yubico

# Encuesta sobre el estado de la autenticación en las empresas a escala mundial

Cómo las empresas modernas están adoptando la MFA (autenticación de múltiples factores) para afrontar el phishing

## Resumen ejecutivo

La autenticación desempeña un papel fundamental en el panorama actual de la ciberseguridad, ya que determina si los ataques consiguen acceder y causar estragos, o son detenidos en seco. A medida que las empresas adoptan modelos de trabajo híbridos y aprovechan los servicios en la nube, cada vez resulta más complicado hacer bien la autenticación, y equivocarse, dada la frecuencia, el crecimiento y los daños de los ciberataques, puede conllevar graves consecuencias. Utilizar una autenticación obsoleta o ineficaz pone en riesgo tanto la seguridad como la productividad, por lo que Yubico decidió investigar más a fondo cómo gestionan las empresas su autenticación preguntándoles directamente.

**Más de 16 000**
respuestas

organizaciones con
**entre 1 y más de 2000**
empleados

**en 8**
países

Nuestra encuesta inaugural sobre el estado de la autenticación en empresas de todo el mundo se diseñó para obtener una instantánea global de la autenticación. Recibimos más de 16 000 respuestas, desde empleados principiantes hasta propietarios de empresas, en organizaciones de entre uno y más de 2000 empleados, en ocho países: Reino Unido, Estados Unidos, Australia, Nueva Zelanda, Singapur, Francia, Alemania y Suecia.

Los resultados se recogen y contextualizan en el siguiente informe. Ofrecen una visión detallada y objetiva de las prácticas y actitudes que impulsan la autenticación en empresas reales. Las cifras demuestran que las organizaciones son conscientes de que están expuestas y se ven perjudicadas por los ciberataques. Sin embargo, pocos han tomado medidas significativas para sustituir las prácticas de autenticación heredadas, como el factor único o la autenticación móvil, por mejores prácticas como la autenticación multifactor resistente al phishing (MFA).

Cuando se realiza correctamente, la MFA moderna ofrece una forma relativamente sencilla, asequible y eficaz para cualquier organización para mejorar su seguridad, pero la mayoría de las empresas no están utilizando esto a su favor. Este informe, basado en amplios datos de encuestas, revela dónde deben mejorar aún las prácticas de autenticación y ayuda a las organizaciones a comprender cómo y por qué.

59% de los empleados

aún confía en **nombre de usuario y contraseña** como método principal para autenticarse en sus cuentas

## Phishing

Engañar a los usuarios para que proporcionen credenciales de acceso u otros datos sensibles

## Autenticación de un solo factor

Autenticación basada en un único factor, normalmente una contraseña personal

## Autenticación multifactor

Autenticación que requiere uno o más factores adicionales, como una notificación push, un código de un solo uso o una llave criptográfica

## MFA resistente al phishing

Autenticación multifactor resistente a los atacantes que interceptan, o incluso engañan a los usuarios para que revelen información de acceso

# Las prácticas de autenticación de las empresas no cambian

### ¿Cuáles son las principales formas de autenticar las cuentas de su empresa?*


* Se admiten varias respuestas

A pesar de los grandes avances en la manera en que las empresas utilizan las TI, la manera en que gestionan la autenticación no ha cambiado con la misma rapidez. La autenticación de factor único, basada en proporcionar un nombre de usuario y una contraseña, sigue siendo el principal medio de autenticación (por un amplio margen), a pesar de que existen abundantes pruebas de que los malhechores pueden comprar, robar o romper esas credenciales con facilidad. Los datos son demoledores: la forma menos segura de autenticación es también la más común.

El 30% de los encuestados utiliza la autenticación móvil por SMS, los gestores de contraseñas y las aplicaciones de autenticación que permiten la MFA. La necesidad de un segundo paso de autenticación dificulta el acceso no autorizado, pero estos métodos tienen fallos. Los textos pueden ser interceptados en el camino, las aplicaciones pueden ser explotadas y cualquier forma de MFA que dependa de los teléfonos es vulnerable a los dispositivos perdidos, rotos o robados. Son mejores que la autenticación de un solo factor, pero distan mucho de ser perfectas.

Las llaves de seguridad ofrecen el tipo de MFA resistente al phishing que exigen los gobiernos de todo el mundo, incluidos los organismos federales de EE. UU. Las llaves de seguridad se consideran la regla de oro de la MFA, pero las mencionó menos del 20% de los encuestados. Además, más del 10% no sabía cómo se autenticaba su empresa o no utilizaba ningún tipo de autenticación. Esta pregunta revela que la mayoría de las empresas son vulnerables (en gran medida) como consecuencia de una autenticación débil de un solo factor e incluso entre los que ya disponen de MFA, el riesgo de ataques de phishing y de problemas de autenticación sigue siendo alto. La adopción de la MFA por parte de las empresas todavía tiene un largo camino por recorrer.

El 22% de los empleados

*****

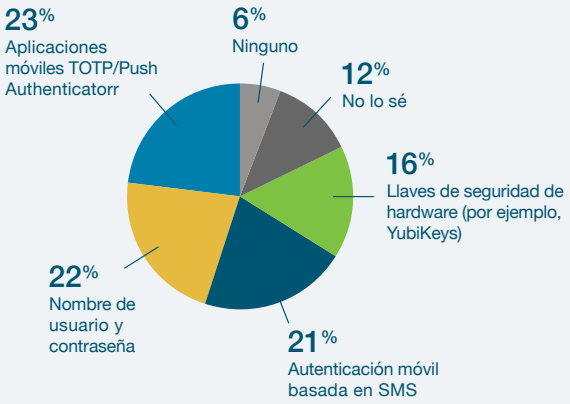
cree que el nombre de usuario y la contraseña **son más seguros**

## ¿Por qué las llaves de seguridad son ideales para la autenticación?

Exigir una llave física específica para acceder a las cuentas en línea anula por completo el riesgo de ataques remotos. Las llaves de seguridad contienen un código criptográfico único que no se puede extraer y los protocolos FIDO2 significan que las llaves solo responderán a fuentes de confianza, lo que las hace resistentes a la suplantación de identidad. Las llaves de seguridad vienen en una variedad de factores de forma (USB-A, USB-C, Lightning, NFC) para interactuar fácilmente con más dispositivos y, como la forma de MFA en la que más confían los profesionales y expertos en seguridad, son ideales para una autenticación robusta.

# La percepción no es la realidad

### ¿Cuál cree que es el método más seguro para la autenticación?




Es una señal positiva de que cerca de una cuarta parte de los encuestados enumeraran las aplicaciones de autenticación (como Google Authenticator u Okta) como el método de autenticación más seguro. Estas proporcionan una mejora significativa de la seguridad con respecto a la autenticación de un solo factor y también algunas formas de multifactor. Estas aplicaciones pueden ser problemáticas porque dependen de tener acceso al propio teléfono y son vulnerables a ataques de phishing sofisticados. Aun así, el hecho de que ocuparan el primer puesto sugiere que la gente es cada vez más consciente de una autenticación segura frente a una insegura.

Sin embargo, la respuesta que quedó en un cercano segundo lugar, nombre de usuario y contraseña, socava esta afirmación. **Más de una quinta parte de los encuestados creía que las credenciales de inicio de sesión básicas no solo eran seguras, sino las más seguras,** a pesar de que ha habido años de advertencias generalizadas y formación corporativa centrada en la inseguridad de las contraseñas en particular. En tercer lugar se situó la autenticación móvil basada en SMS, que es mejor que nada, pero está ampliamente considerada como la forma más insegura de MFA por su alto riesgo de phishing. En comparación con las aplicaciones de autenticación, casi el doble de las personas identificó los factores de autenticación con fallos de seguridad evidentes como las opciones más seguras disponibles, lo que sugiere una enorme brecha de percepción en torno a la autenticación.

Refuerza esta conclusión el hecho de que solo 1 de cada 6 empleados señaló las llaves de seguridad como la opción más segura. El porcentaje se elevó al 42% en el nivel de directivos, lo que podría indicar que los empleados más júnior necesitan mejor formación sobre la MFA (junto con opciones más seguras).

El 61 % de los empleados y el 79% del personal de niveles directivos

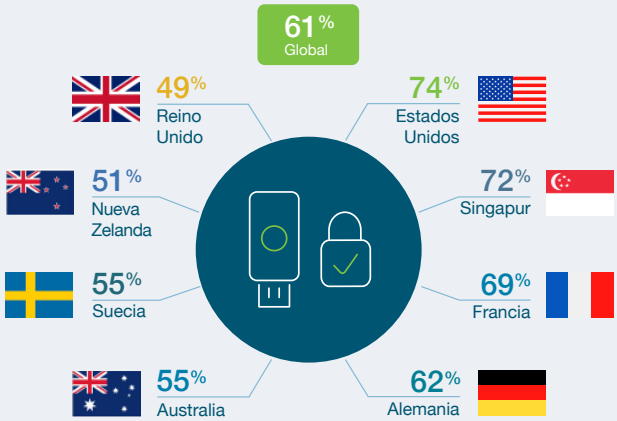
creen que su organización necesita actualizarse a una **MFA moderna y resistente al phishing** (como las llaves de seguridad de hardware)

## Los usuarios avanzados eligen la MFA resistente al phishing

Los datos de la encuesta contenían una interesante revelación: **entre los encuestados que inician sesión en más de 9 cuentas o aplicaciones a diario, la gran mayoría (76%) desea que su organización adopte una MFA resistente al phishing.** Esa cifra cayó por debajo del 40% en el caso de las personas que no inician ninguna sesión diaria de media. Es lógico que estos usuarios avanzados den prioridad a la seguridad y a una autenticación más sólida. También tiene sentido que prefieran la MFA resistente al phishing en particular, que ofrece un inicio de sesión mucho más rápido que las aplicaciones de autenticación que requieren nuevos códigos de verificación de un solo uso para cada inicio de sesión en una cuenta.

# La gente tiene sentimientos contradictorios sobre la autenticación

### Mi organización necesita actualizarse a una MFA moderna resistente al phishing (como las llaves de seguridad de hardware)




Más del 60% de los encuestados coincidió en que su organización necesita actualizarse a una MFA resistente al phishing (el 79% a niveles directivos), y cerca de una cuarta parte indicó estar «totalmente» de acuerdo. Tal vez lo más revelador sea que apenas un 10% de los encuestados se mostró en desacuerdo y menos de un 5%, en fuerte desacuerdo. La encuesta muestra un fuerte apoyo a la incorporación de la MFA resistente al phishing y una oposición poco significativa. Parece que una MFA robusta es una política con la que la gente ya está de acuerdo, especialmente entre los cargos directivos.

Sin embargo, los resultados de otra pregunta de la encuesta complican esta conclusión: En relación con las opciones de autenticación que ofrece su organización, ¿cree que son suficiente seguras? Casi el 80% de los encuestados se mostró de acuerdo con esta afirmación y solo el 15% se mostró en desacuerdo. El escepticismo sobre la seguridad fue mayor entre los encuestados franceses y menor entre los encuestados estadounidenses, pero los encuestados de todo el mundo consideraban que la seguridad era al menos suficiente.

Basándonos en algunas de las lagunas de percepción expuestas en la pregunta anterior, es justo preguntarse con qué precisión puede evaluar la gente la seguridad. Dejando esto a un lado, los datos sugieren que, aunque la gente piensa que la seguridad es adecuada, también reconoce que hay margen de mejora y que la MFA resistente al phishing es una pieza que falta allí donde está ausente.

El 78% de los encuestados

ha estado expuesto a un ciberataque en su vida personal en los últimos 12 meses

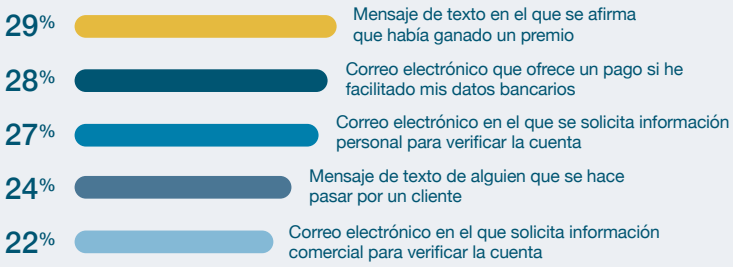
El 60% de los encuestados

ha estado expuesto a un ciberataque en el trabajo en los últimos 12 meses

# Los ciberataques son una realidad

## ¿A qué tipos de ciberataques ha estado expuesto en los últimos 12 meses?*

Las 5 respuestas más comunes




* Se admiten varias respuestas

Las cifras también ponen de relieve el predominio de las tácticas de phishing. En ambos entornos, los ataques aparecieron en forma de mensajes de texto, correos electrónicos o notificaciones push en los que se solicitaba información privada, y en algunos casos esos avisos procedían de organizaciones aparentemente «fiables». Los encuestados confirman que los ataques de phishing siguen siendo una popular y potente forma de ataque que se dirige a las personas donde y cuando menos lo esperan.

La autenticación puede ser un punto fuerte o débil frente a estos ataques. Con la MFA resistente al phishing, no importa si un ataque inicial de phishing tiene éxito y los hackers acceden a las credenciales de inicio de sesión de un usuario. Mientras los atacantes no puedan comprometer también la segunda capa de la MFA, quedarán bloqueados de la cuenta y el ataque fracasará. Sabiendo que la mayoría de las personas se enfrentan con frecuencia a ataques de phishing, y que la mayoría de las empresas siguen utilizando la autenticación de un solo factor, una MFA más fuerte se convierte en obligatoria.

### Spear phishing

Ataques de phishing dirigidos a personas muy concretas, como administradores de sistemas

### Ataque de whaling

Los ataques de phishing dirigidos a empleados de alto nivel ejecutivo

### Vishing

Ataques de phishing por teléfono y mensajes de voz en los que la identidad de la otra persona es difícil de confirmar

### Smishing

Ataques de phishing que tienen lugar a través de texto o chat en los que la confianza está implícita y la información fluye libremente

## Los ataques pueden tener graves consecuencias

La encuesta muestra que cualquier exposición a ciberataques conlleva riesgos preocupantes y una alta probabilidad de daños, potencialmente devastadores. **Menos del 30% de los encuestados no vio consecuencias como resultado de los ataques** (aunque estos datos también incluyen a empleados subalternos que pueden no haber estado al tanto de las consecuencias de un ataque). El 35% de los encuestados experimentó daños en su reputación y, del mismo modo, el 35% sufrió daños en sus beneficios. De forma igualmente alarmante, el 17% perdió empleados a causa de los ciberataques y el 20% tuvo una suspensión de sus operaciones. Todo está en juego en un ciberataque.

# Las consecuencias eclipsan las correcciones

### Ha dicho que ha estado expuesto a un ciberataque en los últimos 12 meses en el trabajo*

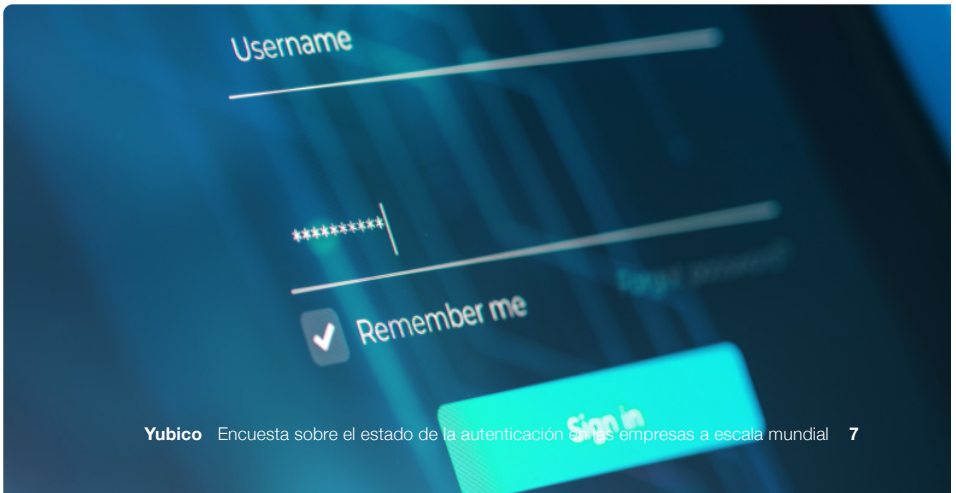
**¿Qué nuevas tecnologías o políticas de seguridad, en su caso, implantó su organización como resultado?**

- 29% Restablecimiento del nombre de usuario y la contraseña
- 28% Protección actualizada de los puntos de enlace
- 24% Formación obligatoria de los empleados en materia de seguridad
- 22% Aplicación TOTP/Push Authenticator
- 21% Acceso restringido a sitios de terceros
- 20% Hardware actualizado/parcheado
- 20% Gestor de contraseñas
- 17% Llaves de seguridad de hardware (por ejemplo, YubiKeys)
- 17% Acceso con tarjeta inteligente
- 15% Tokens de contraseña de un solo uso (OTP)

* Se admiten varias respuestas

Dadas las consecuencias, cabría esperar que las empresas pusieran en marcha mejoras sólidas, pero no siempre parece ser así. La respuesta más habitual, restablecer los nombres de usuario y las contraseñas, no impide que los piratas informáticos vuelvan a robar las credenciales y repitan el mismo ataque, lo que perpetúa el problema. La formación en seguridad, otra respuesta común, hace que la gente sea más consciente, pero no hace nada para impedir realmente que se produzca o tenga éxito la explotación de credenciales. Las aplicaciones de autenticación, en el cuarto puesto, fueron la primera mención de la MFA, y las llaves de seguridad quedaron en último lugar.

El hecho de que la MFA resistente al phishing se utilizara tan poco en respuesta a los ataques a pesar de ser la forma más segura de autenticación es preocupante. Aún más preocupante es que algunas empresas no estén tomando más medidas para actualizar la ciberseguridad y mejorar la autenticación tras los ataques. Los datos de la encuesta revelan una notable disparidad entre el riesgo de ciberataques y la respuesta. La autenticación mejorada aborda directamente esa disparidad y cierra rápidamente las brechas de seguridad que permitieron el ataque original.

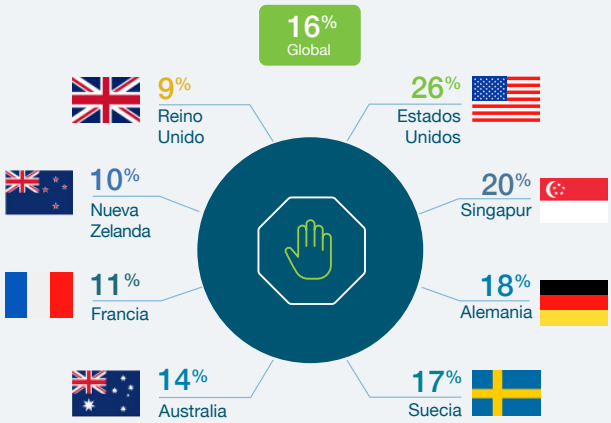


## Una adopción lenta conlleva riesgos

La MFA tiene pocas barreras de entrada y, sin embargo, solo el 12% de las empresas encuestadas ha implantado la MFA en todas las aplicaciones y servicios utilizados. Preguntamos a los encuestados qué les frena a la hora de implantar una autenticación sólida, incluso cuando admiten estar preocupados por los ataques. Ser lento a la hora de adoptar esta tecnología fue la respuesta más numerosa (19%), pero fue seguida de cerca por la percepción de que la MFA era cara (19%), innecesaria (16%), consume mucho tiempo (16%), es complicada de implantar (15%) o de difícil uso (14%).

# La autocomplacencia frena el progreso

### Mi organización no ha adoptado la MFA a través de apps y servicios porque no le preocupa ser víctima de un ataque




A pesar de su reputación como líder mundial en ciberseguridad, más de una cuarta parte de las empresas estadounidenses limita el uso de la MFA porque no cree que esté en riesgo de ciberataque. Esto significa que estas empresas y los datos de sus clientes son vulnerables a los ataques de phishing.

La verdadera protección contra la ciberdelincuencia requiere el uso de la MFA en todas las aplicaciones y servicios, pero esto solo es cierto para el 12% de las organizaciones encuestadas. Las tasas más bajas se registraron en Alemania (6%) y en las empresas de entre 1 y 9 empleados. Las tasas más elevadas fueron en el Reino Unido (16%) y en las empresas de más de 500 empleados. La MFA universal se considera una buena práctica de autenticación y una parte vital de la ciberseguridad. No obstante, para la mayoría empresas, las barreras percibidas parecen superar a los beneficios.

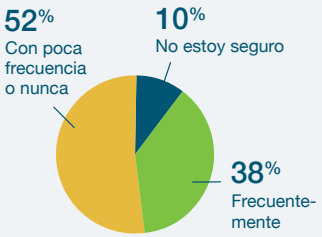
Los datos de la encuesta ya han revelado que las empresas a menudo malinterpretan su protección en relación con los ataques a los que se enfrentan. Algo parecido ocurre aquí, donde la MFA se considera más difícil y menos necesaria de lo que realmente es. Esta actitud arroja luz sobre por qué la MFA resistente al phishing todavía no es la norma y el motivo por el cual los atacantes siguen explotando la autenticación con tanta frecuencia. También apunta a una solución de ciberseguridad sin explotar que no hay razón para evitar.

## Los ciberataques quitan el sueño

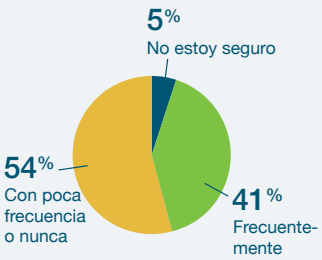
Cuando se les pidió que enumeraran las cinco principales preocupaciones en materia de ciberseguridad que les quitaban el sueño, los encuestados respondieron: ser hackeado en una cuenta privada, ver un dispositivo móvil comprometido, violación de datos, ver los datos de los clientes comprometidos y el hackeo de las cuentas de la organización. **Menos del 30% afirmó que ninguna preocupación en materia de ciberseguridad le quitaba el sueño.** Los profesionales de todos los niveles (especialmente los altos directivos) están preocupados por la ciberseguridad y ven las consecuencias, tanto para ellos como para su empresa. La respuesta institucional, sin embargo, no ha estado a la altura de las ansiedades individuales.

# La seguridad no es prioritaria

**La ciberseguridad se debate en reuniones de los consejos de administración**




**Se exige a los empleados que completen formaciones sobre ciberseguridad**




Los ciberataques y cómo prevenirlos deberían estar en la mente de todas las organizaciones, estén donde estén en el mundo. Los datos de la encuesta, sin embargo, muestran que para la mayoría de las empresas el tema se discute con poca frecuencia o nunca, y revelan grandes disparidades entre los enfoques a escala mundial. Estados Unidos está a la cabeza: La ciberseguridad se discute con frecuencia en las reuniones de los consejos de administración en el 60% de las empresas, frente a la media mundial del 38%, siendo Nueva Zelanda el país más rezagado con un 24%. Del mismo modo, el 62% de los empleados de las empresas estadounidenses están obligados a seguir una formación en ciberseguridad, frente a una media mundial del 42%, con Nueva Zelanda de nuevo a la cola, con un 32%.

Unos empleados informados y vigilantes son esenciales para el éxito de cualquier estrategia de ciberseguridad, pero en la mayoría de las organizaciones no se les está dando la formación o el equipo que necesitan para ser ciberdefensores eficaces. La MFA resistente al phishing garantiza que la autenticación siga siendo segura hasta que (y después de) los esfuerzos educativos se pongan al día.

## Los empleados estadounidenses corren el riesgo de sufrir filtraciones de datos

Puede que Estados Unidos lidere el mundo en lo que respecta a la educación de los empleados en materia de ciberseguridad, pero aún queda mucho camino por recorrer. Los empleados estadounidenses tienen un récord nada envidiable: son los que menos cuidan sus contraseñas. Un increíble 62% de los estadounidenses ha escrito o compartido una contaseña en los últimos 12 meses. Esta cifra se compara desfavorablemente con la media mundial del 54%. Con un 44%, Nueva Zelanda es el país cuyos empleados cuidan más sus contraseñas, a pesar de que se les ofreció menos formación en ciberseguridad.

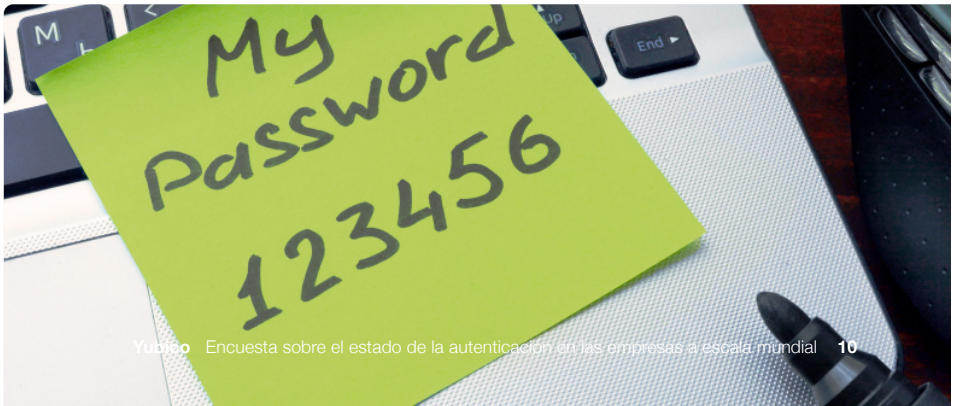
# La ciberhigiene tiene un gran margen de mejora

### ¿Ha hecho lo siguiente al menos una vez durante los últimos 12 meses?


La encuesta planteaba una serie de preguntas para explorar la frecuencia con la que los empleados adoptan comportamientos de riesgo que afectan a la ciberseguridad y ponen en peligro la autenticación. Es inevitable que la personas, especialmente los profesionales deseosos de ser productivos y eficientes, empujarán los límites de la ciberseguridad. La pregunta es: ¿con qué frecuencia y de qué manera?

Resulta tranquilizador el hecho de que un gran porcentaje de los encuestados nunca, o casi nunca, se involucra en prácticas inseguras. Dicho esto, basta un error para desencadenar un ataque. Además, estar dispuesto a saltarse o infringir las normas, aunque solo sea ocasionalmente, sugiere que la gente no sabe lo suficiente sobre ciberseguridad o no se preocupa lo suficiente por ella. De hecho, una de las revelaciones más asombrosas de la encuesta es que el 54% de los empleados admite haber escrito o compartido una contraseña en los últimos 12 meses, lo que revela problemas generalizados, pero probablemente pasados por alto en relación con la seguridad de las cuentas.

En conjunto, las respuestas a esta pregunta ponen de relieve las formas complejas e imprevisibles en que se desarrollan los agujeros en la ciberseguridad. Las libertades ocasionales pueden no ser un problema a nivel individual, pero ampliado a todos los empleados significa que, un enorme número de fallos de seguridad podrían estar ocurriendo y solapándose a la vez. Exigir una MFA resistente al phishing en todas las cuentas evita que estas vulnerabilidades permitan que los ataques exploten y se conviertan en incidentes graves.



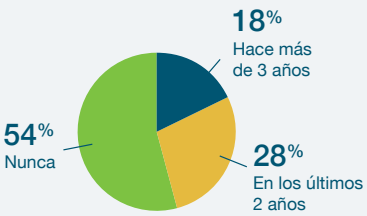
## Cuando la autenticación se convierte en una emergencia

La encuesta muestra que la mayoría de la gente inicia sesión en entre una y cinco cuentas o aplicaciones a diario, y una cuarta parte se conecta a seis o más. No poder autenticarse debido a la pérdida o robo de un dispositivo es más que un inconveniente, es un obstáculo insuperable para lograr cualquier cosa. La autenticación de factor único plantea la mayor responsabilidad, pero una forma errónea de MFA también conlleva responsabilidades.

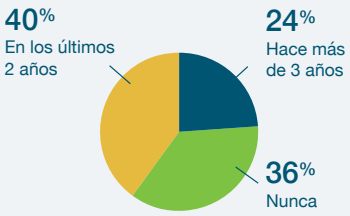
# Lo que más nos importa son nuestras llaves

### ¿Cuándo fue la última vez que perdió o se le rompió el teléfono, o que perdió las llaves de casa o del coche?

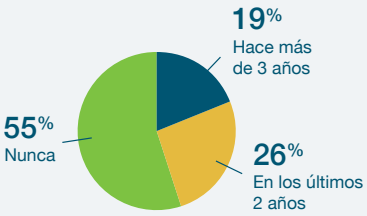
**Pérdida de teléfono**



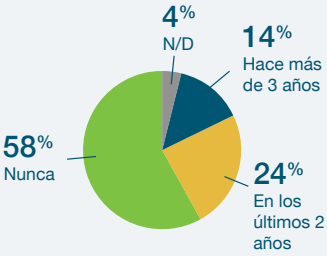

**Rotura del teléfono**




**Pérdida de las llaves de casa**



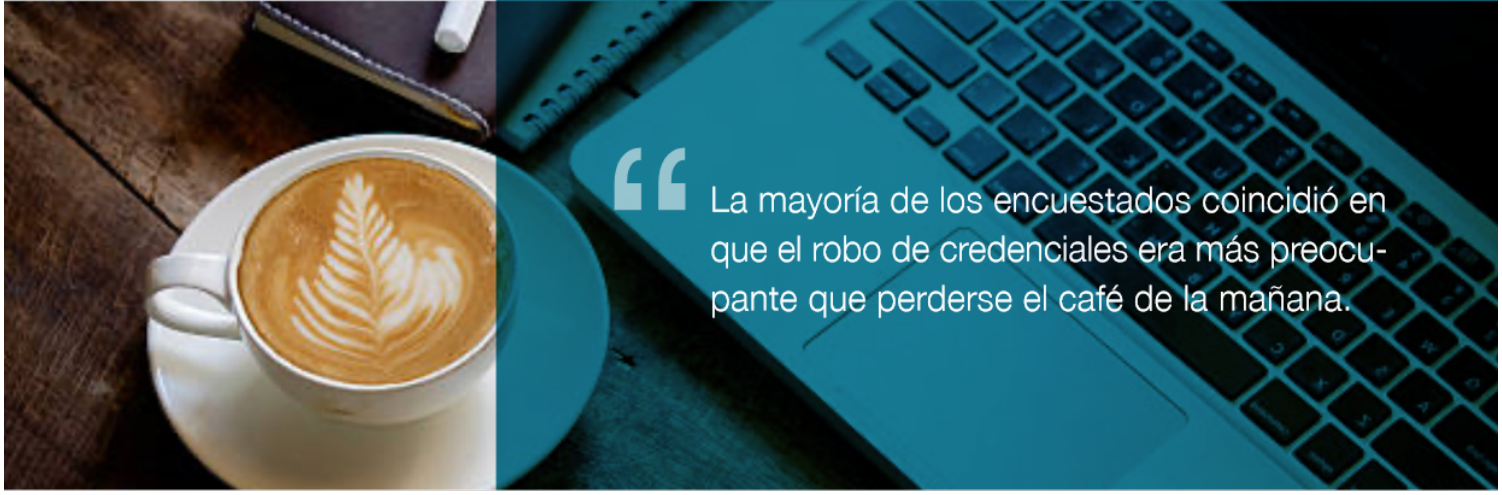

**Rotura de las llaves del coche**




Cuando alguien sale de casa o de la oficina suele llevar consigo dos cosas esenciales: su teléfono y sus llaves. Los datos muestran que casi una cuarta parte de las personas rompió el teléfono solo en el último año y apenas un 36% no lo había roto nunca. Algo más del 50% de los encuestados nunca había perdido el teléfono, pero no es nada raro. La mayoría de las personas nunca había perdido las llaves de su coche o de su casa, ni recientemente ni nunca.

Dado que la autenticación multifactor depende a menudo de que alguien tenga su teléfono o una llave de seguridad para pasar el segundo factor, los índices de pérdida importan. Un teléfono roto podría hacer que el acceso fuera inconveniente (incluso imposible) y un teléfono perdido podría caer en las manos equivocadas. En particular, los directores son los que más teléfonos pierden, poniendo en peligro todo el acceso que depende de ese teléfono.

A medida que las empresas empiezan a explorar la incorporación de la MFA en todas las aplicaciones y servicios, deben comparar los puntos fuertes y débiles de los distintos «segundos» pasos. Los teléfonos, con los que interactuamos constantemente, son siempre vulnerables a lo inesperado. Las llaves, en cambio, viven sobre todo en el interior de bolsillos y bolsas, lo que explica que se pierdan menos con frecuencia. La MFA basada en llaves de seguridad y no en teléfonos se adapta mejor a la forma en que la gente vive realmente.



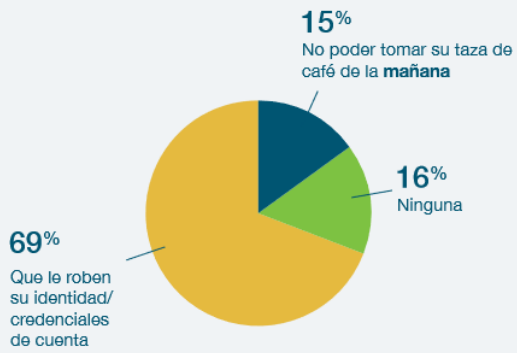
> La mayoría de los encuestados coincidió en que el robo de credenciales era más preocupante que perderse el café de la mañana.

## YubiKeys

YubiKeys, son llaves de seguridad de hardware y ofrecen una MFA resistente al phishing que eleva la autenticación en todos los sentidos. Las llaves de seguridad hacen que la autenticación sea inmune a los intentos de phishing y que las cuentas sean inaccesibles para todo el mundo, excepto para la única persona que tenga la llave correcta. Perder la llave es un riesgo menor y sustituir la llave es más fácil que sustituir un teléfono. Más que una simple llave de seguridad, Yubico ofrece una MFA empresarial solución adecuada para pequeñas y grandes empresas de todos los sectores, y especialmente en aquellos sectores que se enfrentan a amplias normativas de seguridad.

## A la gente le importan sus credenciales

**¿Le preocupa más que le roben sus credenciales de identidad/cuenta o no poder tomar su taza de café de la mañana?**




Por suerte, mucha más gente se preocupa por sus credenciales de identidad/cuenta que por su café de la mañana, lo que encierra una verdad importante: la gente se preocupa por proteger sus cuentas. Ven las amenazas y comprenden los riesgos, por eso sitúan la seguridad de las cuentas muy por encima incluso del café. Como muestran los datos de la encuesta una y otra vez, la gente quiere una autenticación fuerte y multifactorial, pero solo si es sencilla, fluida y segura.

A medida que el riesgo cibernético empeora en todos los sentidos, aumento de los ataques, profundización de los daños, ampliación de los requisitos de cumplimiento, las empresas necesitan tomarse en serio una MFA robusta. Es el área principal, más importante y con mayor impacto en la que centrarse Y, como los datos de la encuesta revelan, es un área que no está a la altura en la mayoría de las organizaciones. Apueste por una MFA resistente al phishing para lograr los mayores avances en ciberseguridad Y elija YubiKeys para obtener un método directo que le permita adoptar una postura de seguridad sólida y conforme a las normas.

La encuesta se realizó entre el 30 de Agosto y el 14 de Septiembre de 2022, en colaboración con Censuswide.

yubico

## Sobre Yubico

Yubico, creador de la YubiKey, permite un inicio de sesión seguro y fácil para todos. Es la empresa líder en el seguro a ordenadores, dispositivos móviles, y más. a nivel global. Yubico es creador y uno de los principales contribuyentes a los estándares de autenticación FIDO2, WebAuth y FIDO Universal 2nd Factor (U2F) y sistemas de autenticación abierta.

Las YubiKeys son el estándar más alto para una autenticación multifactor (MFA) resistente al phishing. Permiten que un solo dispositivo trabaje con cientos de aplicaciones, servicios de consumidores y empresas

Yubico es una empresa privada, presente en todo el mundo.
Para más información, visite: www.yubico.com

**Yubico AB**
Kungsgatan 44
2.a planta
SE-111 35 Estocolmo
Suecia

**Yubico Inc.**
5201 Great America Pkwy
Suite 122
Santa Clara, CA 95054
USA