EN BÚSQUEDA DE MAYOR SEGURIDAD

Passwordless: cómo funciona este modelo y cuáles son los beneficios de la autenticación sin contraseñas

Actualmente, diversas aplicaciones –entre las más populares Apple y Google– cuentan con herramientas de este tipo, con las cuales se puede dar ingreso a las cuentas mediante teléfonos con reconocimiento facial, huella digital, o bien, con el uso de llaves de seguridad y sin la necesidad de recordar y digitar claves.

DIEGO AGUIRRE

Hace poco más de una semana, y al igual que cada 28 de enero, se conmemoró a nivel internacional el Día de la Privacidad de la Información –también conocido como Día Internacional de la Protección de Datos Personales–, fecha en que se busca promover las mejores prácticas y modelos de resguardo de la seguridad de la identidad de las personas.

Ante este escenario de fuerte avance de la tecnología y, en paralelo, de las amenazas, uno de los modelos que han ganado ampliamente terreno en el combate de los riesgos propios de la digitalización es el de *passwordless* o autenticación sin contraseñas, el cual busca ser un proceso de verificación de un usuario sin que este deba ingresar claves alfanuméricas, aumentando así la seguridad y la facilidad de su uso en las distintas cuentas, tanto a nivel usuario como institucionales.

Milflen Torres, jefe de Infraestructura y Seguridad de ITQ Latam, explica que en la actualidad los procesos de autenticación a los que son sometidos los usuarios para acceder a sus servicios en línea, como sistemas de correo, cuentas de banco y aplicaciones, presentan diversas vulnerabilidades, debido a que se utilizan claves estáticas que a pesar de ser modificadas cada cierto período de tiempo pueden ser identificables a través de patrones comunes como unificaciones entre nombre, fechas de nacimiento y nombres de hijos.

"Para mejorar este escenario ya se cuenta con aplicaciones de Multifactor de Autenticación que une al menos una contraseña conocida y, adicionalmente, una segunda verificación a través de un patrón más conocido como *token*. El procedimiento, sin embargo, genera ciertas fricciones e incomodidades en los usuarios. Y para solucionarlas, nace el concepto del mecanismo de acceso a la información y recursos de los usuarios sin contraseña, es decir, *passwordless*, asegurando con un fuerte sistema que la autenticación del usuario es real y sin introducir contraseñas particulares en cada sistema o recurso del usuario", detalla Torres.

En sencillo, mediante estos modelos se obvia la contraseña, centrando el cifrado y la autenticación en lo que tengo o quién soy. Primero se solicita un nombre de usuario o dirección de correo electrónico en el servicio en el que quiere autenticarse, luego este envía una notificación o código de verificación a su dispositivo confiable o se solicita una verificación biométrica, donde posteriormente el usuario proporciona la verificación correcta con lo que puede acceder al servicio.

Alejandro Barros, investigador del Centro de Sistemas Públicos (CSP) de Ingeniería Industrial de la Universidad de Chile, comenta que hoy en día diversas aplicaciones cuentan con herramientas de este tipo, por ejemplo: teléfono con reconocimiento facial, o bien el uso de llaves de seguridad. "Cada vez más se están incorporando estas tecnologías, sobre todo a sus aplicaciones en la nube (MS, Google y otros), con servicios como Windows Hello, Touch ID y Face ID, entre otros", señala.

Mayor seguridad y múltiples beneficios

A juicio de los expertos, para muchos de los usuarios el uso de las contraseñas es un dolor de cabeza, ya que hay que recordar constantemente las credenciales del trabajo, *homebanking*, supermercado, tiendas de ropas, portal de compras, *e-mail* personal, redes sociales, entre otros. Adicionalmente, el uso de usuario y contraseña suele ser el vector principal para ataques informáticos, estafas *online*, y muchas veces perder estas coordenadas significa comprometer la vida digital de las personas.

CRECIMIENTO

Ante el avance de la tecnología y las amenazas, ha ganado terreno es el *passwordless* o autenticación sin contraseñas.

Debido a lo anterior es que el *passwordless* ofrece múltiples beneficios y atributos frente a un proceso de autenticación tradicional, simplificando la tarea, elevando los niveles de seguridad, facilitando la integración entre canales y reduciendo las posibilidades de fraude.

Maximiliano Olivera, *head of* Sales and Regional Operations de Ubiquo Chile, explica que este modelo ofrece un nivel de seguridad muy superior al de la autenticación tradicional basada en contraseña, debido a que el usuario no necesita compartir sus datos de autenticación con terceros y no hay que preocuparse por robos de contraseña. "Asimismo, reduce significativamente la posibilidad de fraude digital, debido a la mayor dificultad de comprometer los sistemas de autenticación", dice.

Desde la otra vereda, a nivel institucional también existen ventajas versus modelos de autenticación tradicionales. Camilo Mix, asesor en Ciberinteligencia de CronUp Ciberseguridad, comenta que sin contraseñas tradicionales existe un menor mantenimiento y coste para la administración, se simplifican las tareas rutinarias para el personal de TI, disminuyen las probabilidades de ser víctimas de un ataque de *phishing* o sus derivados, y se evita la mala práctica popular de las contraseñas compartidas".

Sin embargo, una desventaja que presenta este modelo en la actualidad es el costo de la implementación. Gabriel Bergel, *associate partner* en Security & Resiliency de Kyndryl Chile, explica que mediante el *passwordless* se debe tener la capacidad de autenticar al usuario a través de los dispositivos o biometría, por lo que hay que invertir en sistemas adecuados, y al mismo tiempo se obliga a hacer la formación del personal para usar este tipo de tecnología. "Otra dificultad es que se produce un único punto de falla, por ejemplo, si se rompe o roban el dispositivo, no se puede autenticar a la persona", finaliza el ejecutivo.

Pelayo Covarrubias, presidente de Fundación País Digital y director de Proyectos Corporativos de la Universidad del Desarrollo (UDD),

FUNDACIÓN PAÍS DIGITAL

Conectividad en localidades remotas y alfabetización de comunidades: los desafíos pendientes en materia digital para 2023

Los trabajos en pos de cerrar la brecha en el acceso que se están llevando a cabo van de la mano con iniciativas que buscan fomentar las competencias digitales a través de capacitaciones y talleres.

DIEGO AGUIRRE

El internet, tanto fijo como móvil, es una herramienta que para muchos se encuentra al alcance de la mano o a tan solo un clic. Sin embargo, lo cierto es que aún quedan varias zonas de Chile que no cuentan con este servicio, ya sea por motivos geográficos, por falta de infraestructura técnica o accesibilidad de los dispositivos. De hecho, el estudio "Brecha en el uso de internet: Desigualdad digital", de Fundación País Digital (FPD), da cuenta de lo anterior, donde la conectividad de la población urbana (81% de uso de internet) versus las zonas rurales (58% de su población usa internet) presenta importantes diferencias.

Bajo este contexto, FPD ha identificado diversos desafíos en materia digital para el 2023, los que van desde la conexión de última milla a la alfabetización de las comunidades. Pelayo Covarrubias, presidente de la entidad y director de Proyectos Corporativos de la Universidad del Desarrollo (UDD), explica que para lograr ese 100% de conectividad es necesario garantizar un mayor acceso a internet, una educación basada en competencias digitales y una constante actualización de las capacidades laborales de las personas. Hoja de ruta que se está llevando a cabo a través del proyecto "Conectando territorios" en localidades remotas del país.

"La clave para acortar las brechas digitales en Chile es la colaboración público-privada, donde se impulsen esfuerzos simultáneos enfocados en cubrir los requisitos técnicos y tecnológicos, pero además, se fomentan competencias digitales a través de capacitaciones y talleres para la población, por supuesto, tomando en cuenta las necesidades de las personas", dice Covarrubias.

El Programa "Conectando territorios" se enmarca en el cumplimiento de las metas del "Plan Brecha cero digital 2022-2025" del Gobierno, cuya motivación es que todos los habitantes del país tengan acceso a conectividad, independiente del lugar en que viven o de las posibilidades económicas que tengan. En sus resultados preliminares, este programa ha permitido conectar vía internet a localidades como Nacimiento, Caimanes, Ruta de la Madera y Villa Mininco.

Cifras de la Subsecretaría de Telecomunicaciones (Subtel) muestran que durante 2022 el uso de 5G avanzó más rápido que cuando partió el 4G, doblando la cantidad de conexiones en la mitad del tiempo. En esa línea, las proyecciones contempladas en el Plan de Transformación Digital Chile 2035 del Senado —basado en los lineamientos del plan estratégico "Un país digital" de FPD— y el plan Brecha digital presentado por la Subtel, indican que hacia 2025 la tecnología 5G alcanzará al 90% de la población, mientras que en 2030 este número llegará al 98% y solo cinco meses después la cifra alcanzará al 100%. Asimismo, se estima que la fibra óptica abarque el 65% de los hogares nacionales hacia 2025, 70% en 2030 y 85% en 2035.