ivanti

Cybersecurity
INSIDERS

Informe de progreso de Confianza cero 2021

ivanti.es

Visión general

La adopción por parte de las empresas del modelo de seguridad de confianza cero está ganando impulso, ya que la mayoría de las organizaciones pretenden implementar capacidades de confianza cero para mitigar el creciente riesgo cibernético, especialmente a raíz del cambio masivo al teletrabajo. Con su principio de verificación del usuario y del dispositivo antes de conceder un acceso condicional basado en el menor privilegio, la confianza cero promete mejorar significativamente la usabilidad, la protección de los datos y la gobernanza.

El informe de confianza cero de 2021 revela cómo las empresas están implementando la seguridad de confianza cero en sus organizaciones, incluyendo los principales impulsores, las tendencias de adopción, las tecnologías, las inversiones y los beneficios.

Para obtener esta información, hemos encuestado a profesionales de la ciberseguridad, desde ejecutivos técnicos hasta profesionales de la seguridad informática, que representan una muestra equilibrada de organizaciones de distintos tamaños en múltiples sectores.

Las principales conclusiones son:

- La confianza se gana mediante la verificación de las entidades incluyendo usuarios, dispositivos y componentes de infraestructura (64%) encabezando la lista de componentes de la confianza cero. Le siguen la protección de datos (63%) y la autenticación/autorización (61%);
- Determinar los privilegios de acceso actuales para todos los usuarios puede ser una tarea desalentadora para asegurarse de que los usuarios están limitados a los niveles de acceso adecuados. Más de 3/4 de las organizaciones (88 %) reconocen que los usuarios pueden tener privilegios de acceso más allá de lo que necesitan;
- Cuando se les preguntó por sus prioridades actuales en materia de seguridad los profesionales de la ciberseguridad mencionaron la mejora de la IAM (68 %) seguida de la de la pérdida de datos (56 %) y el acceso seguro a las aplicaciones (46 %).

Muchas gracias a Ivanti por dar apoyo a este importante proyecto de investigación.

Esperamos que este informe le resulte informativo y útil para seguir protegiendo sus entornos informáticos.

Gracias.

Holger Schulze

Holger Schulze
Director general y fundador
Cybersecurity Insiders

Cybersecurity INSIDERS

Fundamentos de la confianza cero

Hemos preguntado a las organizaciones qué aspectos de la confianza cero les parecen más interesantes. La confianza obtenida a través de la verificación de las entidades, incluidos los usuarios, los dispositivos y los componentes de la infraestructura (64 %), encabeza la lista de componentes básicos de la confianza cero. Le siguen la protección de datos (63 %) y la autenticación/autorización continua (61 %).

¿Qué principios de confianza cero son más convincentes para usted y su empresa?[1]

64%

Confianza obtenida mediante la verificación de la entidad
(por ejemplo, usuario, dispositivo, infraestructura)

63%

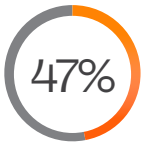
Protección de datos
(por ejemplo, conexión segura)

61%

Autenticación/ autorización continua

Visibilidad y auditoría de los accesos de extremo a

Facilitar el acceso con menos privilegios



47 % Política de acceso centralizada y granular

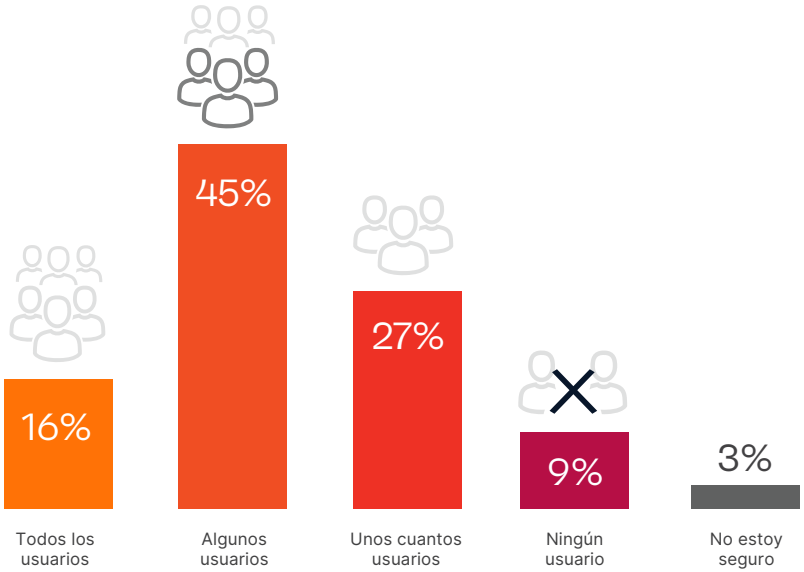
No hay distinción de confianza entre red interna o externa

Privilegios de acceso excesivo

Determinar los privilegios de acceso actuales para todos los usuarios puede ser una tarea desalentadora para asegurarse de que los usuarios están limitados a los niveles de acceso adecuados. Más de 3/4 de las empresas (88 %) admiten que los usuarios pueden tener privilegios de acceso más allá de lo que requieren.

¿Hasta qué punto cree que los usuarios de su empresa tienen privilegios de acceso más allá de lo que requieren?

El 88% reconoce que los usuarios pueden tener privilegios de acceso más allá de lo que requieren



Prioridades de seguridad

Cuando se les preguntó por sus prioridades actuales en materia de seguridad, los profesionales de la ciberseguridad mencionaron la mejora de la IAM (68%), seguida de la prevención de la pérdida de datos (56%) y el acceso seguro a las aplicaciones (46%).

¿Cuáles son las prioridades actuales de su empresa en materia de seguridad?[2]

68%

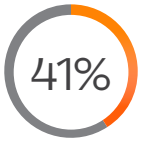
Mejorar la administración de identidad y acceso (IAM)

56%

Prevención de la pérdida de datos (DLP)

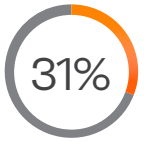
46%

Garantizar el acceso seguro a las aplicaciones alojadas en proveedores de servicios en la nube
(por ejemplo, Microsoft, Amazon, Google)



Habilitar la gestión móvil de puntos finales (EMM)/BYOD
(por ejemplo, usuarios, dispositivos)

Llevar a cabo una inspección profunda de SSL
(por ejemplo, descifrar la sesión segura para el escaneo del programa malignoy el filtrado de web/correo electrónico)



Simplificar el suministro de acceso seguro
(por ejemplo, la experiencia del usuario, la administración)

umentar o sustituir las herramientas de acceso remoto existentes
(por ejemplo, VDI, VPN, RDP)

Acceso a la identidad y prioridades de confianza cero

Hemos preguntado a las empresas en qué controles de seguridad de acceso a la identidad y de confianza cero están invirtiendo. La prioridad, desde el punto de vista de la inversión, es la autenticación multifactor (58 %), seguida de la gestión de la identidad la gobernanza (48 %) y el inicio de sesión único (45 %).

¿Cuál de los siguientes controles de acceso a la identidad/de cero confianza prioriza para invertir en su empresa en los próximos 12 meses?[3]

58%

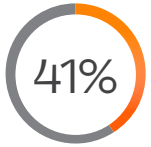
Autenticación multifactorial (MFA)

48%

Gestión y gobierno de la identidad

45%

Inicio de sesión único (SSO)



Gestión de acceso privilegiado (PAM), microsegmentación

Redes privadas virtuales (VPN)

Microsegmentación

Control de acceso a la red (NAC), cortafuegos de aplicaciones web (WAF)

Prioridades de acceso seguro

Cuando profundizamos en las prioridades específicas de acceso seguro, las empresas vuelven a dar prioridad a la autenticación multifactor y a la gestión de cuentas privilegiadas (69%). Le siguen la detección de actividades anómalas y la respuesta a las mismas (58 %), y la protección del acceso desde dispositivos personales no gestionados (55 %).

¿Cuáles son las prioridades de su empresa en materia de acceso seguro para los próximos uno o dos años?

69%

Autenticación multifactorial/ gestión de cuentas privilegiadas

58%

Detección y respuesta a actividades anómalas

55%

Asegurar el acceso desde dispositivos personales no gestionados

Reevaluar la infraestructura de seguridad heredada y considerar el acceso definido por software

Mayor visibilidad y métricas de seguridad para los ejecutivos

Microsegmentación

Retos del acceso seguro

La principal preocupación en cuanto a la seguridad del acceso a las aplicaciones y los recursos es el acceso con exceso de privilegios (60 %), seguido de proporcionar un acceso seguro a los socios (50 %); ambos retos se abordan directamente con la confianza cero.

¿Cuáles son los principales retos a los que se enfrenta su empresa a la hora de asegurar el acceso a las aplicaciones y los recursos?

60%

Acceso de los empleados con exceso de privilegios

50%

Pde los socios accede a aplicaciones y recursos de forma insegura

47%

Ciberataques
(por ejemplo, denegación de servicio, 'scripting' entre sitios, ataque de intermediario, 'phishing')

TI en la sombra

Los procesos manuales son complejos y ralentizan la capacidad de reacción rápida

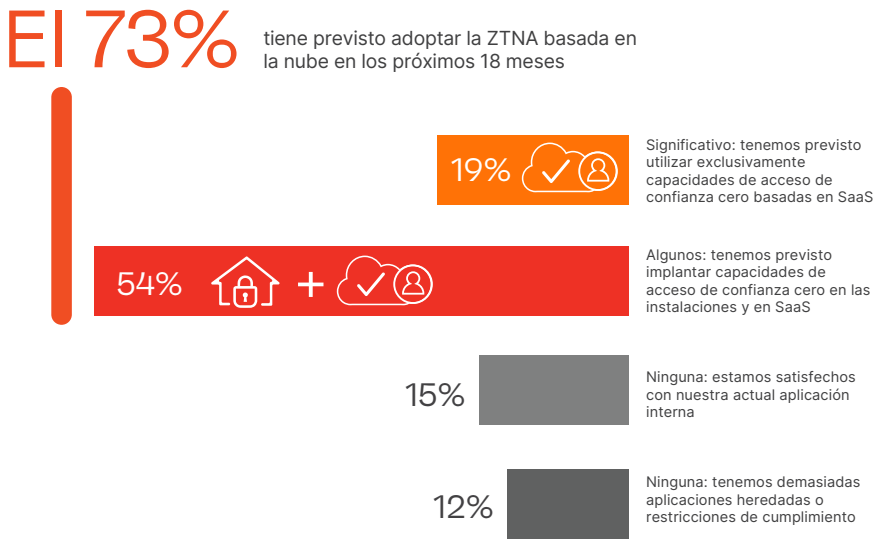
Dispositivos móviles vulnerables, con 'jailbreak' o perdidos que acceden a los recursos

Dispositivos de riesgo que acceden a los recursos de la red
(puntos finales desconocidos, no autorizados, no conformes)

SAAS de confianza cero

La seguridad se está trasladando a la nube, y la ZTNA no es una excepción. Casi tres cuartas partes de los encuestados tienen previsto adoptar una solución ZTNA basada en la nube en los próximos 18 meses.

En los próximos 18 meses, ¿en qué medida tienen usted y su empresa previsto trasladar las capacidades de acceso de confianza cero a SaaS?



Acceso a aplicaciones privadas

Hemos consultado a las empresas sobre sus mayores retos a la hora de proteger las aplicaciones privadas. Para más de la mitad de los encuestados, el acceso seguro a las aplicaciones desplegadas en entornos de nube pública es la mayor preocupación actual (54 %).

Cuando se trata de asegurar el acceso a las aplicaciones privadas, por favor, clasifique lo siguiente en términos de su mayor desafío actual.

54% Acceso a aplicaciones en la nube pública

29% Acceso a aplicaciones en mi centro de datos

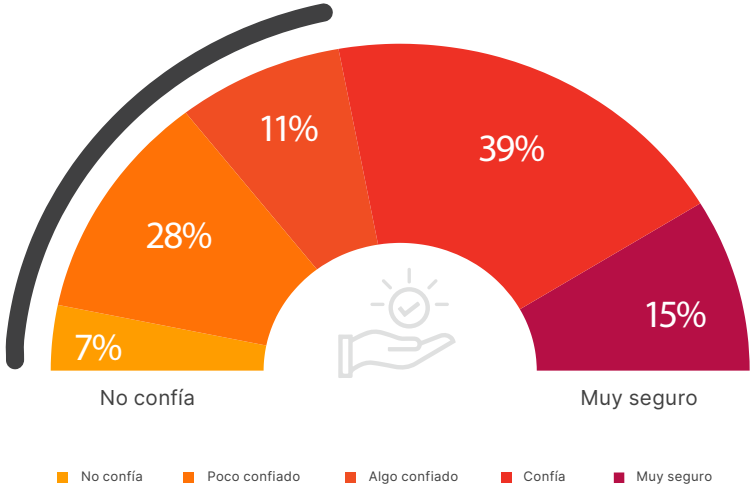
17% Acceso a las aplicaciones en mi oficina central

Confianza cero

Cuando se les pregunta por su confianza en la capacidad de aplicar la confianza cero, casi la mitad de los equipos de seguridad informática de las empresas carecen de confianza (46 %).

¿Qué confianza tiene en aplicar un modelo/redes de confianza cero en su arquitectura de acceso seguro?

El 46% de los equipos de seguridad informática de las empresas no confían en su capacidad para ofrecer confianza cero



Acceso a las aplicaciones en las nubes públicas

Las soluciones tradicionales de acceso remoto no satisfacen los requisitos de los actuales entornos dinámicos y distribuidos de la nube. Cuando se pregunta a los profesionales de la ciberseguridad sobre las situaciones que encuentran al proporcionar un acceso seguro, la solución más mencionada es la de hacer pasar a los usuarios remotos y móviles por los centros de datos para acceder a las nubes de aplicaciones públicas (47 %). Un alarmante 37 % tiene que exponer públicamente las aplicaciones en la nube para permitir a los usuarios remotos y móviles, introduciendo así un riesgo significativo.

¿Con cuál de los siguientes escenarios se ha encontrado a la hora de proporcionar un acceso seguro a las aplicaciones de la nube pública para los usuarios remotos o móviles?

47%

Me veo obligado a hacer pasar a los usuarios remotos por mi(s) centro(s) de datos para acceder a las aplicaciones en la nube pública

37%

Tengo que exponer públicamente mis aplicaciones privadas en la nube pública para proporcionar acceso

35%

No puedo implementar mi dispositivo VPN remoto preferido en entornos de nube pública

Impulsores de la confianza cero

¿Qué motiva a las organizaciones a iniciar o construir una postura de confianza cero? La seguridad de los datos encabeza la lista con un 82 %, seguida de la prevención de infracciones (68 %) y la reducción de las amenazas a los puntos finales (53 %).

¿Cuáles son los impulsores clave para que su organización inicie o aumente una postura de acceso a la identidad/confianza cero?[4]

82%

Seguridad/protección de datos

68%

Prevención de infracciones

53%

Reducir las amenazas a la seguridad de los puntos finales y del IoT

Reducir las amenazas internas

Cumplimiento de la industria/regulación (por ejemplo, HIPAA, GDRP, PCI DSS)

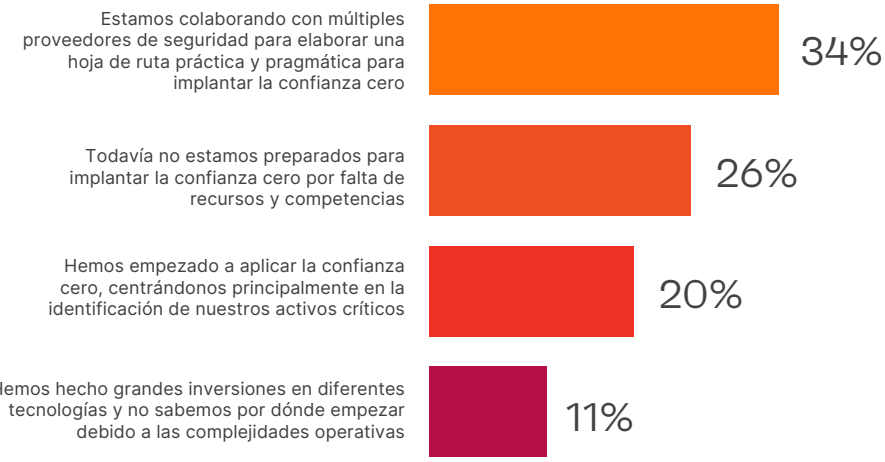
Abordar los problemas de seguridad de las TI híbridas

Eficiencia operativa

Aplicación de la confianza cero

La confianza cero está ganando rápidamente impulso y las empresas están tomando diferentes caminos en la implementación de la tecnología. El enfoque más común que adoptan las organizaciones es asociarse con múltiples proveedores de seguridad para construir una hoja de ruta práctica y pragmática para implementar la confianza cero (34%). Sin embargo, la falta de recursos y conocimientos necesarios (26%) sigue siendo un obstáculo importante para la confianza cero.

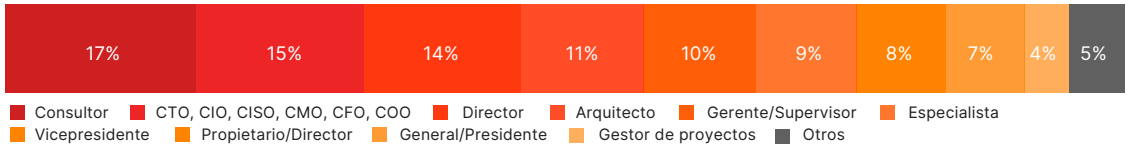
Si la implantación de la confianza cero es un proceso gradual, ¿cómo piensa implantar la confianza cero en su entorno ampliado?[5]



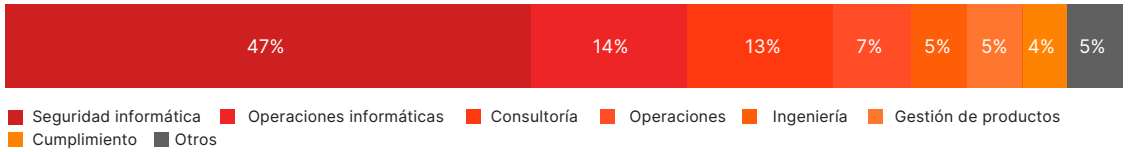
Metodología y datos demográficos

Este informe se basa en los resultados de una exhaustiva encuesta en línea realizada en julio de 2021 a 443 profesionales de la informática y la ciberseguridad en Estados Unidos, con el fin de identificar las últimas tendencias de adopción por parte de las empresas, los retos, las carencias y las preferencias de soluciones relacionadas con la seguridad de confianza cero. Los encuestados van desde ejecutivos técnicos hasta profesionales de la seguridad de TI, representando una sección transversal equilibrada de organizaciones de diferentes tamaños en múltiples industrias.

Nivel profesional

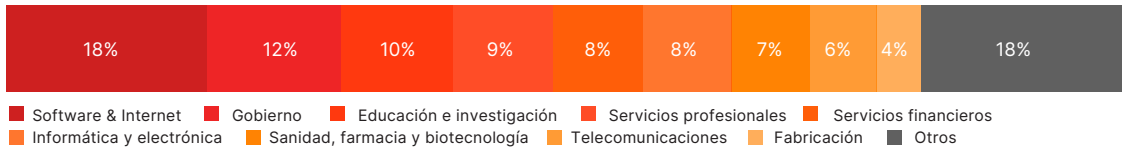


Departamento



Tamaño de la empresa

Industria



ivanti

ivanti.es
+34 91 049 66 76
contact@ivanti.es

Ivanti hace que sea posible trabajar desde “cualquier parte”. En el lugar de trabajo “en cualquier parte”, los empleados utilizan una enorme cantidad de dispositivos para acceder a aplicaciones y datos de TI a través de varias redes para seguir siendo productivos mientras teletrabajan.

La plataforma de automatización Ivanti Neurons conecta las soluciones líderes del sector de gestión unificada de puntos finales, seguridad de confianza cero y gestión de servicios empresariales, ofreciendo una plataforma de TI unificada que permite a los dispositivos autorestablecerse y autoprotegerse y capacita a los usuarios para el autoservicio. Más de 40.000 clientes, entre los que se encuentran 78 de la lista Fortune 100, confían en Ivanti para descubrir, gestionar, proteger y dar servicio a sus activos de TI desde la nube hasta el extremo y ofrecer excelentes experiencias de usuario final a los empleados, dondequiera y comoquiera que trabajen. Para más información, entre en ivanti.es y siga a @GoIvanti.

1. Segregación de recursos 40% | Otros 2%
2. Complementar la detección y respuesta de puntos finales (EDR) 28 % | Mejorar las funciones de seguridad de la SD-WAN 27 % | Mejorar la corrección de vulnerabilidades (por ejemplo, gestión de vulnerabilidades, gestión de parches)
   5 % | Proporcionar una mejor protección contra amenazas móviles (defensa contra amenazas móviles/antiphishing) 2 % | Ninguna 2 % | Otras 4 %
3. Cortafuegos de aplicaciones web (WAF) 35 % | Gestión de dispositivos móviles de la empresa (MDM) 31 % | Cloud Access Security Broker (CASB) 30 % | Análisis de identidades 27 % | Perímetro definido por software (SDP) 26 % | Servicios de directorio de la empresa 17 % | Control total sobre el acceso a la red de confianza cero 12 % | Gestión de la vulnerabilidad/ gestión de parches 9 % | Invisibilidad de los dispositivos de red ante las amenazas 7 % | Antiphishing 7 % | Defensa contra amenazas móviles 5 % | Otros 2 %
4. Cumplimiento interno 28 % | Respuesta a una auditoría o a un incidente de seguridad 28 % | Otros 5 %
5. Otros 9 %