ivanti

Informe de Progreso de Confianza Cero 2020

Cybersecurity Insiders

Visión general

Las filtraciones de datos van en aumento, lo que revela que ninguna organización es inmune a los ciberataques. Una de las causas es que la movilidad de los trabajadores y la computación en la nube han colocado la mayoría de las cargas de trabajo fuera del refugio de las redes corporativas y de la defensa perimetral tradicional. La adopción por parte de las empresas del modelo de seguridad Zero Trust (en adelante, "confianza cero") está creciendo como parte de las iniciativas clave para mitigar el riesgo cibernético. Con su principio de verificación del usuario, del dispositivo y de la infraestructura antes de conceder un acceso condicional basado en el mínimo privilegio, la confianza cero promete mejorar considerablemente la usabilidad, la protección de datos y la gobernanza. Este informe de Progreso de Confianza Cero 2020 muestra cómo las empresas están implementando la seguridad de confianza cero en sus compañías y expone los principales impulsores, la adopción, las tecnologías, las inversiones y los beneficios.

El Informe de Progreso de Confianza Cero 2020 cuenta con la participación de más de 400 responsables de la toma de decisiones en materia de ciberseguridad, desde ejecutivos técnicos hasta profesionales de la seguridad TI, y representando una sección equilibrada de organizaciones de diferentes tamaños en múltiples industrias. Mientras que el 72 % de las organizaciones planean evaluar o implementar capacidades de confianza cero en alguna capacidad en 2020 para mitigar el creciente riesgo cibernético, casi la mitad (47 %) de los profesionales de la ciberseguridad no confían en aplicar un modelo de confianza cero a su arquitectura de Acceso Seguro.

Las principales conclusiones son:

- Confianza y falta de confianza casi iguales en la aplicación del modelo de confianza cero en su arquitectura de acceso seguro (el 53 % tiene confianza, el 47 % no tiene confianza);
- El 53 % tiene previsto trasladar las capacidades de acceso de confianza cero a una implementación de TI híbrida;
- Más del 60 % considera que los principios de confianza cero de autenticación y autorización continuas, la confianza ganada a través de la verificación de la entidad y la protección de los datos son los más convincentes para su organización;
- Más del 40 % ha revelado que la gestión de privilegios, el acceso inseguro de los socios, los ciberataques, los riesgos de la TI en la sombra y el acceso vulnerable a los recursos de los dispositivos móviles y de riesgo son los principales retos para el acceso seguro a las aplicaciones y los recursos;
- El 45 % está preocupado por la seguridad del acceso a las aplicaciones de la nube pública, y el 43 % por las exposiciones del BYOD;
- El setenta por ciento de las organizaciones planea avanzar en sus capacidades de gestion de identidades y accesos;
- El treinta por ciento de las organizaciones busca simplificar la entrega de acceso seguro, incluyendo la mejora de la experiencia del usuario y la optimización de la administración y el aprovisionamiento;
- El 41 % quiere reevaluar su infraestructura de acceso seguro y considerar la posibilidad de un perímetro definido por software (SDP); la mayoría requiere una implementación de TI híbrida y una cuarta parte adopta una implementación de SaaS.

Muchas gracias a Ivanti por apoyar este importante proyecto de investigación.

Esperamos que este informe le resulte informativo y útil para continuar con sus esfuerzos de protección de sus entornos de TI.

Gracias,

Holger Schulze

Principios de la confianza cero

¿Qué principios del paradigma de la confianza cero son los más convincentes para las organizaciones? La autenticación/autorización continua encabeza la lista como componente central de la propuesta de valor de confianza cero, con un 67 %. Le siguen la confianza obtenida a través de la verificación de las entidades, incluidos los usuarios, los dispositivos y los componentes de la infraestructura (65 %), y la protección de los datos (por ejemplo, la conexión segura) (63 %).

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

67%

Autenticación / autorización continua

65%

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

63%

Protección de datos (por ejemplo, conexión segura)

Visibilidad y auditoría de los accesos de extremo a extremo

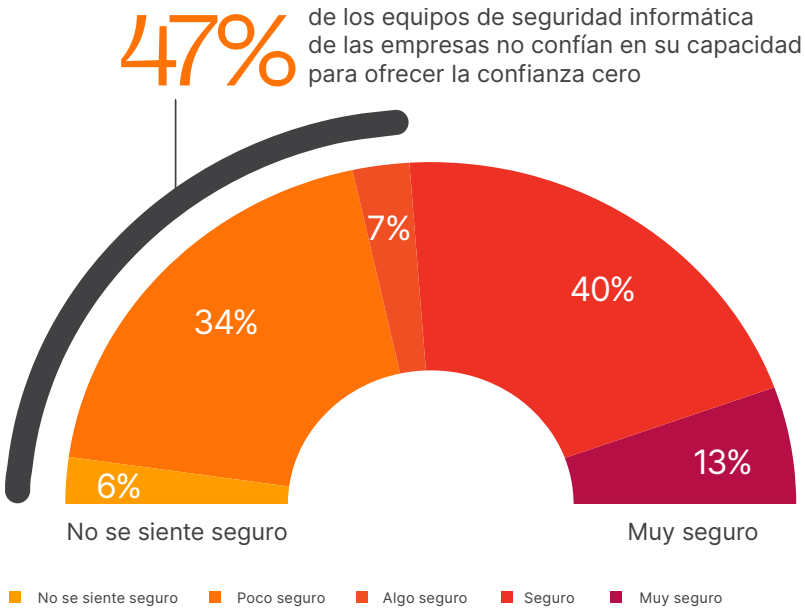
Facilitar el acceso con menos privilegios

Política de acceso centralizada y granula

Confianza cero

Mientras que el 53 % de las organizaciones confía en su capacidad para implantar la confianza cero en su arquitectura de acceso seguro, más del 40 % de los equipos de seguridad informática de las empresas no confían en su capacidad para ofrecer la confianza cero..

¿En qué medida confía en aplicar los principios del modelo de confianza cero en su arquitectura de acceso seguro?



Impulsores de la confianza cero

¿Qué motiva a las organizaciones a iniciar o desarrollar un programa de confianza cero? La seguridad de los datos encabeza la lista con un 85 %, seguida de la prevención de infracciones (70%) y la reducción de las amenazas a los puntos finales (56 %). Más allá del cumplimiento de la industria, de la normativa y del cumplimiento interno, casi un tercio de las empresas quieren abordar los problemas de seguridad de las TI híbridas.

¿Cuáles son los factores clave para que su organización inicie o aumente un programa de gestion de acceso a la identidad/ confianza cero?[2]

85%

Seguridad / Protección de datos

70%

Prevención de la infracción

56%

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

Reducir las amenazas internas

Cumplimiento de la industria / reglamentación (e.g. HIPAA, GDRP, PCI DSS)

Cumplimiento interno

Retos del acceso seguro

¿Cuáles son los principales retos a los que se enfrentan las organizaciones a la hora de asegurar el acceso? Los empleados con privilegios excesivos (62%), el acceso de los socios a los recursos sensibles (55%) y el acceso a los recursos de los dispositivos móviles vulnerables y de riesgo (49%) son los retos más mencionados por las organizaciones.

¿Cuáles son los principales retos a los que se enfrenta su organización a la hora de asegurar el acceso a las aplicaciones y los recursos?[3]

62%

Acceso sobreprivilegiado de los empleados

55%

Socios que acceden a aplicaciones y recursos de forma insegura

49%

Móviles vulnerables y dispositivos de riesgo acceso a recursos (desconocido, no sancionado, no conformes, puntos finales perdidos)

ciberataques (por ejemplo, denegación de servicio, secuencias de comandos en sitios cruzados, ataque de intermediario, phishing)

TI en la sombra

Prioridades de la seguridad

La mejora de la gestión de la identidad y el acceso es la principal prioridad para el 71 % de las organizaciones encuestadas. Le siguen la prevención de la pérdida de datos (59 %) y el acceso seguro a las aplicaciones en la nube alojadas en proveedores de servicios en la nube (45 %).

¿Cuáles son las prioridades actuales de su organización en materia de seguridad?[4]

71%

Mejorar la identidad y Acceso (IAM)

59%

Prevención de la pérdida de datos

45%

Garantizar el acceso seguro a las aplicaciones alojadas en proveedores de servicios en la nube

43%

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

35%

Realización de una profunda Inspección SSL (por ejemplo, descifrado de sesiones seguras descifrado para el escaneo de malware y el filtrado de web/correo)

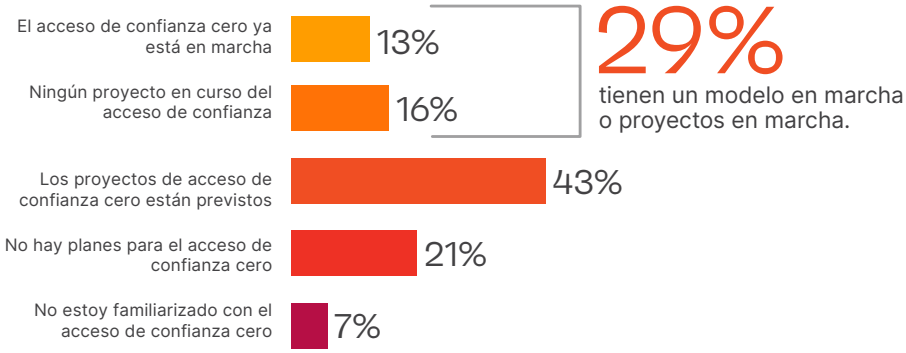
30%

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

Adopción de la confianza cero

Cuando se les preguntó por sus planes para adoptar un acceso de Confianza Cero, el 29% tiene un modelo en marcha o proyectos en curso, mientras que el 43% está en algún tipo de fase de planificación. Sorprendentemente, casi un tercio no tiene planes o no está familiarizado con la Confianza Cero.

¿Qué planes tiene para adoptar un modelo de acceso de confianza cero en su empresa?

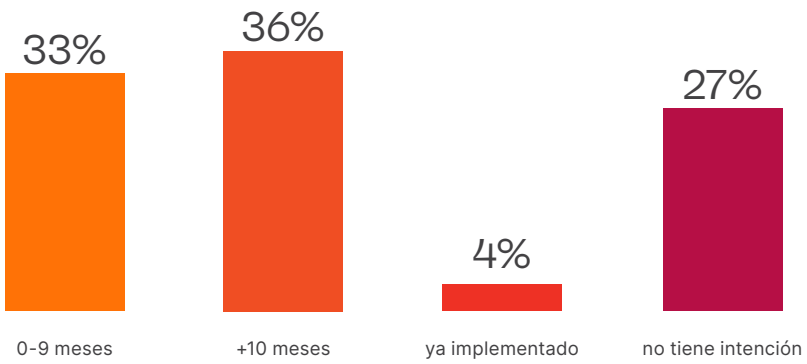


Velocidad de adopción

El interés de la confianza cero se está trasladando a los despliegues iniciales. De hecho, el 33 % de las empresas adoptará la confianza cero en un plazo de 9 meses. Casi un tercio no tiene planes, lo que sugiere cierta confusión sobre el valor o el esfuerzo.

¿En qué plazo de tiempo es más probable que adopte la seguridad de confianza cero?

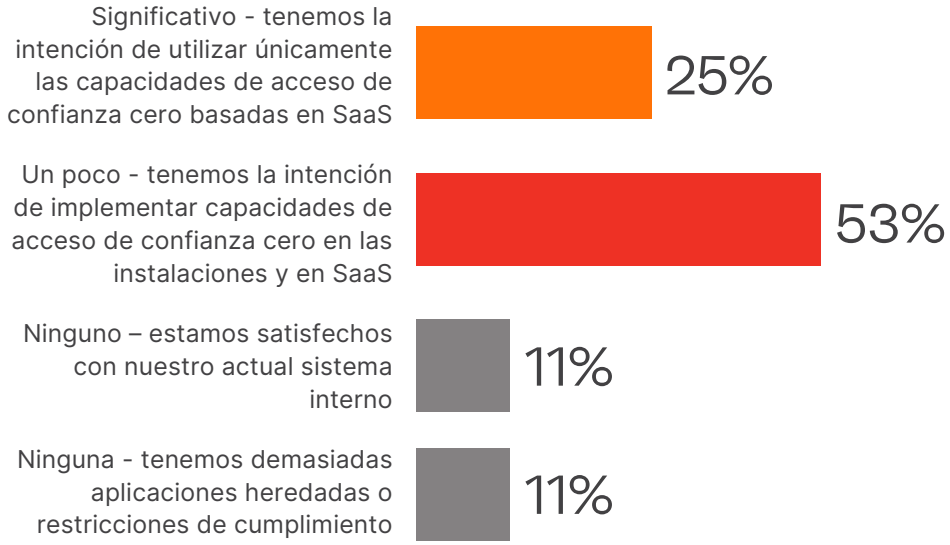
33% de las empresas adoptarán la confianza cero en un plazo de 9 meses.



SaaS de confianza cero

Más de la mitad de las organizaciones planean trasladar las capacidades de acceso de confianza cero a una implementación de TI híbrida (local/SaaS). Una cuarta parte tiene previsto pasar únicamente a una solución de confianza cero basada en SaaS. El 22% no tiene planes de implementar confianza cero basado en SaaS, ya sea debido a aplicaciones heredadas, restricciones de cumplimiento o satisfacción con la protección de acceso implementada actualmente.

Durante los próximos 18 meses, ¿hasta qué punto usted y su organización tienen previsto trasladar las capacidades de acceso de Cero Confianza a SaaS?[5]



Acceso a la confianza cero a las prioridades de inversión

La mayoría de las inversiones en tecnologías de acceso de confianza cero se dirigen a la autenticación de múltiples factores (59%), la gestión y el gobierno de la identidad (48 %) y el inicio de sesión único (44 %). Le siguen el control de acceso a la red y el cortafuegos de aplicaciones web (43 %), la gestión de acceso privilegiado y la microsegmentación (41 %) y las redes privadas virtuales (35%).

¿Cuál de los siguientes controles de acceso a la identidad / confianza cero prioriza para invertir en su organización en los próximos 12 meses?[6]

59%

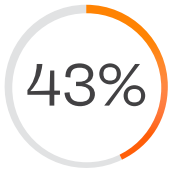
Autenticación multifactor (MFA)

48%

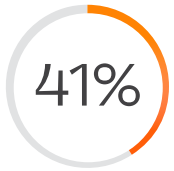
Gestión y gobierno de la identidad

44%

Inicio de sesión único (SSO)



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



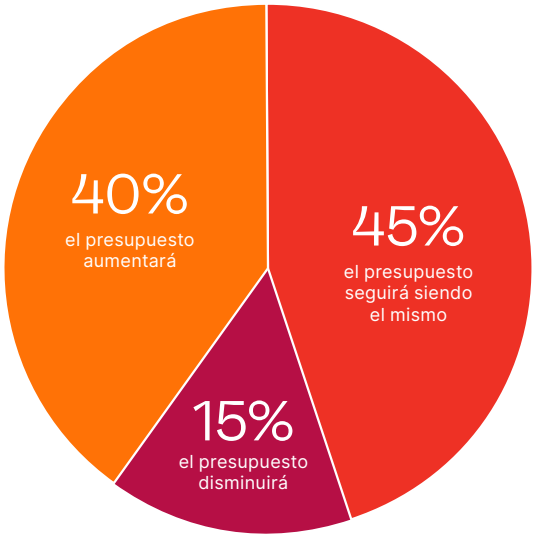
Gestión de acceso privilegiado (PAM), microsegmentación

Redes privadas virtuales (VPN)

Presupuesto de acceso a la confianza cero

El 40 % de las organizaciones esperan un aumento de sus presupuestos relacionados con la gestion de accesos en los próximos 18 meses. Solo el 15 % verá un descenso.

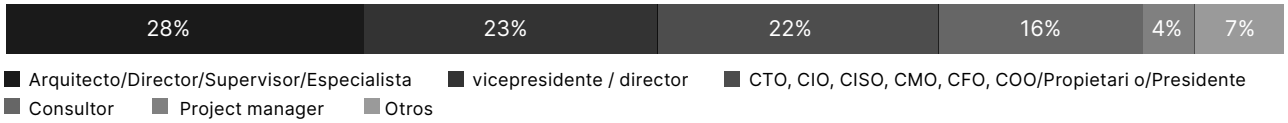
¿Cómo espera que cambie el presupuesto relacionado con la gestión de accesos de su organización en los próximos 18 meses?



Metodología y demografía

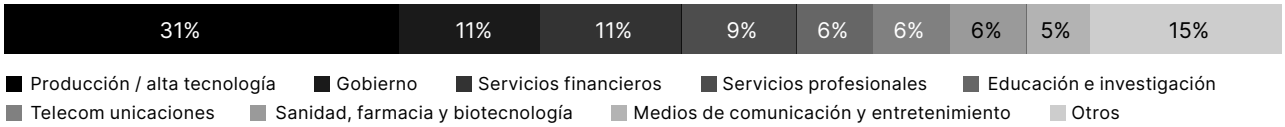
Este informe se basa en los resultados de una exhaustiva encuesta de 413 profesionales de la informática y la ciberseguridad en Estados Unidos, realizada en enero de 2020 para identificar las últimas tendencias de adopción, tendencias, retos, carencias y preferencias de soluciones relacionadas con la seguridad Zero Trust o confianza cero. Los encuestados van desde ejecutivos técnicos hasta profesionales de la seguridad informática, representando una sección equilibrada de organizaciones de distintos tamaños y de múltiples sectores.

Nivel profesional



Tamaño de la empresa

Sector



ivanti

ivanti.com
1 800 982 2130
sales@ivanti.com

1 Segregación de recursos 44 % | No hay distinción de confianza entre la red interna o externa 39 % | Otros 2 %

2 Respuesta a auditorías o incidentes de seguridad 37 % | Eficiencia operativa 33 % | Abordar problemas de seguridad de TI híbridos 31 % | Otros 4 %

3 Los procesos manuales son complejos y ralentizan la capacidad de reacción rápida 37 % | Otros 2%

4 Mejorar las funciones de seguridad de SD-WAN 28 % | Complementar la detección y respuesta de puntos finales (EDR) 27 % | Aumentar o reemplazar las herramientas de acceso remoto existentes (por ejemplo, VDI, VPN, RDP) 24 % | Otros 5 % | Ninguno 2 %

5 Inspección SSL 40 % | Asegurar SD-WAN 27% | Simplificación 26 % | Sustituir la tecnología de seguridad de acceso remoto existente (por ejemplo, VPN) 25 % | EDR 20 % | Ninguno 2 % | Otros 8%.

6 Agente de seguridad de acceso a la nube (CASB) 33 % | Gestión móvil empresarial (MDM) 31 % | Perímetro definido por software (SDP) 28 % | Análisis de identidades 24 % | Servicios de directorio empresarial 17 % | Otros 2 %.