Texto
R. Contreras

LA AUTENTICACIÓN DE DOBLE FACTOR SE IMPONE CON EL TELETRABAJO

¿Quién está al otro lado?

<< La gestión de identidades se ha convertido en una de las principales preocupaciones de las compañías que tienen su plantilla desperdigada en sus hogares y necesitan autenticar a sus usuarios, para evitar brechas de datos, ciberataques y fugas de información.

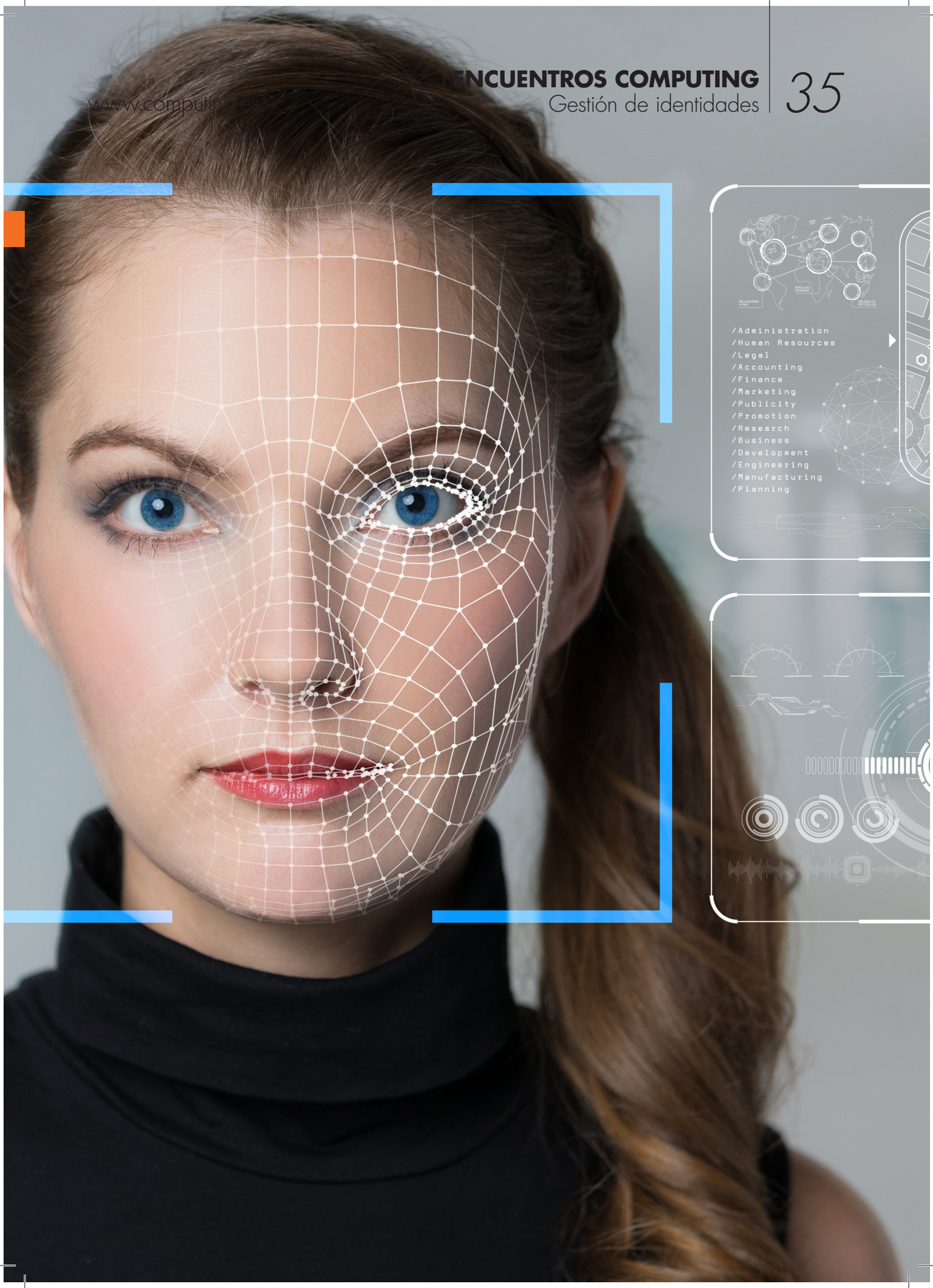
El mundo ya no es el que era, la realidad se ha vestido de digital para poder abordar las nuevas necesidades de comunicarnos y de trabajar. Ya es un imperativo identificar a los usuarios dentro de cualquier sistema corporativo, la gestión de identidades requiere una vuelta de tuerca para que sea cada vez más eficaz y segura. Hay que aceptar nuevas reglas de juego, entender que identificarnos, por muchas molestias que acarree el proceso, es la mejor receta para evitar intrusiones y robos de datos. Empresas como Okta trabajan en esta dirección y los CISO de las compañías saben de sobra los riesgos que corremos si no se establecen unas reglas de seguridad y de autenticación acordes a una nueva realidad más dispersa y sin perímetros concretos. Con esta idea se ha celebrado el encuentro de Computing con responsables de seguridad de grandes marcas para pulsar su visión en este punto y qué estrategias están poniendo en marcha.

Manuel Tarrasa, CIO & CTO de Prosegur, es consciente de este problema. "Cuando llegó la pandemia nos dimos cuenta de que la ciberseguridad iba a ser un problema, todas las empresas nos convertíamos en víctimas propiciatorias de los hackers, por ello, pusimos énfasis en una VPN con doble factor de autenticación". Pero no se conformaron con esta medida, "para evitar otro factor de riesgo definimos una política de seguridad por la que todos los ordenadores fueran corporativos, nunca personales, porque resultaba más fácil securizarlos en serie. La gente tenía que entender que el portátil era un instrumento de trabajo y no para sacar las entradas de un concierto". De esta manera, se restringieron las facilidades de navegación, algo que supuso un cambio de mentalidad y no de carácter tecnológico.

Distintas fueron las circunstancias de Transports Metropolitans de Barcelona, como relata Juan José del Río, responsable de Seguridad TI: "Teníamos VPN configuradas para proveedores y técnicos desde casa. Pero no toda la plantilla tenía estas condiciones. En un fin de semana habilitamos un entorno Citrix para más de 1.000 usuarios y no teníamos doble factor. En este momento estamos en fase de estudio más profundo para hacer una ampliación. Queremos extenderlo a Windows, Linux y al acceso de proveedores".

Equipo especializado de seguridad

José María Córcoles, IT Manager & Business Analyst de Mediapro, se siente un privilegiado por contar con un equipo especializado en seguridad, un hecho diferencial en las empresas. "Nos pilló a contrapié, en un momento de cambio de estrategia, estábamos implantando un cambio de una filosofía on premise a una migración total al cloud". Tras la fase de apagar fuegos, el equipo de seguridad analizó cómo tenía que ser el futuro del puesto de trabajo en el que aparece el concepto perimetral y del puesto endpoint corporativo. "Las primeras actuaciones fueron llevar los equipos a casa, aplicar el doble factor de autenticación y nuevas políticas de seguridad y acceso


/Administration
/Human Resources
/Legal
/Accounting
/Finance
/Marketing
/Publicity
/Promotion
/Research
/Business
/Development
/Engineering
/Manufacturing
/Planning

"La gente de sistemas ve ventajas en el cloud, y nosotros los CISO vemos los problemas"

a este entorno cloud, tanto para los servicios como para los datos, estableciendo dos niveles de seguridad diferentes".

Desde el punto de vista de Maica Aguilar, gerente de Seguridad de Ferrovial, "todas las empresas nos hemos adaptado a esta situación en mayor o menor medida. En nuestro caso, teníamos doble factor de identificación y acceso remoto, pero hubo que adaptar la situación a las necesidades, no es lo mismo el uso diario en un pequeño porcentaje de personas que la utilización de forma masiva para todos los empleados. Aprovisionar todos los accesos fue necesario para cambiar de escenario. Otras acciones realizadas han tenido que ver con la concienciación, dado que el empleado necesitaba estar alerta de los riesgos y los timos cibernéticos que proliferaron. Fueron unos meses críticos, pusimos, además, antivirus gratuitos para sus dispositivos personales".

Javier Montoya, gerente de Sistemas y Seguridad de Agbar, reconoce que, aunque tenían un nivel bastante aceptable, la situación les afectó. "Tuvimos de la noche a la mañana que irnos a trabajar a casa y nos topamos con el problema del ancho de banda. Llevamos

JUAN PER MUÑOZ, CHANNEL ACCOUNT MANAGER, SOUTHERN EMEA DE OKTA

"PROPONEMOS HERRAMIENTAS QUE SECURICEN AL EMPLEADO ALLÁ DONDE ESTÉ"

Okta es una empresa californiana que nació en 2009 y que cuenta con más de 10.000 clientes en todo el mundo y con presencia en 74 países. Sus dos fundadores, Frederic Kerrest y el CEO Todd McKinnon, eran dos directores de ingeniería de Salesforce. A nivel global, somos líderes en gestión de acceso de identidades. En España, llevamos dos años, ya tenemos 50 clientes tanto en el sector público como en el privado, y estamos aproximándonos a la gran cuenta. Desde hace dos años ya adoptamos el modelo de Zero Trust, el perímetro se estaba diluyendo y ya no servía para los empleados, clientes y proveedores. Desde Okta, proponemos tecnologías que securicen al usuario allá donde se encuentre con aplicaciones con sesión de inicio único, herramientas de doble factor o multifactor de autentificación para que cuando los usuarios estén conectados en su red corporativa vía directa, VPN o de visualización, sea de una forma segura y sean productivos para sus empresas.

ASISTENTES

1 Javier Montoya, Agbar | **2** Maica Aguilar, Ferrovial | **3** José María Córcoles, Mediapro | **4** Manuel Tarrasa, Prosegur | **5** Juan José del Río, Transports Metropolitans de Barcelona | **6** José Luis Guerra, Meliá Hotels

muchos años con doble factor de identificación en escenarios de riesgos y estamos evolucionando hacia soluciones multifactor. Esto nos va a permitir una mayor visión de lo que puede estar pasando por detrás. La contraseña y nada es lo mismo".

En este punto coincide Maica Aguilar: "A nivel mundial, cada día nos levantamos con una brecha de datos de usuarios. Una contraseña es como dejar la puerta de tu casa entornada. El muro tradicional no vale, hay que trabajar de otra forma y centrarse en monitorizar".

Para Córcoles, la madurez de las empresas y de las personas son los factores que te van a complicar o facilitar el despliegue. "Tampoco se ha hablado del tema legal, desde el momento que tienes capacidad de IA y geolocalización estamos más preocupados por aspectos legales que en asegurar la continuidad de la información y del negocio. ¿Podemos tener problemas a la hora de aplicar la IA?".

La respuesta a esta cuestión la resuelve la portavoz de Ferrovial: "La regulación está para ayudarnos, el GDPR no impide que tomes las acciones necesarias para el debido control de seguridad de tu compañía. En un ecosistema de empleados, clientes o proveedores debes ejercer ese control y esa responsabilidad te legitima detectar comportamientos anómalos e impedir el acceso a los datos. Por ejemplo, detectar un IP que se comporta de forma anómala es necesaro, GDPR no es un impedimento siempre que se cumpla con lo establecido por la regulación".

¿Es más segura la nube?

En este momento de migración general hacia el cloud, cabe preguntarse si la nube es más segura o, por el contrario, presenta más fragilidad de la prevista. Tarrasa opina que "la nube tiene más medios para luchar en ciberseguridad de fábrica y además es más nueva. Hemos decidido aprovechar el viaje a la nube teniendo la ciberseguridad embebida por diseño. También hay que tener en cuenta los espejismos de tu seguridad on premise, ¿hasta qué punto es segura tu wifi si te puedes conectar pasando por la acera de tu oficina?

Javier Montoya observa la cuestión de un prisma diferente: "La gente de sistemas ve ventajas en el cloud, y nosotros vemos los problemas. Los CISO hacemos de contrapeso como pájaros de mal agüero porque solo vemos el lado oscuro, que lo tiene. Se pueden hacer cosas seguras en la nube, pero no resulta barato. En on premise no eficientas las cosas, pero sí el control".

Maica Aguilar considera que "nubes hay muchas, y todo depende del proveedor". Pero en todo caso, ella afirma que cloud es un imperativo, teniendo en cuenta que la seguridad es una responsabilidad compartida. "Nunca vamos a tener la capacidad de inversión de las grandes de la nube pública, siempre van a ir por delante y cuentan con profesionales de gran nivel". En todo caso, la sensación que mostraban es que las nubes han evolucionado mucho y aportan más de lo que quitan, tienen mucha capacidad y están preparadas para que la seguridad esté inherente; hay que considerarlas como aliadas.

> **"Llevamos muchos años con doble factor de identificación en escenarios de riesgos y estamos evolucionando hacia soluciones multifactor"**

Tarrasa pone la puntilla: "Tu nube puede ser mala, pero puede que tu centro de datos no tenga llave y cualquiera pueda acceder a las instalaciones".

Como premisa, Zero Trust se convierte, como enfatiza Javier Montoya, en un mantra, "la experiencia te dice que no debes confiar, tu proveedor trabaja con otras veinte empresas y puede convertirse en el nexo de unión de un virus o transmisor de un ciberataque". Sin embargo, es un modelo que resulta complejo de implementar, "porque hay que convencer a empresas terceras de que tienen que pasar por el aro de mi ciberseguridad, y a tu empleado lo puedes expedientar, pero a un proveedor no puedes hacer más allá que rescindirle el contrato". ■