Microsoft Security

hypothesis

Informe de adopción de la Confianza Cero

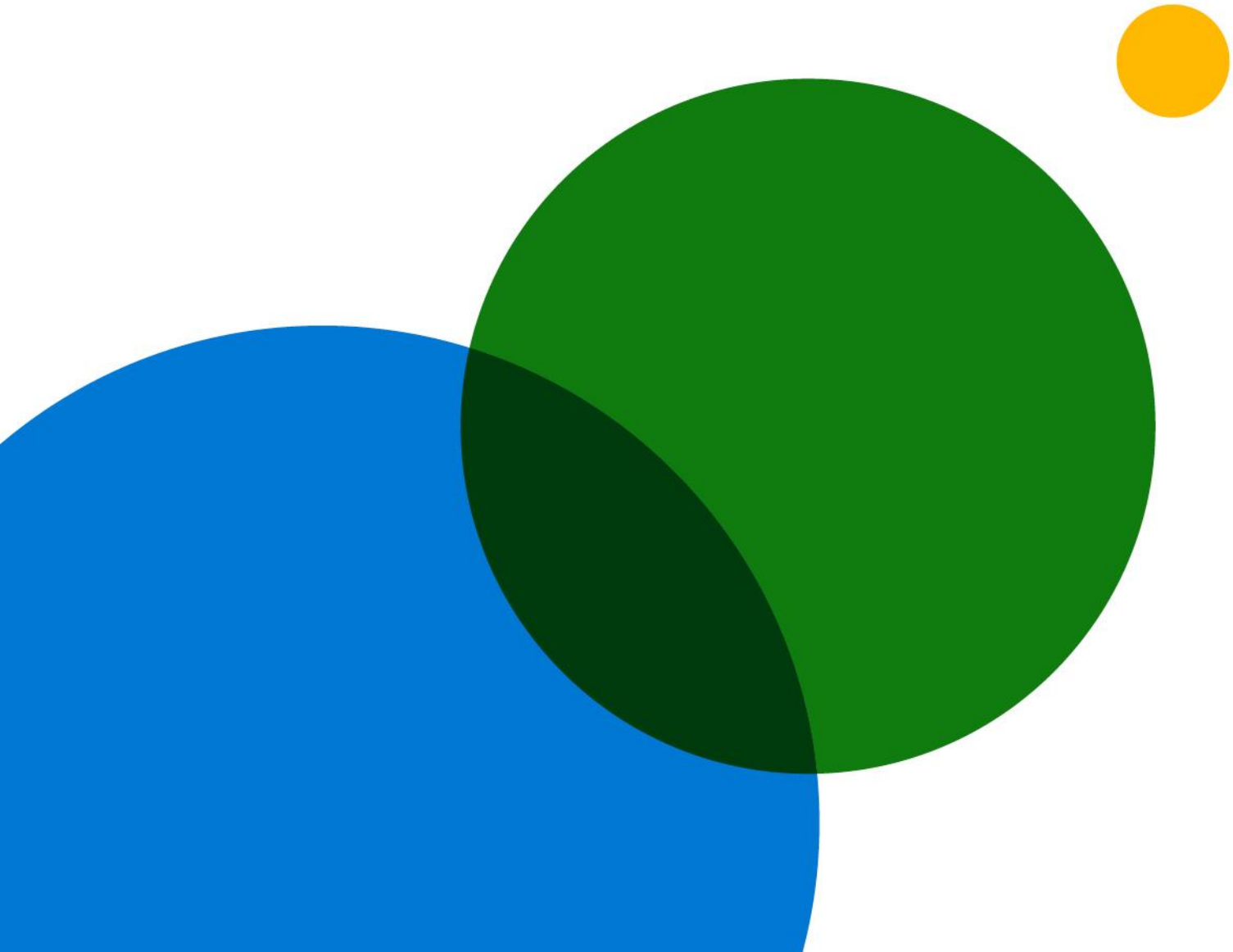


Tabla de contenido

Introducción

Vasu Jakkal / Vicepresidente corporativo, Seguridad, cumplimiento e identidad

Este último año ha sido notable en la evolución de la ciberseguridad y el auge de la Confianza Cero como estrategia orientadora para nuestra industria y organizaciones de todo el mundo.

Al inicio de la pandemia, el lugar de trabajo se convirtió de la noche a la mañana en algo casi totalmente remoto. Este cambio obligó a muchas organizaciones a adaptarse con rapidez para apoyar a los empleados que hacían su trabajo de cualquier manera: mediante dispositivos personales, colaborando a través de servicios en la nube y compartiendo datos fuera del perímetro de la red corporativa. A medida que las organizaciones se adaptaban a esta transformación, también se enfrentaban a ciberdelincuentes cada vez más sofisticados que evolucionan continuamente sus objetivos, tácticas y recursos.

En la actualidad, el trabajo híbrido es la nueva realidad. En este contexto, y ante la rapidez de los cambios, las organizaciones encuestadas nos han dicho que se basan en la Confianza Cero para una mayor agilidad de la seguridad y el cumplimiento, mejor velocidad de detección y corrección de las amenazas, y aumento de la simplicidad y disponibilidad de los análisis de seguridad.

Una arquitectura integral de Confianza Cero, basada en los principios de comprobar explícitamente, utilizar el acceso menos privilegiado y suponer el incumplimiento, crea protecciones dentro y a través de la identidad, los puntos de conexión, las aplicaciones, la infraestructura, la red y los datos, junto con una mayor visibilidad, automatización y orquestación. Aquí en Microsoft no solo recomendamos este enfoque con nuestros clientes y socios, sino que lo adoptamos en nuestro enfoque de seguridad global y desarrollo de software.

En este informe se ilumina el camino de la adopción de la Confianza Cero en diversos mercados e industrias. Esperamos que el aprendizaje obtenido por esta investigación pueda ayudar a acelerar su propia adopción de la estrategia de Confianza Cero, arrojar luz sobre el progreso colectivo de sus compañeros y ofrecer ideas sobre el estado futuro de este espacio en rápida evolución.

Metodología

Microsoft encargó a Hypothesis Group, una agencia de ideas, diseño y estrategia, la realización del informe e investigación sobre la adopción de la Confianza Cero. La investigación incluyó dos fases en los Estados Unidos para destacar las tendencias y el impulso en la adopción de la Confianza Cero, con mercados adicionales agregados en la segunda fase para descubrir las tendencias globales.

La investigación inicial tuvo lugar en agosto de 2020, cuando se llevó a cabo una encuesta en línea de 15 minutos en los Estados Unidos con 300 responsables de la toma de decisiones sobre seguridad (SDM) que participan en las decisiones de estrategia de Confianza Cero en las empresas de una serie de industrias. Además de la encuesta en línea, en septiembre de 2020 se llevaron a cabo en línea cinco entrevistas en profundidad entre los responsables de la toma de decisiones sobre seguridad de los Estados Unidos en una serie de industrias.

En abril de 2021, se llevó a cabo una investigación global en Estados Unidos, Alemania, Japón y Australia/Nueva Zelanda entre un grupo similar de responsables de la toma de decisiones sobre seguridad. Más de 900 participantes respondieron una encuesta en línea de 15 minutos con preguntas sobre la adopción de la estrategia de Confianza Cero, los procedimientos recomendados, los beneficios, los desafíos y cómo piensan invertir en el futuro.

Cosas que debe saber sobre la adopción de la Confianza Cero

01 / Las organizaciones están preparadas para capitalizar la estrategia de Confianza Cero, acelerada por el traslado a un lugar de trabajo híbrido y la Covid-19

Los responsables de la toma de decisiones sobre seguridad (SDM) afirman que el desarrollo de una estrategia de Confianza Cero es su principal prioridad de seguridad, y el 96 % señala que es esencial para el éxito de su organización. Los principales motivadores para adoptar una estrategia de Confianza Cero son la mejora de su postura general de seguridad y la experiencia del usuario final. El cambio hacia un lugar de trabajo híbrido, acelerado por la COVID-19, también está impulsando una mayor adopción de la estrategia de Confianza Cero: el 81 % de las organizaciones empresariales ha iniciado el cambio hacia un lugar de trabajo híbrido, y el 31 % lo ha hecho por completo. Sin embargo, el 94 % tiene preocupaciones sobre la transición, sobre todo, el mal uso de los empleados, el aumento de la carga de trabajo de TI y los ciberataques. Teniendo en cuenta esto, las consideraciones clave para una estrategia incluyen una mayor capacitación de los empleados y la autenticación multifactor (MFA) para garantizar una experiencia de usuario y una transición sin inconvenientes.

02 / La estrategia de Confianza Cero permite flexibilidad en cuanto a dónde pueden empezar a aplicarla las organizaciones, de modo que el enfoque puede adaptarse a sus necesidades

Menos del 15 % de las organizaciones comenzó a implementar una estrategia de Confianza Cero en la misma área de riesgo de seguridad. Esto se debe, en gran parte, a que la implantación se aborda como un proceso integral que abarca los pilares y las capacidades de la arquitectura de seguridad, y no como una serie de tecnologías individuales y dispares. Del mismo modo, el orden en el que se implementan los componentes individuales de Confianza Cero dentro de un área de riesgo de seguridad es muy variable, y los profesionales de la seguridad difieren sustancialmente en los componentes que empiezan a implementar primero

03 / Aunque la estrategia de Confianza Cero está ampliamente adoptada y mejora la capacidad de las organizaciones para administrar las amenazas, aún queda trabajo por hacer

El 76 % de las organizaciones ha empezado al menos a aplicar una estrategia de Confianza Cero, y el 35 % afirma haberla aplicado por completo. Sin embargo, los que afirman estar totalmente implementados admiten que no han terminado de aplicar la estrategia de Confianza Cero en todas las áreas y componentes de riesgo de seguridad. La estrategia de Confianza Cero es convincente porque ofrece mayor agilidad, velocidad de detección de amenazas y mejor capacidad para administrar la seguridad de la Internet de las Cosas (IoT) y la tecnología operativa (OT). La adopción está creciendo en Estados Unidos (del 70 % en agosto de 2020 al 79 % en abril de 2021); Estados Unidos también está más adelantado en la implementación de la Confianza Cero en relación con otros países que empezaron a adoptarla más tarde, y las organizaciones de Estados Unidos afirman estar menos limitadas por los presupuestos. Sin embargo, aunque el 57 % de las organizaciones afirma estar por delante de las demás en lo que respecta a la adopción, cerca de la mitad aún tiene que trabajar más, ya que no han implementado por completo la Confianza Cero en todas las áreas y componentes de riesgo de seguridad.

04 / De cara al futuro, la estrategia de Confianza Cero seguirá siendo una de las principales prioridades y requerirá una cuidadosa toma de decisiones cuando se trate de empleados y proveedores

Se espera que la estrategia de Confianza Cero siga siendo la principal prioridad de seguridad dentro de dos años y las organizaciones prevén aumentar su inversión. Superar los desafíos con sus empleados (incluida la dotación de personal de los equipos de seguridad y la aceptación por parte de la dirección) será clave para duplicar la inversión en Confianza Cero. En cuanto a la estrategia de proveedores, los responsables de la toma de decisiones sobre seguridad tienen una ligera preferencia por trabajar con proveedores integrales o consolidados, ya que la selección de proveedores suele depender de la disponibilidad de conocimientos internos. Los beneficios del enfoque de lo mejor del conjunto incluyen una mayor experiencia, recursos y simplicidad, aunque puede llevar más tiempo de implementación, ser más difícil de integrar en la arquitectura de seguridad existente y aumentar la vulnerabilidad potencial.

Con quiénes hablamos

Mundial

Responsables de la toma de decisiones sobre seguridad
que trabajan en empresas de gran tamaño*

90 %
Familiarizado con la Confianza Cero
Autodeclaración, aprobar una prueba de conocimientos

76 %
en la implementación de la Confianza Cero

24 %
en la planificación/consideración de la Confianza Cero

*más de 1000 empleados en Estados Unidos; más de 500 empleados en Alemania, Japón, Australia/Nueva Zelanda

Aprendizaje general de la investigación

Las organizaciones están preparadas para capitalizar la estrategia de Confianza Cero

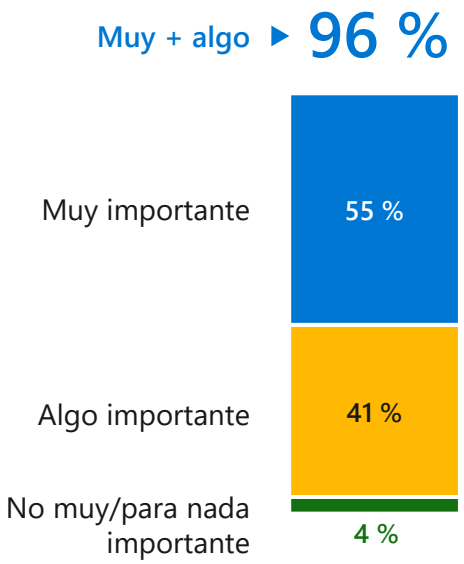
La estrategia de Confianza Cero es la principal prioridad de seguridad en la actualidad en los mercados y las industrias, con un número de organizaciones que han adoptado una estrategia de Confianza Cero en los últimos años. Aunque la Confianza Cero es lo más importante para todos (53 %), es una prioridad especialmente alta para las organizaciones de Estados Unidos (56 %) y Alemania (53 %).

Casi todos los profesionales de la seguridad (96 %) creen que una estrategia de Confianza Cero es fundamental para el éxito de su organización. (Consulte el Anexo 1) Además de reforzar su postura general de seguridad y mejorar la experiencia del usuario final, los profesionales de la seguridad están buscando la estrategia de Confianza Cero para simplificar los procedimientos de seguridad para los empleados. (Consulte el Anexo 2)

Como explica un responsable de la toma de decisiones sobre seguridad en la industria de la hospitalidad de Estados Unidos, "*El objetivo es mejorar nuestra postura de seguridad en general, pero se trata de reducir la fricción en la experiencia del usuario final y facilitarle la vida*".

Además, el 31 % de los profesionales de la seguridad consideran que la estrategia de Confianza Cero es una herramienta importante en el inminente cambio a un lugar de trabajo híbrido después de la pandemia; este factor es especialmente importante en Australia/Nueva Zelanda (44 %).

Anexo 1. La Confianza Cero es fundamental



Anexo 2. Motivadores de Confianza Cero

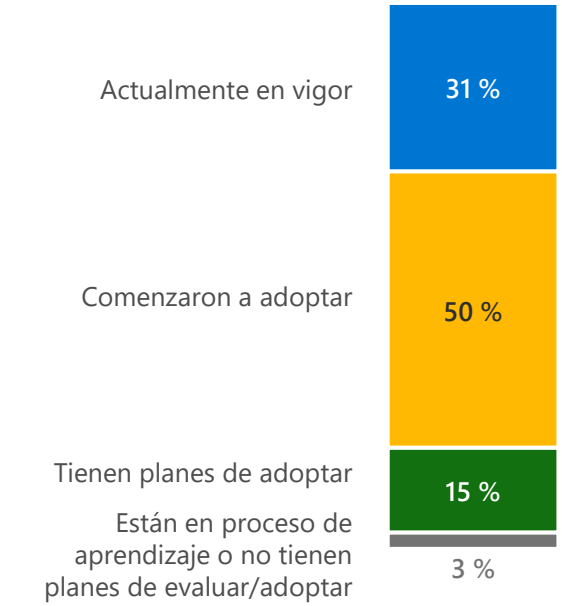
Principales motivadores	
Mejorar la estrategia de seguridad general	47 %
Mejorar la experiencia y productividad del usuario final	44 %
Transformar la manera en que trabajan los equipos de seguridad en conjunto	38 %
Simplificar la pila de seguridad	35 %
Reducir los costos de seguridad	35 %

El cambio a un lugar de trabajo híbrido está impulsando una mayor adopción de la estrategia de Confianza Cero

El 81 % de las organizaciones empresariales ha iniciado la transición hacia un lugar de trabajo híbrido, y el 31 % ya lo ha adoptado por completo. Sin embargo, las tasas de adopción total no son uniformes en todos los mercados: mientras que Australia y Nueva Zelanda lideran el grupo con un 37 %, Alemania está muy por detrás, con solo un 20 % de organizaciones que ya han pasado a un modelo híbrido. (Consulte el Anexo 3)

Aunque los mercados globales avanzan hacia un lugar de trabajo híbrido a ritmos dispares, la gran mayoría (91 %) de las organizaciones que no han finalizado la transición prevén hacerlo en los próximos cinco años. Lo más importante es que el 94 % está preocupado por la transición, con el mal uso por parte de los empleados, el aumento de la carga de trabajo de TI y el mayor riesgo de ciberataques entre los primeros lugares de la lista de preocupaciones. (Consulte el Anexo 4)

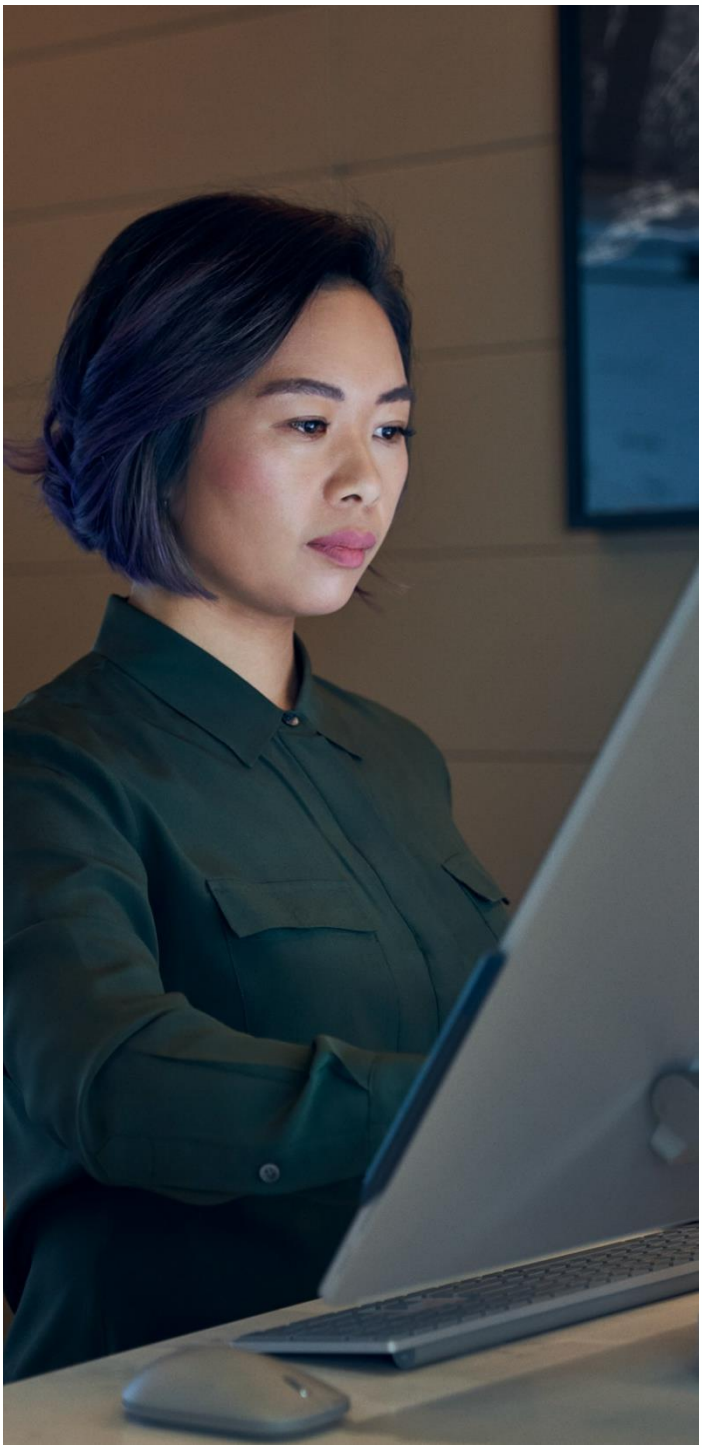
Anexo 3. Intención del lugar de trabajo híbrido



Anexo 4. Preocupaciones del lugar de trabajo híbrido

Empleados que descargan aplicaciones poco seguras	37 %
Un aumento de la carga de trabajo de TI	37 %
Ataques de ransomware	36 %
Ataques de suplantación de identidad (phishing)	35 %
Uso indebido de dispositivos personales	34 %
Acceso no autorizado a los datos	31 %
Incapacidad para administrar todos los dispositivos	30 %
Uso de cuentas personales de correo electrónico	30 %
Incumplimiento de las normativas de datos	24 %

La Covid-19 ha aportado nuevas consideraciones que aceleran el paso a la estrategia de Confianza Cero



En un esfuerzo por minimizar los posibles problemas, las partes interesadas destacan la importancia de aumentar la capacitación de los empleados (54 %) (en especial en Japón [61 %] y Alemania [58 %]) y la autenticación multifactor (50 %) (en especial en Estados Unidos [52 %] y Alemania [56 %]) para garantizar una experiencia de usuario y una transición sin inconvenientes.

Dado que el trabajo remoto e híbrido seguro puede verse favorecido por la estrategia de Confianza Cero, la COVID-19 ha acelerado la adopción de una estrategia de Confianza Cero para el 72 % de las organizaciones, aunque surgen asimetrías entre los mercados. Mientras que la pandemia catalizó la adopción por parte de unas siete de cada diez organizaciones en Estados Unidos (76 %), Japón (71 %) y Australia/Nueva Zelanda (69 %), los índices de implementación han sido notablemente inferiores en Alemania (62 %), quizá debido a una transición más lenta hacia un lugar de trabajo híbrido.

La Confianza Cero está ampliamente implementada en todo el mundo y crece en Estados Unidos

La Confianza Cero no es solo una palabra de moda; es una realidad. El 76 % de las organizaciones ha empezado al menos a aplicar esta estrategia y el 35 % cree que la ha aplicado por completo. Sin embargo, estos datos presentan un panorama demasiado optimista, ya que muchas organizaciones que se consideran plenamente implementadas admiten que no han terminado de ejecutar todas las áreas de riesgo de seguridad. En la actualidad, Estados Unidos está a la cabeza en la adopción de la estrategia de Confianza Cero en relación con otros mercados y sigue creciendo con rapidez: en comparación con agosto de 2020, la implementación de la estrategia de Confianza Cero en Estados Unidos aumentó del 70 % al 79 %, un salto considerable en solo ocho meses. (Consulte el Anexo 5)

Si bien la estrategia de Confianza Cero predomina en la actualidad en el espacio de la seguridad, su ubicuidad es relativamente nueva. El 82 % de las empresas ha aplicado estrategias de Confianza Cero en los últimos tres años, y el 21 % lo ha hecho en los últimos 12 meses. Dicho esto, el 26 % de las organizaciones estadounidenses iniciaron la implementación hace más de 3 años, en comparación con el 19 % de las organizaciones japonesas, el 6 % de las organizaciones de australianas/neozelandesas y el 3 % de las organizaciones alemanas. Esta implementación más temprana en los Estados Unidos (junto con menos restricciones presupuestarias) puede ayudar a explicar la razón por la que las organizaciones en los Estados Unidos están por delante en la adopción de la Confianza Cero en comparación con las organizaciones en otros mercados. En una línea similar, la relativa nascencia de la Confianza Cero en Alemania ayuda a contextualizar sus menores índices de adopción: el 97 % de las organizaciones alemanas no empezaron a implementarla hasta los últimos tres años.

Anexo 5. Implementación de la Confianza Cero

	Estados Unidos (2020)	Estados Unidos	Alemania	Japón	Australia/ Nueva Zelanda
Implementación de la Confianza Cero	70 %	79 %	75 %	76 %	71 %
• Completamente implementada	27 %	44 %	19 %	32 %	28 %
• En curso	43 %	35 %	56 %	44 %	43 %

35 % Implementación completada

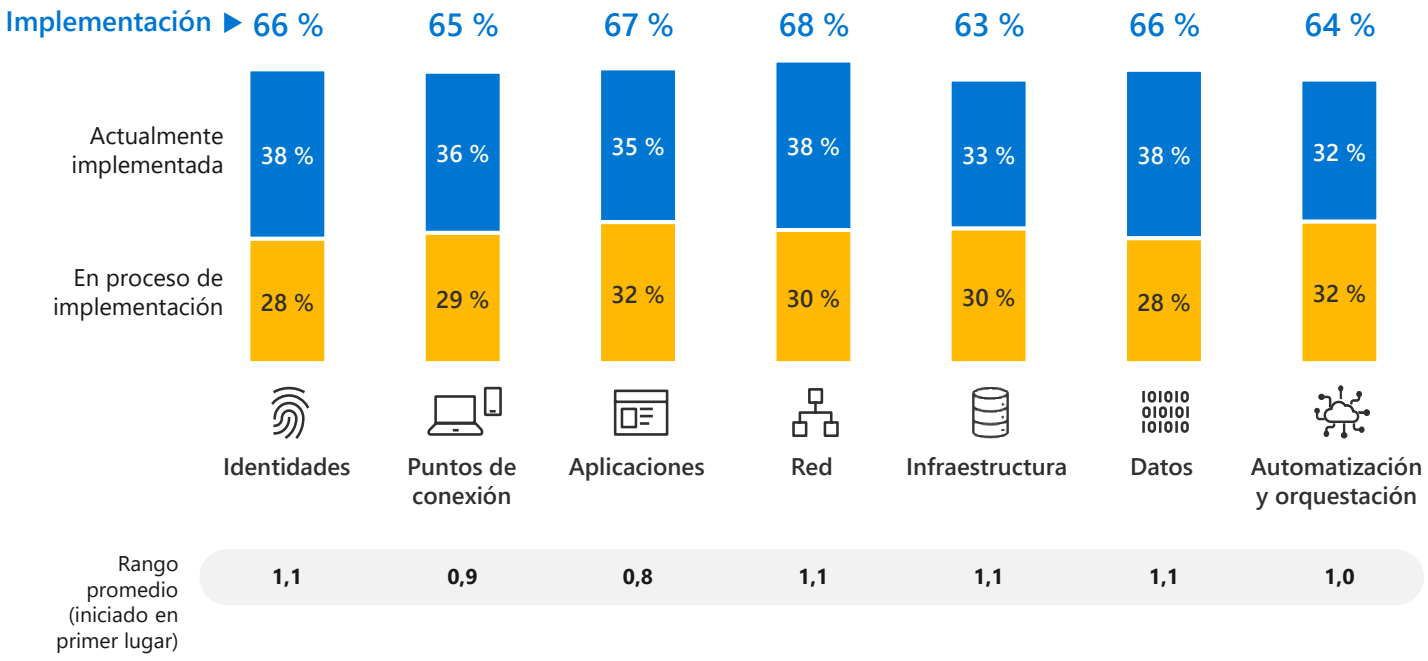
42 % Implementación en curso

No existe un enfoque único para la implementación de la Confianza Cero, lo que permite empezar en cualquier lugar

Ningún área de riesgo de seguridad (Identidades, Puntos de conexión, Aplicaciones, Red, Infraestructura, Datos, Automatización y Orquestación) destaca como punto de partida principal para la estrategia de Confianza Cero, ya que menos del 15 % empieza con la misma área de riesgo de seguridad. Las organizaciones comienzan en diferentes lugares, probablemente en función de sus necesidades y de los recursos internos disponibles. Con el tiempo, buscan adoptar la estrategia de Confianza Cero en todas las áreas de riesgo de seguridad para garantizar una protección aún mayor contra las amenazas, por lo que la Confianza Cero se percibe como una estrategia integral que debe completarse con el tiempo. (Consulte el Anexo 6)

Más allá de las áreas de riesgo de seguridad de la estrategia de Confianza Cero, las organizaciones tienen que identificar los componentes individuales de cada área de riesgo de seguridad para priorizar. En el caso de los Puntos de conexión, las Aplicaciones, la Red, los Datos y la Automatización/Orquestación, no hay un punto de partida claro; los profesionales de seguridad varían sustancialmente en cuanto a los componentes que se consideran prioritarios. Sin embargo, la autenticación sólida suele implementarse primero para las Identidades, y las herramientas de detección de amenazas son una clara prioridad dentro de la Infraestructura. (Consulte el Anexo 7)

Anexo 6. Implementación actual de la Confianza Cero: áreas de riesgo de seguridad



Anexo 7. Implementación de componentes de Confianza Cero (principales 3): posición n. ° 1 (se implementó primero)

Identidades	
Autenticación sólida (es decir, autenticación multifactor, autenticación sin contraseña)	32 %
Detección y corrección automatizadas de riesgos	27 %
Directivas de acceso adaptable para controlar el acceso a los recursos	22 %

Aplicaciones	
Detección continua Detección de TI y evaluación de riesgos	23 %
Control de acceso granular a sus aplicaciones (como visibilidad limitada o solo lectura)	22 %
Control de acceso a las aplicaciones basado en directivas	20 %

Infraestructura	
Acceso del equipo de operaciones de seguridad a las herramientas de detección de amenazas	25 %
Protección de cargas de trabajo en la nube a través de nube híbrida y multinube	19 %
Visibilidad granular y control de acceso en todas las cargas de trabajo (máquinas virtuales, servidores, etc.)	17 %

Automatización y orquestación	
La visibilidad de extremo a extremo se establece con una plataforma centralizada de investigación y respuesta	29 %
Los datos de amenazas se recopilan y analizan en dominios (identidades, puntos de conexión, aplicaciones, red, infraestructura)	28 %
Se habilita la investigación y la respuesta automatizadas	22 %

Puntos de conexión	
Directivas/controles de prevención de pérdida de datos para todos los dispositivos administrados y no administrados	27 %
Evaluación de riesgos de dispositivos en tiempo real/detección de amenazas de punto de conexión	26 %
Los dispositivos se registran con el proveedor de identidades	24 %

Red	
Controles de acceso seguro para proteger las redes	25 %
Protección contra amenazas y filtrado con señales basadas en el contexto	24 %
Todo el tráfico está cifrado	20 %

Datos	
Las decisiones de acceso se rigen por el motor de directivas de seguridad	21 %
Los datos se clasifican y etiquetan	21 %
Los archivos más confidenciales están protegidos de forma persistente con cifrado	20 %

No lo vimos como una serie de tecnologías, y sí como una estrategia y un enfoque para tratar todos los recursos de los usuarios, ya sea dentro o fuera de nuestra red, como no confiables hasta que se pudieran verificar".

Responsable de la toma de decisiones sobre seguridad de Estados Unidos

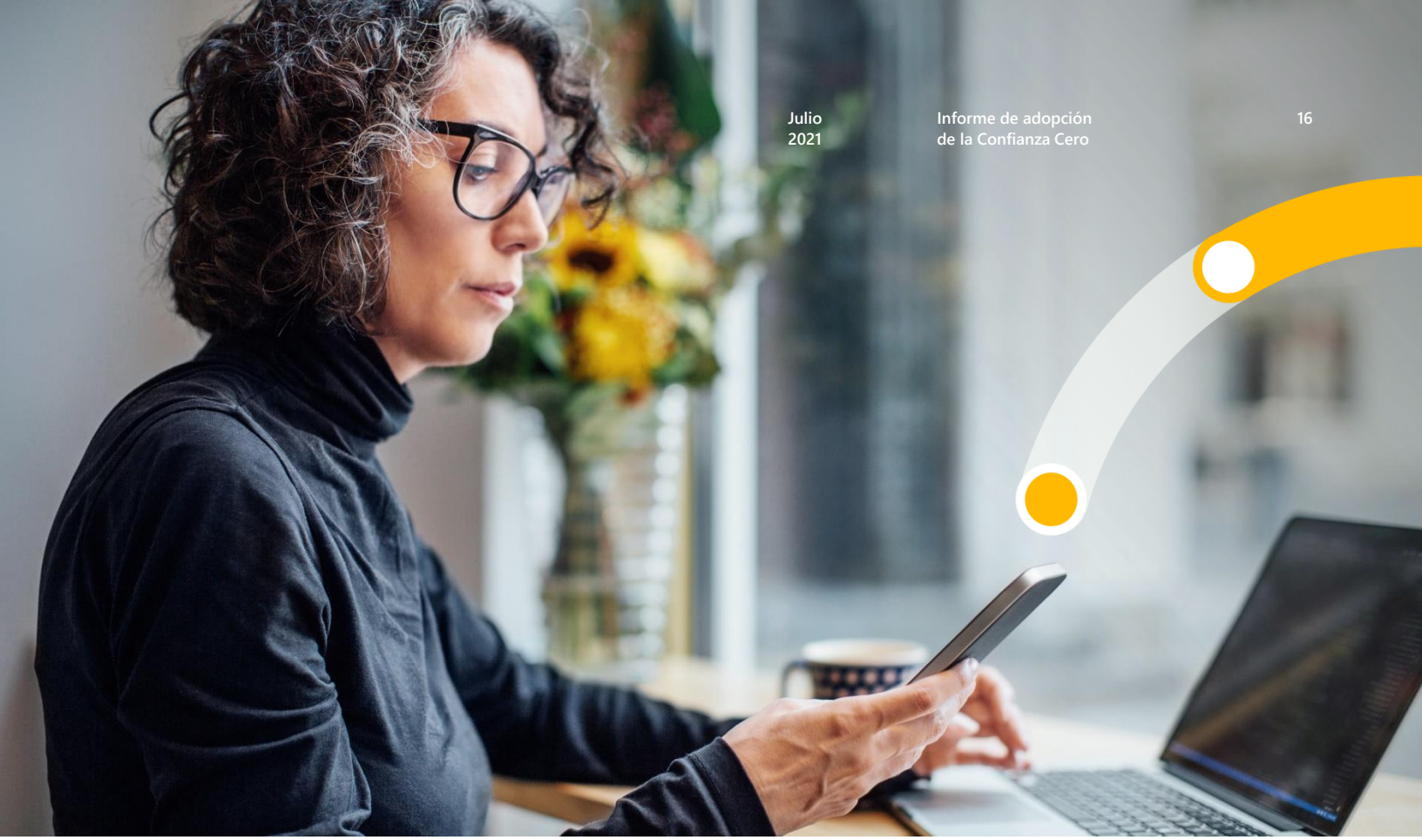
Hospitalidad

Una vez que las organizaciones comienzan a implementar una estrategia de Confianza Cero, los principales beneficios son una mayor agilidad, velocidad y protección; las ventajas de los recursos son menos comunes

Una vez implementada la estrategia de Confianza Cero, las organizaciones se benefician de una mayor agilidad (37 %), velocidad (35 %) y protección de los datos de los clientes (35 %). (Consulte el Anexo 8) Sin embargo, los beneficios directos para los empleados, como la liberación del equipo de seguridad (27 %) y la necesidad de menos recursos para administrar la infraestructura (22 %), son menos frecuentes.

Es importante destacar que las organizaciones creen que su estrategia de Cero Confianza les ayudará a administrar la mayoría de las amenazas y los cambios en el entorno, especialmente en lo que respecta a la seguridad de la IoT y la OT (47 %).

Anexo 8. Beneficios de la Confianza Cero



Las organizaciones se sienten seguras al sacar el máximo partido a su estrategia de Confianza Cero

El 79 % confía en su capacidad para hacer frente a las amenazas de seguridad en su conjunto, aunque esta confianza disminuye cuando la amenaza implica una fabricación de la verdad: los encargados de la toma de decisiones sobre seguridad se sienten menos seguros a la hora de hacer frente a las amenazas que implican identidades sintéticas (20 %) y "deepfakes" (10 %).

A la vista de los beneficios obtenidos, la Confianza Cero suele beneficiar a las asociaciones positivas. En los cuatro mercados, los responsables de la toma de decisiones sobre seguridad consideran que el enfoque de sus organizaciones es a la vez práctico y ambicioso, y lo describen como seguro (37 %) y eficiente (31 %), así como motivador (25 %), inspirador (25 %) y emocionante (25 %). En Japón, concretamente, los profesionales de la seguridad describen la Confianza Cero como exigente (27 %) y transformadora (25 %), lo que sugiere que, aunque no es fácil de aplicar, sus beneficios son de gran alcance una vez adoptada.

Muchos creen que están a la delantera con la implementación de la Confianza Cero, pero todavía les queda por hacer

Mientras que solo el 35 % de las organizaciones ha implementado por completo su estrategia de Confianza Cero, el 52 % señala que está por delante de donde planificaba estar y el 57 % cree que está por delante de otras organizaciones. Las organizaciones se consideran especialmente adelantadas a otras en Japón (66 %) y Australia/Nueva Zelanda (63 %). Aunque la confianza abunda en todos los mercados, parece haber un abismo entre la percepción y la realidad: entre los que se sienten por delante de otras organizaciones, solo el 42 % afirma haber aplicado con plenitud una estrategia de Confianza Cero. (Consulte el Anexo 9)

Si bien muchas organizaciones confían en su estrategia de Confianza Cero y se sienten preparadas para hacer frente a futuras amenazas de seguridad, aún queda mucho trabajo por hacer para implementar completamente todas las áreas de riesgo. Por ejemplo, entre las organizaciones que consideran que su estrategia de Confianza Cero está completamente implementada, en la actualidad casi la mitad no la ha implementado en las áreas de riesgo de seguridad, siendo la infraestructura y las identidades las que menos se han implementado.

Anexo 9. Comparación de la implementación de la Confianza Cero

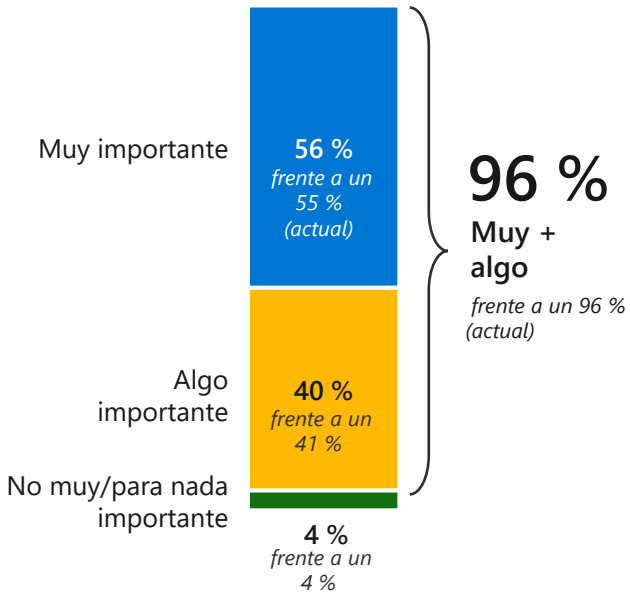
	Estados Unidos	Alemania	Japón	Australia/ Nueva Zelanda
Por delante	59 %	46 %	66 %	63 %
A la par	40 %	52 %	34 %	32 %
Por detrás	2 %	2 %	0 %	6 %

De cara a los próximos dos años, la estrategia de Confianza Cero continuará siendo una de las principales prioridades de seguridad

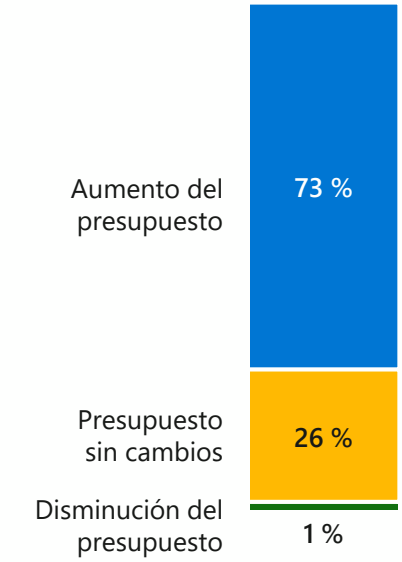
Las organizaciones se han sumado a la estrategia de Confianza Cero y los responsables de la toma de decisiones afirman que continuará siendo la principal prioridad de seguridad en los próximos dos años. Se proyecta que la importancia relativa de la estrategia de Confianza Cero como iniciativa de seguridad aumente (del 53 % al 58 %) para 2023, ya que los responsables de la toma de decisiones de seguridad prevén que la estrategia continuará siendo fundamental para el éxito general (96 %). (Consulte el Anexo 10)

La importancia prevista es especialmente alta entre las organizaciones japonesas, ya que el 70 % afirma que la estrategia de Confianza Cero será muy importante en los próximos dos años, en comparación con el promedio general del 56 %. También se espera que los presupuestos de la estrategia de Confianza Cero crezcan, ya que el 73 % de las organizaciones espera aumentar sus presupuestos. Aunque esta cifra es ligeramente inferior en Alemania (67 %), donde el 31 % prevé que sus presupuestos se mantendrán sin cambios. (Consulte el Anexo 11)

Anexo 10. Importancia prevista de la Confianza Cero en los próximos dos años

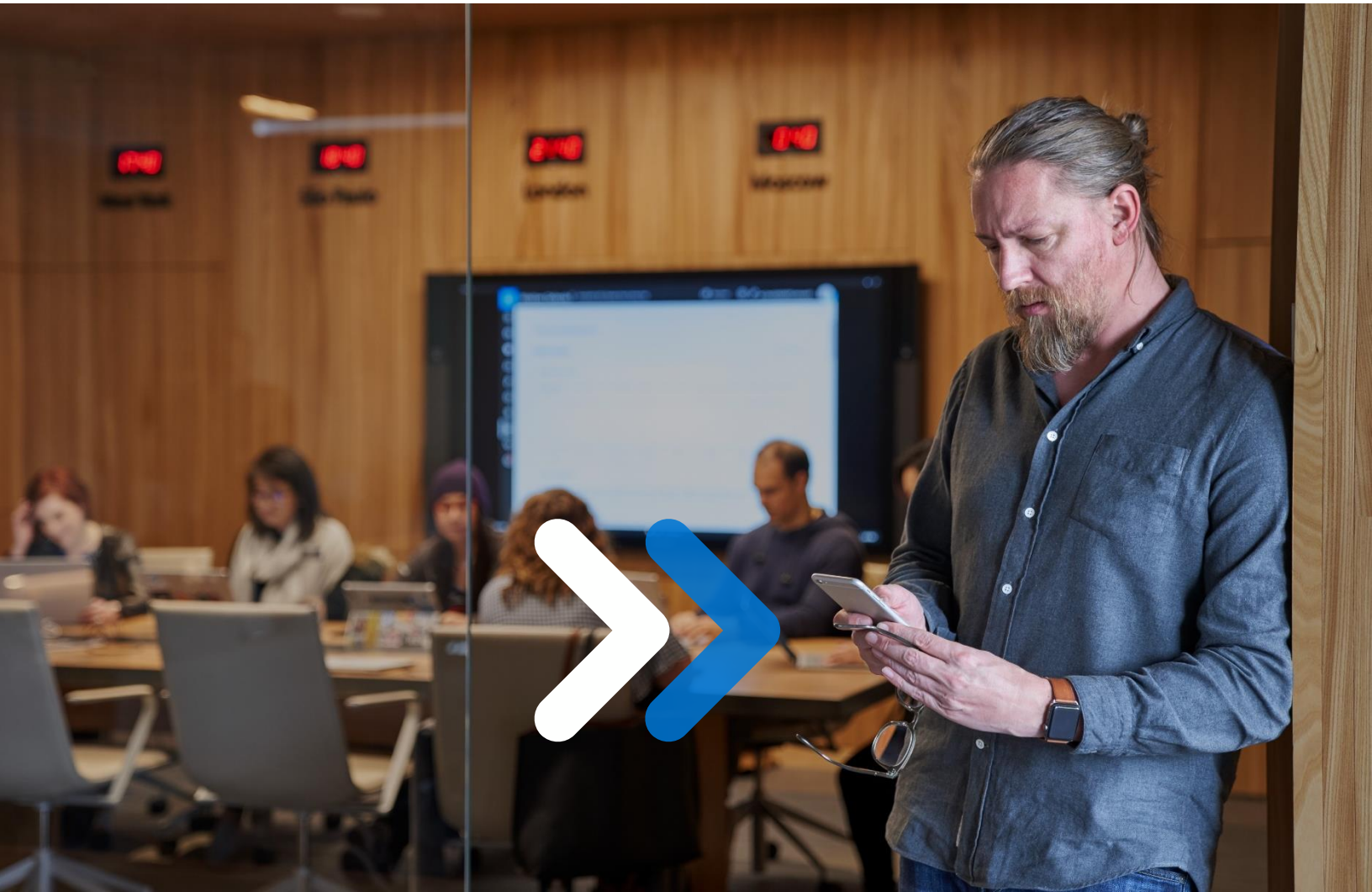


Anexo 11. Importancia prevista del presupuesto de Confianza Cero en los próximos dos años



Demostrar el éxito de la estrategia de Confianza Cero podría impulsar nuevas inversiones

Las organizaciones que han adoptado con entusiasmo la Confianza Cero esperan duplicar su inversión en los próximos dos años, y las que aún no han empezado a adoptarla corren el riesgo de quedarse más atrás. Estas organizaciones no solo están a la zaga de sus contrapartes completamente implementadas cuando se trata de priorizar la Confianza Cero en sus planes de seguridad (42 % frente a un 66 %) y de prever aumentos de presupuesto (66 % frente a un 72 %), sino que también se sienten significativamente menos seguras a la hora de administrar la IoT y la seguridad de OT en el futuro (40 % frente a un 53 %).



Superar los desafíos con los empleados será clave para duplicar la inversión en Confianza Cero

A pesar de los rápidos avances en la adopción de la estrategia de Confianza Cero, las organizaciones deben superar un sinfín de desafíos si quieren continuar avanzando en su implementación. (Consulte el Anexo 12) Los desafíos de recursos y liderazgo son los más frecuentes dentro de estas categorías. El tiempo necesario para aplicar las estrategias de Confianza Cero y la falta de apoyo por parte de los directivos encabezan la lista de obstáculos, destacándose este último especialmente en Australia/Nueva Zelanda (65 %).

Además, las limitaciones presupuestarias (que el 45 % de las organizaciones identifican como un obstáculo) probablemente también desempeñan un papel en los desafíos de recursos y liderazgo.

Por ejemplo, el 21 % de los responsables de la toma de decisiones de seguridad citan las dificultades para demostrar el ROI de una inversión en Confianza Cero como una barrera para la implementación, un desafío que puede llevar a la falta de aceptación por parte de la dirección. Debido a que los mercados no estadounidenses tienen más probabilidades de tener limitaciones presupuestarias (el 60 % de las organizaciones en Japón; el 57 % de las organizaciones en Alemania, el 57 % de las organizaciones en Australia/Nueva Zelanda), es posible que esto tenga un efecto dominó, que lleve a una menor y más lenta implementación de las estrategias de Confianza Cero en Japón, Alemania y Australia/Nueva Zelanda en comparación con Estados Unidos.

Anexo 12. Barreras de la Confianza Cero

Desafíos de recursos 60 %	Liderazgo 53 %	Tecnológicas 46 %	Proveedor 46 %	Restricciones presupuestarias 45 %
20 % Tarda mucho en aplicarse	**20** % Falta de apoyo por parte de la dirección general de la empresa	**21** % Dificultad para integrar soluciones de seguridad	**21** % Requiere soporte de implementación de los proveedores	**21** % Costo de implementar una estrategia de Confianza Cero
19 % Falta de administración del cambio interno	**19** % Falta de apoyo de las partes interesadas	**19** % Incompatibilidad con los sistemas heredados	**21** % Dificultad para identificar a los proveedores correctos	**21** % Dificultad para demostrar el ROI
18 % Requiere más materiales educativos	**19** % Requiere ayuda para plantear un argumento comercial convincente	**19** % Dificultad para escalar en toda la organización	**17** % Incapacidad para hallar socios innovadores	**14** % No cuenta con un presupuesto lo suficientemente grande
17 % No es necesaria para una organización de nuestro tamaño	**18** % Falta de aceptación de la organización			
16 % No tiene el talento adecuado para implementar correctamente				

“ La aceptación inicial fue un reto, pero una vez que acordamos como partes interesadas que íbamos a invertir en este proyecto, todo el mundo estuvo de acuerdo”.

Responsable de la toma de decisiones sobre seguridad de Estados Unidos

FinTech

Los responsables de la toma de decisiones sobre seguridad tienen una leve inclinación por los proveedores integrales o consolidados

Cuando se trata de la estrategia de proveedores de Confianza Cero, las organizaciones se enfrentan a la posibilidad de adoptar un enfoque de "lo mejor del conjunto" o de "lo mejor en su clase". La primera estrategia implica la adquisición de un conjunto de productos para toda la arquitectura de Confianza Cero de un proveedor integral o consolidado, una solución que, según los responsables de la toma de decisiones sobre seguridad, ofrece más experiencia, recursos y simplicidad para aquellos que no disponen de recursos internos. Sin embargo, este enfoque plantea problemas como el aumento de la vulnerabilidad y la falta de flexibilidad. (Consulte el Anexo 13)

Esta última estrategia, la mejor en su clase, consiste en obtener componentes tecnológicos individuales de Confianza Cero de proveedores especializados. A diferencia de lo mejor del conjunto, esta estrategia se apoya en proveedores especializados en diferentes áreas, por lo que ofrece mayor flexibilidad y puede alinearse más con la estrategia de la organización. Sin embargo, los profesionales de la seguridad consideran que las mejores soluciones en su clase son más costosas, que requieren más recursos y que impiden la visibilidad, inconvenientes que, en última instancia, provocan problemas presupuestarios y de proveedores. (Consulte el Anexo 14)

Aunque las organizaciones están muy divididas, una ligera mayoría de los responsables de la toma de decisiones sobre seguridad (55 %) prefiere trabajar con los proveedores integrales (lo mejor del conjunto). (Sin embargo, las organizaciones en Australia/Nueva Zelanda se inclinan en la dirección opuesta, con un 52 % que prefiere la mejor en su clase).

Anexo 13. Beneficios y barreras del enfoque "lo mejor del conjunto": clasificados en las 2 primeras posiciones

⊕ Beneficios del enfoque "lo mejor del conjunto"	
El proveedor tiene experiencia en soluciones específicas de la industria	24 %
Más recursos disponibles para ayudar a planificar la estrategia de Confianza Cero	23 %
Simplificación de la pila de seguridad	22 %

⊖ Inconvenientes del enfoque "lo mejor del conjunto"	
La dependencia de un solo proveedor aumenta la vulnerabilidad	34 %
Requiere una integración más compleja con la arquitectura heredada	33 %
Menos flexibilidad para el funcionamiento especializado	29 %

Anexo 14. Beneficios y barreras del enfoque "lo mejor en su clase": clasificados en las 2 primeras posiciones

⊕ Beneficios del enfoque "lo mejor en su clase"	
Flexibilidad para buscar las mejores soluciones para cualquier componente de la estrategia de Confianza Cero	33 %
Puede alinear más estrechamente la solución con la arquitectura o estrategia de mi organización	30 %
Mayor oportunidad de innovar con diversos proveedores	26 %

⊖ Inconvenientes del enfoque "lo mejor en su clase"	
Mayores costos	29 %
Incapacidad para compartir datos a través de las diferentes soluciones	26 %
Alto volumen de soluciones para que los equipos internos adopten y administren	26 %

Conclusión

A medida que los riesgos de seguridad se tornan no solo más frecuentes, sino más nefastos, las organizaciones de todos los mercados e industrias están optando por una estrategia de Confianza Cero que nos guía a "nunca confiar, siempre comprobar". La estrategia de Confianza Cero es la máxima prioridad en materia de seguridad para las organizaciones que pretenden mejorar su postura general de seguridad, la experiencia del usuario final y la productividad, simplificar los procedimientos de seguridad para los empleados y reducir los costos. Sin embargo, aunque los beneficios de una estrategia de Confianza Cero están bien establecidos, la limitación de recursos y el escepticismo de los líderes impiden su aplicación universal.

La adopción de la estrategia de Confianza Cero se ha acelerado en los últimos tres años, en parte debido a la pandemia de COVID-19. En esencia, el cambio a lugares de trabajo remotos e híbridos está impulsando una mayor adopción de enfoques de Confianza Cero, que prometen proteger los sistemas y los datos incluso cuando los empleados acceden a ellos fuera de las instalaciones, a veces en dispositivos personales. La adopción acelerada debido a la COVID es un buen indicador de la preparación para la Confianza Cero en general, ya que las organizaciones que adoptaron la estrategia durante la pandemia la implementaron en más áreas de riesgo de seguridad que sus contrapartes.

Dicho esto, incluso los más avanzados en la adopción de la estrategia de Cero Confianza tienen trabajo por hacer, y las percepciones erróneas de las organizaciones sobre su propia madurez de Cero Confianza pueden dejar a algunos con vulnerabilidades que ni siquiera saben que tienen.

La mayoría de las organizaciones de todos los mercados creen que la importancia de una estrategia de Confianza Cero aumentará con el tiempo y esperan que sus presupuestos aumenten a su vez. Este cambio de prioridad previsto es especialmente crucial para los mercados no estadounidenses, en los que las preocupaciones presupuestarias son obstáculos importantes para la adopción. Esforzarse por una implementación completa puede ser financiera y logísticamente abrumador; aun así, los beneficios de un enfoque de Confianza Cero son innegables, y Microsoft estará allí para guiar y apoyar a las organizaciones mientras se embarcan en esta frontera floreciente.

Para obtener más información sobre la Confianza Cero y evaluar la madurez de la Confianza Cero de su organización, visite

aka.ms/zerotrust

Objetivos detallados de la investigación y reclutamiento del público

Los objetivos de la investigación eran:

1. Comprender el estado actual de los enfoques de Confianza Cero
2. Descubrir la mentalidad, los procedimientos recomendados, los beneficios y los desafíos de la adopción de enfoques de Confianza Cero
3. Explorar el futuro de los enfoques de Confianza Cero
4. Contextualizar las innovaciones y tendencias en los enfoques de Confianza Cero

Para cumplir con los criterios de evaluación, los responsables de la toma de decisiones sobre seguridad debían:

Ser responsables de la seguridad en su organización, incluida la ciberseguridad, las operaciones de seguridad, la protección contra amenazas, la administración de identidades, la administración de riesgos, la seguridad de las aplicaciones, el análisis forense digital y la respuesta ante incidentes

Ser empleados a tiempo completo en una empresa de gran tamaño (más de 1000 empleados en los EE. UU.; más de 500 empleados en Alemania, Japón, Australia o Nueva Zelanda)

Tener entre 25 y 75 años

Familiarizado con la Confianza Cero

Participar en la toma de decisiones para el desarrollo/implementación de estrategias de Confianza Cero

De los 911 responsables de la toma de decisiones sobre seguridad entrevistados para la oleada de investigación en abril de 2021:

En los Estados Unidos, se entrevistó a 477 responsables de la toma de decisiones sobre seguridad

En Alemania, se entrevistó a 201 responsables de la toma de decisiones sobre seguridad

En Australia/Nueva Zelanda, se entrevistó a 126 responsables de la toma de decisiones sobre seguridad

En Japón, se entrevistó a 107 responsables de la toma de decisiones sobre seguridad

Nota: La investigación se llevó a cabo durante la pandemia mundial de COVID-19, que se encontraba en diferentes etapas de escalada/contención