La brecha de confianza cibernética: por qué la familiaridad no es suficiente en la era de la IA

Índice de confianza cibernética de WatchGuard

Cómo los empleados evalúan, en qué confían y cómo verifican las señales digitales en la era de la IA.



ENCUESTADOS

Más de 500 empleados a tiempo completo

PAÍSES

Estados Unidos, Reino Unido, Francia, Alemania, Italia, Portugal, España y Australia

INDUSTRIAS

Atención médica, servicios financieros, seguros, servicios jurídicos, comercio minorista, hospitalidad, gobierno, educación y otros.



Índice

01 Introducción

02 Principales hallazgos

03 El índice de confianza cibernética: mayor confianza, verificación desigual

04 La verificación no es un hábito constante

05 La familiaridad tiene un peso considerable

06 El riesgo de suplantación de los directivos

07 La confianza en la era de los deepfakes

08 Los empleados detectan deficiencias en sus organizaciones y los empleadores deben actuar

09 La IA agrega complejidad a la seguridad organizacional

10 La confianza cibernética y los hábitos de verificación por industria

11 La confianza cibernética y los hábitos de verificación por país

12 La perspectiva de WatchGuard: cómo pueden las organizaciones cerrar la brecha de confianza cibernética

13 La visión de WatchGuard: cómo pueden ayudar los MSP

01. Introducción

Los empleados confían en personas conocidas, identidades reconocibles y canales de comunicación establecidos para decidir en quién y en qué confiar. Sin embargo, la verificación independiente sigue siendo irregular, incluso cuando una solicitud implica dinero, credenciales o información confidencial. La brecha de confianza cibernética surge cuando la confianza en quien aparentemente se comunica prevalece sobre el proceso utilizado para confirmar su identidad. Las voces y los videos generados por IA, así como otras formas de suplantación, hacen que esta distinción tenga consecuencias cada vez más importantes.

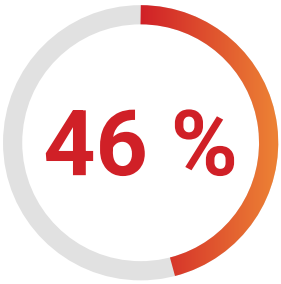
Una encuesta global realizada a más de 500 empleados a tiempo completo de Estados Unidos, Reino Unido, Francia, Alemania, Italia, Portugal, España y Australia revela esta contradicción: el 46 % afirma que confía más en las comunicaciones digitales que hace cinco años, mientras que el 55 % no siempre verifica de manera independiente las solicitudes confidenciales. Los resultados señalan la necesidad de adaptar las prácticas de verificación a las formas en que los empleados se comunican y utilizan la IA. Los empleadores pueden abordar esta brecha mediante formación práctica, procedimientos de verificación claros, políticas responsables de concientización sobre seguridad y de uso aceptable, y controles de seguridad por capas. El objetivo es que la confianza esté mejor fundamentada y que la verificación se convierta en una práctica habitual.

La brecha de confianza cibernética surge cuando la confianza en quien aparentemente se comunica prevalece sobre el proceso utilizado para confirmar su identidad.



El objetivo es que la confianza esté mejor fundamentada y que la verificación se convierta en una práctica habitual.

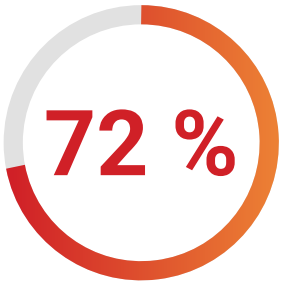
02. Principales hallazgos



confía más en las comunicaciones digitales que hace cinco años.



no siempre verifica de manera independiente las solicitudes confidenciales.



hizo clic en un vínculo o abrió un archivo adjunto porque parecía provenir de alguien que conocía.

1 **La confianza aumenta, mientras que la verificación sigue siendo irregular:** el 46 % confía más en las comunicaciones digitales que hace cinco años, frente al 31 % que confía menos; el 55 % no siempre verifica de manera independiente las solicitudes confidenciales.

2 **La familiaridad influye en las decisiones:** el 72 % hizo clic en un vínculo o abrió un archivo adjunto porque parecía provenir de alguien que conocía.

3 **La identidad de los directivos puede hacer que las solicitudes confidenciales resulten convincentes:** el 42 % probablemente confiaría en un mensaje de texto urgente del director ejecutivo que solicitara un pago o datos confidenciales sin verificarlo; el 40 % afirma lo mismo sobre un mensaje de voz.

4 **Las señales visuales y auditivas siguen teniendo influencia:** el 53 % se basa en el rostro, la voz o el nombre para mostrar de una persona para verificar una solicitud inusual o confidencial por video, frente al 28 % que da prioridad a otro canal o procedimiento organizacional.

5 **Los empleados detectan deficiencias en la preparación de sus organizaciones:** solo el 21 % considera que su organización está completamente preparada para un ciberataque importante; el 38 % identifica la capacitación insuficiente o la falta de concientización de los empleados como el principal obstáculo para estar preparados.

03. El índice de confianza cibernética: mayor confianza, verificación desigual

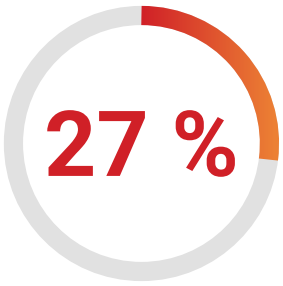
El índice de confianza cibernética evalúa la confianza de los empleados en las comunicaciones digitales junto con sus hábitos de verificación. Los resultados muestran que el 46 % de los empleados afirma que confía más en las comunicaciones digitales que hace cinco años, frente al 31 % que confía menos, lo que genera un saldo neto de confianza de +15 puntos porcentuales. Este saldo describe los cambios declarados en los niveles de confianza y no constituye una puntuación compuesta de seguridad. Al analizarlo junto con una verificación inconsistente, establece la principal preocupación del informe: el aumento de la confianza en las comunicaciones digitales debe estar respaldado por verificaciones confiables.

Indicador del índice	Hallazgo	Qué mide
Aumento de la confianza en los últimos cinco años	**46 %**	Dirección del cambio declarado
Disminución de la confianza en los últimos cinco años	**31 %**	Dirección del cambio declarado
Saldo neto de confianza	**+15 puntos porcentuales**	Confianza en aumento menos confianza en disminución
Solicitudes confidenciales que no siempre se verifican	**55 %**	Regularidad de las prácticas de verificación declaradas
Información generada por IA que siempre se verifica	**32 %**	Hábito declarado de verificar la información

04.La verificación no es un hábito constante



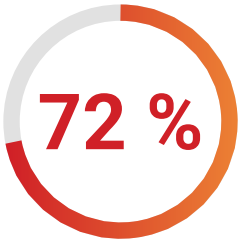
no siempre verifica de manera independiente quién envía una solicitud antes de actuar cuando esta implica dinero, credenciales, información confidencial o acceso a cuentas.



verifica solo algunas veces, rara vez o nunca.

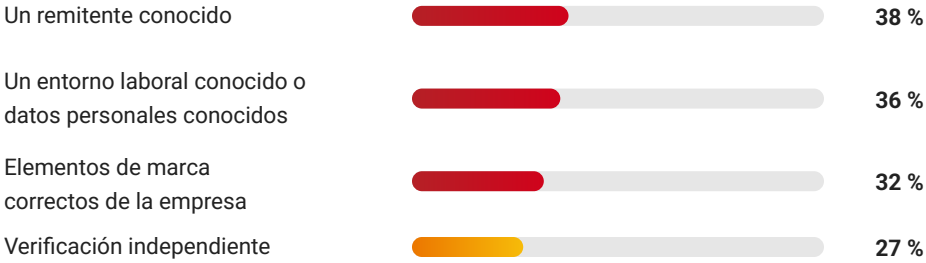
Más de la mitad de los encuestados (55 %) afirmó que no siempre verifica de manera independiente quién envía una solicitud antes de actuar cuando esta implica dinero, credenciales, información confidencial o acceso a cuentas. Del total de encuestados, el 27 % verifica solo algunas veces, rara vez o nunca. Esta distinción es importante, ya que verificar de manera irregular no es lo mismo que no verificar nunca. Sin embargo, un proceso que depende del criterio individual puede dejar margen para excepciones en momentos de consecuencias importantes.

05. La familiaridad tiene un peso considerable



hizo clic en un vínculo o abrió un archivo adjunto porque parecía provenir de alguien que conocía.

Qué hace que una solicitud digital parezca confiable

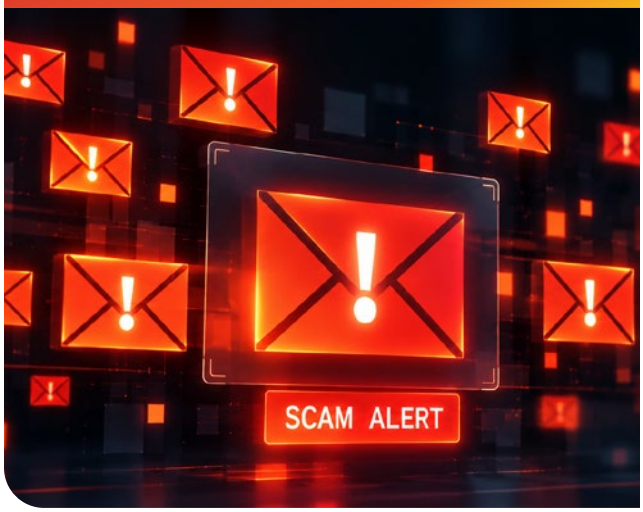


La familiaridad ayuda a explicar por qué puede pasarse por alto la verificación. La encuesta reveló que el 72 % de los encuestados hizo clic en un vínculo o abrió un archivo adjunto porque parecía provenir de alguien que conocía. Al preguntarles qué hace que una solicitud digital parezca confiable, el 38 % mencionó un remitente conocido, el 36 % indicó un entorno laboral conocido o datos personales familiares y el 32 % señaló que los elementos de marca de la empresa fueran los correctos. Solo el 27 % de los encuestados eligió la verificación independiente.

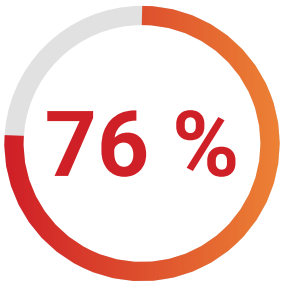
Hacer clic en contenido familiar no constituye, por sí solo, una prueba de que se haya cometido un error de seguridad. El problema surge cuando los nombres, el contexto y los elementos de marca reconocibles se confunden con una autenticación. Las organizaciones deben enseñar a los empleados a considerar estas señales como elementos de contexto y a confirmar las solicitudes importantes mediante un proceso establecido e independiente. Por último, las organizaciones también deben capacitar a los empleados sobre concientización en seguridad, el uso aceptable y las políticas adecuadas de transacciones financieras a través de sesiones de capacitación enfocadas.

CONCLUSIÓN CLAVE

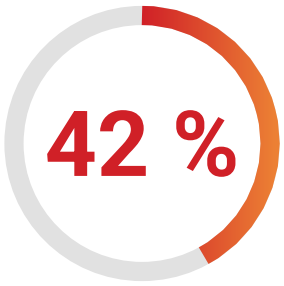
Las organizaciones deben enseñar a los empleados a considerar estas señales como elementos de contexto y a confirmar las solicitudes importantes mediante un proceso establecido e independiente.



06. El riesgo de suplantación de los directivos



confía en los gerentes o altos directivos al tomar decisiones laborales importantes.



probablemente confiaría en un mensaje de texto urgente del director ejecutivo que solicitara un pago o datos confidenciales sin verificarlo.



probablemente confiaría en un mensaje de voz urgente del director ejecutivo que solicitara un pago o datos confidenciales sin verificarlo.

Las organizaciones suelen tomar medidas deliberadas para que la confianza de los empleados en la dirección sea una parte habitual del entorno laboral. Esto se refleja en el hecho de que el 76 % de los encuestados confía en los gerentes o altos directivos al tomar decisiones laborales importantes. Aunque esta confianza beneficia la cultura corporativa y la moral de los empleados, también puede hacer que una solicitud falsa que aparenta provenir de un directivo resulte aún más convincente. De hecho, el 42 % de los trabajadores de todo el mundo probablemente confiaría en un mensaje de texto urgente que aparentemente proviniera del director ejecutivo o propietario de la empresa y solicitara un pago o datos confidenciales sin verificarlo. El 40 % afirma lo mismo respecto de un mensaje de voz que parece ser de ese directivo.

CONCLUSIÓN CLAVE

La identidad de un directivo y la urgencia de una solicitud nunca deben justificar una excepción a los requisitos de verificación.

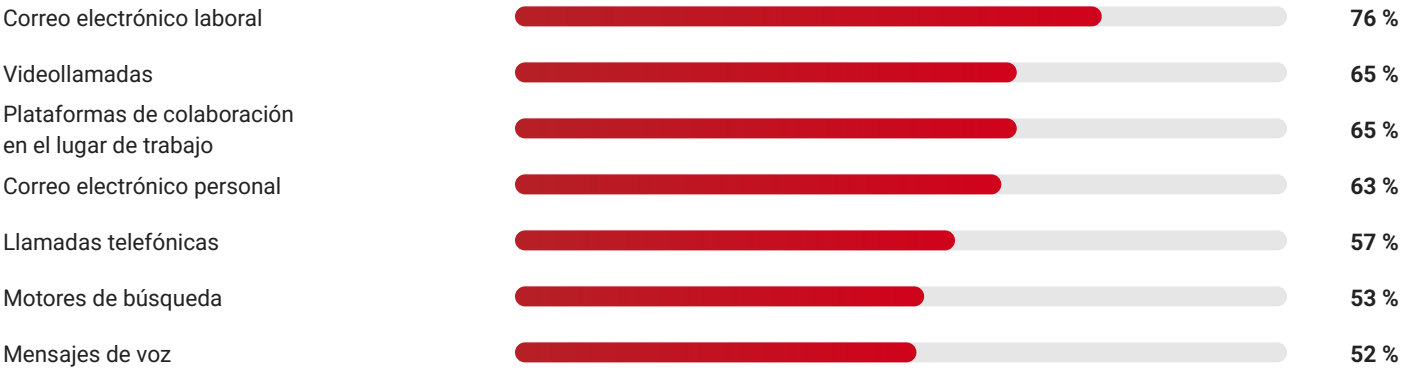
Estas respuestas miden la confianza implícita, no la disposición de un empleado a completar una transacción que sabe que es fraudulenta. Sin embargo, la identidad de un directivo y la urgencia de una solicitud nunca deben justificar una excepción a los requisitos de verificación. Los resultados señalan una prioridad clara para las organizaciones: los empleados necesitan tanto un procedimiento de confirmación establecido como el respaldo explícito de la dirección para utilizarlo.

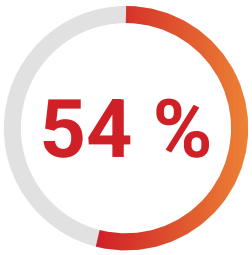


07. La confianza en la era de los deepfakes

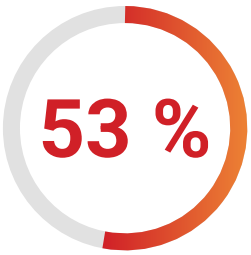
La misma dependencia de las señales familiares se extiende a los canales de comunicación cotidianos. El correo electrónico laboral es el canal más confiable: el 76 % de los trabajadores de todo el mundo confía en la información que recibe a través de este medio. Las videollamadas y las plataformas de colaboración laboral registraron un 65 % cada una, seguidas del correo electrónico personal (63 %), las llamadas telefónicas (57 %), los motores de búsqueda (53 %) y los mensajes de voz (52 %). La confianza general en un canal no necesariamente indica un comportamiento inseguro, pero no permite autenticar todos los mensajes ni validar todas las respuestas que se reciben a través de él.

Los canales de comunicación más confiables





informó haber encontrado una estafa generada por IA, un deepfake, un intento de suplantación o una comunicación fraudulenta.



se basó en el rostro, la voz o el nombre para mostrar de una persona para verificar su identidad.



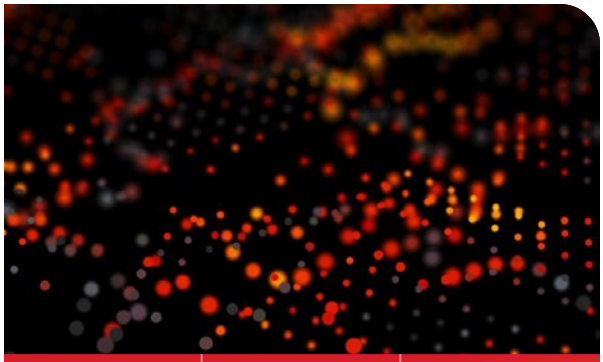
afirmó dar prioridad a otro canal de verificación o procedimiento organizacional.

Esta falta de consistencia tiene consecuencias más importantes cuando es posible imitar rostros y voces familiares. Más de la mitad de los encuestados (54 %) informó haber encontrado una estafa generada por IA, un deepfake, un intento de suplantación o una comunicación fraudulenta. La pregunta agrupaba estas situaciones y no permite determinar que todos los casos hayan involucrado IA. Ante una solicitud inusual o confidencial por video, el 53 % se basó en el rostro, la voz o el nombre para mostrar de una persona para verificar su identidad, mientras que solo el 28 % afirmó dar prioridad a otro canal de verificación o procedimiento organizacional. Una apariencia familiar puede generar confianza, pero no debe reemplazar la confirmación de identidad mediante un método de contacto aprobado previamente. La verificación debe activarse en función de las consecuencias de la solicitud, incluso cuando la interacción parezca creíble.

CONCLUSIÓN CLAVE

La verificación debe activarse en función de las consecuencias de la solicitud, incluso cuando la interacción parezca creíble.

La IA generativa plantea un desafío adicional de verificación tanto para los empleados como para sus organizaciones. Menos de la mitad de los encuestados (47 %) confía en las herramientas de IA generativa. Sin embargo, solo el 32 % afirmó que siempre verifica la información generada por IA antes de actuar, mientras que el 34 % lo hace solo algunas veces, rara vez o nunca. El proceso de verificación adecuado depende del caso de uso específico. Una sugerencia informal para una sesión de lluvia de ideas y un resultado que influye en un compromiso con un cliente, una decisión financiera o una medida de seguridad tienen consecuencias diferentes. La gobernanza de la IA debe establecer explícitamente estas distinciones e indicar cuándo los empleados deben consultar fuentes autorizadas u obtener una revisión por parte de personal calificado.

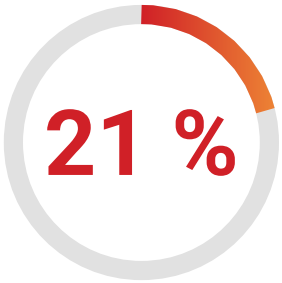


47 %
confía en las herramientas de IA generativa.

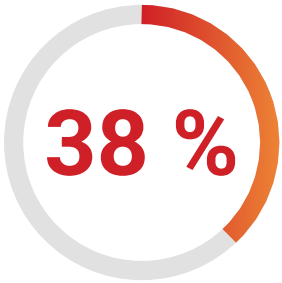
32 %
siempre verifica la información generada por IA antes de actuar.

34 %
lo hace solo algunas veces, rara vez o nunca.

08. Los empleados detectan deficiencias en sus organizaciones y los empleadores deben actuar



considera que su organización está completamente preparada para prevenir o resistir un ataque de ciberseguridad importante.



mencionó la falta de concientización de los empleados o la capacitación insuficiente.

Estos desafíos de verificación plantean una cuestión más amplia sobre la preparación de las organizaciones. Solo el 21 % de los encuestados considera que su organización está completamente preparada para prevenir o resistir un ataque de ciberseguridad importante. Esto no significa que los demás empleados consideren que sus organizaciones no están preparadas, pero sí demuestra que la confianza plena en las defensas de las organizaciones es limitada. Al preguntarles cuál era el principal obstáculo para mejorar la preparación de sus organizaciones, el 38 % de los empleados mencionó la falta de concientización de los empleados o la capacitación insuficiente.

La formación de los empleados es una responsabilidad de la organización, y estas respuestas señalan la concientización y la capacitación como prioridades de mejora. La capacitación debe complementarse con procedimientos de aprobación viables, canales accesibles para informar incidentes y medidas de protección técnicas. Los empleados deben saber qué situaciones requieren verificación, cómo llevarla a cabo y a quién acudir cuando reciben una solicitud bajo presión. En última instancia, la confianza en el nivel de preparación debe contrastarse con simulacros y pruebas operativas.

09. La IA agrega complejidad a la seguridad organizacional



de los empleados confía en que su empleador utiliza la IA de manera responsable y segura.

La necesidad de contar con el respaldo de la organización también se extiende a la IA: solo el 56 % de los empleados confía en que su empleador utiliza la IA de manera responsable y segura. Los empleadores pueden ayudar a los empleados a tomar decisiones informadas si explican cómo se seleccionan las herramientas de IA aprobadas, cómo se protege la información confidencial y en qué situaciones se aplica la supervisión humana. Las políticas actualizadas deben traducir estos compromisos en decisiones cotidianas sobre el ingreso de datos, el uso compartido de resultados y la aplicación de recomendaciones.

10. La confianza cibernética y los hábitos de verificación por industria

Las comparaciones entre industrias muestran que la confianza y la verificación no siempre evolucionan de la misma manera. Los encuestados del sector de servicios financieros manifiestan el mayor nivel de confianza en el contenido digital, pero menos de la mitad siempre verifica las solicitudes confidenciales. El sector de atención médica registra la mayor proporción de personas que siempre verifican, aunque muchos encuestados también confiarían en un mensaje de texto urgente del director ejecutivo. Los encuestados del sector gubernamental son los más escépticos respecto del contenido digital y los mensajes de texto del CEO, pero menos de la mitad siempre verifica. Por lo tanto, un menor nivel de confianza, por sí solo, ofrece pocas garantías sobre los hábitos de verificación.

Industria	Muestra (n)	Confianza en el contenido	Confianza en los mensajes de texto del director ejecutivo	Verificación constante	Nivel de preparación
Atención médica	79	63 %	57 %	63 %	68 %
Servicios financieros	100	72 %	65 %	43 %	71 %
Seguros	27	56 %	41 %	22 %	52 %
Servicios jurídicos	26	46 %	35 %	38 %	46 %
Comercio minorista	44	41 %	30 %	39 %	48 %
Hospitalidad	22	32 %	32 %	36 %	27 %
Gobierno	30	30 %	23 %	47 %	47 %
Educación	53	42 %	40 %	42 %	53 %
Otro	131	40 %	30 %	47 %	47 %

Las prioridades prácticas varían según la industria. Los sectores de servicios financieros y atención médica deben reforzar las verificaciones independientes de las solicitudes de los directivos. La industria de seguros registra la menor proporción de personas que siempre verifican, lo que señala la necesidad de establecer procedimientos más sencillos y uniformes. La baja percepción del nivel de preparación y la confianza limitada para reconocer la suplantación en el sector de hospitalidad justifican un enfoque centrado en la capacitación y el acceso a asistencia. Las preocupaciones sobre la dotación de personal entre los encuestados del sector de servicios jurídicos señalan la necesidad de soporte en materia de seguridad. En todos los sectores, el objetivo es convertir la verificación en una práctica habitual, en lugar de suponer que la confianza o el escepticismo, por sí solos, darán lugar a comportamientos seguros. Estos son resultados descriptivos obtenidos de subgrupos pequeños de cada industria.

11. La confianza cibernética y los hábitos de verificación por país

Los resultados por país refuerzan la distinción entre la confianza y la verificación. Los encuestados de Estados Unidos son los más propensos a confiar en un mensaje de texto urgente del director ejecutivo (59 %), a pesar de informar hábitos de verificación relativamente sólidos. Australia registra la tasa más alta de personas que siempre verifican la información (69 %), lo que demuestra que la confianza en el contenido digital puede coexistir con una verificación constante. Los encuestados del Reino Unido muestran mayor escepticismo ante los mensajes de texto del director ejecutivo, pero solo alrededor de la mitad siempre verifica las solicitudes sensibles. Estas preguntas independientes describen las actitudes y los hábitos de cada muestra nacional, pero no demuestran que las mismas personas tengan comportamientos contradictorios.

País	Muestra (n)	Confianza en el contenido	Confianza en los mensajes de texto del director ejecutivo	Verificación constante	Nivel de preparación
Estados Unidos	113	62 %	59 %	65 %	73 %
España	62	44 %	48 %	31 %	40 %
Reino Unido	63	40 %	24 %	52 %	51 %
Alemania	54	52 %	43 %	22 %	57 %
Italia	55	44 %	38 %	36 %	42 %
Portugal	54	41 %	39 %	28 %	50 %
Australia	51	59 %	39 %	69 %	67 %
Francia	60	53 %	33 %	42 %	45 %

Alemania registra la tasa más baja de personas que siempre verifican la información (22 %), mientras que Portugal y España también presentan tasas relativamente bajas. Las organizaciones deben priorizar procedimientos de verificación fáciles de seguir en estos países, sin perder de vista que otros encuestados afirman que generalmente verifican. Las preocupaciones relacionadas con la capacitación en España, Portugal y Francia, así como las relacionadas con la concientización en Estados Unidos, respaldan la necesidad de ofrecer formación adaptada a cada contexto local. La respuesta práctica es establecer un estándar de verificación común, aplicado mediante contenidos en el idioma local, escenarios relevantes para cada rol y soporte accesible. Las diferencias en la confianza de los empleados en la IA y en la preparación que perciben de sus organizaciones pueden orientar conversaciones de seguimiento. Sin embargo, estas pequeñas muestras por país no permiten establecer clasificaciones nacionales del desempeño en ciberseguridad.



12. La perspectiva de WatchGuard: cómo pueden las organizaciones cerrar la brecha de confianza cibernética

Las organizaciones pueden incorporar la verificación a las actividades habituales de trabajo si alinean las políticas, el comportamiento de la dirección, la formación y la protección técnica. Las seis prioridades siguientes pueden ayudar a mejorar la confianza y la seguridad en todos los niveles de la organización.

1

Hacer obligatoria la verificación de las solicitudes sensibles

Exija confirmar los cambios de pago, las transferencias de datos confidenciales y las solicitudes de acceso inusuales mediante un método de contacto establecido previamente. Utilice un número de teléfono de un directorio conocido o un flujo de trabajo aprobado, en lugar de los datos de contacto incluidos en la solicitud. Exija una aprobación adicional para las transacciones de alto impacto y aplique estas reglas también a los directivos.

2

Capacitar a los empleados para que sigan un procedimiento cuando algo parezca convincente

Utilice ejercicios realistas que incluyan mensajes de texto de directivos, voces conocidas, videollamadas y plataformas de colaboración que se adapten a los escenarios y las decisiones que toma cada rol. Practique cómo hacer una pausa, confirmar la solicitud e informar sobre ella bajo presión de tiempo, para poner a prueba los entornos de trabajo. Enseñe el procedimiento de verificación sin hacer que el éxito dependa de que los empleados detecten defectos visuales o de audio.

3

Publicar reglas claras sobre el uso de la IA

Identifique las herramientas aprobadas, los datos confidenciales que no se pueden ingresar, los usos permitidos y los responsables correspondientes. Defina cuándo los resultados requieren verificar las fuentes, una revisión humana especializada o una aprobación formal antes de actuar. Aborde el tratamiento de la información confidencial, los datos de los clientes y el acceso de la IA a los sistemas empresariales. Ofrezca a los empleados un canal para plantear dudas sobre usos inciertos y revise los permisos a medida que cambien las herramientas y los flujos de trabajo.

Actualice la capacitación sobre concientización en seguridad y las políticas de comunicación para contemplar cómo se puede utilizar la IA para aprovechar la familiaridad y la confianza. Asegúrese de que los empleados sepan cómo la IA, los videos y audios falsificados mediante deepfakes y los actores maliciosos pueden generar comunicaciones que parezcan provenir de personas en quienes normalmente confiarían. Además, anímelos a seguir los procedimientos de validación de todos modos.

4

Brindar protección por capas a los empleados

Priorice la autenticación multifactor resistente a la suplantación de identidad, junto con el filtrado de correo electrónico, la protección de los endpoints y los controles de acceso. Aplique el principio de privilegio mínimo y mantenga los sistemas actualizados de manera oportuna. Combine estas medidas de protección con copias de seguridad probadas y procedimientos de respuesta, de modo que un error individual tenga menos posibilidades de convertirse en un incidente de mayor alcance.

5

Hacer que informar incidentes sea fácil y seguro

Ofrezca un canal visible para informar sobre posibles casos de suplantación, clics accidentales o divulgaciones involuntarias de información, y brinde asistencia oportuna. Los líderes deben respaldar explícitamente a los empleados que cuestionen solicitudes inusuales, incluso cuando provengan de ellos mismos. Explique qué sucede después de recibir una denuncia y proporcione retroalimentación para que informar un incidente se convierta en una acción útil y respaldada.

6

Medir los comportamientos y las respuestas

Realice un seguimiento de las verificaciones independientes exitosas en ejercicios controlados, la rapidez con que se informa y la divulgación de datos confidenciales, junto con la cobertura técnica y el desempeño de respuesta. Evalúe el progreso según el puesto y la ubicación, y utilice los resultados para mejorar los flujos de trabajo y la orientación. La finalización de la capacitación y la confianza de los empleados son indicadores útiles, pero ninguno de ellos demuestra por sí solo que la organización esté preparada.

13. La visión de WatchGuard: cómo pueden ayudar los MSP

Los proveedores de servicios administrados pueden ayudar a las organizaciones a convertir estas prioridades en un programa de seguridad práctico y repetible, especialmente cuando cuentan con personal interno limitado. Comience por identificar los flujos de trabajo de mayor impacto, como las aprobaciones de pagos, los cambios en las nóminas, el restablecimiento de credenciales, el intercambio de información confidencial y el uso de la IA. Determine en qué casos los empleados se basan en la confianza informal. Establezca procedimientos de confirmación documentados, directorios de contactos aprobados, responsabilidades claras de escalamiento y capacitación según el puesto. Utilice los resultados por industria para seleccionar escenarios realistas y los resultados por país para adaptar el idioma y la modalidad, sin dejar de aplicar el mismo estándar de verificación en toda la organización.

Luego, los MSP pueden implementar y gestionar medidas de protección por capas, como la autenticación multifactor resistente a la suplantación de identidad, la seguridad del correo electrónico y de los endpoints, el acceso con privilegios mínimos y la supervisión. También pueden ayudar a mantener inventarios de herramientas de IA aprobadas, configurar controles de acceso y manejo de datos, y probar los procedimientos de respuesta y recuperación junto con los clientes. Las revisiones periódicas del servicio deben relacionar la cobertura técnica con la evidencia del comportamiento: si los empleados verifican las solicitudes sensibles, con qué rapidez informan sobre posibles problemas y si los equipos actúan en consecuencia. Esto ofrece a los empleadores una base más clara para mejorar que las cifras de confianza o finalización de cursos por sí solas, y ayuda a los empleados a desarrollar hábitos confiables con soporte accesible.

Los proveedores de servicios administrados pueden ayudar a las organizaciones a convertir estas prioridades en un programa de seguridad práctico y repetible, especialmente cuando cuentan con personal interno limitado.



Las revisiones periódicas del servicio ofrecen a los empleadores una base más clara para mejorar que las cifras de confianza o finalización de cursos por sí solas, y ayudan a los empleados a desarrollar hábitos confiables con soporte accesible.

Acerca de la investigación

La encuesta abarca a empleados de tiempo completo de ocho países. Los desgloses por país y por industria incluyen 512 encuestados cada uno. El tamaño de las muestras por país oscila entre 51 y 113 personas; las muestras de las industrias identificadas oscilan entre 22 y 100 personas, mientras que 131 encuestados se clasificaron en la categoría “Otro”. Los porcentajes están redondeados.

Los hallazgos miden actitudes, hábitos, experiencias y percepciones autoinformadas sobre la preparación de las organizaciones, no comportamientos observados ni resultados de seguridad auditados.

WatchGuard Technologies es líder mundial en ciberseguridad unificada y diseñada para proveedores de servicios administrados (MSP). Desde hace más de 30 años, WatchGuard define la manera en que los MSP ofrecen seguridad a escala e innova continuamente para mantenerse a la vanguardia de cada cambio importante en el panorama de las amenazas. La Unified Security Platform® de WatchGuard, impulsada por IA, ofrece protección de identidades, endpoints y redes alineada con Zero Trust en una plataforma única e integrada, lo que permite a los MSP reducir la complejidad operativa, mejorar los resultados de seguridad y hacer crecer sus negocios de manera más eficiente. Gracias a la confianza de más de 25 000 MSP que protegen a más de 1,5 millones de clientes en todo el mundo, WatchGuard permite a los partners ofrecer resultados de seguridad sólidos y medibles para clientes de todo el mundo. Visite watchguard.com/es para obtener más información.

No se proporcionan garantías expresas o implícitas en este documento. Todas las especificaciones están sujetas a cambios, y todas las funcionalidades, las características o los productos futuros previstos se suministrarán según su disponibilidad. ©2026 WatchGuard Technologies, Inc. Todos los derechos reservados. WatchGuard, el logotipo de WatchGuard, Unified Security Platform, y AuthPoint son marcas comerciales registradas de WatchGuard Technologies, Inc. en los Estados Unidos y/o en otros países. Los demás nombres comerciales son propiedad de sus respectivos dueños. N.º de pieza WGCE67993_103026