Añarbe, que no existe una solución de ciberseguridad milagrosa y que la Inteligencia Artificial y la gestión de identidades son tecnologías a tener en cuenta en un futuro cercano.

Rosalía Arroyo

‘Seguimos trabajando con passwords, y esto en algún momento se tendrá que acabar’

(Enrique Solís, Aguas de Añarbe)

Enrique Solís González pertenece a la generación del Spectrum, el ordenador que conquistó Europa en los ’80, con el que muchos empezaron en un mundo digital sin conectividad, y con el que el actual CIO y CISO de Aguas de Añarbe aprendió a programar. La pasión se mantuvo durante años y le llevó a escoger la carrera de Ingeniería Informática, interesándose especialmente por las áreas de redes y sistemas. Durante los años de facultad, tiempos de monitores monocromo, fue cuando surgió la World Wide Web y aparecieron los primeros navegadores, recuerda durante una conversación en la que nos cuenta que sus primeras experiencias laborales estuvieron relacionadas con la administración de

"Buscas un producto que en función del benchmark conseguido, lo que te han contado, lo que has investigado tú o las pruebas de concepto que hayas podido realizar, te funcione y sea interesante"

sistemas “donde ya existía la preocupación por la seguridad. Aunque es cierto que en aquella época todo era bastante más básico”.

Pero por básico que fuera, el tema de la seguridad informática despertó su interés, y por su cuenta “investigaba, hacía pruebas y montaba pequeños laboratorios en casa”, hasta terminar realizando un Máster en Seguridad de las TIC después de unos años trabajando. Tuvo claro desde el principio que la seguridad “es fundamental para acometer la transformación digital de manera sólida y sin fisuras, y que es necesario contar con una estrategia de ciberseguridad que acompañe a todo el proceso”. Además, también hay una serie de regulaciones que cumplir, y políticas que elaborar, asegura el CIO y CISO de Aguas de Añarbe.

CISO:, evolución, retos y cualidades

Sobre la evolución de la figura del CISO, explica Enrique Solís que antes tenían un rol mucho más técnico; “en muchos casos no había un puesto definido como tal. Estaban integrados en otros departamentos y entre sus funciones había algunas referentes a la seguridad, pero sin existir ese rol específico”. Añade lo que muchas veces e injustamente se ha dicho de ellos: que se les veía como la persona que impedía hacer ciertas cosas; “pero es cierto que todo ha evolucionado. La transformación digital está creando un ecosistema mucho más complejo para las empresas, la tecnología avanza a un paso muy rápido y eso hace que la defensa de estos sistemas sea mucho más complicada. Al final, hoy en día hay más conciencia de que es necesario tener una estrategia de ciberseguridad”.

La existencia de cada vez más regulaciones de seguridad, desde el ENS, al reglamento de protección de datos, o los específicos de cada sector “exigen de algún modo tener una cultura de seguridad y una gestión de la misma; asegura Enrique Solís añadiendo que los responsables de ciberseguridad ya no son personas tan técnicas, sino que se han convertido en “traductores entre un idioma técnico y un idioma de negocio”, lo que ha hecho que el CISO tenga que desarrollar una mayor visión del

negocio para poder alinearse con los objetivos de la empresa.

"Los CISO actuales han de tener conocimientos especializados organizativos, técnicos y jurídicos. Tienen un rol más estratégico, entre sus funciones están las de, gestionar normas y riesgos, proponer las políticas de seguridad, desarrollar y aplicar esas políticas y ser quien asume la responsabilidad y el compromiso."

Sobre los retos de seguridad a los que se enfrenta el CISO de Aguas de Añarbe "son los derivados de aplicar la ciberseguridad en un entorno industrial, a lo que se suma el hecho de que proveemos un servicio esencial para la ciudadanía". Explica el directivo que la gestión de las infraestructuras es cada vez más digital, cada vez hay mayor convergencia entre el mundo IT y el OT, y que en el caso de su compañía "para tomar decisiones correctas es vital que la información que se recoge de los sistemas cumpla el principio de integridad, que no haya sido manipulada".

"Hay que ser capaz de concienciar de los riesgos que hay y hacer partícipe a todo el personal, incluida la dirección"

El segundo reto es el de disponibilidad, porque "al ofrecer un servicio que es esencial para la ciudadanía una parada debida a un fallo o a un ciberataque puede tener consecuencias serias que pueden afectar a la salud de las personas o causar daños al ecosistema".

Y, finalmente, Enrique Solís menciona un tercer reto: la menor madurez en ciberseguridad que existe en el mundo industrial frente al mundo IT. Según Solís "lo que antes no se conectaba ahora sí se conecta. Y así como en el mundo IT ya llevan años con esto asumido, en el mundo OT todavía

existe una cierta falta de madurez. Además, muchas de las instalaciones industriales no se han actualizado desde el día que se pusieron en producción, cuando la ciberseguridad no era un requisito de diseño".

Cuando preguntamos a Enrique Solís por las cualidades que debería tener un buen CISO asegura que "lo primero de todo te tiene que gustar mucho porque tu trabajo no acaba cuando sales de la oficina". Añade que el trabajo de CISO te obliga a estar actualizado constantemente "porque ahora no pasan meses hasta que se explota una vulnerabilidad, sino horas", y que se tiene que convivir con el hecho de que "por muy bien que hagas tu trabajo, la seguridad 100% no existe, no todo depende de ti".

Por otra parte, se necesita hacer una gestión del estrés importante, y mantener una actitud proactiva "no sólo tienes que saber reaccionar cuando ya ha pasado, sino que tienes que prepararte, anticiparte un poco en la medida que puedas".

Por último, "tienes que ser buen comunicador. Lo que nosotros vemos como seguridad otras partes de la empresa lo pueden ver como un incordio y hay que ser capaz de concienciar de los riesgos que hay y hacer partícipe a todo el personal, incluida la dirección".

Amenazas y tecnologías

No todas las empresas son iguales, y por tanto no todas se ven afectadas de igual manera por el mismo tipo de amenaza. A Enrique Solís los ataques llamados de fraude al CEO no son los que más le preocupan; ser una empresa no demasiado grande, donde todo el mundo se conoce y hay un fuerte componente de concienciación, son algunas de las razones.

La amenaza que más preocupa al CISO de Aguas de Añarbe "es sobre todo el malware, y en especial el ransomware". Comenta que cada vez hay más ataques, que cada vez son más sofisticados y que

"Por muy bien que hagas tu trabajo, la seguridad 100% no existe, no todo depende de ti"

"Para tomar decisiones correctas es vital que la información que se recoge de los sistemas cumpla el principio de integridad, que no haya sido manipulada"

los dirigidos son especialmente preocupantes porque son más difíciles de parar.

"El cibercrimen ha pasado a ser un negocio muy lucrativo y está consolidándose como el delito del futuro. Los autores y grupos de ransomware han descubierto que dirigirse a organizaciones industriales es muy beneficioso y que encima gozan de un alto grado de impunidad".

"No existe una solución milagrosa", dice Enrique Solís cuando le preguntamos qué tecnologías de seguridad deberían ser imprescindibles en cualquier empresa. La opción de este experto es desarrollar múltiples capas de seguridad, de manera que "si una salvaguarda en particular falla, existirán otras en las capas inferiores que mantendrán el riesgo en niveles aceptables".

Dicho esto, opina que "si tenemos que empezar por algo, yo diría que es básico un NGFW que nos permita segmentar y controlar el tráfico que circula por nuestra red, filtrar tanto por IPs como por servicios, realizar DPI (Deep Packet Inspection) además de otras funcionalidades como Antivirus, IDS/IPS, Anti DoS, gestión de vpn para accesos remotos,…

Además, seguimos viendo que el correo electrónico sigue siendo hoy en día el principal vector de ataque con lo cual son necesarias herramientas para la protección del correo.

También es necesario proteger los endpoints que son otro de los principales puntos de entrada del malware. El malware es cada vez más sofisticado y es necesario acudir a tecnologías avanzadas que ya no solo se basen en detectar patrones de firmas, sino que, mediante el análisis de comportamiento, identifiquen y desactiven amenazas desconocidas en tiempo real, y que además nos ayuden a la hora de automatizar los procedimientos de respuesta y corrección."

Cuando planteamos qué tecnologías de seguridad serán imprescindibles en un futuro, opina que

"El malware es cada vez más sofisticado y es necesario acudir a tecnologías avanzadas que ya no solo se basen en detectar patrones de firmas"

"con las compañías invirtiendo en más tecnologías inteligentes y en automatización, y con la adopción de la Industria 4.0, (el cloud, dispositivos IoT) es vital que las soluciones de ciberseguridad sigan el ritmo de la adopción de tecnología para garantizar que las ventajas superan los riesgos", y apuesta por la Inteligencia Artificial y la gestión de identidades, mencionando Blockchain como una tecnología que tendrá un papel importante en el futuro. "Seguimos trabajando con passwords, y esto en algún momento se tendrá que acabar", añade.

Ahondando en la Inteligencia Artificial dice Enrique Solís que en realidad no se busca de manera independiente, "sino que buscas un producto que en función del benchmark conseguido, lo que te han contado, lo que has investigado tú o las pruebas de concepto que hayas podido realizar, te funcione y sea interesante". Añade que la inteligencia artificial es una herramienta más, capaz de hacer ciertas cosas mejor que los humanos, como el análisis y correlación de grandes cantidades de datos.

Enlaces de interés...

- 'La inspección de tráfico de red en tiempo real es fundamental' (Jesús M. Doña, EMASA)
- 'En general, no se aprovecha todo el potencial que ofrece la tecnología que has implantado' (Gustavo Lozano, ING)
- 'La IA nos ayuda muchísimo, pero hay que acompañarla con inteligencia humana' (José Israel Nadal, Age2)
- '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)

FORO it Digital Security

EVENTO ONLINE:

28 DE OCTUBRE DE 2022

PROTEGIENDO EL NUEVO PERÍMETRO

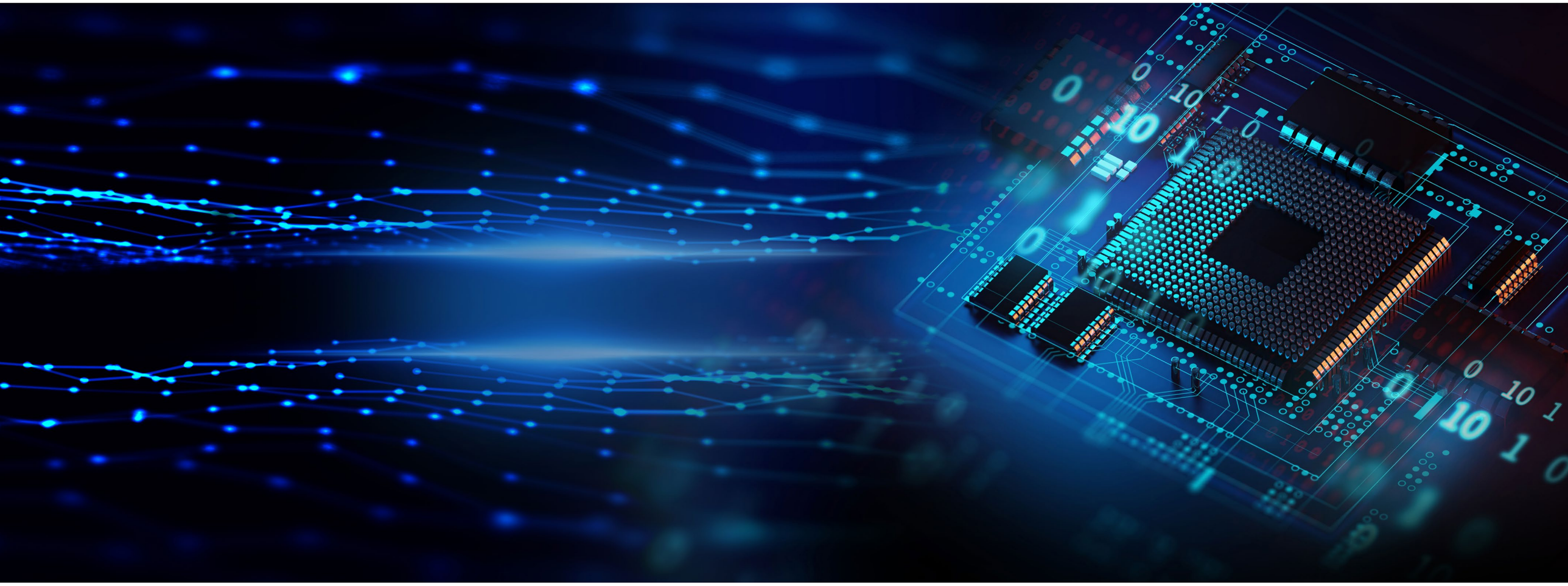
‘La concienciación del usuario es un pilar básico de una buena estrategia integral de seguridad’

(Roberto Alunda, Mediapro)

Ser un buen gestor, tener background técnico o tener visión empresarial son algunas de la cualidades que debe tener un buen CISO. Lo asegura Roberto Alunda, responsable de ciberseguridad de Mediapro a nivel global. Dice también el directivo que la concienciación, formación y actualización en seguridad de los usuarios es uno de los retos del CISO; que el phishing le preocupa más que el ransomware y que, de cara al futuro, habrá que ver cómo evolucionan los requerimientos de las empresas porque… ¿serán los mismos?

Rosalía Arroyo

No hay un camino definido para llegar a ser responsable de ciberseguridad. Lo habitual es que la inquietud personal y profesional vaya creando un camino plagado de autoaprendizaje. En el caso de Roberto Israel Alunda Espinosa, actual Global CISO del Grupo Media Pro, los inicios se dieron en el mundo de las telecomunicaciones, desde donde ha llevado la infraestructura de seguridad, sido responsable de comunicaciones y responsable de TI, entre otros, hasta llegar al cargo que ocupa actualmente.



"La combinación de personas y tecnologías es en lo que se debe basar una buena estrategia de ciberseguridad"

Respecto a la evolución de la figura del CISO, dice Roberto Alunda que ha pasado "de ser una figura inexistente a liderar la seguridad de las empresas". Asegurando que no hay dos empresas iguales a la hora de establecer directrices de IT o seguridad, dice también que la del CISO debería evolucionar a una figura que centralice todos los aspectos de seguridad, desde los relacionados con los procesos de negocio a los de usuario o la infraestructura, "para poder establecer una estrategia única y global".

Sobre el futuro del CISO "está muy ligado a la importancia que, por fin, después de muchos años, se está dando a la seguridad", dice Roberto Alunda, añadiendo que a medida que las empresas entiendan y aumenten la importancia de la seguridad que debe darse a los activos y usuarios, "el CISO como tal se convertirá en una figura clave para la empresa, si no lo es ya".

Comenta también el CISO Global de Mediapro que la figura del CISO debe evolucionar hacia un espacio único; "no todas las empresas tienen una

seguridad independiente, sino que suele recaer dentro de los departamentos de IT, y creo que debería ser independiente", manteniendo por supuesto la fluidez y colaboración con el resto de departamentos.

"Ser un buen gestor" es una de cualidades que debe tener un buen CISO. Añade Roberto Alunda que también debe tener "un background técnico importante" y destaca que tener una foto global de la seguridad de una empresa desde la base de conocimientos técnicos, además de normativos, "facilita establecer una estrategia de seguridad adecuada para la empresa". No se olvida de mencionar la necesidad de tener una visión empresarial que permita al CISO "adaptar la seguridad a la empresa, y no al revés".

Amenazas y tecnología

Preguntado por los principales retos de seguridad a los que se enfrenta Mediapro, comenta el CISO de esta compañía que se tienen los comunes a todas las empresas, como es "la necesidad de evolucionar constantemente tus sistemas de seguridad para hacer frente a las nuevas amenazas que aparecen continuamente". Añade que un reto importante es la concienciación, formación y actualización en seguridad de los usuarios, para después identificar como retos específicos de Mediapro el tamaño y la dispersión de la compañía, que tiene 60 sedes repartidas en 40 países y un core de negocio muy variado, por lo que "establecer un conjunto de estrategias y políticas únicas no siempre es fácil".

"El apoyo de la IA en la ciberseguridad es fundamental"

La amenaza que le quita el sueño es… “el ransomware, como a todo el mundo”, además del phishing, porque una vez robada la identidad del usuario se pueden generar incidentes de seguridad que realmente no se detectan de manera inmediata y en general suelen tener consecuencias destacables, asegura Roberto Alunda.

La concienciación del usuario “es fundamental. Es un pilar básico de una buena estrategia integral de seguridad”, dice el CISO Global de Mediapro, añadiendo que “es la primera línea de defensa porque los sistemas de seguridad que vienen después están para cuando esta línea ya se ha traspasado”. Dice también Roberto Alunda que la seguridad dentro de la empresa “es tan importante o más que la externa”, algo que hace años sonaba extraño pero que el tiempo ha demostrado y que se ha ido aterrizando en los sistemas de gestión de identidades y accesos, tecnologías SSO (Single Sign-On), cuentas privilegiadas, etc.

Sobre la inteligencia artificial, que muchos consideran imprescindible y otros cuestionan, dice Roberto Alunda que “depende mucho de las expectativas que se tenga en torno a ella”. Explica que nadie espera que una IA sea capaz de establecer una política de seguridad teniendo una foto global del grupo, entendiendo el negocio y gestionando un equipo, y por lo tanto hay que tener otro tipo de expectativas. Dice también el directivo que con la inteligencia artificial se mejora muchísimo la

"Con 60 sedes repartidas en 40 países y un core de negocio muy variado, establecer un conjunto de estrategias y políticas únicas no siempre es fácil"

"El CISO como tal se convertirá en una figura clave para la empresa, si no lo es ya"

anticipación de amenazas; que el procesamiento de datos y la toma de decisiones de manera automatizada es algo espectacular y que, en general "el apoyo de la IA en la ciberseguridad es fundamental". No se olvida de recordar que las amenazas son cada vez más sofisticadas y que "hay que estar preparados casi con las mismas armas"

Basado en su experiencia, la protección de endpoints, "si es posible con sistemas EDR", además de la seguridad en la capa DNS, los enfoques Zero Trust, segmentación de redes y seguridad interna son los pilares básicos de seguridad.

En seguridad, ¿todo es tecnología? "Yo creo que el factor humano es importante". Explica que la formación y concienciación del usuario es el primer paso hacia un sistema de seguridad, y que la externalización de los servicios, el contar con un gran equipo de seguridad "es una de las claves del éxito. La combinación de personas y tecnologías es en lo que se debe basar una buena estrategia de ciberseguridad".

Sobre las tecnologías que serán necesarias en un futuro, menciona el CISO de Mediapro que no son otras que las que ya están empezando a implementarse, como arquitecturas SASE basadas en entornos SD-WAN, un camino que "nosotros quisimos iniciar hace cinco años con las condiciones que había entonces y que la mayoría de las empresas tendrán que seguir, si no lo han hecho ya".

Asegurando que ya nadie se acuerda de lo que sucedió en la pandemia, del impacto del teletrabajo, responde el directivo que "habrá que ver cómo evolucionan los requerimientos de las empresas", porque todo parece indicar que a finales de año los empleados volverán de manera masiva a las oficinas. "En esa situación, ¿se volverá trabajar como antes? Los requerimientos de las empresas, ¿serán los anteriores?", son algunas de las preguntas que plantea Roberto Alunda, añadiendo que hay que esperar lo que nos depara este año en seguridad.

Enlaces de interés...

- 'La inspección de tráfico de red en tiempo real es fundamental' (Jesús M. Doña, EMASA)
- 'En general, no se aprovecha todo el potencial que ofrece la tecnología que has implantado' (Gustavo Lozano, ING)
- 'La IA nos ayuda muchísimo, pero hay que acompañarla con inteligencia humana' (José Israel Nadal, Age2)
- '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)

Forcepoint ONE

Welcome to the power of ONE

ONE Platform

ONE Console

ONE Agent

Forcepoint

www.forcepoint.com

‘Nos gusta pensar que abordamos la seguridad de una manera holística, integral’

(Javier Gallego, Dell Technologies)

Hace unos meses se presentaba la nueva generación de servidores Dell EMC PowerEdge. Una nueva propuesta compuesta por casi 20 máquinas que giran en torno a tres ejes: adaptabilidad, infraestructura autónoma y seguridad. Precisamente de este último hablamos con Javier Gallego, Sales Director de Data Center Compute Solutions de Dell Technologies.

La seguridad no es un tema ajeno a Dell Technologies. Sólo hay que recordar que hace poco más de cuatro años existía Dell Security, una unidad de negocio donde fluía el conocimiento acumulado de empresas como Quest o SonicWall. La compra de EMC por parte de Dell llevó a esta última a desprenderse de su negocio de seguridad con la venta de Sonicwall a Francisco Partners en noviembre de 2016. Por otra parte, Michael Dell es el propietario de SecureWorks, una empresa que ofrece servicios de consultoría, servicios profesionales, así como monitorización y gestión de amenazas.

Nos explica Javier Gallego, Sales Director de Data Center Compute Solutions de Dell Technologies, que el actual portfolio de la compañía incluye sistemas de computación, sistemas de almacenamiento, de red, y puestos de trabajo, “y nos gusta pensar que abordamos la seguridad de una manera holística, integral. No solo diseño, sino también en todo lo que es la configuración y la operación de los sistemas”. Añade el directivo que, en lo que respecta al centro de datos, “si bien no somos una empresa que se identifica como empresa de ciberseguridad per se, sí tenemos en cuenta todas estas necesidades desde el diseño a todo lo que tiene que ver con la gestión de software que va dentro de los sistemas,

"En nuestro dominio intentamos lograr la seguridad por defecto y hacer diseños lo más seguros posibles"

"El camino para avanzar de una manera más innovadora es tener una visión completa e información en tiempo real de lo que ocurre para detectar patrones"

asegurándonos de que no haya manipulación ni haya vulnerabilidades tanto en la parte de computación, como en la de red y la de almacenamiento".

Para el directivo de Dell, ser uno de los principales vendedores de computación representa una "responsabilidad añadida" en torno a la seguridad. Menciona una rigurosa gestión de la cadena de suministro, así como del control de todo el software que va dentro del servidor que le permite asegurar "que la configuración de hardware y software que salió de nuestra fábrica hasta que llega a casa del cliente no se ha manipulado ni alterado".

Sobre el almacenamiento, dice Javier Gallego que la seguridad del dato es vital, y que para ello es esencial asegurarse de que el dato no se altere ni manipule. La compañía hace frente al reto del ransomware ofreciendo a sus clientes soluciones de recuperación. "Tener una segunda copia no necesariamente es un sistema de protección porque en muchas ocasiones no sabemos desde cuándo hemos sido atacados". Dice Javier Gallego, añadiendo que la apuesta de Dell pasa por ofrecer la capacidad de tener una copia de seguridad no alterada y, segundo, tener capacidad de análisis para entender cuándo los datos han podido ser alterados de una manera artificial o sospechosa, aspectos que son "clave para que el servicio pueda ser restituido ante estos ataques".

Para Javier Gallego la propuesta va más allá de una solución de backup tradicional. La aproximación, explica, es mantener los datos a salvo almacenándolos de manera unidireccional, aplicar políticas

de no alteración y no manipulación y, si se detecta cualquier tipo de ataque malicioso, poder rebobinar, volver hacia atrás, al punto en que el ataque se produjo; “esta capacidad de analítica y de rebobinar y bobinar, y que además este software malicioso no contagie la copia crítica, es fundamental”.

¿Qué peso tienen este tipo de características específicas a la hora de comercializar estos productos? Responde Javier Gallego que el peso es mucho, que están observando cómo en las agendas de CIOs, CISOs y CTOs se plantean estas problemáticas y se busca “una aproximación más integral y más innovadora”. Añade que “en la medida que somos proveedor extremo a extremo de soluciones de puesto de trabajo, computación, red, almacenamiento, y recuperación, podemos ofrecer una solución completa no sólo desde el almacenamiento o backup tradicional, sino añadiendo la capacidad de estar protegido contra estos ataques”.

Llegados a este punto asegura el directivo de Dell que en algunos casos los proyectos pasan por desplegar productos hardware o software adicionales, y en otros por activar funcionalidades que el cliente ya tenía. Como ejemplo la solución de monitorización y analítica, Dell CloudIQ, que históricamente se ha estado utilizando para monitorizar los sistemas de almacenamiento, de backup, y predecir fallos; “ahora esta capacidad de IA y ML se está utilizando, además, para predecir ataques porque somos capaces de detectar comportamientos anómalos”. Esta herramienta está disponible de manera gratuita para los clientes de Dell.

Mercado en ebullición

No sé si al mismo ritmo del mercado, pero la seguridad evoluciona. Por cada nueva tecnología que aparece surgen diferentes formas de protegerla. En ciberseguridad el mundo de las startups es rico y complejo: por cada compra que lleva a la consolidación aparecen jóvenes empresas que promueven el cierre de un gap de seguridad. Al mismo tiempo, los players de seguridad tradicionales avanzan e innovan, y fabricantes como Dell, añaden opciones de seguridad en sus productos. El resultado es un mercado en plena ebullición, rico en innovación y sin una consolidación a corto ni medio plazo.

Dell CloudIQ, que históricamente se ha utilizado para monitorizar los sistemas y predecir fallos, se está utilizando ahora para detectar y predecir ataques

"Ser uno de los principales vendedores de computación representa una responsabilidad añadida en torno a la seguridad"

Enlaces de interés...

- Dell simplifica la recuperación ante ciberataques con nuevas soluciones
- Dell anuncia nuevas ofertas de seguridad para endpoints
- Dell y AWS protegen los datos de los clientes de los ataques de ransomware

Dice Javier Gallego que, como fabricante, Dell tiene su "cuota de responsabilidad a la hora de entender que nuestros productos, sean software o hardware, ya no residen, como ocurría antes, en un centro de datos, sino que nuestras solucionen viven en el Edge, en plataformas tradicionales y en el cloud. Nosotros tenemos una cuota responsabilidad de asegurar esos tres ejes sin ninguna duda". No significa esto, añade, que vayamos a intentar sustituir a los fabricantes tradicionales de seguridad; "en nuestro dominio intentamos lograr la seguridad por defecto y la no confianza por defecto, y hacer diseños lo más seguros posibles, no más".

El Edge y más allá

"El Edge se está convirtiendo en un mercado en sí mismo", asegura el responsable de soluciones de centro de datos de Dell, explicando que en la digitalización de las empresas no solo hay que asumir un avance tecnológico, sino que se está difuminando el perímetro de seguridad porque tenemos datos sensibles que ya no solo están en los centros de datos tradicionales, sino también en sedes remotas, en fábricas, etc.

En un futuro, ¿hacia dónde crees que se avanzará? "Vamos a seguir procurando que los sistemas sean seguros por diseño, que no haya alteración del hardware o del software en los procesos de fabricación o de despliegue en los clientes, y vamos a seguir activando funcionalidades específicas de seguridad en toda la gama, ya sea cómputo, red o almacenamiento". Además de lo mencionado, añade Javier Gallego que "el camino para avanzar de una manera más innovadora es tener una visión completa e información en tiempo real de lo que ocurre para detectar patrones". it

Compartir en RRSS

La Industria 4.0 ha acelerado la convergencia IT/OT. ¿Sabe qué hay en su red?

Detecte y mitigue las ciberamenazas antes de que provoquen incidentes de seguridad o paradas operativas.

FORESCOUT®

Automated cybersecurity across your digital terrain

www.forescout.com

it TRENDS

SEPTIEMBRE 2022

La digitalización de la pyme,

alimentando la productividad de nuestro tejido empresarial

TAMBIÉN EN ESTE NÚMERO...

UNA PUBLICACIÓN DE it Digital MEDIA GROUP

it TRENDS

Directora Arancha Asenjo arancha.asenjo@itdmgroup.es

Coordinadora Arancha Lafuente arancha.lafuente@itdmgroup.es

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

Diseño revistas digitales Eva Herrero

Producción audiovisual Miss Wallace, Alberto Varet

Fotografía Ania Lewandowska

it Digital MEDIA GROUP

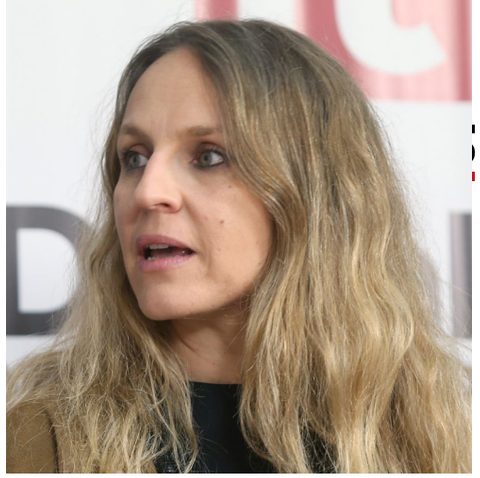
Director General
Juan Ramón Melara juanramon.melara@itdmgroup.es

Director de Contenidos
Miguel Ángel Gómez miguelangel.gomez@itdmgroup.es

Directora IT Events & Lead Gen Programs
Arancha Asenjo arancha.asenjo@itdmgroup.es

Directora División Web
Bárbara Madariaga barbara.madariaga@itdmgroup.es

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



Digitalizarse ya no es la cuestión

La transformación digital del tejido empresarial ha demostrado ser clave para la continuidad de los negocios, especialmente para unas pymes que están sufriendo los estragos de esta crisis que comenzó con los efectos del covid y se está alargando por el difícil contexto macroeconómico y geopolítico que estamos viviendo en estos momentos. Por esta razón, digitalizarse o no ya no es (o no debería ser) una decisión que las pequeñas y medianas empresas debieran plantearse.

Lo que sí deben medir bien las pymes, y cualquier organización, es cómo y dónde se invierte en tecnología para aprovechar su máximo potencial. En este sentido, Forrester publicaba recientemente algunas recomendaciones para enfocar adecuadamente esas inversiones de TI: obtener valor antes de reducir costes, reducir costes que no aportan valor al cliente y centrarse en la innovación pragmática.

Para alentar ese cambio, el Gobierno de España ha puesto en marcha el programa Kit Digital que entregará hasta 12.000€ a las pymes para dar su salto tecnológico. El plan se encuentra en fase de ejecución, tal y como explicó **Red.es** en la entrevista concedida durante el webinar "Tendencias tecnológicas que aportan valor al ecosistema pyme" celebrado el pasado mes de julio en nuestra web, para el que también contamos con la participación de **Adigital** y el **Cluster Cybermadrid** como invitados, y con **Quistor**, **NFON** y **KipmiON** como patrocinadores del encuentro.

La combinación de fondos, proveedores, tecnología y conocimiento alentará a las pequeñas y medianas empresas a acelerar su transformación digital y prepararse mejor para afrontar la situación actual. Intensa actividad, por tanto, la que tendremos por delante en el mercado tecnológico español en los próximos meses con la ejecución de estos planes que tanto ayudarán a las pymes a mantener su nivel de actividad y a los agentes digitalizadores a generar nuevas oportunidades de negocio. ■

Arancha Asenjo
Directora IT Trends
www.ittrends.es

QUISTOR

ORACLE | Partner

Alta disponibilidad y ciberseguridad en BBDD Oracle

Leer más

www.quistor.com

La tecnología jugará un nuevo papel **más alla de la transformación digital**

En los últimos años el auge digital ha llevado a muchas empresas a centrarse en la adopción de nuevas tecnologías, pero la importancia de lo digital es cada vez menor a medida que la tecnología se vuelve ubicua y menos relevante. En el futuro, las inversiones de las empresas se reconducirán de nuevo hacia activos más tangibles y vinculados a la producción y el negocio, mientras que seguirán cosechando los beneficios de la transformación digital.

La digitalización ha avanzado considerablemente en las dos últimas décadas, en las que muchas industrias tradicionales han invertido grandes recursos en la adopción de tecnologías digitales para llevar a cabo esta transformación y adaptarse a la nueva realidad de la producción y los negocios. Los investigadores de Gartner acaban de publicar un informe en el que anuncian una nueva era de productividad digital, en la que surgirán nuevos desafíos mientras las organizaciones tratan de aprovechar los beneficios de la digitalización.

Anticipan que el hype de lo digital va a ceder terreno ante otras necesidades más prácticas, lo que llevará a redirigir las inversiones hacia activos reales enfocados a crear productos y servicios. Aunque afirman que no se trata de un declive de lo digital en sí mismo, sino que es un paso necesario para que las tecnologías digitales se conviertan en "un motor sostenible de prosperidad económica". En esta nueva etapa se acabará la "exageración digital", bajará la especulación y el capital financiero se volverá a asociar al capital de producción, empleando la tecnología para fines más productivos.

Ed Gung, vicepresidente ejecutivo de investigación de la junta de investigación, señala que "a medida que se desvanezca la exageración en torno a la digitalización y disminuyan las estrategias impulsadas por el miedo a la disrupción digital, comenzaremos a ver mejores decisiones comerciales que conduzcan a una inversión real en activos productivos, ganancias de productividad, crecimiento del PIB y mejoras en los estándares de vida en todo el mundo".

Con ello quiere decir que la transformación digital ha llegado al punto en el que las organizaciones se enfocan en la recolección del valor de sus inversiones, en forma de una mayor productividad. Gung señala que la palabra digital dejará de representar un gran reclamo, como ha sido en las dos últimas décadas, y afirma que "las expectativas cambiarán y surgirán nuevos desafíos para los líderes tecnológicos". En su informe, Gartner describe las cuatro señales que presagian el cambio a una nueva era:

En esta nueva etapa se acabará la "exageración digital", bajará la especulación y el capital financiero se volverá a asociar al capital de producción, empleando la tecnología para fines más productivos

LA TECNOLOGÍA SE VUELVE OMNIPRESENTE, PERO MENOS VISIBLE

En los últimos años la tecnología digital se ha vuelto ubicua y muy común entre los consumidores, las empresas y los gobiernos, y poco a poco la tecnología informática subyacente irá

quedando en un segundo plano, siendo simplemente una herramienta para lograr un fin, perdiendo su preponderancia. En opinión de Gartner, esto plantea nuevas preguntas y retos para las grandes empresas, que cuestionarán cada vez más el verdadero valor de la infraestructura TI. Pero no podrán obviar la importancia de la tecnología para poder ofrecer servicios eficaces y de baja latencia a sus clientes.

LOS NEGOCIOS DIGITALES SE GENERALIZAN Y NECESITAN EVOLUCIONAR

La integración de tecnologías digitales en las industrias tradicionales progresa a buen ritmo, extendiéndose a todo el negocio, y en

TECNOLOGÍAS EMERGENTES QUE IMPULSARÁN LA INNOVACIÓN A PARTIR DE 2022

El avance digital en campos como la nube, la automatización basada en IA o las experiencias inmersivas se apoya en tecnologías emergentes que abren nuevos caminos y modelos de negocio. Los expertos de Gartner destacan en su último hype cycle tres áreas de tecnologías emergentes que están atrayendo la atención de la industria.

1 DESARROLLO DE EXPERIENCIAS INMERSIVAS. Las experiencias digitales evolucionan hacia lo inmersivo y esto se logrará gracias a varias tecnologías emergentes que facilitarán la creación de entornos virtuales para diferentes ámbitos empresariales y destinados al gran consumo. En este campo las más importantes son el metaverso, los tokens no fungibles (NFTs), las superaplicaciones y la Web 3. También tendrán un papel importante otras innovaciones como la identidad descentralizada, los humanos digitales o los gemelos digitales, que serán fundamentales para construir nuevos modelos de negocio en el Internet del futuro, donde surgirán nuevas vías de ingresos basadas en experiencias inmersivas.

2 AUTOMATIZACIÓN DE LA INTELIGENCIA ARTIFICIAL. La IA se expande a nuevos entornos y en el futuro formará parte de infinidad de aplicaciones, productos y servicios digitales. Es necesario avanzar en la creación de modelos de IA más especializados, cuyo desarrollo, capacitación e implementación deberá automatizarse para acelerar la entrega de soluciones basadas en IA. En Gartner opinan que la automatización de la IA redefinirá el papel de los humanos en el desarrollo de la inteligencia artificial, ofreciendo predicciones y decisiones más precisas y acelerando la obtención de beneficios. Las tecnologías que respaldarán la automatización acelerada de la IA son los sistemas autónomos, la inteligencia artificial causal, los modelos básicos, la IA de diseño generativo y la generación de código de aprendizaje automático. Ayudarán a impulsar la automatización de la IA, facilitarán su integración a nuevos niveles e impulsarán los beneficios derivados de la IA.

3 ENTREGA DE TECNOLOGÍA OPTIMIZADA. En Gartner opinan que los negocios digitales de éxito se construyen, no se compran, y que las tecnologías emergentes que pueden ayudar a lograrlo se centran en las comunidades de creadores de productos, servicios y soluciones. Lo que caracteriza a estas tecnologías emergentes es que proporcionan información y comentarios que contribuyen decisivamente a acelerar la entrega de productos, servicios y soluciones de los tecnólogos y aumentan la sostenibilidad de las operaciones comerciales. Destacan especialmente las FinOps aumentadas, los ecosistemas de datos en la nube, la sostenibilidad de la nube, el almacenamiento computacional, la arquitectura de malla de ciberseguridad, la observabilidad de datos, la gobernanza dinámica del riesgo, las plataformas de nube de la industria, la arquitectura mínima viable, el desarrollo impulsado por la observabilidad, OpenTelemetry y la ingeniería de plataforma.

poco tiempo dejará de ser un factor diferenciador para muchas empresas. Muchas de las más importantes están dejando de pretender convertirse en empresas tecnológicas, y están reenfocándose en modernizar su negocio a través de la tecnología, sin que esta sea el punto central de su estrategia. Gartner opina que, con el paso del tiempo, la tecnología digital se convertirá en "una dimensión más en la que compiten las empresas, como son las redes de distribución, los activos de capital, los derechos de explotación, las relaciones con los clientes o el contenido", entre otras áreas.

MAYOR REGULACIÓN DE LOS GIGANTES DIGITALES

La transformación digital de la sociedad y la economía ha impulsado el negocio de los gigantes digitales hasta situarlos entre las empresas de mayor capitalización del mundo. El avance digital que han realizado estos años ha generado gran controversia por el uso que hacen de la tecnología y los datos de las personas y las empresas, y los reguladores no han sido capaces de controlar sus actividades. Pero esto va a cambiar en los próximos años, permitiendo a las empresas más pequeñas competir en mejores condiciones con los gigantes tecnológicos. Gartner cree que a medida que el mercado tecnológico se vuelva más fragmentado y verticalizado, será más crítico para las empresas combinar la experiencia tecnológica con el conocimiento del dominio digital.

ENFOQUE EN LA RESILIENCIA ANTE EL MAYOR RIESGO TECNOLÓGICO

La progresiva integración de tecnologías digitales en las operaciones comerciales y gubernamentales, en la infraestructura y la vida cotidiana de las personas, aumenta el riesgo y la complejidad de la gestión de riesgos. Al mismo tiempo, la prisa por mejora la optimización y la eficiencia de las operaciones, dentro de las empresas y entre ellas, están generando una mayor interdependencia global, por lo que los problemas que surgen en un punto de la red empresarial pueden repercutir en otros puntos del globo.

Para combatir estos riesgos las empresas están empezando a optimizar sus redes digitales para incrementar su resiliencia y su eficiencia, y esta tendencia cobrará mucha importancia en el futuro, como forma de ganar ventajas competitivas en un ecosistema donde crece la incertidumbre y el riesgo. ■

MÁS INFORMACIÓN

- Gartner: Hype Cycle for Emerging Technologies, 2022
- La automatización empresarial será más inteligente en 2022
- Los ejecutivos quieren ampliar el alcance de la automatización en sus empresas
- Informe "Digital Twins: Adding Intelligence to the Real World"

La integración de tecnologías digitales en las industrias tradicionales progresa a buen ritmo, extendiéndose a todo el negocio, y en poco tiempo dejará de ser un factor diferenciador para muchas empresas

NFON

MÁS INFORMACIÓN

Con Cloudya

Tienes una plataforma
de comunicación en la nube

¡para todo!

KIT DIGITAL

El metaverso abre nuevos caminos
para las empresas de productos y servicios

Los entornos virtuales creados en el metaverso proporcionarán un escaparate ideal para infinidad de productos y servicios que los consumidores podrán ver y probar digitalmente. Aunque el metaverso todavía no ha tomado una forma definitiva se están realizando inversiones multimillonarias en el desarrollo de ecosistemas virtuales donde los vendedores podrán expandir su negocio.

El metaverso está generando grandes expectativas ¡para muchas industrias, que ven en este concepto de mundo virtual un nuevo canal con infinidad de posibilidades para expandir el negocio. En estos entornos las personas utilizarán un avatar para navegar por un universo virtual en el que las marcas podrán promocionar sus productos y servicios a través de experiencias digitales. Esto ofrece numerosas posibilidades para industrias como el comercio minorista, la automoción, la promoción inmobiliaria, las finanzas, el turismo y muchos otros sectores.

Un informe elaborado por McKinsey revela que la inversión total en el metaverso alcanzará unos 120.000 millones de dólares este año, destinados a construir entornos donde vender productos y servicios. Y sus investigadores es-

peran que para 2030, más del 50% de los eventos en vivo y el 80% del comercio electrónico podrían desarrollarse en el metaverso, aunque sea parcialmente. Esto genera nuevas esperanzas y también un a cierta reticencia para muchos vendedores, que ven en el metaverso un ecosistema complejo y difícil de abordar. Pero los expertos consideran que es más fácil de lo que parece y que las empresas que no crucen esta nueva frontera corren el riesgo de perder muchas ganancias.

En un informe publicado por la firma Capgemini sus investigadores aclaran los principios básicos del metaverso, definiéndolo como una variedad de entornos virtuales a los que se puede acceder a través de pantallas o gafas de realidad virtual, empleando avatares para interactuar con el entorno y realizar transacciones. Y cualquier operación que se realice dentro del metaverso permanece, por ejemplo, la adquisición de bienes y servicios. Estos espacios se componen de un front-end inmersivo, un entorno virtual 3D y una infraestructura back-end que valida las transacciones a través de tokens y blockchain, otorgando permisos de propiedad válidos.

Los proveedores de productos y servicios que quieran posicionarse en el metaverso tienen ante sí dos caminos posibles. Uno es construir equivalentes virtuales de productos, como puede ser un vehículo, una prenda de ropa o un dispositivo, que se podrían utilizar de forma virtual. Otro camino posible es adquirir terrenos o construir un espacio virtual propio para exponer productos y servicios de cualquier naturaleza. Cada marca deberá valorar si entrar a formar parte de un metaverso creado por otras partes o construir el suyo propio, y en ambos casos existen muchas oportunidades de desarrollo de negocio, y de promoción a través de eventos y experiencias digitales. Gracias a las salas de exhibición virtuales es posible vender a los consumidores, pero también es un terreno fértil para los negocios B2B.

Cada marca deberá valorar si entrar a formar parte de un metaverso creado por otras partes o construir el suyo propio

Los expertos señalan que para hacer negocios en el metaverso las empresas de productos y servicios, la mayoría fuera del ámbito de la tecnología, necesitan desarrollar una estrategia centrada en el valor. Por ello, recomiendan no dar este salto tecnológico sin tener un plan, en el que deberían definir cuáles son sus objetivos para el metaverso. En su informe, emiten una serie de recomendaciones a estas empresas.

Explican que la clave está en la experimentación y, dado que todavía no está clara la forma que tomará el metaverso, es importante poner sobre la mesa todas las ideas e hipótesis sobre lo que pueden realizar en el metaverso, y realizar pruebas de concepto para identificar las vías más prometedoras. Y destacan que, incluso si no se pueden identificar casos de uso de alto potencial a corto plazo, estos irán surgiendo en el futuro. Por ello es importante recopilar información sobre cómo los usuarios interactúan con sus ofertas, y es vital lanzar proyectos piloto para obtener esta información. Asimismo, esto permitirá probar y pulir los proyectos iniciales, descartar aquellos que muestran indicios de fracaso e identificar nuevas oportunidades.

Para los expertos es muy importante que las empresas no se centren exclusivamente en la parte tecnológica del metaverso, lo que podría generar atascos y dejar casos de uso sin desarrollar. En cambio, recomiendan centrarse en el caso de uso comercial y confiar en que la tecnología facilitará su desarrollo. Y señalan como ejemplo el avance de tecnologías consideradas como básicas para los negocios en el metaverso, como los contratos para transacciones virtuales. Además, ya han surgido vendedores de terrenos virtuales que proporcionan a los clientes empresariales un lugar donde desarrollar sus iniciativas de negocios en el metaverso. ■

MÁS INFORMACIÓN

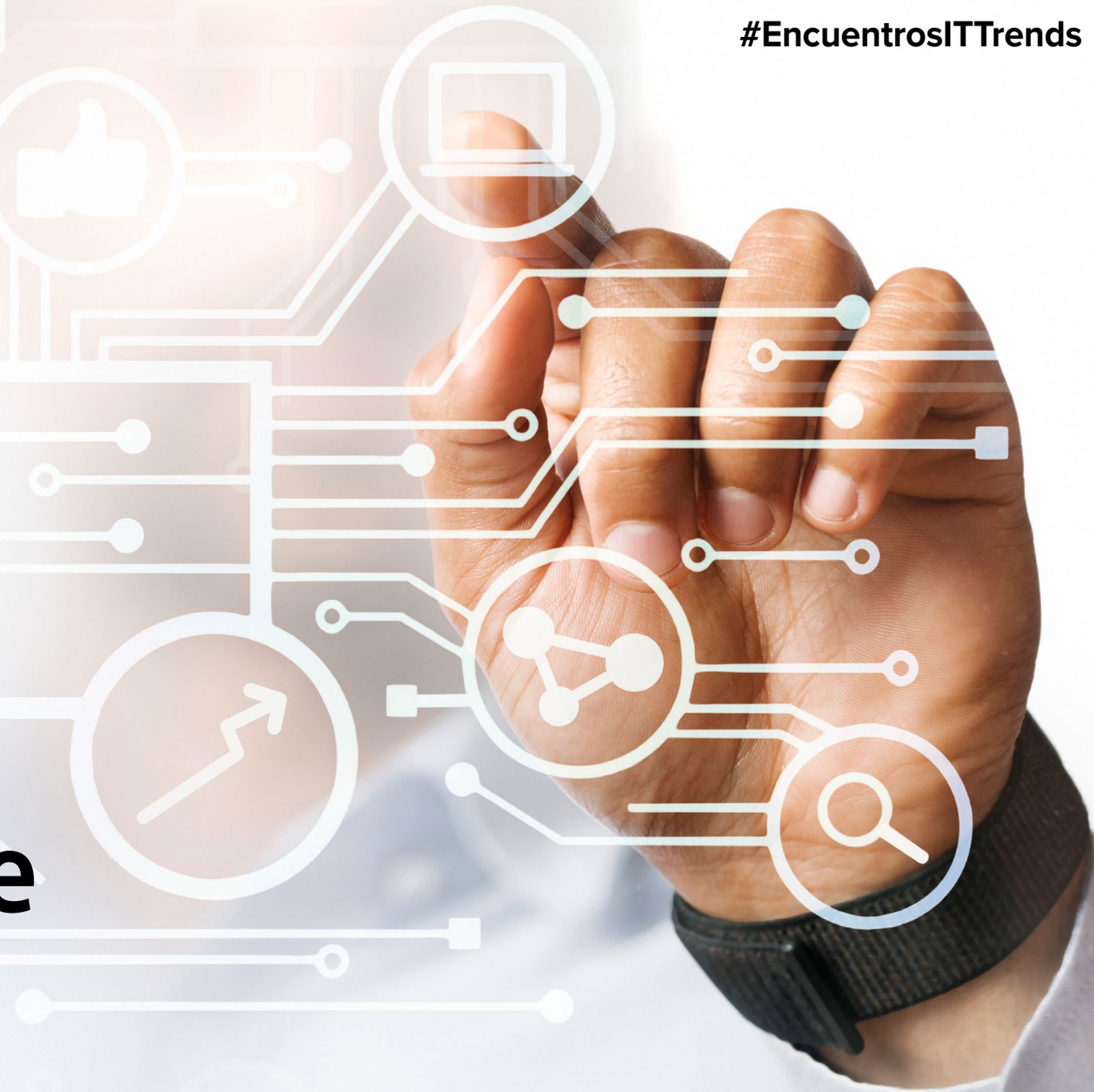
- Ecosistemas, efecto de red, la nube y los datos, puntos en común de las grandes tecnológicas extrapolables al negocio del Metaverso
- Metaverso y videojuegos se alían para superar los 2.000 millones € en España en 2023
- Ordenando el metaverso. Claves para no quedarte fuera del ciclo de innovación
- El futuro de los NFTs está ligado al metaverso

itTRENDS

#EncuentrosITTrends

Tendencias tecnológicas

que aportan valor al ecosistema pyme



adigital QUISTOR NFON kipmiOn® Informática Sistemas Soluciones

La digitalización de la pyme,
alimentando la productividad de nuestro tejido empresarial

El grado de madurez digital de las pequeñas y medianas empresas es un factor fundamental para mejorar la competitividad del conjunto del tejido productivo, y las españolas son conscientes de ello. En cuatro años, siete de cada diez pymes españolas habrán incrementado notablemente su inversión en TI para ser más resilientes y capitalizar las condiciones de mercado.

Para finales de 2022, el 10% de las pymes representará el 20% de la creación de nuevos puestos de trabajo en las economías desarrolladas. No cabe duda de que su peso en el economía es elevado. Según un estudio llevado a cabo por IDC, el grado de madurez digital de este tipo de organizaciones es esencial para aumentar competitividad del conjunto del tejido productivo y, según sus conclusiones, las pymes son conocedoras de ello, ya que, en cuatro años, el 70% las pymes españolas habrán incrementado notablemente su inversión en TI para ser más resilientes y capitalizar las condiciones de mercado.

LA PEQUEÑA Y MEDIANA EMPRESA REPRESENTA UN CUARTO DE LA INVERSIÓN TOTAL EN TI

Según apunta el informe, la inversión total de TI en España en el año 2021 ascendió a más de 49.000 millones de euros, de los cuales 12.000 millones correspondieron a pequeñas y medianas empresas, es decir, el 25% del total. El crecimiento previsto para este año es ligeramente inferior al 4% y, entre las principales demandas de tecnología por parte de las pymes, destacan especialmente la Inteligencia Artificial, que crecerá por encima del 30% a lo largo de 2022, junto a los entornos cloud, con un 30%.

USO DE TECNOLOGÍAS DIGITALES POR EMPRESAS EN ESPAÑA

El Observatorio Nacional de Tecnología y Sociedad ha creado Brújula, una publicación que busca detectar el impacto de las tecnología en las personas y dar orientación sobre los indicadores de la sociedad digital. Dentro de esta colección, el informe Uso de tecnologías digitales por empresas en España, desgrana las claves de la digitalización y las inversiones de las compañías españolas.

Las inversiones en aplicaciones colaborativas y ciberseguridad registrarán aumentos superiores al 19% y 12%, respectivamente.

En cuanto a la prioridad de inversión de las pymes en el corto y medio plazo, el estudio ha identificado cuatro bloques relevantes: todo lo relacionado con el cliente para mejorar las interacciones con sus productos y servicios, la toma de decisiones basadas en datos, especialmente en lo relacionado con la monetización; la securización de estos datos y, finalmente, la conexión de la pyme con el ecosistema y su impacto operativo en la distribución.

En el contexto de digitalización integral postpandemia, el análisis de IDC resalta los beneficios de la virtualización como la fuente de oportunidad que la pyme, que ya ha comprobado las ventajas de adoptar cloud en la gestión del puesto de trabajo y están avanzando en la gestión de clientes (CRM) y de procesos (ERP).

En la misma línea, el estudio también sostiene que, para ayudar en todos estos procesos, un gran aliado para las pymes son las soluciones o plataformas integradas y estandarizadas que "democratizan" el acceso a la digitalización holística. En este punto cabe destacar el importante papel como asesores de los proveedores de software independientes (ISV).

CLAVES PARA LA DIGITALIZACIÓN

En primer lugar, contar con socios relevantes va a suponer un rol crucial en la competitividad de las pequeñas y medianas empresas: IDC pronostica que el 20% de las menos digitalizadas deberán ampliar sus alianzas si buscan seguir en el mercado en 2023. Por el contrario, el 30% de las pymes más maduras participarán activamente en los ecosistemas para crecer y expandirse.

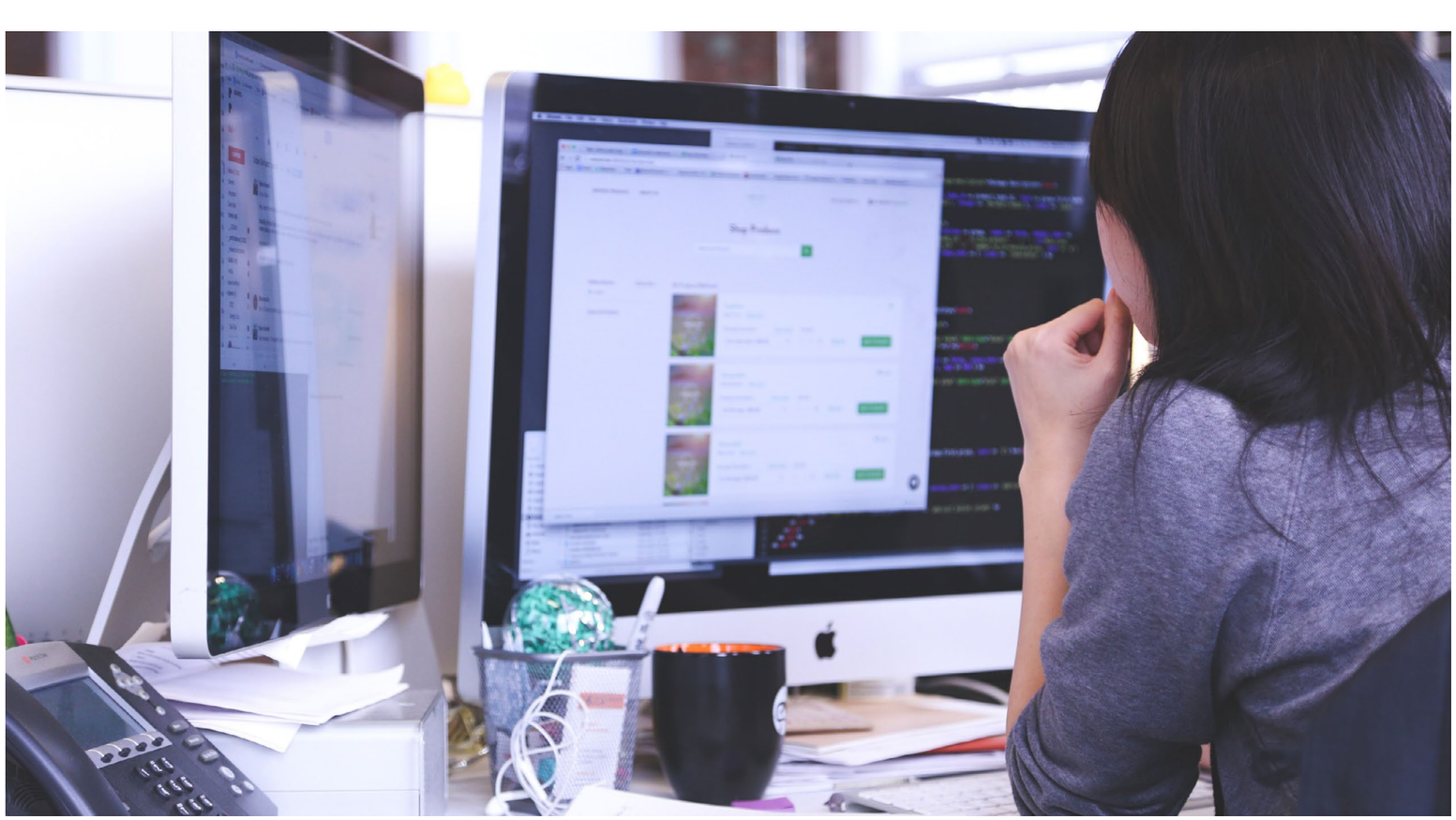
Por otra parte, está la innovación y disrupción digital como modelo de negocio, que está en auge, según el estudio. Para 2024, el 75% de las startups habrá adoptado tecnologías de próxima generación desde su inicio.

Finalmente, la experiencia del cliente, gracias a la tecnología y una conectividad mejorada, donde 5G comenzará a generar casos de uso de alto valor y en el que la capacidad de co-

nocimiento y personalización de la oferta a los clientes de un salto cuantitativo y cualitativo a través de tecnologías como el Machine Learning. El estudio confirma que en dos años el 33% ya ofrecerá a sus experiencias virtuales y orientadas a datos.

DIGITALIZACIÓN DE LAS PYMES

Pero para ver la realidad, más allá de las tendencias, hay que fijarse en los datos proporcionados por el ONTSI. En 2022, el Observatorio Nacional de Tecnología y Sociedad ha creado Brújula, una publicación diseñada para detectar el impacto de las tecnología en las personas y dar orientación sobre los indicadores de la sociedad digital. Dentro de esta colección, el informe Uso de tecnologías digitales por empresas en España, desgrana las claves de la digitalización y las inversiones de las compañías españolas, y una de las principales conclusiones es que las empresas españolas han acelerado su transformación digital en 2021, incrementando el uso de tecnologías emergentes tales como la IA, Analítica, Cloud e IoT,



COVID-19 Y LA ADOPCIÓN DE TECNOLOGÍA EN LAS PYMES

Las pequeñas y medianas empresas (pyme) representan más del 90% de todas las empresas del mundo y crean siete de cada diez puestos de trabajo, pero tienen entre siete y diez menos posibilidades de utilizar determinadas tecnologías que las más grandes. En este contexto, el Foro Económico Mundial desarrolló un Protocolo de Políticas con el objetivo de reducir barreras y promover la adopción de la tecnología digital por parte de las pyme. El protocolo identificó cinco retos principales: personas y capacidades financiación; proceso e infraestructura; tecnología y preparación; estrategia; y ecosistema.

En este informe, el Foro Económico Mundial tiene como objetivo proporcionar información sobre cómo la COVID-19 ha afectado a la adopción de tecnología por parte de las pyme. El estudio pretende complementar y mejorar el Protocolo de Políticas y aportar una contribución novedosa al conjunto de trabajos que buscan comprender los retos que rodean a la tecnología digital en las pyme y facilitar la adopción de la tecnología digital en estas empresas.

siendo esta última la que más ve crecer su uso. En concreto, ha sido adoptada por el 28% de las empresas.

En cuanto a la tecnología más extendida es Cloud, dado que una de cada tres compañías ya está consumiendo servicios en la nube, con niveles todavía lejanos a otras tecnologías más establecidas, como la firma electrónica (82%), los medios sociales (67%) o los sistemas de intercambio electrónico de datos (52%).

Sin embargo, este proceso de digitalización no es uniforme en todos los tamaños ni en todos los sectores. De hecho, la diferencia en el grado de transformación digital de las pymes, respecto a las grandes compañías, es importante, sobre todo en tecnologías como la computación en la nube, el intercambio automático o la Inteligencia Artificial.

LA PYME Y LA INTELIGENCIA ARTIFICIAL

Una de las tecnologías emergentes con mayor aplicabilidad en todos los sectores es la Inteligencia Artificial, si bien la adopción es todavía incipiente en todo tipo de empresas. De hecho, solo un 8% de las empresas españolas ha implementado esta tecnología, siendo Madrid, con un 11,5%, la comunidad autónoma donde las empresas han apostado más por la IA.

Evidentemente, la presencia de la IA en las grandes empresas es mayor que en el resto. Así, una de cada tres grandes firmas ya usa la IA, mientras que el porcentaje se reduce al 14% en las medianas y solo alcanza el 6% en las pequeñas. Por sectores, TIC y Comunicaciones cuentan con un mayor número de empresas que apuestan por la IA, mientras que Construcción o Metalurgia ocupan los últimos lugares del ranking.

Frente a las ventajas evidentes que ofrece el uso de esta tecnología, las principales razones que aducen las empresas para no usar la IA es la falta de conocimientos (3%), los altos costes (3%), la disponibilidad o calidad de los datos necesarios para aplicar estas tecnologías (2%), la incompatibilidad con equipos, software o sistemas existentes (2%), la falta de claridad sobre las consecuencias legales (2%) o problemas con la protección de datos (2%).

BIG DATA EN LA PEQUEÑA Y MEDIANA EMPRESA

Con la reducción de costes como objetivo, las empresas se han adentrado en el Big Data. De hecho, ya el 11% de ellas lo están utilizando, si bien el porcentaje es muy superior en las grandes (29%). En el caso de las medianas, hablamos de un 18%, mientras que en las pequeñas apenas llega al 9%, pese a que el desarrollo de la nube y la existencia de herramientas analíticas fáciles de usar hacen que esta tecnología emergente sea algo más asequible.

También hay diferencia en cuanto a los datos que se emplean para los análisis. Frente a

DIGITALIZACIÓN DE LA PYME: CRECIENDO DESDE LAS PLATAFORMAS DE COLABORACIÓN

En un tejido empresarial como el español, donde el peso de la pequeña y mediana empresa es muy superior a otros países europeos, el grado de madurez digital de este tipo de organizaciones es un factor fundamental para mejorar la competitividad del conjunto del tejido productivo.

De cara a facilitar el crecimiento de las Pymes, resulta fundamental hacer una aproximación holística de la digitalización que incluya las herramientas de colaboración, donde el avance en estos últimos años ha sido destacable pero abarque el resto de las áreas de negocio de la empresa. Así, la inteligencia del dato y comercial, la gestión de los clientes (CRM), la automatización de procesos y las herramientas de gestión de recursos (ERP) deben acompañar en este viaje hacia las tecnologías digitales.

un 52% de las grandes firmas que utilizan datos propios, dado que tienen mayor capacidad para generarlos y tratarlos, el porcentaje en las pequeñas empresas se queda en un 20%, que complementan los análisis de datos con otras fuentes externas de información.

LA EMPRESA ESPAÑOLA SE SUBE A LA NUBE

Como decíamos, de las tecnologías emergentes es el Cloud Computing la más extendida entre las compañías españolas, y es que un 32% de ellas declararon haber utilizado servicios en la nube. Aunque, como ocurre con el resto de tecnologías, no es igual la presencia en cloud de las grandes firmas (68%), que de las medianas (48%) o de las pequeñas (29%).

Los servicios más solicitados son el correo electrónico y el almacenamiento de ficheros, el 81 y 80%, respectivamente. Además, el cloud se emplea como servidor de bases de datos (70%) y para proveer software (64%) y aplicaciones informáticas de seguridad (63%), así como para software financiero o contable (41%), software para tratar información sobre clientes (39%), para ejecutar el software de la empresa (36%), aplicaciones informáticas de planificación de recursos empresariales (34%) y plataformas informáticas que alojan entornos de desarrollo, prueba o implementación de aplicaciones (30%).

FUERTES EXPECTATIVAS CON IOT

Siguiendo la línea mostrada por los datos de este informe, Internet de las Cosas es, y se espera que siga siendo, la tecnología emergente con mayores ratios de crecimiento. Las grandes empresas tienen mayor propensión a utilizar IoT: su empleo casi duplica al de las pequeñas. Destaca la gran adopción de esta tecnología por los sectores de energía y agua (63%), la industria de alimentación, textil, madera y artes gráficas (54%) y de fabricación electrónica, informática, material eléctrico, vehículos y muebles (53%). La mayor parte de las empresas que usan IoT lo emplean para aspectos relacionados con la seguridad de las instalaciones (76%). A mucha distancia están otras aplicaciones, como la gestión de consumo de energía (29%), mantenimiento (22%) y logística (21%), procesos de producción (19%) y servicio al cliente (15%).

COMPARTICIÓN ELECTRÓNICA DE DATOS

Pero si hay dos tecnologías que muestran la intensidad digital de las empresas españolas, estas son el ERP y el CRM. En el caso del primero, estaba presenten en 2021 en más de la mitad de las empresas de nuestro país, alcanzando casi el 48% entre las pequeñas y elevándose al 71% entre las medianas. Por lo que respecta el CRM, el porcentaje de uso global se sitúa por debajo de la mitad de las empresas (41,8%), si bien, en este caso, el informe no distingue los porcentajes en función del tamaño de las empresas. ■

MÁS INFORMACIÓN

- Uso de tecnologías digitales por empresas en España
- Digitalización de la pyme: creciendo desde las plataformas de colaboración
- Covid-19 y la adopción de tecnología en las pymes
- Ocho de cada diez pymes creen que aumentarán su facturación con la digitalización
- Las pymes españolas, optimistas sobre su capacidad de atraer y retener el talento

Si te ha gustado este artículo, compártelo

#ENCUENTROSITTRENDS

Tendencias tecnológicas que aportan valor al ecosistema pyme

El tejido empresarial español está constituido en su mayor parte por pequeñas y medianas empresas. De hecho, un 99 por ciento de las compañías de nuestro país se encuentran en esta categoría. Su digitalización es fundamental para aumentar la competitividad, tanto de ellas como de la economía española. Por este motivo, es esencial ir dando pasos progresivos en este camino, algunos de los cuales analizamos en este encuentro desde diferentes ángulos: el institucional, el empresarial y el tecnológico.

#EncuentrosITTrends

Aunque hace un par de años parecían mostrarse más reticentes a apostar por la digitalización que las firmas de mayor tamaño, lo cierto es que se ha producido una aceleración de la transformación digital tanto en las medianas como en las organizaciones más pequeñas, independientemente de su sector. Estas últimas tienen la oportunidad única de beneficiarse de las ayudas provenientes de los Fondos Europeos Next Generation UE mediante la solicitud del Kit Digital.

De todo esto hablamos en este Encuentro IT Trends en el que hemos repasado:

- ¿Cómo las pymes pueden obtener ventajas de las tendencias tecnológicas actuales?
- ¿Cómo están generando valor gracias a la tecnología?
- ¿Qué les está aportando en este 2022?
- ¿Qué tecnologías permiten a las pequeñas y medianas empresas ganar productividad?
- ¿Cómo solicitar y sacar el máximo provecho al Kit Digital?

Puedes leer las principales conclusiones de este Encuentro IT Trends a continuación. ■

ALBERTO MARTÍNEZ LACAMBRA, DIRECTOR GENERAL, RED.ES

“La digitalización ha calado en las pymes”

Una de las asignaturas pendientes de la pequeña y mediana empresa española es la digitalización, o, así al menos, se percibe en nuestro país. ¿Es esto cierto? ¿Se están dando los pasos adecuados para elevar el nivel tecnológico de nuestras pymes?

Tal y como explicaba Alberto Martínez Lacambra, director general de Red.es, en la sesión inaugural del Encuentro IT Trends: Tendencias Tecnológicas que aportan valor a la pyme, “existe espacio de mejora. Creo que están progresando de manera adecuada. No podemos olvidar la crisis que tuvimos en 2008 y, posteriormente, la pandemia, y el objetivo de las pymes ha sido sobrevivir. Pero es cierto que la Covid nos ha dejado claro que la digitalización ha venido para quedarse, y el concepto cultural de la digitalización ha calado en las pymes”.

“Evidentemente”, añadía, “se puede mejorar, algo que podemos ver claramente en la productividad. Si analizamos este dato en las empresas grandes y medianas en comparación con sus homólogas europeas, la productividad es similar, pero hay espacio de mejora en las pequeñas de menos de 50 empleados, por lo

“EXISTE ESPACIO DE MEJORA EN LA PRODUCTIVIDAD DE LAS PEQUEÑAS EMPRESAS”

que hay que empujarles hacia la senda de la digitalización, porque eso mejorará, sin duda, su nivel de productividad".

Una clara señal de esta necesidad son las cifras del portal Acelera Pyme, abierto el pasado mes de noviembre y que cuenta ya con "220.000 pymes registradas, sobre todo pequeñas empresas".

TECNOLOGÍAS PARA DIGITALIZAR A LAS PEQUEÑAS Y MEDIANAS EMPRESAS

En palabras de Alberto Martínez Lacambra, "en el caso de las más pequeñas, se está trabajando para que se incorporen a las soluciones básicas de digitalización. Pero eso es un paso, y podemos ver tres niveles: estas soluciones básicas de digitalización, el cambio cultural, y la digitalización avanzada, donde hablamos de tecnologías habilitadoras. Necesitamos que entren todas en la senda de la digitalización para favorecer el cambio cultural y que lleguen todas a esas tecnologías habilitadoras, que van a ser de extrema relevancia para el futuro de nuestras empresas y nuestra economía".

Pero no todas las empresas han iniciado el camino. Tal y como explicaba el director general de Red.es, "se trata de una cuestión de supervivencia. Es necesario hacerlo para avanzar en la digitalización. Las que no se han ido sumando ha podido ser por una cuestión cultural, y la Covid ha puesto sobre la mesa la necesidad del cambio; o por una cuestión económica, y ahora con el Kit Digital tienen una gran oportunidad".

"Estoy convencido que todas las empresas que lo soliciten y cumplan los requisitos, podrán acceder a la ayuda"

KIT DIGITAL

Tecnológicamente, el Kit Digital ofrece "soluciones básicas de digitalización. Es un programa de adopción digital para nuestras pymes, sobre todo las de menos de 50 empleados. Cuenta con una dotación de 3.000 millones de euros, y un objetivo de llegar a 1 millón de compañías".

Las empresas entre 10 y 50 empleados, nos explicaba, "recibirían 12.000 euros, las empresas de entre 3 y 10 empleados 6.000, y las de menos de 3 empleados 2.000 euros. La primera convocatoria, de 10 a 50 empleados, se lanzó en marzo y contamos con más de 65.000 solicitudes y ya hemos otorgado alrededor de 20.000 subvenciones. La siguiente convocatoria se publica en julio y la tercera entre octubre y noviembre".

Cada convocatoria se abre con 500 millones, ampliables según se necesiten más recursos, por lo que "estoy convencido que todas las empresas que lo soliciten y cumplan los requisitos, podrán acceder a la ayuda", apuntaba Alberto Martínez Lacambra.

Se trata de un programa de digitalización de pymes y, como señalaba el director general de Red.es, "parecía razonable que las pymes digitalizadoras locales pudieran participar en él. Por tanto, hay una figura extremadamente importante, el Agente Digitalizador, para instalar las soluciones. En este momento contamos con casi 9.000 agentes digitalizadores, y es una gran oportunidad para el sector. Es un magnífico ejemplo de colaboración público-privada". ■

MARÍA LÁZARO ÁVILA, DIRECTORA DE DESARROLLO Y MARKETING DE ADIGITAL

“La digitalización es un factor fundamental para la competitividad”

Adigital publicó a principios de año su informe anual que mide el impacto de la digitalización en la economía española, un dato que en la última revisión muestra un incremento de tres puntos sobre el pasado año en el aporte de la economía digital al Producto Interior Bruto.

La Asociación Española de la Economía Digital participó en el Encuentro IT Trends: Tendencias Tecnológicas que aportan valor a la pyme, representada por su directora de desarrollo y marketing, María Lázaro Ávila, que nos explicó que, a la luz de los datos del informe La Economía Digital en España, “la economía digital representó el 22% del PIB, tres puntos más que el año anterior. Pero si analizamos el impacto directo, llegó al 11,9% del PIB, lo que supone también dos puntos más que el año precedente, lo que demuestra que la digitalización de la economía es un proceso creciente, constante y que es fundamental para la competitividad y el crecimiento del país. Las empresas más digitalizadas son las más competitivas y las que ha resistido mejor el impacto de la pandemia. Son las que más han crecido durante la pandemia.

“ES FUNDAMENTAL EL IMPULSO AL TALENTO DIGITAL”

Hemos visto también que el cambio producido durante la pandemia ha sido estructural, no hay marcha atrás. Tenemos la oportunidad de convertirnos en hub digital para generar nuevos productos y servicios que nos ayuden a mejorar aún más la competitividad".

PROGRESOS EN LA DIGITALIZACIÓN DE LAS PYMES

En opinión de María Lázaro Ávila, "si nos remitimos a los datos, en el Índice DESI España ocupa el puesto 16 en la utilización de la tecnología por parte de las empresas, muy por detrás de otros países, algo significativo porque las pymes representan el 99% de las empresas y generan el 36% del empleo, 17 puntos más de otros países, como Alemania. Sigue habiendo dificultades para que las empresas españolas integren la tecnología, pero nuestra labor es ayudarles para que podamos seguir avanzando".

La digitalización es, en palabras de nuestra entrevistada, "un factor fundamental en la competitividad, porque te permite acceder a nuevos clientes, mejorar la internacionalización, permite ser más eficiente...".

En el caso de Adigital, "trabajamos en varios ejes. Por una parte, nuestra vocación es ejercer de puente entre la Administración Pública y las organizaciones privadas en todo lo relacionado con cuestiones como la Inteligencia Artificial, la Economía del Dato, la gestión del talento digital... Desde nuestra asociación, apoyamos todos los procesos de digitalización de las pymes y cubrimos todo un espacio digital que dinamizamos con iniciativas de innovación abierta, promoción y difusión de tendencias en digitalización, la elaboración de métricas... Pensamos que es muy importante también el impulso de la cultura digital en la ciudadanía para la adopción responsable de la tecnología y para la promoción del talento que nos permita cerrar la brecha entre la formación y la demanda de talento digital".

Asimismo, continuaba, "somos Agentes Digitalizadores con soluciones avaladas por instituciones públicas, como el Sello Confianza Online, que acredita la transparencia de los e-commerce; el Servicio de Lista Robinson; o el Certificado de Empresa Digitalizadora, que avala la experiencia de los proveedores de servicios digitales".

FACTORES DE LA DIGITALIZACIÓN

Para María Lázaro Ávila, "es fundamental que la digitalización se asuma desde la propia dirección de la empresa, para que cale en el resto de la organización. Es fundamental el impulso al talento digital, porque las profesiones tecnológicas son las que más inversión van a atraer y las que generan menos temporalidad en el empleo. Es importante que las grandes compañías se impliquen en el apoyo y promoción de la digitalización de las más pequeñas y que las empresas tengan presente la necesidad de inversión en tecnología y comunicaciones, que pueden mejorar sus procesos de forma significativa".

> **"Es fundamental que la digitalización se asuma desde la propia dirección de la empresa, para que cale en el resto de la organización"**

Existen actualmente muchos programas y mucha inversión centrada en promover la digitalización de las pymes, y es importante "estar pendientes de cuándo y cómo se convocan todas estas ayudas. Somos conscientes de que esto es difícil, por lo que nosotros ofrecemos un servicio específico para ello para nuestros asociados, asesorándoles y acompañándoles en el proceso para poder aprovecharlas". ■

#MESAREDONDA

Tendencias tecnológicas que aportan valor al ecosistema pyme

Son múltiples y variadas las tendencias tecnológicas que ayudan a las empresas en sus procesos de modernización y digitalización, que les permiten incrementar su productividad y competitividad, y que les capacitan para crecer y consolidarse en un mercado cada día más exigente. Sin embargo, por su propia naturaleza, las pequeñas y medianas compañías tienen una serie elementos diferenciadores que impactan de forma directa en la tecnología que pueden usar y aprovechar.

Para hablar de ello, en el Encuentro IT Trends: Tendencias Tecnológicas que aportan valor a la pyme, se organizó una mesa redonda que contó con la participación de Sem

Sem Guillem (KipmiON Tecnología), María José García Brao (NFON), y Luis Mediero (Quistor), comentan en esta mesa redonda las principales tendencias tecnológicas que aportan valor a la pyme. Clica en la imagen para ver el vídeo.

“Tenemos que dejar claro a la pyme que los beneficios de la digitalización superarán ampliamente las inversiones realizadas”

SEM GUILLEM, SOCIO GERENTE, KIPMION TECNOLOGÍA

Guillem, socio gerente de KipmiON Tecnología; María José García Brao, directora de ventas de canal de NFON; y Luis Mediero, tech manager de Quistor, y en la que se puso el foco en las diferentes tendencias tecnológicas que aportan valor a las pequeñas y medianas empresas.

USO DE SERVICIOS CLOUD

Una de estas tecnologías es la nube. El uso de servicios cloud es una práctica generalizada en las grandes empresas, pero no tanto en las pymes. Según el ONTSI, solo el 29% de las pymes lo hacen, frente al 48% de las medianas y el 68% de las grandes. Pero ¿es imprescindible la nube para la digitalización?

Tal y como comentaba Luis Mediero, “la nube es una pieza fundamental, pero no siempre es imprescindible. Está muy relacionado con el uso que dan las empresas a su base de datos, y algunas cuentan con normas expresas que impiden que estos datos salgan de sus instalaciones, con lo que no pueden usar la nube. Para otras, las comunicaciones no ofrecen la respuesta necesaria y prefieren tener la base de datos on-premise. Esto pasa, incluso, con desarrollos muy digitalizados en algunos clientes. Es muy importante hacer un análisis completo de la situación real de la seguridad, las comunicaciones y la arquitectura global antes de emprender un proyecto cloud, sobre todo cuando hay bases de datos implicadas”.

En palabras de María José García Brao, “la nube es un medio. Lo que es imprescindible es la digitalización, porque les abre grandes oportunidades de crecimiento y les permite subsanar la brecha tanto funcional como territorial que les diferencia de las grandes empresas. La digitalización les va a permitir crear nuevos modelos de negocio. La nube ofrece un sinfín de beneficios para las pymes, tanto económicos como tecnológicos. Al ser un modelo de pago por uso, el cliente no necesitará un gran desembolso inicial, y podrá optimizar sus recursos según sus necesidades. Además, la pyme podrá incorporar soluciones y redefinir su modelo cuando lo precise, accediendo a tecnología solo disponible antes para las grandes corporaciones. La nube le va a permitir que su negocio siempre esté en vanguardia”.

Finalizaba esta primera ronda de opiniones Sem Guillem destacando que “lo que es imprescindible es la digitalización y avanzar en el nivel de madurez digital de estas empresas. La nube es una herramienta necesaria para implementar algunos servicios de forma rápida y económica, pero existen otras opciones, aunque haciéndolo sin la nube puede sobredimensionar el gasto y no optimizar la inversión, algo innecesario hoy en día. La nube ha democratizado la tecnología para la pequeña empresa. Podemos implementar mucha tecnología y soluciones desde un único usuario con posibilidad de escalarlos”.

“La nube es una herramienta, pero ofrece un sinfín de beneficios para las pymes, tanto económicos como tecnológicos”

MARÍA JOSÉ GARCÍA BRAO, DIRECTORA DE VENTAS DE CANAL, NFON

RETOS PARA LA DIGITALIZACIÓN DE LAS PYMES

Apuntaba María José García Brao (NFON) que el primer reto es cultural, “no puede haber una transformación digital si no hay un cambio cultural. Muchas veces nos encontramos con la necesidad de evangelizar en estas empresas. En ocasiones, estas compañías, por la falta de recursos personales, la digitalización no es prioritaria en su negocio hasta que se convierte en una obligación. A esto se suma el miedo a la tecnología y, en algunos casos, una falta de visión a largo plazo. Hay que convencer al gerente de que las nuevas tecnologías dan valor a su empresa y les permiten diferenciarse. Además, hay que explicarles que el cambio puede ser gradual. Hecho esto, lo que nos piden es ahorro de costes, simplificación de los procesos, mejoras de la producción, con más ingresos o más clientes, y que los acompañemos y demos soporte y asesoramiento constante”.

Para Sem Guillem (KipmiON Tecnología), “los clientes no deciden digitalizarse en un momento dado, sino que se acercan a nosotros con una necesidad que tienen que solucionar, porque han tenido un problema, o porque necesitan mejorar algún proceso, y eso genera un punto de entrada de la digitalización. Pero, en general, hay que convencer a los responsables de que necesitan un cambio más profundo del que esperaban, pero que mejorará otros puntos del negocio e incrementará la productividad, y de que su equipo podrá asumir el cambio. Hay que hacer entender a las empresas que en el mercado actual necesitan herramientas adecuadas para competir y diferenciarse, porque el cliente es cada día más exigente en todos los aspectos de la empresa, algo imposible de alcanzar si no tienes tu empresa preparada. Tenemos que hacerle entender que es el momento de dar el paso para preparar el siguiente gran cambio”.

Desde el punto de vista de Luis Mediero (Quistor), “es importante que los pilares sobre los que se va a construir la digitalización sean los adecuados. Algunas empresas no lo han hecho así, y eso puede causar la necesidad de rehacer el trabajo. Hay que analizar sus necesidades para entender cómo digitalizarse. Tras esto, hay otros dos desafíos: mantener la continuidad del negocio, para no generar un problema grave para la empresa; y potenciar la seguridad, con los elementos necesarios para cumplir la normativa y proteger el negocio”.

CLAVES PARA LA COMPETITIVIDAD

Para la competitividad, recordaba Sem Guillem desde KipmiON Tecnología que la digitalización es fundamental “para mejorar todos los procesos de la empresa. Lo que más nos

“Es muy importante hacer un análisis completo de la situación real de la seguridad, las comunicaciones y la arquitectura global antes de emprender un proyecto”

LUIS MEDIERO, TECH MANAGER, QUISTOR

demandan son las soluciones para potenciar la comunicación y la colaboración entre los diferentes elementos de la empresa. Proporcionarles herramientas básicas para que los usuarios puedan interactuar de forma segura con compañeros, proveedores, colaboradores y clientes es fundamental. Con el trabajo remoto, las empresas también valoran los escritorios virtuales, creando un entorno corporativo seguro independientemente del lugar desde el que se trabaje, y ayudando a las empresas a captar talento. La nube es una herramienta, y con la digitalización llega el dato, que abre un nuevo horizonte para que las empresas entiendan mejor a su cliente y su negocio. Los servicios de datos también se han visto democratizados por la nube, ayudando a las empresas a reducir las incertidumbres y ayudando en la toma de decisiones y en la creación de nuevos negocios. Son soluciones que cada día son menos complejas de usar y que requieren menos conocimiento y experiencia para obtener resultados. En definitiva, tenemos que dejar claro a la pyme que los beneficios de la digitalización superarán ampliamente las inversiones realizadas”.

Añadía Luis Mediero desde Quistor que “el dato es fundamental. Es el oro de la empresa. Cuando digitalizas acumulas datos, y si no lo explotas estás perdiendo competitividad y negocio. Hay muchas herramientas que, sobre un set de datos, permiten procesar información para aportar competitividad al negocio, pero para una pyme a veces esto resulta complejo, tanto por el conocimiento como por el coste. Hay que proporcionales esta capacidad sin necesidad de realizar inversiones añadidas, como ha hecho Oracle en la versión 19 de su base de datos. El futuro de la competitividad de las empresas está en el dato y en su aprovechamiento”.

Desde NFON, María José García Brao se mostraba de acuerdo con sus compañeros de mesa, y recalcaba la necesidad de contar con herramientas para ayudarles “a mejorar procesos, mejorar la comunicación de los empleados o generar ahorros de costes, como puede ser una centralita digital. Pero, cuando hablamos de competitividad, hay que poner el foco en herramientas que sean importantes en la relación con los clientes, como puede ser un CRM, un sistema de gestión de llamadas o un contact center para generar una comunicación integral entre la empresa y los clientes, tanto actuales como potenciales”. ■

Tendencias Tecnológicas que aportan valor a la pyme: Propuestas Tecnológicas

“En ciberseguridad, en ocasiones, la base de datos es la gran olvidada”. Luis Mediero (Quistor)

“La nube aporta a las centralitas capacidades muy beneficiosas para los clientes”. María José García Brao (NFON)

“Cloud permite ofrecer servicios de calidad a un precio asequible”. Sem Guillem (Kipmion Tecnología)

DAMIÁN RUIZ SORIANO, PRESIDENTE, CLUSTER CYBERMADRID

“Los números demuestran que partimos de una situación de déficit en ciberseguridad en la pyme”

La ciberseguridad es un aspecto sumamente importante para las pequeñas y medianas empresas, tanto para proteger sus activos como para generar confianza en los consumidores de sus productos y servicios.

Tal y como recalcaba Damián Ruiz Soriano, presidente del Cluster CyberMadrid, en la sesión de clausura del Encuentro IT Trends: Tendencias Tecnológicas que aportan valor a la pyme, “hay dos grandes retos de estas empresas. El primero, alcanzar un nivel mínimo de ciberseguridad. Los números demuestran que partimos de un déficit en materia de seguridad en las pymes. El segundo, la transformación digital, y esta no puede producirse sin la seguridad adicional necesaria”.

NECESITAN ALGO MÁS QUE LA TECNOLOGÍA

En opinión de Damián Ruiz Soriano, “estamos minusvalorando a la pyme. Este tipo de empresas es consciente de su nivel de digitalización y de su falta de una ciberseguridad adecuada, pero el problema es que suelen

“SI QUEREMOS QUE ALCANCEN UN NIVEL BÁSICO DE CIBERSEGURIDAD, NECESITAMOS OFRECERLES UN ACOMPAÑAMIENTO MUY ESTRECHO”

tener el foco puesto en otros aspectos de su día a día, y, en algunos casos, en modo de supervivencia. Por tanto, necesitan que los acompañemos e, incluso, que les hagamos el trabajo. Si queremos que alcancen un nivel básico de ciberseguridad, necesitamos ofrecerles un acompañamiento muy estrecho, muy facilitador y casi transparente. Quieren digitalizarse y contar con ciberseguridad, pero su foco es el negocio. O les acompañamos y les facilitamos la tarea, o no perciben la urgencia y ni siquiera saben por dónde empezar".

Esto no supone, añade, "que ellos no tengan responsabilidad. Tienen que ser responsables, asumir sus riesgos, concienciarse y formarse, pero tenemos una obligación por parte de los jugadores del mercado de ciberseguridad de ayudarles".

"La pyme tiene que ser responsable, asumir sus riesgos, concienciarse y formarse, pero tenemos una obligación por parte de los jugadores del mercado de ciberseguridad de ayudarles"

EL APORTE DEL KIT DIGITAL

Iniciativas como la del Kit Digital son, en palabras de Damián Ruiz Soriano, "interesantes, pero tiene que mejorarse el aspecto de ciberseguridad. Por eso desde CyberMadrid hicimos una propuesta de un ecosistema de oferta/demanda/productos para el Kit Digital porque no lo contempla de forma adecuada. De sus diez áreas, solo las dos últimas son referidas a la ciberseguridad, que son, precisamente, las dos con menor cuantía económica asignada. No se le ha dado la importancia debida a la ciberseguridad, y frente a una necesidad evidente y básica hay otros módulos opinables. Creo que todas las líneas del Kit deberían tener, en paralelo, un desarrollo de ciberseguridad, porque no se puede hacer analítica de datos o comercio electrónico sin una seguridad adecuada".

Tal y como indicaba su presidente, el Cluster CyberMadrid "cuenta con una estrategia de foco en pyme, poniendo sobre la mesa la necesidad de incrementar la seguridad

en este segmento, intentando facilitar la resolución de las necesidades de las empresas, con productos diseñados para pyme. Además, estamos incentivando elementos como el ciberseguro, y colaborando en todos los foros donde soliciten nuestra ayuda, ya sea con entidades públicas o privada". ■

Tendencias tecnológicas que impactan en la gestión de datos moderna

¡Descárgatelo ahora!

itTRENDS

itTRENDS

OPINIÓN

El Metaverso, un mundo virtual con impacto físico

ESTHER SÁNCHEZ,
Directora de Innovación de Vodafone Business

Un nuevo fenómeno tecnológico, un mundo virtual, universos paralelos o un nuevo entorno digital... Son algunas de las frases con las que se ha tratado de definir al nuevo fenómeno de moda: el Metaverso.

Si hasta hace relativamente poco éramos meros espectadores incapaces de crear lugares en los que desarrollar experiencias más allá del plano físico, hoy es inevitable pensar en el metaverso sin asociarlo a las nuevas estrategias empresariales.

Este universo virtual es ya una de las mayores apuestas de los inversores de cara a los próximos años. En total, Bloomberg Intelligence calcula que para 2024 el tamaño del mercado del metaverso alcanzará los 800.000 millones de dólares.

¿Cómo se beneficiarán las empresas de este nuevo fenómeno tecnológico? Las compañías tendrán la posibilidad de desarrollar nuevos modelos de negocio en el Metaverso, algunos que ni siquiera existen hoy en día. Se trata de una transición que incluso afectará a la industria: las operaciones se planificarán de forma virtual en factorías, minerías y puertos gracias a avances como el 'digital twin', que ya permite a numerosas empresas manipular maquinaria pesada en remoto, reproduciendo su funcionamiento a través de programas informáticos.

Estas tecnologías están facilitando la transición del internet 2D al 3D, es decir, de un internet informacional a un internet experiencial para el usuario. Se podrán realizar todo tipo de actividades sin moverse del sofá: desde visitar cualquier rincón del planeta, hasta practicar deportes extremos, comprar o vender sin límites, o asistir a clases, museos y espectáculos.

Unido a lo anterior, el Metaverso permitirá una gran capacidad para socializar, compartir y disponer de contenidos a un nivel exponencial, algo que actualmente no ofrece ningún otro entorno digital. En este nuevo universo, el "Yo virtual" pasará de ser una mera marca personal verificada por un tercero, a ser un auténtico avatar digital, capaz de desarrollarse independientemente del control externo.

Para lograr que cualquier estrategia y modelo de negocio funcionen en el metaverso, habrá que reinventar disciplinas como el marketing y adaptarlas al nuevo mundo de la publicidad virtual; la captura y análisis de los datos en tiempo real a través de soluciones de IA y analytics serán fundamentales; y el uso de las tecnologías de realidad virtual y realidad aumentada, junto con los NFTs o el blockchain, serán clave para generar experiencias de compra totalmente diferentes y adaptadas a un nuevo consumidor digital.

Será imprescindible la colaboración entre multitud de actores: empresas consolidadas, startups, instituciones, grandes corporaciones y autónomos. Y con esa mirada puesta en la

El metaverso supondrá un antes y un después en muchos sectores económicos e industriales, en las empresas y estrategias de las compañías, y probablemente en la vida de millones de personas

colaboración, desde Vodafone hemos puesto en marcha nuestro '5G Lab', un espacio de encuentro entre empresas, instituciones y desarrolladores del metaverso con el objetivo de impulsar la creación del primer metaverso abierto a las empresas, donde el retail será uno de los sectores con mayor impacto.

El metaverso supondrá un antes y un después en muchos sectores económicos e industriales, en las empresas y estrategias de las compañías, y probablemente en la vida de millones de personas. Lo que está claro es que, aun siendo un fenómeno que se encuentra en fase de despegue, es muy importante que las empresas formen parte de él desde ya y se suban a este carro de innovación, porque esta disrupción tecnológica es comparable al fenómeno de internet... ¿Imaginas tu vida o tu empresa sin internet? ■

MÁS INFORMACIÓN

- Ordenando el metaverso. Claves para no quedarte fuera del ciclo de innovación
- Los gemelos digitales ayudan a avanzar hacia la sostenibilidad
- Tecnologías emergentes que impulsarán la innovación a partir de 2022
- Qué son los NFTs y cómo funcionan
- Las cinco tecnologías con mayor impacto en innovación en el futuro

Si te ha gustado este artículo, compártelo

FORO TECH & BUSINESS
it User

Innovación y tecnología

dinamizadores del cambio empresarial

28 de septiembre · 9:30 h

REGISTRO

Tendencias tecnológicas que impactan en la gestión de datos moderna

¡Descárgatelo ahora!

it TRENDS

El cifrado post-cuántico puede no venir solo.

La ciberseguridad llama a la puerta

E. Frechoso Muñoz

Cuando se habla de computación cuántica puede parecer que se trata de ciencia ficción, pero la realidad es todo lo contrario, pues en los últimos años esta disciplina ha sumado notables avances y son cada vez más las compañías que se suben al tren del I+D+i en esta materia. De hecho, los investigadores anticipan que el mercado de la criptografía cuántica alcanzará un valor de 291,9 millones de dólares en 2026 a medida que más organizaciones busquen o inviertan para protegerse contra futuras amenazas cuánticas. Pero ¿qué implicaciones tiene esto para la seguridad?

Tal es el interés que está generando la criptografía cuántica que muchos expertos coinciden en apuntar que se trata ya no de uno de los temas de mayor actualidad en el mundo de las TI, sino del futuro de la informática. Sin embargo, democratizar la computación cuántica para convertirla en algo masivo, o demostrar su eficiencia allí donde se aplique garantizando costes competitivos, es harina de otro costal.

Pero antes de profundizar en los beneficios y riesgos asociados a la computación cuántica, y/o en su término evolucionado, computación post cuántica (PQ) veamos en qué consiste exactamente esta materia, qué supondrá su aplicación para las organizaciones y, como no podía ser de otra manera, cómo afectará o qué implicaciones tendrá para la ciberseguridad en el futuro.

Para ello, hay que partir de la base de una premisa que puede parecer obvia: los avances informáticos y tecnológicos han ayudado a incrementar el nivel de ciberseguridad de los sistemas, aunque también han servido para vulnerarla, porque como en todo, existe la otra cara de la moneda y donde unos ven una forma de proteger mejor la información confidencial, otros buscan la posibilidad de robarla para aprovecharse de ella.

Un avance para mejorar la ciberseguridad en este sentido es la aplicación de la mecánica cuántica a la criptografía para cifrar los mensajes, es decir, lo que ha dado lugar a la criptografía cuántica. Esta técnica lo que posibilita es que solo se puedan descifrar los mensajes de manera correcta por el destinatario previsto. Si un tercero intercepta el mensaje, al observarlo lo alteraría de manera que la información transmitida en él sería distinta a la que

se quería enviar y, por tanto, sería inútil para él.

Comparado con otros sistemas de encriptación tales como la criptografía asimétrica, que utilizan las matemáticas para crear claves privadas seguras, la criptografía cuántica se nutre de la física cuántica para crear las claves de cifrado seguras que solo poseen el emisor y el receptor.

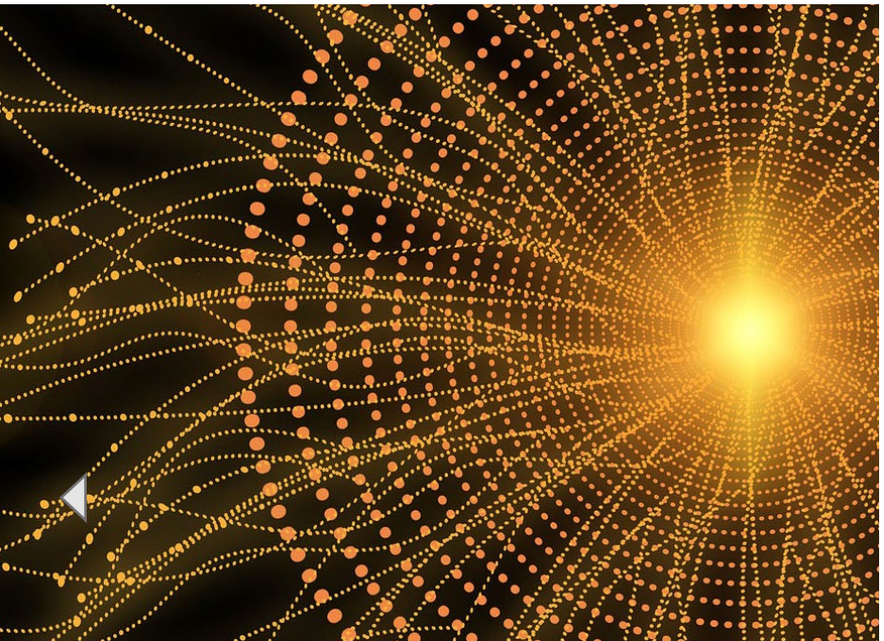
Los sistemas de cifrado actuales multiplican números primos muy elevados para generar las claves de cifrado. Por su parte, los protocolos de criptografía cuántica utilizan los fotones -la unidad de energía más pequeñas de una onda de luz- y sus propiedades cuánticas para cifrar los mensajes.

Dado lo positivo de estos avances para la ciberseguridad y con vistas a reforzarla a la hora de transmitir información, el Instituto Nacional de Estándares y Tecnología (NIST) del Departamento de Comercio de Estados Unidos, puso en marcha un concurso hace seis años sobre el proceso de

Pasos para prepararse para el futuro

Algunos de los factores importantes de la criptoagilidad y las preguntas clave que se deben hacer al preparar un negocio para un futuro post cuántico, según recomiendan desde Utimaco, son:

- **Considerar la velocidad de ejecución:** piense en cuánto tiempo le llevará a su empresa migrar los protocolos de encriptación actuales a la nueva encriptación post cuántica. Asegúrese de que piensa en el futuro y trate de responder a cómo podrá proteger sus sistemas dentro de 20 años. A la hora de considerar la computación post cuántica, no se pueden tomar por duraderas las soluciones inmediatas, ni siquiera las que protegerán a las empresas durante los próximos 10 años.
- **Examinar el ciclo de vida de su producto:** si el ciclo de vida de su producto tiene más de cinco años desde el diseño hasta la comercialización, está en problemas. Sectores como el de la automoción, la medición inteligente, la administración pública, las infraestructuras críticas y el IoT industrial tardan entre 2 y 4 años en diseñar productos que permanezcan en el mercado durante 7 años o más. Prepararse para la computación cuántica supone diseñar medidas de seguridad cuántica en el ADN de los productos de hoy en día para garantizar que sean seguros de usar en un mundo post cuántico. Para ello, empiece por preguntarse qué requisitos exactos necesita su empresa.
- **Planificar el coste:** la implementación de un firmware seguro para lo cuántico o el desarrollo y ejecución de algoritmos seguros cuánticos es posible, pero con un gran coste y esfuerzo. Es importante empezar a planificar estos costes ahora para ahorrarle a la empresa dolores de cabeza en el futuro.



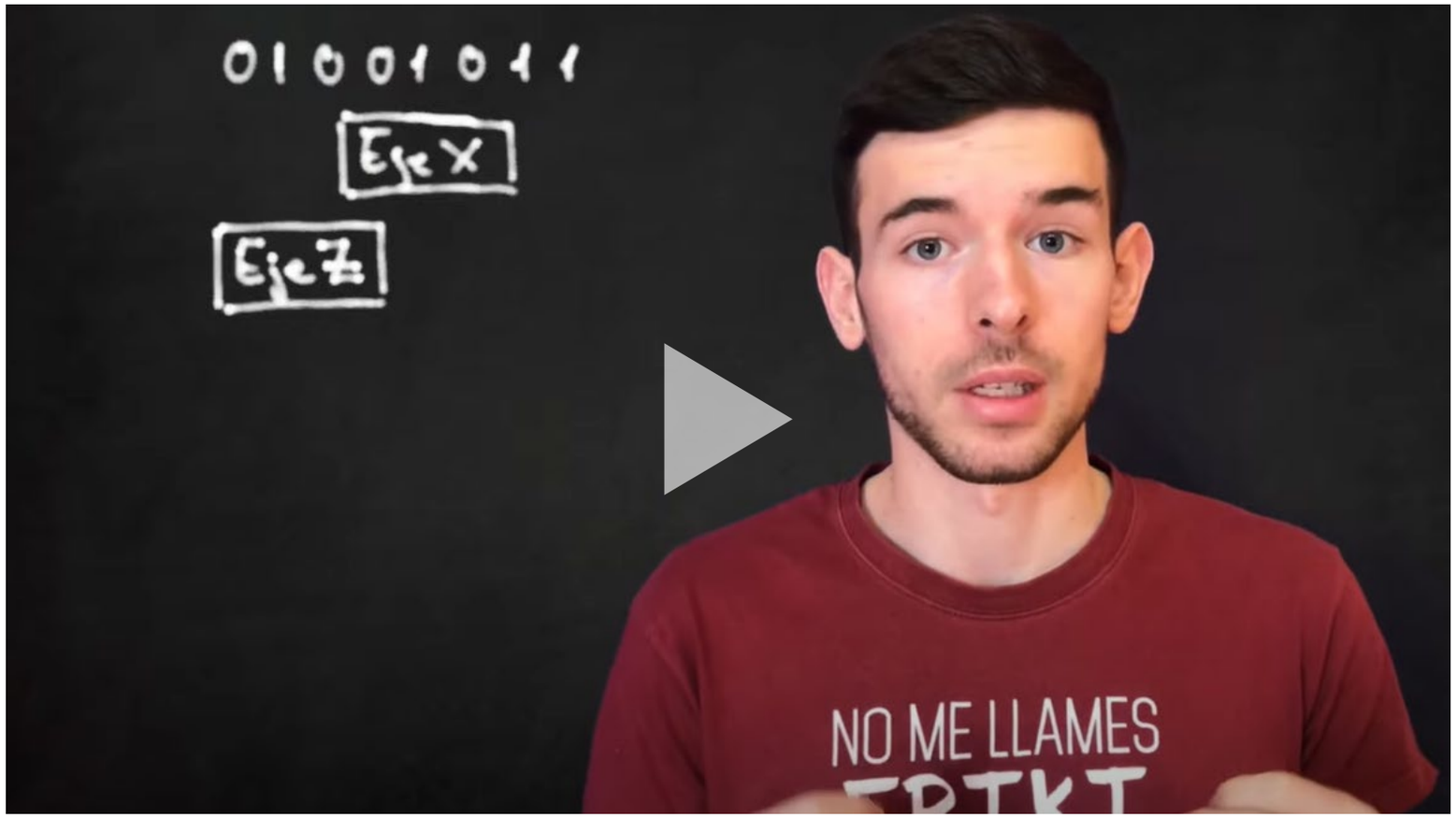
estandarización de la criptografía post cuántica en el que se pedía a criptógrafos de todo el mundo que diseñaran y examinaran métodos de cifrado resistentes al ataque de una futura computadora cuántica, mucho más potente que las máquinas disponibles en la actualidad.

Esta iniciativa está dando sus frutos, pues en la tercera ronda del concurso, el NIST confirmó el pasado mes de julio la selección de los primeros cuatro algoritmos resistentes a la tecnología cuántica que pasarán a formar parte del estándar criptográfico post cuántico de la agencia. Se trata de CRYSTALS-Kyber para el cifrado general debido a su velocidad y sus pequeñas claves de cifrado, y de los algoritmos CRYSTALS-Dilithium, FALCON y SPHINCS+ para las firmas digitales, utilizadas para la autenticación de identidad.

Optimismo, pero con prudencia

Este anuncio supone un nuevo hito para asegurar los datos sensibles frente a la posibilidad de futuros ciberataques procedentes de ordenadores

Es un hecho que los ordenadores cuánticos, tarde o temprano, supondrán una amenaza inevitable para la seguridad digital



CRIPTOGRAFÍA CUÁNTICA (BB84)

CLICAR PARA VER EL VÍDEO

cuánticos. Por tanto, con estos cuatro algoritmos se da un nuevo paso en la carrera por la estandarización de la criptografía post cuántica del NIST, un proceso que resultará clave a la hora de ayudar a las organizaciones a identificar qué soluciones implementar en sus entornos para proteger sus datos contra las amenazas post cuánticas, que se espera que estén disponibles en 2030.

Los expertos del sector coinciden en calificar esta noticia como positiva y necesaria para evitar un incremento de los riesgos de seguridad derivados de esta nueva tecnología, pero también coinciden a la hora de pedir cierta prudencia al valorarlo. “Aunque se cree que los cuatro algoritmos identificados por el NIST son seguros desde el punto de vista cuántico, dado que aún no se han desarrollado ordenadores cuánticos a gran escala, existe la posibilidad de que las pruebas en el mundo real demuestren que no lo son”, señala Nils Gerhardt, CTO de Utimaco.

Por su parte, Andreu Bravo, Socio Risk Advisory Cyber de Deloitte, recuerda que “debemos entender que éste no es más que un primer paso en un camino lleno de retos: quedan por delante, al menos dos años de pruebas, evaluaciones y mejoras; siempre confiando en que el proceso fluya con normalidad, para validar su efectividad antes de comenzar a realizar implementaciones masivas, así como esperar a que la estandarización del NIST se extienda a los marcos de regulación criptográficos actuales. Igualmente, se debe incorporar además en los esquemas de seguridad nacional, y en los procesos y mecanismos de firma reconocida, y de intercambio de claves”.

Precisamente, al hilo de las fases de evaluación que quedan, que pueden conllevar que algunos de los cuatro algoritmos seleccionados puedan ser eliminados o añadidos en la siguiente ronda, Gerhardt, advierte de que “esto supone un reto para los profesionales de la seguridad que se ocupan de la migración de la criptografía resistente a la tecnología cuántica, ya que podrían apostar por

"La arquitectura de esos sistemas carece de memoria y procesador y ni siquiera existen lenguajes de programación estándar que se puedan utilizar sobre computadoras cuánticas. Eso supone que mayoría de los ciberdelincuentes no tendrán acceso a computadoras cuánticas para utilizarlas en su beneficio, ni se podrán desarrollar y distribuir malwares con afectación múltiple"

Andreu Bravo, Socio Risk Advisory Cyber, Deloitte

migrar a un algoritmo que se demuestre que no es seguro en las pruebas posteriores o en las pruebas con ordenadores cuánticos reales". Por lo tanto, "es importante que las organizaciones hagan el cambio para convertirse en "cripto ágiles", es decir, se vuelvan capaces de cambiar los sistemas criptográficos que utilizan cuando sea necesario", subraya el directivo de Utimaco.

En este sentido, "todo el mundo está a la espera del resultado final y de las recomendaciones definitivas del NIST, momento en el que todos los organismos de estandarización tendrán que adoptar cambios y actualizar los protocolos que se basan en la criptografía", añade Eric Piroux, director del Centro de Excelencia de Seguridad Digital para EMEA de Entrust. "Mientras tanto, las organizaciones ya pueden empezar a probar y experimentar con la integración de estos algoritmos en sus estrategias y oferta criptográfica".

En definitiva, aún quedan bastantes pasos -y muy importantes- por dar para estar preparados y poder enfrentarnos a los nuevos riesgos de seguridad asociados a esa nueva tecnología. De entre todos ellos, el más preocupante es que la llegada de los primeros sistemas de computación cuántica estables permitirá, entre otras cosas, obtener en tan solo unas horas/días, claves de cifrado consideradas hasta ahora como invulnerables por su naturaleza polinómica, al basar su fortaleza en la capacidad y el tiempo de cálculo necesario para factorizar en números primos, apuntan desde Deloitte.

Disponer cuanto antes de algoritmos criptográficos resistentes permitirá que, antes de la llegada de los sistemas de computación cuántica, se pueda contar con el tiempo necesario para volver a cifrar y firmar toda la información existente, ya sea que esté almacenada y cifrada o firmada previamente con los algoritmos actuales. “Además, se tendrán que generar hashes robustos que garanticen a lo largo del tiempo la confidencialidad y la autenticidad de documentos cifrados y firmados anteriormente, y asegurar la implantación y la madurez de otros procesos criptográficos críticos como la generación y el intercambio de claves”, explica Bravo.

Hablemos de retos

Es un hecho que los ordenadores cuánticos, tarde o temprano, supondrán una amenaza inevitable para la seguridad digital. Dentro de una década un ordenador cuántico será lo suficientemente potente como para romper la criptografía tal y como se conoce hoy en día, “y algunos actores de amenazas ya están almacenando conjuntos de datos cifrados de entornos pirateados que esperan descifrar una vez que los ordenadores cuánticos alcancen la escala y la accesibilidad necesarias”, recuerda el CTO de Entrust.

Pero para entender los retos que supondrá la computación cuántica en la ciberseguridad, hay que comenzar por entender los dos principales fundamentos de la física cuántica aplicados en la computación: la superposición de estados y el entrelazamiento.

El primero de esos dos principios, la superposición de estados, supone un cambio total en el

"La migración a los algoritmos seguros para el cálculo cuántico podría llevar varios años. Para sectores como el de la sanidad y las infraestructuras críticas, la transición ya está en marcha debido al ciclo de vida de la tecnología y a los datos de larga duración que tienen que garantizar para que sigan siendo seguros"

Eric Piroux, director de Centro de Excelencia de Seguridad Digital en EMEA, Entrust

Las empresas tendrán que entender qué datos necesitan ser protegidos durante largos períodos de tiempo y cuáles carecerán de valor para los ciberdelincuentes para determinar dónde se puede utilizar la criptografía post cuántica y la criptografía convencional

paradigma de la computación, tal y como se entendía hasta ahora. De un universo digital en el que la unidad de medida es el bit -con únicamente dos valores posibles (0 y 1)-, se pasa a un escenario en el que la unidad básica es el bit cuántico o "qubits. El qubit, puede tener cualquier valor combinado entre 0 y 1. Es decir, podría ser 0 o 1, podría ser 1 y 0 al 50%, respectivamente, o 20%, 1 y 80%, 0, etc. Para añadir complejidad, la incorporación del principio del entrelazamiento hace que el estado de un qubit varíe, dependiendo del estado de otros qubits y de cualquier operación que se realice en cualquiera de ellos, de tal forma que poner a cero un qubit o, simplemente leer el valor que almacena, afectará al valor almacenado por cualquier otro qubit entrelazado,

Sin entrar en más detalle, y teniendo en cuenta lo anterior, puede entreverse que las posibilidades en cuanto a generación de combinaciones, estabilidad y predicción de los valores resultantes, son superlativamente superiores a la computación tradicional. Eso, unido al aumento de velocidad y eficiencia de estas tecnologías, por la posibilidad de evaluar múltiples combinaciones de estados a la vez, hace que su aplicación en el campo de la criptografía plantee retos importantes.

Según Bravo, el primero de ellos será "la obsolescencia inmediata de los algoritmos asimétricos actuales (RSA y Curva Elíptica son dos buenos ejemplos), basados en factorización (descomposición de grandes números en números primos) y considerados invulnerables por los recursos y el tiempo necesario (cientos o miles de años) para obtener una clave mediante fuerza bruta, pero que al utilizar computación cuántica los plazos quedarán reducidos a minutos o días".

Es un hecho que los nuevos dispositivos son un blanco atractivo para los ciberataques, lo que se traduce en un mayor riesgo para las organizaciones. "Con la aparición de la computación cuántica la infraestructura debe evolucionar para proteger las claves criptográficas, los algoritmos y los protocolos que a su vez protegen la infraestructura", dice por su parte Gerhardt. "Por tanto, el sector de

Tres simples parámetros

Adoptar sistemas resistentes a criptografía cuántica depende de tres simples parámetros, según Entrust:

1. **Vida útil:** número de años durante los cuales el sistema cibernético debe proteger los datos.
2. **Período de migración:** número de años necesario para migrar el sistema a una solución cuántica segura.
3. **Período de amenaza:** número de años antes de que actores relevantes puedan violar sistemas vulnerables a criptografía cuántica.

Si el período de amenaza es menor que la suma de vida útil y tiempo de migración, las organizaciones no podrán proteger sus activos ante ataques cuánticos.

"El sector de la ciberseguridad debe dar prioridad al hardware y al software criptográfico para garantizar la existencia de medidas, protecciones y comportamientos actualizados contra amenazas y vulnerabilidades cada vez más innovadoras, ahora y en el futuro"

Nils Gerhardt, CTO, Utimaco

la ciberseguridad debe dar prioridad al hardware y al software criptográfico para garantizar la existencia de medidas, protecciones y comportamientos actualizados contra amenazas y vulnerabilidades cada vez más innovadoras, ahora y en el futuro".

En cuanto a las empresas, todas tendrán que adaptarse a la seguridad en la era de la computación cuántica. Una vez que los ordenadores cuánticos sean lo suficientemente potentes como para romper el cifrado que se utiliza hoy en día, no solo se podrán revelar los datos futuros de las empresas, sino también los datos pasados que hayan sido interceptados y almacenados por los atacantes. "Los contratos firmados digitalmente podrían reescribirse, y también podría ser posible robar datos hoy y descifrarlos más tarde, cuando la tecnología esté disponible", advierte el directivo de Utimaco.

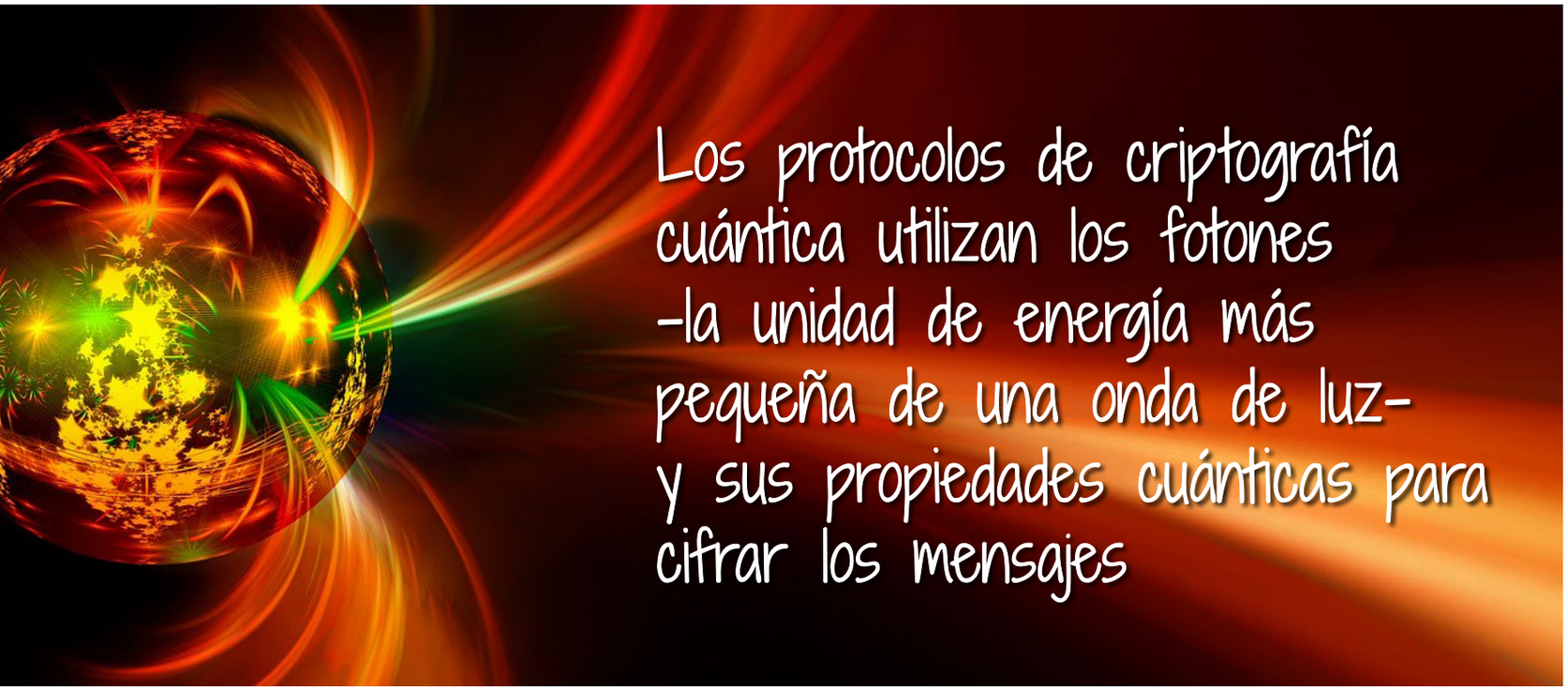
De ahí que, aunque el plazo para la computación post cuántica parece muy lejano, el cambio a algoritmos seguros para lo cuántico no es solo un ciclo regular de actualización de la criptografía. "La migración a los algoritmos seguros para el cálculo cuántico podría llevar varios años. Para algunos sectores, como el de la sanidad y las infraestructuras críticas, la transición ya está en marcha debido al ciclo de vida de la tecnología y a los datos de larga duración que tienen que garantizar para que sigan siendo seguros", dice Piroux.

Para ponerlo en perspectiva, pensemos en la migración de SHA-1 a SHA-2. Se avisó con mucha antelación, hubo mucho tiempo para prepararse y, en general, se consideró una migración sencilla. Sin embargo, cuando llegó el momento, algunas organizaciones tuvieron verdaderos problemas, algunas incluso todavía están trabajando en ello. "Pues bien, el cambio a los algoritmos seguros post cuánticos ni siquiera se compara, así que el momento de empezar a prepararse es ahora", añade del directivo de Entrust.

Preparación: el quid de la cuestión

La promesa de un ordenador que, sobre el papel, tiene el potencial de superar las capacidades incluso de los superordenadores más rápidos de hoy en día tiene entusiasmados a muchos actores del sector tecnológico, lo que ha llevado a cantidad de nuevas empresas a centrar sus esfuerzos en esta disciplina, tal y como se indicaba con anterioridad.

Hace tiempo que se plantea el impacto que tendrá la computación cuántica en los métodos de cifrado que se utilizan actualmente. Pero aquí surgen varias preguntas como: ¿Hasta qué punto es factible la computación cuántica en su estado actual? ¿Qué significa el desarrollo de la tecnología cuántica para



la industria de la seguridad? ¿Cuándo se verá que la computación cuántica esté accesible para los ciberdelincuentes? O ¿cómo será posible proteger en el futuro los archivos cifrados con los métodos actuales?

"Afortunadamente, el desarrollo de tecnología cuántica es extremadamente costoso, y no parece que vaya a estar al alcance de cualquiera durante, al menos, la próxima década", asegura Bravo, que explica que la arquitectura de esos sistemas carece de memoria y procesador y ni siquiera existen lenguajes de programación estándar que se puedan utilizar sobre computadoras cuánticas. "Esto quiere decir que la mayoría de los ciberdelincuentes no tendrá acceso a computadoras cuánticas para utilizarlas en su beneficio, ni se podrá desarrollar y distribuir malware con afectación múltiple", subraya el directivo.

En este sentido, los expertos consultados señalan que se minimizará el nivel de exposición frente a amenazas. Sin embargo, no se puede decir lo mismo del uso que le darán las grandes compañías que ya están invirtiendo y avanzando en el desarrollo de los primeros modelos de computadoras cuánticas.

"Tampoco sabemos cómo responderán los gobiernos que, probablemente y argumentando objetivos de defensa, las utilizarán como mínimo para el descifrado y supervisión continua de cualquier tipo de información que puedan considerar una amenaza contra la estabilidad de su país o de sus propios intereses", explica Bravo. "Precisamente, algunos gobiernos ya están interceptando, copiando y almacenando toda la información cifrada mediante criptografía asimétrica convencional que pasa por sus sistemas o por sus infraestructuras de telecomunicaciones, con el objetivo de poder descifrarla en cuanto dispongan de las primeras computadoras cuánticas estables. Aunque posiblemente, buena parte de esa información para entonces ya estará obsoleta"

Por su parte, las empresas tendrán que entender qué datos necesitan ser protegidos durante largos períodos de tiempo y cuáles carecerán de valor para los ciberdelincuentes para determinar dónde se puede utilizar la criptografía post cuántica y la criptografía convencional, indican desde Utimaco. Una vez hecho esto, se puede crear una prueba de concepto que utilice criptografía post cuántica o métodos híbridos para proteger los datos y extenderla a todos los activos digitales de una empresa. En el caso de algunos sistemas, bastará con pasar de un método a otro, mientras que los sistemas heredados podrían tener que ser actualizados o sustituidos de forma significativa.

Así pues, las empresas deben prepararse ya para la seguridad post cuántica, introduciendo una cripto-agilidad que permita cambiar la tecnología de encriptación por la más adecuada en un escenario determinado. Tal y como destaca Gerhardt, "los módulos de seguridad de hardware (HSM) son un ejemplo de cómo la resistencia cuántica está

disponible hoy en día. Si se combinan con un conocimiento profundo de lo que es y no es resistente frente a la tecnología cuántica en la infraestructura de una empresa, las organizaciones pueden asegurar sus datos mucho antes de que la computación cuántica entre en la corriente principal".

Respecto a cómo proteger en un futuro los archivos cifrados con métodos actuales, desde Deloitte puntualizan que "precisamente, el objetivo de los algoritmos seleccionados y aprobados recientemente por el NIST es conseguir cifrar ficheros con computadoras convencionales, minimizando el riesgo de que, en un futuro, esos archivos puedan ser descifrados desde computadoras cuánticas".

Para ello, es necesario seguir de cerca su efectividad a medida que se vaya extendiendo su uso, verificando que no surja ninguna vulnerabilidad desconocida hasta ahora. Y precisamente, para que se extienda su uso, también hará falta que, previamente, los sistemas operativos y aplicaciones actuales implementen esos algoritmos en sus librerías de cifrado. "Este proceso de despliegue, aunque en principio no parece muy complicado desde el punto de vista técnico, en muchos casos puede verse muy ralentizado, si no bloqueado, por la necesidad de que organismos públicos, o incluso naciones, lo homologuen y autoricen el uso de esos algoritmos como mecanismo de cifrado aceptado en el intercambio de información y/o en el almacenamiento de ciertos tipos de datos", explica Bravo.

A continuación, y una vez esté disponible la implementación de algoritmos resistentes, y haya sido autorizado su uso, las empresas deberán identificar toda la información sensible que ya tienen almacenada y cifrada mediante criptografía asimétrica actual y volverla a cifrar mediante los nuevos algoritmos de cifrado resistente, destruyendo posteriormente todas las copias de ficheros cifradas con los algoritmos vulnerables. Igualmente, "también será importante revisar y mejorar si procede los mecanismos de gestión y preservación de las claves de cifrado generadas y utilizadas por los algoritmos resistentes (bien sea mediante tecnologías HSM o desplegando nuevos controles técnicos y procedimentales) y los de generación de hashes e intercambio de claves", añade el socio de Deloitte.

¿Se volverá imprescindible?

Los procesos de digitalización en las empresas cada vez son mayores y van más deprisa. Lo mismo ocurre en nuestro día a día. El proceso de hiperconexión e interconexión crece a diario, por eso, la llegada de la computación cuántica marcará un punto de inflexión en todo lo relacionado con el plano digital.

"Las capacidades ofrecidas por la computación cuántica, aprovechadas desde el lado oscuro, se convertirán en nuevas amenazas que permitirán obtener claves de descifrado o de firma con las que, por ejemplo, poder leer cualquier información encriptada con los algoritmos actuales, o suplantar identidades basadas en firmas de autenticación o falsificar documentos y transacciones basadas en firma digital", dice Bravo.

La única manera de contrarrestar efectivamente esas nuevas amenazas consistirá en implementar las mismas propiedades de superposición y de entrelazado en nuevos algoritmos y procesos criptográficos, generando, por ejemplo, claves de cifrado

Para entender los retos que supondrá la computación cuántica en la ciberseguridad, hay que comenzar por entender los dos principales fundamentos de la física cuántica aplicados en la computación: la superposición de estados y el entrelazamiento

mucho más diversas fruto de la superposición de los valores intermedios entre 0 y 1 que, además, gracias al principio de entrelazado, permitirán detectar de inmediato accesos no autorizados.

Sin embargo, una cosa importante que hay que entender sobre los ordenadores cuánticos es que no están diseñados para sustituir a los ordenadores tradicionales en todos los aspectos de nuestra vida. La fuerza de un ordenador cuántico reside en su capacidad para realizar simulaciones complejas y procesar sistemas no lineales, como los patrones meteorológicos y climáticos, el diseño de máquinas biónicas o la búsqueda de números primos.

Por otro lado, “el superordenador clásico seguirá teniendo ventaja cuando se trate de ofrecer resultados concretos y resolver problemas lineales. En definitiva, los ordenadores cuánticos no son una solución mágica que nos empujará a la siguiente evolución de la informática; lo más probable es que sigamos utilizando los ordenadores clásicos y los cuánticos de forma paralela de una u otra manera”, matiza Martin Roesler, director del equipo de investigación FTR de Trend Micro.

Acogida por parte de las organizaciones

A la hora de ver si las organizaciones están apostando por el desarrollo de la seguridad en materia de cifrado cuántico y de la acogida que esta disciplina está teniendo en el mercado, conviene puntualizar que, al igual que ocurre con otras tecnologías, encontramos que las empresas se hallan en diferentes etapas de su viaje hacia la criptografía cuántica. Es más, podría afirmarse que la mayoría de ellas se encuentran en una fase embrionaria. “Para algunas, esto se debe a la falta de concienciación sobre esta tecnología en desarrollo y sus repercusiones, para otras a la falta de recursos que dedicar, mientras que otras están esperando a que se desarrollen más los algoritmos cuánticos resistentes y la maduración de la tecnología”, declara Piroux.

Por sectores, “algunos, como el de la automoción, ya han empezado a utilizar la seguridad post cuántica, mientras que otros, como el de la defensa y el de la energía, es probable que ya hayan realizado el cambio para convertirse en “criptoagentes”, es decir, ser capaces de cambiar los sistemas criptográficos que utilizan cuando sea necesario ”, apunta Gerhardt.

Mientras que, si atendemos al ránking por países e inversiones, encontramos que China, con un plan de inversión de 10.000 millones de dólares, seguida de Estados Unidos, también con inversiones mil millonarias, lideran la carrea cuántica. A mucha menor escala se sitúan las inversiones de nuestro país, que cuenta con 22 millones procedentes de los Fondos de Recuperación Europeos. Sin embargo, España ya dispone de un buen ecosistema de instituciones avanzadas en cuántica distribuidas en 25 centros de 14 comunidades autónomas a través de la Red Española de Supercomputación y gestionada desde el Barcelona Supercomputer Center, liderando el proyecto Quantum Spain, en el que esperan invertirse hasta un total de 60 millones en 3 años

para lograr alcanzar el objetivo de disponer de una computadora cuántica de 20 qubits en 2025.

En cualquier caso, Piroux aclara que “probablemente España, como muchos otros países del mundo, busque la orientación del NIST sobre las mejores prácticas de cifrado resistente a la tecnología cuántica. Como miembro de la Unión Europea, las organizaciones españolas también tendrán que asegurarse de que cumplen con cualquier normativa establecida para la región”. Esto significa que habrá que esperar.

Aunque hay precisión en cuanto a las fechas en las que la computación cuántica será una realidad, las inversiones y los resultados que se están obteniendo en la resolución de problemas complejos, apuntan en que podría ser antes de lo previsto inicialmente. Cada vez hay más casos que demuestran su eficiencia y aplicación práctica, aunque no exista aún normalización entre ellos, explican los expertos.

De todo esto la principal conclusión que se extrae es que está demostrado que la llegada de la computación cuántica supondrá una brecha de seguridad crítica para quien no se haya preocupado por incorporar algoritmos criptográficos resistentes en sus procesos de firma, cifrado y autenticación y no haya cifrado su información confidencial mediante estos algoritmos e incrementado la longitud de sus claves simétricas. No importa el tamaño de las empresas, ni el sector al que pertenezcan. Su información y sus sistemas estarán expuestos frente a quién sí tenga acceso a computadoras cuánticas, aseguran desde Deloitte.

Los expertos en seguridad y los científicos predicen que las computadoras cuánticas algún día podrán descifrar los métodos de encriptación comúnmente utilizados. Esto permitirá que el correo electrónico, la banca segura, las criptomonedas y que los sistemas de comunicaciones sean vulnerables a nuevas ciberamenazas. Por tanto, aunque puede ser demasiado pronto para revisar por completo los protocolos de seguridad para prepararse para la computación cuántica, no estaría demás que las organizaciones empezaran a planificar el futuro. Construir un sistema seguro frente a posibles ataques que utilicen la tecnología cuántica podría llevar años. Por lo tanto, a medida que nos adentramos en un mundo en el que la computación cuántica es una opción viable, lo mejor es tener una perspectiva a largo plazo de lo que nos deparará el futuro y estar preparados con antelación.

Enlaces de interés...

- El NIST aprueba los primeros algoritmos de cifrado resistentes a la computación cuántica
- Esta es la hoja de ruta de IBM para ofrecer un sistema cuántico de más de 4.000 cúbits
- Así es el proyecto español que investiga el uso de la informática cuántica en sectores clave
- El Gobierno concederá una subvención de 22 millones para crear un ecosistema de computación cuántica

Compartir en RRSS

it User
TECH & BUSINESS

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

JOSÉ MANUEL NAVARRO

CMO MOMO GROUP

José Manuel Navarro Llena es experto en Marketing, Durante más de treinta años ha dedicado su vida profesional al sector financiero donde ha desempeñado funciones como técnico de procesos y, fundamentalmente, como directivo de las áreas de publicidad, imagen corporativa, calidad y marketing. Desde hace diez años, basándose en su formación como biólogo, ha investigado en la disciplina del neuromarketing aplicado, lo que le ha permitido dirigir, coordinar e impartir formación en diferentes masters de neuromarketing en escuelas privadas y en universidades públicas. Es Socio fundador de la agencia de viajes alternativos Otros Caminos, y de la entidad de dinero electrónico con licencia bancaria otorgada por el Banco de España SEFIDE EDE de la que en la actualidad es director de Marketing. Autor de "El Principito y la Gestión Empresarial" y "The Marketing, stupid", además de colaborador semanal desde 2006 en el suplemento de economía Expectativas del diario Ideal (Grupo Vocento).

El efectivo ha muerto.

Larga vida al efectivo

En los ecosistemas naturales el concepto de biodiversidad se aplica tanto al número de poblaciones de diferentes especies que conviven en un espacio común, como a la pluralidad de interacciones perdurables que ocurren entre ellas y, a su vez, con su entorno. Los organismos interactúan recíprocamente conformando un todo estable en el que la diversidad ecológica garantiza su equilibrio y, por tanto, su continuidad. Los cambios en las condiciones del entorno influyen de manera decisiva en el número de especies y, a su vez, las variaciones en éstas pueden implicar modificaciones substanciales en el medio ambiente. La desestabilización del ecosistema por variables imprevistas ocasiona un importante desequilibrio inicial que solo el tiempo y determinadas circunstancias estabilizarán conformando un nuevo ecosistema en el que operarán unas reglas de relación intra e interespecíficas distintas a las originales. Puede suceder que algunas especies prosperen más y otras desaparezcan, pero siempre existirán organismos que desempeñan un papel básico y fundamental para sustentar la cadena trófica y la pervivencia del conjunto, sin cuya participación no sería posible la vida de esas poblaciones (comunidad biótica).

La influencia que los cambios drásticos en la biodiversidad producen en el medio natural y, consiguientemente, en el bienestar de las sociedades humanas, en su actividad y desarrollo económico y, sin duda, en el medio de vida de las generaciones futuras. El cambio climático, por ejemplo, es el resultado de múltiples y consecutivos ataques contra la biodiversidad a lo largo de los diferentes ecosistemas del planeta, hecho advertido y predicho por la comunidad científica décadas atrás y cuyas primeras consecuencias, por desgracia, estamos sufriendo ya en forma de desastres naturales que comprometen la seguridad física y alimentaria de todos los habitantes del planeta.

Valga esta introducción para hacer una extrapolación a lo que venimos denominando como “ecosistema de pagos”, el cual ha pasado en unos pocos años de ser un sistema sencillo en el que coexistían unos pocos elementos (efectivo, tarjetas, cheques, transferencias) a otro en el que las soluciones digitales han aportado variables que han enriquecido su “biodiversidad”, aunque también lo hayan hecho más complejo, ampliando tanto su espacio geográfico como los métodos y medios de relación entre todos los actores implicados (consumidores, comercios, administración pública, reguladores, entidades financieras, plataformas y proveedores de servicios de pago, Fintech, Bigtech…).

Se solía pensar que los ecosistemas muy ricos en especies son más estables frente a perturbaciones

exógenas, pero ya se sabe que, en determinadas condiciones, una elevada biodiversidad puede volverlos inestables y altamente vulnerables al verse afectados de diversas maneras los componentes individuales de su estabilidad. En el caso de los ecosistemas de pagos deberíamos hacer un ejercicio de imaginación para sopesar cómo un sistema estable durante mucho tiempo, con pocos instrumentos de pago, puede no solo sufrir la desaparición de alguno de ellos (como está sucediendo con los cheques), sino ver comprometida su evolución por la irrupción de nuevos esquemas que perturban el modelo e, incluso, pueden generar crisis de concepto o económicas (pensemos en las criptomonedas y la actual situación de caída de su valor y cuestionamiento sobre su permanencia o reinvención).

Pasar de usar recursos tangibles, como el efectivo o las tarjetas, a utilizar dispositivos electrónicos (como cuentas eMoney o billeteras digitales) ha supuesto una evolución hasta cierto punto normal en la medida que la tecnología ha ido aportando nuevos medios y soluciones al mismo ritmo que se han ido aplicando innovaciones a otras áreas y sectores de la actividad diaria de los ciudadanos. En cambio, la irrupción de lo virtual (“metamercado” que definimos en un artículo anterior) exigirá desarrollar un modelo de relación que, como en

> No cabe duda de que la sociedad es cada vez más digital y que la tecnología evoluciona a una velocidad vertiginosa, circunstancias a las que no puede sustraerse la industria de pagos

todas las revoluciones industriales (al menos en las cuatro ya sucedidas), mantenga las conexiones humanas intactas.

Se pueden cambiar las fuentes de energía básicas, las actividades industriales se pueden hacer más dinámicas, pasar de la localización territorial a la globalización y replegarse de nuevo a lo local puede ser una fórmula necesaria que acompañe a la sustentación de la economía (en términos absolutos), los canales de distribución pueden diversificarse y especializarse, los datos y la información se pueden convertir en los recursos más valorados y los algoritmos pueden transformar los procesos laborales y de toma de decisiones en diversos ámbitos; pero la augurada quinta revolución industrial, basada en el desarrollo de la computación cognitiva que unirá máquinas y humanos, no podrá obviar el mantenimiento de las conexiones humanas en su versión más real y física.

Tanto las posesiones digitales (p.ej.: una llista de Spotify) como los pagos electrónicos (p.ej.: eCommerce) constituyen ya parte de nuestra singular forma de cohesión en las diferentes comunidades humanas; pero ¿cómo puede una posesión digital única y no replicable (NFT), pagada mediante una criptodivisa sujeta a variaciones de valor impredecibles, irrumpir en el "ecosistema de pagos" sin influir a la larga en su estabilidad? Habrá que observar su evolución, si bien, por el momento, lo que se está haciendo es replicar lo que sucede en el mundo real (por ejemplo, comprar una obra de arte tokenizada mediante una criptomoneda a la que se le aplica una referencia de cambio en moneda fiat), hecho que limita otras opciones más creativas de uso y aplicación.

No podemos pensar en la complejidad que podría suponer la entrada de las más de veinte mil criptomonedas que existen en la actualidad en el mercado de pagos global, aunque muchas de ellas terminen por desaparecer en los próximos meses. Pero sí podemos fijarnos en los más de 250 métodos de pago locales que existen en el mundo, porque ello nos permitiría reducir el foco de observación a cada ecosistema de pago local y poner atención en cómo responde a las interrelaciones de cada

> Pasar de usar recursos tangibles, como el efectivo o las tarjetas, a utilizar dispositivos electrónicos (como cuentas eMoney o billeteras digitales) ha supuesto una evolución hasta cierto punto normal en la medida que la tecnología ha ido aportando nuevos medios y soluciones

Las generaciones más jóvenes, que apuestan claramente por las nuevas tecnologías y se despegan de los métodos tradicionales, serán los futuros compradores que definirán la forma de relacionarse con los futuros comerciantes

uno de sus componentes. En el caso de España, según el último informe de Adyen, los medios de pago digitales solo son usados por el 43% de la población para realizar compras, en tanto que el 20% prefiere no utilizarlos por desconfianza o por no querer perder el control del gasto. Estos datos se corresponden con la preferencia de uso de la tarjeta de crédito/débito (84%) y del dinero en efectivo (65%). En magnitudes inferiores quedan otros métodos como las billeteras electrónicas, los pagos "in-app", las transferencias, las domiciliaciones, los pagos aplazados (BNPL), Bizum, "one click", P2P/P2B en redes sociales, "pay by link", "tap top pay", pago con QR, …

En todo caso, si en 2015 un grupo de expertos predijeron en el informe El futuro del dinero, la desaparición del efectivo y la hegemonía de las criptodivisas, siete años después el primero mantiene su fortaleza y las segundas están en el punto crítico de una "criptoburbuja" a punto de estallar. En parte, esta situación puede darse porque la seguridad en la transacción y la protección contra el fraude son las razones fundamentales que condicionan la forma de pago (9 de cada 10 consumidores valoran estos atributos como requisitos a la hora de realizar una compra), hecho que solo garantiza el dinero efectivo.

Si recordamos las tres funciones que los economistas clásicos asignan al dinero (medio de intercambio, unidad de contabilidad y almacenamiento de valor), observamos que para el concepto de dinero (bancario, digital o electrónico) son perfectamente válidas, pero para el dinero físico (moneda) habría que complementarlas con otras cruciales como son la preservación de la libertad individual y la independencia de cualquier intermediario (financiero o fiscalizador).

Sería necesario remontarse a Mesopotamia hace 5.000 años para comprender que el dinero aparece como instrumento para materializar operaciones de préstamo en el que surgen dos posiciones: la del acreedor, que asume el rol de "la parte dominante o poderosa"; y la del deudor, que pasa a ser la "parte dominada o sumisa". Lo extraordinario en aquel momento es que no se formalizaba con monedas o con otros instrumentos similares, sino con contratos en los que se asumian compromisos cuyo incumplimiento acarreaba graves consecuencias para el deudor, quien se sometía a las reglas vigiladas por las instituciones que surgieron para proteger al

acreedor o prestamista. Las deudas dejaron de ser una obligación económica para convertirse en una obligación moral. Las primeras monedas aparecieron más de 2.200 años después y, aunque también puedieron participar del sistema de préstamo, consiguieron con el tiempo mantener el carácter de obligación económica y soportar revalorizaciones y devaluaciones a criterio de los gobernantes.

Según el Study on the payment attitudes of consumers in the euro área, realizado por el Banco Central Europeo en 2020, el 73% de los pagos realizados en comercio físico (POS) fueron con dinero efectivo, así como el 48% de los pagos hechos entre personas (P2P). Solo países como Estonia, Finlandia y Holanda bajan del 50% en los pagos realizados en POS. En el caso de España, el efectivo supuso el 82% de todos los pagos registrados y el 66% del volumen de las transacciones. Estos datos contrastan con los de la Encuesta Nacional sobre el uso del efectivo, realizada por el Banco de España en el mismo año, donde se destaca que el 35,9% de los ciudadanos manifestaron utilizar el efectivo como medio de pago más habitual.
La Covid19, el repliegue de sucursales y cajeros llevado a cabo por la banca y la presión de la tecnología habrán matizado estos porcentajes en los dos últimos años, con seguridad, aún más a la baja de lo que vienen haciendo en la última década. No obstante, ¿vamos hacia una sociedad sin efectivo?

Francamente, creo que no. A factores como la preservación de la libertad individual y la independencia de cualquier intermediario, como indicábamos más arriba, hay que añadir otros como: la privacidad o anonimato en las transacciones, la inmediatez en la ejecución, la facilidad de uso, el control del gasto y el aprendizaje de las reglas básicas para la administración de la economía individual.

Las generaciones más jóvenes, que apuestan claramente por las nuevas tecnologías y se despegan de los métodos tradicionales, serán los futuros compradores que definirán la forma de relacionarse con los futuros comerciantes (ver informe Impulsando el futuro de los pagos. 10 mega tendencias). No obstante, estas tendencias digitales se encuentran con el freno del valor que le siguen dando al efectivo, a la inmediatez de su uso y a la libertad de elegir sin condiciones asociadas a la forma de pago, tal como también se deduce de las conclusiones recogidas en el informe Study on New Digital Payment Methods realizado por Kantar Public.

> La irrupción de lo virtual exigirá desarrollar un modelo de relación que, como en todas las revoluciones industriales, mantenga las conexiones humanas intactas

Siendo conscientes de esta realidad, ya son varios los países europeos que han legislado sobre la obligatoriedad de garantizar el acceso al efectivo y a satisfacer determinados servicios con él. No solo para permitir que poblaciones de las que se han retirado las entidades financieras, que los mayores de edad y que los sectores excluidos financieramente puedan gestionar su dinero, sino para mantener este recurso como sistema confiable de intercambio universalmente aceptado y demandado.

No cabe duda de que la sociedad es cada vez más digital y que la tecnología evoluciona a una velocidad vertiginosa, circunstancias a las que no puede sustraerse la industria de pagos; bien al contrario, deben servir de acicate para que las soluciones creadas por ella para consumidores, comercios e intermediarios sean convenientes, pertinentes y confiables más allá del aspecto innovador que incorporen. El problema será la excesiva proliferación de aplicaciones y métodos de pago, no ya porque todas ellas tengan que mantener unos estándares de seguridad, transaccionales y regulatorios, sino porque cuando el abanico de opciones es demasiado amplio, el usuario (con independencia de su edad) termina por adoptar los más sencillos y convencionales. De ahí que tarjetas y efectivo sigan manteniéndose como los principales métodos a nivel global.

No olvidemos que, como el exceso de diversidad en todos los ecosistemas biológicos, el crecimiento descontrolado de los elementos que conforman un entorno puede llevarlo al colapso cuando se supera el "límite de carga". Es decir, en un ecosistema de pagos en el que siga creciendo el número de las diferentes soluciones disponibles, la saturación podría implicar la desaparición de la mayoría de ellas y comprometer el futuro de intermediarios y proveedores de servicios de pago. La alternativa sería converger hacia un sistema de aceptación universal en el que, con independencia de cómo se realicen los pagos y los canales usados, todos los actores que intervengan manejen a lo sumo tres métodos: dinero físico, tarjetas y dinero electrónico. Para este último, las soluciones deberían estar basadas en una cuenta eMoney habilitada para realizar transacciones inmediatas (tiempo real) en moneda fiat o CBDC (en nuestro caso, euro digital).

Otra cuestión será abordar la reconversión de la arquitectura actual que soporta la relación entre consumidores, entidades financieras, proveedores de pago y comercios. Cambiarla implicará reinventar la estructura que soporta el modelo de economía actual, empezando por cómo se emitiría el dinero y siguiendo por quién y cómo se gestionaría su propiedad. Pero esto sería objeto de otra reflexión. Necesaria y urgente.

Enlaces de interés...

- Informe de Adyen de Métodos de pago
- El futuro del dinero
- Study on the payment attitudes of consumers in the euro área
- Encuesta Nacional sobre el uso del efectivo
- Impulsando el futuro de los pagos. 10 mega tendencias
- Study on New Digital Payment Methods

it Reseller TECH&CONSULTING

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

Comunicación “Protópica”

Cómo comunicar en un mundo inmerso en la tormenta perfecta

Decía Kevin Kelly, quien acuñó el término “protopía”: “No creo en la utopía, creo en la protopía — que, a través del progreso y el proceso, mañana será un poco mejor que hoy.”

MANUEL LÓPEZ

ASESOR DE COMUNICACIÓN

Madrileño de nacimiento, horchano de adopción, informático de profesión, con más de 35 años de experiencia en el sector de TI, ha desarrollado la mayor parte de su carrera profesional en HewlettPackard, donde ocupó cargos de responsabilidad en diferentes áreas como consultoría, desarrollo de negocio, marketing, comunicación corporativa o PR. Actualmente dedica la mayor parte de su tiempo a asesorar a starups en temas relativos a la comunicación, desde su posición de partner en la plataforma de profesionales goXnext

Asimismo, en un post en su web kk.org, apunta: “Creo que nuestro destino no es ni la utopía ni la distopía ni el statu quo, sino la “protopía”. “Protopía” es un estado que es mejor hoy que ayer, aunque podría ser solo un poco mejor. “Protopía” es mucho más difícil de visualizar, debido a que una “Protopía” contiene tantos problemas nuevos como beneficios nuevos, esta interacción compleja de trabajar y romperse es muy difícil de predecir.

Hoy nos hemos vuelto tan conscientes de las desventajas de las innovaciones y tan decepcionados con las promesas de las utopías pasadas, que ahora nos resulta difícil creer incluso en la “Protopía”: que mañana será mejor que hoy. Nos resulta muy difícil imaginar cualquier tipo de futuro en el que nos gustaría vivir.”

Estamos inmersos en una tormenta perfecta. Si nadie lo remedía, se están juntando todos los factores para producir la tormenta perfecta. Todo comenzó a primeros de año cuando Rusia inició la invasión de Ucrania, entonces todavía seguíamos inmersos en la gran pandemia que llevamos soportando los últimos 2 años. A partir de ahí, nos encontramos con todos los ingredientes de la tormenta económica perfecta: inflación de 2 dígitos, recesión inminente, conflictos bélicos por doquier, energía cara y escasa, sequía galopante… y así podríamos seguir sumando factores que hacen que la tormenta económica que se avecina sea de las que hacen época.

Y ante estas circunstancias, ¿cómo debe afrontar la comunicación de las empresas, tras este verano sofocante, el otoño caliente que se avecina?

Creo que va a ser un otoño realmente caliente para la comunicación. En un momento en el que la desinformación campa a sus anchas por todos lados, en el que la política intenta dominar el relato y no solamente el político, sino el relato en todas y cada una de las facetas de la vida que afectan al

Comunicar en tiempos difíciles es todavía más complicado que hacerlo en tiempos de bonanza económica. La comunicación "Protópica" tiene la obligación de ser imaginativa

ciudadano; comunicar se me antoja más difícil que nunca.

En estas circunstancias podemos plantearnos una comunicación utópica, donde todo va a ser de color de rosa y maravilloso e intentaremos convencer a nuestro cliente que con nosotros todo va a ir mejor, o una comunicación distópica, donde todo va a ir a peor y lo que tenemos que hacer es facilitar el "sálvese quien pueda" a nuestro cliente. O podemos apostar por una comunicación "Protópica" haciendo que mañana sea un poco mejor que ayer y convenciendo a nuestro cliente de que somos sus aliados en este camino hacia la "Protopía".

Podríamos hacer una analogía, casi filosófica, definiendo la Propaganda como la Utopía, la Realidad como la Distopía y la Comunicación como la "Protopía".

Y puestos a filosofar, definamos la "Comunicación Protópica":

Personalizada

En tiempos tan difíciles como lo que nos esperan, los clientes esperan soluciones a sus problemas y no generalidades y buenas palabras. Es por ello que debemos hacer una comunicación lo más personalizada para nuestro público objetivo, centrándonos en la solución de sus problemas y no en intentar colocar nuestro producto como sea. Debemos huir de la utopía que representa la propaganda, de la distopía que parece que va a ser la realidad y hacer una comunicación "Protópica", aportando soluciones para hacer el mundo un poquito mejor cada día para nuestros clientes.

Resiliente

Capacidad de adaptación de un ser vivo frente a un agente perturbador a un estado o situación adversos, es la definición de la RAE para resiliencia. Para la comunicación "Protópica" es una aproximación muy adecuada, ya que será necesario adaptarse permanentemente dentro de una situación económica y social muy adversa. Nuestra comunicación tiene que ser resiliente en todos los aspectos, pero sobre todo en la faceta de adaptarse a los cambios para solucionar los problemas de nuestros clientes.

Organizada, Ordenada

Debemos organizar y ordenar detenidamente nuestra comunicación. Cuando vivimos tiempos convulsos debemos de estructurar muy bien

Nos hemos vuelto tan conscientes de las desventajas de las innovaciones y tan decepcionados con las promesas de las utopías pasadas, que ahora nos resulta difícil creer incluso en la "Protopía"

nuestro mensaje e intentar no confundir al receptor de este. Es pues momento de pensar, de estructurar, de organizar y ordenar nuestra comunicación, para transmitir de forma positiva nuestro mensaje y ser parte importante del desarrollo de nuestra empresa.

Transparente

Es fundamental que comuniquemos transparentemente. En tiempos de posverdad y desinformación, lo más apropiado es comunicar con total transparencia, huyendo de mensajes de propaganda, tratando de engañar a los clientes para conseguir likes, seguidores o visitantes a nuestros recursos digitales. La transparencia y la alineación con nuestro negocio juegan un papel fundamental en tiempos adversos como los que vamos a vivir en lo que queda de 2022 y a lo largo de 2023.

Objetiva

En momentos difíciles, la objetividad es algo muy valorado por los clientes. No son tiempos de rodeos, de circunloquios, de mensajes tendenciosos o interesados; debemos comunicar con total objetividad y siempre pensando en nuestro consumidor objetivo y en nuestro negocio intentando que cada

día aporte un poco más a la solución de los problemas de nuestros clientes.

Práctica
Son momentos de ir al grano y dejarnos de florituras. Van a ser unos tiempos donde la famosa frase de Voltaire “Lo perfecto es enemigo de lo bueno” será algo así como el leitmotiv para la comunicación “Protópica”. Debemos ser prácticos en todos los sentidos, desde la definición del mensaje, hasta el control del gasto de la comunicación.

Imaginativa, Incitadora
Comunicar en tiempos difíciles es todavía más complicado que hacerlo en tiempos de bonanza económica. La comunicación “Protópica” tiene la obligación de ser imaginativa para pensar en un mundo mejor hoy que ayer. Y a la vez incitadora, para que nuestros clientes objetivo se sientan motivados, empujados a comprar nuestros productos para hacer que su mundo sea un poco mejor cada día.

Coordinada, Contextualizada
Estamos dentro de un mundo multicanal, donde el usuario está permanentemente bombardeado por todo tipo de medios, de compañías, de mensajes, de propuestas, de propagandas, de desinformaciones, … En este mundo tan “infotoxicado” es necesario que nuestra comunicación esté perfectamente coordinada para que llegue nítida a nuestros clientes en tiempo y forma y contextualizada para que se aleje del ruido al que están expuestos permanentemente los usuarios de nuestro mundo digital.

Avalada
No son tiempos de experimentos. La comunicación “Protópica” debe utilizar siempre que sea posible métodos contrastados y avalados para llegar a nuestro público objetivo, tenemos que asegurar el mayor impacto posible, así como el mayor ROI para nuestra empresa.

Así pues, en este otoño caliente del 2022, que será el preludio de tiempos complicados, apostemos por la “Protopía” y hagamos una comunicación adaptada a los tiempos que nos tocará vivir, proponiendo un futuro mejor cada día, para que nuestros clientes sigan confiando en nosotros.

Y en esto es en lo que estamos: Encuentros con la comunicación, para evitar desencuentros y frustraciones con la comunicación.

Enlaces de interés…

- KK.org, The Technium – Protopia
- Utopia is a dangerous ideal: we should aim for ‘protopia’, Michael Shermer
- Protopia Futures [Framework], Monika Bielskyte on Medium

En tiempos de posverdad y desinformación, lo más apropiado es comunicar con total transparencia, huyendo de mensajes de propaganda

¿Cuál es la situación de la empresa española en relación con la digitalización?

¿Qué tecnologías son las que están impulsando la transformación digital?

Descubra las últimas tendencias en el Centro de Recursos IT User

Tecnología para tu Empresa

Con la colaboración de:

Camerfirma AN INFOCERT COMPANY

NFON

Synology