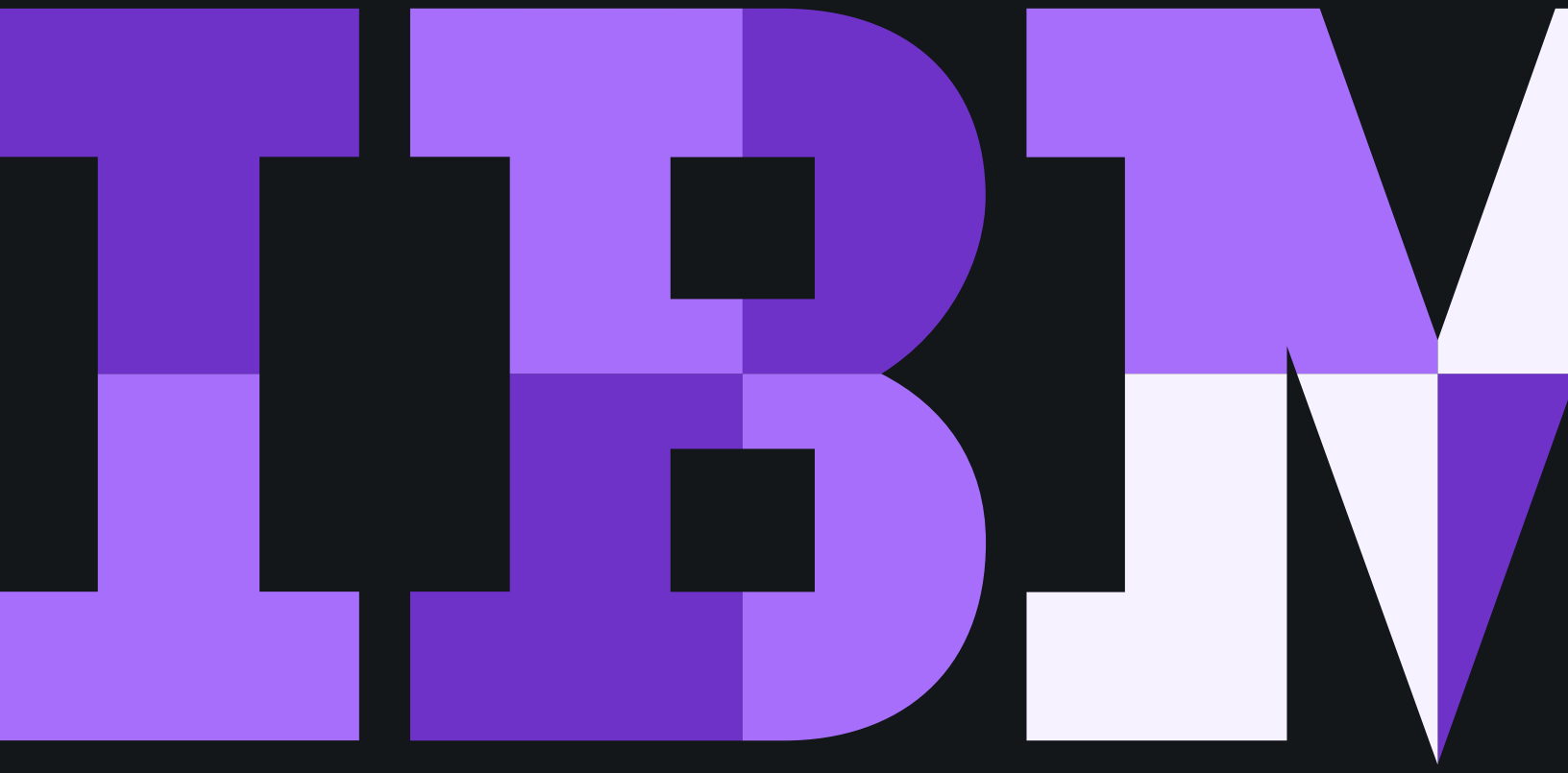
IBM **Security**

Enero de 2020

Fomentar la confianza digital para crear mejores experiencias

Abra nuevas oportunidades de ingresos con una confianza digital transparente y segura



IBM

Contenido

3 Crear confianza en un mundo digital

3 Discernir el contexto para establecer confianza

4 Alinear la seguridad empresarial con la confianza

5 Mantener la seguridad de la empresa

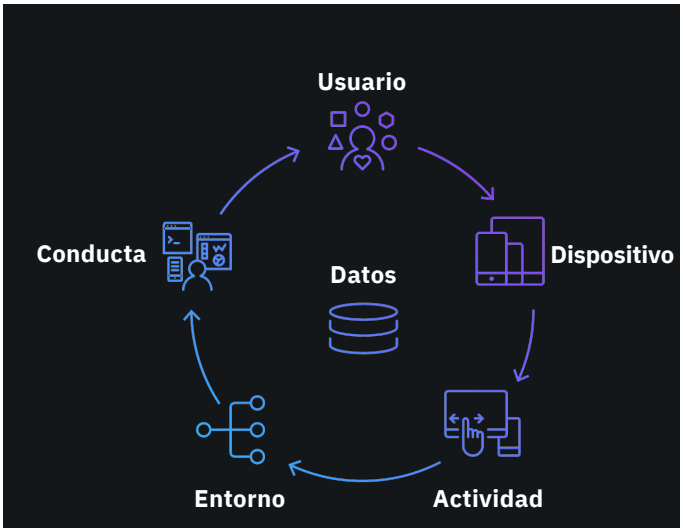
6 Impulsar la transformación digital a través de una base de confianza

7 La seguridad puede abrir oportunidades

Crear confianza en un mundo digital

Como seres humanos, confiamos en nuestros sentidos, memoria e inteligencia para crear confianza. Pero, ¿qué sucede ante la ausencia de esas herramientas? En el mundo digital, se necesita un conjunto complejo de herramientas de información, identificación y seguridad para crear confianza.

La confianza digital es una alineación de controles y privilegios de privacidad que ocurre cuando el usuario indicado tiene el acceso indicado a los datos indicados por la razón y el motivo indicados. Los beneficios de la confianza digital se extienden más allá de la seguridad. Cuando se implementa cuidadosamente, con fluidez y teniendo en mente la experiencia del usuario, la confianza digital puede ofrecer un mayor atractivo que permite una mejor productividad y más oportunidades para el crecimiento de los ingresos.



Obtenga el contexto necesario para analizar el riesgo y crear confianza digital

Discernir el contexto para establecer confianza

Sus clientes le han encargado la protección de su información personal. Además, como profesional de la seguridad, se le ha confiado la protección de la empresa. Hay requisitos de privacidad y cumplimiento a tener en cuenta, cambios empresariales a sortear y, en medio de todo, ataques cibernéticos cada vez más sofisticados que emanan de una comunidad global de estafadores. Sin embargo, los usuarios todavía esperan mecanismos de seguridad que sean simples y fluidos.

En el pasado, su empresa puede haber buscado principalmente soluciones de gestión de identidad y acceso (IAM, por sus siglas en inglés) para crear confianza. **Pero la confianza digital es más que establecer una identidad. Es una combinación de análisis y comprensión que superpone los conocimientos contextuales sobre la identidad** al considerar:

- El usuario y sus atributos únicos.
- El dispositivo y la autenticación específica en el punto final, como las huellas digitales.
- La actividad relacionada con los datos, la aplicación y el usuario.
- El entorno del usuario y el entorno de la red.
- El comportamiento del usuario según lo determinado por el análisis de uso.

Alineación de la seguridad empresarial con la confianza

Como en el caso de cualquier relación, las relaciones digitales se componen de varias pequeñas interacciones a lo largo del tiempo. Con conjunto, estas interacciones proporcionan una visión acumulativa de quiénes somos: nuestros comportamientos, intereses, responsabilidades y roles. Sin embargo, en un mundo digital, las empresas necesitan probar y validar continuamente esas relaciones a medida que las personas se desplazan entre dispositivos, redes, aplicaciones y canales. Esto puede crear fricción cuando a los usuarios se les piden repetidamente contraseñas, pasos de autenticación adicionales o, a veces, se les niega el acceso legítimo a las aplicaciones.

El objetivo de la confianza digital debe ser crear una experiencia segura y sin fricciones para los usuarios. Para lograrlo, las organizaciones deben combinar las tecnologías y procesos de seguridad correctos para automatizar los mecanismos de confianza en lugar de depender de los controles manuales. Por ejemplo, reemplazar una contraseña para cada aplicación con un inicio de sesión único o usar análisis avanzados para iniciar una autenticación de nivel superior, son maneras efectivas de activar los controles de seguridad sin inhabilitar a los usuarios.

Logre una seguridad silenciosa con IBM Security Identity & Access Management

Como empresa, usted debe asegurarse de que las personas indicadas tengan el acceso correcto a los datos en el momento adecuado. Haga lo correcto para sus empleados con IBM Identity & Access Management.

Mire el video

El marco de confianza digital adecuado aprovecha tecnología avanzada, como la detección de fraudes basados en IA, la gestión sólida y fluida de identidad y acceso, la seguridad de los datos con un conjunto integrado de capacidades, y la seguridad móvil con una gestión unificada de múltiples dispositivos. Al combinarlas, estas tecnologías pueden ayudar a su empresa a:

- Extender la seguridad y la identidad de forma fluida entre los sistemas locales y basados en la nube.
- Combinar las tecnologías nuevas y heredadas para crear una base de confianza compartida.
- Agilizar los procesos de seguridad y reducir los costos asociados en toda la organización.
- Brindarles a los equipos de seguridad la visibilidad interfuncional que realmente les permita trabajar en equipo.

IBM Security ayuda a las empresas a crear una plataforma de confianza digital de clase mundial con nuestras soluciones y servicios. Ofrecemos IBM Security Guardium para proteger los datos y garantizar el cumplimiento, IBM Security Identity & Access Management para gestionar las identidades de manera eficiente y validar el comportamiento de los usuarios, e IBM Security MaaS360 para gestionar la seguridad móvil en toda la empresa y más allá.

Mantener la seguridad de la empresa

Crear confianza con sus clientes le ha costado años de esfuerzo, así que quiere mantenerla. Cumplir con los requisitos de cumplimiento y prevenir el fraude puede hacer algo más que proteger su reputación: puede mejorar sus resultados. Usted puede fortalecer la seguridad y simplificar los procesos de inicio de sesión y autenticación, todo mientras navega dentro de los límites de la privacidad, el consentimiento y el cumplimiento. Al aprovechar tecnologías avanzadas como la inteligencia artificial y el análisis del comportamiento, puede equipar mecanismos silenciosos para establecer una confianza digital.

Debido a que las identidades se mueven constantemente entre ubicaciones, dispositivos y aplicaciones, los controles de seguridad deben ser ágiles e invisibles. Esta seguridad ágil e invisible puede adoptar una variedad de formas, que incluyen:

- Controles de autenticación individual y multifactor fáciles de implementar que admiten experiencias fluidas.
- Fuertes mecanismos de autenticación de nivel superior que solo se activan para usuarios en riesgo.
- Pantallas de registro único y barras de inicio de aplicaciones unificadas que simplifican el acceso en varios dispositivos y entre aplicaciones.

IBM Security puede proteger su empresa al tiempo que conserva excelentes experiencias para el usuario. Los servicios de IBM Security pueden ayudarle a identificar, clasificar y proteger los datos críticos. IBM Security Guardium: supervisa la actividad del usuario y alerta a los equipos de seguridad sobre el acceso no autorizado, al tiempo que protege sus datos a través de controles de seguridad como la encriptación, el enmascaramiento y la tokenización. IBM Security Identity & Access Management soporta el cumplimiento normativo (FFIEC, 2FA, PSD2, etc.), gestiona de forma centralizada las certificaciones de acceso, simplifica las incorporaciones y salidas, y prepara su empresa para adaptarse a los nuevos requisitos normativos a medida que surjan. IBM Security Trusteer ofrece protección avanzada contra el fraude utilizando consorcios de datos e IA para hacer un seguimiento de las tendencias en el panorama del fraude en diferentes organizaciones, y luego comparte esos datos para proteger y establecer líneas de defensa.

Obtenga una protección de datos más inteligente con IBM Security Guardium

La protección de datos inteligente vigila con perspicacia, automatiza con un propósito y escala a medida que usted innova. Descubra cómo IBM Security Guardium puede proteger su mundo.

Mire el video

IBM Security Guardium supervisa la actividad del usuario y alerta a los equipos de seguridad sobre el acceso no autorizado.

Impulsar la transformación digital a través de una base de confianza

El impulso hacia la transformación digital está liderado por la promesa de innovación, eficiencia y mejores experiencias. La presencia de la seguridad y la confianza está implícita en dicha promesa. **Las empresas que ofrezcan con éxito experiencias digitales seguras y sin contratiempos serán ganadoras en el mercado digital, ya sea en forma de una mayor productividad de los empleados o de una mayor lealtad de los clientes**. Del mismo modo, aquellas empresas que no alinean sus mecanismos de seguridad con las expectativas de los usuarios encontrarán esa transformación plagada de percances.

¿Qué esperan los usuarios digitales? Seguridad con sencillez. Quieren la protección de la autenticación multifactor sin el trabajo manual de autenticarse varias veces. Quieren herramientas de autoayuda que sean fáciles de usar, ya sea que hayan perdido una billetera o que simplemente hayan perdido una contraseña. Y quieren que su identidad los acompañe sin inconvenientes a través de dispositivos y aplicaciones.

IBM Security puede ayudarle a crear esa base digital de confianza. IBM Security Identity & Access Management ofrece un inicio de sesión único seguro para que los usuarios puedan iniciar sesión una sola vez en las aplicaciones sin requerir contraseñas una y otra vez. IBM Security MaaS360 ofrece a los usuarios la libertad de acceder a las aplicaciones desde cualquier lugar sin sacrificar la seguridad. IBM Security Trusteer protege contra el fraude al tiempo que proporciona funciones ininterrumpidas de incorporación e inicio de sesión que activa de forma inteligente la autenticación de nivel superior solo cuando hay factores de riesgo presentes.

Cree confianza de identidad digital con IBM Security Trusteer.

Con IBM Security Trusteer, sus clientes pueden ir acompañados de sus identidades y relaciones de confianza en el viaje digital con su empresa.

Mire el video

La seguridad puede abrir oportunidades

El enfoque correcto de la confianza digital va más allá de la seguridad para ver la oportunidad que se presenta al crear mejores experiencias para el usuario. En el pasado, la seguridad en forma de largos formularios de registro y múltiples peticiones de contraseña era vista por los usuarios como una barrera para mejorar la experiencia. Lo que los usuarios realmente quieren son mecanismos de seguridad que ocurran tras bambalinas, ya sea una identidad digital que los siga a través de los dispositivos, o análisis discretos del comportamiento que detecten anomalías sutiles, como la forma en que un usuario sostiene su dispositivo.

Piense en cómo se crea la confianza digital en la actualidad. En muchos casos, la obligación de autenticarse recae en el usuario. **Ingresan una contraseña, ingresan un código, responden a una solicitud, etc. Sin embargo, imagine una experiencia diferente, donde las contraseñas se reemplazan por autenticación silenciosa que ocurre automáticamente como parte de un tejido más amplio de confianza contextual...** uno que el usuario nunca toca y nunca ve. En lugar de presentarles los mismos desafíos de confianza a todos los usuarios, solo el pequeño porcentaje de usuarios que presentan riesgo recibe el desafío. Los datos seguirían protegidos, las cuentas aseguradas y la confianza establecida, pero sin la experiencia negativa de tratar a cada usuario como una amenaza potencial.

Las empresas que crean confianza digital correctamente tienen el potencial de establecer relaciones más sólidas, más largas y más rentables con los usuarios.

Las soluciones de confianza digital de IBM Security pueden ayudarle a crear esas relaciones confiables y extenderlas ininterrumpidamente a través de dispositivos y aplicaciones. IBM Security ofrece una solución de confianza digital completa que combina descubrimiento de datos, protección de datos, gestión de identidad y acceso, autenticación, gestión de riesgos, detección de fraudes e inteligencia de amenaza global, que incluye:

IBM Security Trusteer: inteligencia en la nube, IA y aprendizaje automático que se combinan para ayudar a proporcionar una garantía de identidad digital continua con autenticación ininterrumpida y potente detección de fraudes.

IBM Security MaaS360: una solución basada en IA para la gestión unificada de puntos finales ofrecida en la nube y diseñada para proteger datos, respaldar la privacidad y el cumplimiento y ofrecer experiencias móviles seguras y sin interrupciones.

IBM Security Guardium: una completa plataforma de protección que analiza los riesgos de privacidad y cumplimiento, protege los datos y supervisa continuamente las vulnerabilidades.

IBM Security Identity & Access Management: brinde seguridad silenciosa con funciones de gestión de identidad y acceso tras bambalinas que incluyen inicio de sesión único, autenticación multifactor y control de acceso.

IBM **Security**

IBM Global Services
Route 100
Somers, NY 10589
EE. UU.

Producido en Estados Unidos de América
Enero de 2020

WAGXLGAJ