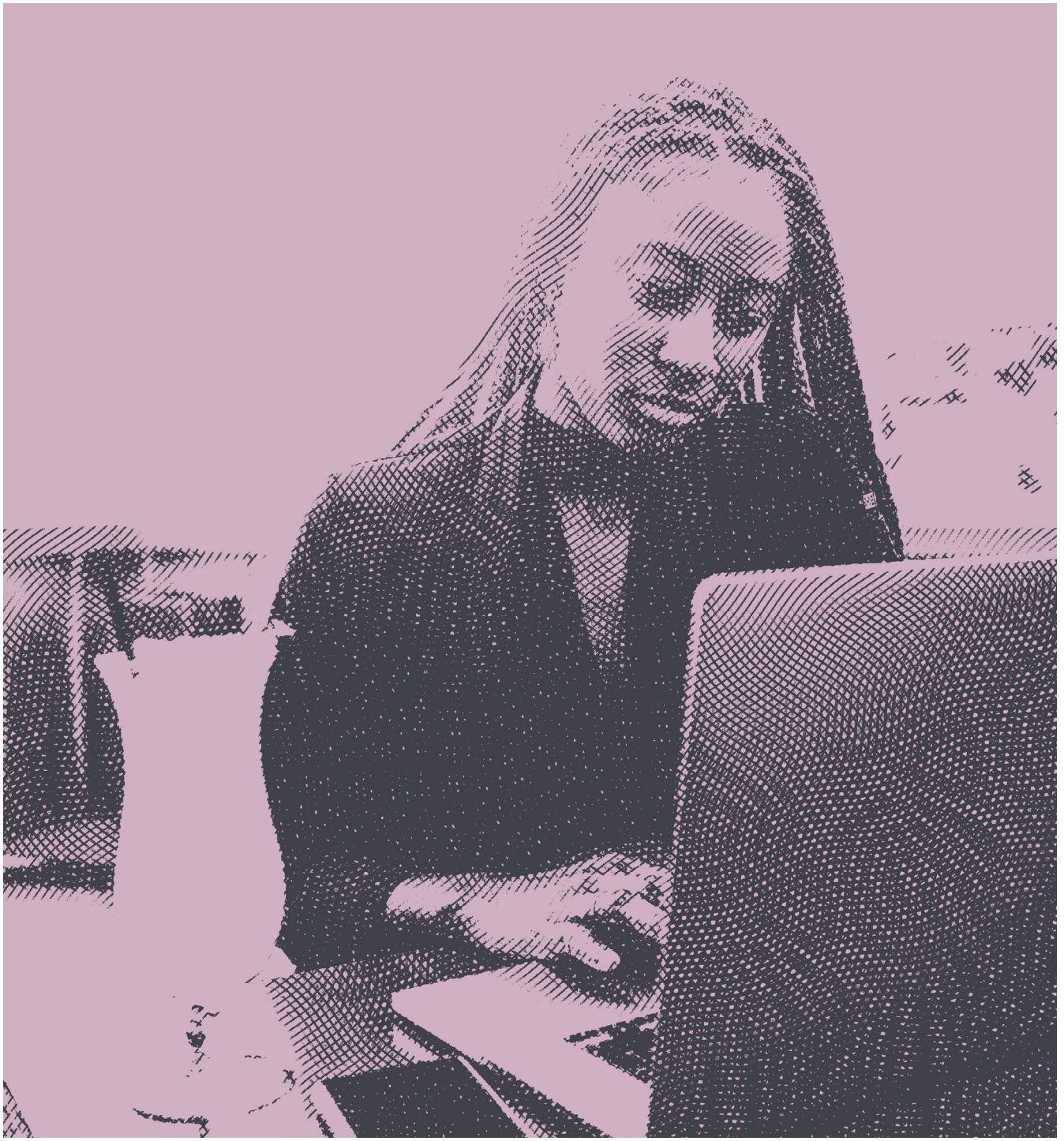
Índice de Confianza Digital de Okta

Explorando el lado humano de la confianza en un mundo en constante cambio



okta

Contenido

> La confianza es una relación de complicidad con lo desconocido.
>
> Rachel Botsman, de la Escuela de Negocios Saïd de la Universidad de Oxford

Introducción: la confianza comienza con la seguridad

Los hechos ocurridos en el año 2020 pusieron la noción de confianza en el primer plano de nuestras vidas. Casi de la noche a la mañana, la confianza en gobiernos e instituciones se convirtió en un asunto de importancia para la gran mayoría. La confianza de los clientes en las marcas se volvió muy importante para conseguir resultados en medio de una severa recesión económica. Muchas organizaciones se han visto obligadas a superar antiguas reservas, confiar en que sus empleados trabajen desde casa (WFH) y confiar en los canales digitales como única forma de servir a sus clientes.

Todo esto sucede en medio de un escenario de creciente preocupación por la seguridad, provocada por un volumen de filtraciones de datos nunca visto y por la actividad de las ciberamenazas, una aplicación estricta de una legislación de protección de datos, fraudes oportunistas mediante la ingeniería social y un creciente nivel de exigencia de privacidad entre los consumidores. Según una estimación de la INTERPOL, el fraude por phishing ha aumentado un 59% a raíz de la pandemia, junto con el crecimiento de malware, ransomware, dominios maliciosos y noticias falsas, una señal de que los delincuentes buscan explotar el miedo y la incertidumbre causados por la inestabilidad social y económica.

Para las empresas, la seguridad empieza con la confianza. Es decir, para impulsar una seguridad eficaz, primero debe concebirse como una organización en la que los empleados, socios y clientes fuera del perímetro tradicional, centrado en la oficina, pueden confiar para acceder a datos y sistemas sensibles. Sin embargo, lo contrario es igualmente cierto: la confianza comienza con la seguridad. En otras palabras, la mejor manera de impulsar la confianza entre esas partes interesadas principales es ofrecer herramientas y políticas de seguridad eficaces, especialmente aquellas que se centran en gestionar perfectamente las identidades de los usuarios.

Este es el camino más rápido para mejorar la productividad y fomentar la lealtad y el compromiso, no sólo entre los empleados y los socios, sino también entre los clientes.

Para profundizar en el tema, Okta realizó esta nueva encuesta entre más de 13.000 empleados de oficina, incluyendo más de 1000 en España, para ayudar a responder las siguientes preguntas:

¿Qué parte de nuestra confianza se construye, mantiene y quiebra en el mundo digital?

Fuera de las interacciones humanas, ¿en qué grado confiamos cuando sólo interactuamos a través de nuestras pantallas?

¿Están las marcas, las empresas y los gobiernos haciendo lo suficiente para generar confianza?

¿Qué factores externos están cambiando nuestra disposición a confiar a través de los canales digitales?

Metodología:

Todas las cifras, a menos que se indique lo contrario, proceden de YouGov Plc. El tamaño total de la muestra fue de 13.163 trabajadores de oficinas de España, Reino Unido, EE.UU., Australia, Alemania, Francia, Italia, Suecia, Países Bajos y Japón. Esto incluye 1013 encuestados procedentes del España. El trabajo de campo se realizó entre el 26 de noviembre y el 10 de diciembre de 2020. La encuesta se realizó por Internet.

A continuación, le presentamos el Índice de Confianza Digital de Okta: nuestro estudio que explora el lado humano de la confianza digital en un mundo cada vez más condicionado por los efectos de la pandemia. Concluimos con recomendaciones para personas, empresas y organizaciones públicas sobre cómo pueden construir y ofrecer una confianza humana real.

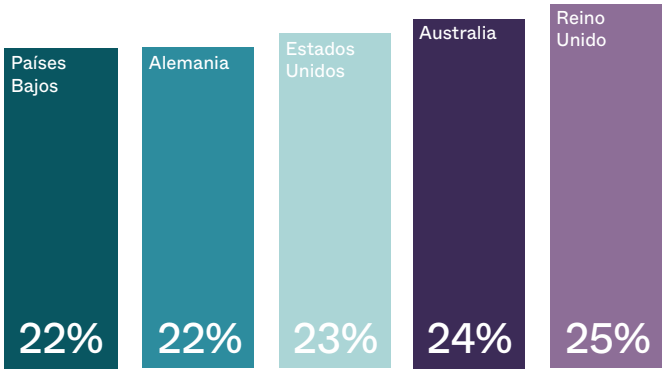
> La confianza llega a pie, pero se va en un Ferrari.
>
> Mark Carney, gobernador del Banco de Canadá

Sección 1

¿Qué hace que los consumidores confíen en las marcas?

En 2020, con su inevitable giro hacia el trabajo a distancia, los trabajadores de oficinas se han convertido en unos usuarios expertos en tecnología digital, dedicando mucho más tiempo y comprando mucho más por internet. Solo en el Reino Unido, **se prevé** que los consumidores gastarán más de 141.000 millones de libras esterlinas este año solo en compras por Internet, lo que supone un crecimiento de casi el 35% con respecto a 2019, y en España, **siete de cada diez internautas** ya compra online. Como 2021 es un año de transición hacia prácticas online más consolidadas, las marcas se enfrentan al reto de crear nuevos modelos de confianza y lealtad con sus partes interesadas.

La confianza se gana con dificultad, pero se pierde fácilmente, y aunque los valores éticos son cada vez más apreciados por los accionistas, los inversores y los consejos de administración, nos dimos cuenta de que cuando se trata de los clientes, es más importante acertar con lo esencial. Alrededor del 39% de los encuestados del Reino Unido y del resto del mundo dijeron que la fiabilidad del servicio era el criterio que más les hacía confiar en una marca digital, como garantizar que los artículos llegaran a tiempo y en buenas condiciones. La seguridad también era clave para ellos: una cuarta parte (25%) dijo que tener opciones de acceso seguro como la autenticación multifactorial (MFA) y otras medidas ayudaría a fomentar la confianza en la marca. Esta necesidad de seguridad fue aún más evidente para los encuestados en Australia (24%), los EE.UU. (23%), Alemania (22%) y Países Bajos (22%), mientras que España la percepción es menor (17%) [Q1]



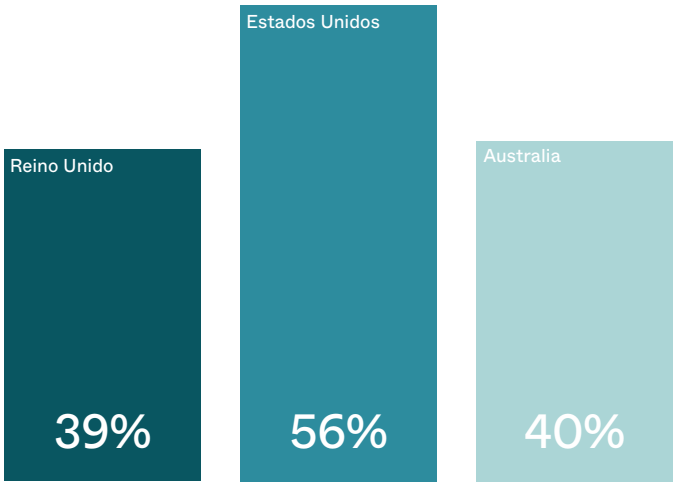
Porcentaje de encuestados que cree que tener opciones de inicio de sesión seguras, como la autenticación multifactorial (MFA), ayudaría a fomentar la confianza en la marca.

Las brechas de seguridad importan

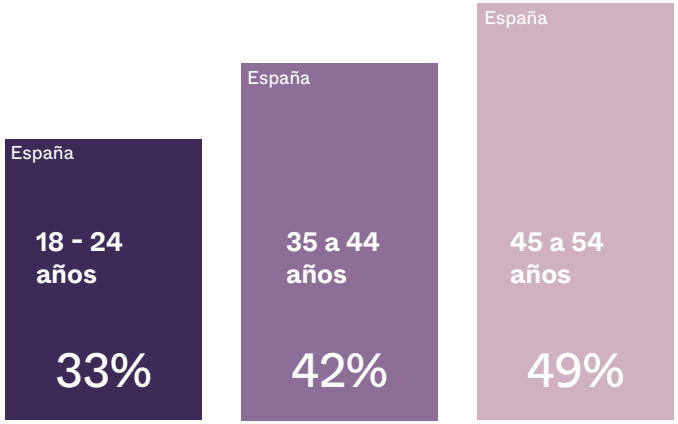
Eso no quiere decir que la ética no tenga ninguna importancia: el 11% de los encuestados españoles señalaron que es el factor más importante para impulsar la confianza. También juegan un papel importante para los consumidores al decidir con qué marcas no hacer negocios, específicamente en términos de "ética de los datos". Los dos principales factores que, según los encuestados, les hacen más susceptibles de desconfiar de una marca son el uso indebido o la venta intencionada de datos personales (47% mundial y tan solo 28% en España) y la filtración de datos (14% en España frente al 17% mundial). [Q2]

Ambas no son tan solo una cuestión de ética para las empresas digitales, sino también prácticas que podrían atraer la ira de los responsables de la protección de datos. Para escapar del enfado de los clientes y de las posibles consecuencias para la reputación y las finanzas, las organizaciones deben garantizar que la seguridad de sus datos es adecuada para su finalidad, empezando por una gestión de la identidad según las mejores prácticas.

El uso indebido o la venta deliberada de datos se consideró igualmente el principal motivo de desconfianza hacia una marca por parte de todos los mercados. Pero mientras que las irregularidades en los datos fueron la segunda mayor preocupación de los encuestados en países como Australia (16%), los Estados Unidos (15%) y Países Bajos (13%), los errores o las molestias fueron un factor decisivo en la ruptura de la confianza de los encuestados en Francia (23%), España (21%) y Suecia (16%). Esto es otro claro aviso de que, si bien la ética de los datos sigue siendo de suma importancia, no hay que dejar de lado el servicio al cliente.



Porcentaje de encuestados que han perdido la confianza en una empresa debido a a una violación de datos o similar.



Porcentaje de encuestados que dejaron de utilizar permanentemente los servicios de una empresa tras una infracción.

Cuando la confianza desaparece

Está comprobado que la confianza es vital para que las marcas digitales tengan éxito en el competitivo panorama empresarial actual. El 74% de los encuestados españoles dijeron que sería improbable que compraran a una compañía en la que no confiaran, [Q3] y el 46% admitió que tendría serias reservas sobre comprar en un sitio web del que nunca había oído hablar antes. [Q4]

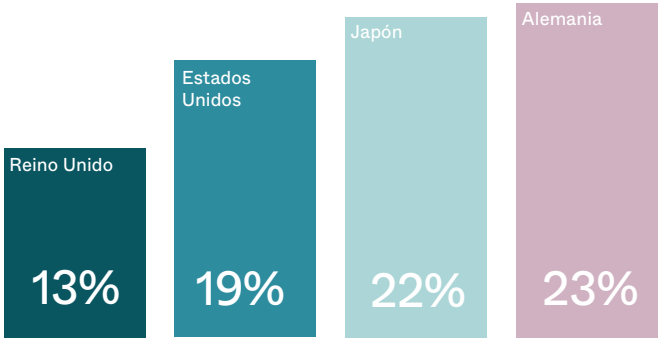
Una vez que se han granjeado esa confianza, las marcas no deben tener dudas de que deben trabajar duro para conservarla, y que una ciberseguridad eficaz es la clave para lograrlo. Casi dos quintas partes (41%) de los encuestados en España dijeron que habían perdido la fe en una empresa debido a una filtración de datos o similar, siendo esta cifra aún más alta en los EE.UU. (56%). Después de esto, el 41% de los usuarios españoles dejaron de hacer uso en forma permanente de los servicios de la compañía, el mismo porcentaje (41%) eliminaron su cuenta y otro 41% cambiaron sus configuraciones, tales como contraseñas y direcciones de correo electrónico, lo que pone de relieve la importancia de un acceso seguro para mantener la confianza en todo momento.

Es interesante observar que los encuestados españoles más jóvenes tienen una mayor tolerancia a una mala gestión de datos y seguridad de las marcas con las que trabajan. Alrededor del 33% de los jóvenes de 18 a 24 años dijeron que habían dejado de usar los servicios de una empresa de forma permanente después de una filtración, frente al 42% de los adultos de 35 a 44 años o el 49% del grupo de edad entre 45 y 54. Teniendo en cuenta que las generaciones más jóvenes se convertirán en el motor de crecimiento de la economía del futuro, las marcas deben asegurarse de que sus empleados estén alineados con estas expectativas de ciberseguridad.

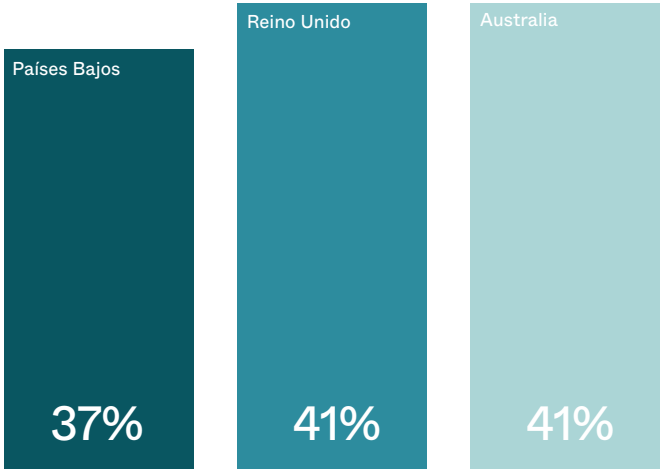
> Las nuevas generaciones se convertirán en los responsables de la toma de decisiones del futuro, así que es importante prepararse y garantizar un buen servicio, y la ciberseguridad está en el corazón de las operaciones para alinear las necesidades de los clientes con las prioridades de las empresas.
>
> Jesper Frederiksen, VP & GM EMEA, Okta

Mucho trabajo por delante

Todavía hay mucho trabajo por hacer. Una considerable minoría del 14% de los encuestados de España dijo que no confiaba en ningún canal digital para manejar sus datos de forma segura, menos que en a Alemania (23%), Japón (22%) y los EE.UU. (19%) pero similar a Reino Unido (13%). Y quedó claro que los españoles confían igual en las aplicaciones de comunicación en el lugar de trabajo (10%) como en las personales (10%). Los más confiables de todos los canales digitales en España fueron los sitios web del gobierno (26%), frente a británicos (41%), australianos (41%) y neerlandeses (37%). [Q5] Esto es sin duda algo positivo. A pesar de las preocupaciones iniciales sobre el tratamiento de los datos personales y de la COVID-19 de los ciudadanos, no ha habido ninguna brecha importante hasta la fecha, y el control permanente parece estar impulsando la mejora de los estándares de seguridad de los datos.



Porcentaje de encuestados que no confían en ningún canal digital para el tratamiento seguro de sus datos.



Porcentaje de los encuestados que creen que los sitios web gubernamentales son los más fiables.

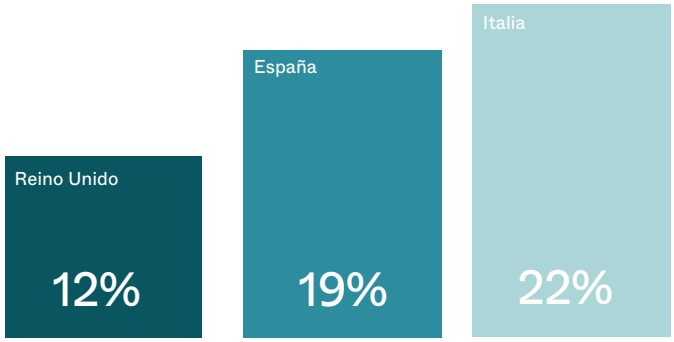
> Es una gran noticia que la gente, por encima de cualquier otro canal digital, confíe en los sitios web de los gobiernos a la hora de gestionar sus datos. Es importante que las administraciones públicas sigan priorizando las medidas de ciberseguridad y que mantengan seguros los datos de los ciudadanos.
>
> Jesper Frederiksen, VP & GM EMEA, Okta

Sección 2

Cómo ha cambiado la pandemia el comportamiento de los usuarios

Casi la tercera parte (31%) de los encuestados españoles dijeron que “siempre” o “a menudo” trabajan actualmente desde su domicilio, y estos mismos empleados exigirán más flexibilidad en las políticas de teletrabajo una vez que la crisis haya remitido. Sin embargo, mientras que se encuentran aislados en casa, muchos han estado expuestos a un aumento de las ciberamenazas dirigidas a robar tanto sus credenciales de acceso corporativo como sus datos de identidad personal. El phishing se ha convertido en 2020 en la táctica preferida de muchos ciberdelincuentes. Han cosechado un gran éxito utilizando el señuelo de la información sobre las vacunas COVID-19, o las frecuentes (pero falsas) novedades de instituciones de confianza como la OMS, para engañar a los destinatarios y conseguir que hagan clic en ellas. Solo en abril, **Google informó** que había bloqueado 18 millones de correos electrónicos diarios de malware y phishing relacionados con la COVID-19.

Como consecuencia, quizás no sea sorprendente que el 36% de los encuestados españoles dijeran que se han vuelto más prudentes a la hora de proporcionar información personal de ellos mismos en Internet. A pesar de todas las amenazas, un 27% afirma que ahora son algo o mucho menos desconfiados a la hora de hacerlo. El teletrabajo también ha hecho que los encuestados sean más cuidadosos con los correos electrónicos de phishing (35%), las violaciones de datos (33%) e incluso las “deepfakes” generadas por la IA que se usan para difundir información falsa (31%). [Q8]



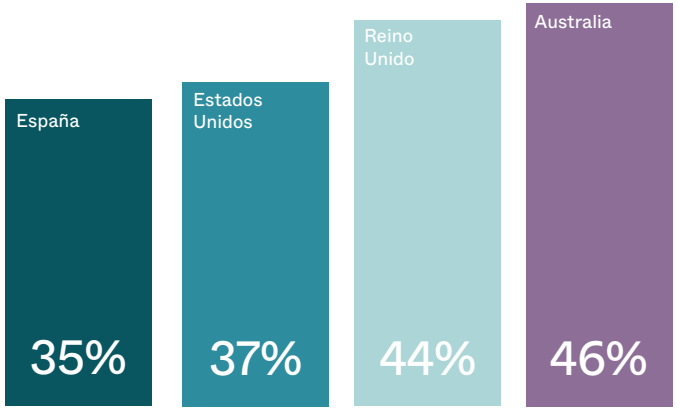
Porcentaje de encuestados que creen que el robo de contraseñas es una preocupación.

Los encuestados creen que corren mayor probabilidad de sufrir un robo de identidad (15%), lo que es comprensible dado el aumento de los ataques de phishing a los que muchos se han visto sometidos. Mientras que el robo de contraseñas representaba una cierta preocupación para el 12% de los encuestados del Reino Unido, en Italia (22%) y España (19%) se sentían considerablemente más expuestos a este problema, lo que demuestra que el camino hacia la autenticación sin contraseñas se convertirá en algo necesario. El malware (19%) y las filtraciones de datos (13%) completan las principales preocupaciones. Cabe recordar que un individuo puede estar expuesto a ciberamenazas no sólo a través de ataques dirigidos a sí mismo y a sus dispositivos, sino también a sus convivientes, que pueden tener comportamientos peligrosos online.

> “El perfil de peligro, cuando se trabaja desde casa, se intensifica por múltiples razones adicionales. Las personas se han encontrado compartiendo dispositivos y redes domésticas, así como espacios físicos, lo que incrementa el riesgo y compromete el material escrito y la confidencialidad de las llamadas de audio. Los ‘compañeros de trabajo’ de hoy pueden ser desde familiares de confianza hasta compañeros de piso prácticamente desconocidos, mientras que se elimina la tranquilidad de tener a mano colegas y un servicio de asistencia informática. Además, la conducta y la cultura de seguridad que los trabajadores adoptaron previamente, puede verse comprometida inconscientemente al hacer malabarismos con la conciliación laboral y doméstica.
>
> Ben King, CSO EMEA, Okta

Es hora de que una mayor transparencia

La principal explicación dada por los encuestados españoles para su mayor cautela en Internet durante la pandemia, fue la cobertura de los medios de comunicación sobre las amenazas online (35%), la misma que los de Australia (46%), los EE.UU. (37%) y Reino Unido (44%). Si bien es positivo ver a los periodistas cumpliendo un importante papel en la educación del público, existe una clara oportunidad para que las marcas digitales mejoren la concienciación sobre estos temas entre sus clientes, creando así confianza. Al combinar estos esfuerzos con herramientas como el MFA, pueden proporcionar una mayor seguridad a unos consumidores que se sienten intranquilos, impulsando los ingresos y la diferenciación competitiva.



Porcentaje de encuestados que creen que la cobertura de los medios de comunicación sobre las amenazas aumentó su precaución en Internet durante la pandemia.

Del mismo modo, las empresas tienen un papel que desempeñar aquí. Al mejorar la concienciación, actualizar la tecnología heredada que pueda ser vulnerable a las amenazas en línea, y demostrar la eficacia de las medidas de seguridad como el antimalware de los terminales, pueden proporcionar a los trabajadores la confianza de encontrarse igualmente bien protegidos en casa como en la oficina. Esto beneficia indirectamente a las marcas digitales de terceros, pero también a su propia organización: el aumento de la confianza en las herramientas que los empleados utilizan para el teletrabajo contribuirá en última instancia a mejorar la productividad.

Sección 3

¿Cómo están respondiendo las organizaciones?

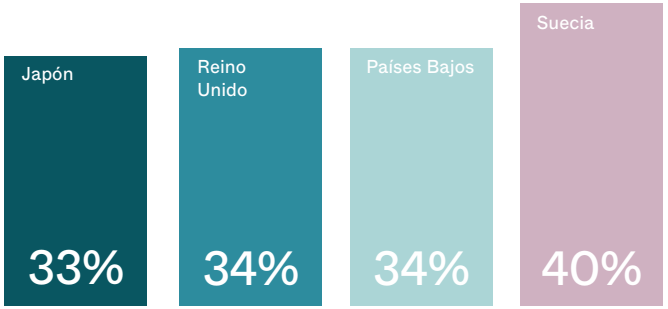
Muchos empresarios han tomado medidas para hacer frente al aumento de las ciberamenazas que se ciernen sobre sus trabajadores en remoto. Nuevas aplicaciones y tecnologías de seguridad, como el MFA (36%), fue la medida más utilizada, seguida de una mejor formación del personal (30%). Ambas son fundamentales para ayudar a estimular la confianza de los empleados en la que se sustenta el éxito de las empresas.

Sin embargo, más preocupante es el hecho de que el 20% de los encuestados afirmaron que su empleador no había hecho nada hasta ahora para combatir un aumento de las amenazas en línea relacionadas con la pandemia. Este porcentaje fue aún mayor en los sectores inmobiliario (42%), educativo (31%) de medios de comunicación y marketing (25%) y de ocio y entretenimiento (27%).

> “En el caso de aquellas empresas que no son nativas digitales, los empleados suelen trabajar desde una posición tecnológicamente menos avanzada, lo que impide percatarse ni plantearse la introducción de controles para combatir las amenazas en línea. Aquellas que tradicionalmente se han enfrentado a unos niveles más elevados de ciberamenazas, como la banca, tecnología y comercio minorista, es probable que también hayan dispuesto de un presupuesto de seguridad proporcionalmente mayor al de otras industrias consultadas. En todos estos sectores, los CIO y los CSO se han visto obligados a dividir su tiempo entre atender las necesidades específicas de su industria y hacer frente a las exigencias de seguridad, a menudo dos tareas muy diferentes.
>
> Ben King, CSO EMEA, Okta

Además, más de un tercio (34%) de los trabajadores de oficina manifestaron que no sabían si su empresa había tomado medidas de seguridad proactivas, y lo mismo ocurrió en Suecia (40%), Países Bajos (34%) y Japón (33%). [Q10]

Esto es particularmente desconcertante ya que apunta a una falta de transparencia entre los responsables de las empresas y de las áreas de TI y sus empleados. Podrían estar utilizando los mejores sistemas de ciberseguridad del mundo, pero si los trabajadores no lo saben, su empresa no podrá fomentar una mayor confianza con su personal.



Porcentaje de encuestados que no sabía si su empresa había tomado medidas de seguridad proactivas.

> Los ciberdelincuentes siempre están estudiando nuevas fórmulas, y los trabajadores son conscientes de ello, por ello muchos se muestran temerosos ante la suplantación de identidad, las filtraciones de datos y los nuevos riesgos, como el deepfake. Las empresas deben, por lo tanto, asegurarse de mantenerse por delante en la medida de lo posible y combatir estas nuevas amenazas con nuevos enfoques.
>
> Ben King, CSO EMEA, Okta

Está claro que, si aún no lo han hecho, los responsables de TI deben empezar en 2021 a desplegar soluciones de gestión de identidades para impulsar la seguridad basada en la confianza, con el fin de mejorar la productividad del personal y reducir al mínimo los peligros potenciales. Además, deben ser más transparentes en cuanto a las nuevas tecnologías y las políticas de seguridad para las que están diseñadas.

Sección 4

Conclusión y recomendaciones

IDC **define** la confianza como la condición que "permite que se tomen decisiones entre dos o más entidades, reflejando el nivel de confiabilidad entre ellas" y es una "ampliación de la conversación sobre seguridad para incluir atributos como el riesgo, el cumplimiento, la privacidad e incluso la ética comercial". Es un concepto que ningún responsable tecnológico o empresarial puede ignorar actualmente, ya que la transformación digital amplía la superficie de los ciberataques y, simultáneamente, abre nuevos canales para relacionarse con los clientes y apoyar a los empleados. Cuando se hace bien, la confianza no sólo mitigará el daño, sino que impulsará los ingresos y el valor para las organizaciones.

En la empresa se parte de un enfoque Zero Trust centrado en la identidad, y el objetivo final de políticas de acceso basadas en el riesgo, la autenticación continua y adaptativa y el acceso libre de obstáculos. La pandemia ha acelerado la necesidad de este tipo de enfoques para que las organizaciones puedan confiar en que sus usuarios remotos son quienes dicen ser, ya que los impostores tratan de infiltrarse cada vez más en las redes corporativas. También es necesario fomentar la confianza entre los empleados para que puedan trabajar de forma más productiva.

Pero el concepto de confianza también se extiende a las interacciones con los clientes. Las modernas empresas digitales necesitan alimentar constantemente esa confianza como administradores responsables de los datos de sus clientes. Hacerlo así impulsará la lealtad y el éxito, incluso cuando los ladrones de datos e identidades intensificaron sus esfuerzos durante la pandemia. También en este contexto, la confianza comienza con la seguridad, con la identidad como eje central. Esto implica que las marcas digitales ofrezcan a sus clientes las herramientas que necesitan para autenticarse de forma fluida y segura.

Este es un resumen de nuestras principales recomendaciones:

Los líderes empresariales y de TI deben ser transparentes con los empleados que trabajan remotamente, sobre las medidas y políticas de ciberseguridad que están implementando para fomentar la confianza y el compromiso de su personal.

Las nuevas herramientas de seguridad como el MFA y la biometría para la autenticación sin contraseñas, son fundamentales para protegerse contra el robo de identidad de los consumidores y asegurar el acceso remoto de los trabajadores.

Se necesita más formación interna sobre la protección contra el phishing y sobre las mejores prácticas de seguridad para mitigar los riesgos del teletrabajo.

Mantenga al día su plan de seguridad para asegurarse de que tiene en cuenta el escenario cambiante de las amenazas y el marco normativo sobre riesgos.

Demuestre a los trabajadores en remoto, la eficacia de las medidas de seguridad para darles la tranquilidad de que están protegidos tanto en sus hogares como en la oficina.

Los gobiernos y los servicios digitales deben seguir dando prioridad a las medidas de ciberseguridad y privacidad para mantener seguros los datos de los ciudadanos durante la pandemia y en la nueva normalidad.

La ética de los datos es importante para los clientes, por lo que las empresas deben asegurarse de que cumplen las disposiciones legales, evitando el uso indebido y reduciendo el riesgo de infracciones, así como satisfaciendo las expectativas de los consumidores.

Asegúrese de que su organización cumpla con las expectativas de seguridad y privacidad de los consumidores más jóvenes, para fomentar la lealtad entre un grupo económicamente relevante.

Sección 5

Proteger la empresa del futuro con Okta

La identidad es la base para construir organizaciones seguras y basadas en la confianza. Con Okta Identity Cloud, los líderes empresariales de todo el mundo pueden crear con confianza las mejores experiencias digitales para sus empleados y clientes.

Proteja a sus empleados, dondequiera que se encuentren, con las **soluciones de identidad de la fuerza de trabajo de Okta**. Consiga las herramientas para asegurar y automatizar su migración a la nube, con compatibilidad total para entornos híbridos a lo largo del proceso.

Utilice las **soluciones de identidad de clientes** de Okta para construir experiencias de cliente seguras y sin interrupciones que encantarán a sus desarrolladores y usuarios.

Sobre Okta

Okta es el principal proveedor independiente de identidad para la empresa. Okta Identity Cloud permite a las organizaciones conectar de forma segura a las personas adecuadas con las tecnologías adecuadas en el momento adecuado. Con más de 6.500 integraciones preparadas con aplicaciones y proveedores de infraestructura, los clientes de Okta pueden utilizar fácilmente y con seguridad, las mejores tecnologías para su negocio. Más de 9400 organizaciones, incluyendo Engie, JetBlue, Nordstrom, Takeda Pharmaceutical, Teach for America, T-Mobile y Twilio, confían en Okta para ayudar a proteger las identidades de sus empleados y clientes.

Okta.com