Benchmark Insights

IBM **Institute for Business Value**

Primeros pasos para utilizar la seguridad de zero trust

Guía para construir cibertolerancia ante fallas

IBM

¿Cómo puede contribuir IBM?

IBM Security pone en marcha la zero trust con un enfoque de seguridad moderno y abierto que se alinea con las prioridades de su negocio. Para más información, visite: ibm.com/security/zero-trust

Para entender mejor cómo las organizaciones están implementando la seguridad de zero trust, el IBM Institute for Business Value (IBV) se asoció con Oxford Economics para encuestar a más de 1,000 ejecutivos de operaciones y seguridad de organizaciones de 15 industrias de todo el mundo (ver “Metodología de investigación” en la página 16).

Por Chris McCurdy,
Shue-Jane Thompson,
Lisa Fisher
y Gerald Parham

Principales conclusiones

Los nuevos modelos de negocio están acelerando la transformación de la seguridad.

A medida que los riesgos evolucionan y surgen nuevas amenazas, los modelos tradicionales de seguridad que se basan en perímetros definidos y en la confianza implícita están quedando obsoletos. Las empresas que trascienden los límites funcionales y organizacionales tradicionales requieren un modelo de seguridad que sea más holístico, de varios niveles y basado en eventos.

La seguridad de zero trust ofrece claras ventajas operativas.

La zero trust es un enfoque dinámico de la seguridad en el que las solicitudes se validan mediante una combinación de controles de acceso, gestión de la identidad y datos contextuales. Las organizaciones con las funcionalidades y recursos de zero trust más maduros (conocidos como “pioneros en zero trust”) han reducido los gastos, aumentado la efectividad de su seguridad cibernética y cuentan con mayores tasas de retención de recursos cibernéticos.

Los líderes de la zero trust destacan en 4 competencias básicas.

La zero trust mejora la cibertolerancia a las fallas al transformar la confianza en una variable operativa. El dominio de cuatro competencias centrales y otras prácticas asociadas impulsan el éxito de la zero trust.

—

El precio del progreso

Las organizaciones han respondido a la pandemia de COVID-19 acelerando la transformación digital de su negocio al ampliar sus huellas en la nube, incrementar sus fuerzas de trabajo remotas y mediante la integración de sus cadenas de suministro. Como resultado, nuestra investigación indica que el porcentaje de trabajadores remotos atendidos por la función de seguridad aumentó un 41% entre finales de 2019 y a lo largo de 2020.

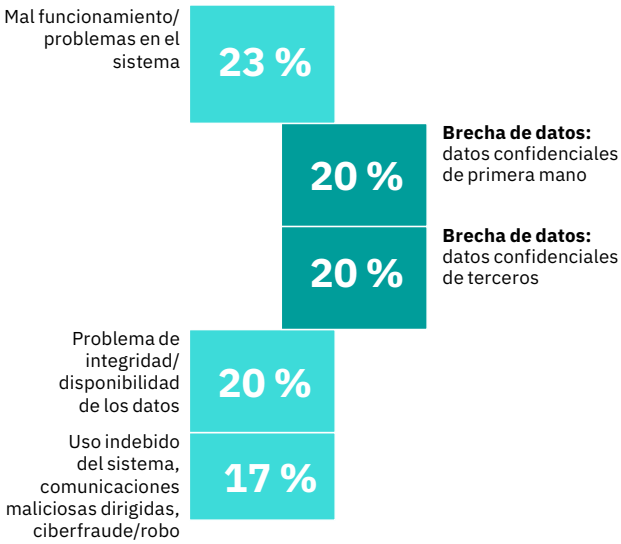
Pero el hecho de trasladar la comunicación, el negocio y las interacciones personales a Internet también ha aumentado significativamente las áreas susceptibles de ataque, lo que ha provocado un aumento enorme de los incidentes de seguridad cibernética y de registros expuestos (ver Figura 1).[1] A medida que las cargas de trabajo se trasladan a la nube, las amenazas se desplazan con ellas. Nuestra investigación indica que, en 2020, más del 90 % de los ciber-incidentes se originaron en entornos de nube.

—

Figura 1

Datos expuestos

La ampliación de las interacciones en línea hace que las brechas de datos sean más comunes



P. Del total de incidentes de seguridad cibernética detectados por su organización, ¿cuál fue la distribución por tipo?

70 %

de las organizaciones son incapaces de asegurar los datos que se mueven a través de varios entornos de nube e instalaciones, un profundo impedimento para alcanzar valor.

92 %

de las organizaciones carecen de la capacidad de habilitar y extender de forma segura nuevas funcionalidades nativas de la nube a sus socios internos y externos.

150 días:

el tiempo que se tarda en cubrir las vacantes de cibertalento con candidatos cualificados, lo que provoca brechas de conocimiento y responsabilidad que pueden elevar la exposición al riesgo.

A pesar de que los servicios compartidos basados en la nube y los entornos de trabajo colaborativo son vitales para obtener resultados comerciales, estos entornos requieren un nuevo enfoque más flexible, receptivo y cooperativo para las operaciones de seguridad. Con el objetivo de aprovechar las ventajas de este nuevo enfoque, los líderes están modernizando sus operaciones de TI y OT basándose en los principios de la zero trust (ver "Perspectiva: ¿Qué hace que la zero trust sea diferente?").

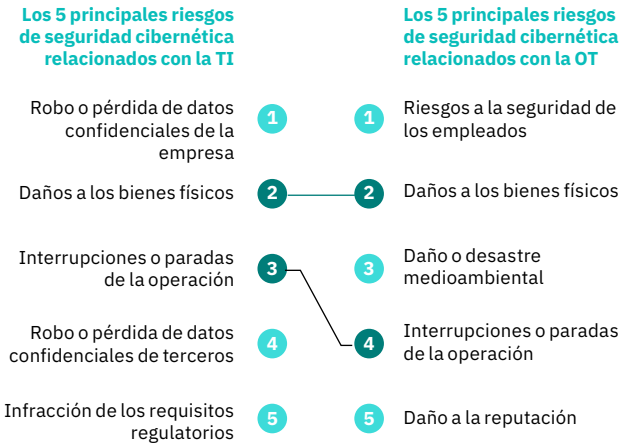
Valioso pero vulnerable: la seguridad de la infraestructura crítica

La propia naturaleza de la infraestructura crítica implica una relación dinámica entre confianza y riesgo. A medida que las operaciones migran a tener una presencia en línea, tanto las redes de TI como las de tecnología operativa (OT) están expuestas a riesgos. El ataque de ramsomware de Kaseya de julio de 2021, por ejemplo, afectó a aproximadamente 2,000 organizaciones y resultó en pedidos de rescate de más de USD$70 millones. Nuestra dependencia de los entornos de TI y OT significa que la infraestructura crítica está cada vez más vulnerable a las nuevas amenazas (ver Figura 2).[2]

Figura 2

Riesgo de interconexión

Los riesgos de TI y OT son complejos e interdependientes



P. ¿Cómo calificaría los riesgos de seguridad cibernética mencionados? El gráfico muestra las respuestas de alto y muy alto.

Los enfoques tradicionales de seguridad cibernética se basan en permisos y límites de red discretos, pero las redes actuales están definidas por servicios dinámicos y límites difusos.

La confianza es la base de la colaboración y la cooperación de negocios. A medida que estas funcionalidades se tornan esenciales para el valor de las ofertas, la forma en que pensamos en la confianza cambia rápidamente. Mientras que los enfoques tradicionales de ciberseguridad se basaban en permisos y límites de red discretos, las redes actuales se definen por servicios dinámicos y límites difusos. Las plataformas digitales actuales generan valor al estar interconectadas y compartir información entre varias partes.

Las tensiones pueden ser inevitables. Muchos sistemas de OT se han basado tradicionalmente en su aislamiento, pero la exigencia de conocimientos de los dispositivos conectados y los sistemas inteligentes hace que estas prácticas sean difíciles de mantener. En todo caso, la falta de conectividad puede hacer que las vulnerabilidades existentes sean más difíciles de solucionar.

Para empeorar las cosas, los riesgos pueden producirse en cascada: una falla en un sistema suele provocar fallas en otros. Quienes provocan las amenazas son cada vez más sofisticados en su capacidad para aprovechar las deficiencias de los controles de seguridad de TI y OT(ver “Perspective: The convergence of IT and OT systems elevates risk exposure”).[3] Aunque los impactos potenciales son significativos, estos riesgos pueden ser difíciles de prever.

El cibercrimen como servicio es una tendencia nueva e inquietante.[4] Estos servicios, los cuales se pueden adquirir a través de foros de hackers, ventas directas en la web y en la dark web mediante criptomonedas, utilizan sofisticadas exploraciones de delitos cibernéticos generalmente coordinados como botnets, ataques de denegación de servicios distribuidos (DDoS), fraudes con tarjetas de crédito, software malicioso, spam y ataques de phishing.

De hecho, a raíz del ataque cibernético del oleoducto de Colonial, el presidente de Estados Unidos, Joseph Biden, emitió una orden ejecutiva para mejorar la postura de seguridad cibernética de la industria e infraestructura críticas. Esto incluye una directiva para que los organismos federales elaboren planes de implantación de arquitecturas de zero trust en un plazo de 60 días a partir de la orden.[6]

Perspectiva: ¿Qué hace diferente a la seguridad de zero trust?

En principio, la zero trust es un enfoque preventivo de la seguridad que presupone que los actores maliciosos ya han penetrado las defensas de red de la organización. Las operaciones de TI y seguridad cibernética se reconocen como funcionalmente interdependientes. Como resultado, la capacidad de la organización para percibir, evaluar y responder a los eventos es mucho más dinámica, y generalmente ocurre en tiempo casi real. Esta conciencia holística que abarca las operaciones informáticas y cibernéticas hace que las funcionalidades de zero trust sean verdaderamente transformadoras.

En la práctica, la zero trust crea un puente entre los dominios operativos y de seguridad cibernética al exigir autenticación y verificación para cada intercambio de valor. Dado que un modelo operativo de zero trust no depende únicamente de asegurar los perímetros, este es muy adecuado para los ecosistemas compartidos en los que los límites organizativos son difusos y el valor se intercambia en forma de servicios. Al hacer que la confianza sea una variable operativa y transaccional, los terceros pueden soportar incluso las cargas de trabajo más sensibles y las funcionalidades fundamentales.

Perspectiva: La convergencia de los sistemas de TI y OT eleva la exposición al riesgo

Las principales preocupaciones de los ejecutivos en relación con las tecnologías de la información son la exposición de datos confidenciales, las implicaciones a largo plazo de las violaciones de seguridad exitosas y la conformidad regulatoria. Sus principales preocupaciones relacionadas con la OT son la seguridad de las personas, los activos físicos y el entorno, así como cualquier impacto resultante en las operaciones y la reputación de la organización.

Aunque los riesgos de seguridad cibernética relacionados con los entornos de TI y OT no son siempre los mismos, generalmente se refuerzan mutuamente. Como ha demostrado el hackeo de Colonial Pipeline, una falla en un área, como una contraseña de un sistema informático expuesta, puede provocar fallas en otras, como la disminución de la disponibilidad y confiabilidad de la plataforma de OT.[5]

Beneficios de zero trust

Nuestro análisis revela que el 23 % de las organizaciones, un grupo al que denominamos “pioneros de zero trust”, van por delante de sus pares en la implementación de funcionalidades de esta tecnología en sus entornos de TI y OT y en sus interacciones con los socios del ecosistema.

Estas organizaciones han configurado sus operaciones de TI y seguridad como un patrimonio único. Son competentes en la colaboración interna y externa para administrar el riesgo de seguridad cibernética. Han modernizado sus operaciones de seguridad relacionadas con marcos interdependientes de gestión, riesgo y conformidad. Aplican ampliamente la nube, la analítica basada en la IA y la automatización. Además seleccionan, desarrollan y retienen recursos de seguridad cibernética cualificados para habilitar funcionalidades de confianza nula a través de sus patrimonios digitales.

Y, lo que es más importante, sus operaciones de seguridad pueden adaptarse a la complejidad del entorno empresarial actual, ya sea habilitando un personal remoto; supervisando los puntos finales, las aplicaciones, los datos y el tráfico de red; o analizando los comportamientos de los empleados, los clientes y los socios para identificar las amenazas emergentes.

¿Qué es lo que distingue a los considerados “pioneros” de zero trust?

Según nuestro estudio, los pioneros de Confianza Nula dedican un porcentaje similar de sus presupuestos y recursos de TI a la seguridad cibernética que sus pares, pero están obteniendo beneficios significativamente mayores tanto a nivel comercial como de seguridad desde dicho enfoque.

De hecho, el doble de los pioneros afirman haber reducido significativamente sus gastos operativos y de capital en materia de seguridad, al tiempo que han aumentado la eficacia de sus funcionalidades de seguridad cibernética. En particular, han logrado:

- Mejorar sus funcionalidades de detección y respuesta, reduciendo drásticamente la filtración de datos confidenciales. En caso de vulnerabilidades, su capacidad para limitar la propagación del software malicioso reduce el impacto para la organización.
- Se ha dado prioridad a la capacidad de establecer y mantener conexiones seguras entre los socios del ecosistema, lo que les permite capitalizar mejor sus inversiones en nube.
- Invertido más de su presupuesto de ciberseguridad para mejorar las habilidades de sus recursos humanos. Como resultado, sus índices de retención de recursos cibernéticos son un 10% mayores que los de otras organizaciones.

El éxito de los pioneros de la confianza nula es prueba fehaciente sobre las ventajas de una estrategia integral para estos sistemas. Estas organizaciones se encuentran en una posición favorable para lograr una mayor eficiencia operativa y mejores resultados comerciales. Otras organizaciones pueden obtener beneficios similares si comprenden y aplican las funcionalidades operativas esenciales para el éxito de la confianza nula.

Los pioneros de zero trust dedican un porcentaje similar de sus presupuestos de TI a la seguridad cibernética, pero logran beneficios significativamente mayores.

Primeros pasos: Definición de un plan de zero trust

Los pioneros de la confianza nula están casi dos veces más adelantados en la aplicación de las 4 competencias principales:

1. Una base sólida para las operaciones de seguridad de confianza nula guiada por controles de gestión, riesgo y conformidad, y reforzada con analítica basada en la IA.

2. Funcionalidades de automatización y orquestación de seguridad, recursos que incrementan el alcance, el escalado, la visibilidad y la eficiencia de las operaciones de seguridad en entornos operativos de nube híbrida.

3. Una metodología de controles de seguridad de confianza cero para supervisar, administrar y ayudar a defender los recursos críticos, incluyendo usuarios, datos, redes, dispositivos y cargas de trabajo.

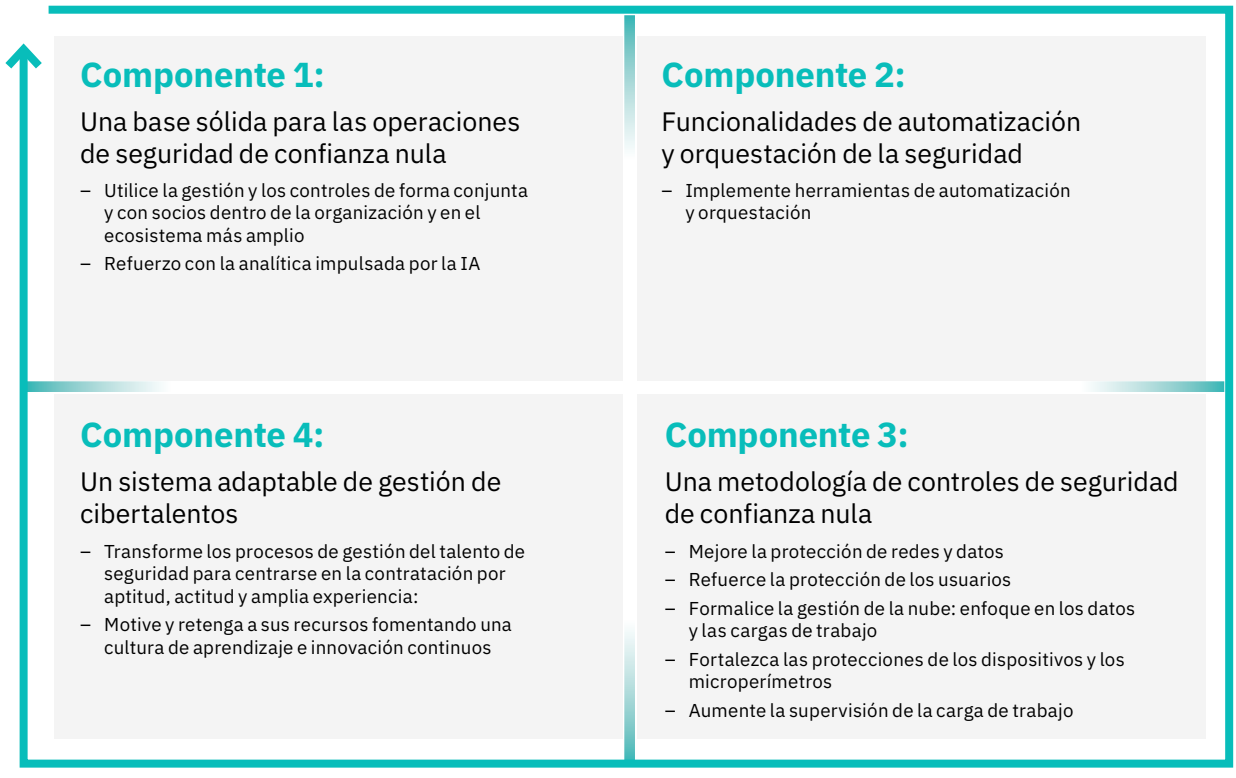
4. Un sistema de gestión del cibertalento adaptable que prioriza la combinación de talento y tecnología para lograr mejores resultados de seguridad.

Cada uno de estos elementos se lleva a cabo a través de una serie de prácticas y actividades que se refuerzan mutuamente. Es especialmente importante que nuestro análisis de datos subraye hasta qué punto estas prácticas y actividades dependen unas de otras. En otras palabras, las 4 competencias fundamentales trabajan en conjunto para lograr los beneficios asociados a la confianza nula (ver Figura 3).

Figura 3

Design con enfoque en la seguridad

Las funcionalidades de confianza nula se refuerzan mutuamente



Fuente: análisis de datos de IBM Institute for Business Value

En conjunto, una mayor conciencia del riesgo y los controles de propagación de software malicioso reducen significativamente la exposición a los ciberataques.

Dado que los patrimonios informáticos y cibernéticos de cada organización reflejan necesidades distintas, cada ruta hacia la confianza nula será única. Los factores que influirán en la ruta de una organización incluyen su estrategia de negocio y sus modelos operativos; la disponibilidad de presupuesto y recursos; la amplitud y profundidad de las relaciones sociales; las implementaciones y limitaciones tecnológicas existentes; y las demandas regulatorias y competitivas específicas de la industria y la región.

Reconociendo la diversidad de estos factores, nuestro enfoque prioriza la practicidad, la flexibilidad y la virtud de aprovechar las funcionalidades y recursos existentes. Nuestras recomendaciones, derivadas de los insights sobre el desempeño operacional, se basan en los resultados del mundo real en una serie de entornos operativos, desde organizaciones jóvenes centradas en el crecimiento hasta organizaciones maduras centradas en la transformación.

Para cada componente, ofrecemos una explicación, sus beneficios asociados y las prácticas y actividades necesarias para conseguirlo.

Componente 1: Establezca una base sólida para las operaciones de seguridad de confianza nula

Los pioneros de la confianza nula han integrado las funcionalidades y recursos de estos sistemas en sus arquitecturas y operaciones de seguridad predominantes. Las funcionalidades y recursos fortalecen, en lugar de sustituir, las tecnologías, procesos y habilidades existentes.

Estas organizaciones han desarrollado una cultura de concientización sobre la seguridad basada en prácticas modernas y controles automáticos. Esta cultura aumenta la conciencia sobre los riesgos de seguridad mediante políticas que definen quién y qué puede acceder a los activos de red, aplicación y datos comunes.

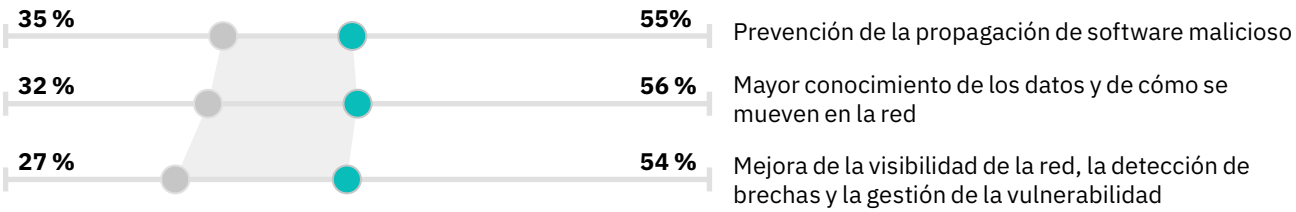
Estas políticas se complementan con las soluciones técnicas de seguridad que las hacen cumplir sistemáticamente. Este entorno puede ayudar a identificar dispositivos, aplicaciones, servicios y comportamientos susceptibles a vulnerabilidades, y luego utilizar controles automáticos para ayudar a solucionar dichas amenazas y vulnerabilidades.

En el caso de que existan violaciones de seguridad, la capacidad de los pioneros para prevenir la propagación de software malicioso ayuda a contener los riesgos, limitando la probabilidad de que se produzcan fallas posteriores (ver Figura 4). En conjunto, una mayor conciencia del riesgo y los controles de propagación de software malicioso reducen significativamente la exposición a los ciberataques.

Figura 4

Ver y comprender

Mejor visibilidad de la red, mejores resultados



Todos los demás | **Pioneros en confianza nula**

P. ¿En qué medida su organización ha obtenido cada uno de los beneficios mencionados de su enfoque de la seguridad? Los porcentajes reflejan que los encuestados seleccionaron un grado significativo o muy grande.

Además, los pioneros de la confianza nula trabajan con socios para optimizar la gestión y los reportes del ciber riesgo. Guiados por metodologías específicas de gestión, riesgo y conformidad, comunican de forma proactiva las nuevas amenazas en toda la empresa y a los socios estratégicos y proveedores externos. Su uso de metodologías de ciclo de vida de desarrollo de sistemas estándar (SDLC) y DevSecOps estandariza funcionalidades fundamentales para operaciones de seguridad y gestión, facilitando aún más la eficiencia.

Gracias a la amplia aplicación de la seguridad cibernética analítica avanzada para detectar incidentes y responder a ellos, los pioneros de confianza nula supervisan un mayor porcentaje de comunicaciones de la red (55 %) y de dispositivos de puntos finales (68 %) en busca de vulnerabilidades y violaciones de políticas, en comparación con el 45 % y el 60 % de los pares, respectivamente. Cuanto más visión tenga una organización (dispositivos de tráfico y terminales de puntos finales, por ejemplo), mayor será su capacidad para identificar y solucionar posibles amenazas. Una mayor visibilidad aumenta la probabilidad de éxito.

La mayoría de los pioneros indican que han aumentado significativamente su conocimiento de cómo se mueven los datos en sus redes. Aproximadamente 1.5 veces más pioneros han mejorado sus funcionalidades de visibilidad de la red, la detección y la gestión de la vulnerabilidad, en comparación con sus pares (ver Figura 4).

Componente 1:

Establezca una base sólida para las operaciones de seguridad de zero trust

Supervise las comunicaciones de red para detectar actividades sospechosas

45% Todos los demás

55% Pioneros en confianza nula

Supervise los dispositivos de puntos finales en busca de vulnerabilidades y violaciones de las políticas

60% Todos los demás

68 % Pioneros en confianza nula

Cómo hacerlo

Utilice la gestión y los controles de TI con los socios en de la organización y en el ecosistema de manera más amplia

Utilice la analítica basada en la IA para distinguir las excepciones y activar los controles automáticos

Los modelos de seguridad de IA automatizadas pueden reconocer comportamientos anormales, evaluar vulnerabilidades y distinguir nuevas amenazas.

1

En particular, dos de estas prácticas pueden ayudar a las organizaciones a establecer una base sólida para las operaciones de seguridad de confianza nula:

1. Utilice la gestión y los controles de TI con socios en la organización y en el ecosistema de manera más amplia para aumentar la visibilidad y la eficacia de los esfuerzos de mitigación del riesgo cibernético:

- Proporcione capacitación en seguridad y concienciación a los empleados: los conocimientos, habilidades y capacidades necesarios para defender a la organización.
- Aplique metodologías y programas de gobernanza, gestión de riesgos y conformidad, para identificar, evaluar y mitigar el ciberriesgo. Equilibrar los niveles de riesgo aceptables con los objetivos de negocio y los requisitos de conformidad. Coordine estos esfuerzos con los socios del ecosistema para lograr mejores economías de escala.
- Implemente una política de prevención de pérdida de datos (DLP). Defina cómo su organización puede compartir y proteger los datos para implementar herramientas que eviten que los usuarios envíen información sensible o crítica fuera de la red principal. Coordine estos esfuerzos con los socios utilizando la infraestructura compartida.
- Integre la seguridad en el proceso de desarrollo del software. Las metodologías nativas de la nube, como DevSecOps, permiten a las organizaciones trabajar con sus socios de manera más eficiente, en particular mediante la adopción de enfoques comunes de operaciones y gestión de la seguridad.[7]

2. Utilice la analítica basada en la IA para distinguir las excepciones, activar los controles de resolución y evitar que los actores de amenazas utilicen técnicas de exploración y explotación automáticas:

- Implemente funcionalidades de telemetría de seguridad cibernética avanzada, incluyendo monitoreo y analítica para la detección y resolución de incidentes. Reduzca la dependencia de la detección manual de amenazas utilizando procesos de investigación automáticos impulsados por la IA para datos de alto valor, activos, segmentos de red y servicios de nube.

  Las amenazas pueden ser clasificadas y priorizadas para activar alertas según los ataques clásicos e indicadores de vulnerabilidades (IOC). Para mejorar la eficiencia operacional, las organizaciones pueden complementar las soluciones de telemetría existentes con funcionalidades de detección y respuesta en el punto final (EDR) y en la capa cruzada (XDR).
- Aplique la IA para automatizar la construcción de modelos, realizar el seguimiento del comportamiento normal y distinguir la actividad anómala. Los modelos automatizados de seguridad de IA pueden reconocer los comportamientos normales (versus los anormales), evaluar las vulnerabilidades de forma dinámica y distinguir la actividad anómala que puede indicar nuevas amenazas. Los modelos pueden utilizar estas entradas para calificar y cuantificar la exposición al riesgo potencial.

Componente 2:

Fortalezca las operaciones mediante funcionalidades de automatización y orquestación de seguridad

Reducción significativa de los costos de capital y operativos de seguridad

61 %
Pioneros en confianza nula

Ha reducido drásticamente el ámbito y el costo de las iniciativas de conformidad

50%
Pioneros en confianza nula

Cómo hacerlo

Establezca un centro de operaciones de seguridad en todo el ecosistema (SOC)

Implemente una única plataforma independiente de la nube con visibilidad en todos los proveedores

Aplique las recomendaciones de seguridad de la IA para detectar comportamientos anómalos

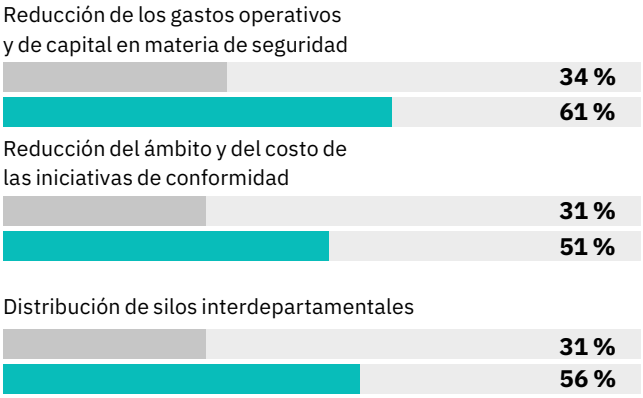
Componente 2: Fortalezca las operaciones mediante funcionalidades de automatización y orquestación de seguridad

Los pioneros de Confianza Nula han adoptado la automatización y la orquestación de la seguridad, aumentando el ámbito, el escalado y la eficiencia de sus operaciones de seguridad. El 61 % de los pioneros de la confianza nula indican que esto ha reducido significativamente sus costos operativos y de capital en materia de seguridad, mientras que la mitad de ellos indican que esto ha reducido drásticamente el ámbito y el costo de las iniciativas de conformidad (ver Figura 5).

Figura 5

La ventaja de costo

La automatización y la orquestación incrementan el ámbito, el escalado y la eficiencia



P. ¿En qué medida su organización ha obtenido cada uno de los beneficios mencionados de su enfoque de la seguridad? Los porcentajes reflejan que los encuestados seleccionaron un grado significativo o muy grande.

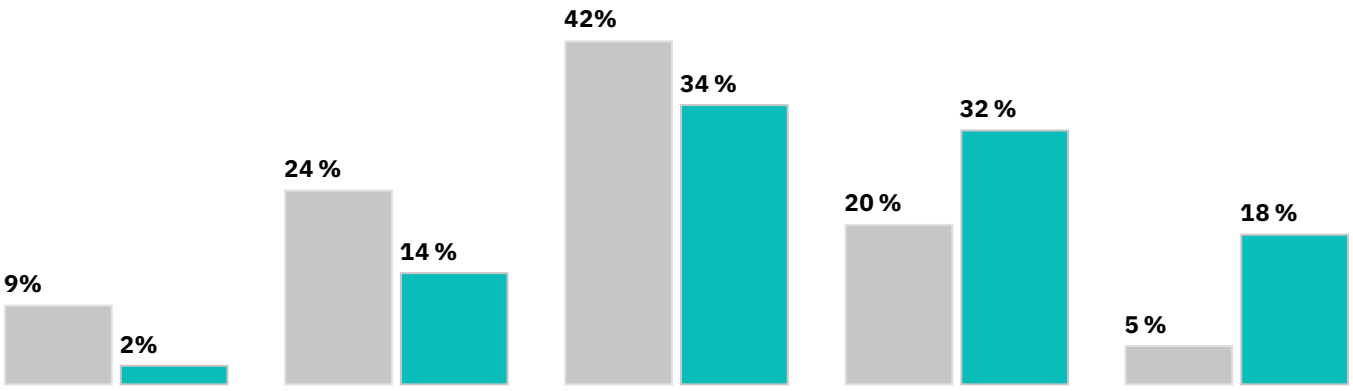
Las soluciones de automatización y orquestación, como la gestión de incidentes y eventos de seguridad (SIEM), la orquestación, automatización y respuesta de seguridad (SOAR) y la XDR, proporcionan una visión holística de las amenazas. Al ver las amenazas en el contexto de los datos, las aplicaciones, las redes y los dispositivos de la empresa, estas soluciones mejoran las investigaciones de seguridad, facilitando a los pioneros aumentar la agilidad de sus operaciones de seguridad y mejorar sus capacidades de respuesta a incidentes.

Además, las capacidades de seguridad de confianza nula de la nube de los pioneros son amplias. 1 de cada 3 puede operar en entornos de nube híbrida, al tiempo que aprovechan todas las ventajas de los datos que fluyen de forma segura a través y entre varios entornos de nube e instalaciones. 1 de cada 5 puede llevar esto aún más lejos (ver Figura 6). Disponen de las funcionalidades para habilitar y extender de forma segura nuevas funcionalidades de negocio y operativas nativas de la nube a socios internos y externos.

Figura 6

La ventaja de la nube

Capacidades maduras de seguridad de nube que permiten nuevos modelos de negocios de plataforma



Evaluación
Operaciones de nube de seguridad en fase inicial

Inversión
Implementación(es) de seguridad de nube de en marcha, logrando valor

Integración
La infraestructura/ el proceso puede operar bajo entornos de nube híbrida

Optimización
Los datos fluyen de forma segura en varios entornos locales y de la nube

Innovación
Modelos de negocio de plataforma/ecosistema habilitados de forma segura

Todos los demás | **Pioneros en zero trust**

P. ¿Qué afirmación describe mejor la madurez de las funcionalidades de seguridad de la nube de su organización? Seleccione una.

El 60% de los pioneros aceptan que su enfoque de seguridad ha permitido significativamente la transformación digital y el 54% que ha aumentado las conexiones de confianza y seguridad con los socios externos.

Pero ¿qué es lo que realmente diferencia a los pioneros de la confianza nula? Es su grado de cibertolerancia a las fallas, y su capacidad para capitalizar las eficiencias operativas y las economías de escala. Aprovechan todo el alcance de sus entornos de nube para habilitar nuevas funcionalidades, recursos y nuevos modelos de negocio, junto con sus socios del ecosistema.

Una práctica pionera, en particular, puede ayudar a las organizaciones a lograr una mayor seguridad, tolerancia a las fallas y eficiencia operativa:

1. **Implemente herramientas de automatización y orquestación para mejorar el ámbito, la escala, la visibilidad y la eficiencia de las operaciones de seguridad de confianza nula:**
   - Evalúe continuamente la postura de seguridad de la organización utilizando un centro de operaciones de seguridad (SOC) que abarque todo el ecosistema y que cuente con funcionalidades coordinadas de gestión de incidentes y respuesta a crisis.[8] Priorice las herramientas que proporcionan visibilidad en todo el SOC. Habilite la visibilidad en tiempo real en todas las instalaciones y entornos de nube, incluyendo redes, dispositivos, aplicaciones, usuarios y datos. Esto puede ayudar a los responsables por la toma de decisiones a entender el estado actual de los activos y servicios críticos.
   - Adopte soluciones de seguridad que funcionen en varias nubes e intégrelas con soluciones de varios proveedores. El equipo de SOC debe tener una plataforma única agnóstica a la nube con visibilidad a través de los proveedores para iniciar las investigaciones de cualquier incidente dentro de este entorno, en cualquier lugar dentro del ecosistema.
   - Implemente seguridad inteligente proporcionada por la IA para analizar flujos de datos y detectar comportamientos anómalos. Combine información de seguridad que provenga de varios dominios, así como de fuentes externas, para enriquecer los datos contextuales/metadatos de las interacciones y hacer cumplir las políticas de seguridad. Extienda las capacidades de captura del registro y aplique los mismos procedimientos a través de entornos de nube, escaneando en busca de configuraciones irregulares que pueden señalar indicadores de vulnerabilidades.

Componente 3: Implemente una metodología de controles de seguridad de zero trust

Los pioneros de la confianza nula están integrando este tipo de controles en sus operaciones de seguridad existentes. Los pioneros utilizan la telemetría de seguridad, el análisis del tráfico en tiempo real y las funcionalidades de automatización y orquestación para mejorar la seguridad.

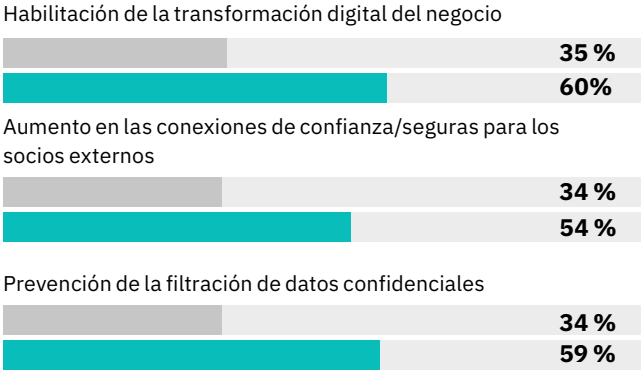
Esto abarca recursos fundamentales como usuarios, dispositivos, datos, redes y cargas de trabajo. Dado que estos recursos operan de forma concertada (normalmente junto con los socios del ecosistema), los pioneros están mejor posicionados para actuar sobre la base de los conocimientos. Esto aumenta la cibertolerancia a las fallas y su capacidad para impulsar nuevas propuestas de valor.

Los beneficios asociados a esto son evidentes. Para los pioneros de la zero trust, el 60 % está de acuerdo con que este enfoque ha permitido de forma significativa la transformación digital de sus organizaciones, mientras que el 54 % está de acuerdo con que ha aumentado la confianza y las conexiones seguras con los socios externos (ver Figura 7).

Figura 7

El poder de la confianza

La zero trust mejora la tolerancia a las fallas y potencia los esfuerzos de transformación digital



Todos los demás | **Pioneros en zero trust**

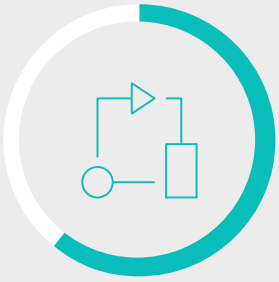
P. ¿En qué medida su organización ha obtenido cada uno de los beneficios mencionados de su enfoque de la seguridad? Los porcentajes reflejan que los encuestados seleccionaron un grado significativo o muy grande.

Componente 3:

Implemente una metodología de controles de seguridad de zero trust

Habilitación de la transformación digital del negocio

Aumento en la confianza y las conexiones seguras para los socios externos.



60 %
Pioneros en confianza nula

54 %
Pioneros en zero trust

Cómo hacerlo

Mejore la protección de redes y datos

Controle el acceso a los datos y administre las identidades digitales

Formalice la gestión de las nubes

Amplíe la visibilidad de todos los puntos terminales que intentan acceder a recursos críticos

Aumente la supervisión de las cargas de trabajo

Transforme la confianza en una variable transaccional mejora la integridad del entorno de las operaciones. Con una mayor visibilidad de los recursos fundamentales, los pioneros operan de forma más eficiente. Al situar los controles de seguridad más cerca de los recursos críticos, por ejemplo, creando microperímetros en torno a activos y servicios específicos, se pueden ampliar los controles de autenticación y validación sin introducir fricciones innecesarias. Esto mejora la tolerancia a las fallas al impedir el acceso no autorizado y la filtración de datos confidenciales (ver Figura 7).

Cuando se considera en su conjunto, este cambio en las operaciones es sutil pero significativo. Al establecer confianza en intervalos predefinidos (utilizando controles de validación y autenticación para eventos y comportamientos específicos) la capacidad de negociar la confianza se convierte en algo dinámico y en tiempo real. Como la confianza puede ajustarse en función de las circunstancias o el contexto, puede habilitar nuevas formas de colaboración y nuevos intercambios de valor.

Las siguientes 5 prácticas y actividades asociadas son fundamentales para establecer una metodología de controles de confianza nula:

1. **Mejore la protección de la red y de los datos, empezando por el establecer un gateway de segmentación para habilitar controles de acceso más granulares:**

– Utilice firewalls de última generación (NGFW) para aumentar los controles de seguridad de la nube. Defina reglas y políticas para NGFWs, gateways de seguridad de correo electrónico y de nube, y soluciones DLP para hacer cumplir las políticas de seguridad de datos y de acceso. Deben ser capaces de funcionar en todos los modelos de alojamiento, ubicaciones, usuarios y dispositivos.

– Realice regularmente descubrimientos y clasificaciones de datos confidenciales a nivel local, en el punto final, en tránsito, y en la nube. Capture suficientes datos y metadatos para poder recrear el contexto completo de cualquier interacción.

  Comprenda dónde residen sus datos más confidenciales, quién tiene acceso a ellos (y cómo), quién accede a ellos (y cuándo), y qué hace con ellos. Esto puede ayudarle a cumplir con los estándares de privacidad de datos y conformidad normativa, así como a supervisar y controlar el acceso a datos altamente confidenciales.

A medida que surgen técnicas para eludir la autenticación (en particular, el abuso de los mecanismos de confianza) se examina la gestión de la identidad como posible origen de la vulnerabilidad.

3

2. Refuerce la protección de los usuarios mediante el control del acceso a los datos y la gestión de las identidades digitales:

– Revise periódicamente las licencias de acceso de los usuarios. Establezca controles basados en roles para el acceso a los datos. Opere según el principio del menor privilegio, con acceso restringido a la información y exigencia de recursos para desempeñar una tarea específica basada en una necesidad legítima reconocida.

  Informar a los usuarios privilegiados sobre los controles y prácticas de seguridad cibernética pertinentes. Documente quién tiene licencia para acceder a recursos sensibles, luego supervise comportamientos y lleve a cabo auditorías para mejorar la visibilidad y distinguir anomalías y potenciales acciones maliciosas.

– Implemente la autenticación multifactor (MFA) para las aplicaciones críticas y los activos de datos. Los empleados deben utilizar la autenticación de dos factores (2FA) o la MFA para identificar las áreas en las que debe centrarse la seguridad personal, así como para prevenir ataques internos.[9] Éstas deben complementarse con una solución de gestión de identidades privilegiada (PIM) y con procesos sólidos de gestión de identidades (IMG).

  A medida que surgen técnicas para eludir la AMF (sobre todo el abuso de mecanismos de confianza como OAuth y SAML) se pone mayor énfasis en la gestión de la identidad como origen potencial de la vulnerabilidad.[10] Mejore las políticas y controles relacionados con la gestión de credenciales y la gestión de secretos.

3. Formalice la gestión de la nube para promover la apertura y la interoperabilidad:

– Establezca un proceso formal de gestión de la nube. Construya su modelo de gestión de la nube sobre políticas y marcos de gestión estandarizados para ayudar a que los gastos de seguridad relacionados con la nube impulsen los objetivos de negocio relacionados con su adopción.

– Establezca la gestión y supervisión de los datos y cargas de trabajo en la nube. Al migrar a la nube, defina claramente cómo se distribuyen las responsabilidades entre su organización y su(s) proveedor(es) de nube.

  En un modelo de responsabilidad compartida, el proveedor suele ser responsable de asegurar y gestionar la infraestructura, y el cliente, de asegurar los datos y las cargas de trabajo que operan en ella. Para mitigar el riesgo de pérdida de datos, así como la no conformidad regulatoria, utilice los servicios de seguridad especializados de su(s) proveedor(es) de nubes.

4. Fortalezca las protecciones de los dispositivos y los microperímetros, extendiendo la visibilidad a cada punto final que intente acceder a recursos fundamentales:

– Realice comprobaciones de estado en los puntos finales antes de permitirles conectarse a la red informática corporativa o a los sistemas de acceso. Utilice soluciones automáticas que exploren e inventaríen nuevos dispositivos de puntos finales.

  Añada nuevos puntos finales a un registro, junto con datos contextuales que detallan los usuarios, recursos y eventos asociados. Los usuarios no autorizados y los dispositivos no gestionados deben ser identificados, perfilados, y se les debe negar el acceso.

5. Aumente la supervisión de las cargas de trabajo:

– Realice un inventario y supervise las configuraciones de carga de trabajo. Implemente una solución de seguridad multinube que proporcione una supervisión centralizada de las instancias de la plataforma de nube, las cargas de trabajo, los ajustes de configuración, los servicios autorizados y las credenciales.

Componente 4:

Desarrolle un sistema adaptable de gestión de cibertalentos

Los pioneros de zero trust tienen tasas de retención de cibertalentos un 10 % más altas que sus pares

60 %
Pioneros en zero trust

50 %
Todos los demás

Cómo hacerlo

Contrate por aptitud, actitud y amplia experiencia

Fomente una cultura de capacitación e innovación continuos que valore el aprendizaje

Componente 4: Desarrolle un sistema adaptable de gestión del cibertalento

Independientemente de la forma en que las organizaciones elijan implementar sus funcionalidades de confianza nula, sin los recursos cibernéticos cualificados podrían enfrentarse a retos para obtener resultados duraderos en materia de seguridad y negocio.[11] Pero muchas organizaciones se esfuerzan por seleccionar y retener estas habilidades. En promedio, toma aproximadamente 150 días en cubrir una vacante con un candidato calificado.

En respuesta, los pioneros de la confianza nula están utilizando un sistema de gestión del cibertalento más dinámico que puede adaptarse a los cambios en las habilidades y exigencias. Sobre todo, basan sus contrataciones dependiendo del potencial, reconociendo que es tan importante tener personas que puedan aprender como personas con habilidades específicas.

Dado que las organizaciones compiten por el mismo talento de alto valor, las que tienen reservas de talento más profundas o diversas tienen una ventaja decisiva. En lugar de no poder cubrir vacantes fundamentales, los programas de desarrollo de capacidades pueden proporcionar perspectivas viables, ayudando a la empresa a mantener una postura de seguridad eficaz.[12]

Los pioneros de Confianza Nula dedican un mayor porcentaje de su presupuesto de seguridad cibernética a desarrollar las habilidades de sus recursos informáticos a través de una cultura de aprendizaje continuo. Esto se refleja en sus índices de retención de cibertalentos, que son un 10 % superiores a los de otras organizaciones (60 % frente al 50 %).

Fomente una cultura que valore no sólo el conocimiento, sino la constancia en el aprendizaje.

4

Dos prácticas pueden servir de base a un sistema de gestión del cibertalento adaptable:

1. Transforme los procesos de gestión del talento de seguridad para centrarse en la contratación por aptitud, actitud y amplia experiencia:

- Defina los requisitos de habilidades, aptitudes y destrezas para cada función dentro de la seguridad cibernética. En combinación con otros objetivos de gestión de desempeño más amplios, esto podría facilitarles a los gerentes la identificación de brechas de habilidades y abordarlas mediante iniciativas de capacitación y reclutamiento. Considere la posibilidad de invertir en soluciones de talento mejoren periódicamente las habilidades de su personal, sus funciones y los criterios de desarrollo, de modo que las variables de talento se actualicen junto con las nuevas tecnologías y los requisitos operativos.
- A la hora de contratar, priorice la evaluación del comportamiento y la competencia más que a la experiencia. Con la llegada de la nube, los eventos de seguridad se multiplican más rápido de lo que muchos equipos pueden administrar. Los profesionales de la seguridad cibernética deben ser flexibles, evolucionando sus habilidades para adaptarse a los riesgos emergentes. También deben ser competentes para trabajar con soluciones de seguridad automáticas. En el caso de las nuevas amenazas, la familiaridad con las tácticas, las técnicas y los procesos de negocio puede superar la experiencia en operaciones de seguridad cibernética.
- Lleve a cabo evaluaciones de aptitud cibernética para identificar habilidades potenciales en el proceso de selección de candidatos. Evalúe las habilidades, actitudes y comportamientos concernientes a la seguridad cibernética de los candidatos exitosos, y luego utilizar estos conocimientos para ampliar la reserva de talento potencial más allá de la organización de seguridad. Esto puede añadir una mayor diversidad a la fuerza laboral, introducir nuevas formas de pensar y ampliar las opciones para abordar los retos de diferentes maneras.

2. Desarrolle y retenga a sus recursos fomentando una cultura de aprendizaje e innovación continuos. Mejore las operaciones de seguridad de zero trust haciendo participar al talento de nuevas maneras:

- Establezca un programa de capacitación para que el personal de seguridad aprenda otras funciones del negocio. Proporcione una visión operativa más profunda de los procesos fundamentales del negocio para entender mejor los riesgos asociados.
- Implemente la IA y otras herramientas para informar los esfuerzos de aprendizaje continuo en todo el ciclo de vida de los recursos humanos. Reconozca el talento potencial identificado durante el reclutamiento y optimizarlo a través del aprendizaje y desarrollo personalizados.
  De este modo, se puede poner rápidamente al día a los nuevos empleados, adoptar el trabajo en equipo en todas las áreas de especialidad, crear un grupo de recursos secundarios para la cobertura de la copia de seguridad y mantener a los equipos de operaciones de seguridad actualizados a medida que surgen nuevas amenazas y aparecen nuevas tecnologías.
- Fomente una cultura que valore no sólo el conocimiento, sino la constancia en el aprendizaje. Proporcione oportunidades de desarrollo y crecimiento profesional para mejorar la retención de personal. Defina los criterios de éxito y las trayectorias profesionales para funciones específicas. Cree incentivos que animen a los principales talentos a compartir su experiencia con otros y a crecer con la organización.

Tome en cuenta estas preguntas para convertirse en un pionero de la zero trust:

- ¿Cómo podemos complementar nuestra arquitectura de seguridad existente con funcionalidades de confianza nula? ¿Qué es fundamentalmente diferente y requiere un nuevo enfoque?
- ¿Con qué métodos está desarrollando nuestra organización una visión integrada de las amenazas para mejorar la visibilidad, incrementar la agilidad de nuestras operaciones de seguridad y mejorar las capacidades de respuesta a incidentes?
- ¿Cómo hemos incorporado los controles de confianza nula en todo nuestro patrimonio digital, incluidas las redes, los datos, los usuarios, las cargas de trabajo y los dispositivos?
- ¿De qué manera podemos adaptar las prácticas de cibertalento para sacar el máximo partido a nuestra estrategia de confianza nula?

Metodología de investigación

En el cuarto trimestre de 2020, el IBM Institute for Business Value, en colaboración con Oxford Economics, encuestó a más de 1,000 líderes de seguridad y operaciones de todos los sectores y zonas geográficas para obtener un conocimiento profundo de lo que constituye una estrategia de seguridad de confianza nula eficaz y de cómo se implementan sus funcionalidades.

Para entender las amenazas a la infraestructura crítica, la encuesta recogió datos sobre los riesgos de seguridad cibernética relacionados con las TI y las OT y la madurez, el rendimiento y la eficacia de las funcionalidades de las organizaciones y sus recursos para administrarlos y mitigarlos. Esto incluyó la adopción de prácticas de vanguardia, así como prioridades e iniciativas para el futuro. También exploró los beneficios que los encuestados han obtenido de su enfoque a las operaciones de seguridad.

El análisis de los datos reveló que el 23% de las organizaciones, un grupo al que denominamos “pioneros de la confianza nula”, están adelantadas en la implementación de funcionalidades de confianza nula para proteger los recursos críticos en los entornos operativos. Al evaluar las medidas de rendimiento y las prácticas de vanguardia, llegamos a la conclusión de que están obteniendo beneficios significativos para el negocio y la seguridad, gracias a este enfoque.

Un análisis factorial confirmatorio (AFC) permitió conocer los factores que impulsan los beneficios. Entre ellos se encuentran las prácticas de ciberriesgo y seguridad operativa; la analítica y la automatización basadas en la IA; y las prácticas de confianza nula para asegurar los datos, las redes, los usuarios, los dispositivos y las cargas de trabajo. A partir de esto, derivamos un enfoque para las operaciones de confianza nula basado en 4 componentes esenciales y un conjunto de prácticas que se refuerzan mutuamente.

Sobre los autores

Chris McCurdy
Vicepresidente y Director General
IBM Security Services
cmccurdy@us.ibm.com

Chris lleva más de 25 años en el negocio de consultoría de TI y ha ayudado a clientes de grandes empresas y gobiernos a diseñar, implementar y gestionar sus complejos programas de tecnología de la información. Dirige la estrategia de comercialización mundial de IBM Security y es responsable de la gestión de las ventas a nivel global. Ha hecho crecer los ingresos del negocio de seguridad de IBM a un ritmo de dos dígitos en los últimos 5 años. Chris es licenciado en Administración de Empresas en Sistemas de Información por la Universidad de Baylor y es Auditor Certificado de Sistemas de Información.

Dra. Shue-Jane Thompson
Senior Partner, Security Strategy & Growth — Distinguished Industry Leader
IBM Global Business Services
shuejane@us.ibm.com
linkedin.com/in/shuejane

Shue-Jane supervisa la innovación de soluciones de seguridad cibernética, la integración y la venta y la entrega de servicios para clientes de todo el mundo. Cuenta con más de 30 años de experiencia en entornos académicos, comerciales, gubernamentales y de gestión de tecnología y negocios internacionales, incluyendo la gestión de muchos programas de TI, cibernéticos, de nube y de operación de misiones a gran escala.

Lisa Fisher
Global Benchmark Research Leader — Industrial, EE&U, T&T and MEA
IBM Institute for Business Value
linkedin.com/in/lisa-giane-fisher
lfisher@za.ibm.com

Lisa es responsable por producir investigaciones de referencia, para todas las industrias y regiones, para prever y articular el impacto de las tecnologías en el negocio desde las perspectivas del ciber riesgo y la seguridad cibernética. Lisa vive y trabaja en Sudáfrica.

Gerald Parham
Global Research Leader—
Seguridad y CIO
IBM Institute for Business Value (IBV)
linkedin.com/in/gerryparham/
gparham@us.ibm.com

Gerald lidera los portfolios de investigación de Seguridad y CIO dentro del IBM Institute for Business Value. Su enfoque principal es la estrategia de seguridad y las cadenas de valor cibernético, en particular la relación entre estrategia, riesgo, operaciones de seguridad, identidad, privacidad y confianza. Tiene más de 20 años de experiencia en liderazgo ejecutivo, innovación y desarrollo de la propiedad intelectual.

Informes de IBV relacionados

Parham, Gerald, Shue-Jane Thomson, Shawn DSouza y Shamla Naidoo. “The new era of cloud security: Use trust networks to strengthen cyber resilience.” Institute for Business Value de IBM. 26 de marzo de 2021 http://ibm.co/cloud-security-cyber-resilience

Comfort, Jim, Blaine Dolph, Steve Robinson, Lynn Kesterson-Townes y Anthony Marshall. “The hybrid cloud platform advantage.” Institute for Business Value de IBM. 2020. https://www.ibm.com/thought-leadership/institute-business-value/report/hybrid-cloud-platform

“2021 CEO Study: Find your essential: How to thrive in a post-pandemic reality.” Institute for Business Value de IBM. 2021. https://www.ibm.com/thought-leadership/institute-business-value/c-suite-study/ceo

Payraudeau, Jean-Stéphane, Anthony Marshall y Jacob Dencik. “Digital Acceleration.” Institute for Business Value de IBM. 2021. https://www.ibm.com/thought-leadership/institute-business-value/report/digital-acceleration

IBM Institute for Business Value

El Institute for Business Value de IBM, que forma parte de IBM Services, desarrolla insights estratégicos basados en hechos para los altos ejecutivos de empresas sobre cuestiones críticas del sector público y privado.

Más información

Para obtener más información sobre este estudio o el Institute for Business Value de IBM, comuníquese con nosotros en iibv@us.ibm.com. Siga @IBMIBV en Twitter y, para obtener un catálogo completo de nuestra investigación o para suscribirse a nuestro boletín mensual, visite: ibm.com/ibv.

Notas y fuentes

1 "IBM 2021 X-Force Threat Intelligence Index". IBM Security. 24 de febrero de 2021. https://www.ibm.com/security/data-breach/threat-intelligence

2 Paul, Kari. "Who's behind the Kaseya ransomware attack – and why is it so dangerous?" *The Guardian*. 7 de julio de 2021. https://www.theguardian.com/technology/2021/jul/06/kaseya-ransomware-attack-explained-russia-hackers; Kenny, Caroline y Pamela Brown. "Greater focus on defense of critical infrastructure against cyberattacks is needed, says cyber agency chief." CNN. 27 de junio de 2021. https://www.cnn.com/2021/06/27/politics/brandon-wales-cyber-security-cnntv/index.html

3 Marks, Joseph "The Cybersecurity 202: The Kaseya attack is a revolution in sophistication for ransomware hackers" *The Washington Post*. 8 de julio de 2021. https://www.washingtonpost.com/politics/2021/07/08/cybersecurity-202-kaseya-attack-is-revolution-sophistication-ransomware-hackers/; Caltagirone, Sergio, Dr. Tom Winston y Kyle O'Meara. "2020 ICS Cybersecurity Year in Review". Dragos. https://www.dragos.com/year-in-review/

4 Kramer, Andrew E., Michael Schwirtz y Anton Troianovski. "Secret Chats Show How Cybergang Became a Ransomware Powerhouse." *The New York Times.* 29 de mayo de 2021. https://www.nytimes.com/2021/05/29/world/europe/ransomware-russia-darkside.html

5 Osborne, Charlie. "Colonial Pipeline attack: Everything you need to know." ZDNet (US Edition). 13 de mayo de 2021. https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know/

6 "Executive Order on Improving the Nation's Cybersecurity." Sitio web de la Sala de Prensa de la Casa Blanca. 12 de mayo de 2021. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

7 Parham, Gerald, Shue-Jane Thomson, Shawn DSouza, y Shamla Naidoo. "The new era of cloud security: Use trust networks to strengthen cyber resilience." Institute for Business Value de IBM. 26 de marzo de 2021 http://ibm.co/cloud-security-cyber-resilience

8 Ibidem.

9 Pollard, Jeff y Stephanie Balaouras. "Craft Zero Trust Security Metrics That Matter - Performance Management: The Zero Trust Security Playbook." Forrester. 24 de marzo de 2020. https://www.forrester.com/report/Craft+Zero+Trust+Security+Metrics+That+Matter/-/E-RES136188?objectid=RES136188

10 Auth, u Open Authorization, es un proceso de autorización. Permite a los servicios de terceros intercambiar información de los usuarios sin que éstos tengan que ceder sus contraseñas. SAML, o Security Assertion Markup Language, es un proceso de autenticación. Ambas aplicaciones pueden utilizarse para el registro único de la web (SSO), pero SAML tiende a ser específico para un usuario, mientras que OAuth tiende a ser específico para una aplicación. Ambos son necesarios y trabajan en conjunto.

11 Johnson, David, Samuel Stern, et al. "Focus On Employees' Daily Journeys To Improve Employee Experience." Forrester. 20 de abril de 2018. https://www.forrester.com/report/Focus+On+Employees+Daily+ Journeys+To+Improve+Employee+Experience/-/E-RES126042?objectid=RES126042

12 Parham, Gerald, Shue-Jane Thomson, Shawn Dsouza y Shamla Naidoo. "The new era of cloud security: Use trust networks to strengthen cyber resilience." Institute for Business Value de IBM. 26 de marzo de 2021 http://ibm.co/cloud-security-cyber-resilience

Sobre Benchmark Insights

Benchmark Insights presenta insights para ejecutivos sobre temas importantes de negocio y tecnología relacionada. Se basan en el análisis de los datos de rendimiento y en otras medidas de evaluación comparativa. Para obtener más información, comuníquese con IBM Institute for Business Value al correo electrónico eniibv@us.ibm.com.

IBM Corporation
Pje. Ing. Enrique Butty 275
C.A.B.A – Argentina
Producido en los Estados Unidos de América
Julio del 2021

BRLA2XP4-LAES-00