



Informe anual de **seguridad**

Indice

-
- 3** Un mensaje del CEO, Mark W. Begor

 - 4** Un mensaje del CTO & CISO, Jamil Farshchi

 - 5** Nuestro impacto: Seguridad en Equifax 2024

 - 6** Panorama actual: Ciberseguridad 2024

 - 7** Nuestras acciones: Iniciativas de seguridad y resultados en 2024

 - 9** De cerca: Nuestra transformación a una autenticación sin contraseñas

 - 11** Colaboración: Nuestra clave para una colaboración exitosa

 - 12** Análisis comparativo independiente

 - 13** Resumen de resultados: Seguridad Equifax 2024

 - 15** Nuestro camino a seguir

Hemos creado, sin duda, uno de los programas de ciberseguridad más avanzados y eficaces del mundo. No obstante, somos conscientes de que nuestra labor en seguridad es un proceso continuo y que nunca termina.

– Mark Begor

Un mensaje de CEO de Equifax

Mark Begor



Mark W. Begor

Director Ejecutivo
Equifax

El 2024 marcó un capítulo lleno de energía en temas de transformación y crecimiento para la Nueva Equifax (New Equifax). Conseguimos avances significativos hacia la finalización de nuestra transformación de datos y tecnología. De cara al futuro, estamos construyendo sobre los sólidos cimientos de Equifax Cloud™ y nuestras capacidades EFX.IA para impulsar la innovación, los nuevos productos y el crecimiento futuro. La ciberseguridad, es un pilar fundamental de nuestro negocio.

Cuando me uní a Equifax en 2018, me comprometí personalmente a posicionar la compañía como líder de la industria en seguridad y a construir una cultura donde la seguridad fuera parte del ADN de nuestro equipo global, donde todos en Equifax fuéramos responsables de la seguridad. Desde entonces, hemos llevado a cabo una transformación integral de nuestra organización para cumplir esa promesa. En 2024, la madurez de nuestro programa de ciberseguridad superó los principales estándares de referencia de la industria por quinto año consecutivo. Además, nuestro score de postura en seguridad continúa superando los promedios de la industria de tecnología y servicios financieros.

Con la publicación de nuestro quinto Informe Anual de Seguridad, celebramos los avances que hemos logrado hasta la fecha en materia de seguridad. Hemos creado, sin duda, uno de los programas de ciberseguridad más avanzados y eficaces del mundo. No obstante, somos conscientes de que nuestra labor en seguridad es un proceso continuo y que nunca termina.

El 2024 recibió una oleada de nuevas amenazas a la infraestructura global de ciberseguridad. El año pasado, respondimos a más de 15 millones de amenazas cibernéticas, es decir, casi 175 intentos hostiles por segundo, lo que representa un aumento del 25 % respecto a 2023. Mantenerse por delante de esas amenazas requiere evolución e innovación continuas. Exige que pensemos constantemente de manera diferente, razón por la cual estoy orgulloso de iniciativas como nuestra transformación pionera en la industria hacia un sistema sin contraseñas y la implementación de tecnología sin contraseñas en Equifax, incluido el uso de datos biométricos, para ayudar a eliminar la amenaza número uno a la que se enfrentan los equipos de seguridad: el robo de credenciales.

De cara al futuro de Equifax, la seguridad sigue siendo una prioridad estratégica fundamental para nuestro negocio. Continuaremos fortaleciendo y evolucionando nuestro posicionamiento y programas de seguridad para responder y anticiparnos a las amenazas de ciberseguridad en constante evolución. Además mantendremos una comunicación transparente sobre nuestras iniciativas de seguridad, compartiendo nuestras lecciones aprendidas en beneficio de la industria en general.

Un mensaje de Equifax CTO & CISO

Jamil Farshchi



Jamil Farshchi

Director de Tecnología y
Director de Seguridad
de la Información
Equifax

Es común oír que “una innovación ágil es incompatible con una seguridad robusta”. En 2024, decidimos desmontar ese mito. Fuimos testigos de un aumento continuo de las amenazas impulsadas por IA y las tensiones geopolíticas, lo que hizo que el panorama de la ciberseguridad fuera más preocupante que nunca, pero no nos quedamos quietos. Modernizamos nuestras defensas, aceleramos la migración al cloud y rompimos esquemas al atacar la raíz de las brechas de seguridad: las credenciales comprometidas.

Así es, este año, implementamos la autenticación sin contraseñas para nuestra plantilla completa, cerca de 22.000 empleados y colaboradores, para aproximadamente 300 aplicaciones internas. No fue sólo una idea audaz protegernos contra la amenaza del robo de credenciales sino que también redujo los costes operativos de soporte técnico, mejoró la productividad de los trabajadores y preparó nuestras defensas contra tácticas de suplantación de la IA como la clonación de voz. Con esta única implementación, optimizamos la experiencia del usuario y fortalecimos la seguridad.

En Equifax no creemos en el falso mito “seguridad vs. velocidad”. Nuestros resultados hablan por sí solos: lanzamos más de 100 innovaciones de nuevos productos (NPI) en 2024 y al mismo tiempo mantuvimos un score de madurez de seguridad que una vez más superó los estándares de referencia de la industria. El Informe Anual de Seguridad de este año es el quinto consecutivo: un testimonio de nuestro compromiso con la transparencia, la colaboración y la mejora continua.

A lo largo de este proceso, hemos publicado nuestro marco de controles, hemos presentado nuestra postura de seguridad en tiempo real en el cloud a los clientes con CloudControl, hemos afianzado nuestras alianzas públicas y privadas y hemos compartido nuestros conocimientos con toda la comunidad.

¿Estoy satisfecho? En absoluto. Sabemos que los adversarios mejoran constantemente su juego, aprovechando los ataques de día cero, las debilidades de la cadena de suministro y, más recientemente, la IA, para encontrar nuevos puntos de acceso. Nuestra respuesta es redoblar nuestros esfuerzos en seguridad. Y la seguridad ya no es una conversación sobre “desacelerar el negocio”; ahora está en el centro de nuestro impulso y crecimiento.

En 2024, los clientes citaron nuestra reputación en materia de seguridad como una de las razones clave por las que eligieron a Equifax. La velocidad y estabilidad de nuestro productos alcanzaron un récord el año pasado y tenemos mucho más que lograr, pero una cosa está clara: **la seguridad y la innovación no son mutuamente excluyentes.**

En nuestro camino hacia el futuro, seguiremos desafiando los límites, descartando esta idea obsoleta y dedicando todos nuestros esfuerzos a ser los mejores en la protección de los datos de los consumidores y en el fomento de una innovación disruptiva en Equifax. Gracias por estar en este trayecto con nosotros.

Nuestro impacto

Seguridad en Equifax 2024

Más de 15 millones

de ciberamenazas neutralizadas cada día: casi 175 intentos hostiles cada segundo, un incremento del 25 % respecto al año anterior.

Más de 210.000

se realizaron simulaciones para poner a prueba a nuestra plantilla global en diversos escenarios de seguridad.

Cerca de 22.000

empleados y contratistas capacitados con módulos de seguridad personalizados, logrando nuestro ratio de clics más bajo hasta la fecha (2,9 %) en simulaciones de phishing dirigidas.

Más de 3.550

questionarios y auditorías de clientes completadas para reforzar la confianza en nuestra postura de seguridad.

Más de 4.200

usuarios externos accedieron a nuestro marco de controles de seguridad y privacidad en más de 80 países.

Más de 2.250

análisis de riesgo detallados sobre proveedores externos críticos y de alto riesgo, identificando posibles fallos de seguridad antes de que puedan explotar.

Más de 700

organizaciones respaldadas a través de Equifax Breach Services, que ofrecen protección de identidad a más de 22 millones de víctimas de violaciones de seguridad en todo el mundo.

Más de 450

profesionales dedicados a la ciberseguridad protegiendo los datos de los consumidores las 24 horas del día.

Más de 370

controles de seguridad automatizados en el cloud y monitorizados en tiempo real, impulsando una respuesta a las amenazas más rápida y un conocimiento de la postura de seguridad casi instantáneo.

Más de 100

innovaciones de nuevos productos lanzadas al mercado de forma segura, lo que demuestra que la velocidad y la seguridad pueden coexistir.

51

certificaciones y autorizaciones conseguidas de auditores externos, acreditando nuestra fortaleza y rigor.

38

evaluaciones de seguridad física completadas para proteger a nuestra gente, datos y activos.

Más de 30

participamos en foros a nivel mundial compartiendo conocimiento y fortaleciendo las defensas colaborativas.

15

ejercicios teóricos realizados simulando escenarios de crisis a nivel ejecutivo y regional.

5

años consecutivos alcanzando un score de madurez de seguridad que supera todos los estándares de referencia de la industria.

2

integraciones de adquisiciones, completadas siguiendo el nuevo y optimizado manual de seguridad.

Menos de 1

minuto de tiempo medio para detectar amenazas ciberneticas, porque no dejamos que los adversarios actúen.

Panorama actual

Ciberseguridad en 2024

Los temas que se presentan a continuación reflejan las tendencias más relevantes del año pasado y la respuesta de Equifax.

Ataques a la cadena de suministro

En 2024, los ataques a la cadena de suministro aumentaron en frecuencia y sofisticación, impulsados por nuestra dependencia de sistemas interconectados. Un solo proveedor comprometido puede afectar ecosistemas enteros, con proyecciones globales que se estiman hasta 138 mil millones de dólares en daños anuales para 2031.¹

¿Nuestro enfoque? Paradigma Zero Trust, unificación del marco de seguridad para fusiones y adquisiciones y expansión de la visibilidad en tiempo real del riesgo de terceros y también cuando Equifax es el tercero. A través de nuestro panel CloudControl, los clientes obtienen información continua sobre la seguridad de los productos Equifax Cloud™, ofreciéndoles la información que necesitan para tomar decisiones de riesgo informadas.

Robo de credenciales + Ingeniería social impulsada por IA

A lo largo de 2024, los atacantes intensificaron la suplantación de identidad basada en inteligencia artificial (deepfakes, phishing realista e ingeniería social dirigida) para explotar el factor humano. El robo de credenciales ya representa la mayoría de las filtraciones de datos, pero la clonación de voz elevó el fraude del servicio de asistencia técnica hasta convertirlo en una amenaza importante.

Equifax lo abordó implementando la autenticación sin contraseña para casi 22.000 empleados y colaboradores, encarando uno de los principales vectores de ataque de la actualidad. También implementamos la tecnología sin contraseña para las llamadas al servicio de asistencia técnica, mitigando una de las principales amenazas ciberneticas emergentes: la clonación de voz basada en IA. Nos hemos apoyado en principios de Zero Trust y más de 210.000 simulaciones de ingeniería social para defendernos de los principales riesgos de hoy y de mañana.

Vulnerabilidades de día cero y ataques de infraestructura

Con el auge del descubrimiento de vulnerabilidades mediante IA, los ataques de día cero apuntaron tanto a las capas de software fundamentales como a los dispositivos de red. Los delincuentes aprovecharon los fallos recién encontrados, a menudo vendidos en mercados clandestinos, para instalar ransomware o establecer puntos de apoyo sigilosos. Muchas empresas tuvieron dificultades para implementar parches suficientemente rápido, lo que reforzó la importancia de los fundamentos como el escaneo constante y procesos de parcheo exhaustivos.

Respondimos impulsando una cobertura de monitorización continua, aplicando parches en el perímetro de forma rápida y reduciendo nuestros tiempos de respuesta a minutos, evitando que los atacantes aprovecharan estas vulnerabilidades.

Evolución del ransomware

Los ataques de ransomware evolucionaron más allá del simple cifrado de datos en 2024. Los atacantes perfeccionaron los ataques de múltiples etapas, deteniendo operaciones, robando datos, utilizando técnicas de doble o triple extorsión... incluso intentando simular una brecha para forzar el pago. Un solo impacto a gran escala puede provocar innumerables pérdidas y afectar negativamente el tiempo de inactividad y la recuperación.

En Equifax, combatimos a los adversarios con una defensa en capas: detección avanzada en terminales, priorización automatizada de parches, arquitectura de confianza cero y sólidos procesos de backup. Nada de esto es perfecto, pero trabajamos incansablemente para mejorar continuamente en todas las áreas.

¹ Cybersecurity Ventures. Software Supply Chain Attacks To Cost The World \$60 Billion By 2025, Newswires, 3 de octubre de 2023. https://world.einnews.com/pr_news/659375862/software-supply-chain-attacks-to-cost-the-world-60-billion-by-2025

Nuestras acciones

Iniciativas de seguridad y resultados de Equifax en 2024

Fortalecemos nuestra cultura donde la seguridad es responsabilidad de todos

Hicimos que fuera más fácil que nunca para nuestros empleados y colaboradores seguir dando prioridad a la seguridad al aumentar la educación y reducir la fricción.



Nuestros empleados y colaboradores destacan en reconocer y evitar enlaces sospechosos.

Realizamos más de 210.000 simulaciones de phishing a nivel global y logramos nuestra tasa de clics más baja hasta la fecha para correos electrónicos de phishing simulados.

Hicimos que los inicios de sesión en Equifax sean más rápidos y seguros que nunca mediante la implementación de la autenticación sin contraseña para nuestros casi 22.000 empleados y colaboradores en todo el mundo, mitigando uno de los principales vectores de amenazas de seguridad.

La seguridad es responsabilidad de todos en Equifax. Todos velamos por la seguridad y cada uno de nuestros empleados y colaboradores está capacitado, empoderado e incentivado para tratarla como una prioridad personal, una que fomenta la confianza y la velocidad.

Una colaboración mejorada entre Tecnología y Seguridad



En 2024, hicimos todo lo posible para fortalecer la colaboración entre nuestras funciones de Tecnología y Seguridad.

Fusionamos Infraestructura Tecnológica con Operaciones de Seguridad y Continuidad del Negocio y Recuperación ante Desastres (BC/DR) con Gestión de Crisis de Seguridad, unificando nuestra capacidad para ejecutar y responder.

Desmintiendo el mito de que la seguridad sofoca la innovación, lanzamos más de 100 innovaciones de nuevos productos (NPI) en 2024 con seguridad integrada desde cero.

Estas y otras optimizaciones garantizaron una **ejecución más fluida y eficiente**, desbloqueando sinergias que permiten que la seguridad acelere (en lugar de ralentizar) los lanzamientos de productos.

Avanzamos en nuestra excelencia operativa



Continuamos perfeccionando nuestras herramientas, datos y personal para maximizar su impacto.

Al emplear mejoras impulsadas por IA, aceleramos los test de penetración, las revisiones de aplicaciones y el análisis de registros para mejorar la detección de amenazas, todo ello manteniendo la supervisión humana.

Este enfoque en la mejora continua produjo resultados significativos. Nuestro equipo de ciberseguridad ha **reducido los tiempos de respuesta a amenazas entre un 60 % y un 99 % año tras año**, evaluado por el tiempo para detectar, responder y resolver incidentes.

Igualmente, nuestro Centro de Operaciones de Seguridad Física simplificó los procesos y aprovechó la automatización para lograr una **mejora del 33% en el tiempo de respuesta a alarmas locales de alta prioridad**, que ahora tiene un promedio de menos de dos minutos.

Continuación

Iniciativas de seguridad y resultados de Equifax en 2024

Riesgo minimizado en la cadena de suministro

Mejoramos la seguridad de nuestra cadena de suministro en todos los niveles.

Incorporamos métricas de la cadena de suministro en las Instantáneas de Seguridad mensuales de nuestros empleados, enfatizando aún más la importancia en la protección de Equifax por su parte a través de una evaluación adecuada de las conexiones y relaciones con los proveedores.

Además, **reestructuramos las validaciones de seguridad de nuestros proveedores**, midiendo nuevos puntos de datos que revelan cómo los terceros manejan los riesgos emergentes.

Para **mejorar el acceso y la visibilidad de nuestros clientes a los productos Equifax**, lanzamos la versión móvil de nuestro panel CloudControl, una solución pionera que proporciona insights continuos sobre la postura de seguridad de los productos Equifax Cloud™.



Colaboración externa escalada

En 2024, continuamos esforzándonos por convertir la transparencia y la colaboración entre empresas y gobiernos en una práctica global habitual.

Jamil Farshchi, CTO & CISO de Equifax, fue coanfitrión de la nueva miniserie sobre ciberseguridad del FBI con el jefe de la división cibernética del FBI, desmitificando la colaboración con las fuerzas del orden.

Nuestro equipo se asoció con los gobiernos de Costa Rica y Chile para ayudar a reforzar su seguridad, cerrando las brechas público-privadas a nivel internacional.

Además, **continuamos defendiendo la comunicación abierta** para adelantarnos a la próxima generación de amenazas globales.



Potenciamos los beneficios

Una buena seguridad es buena para el resultado final y, en 2024, ayudamos a impulsar los objetivos empresariales en cada área de la compañía.

La seguridad ya no se centra solo en un cumplimiento básico, sino también en ayudar a generar nuevos ingresos, ya que **los clientes mencionan nuestro liderazgo en seguridad como una razón clave por la que eligieron Equifax**.

Obtuvimos la **certificación del Marco de Privacidad de Datos (DPF)**, afirmando nuestro compromiso de facilitar de forma segura las transferencias internacionales de datos desde la Unión Europea a los Estados Unidos.



De cerca: nuestra transformación a la autenticación sin contraseñas

Un plan para eliminar las credenciales

Llamada de soporte técnico

Estándar de la industria	Nuestro enfoque
<p>Antecedentes: Se observa un aumento de ataques de ingeniería social dirigidos al acceso al servicio de asistencia técnica</p> <p>Los ciberdelincuentes atacan a las empresas haciéndose pasar por empleados para obtener acceso privilegiado, a menudo engañando al personal de soporte técnico mediante llamadas telefónicas, abusando de "preguntas de seguridad" fácilmente deducibles (por ejemplo, el apellido de la madre).</p> <p>No hay una solución unificada e inmediata</p> <p>No existía ninguna solución única disponible que abordara esta vulnerabilidad de manera confiable y sostenible.</p>	<p>Nueva forma de autenticarse para llamadas de soporte técnico</p> <p>Identificamos un proveedor emergente y trabajamos con él para ajustar la mejor solución para abordar esta vulnerabilidad: implementando una solución de respuesta de voz interactiva (IVR) basada en aplicaciones que permitiera a los empleados autenticarse automáticamente al llamar al soporte técnico de Equifax.</p> <p>Facilitar a los usuarios el acceso sin contraseña</p> <p>Primero implementamos esta herramienta para acceder al servicio de soporte técnico, para minimizar la interrupción de los trabajadores y cerrar un vector de riesgo significativo. Más tarde se usaría para aplicaciones web sin contraseña y acceso VPN.</p>

Ordenadores portátiles y de sobremesa

Estándar de la industria	Nuestro enfoque
<p>Inicios de sesión basados en contraseña</p> <p>Los usuarios acceden a los ordenadores portátiles y de sobremesa autenticándose con protocolos tradicionales de "nombre de usuario y contraseña".</p> <p>No hay ninguna aplicación de terceros involucrada</p> <p>Los inicios de sesión en dispositivos dependen completamente de mecanismos de autenticación integrados en los sistemas operativos, sin la participación de soluciones de terceros.</p> <p>Biometría no habilitada</p> <p>Las limitaciones de infraestructura comunes impiden el uso generalizado de la funcionalidad de autenticación biométrica.</p>	<p>Cambios en la configuración de inicio de sesión del dispositivo</p> <p>Guiamos a los usuarios a través de las acciones necesarias para permitir inicios de sesión sin contraseña en estaciones de trabajo a través de autenticación biométrica.</p> <p>Implementación por fases</p> <p>Implementamos este método para unos cientos de usuarios a la vez durante varios meses, lo que permitió la resolución de problemas iterativos y comunicaciones personalizadas.</p> <p>Bases para componentes posteriores</p> <p>Estos cambios de configuración sentaron las bases fundamentales para las próximas implementaciones sin contraseña (aplicaciones web y VPN).</p>

Segundo
semestre
2023

Primer
semestre
2024

Aplicaciones web y VPN

Estándar de la industria	Nuestro enfoque
Acceso centralizado a aplicaciones web (SSO) Los usuarios acceden a aplicaciones web (como correo electrónico, herramientas de colaboración y otros sistemas críticos para el negocio) a través de un sistema central de inicio de sesión único (SSO).	Integración sin contraseña Integramos nuestro sistema de inicio de sesión único (SSO) existente con un servicio de autenticación sin contraseña, lo que permite a los usuarios autenticarse en la VPN y en ciertas aplicaciones usando sus dispositivos móviles. Las estaciones de trabajo también aplicaron las autenticaciones biométricas.
Protegiendo aplicaciones web con MFA SSO está protegido por una contraseña y autenticación multifactor (MFA).	Comenzamos con opciones de aceptación voluntaria/incentivos Comenzamos con un enfoque de participación voluntaria, permitiendo a los usuarios cambiar voluntariamente a la autenticación sin contraseña. A partir de ahí pasamos progresivamente de los "incentivos" y los recordatorios a adoptar completamente el método sin contraseña por defecto.
Protegiendo la red con MFA El acceso a la red privada virtual (VPN) está protegido por MFA, lo que requiere que los usuarios ingresen una contraseña cuando se conectan a WiFi en remoto, seguida de una verificación basada en el dispositivo móvil.	Comunicación integral Comunicamos la transición con suficiente antelación y con frecuencia a través de numerosos canales (correo electrónico, posts en la intranet, señalización digital, etc.) e incluimos tanto instrucciones técnicas como comunicación de valores. ¡Realmente nos aseguramos de que cada empleado entienda los beneficios de un flujo de trabajo sin necesidad de contraseñas!
Primer paso crítico El inicio de sesión con VPN protegido con contraseña es un primer paso esencial antes de acceder a cualquier recurso de la empresa, lo que hace que los problemas con las contraseñas sean especialmente perturbadores.	
Impacto en los trabajadores en remoto Debido a su naturaleza crítica y su impacto en los trabajadores en remoto, es probable que la migración de sistemas para acceso VPN con credenciales resulte perjudicial para los usuarios finales.	

Segundo
semestre
2024

Colaboración

Nuestra clave para una colaboración exitosa

Los beneficios de un entorno sin contraseñas son indiscutibles. Pero los desafíos que plantea la transición para alejarse del status quo pueden ser abrumadores. Cambiar los patrones de comportamiento establecidos es difícil. La colaboración fue la fuerza multiplicadora que hizo posible esta transformación.

Co-innovamos con nuestro proveedor

Vimos el potencial de la tecnología sin contraseña para minimizar el riesgo y aumentar la comodidad. Con estos beneficios en mente, tomamos una decisión calculada para respaldar el desarrollo de la tecnología durante sus etapas formativas, forjando un circuito de retroalimentación interactivo con nuestro proveedor. Esta asociación transformadora permitió avances (como un nuevo proceso de verificación IVR para llamadas de soporte técnico) que ahora están ayudando a impulsar la adopción en toda la industria. Otras organizaciones de servicios financieros ya están comenzando a adoptar este camino, que conducirá a mejoras sistémicas de seguridad en toda la cadena de suministro global.

Los equipos de Tecnología y de Seguridad se asociaron estrechamente

Esta iniciativa demostró el valor de la sólida colaboración de nuestros equipos de Tecnología y Seguridad. Se asociaron estrechamente desde la planificación hasta la ejecución, garantizando que tanto la experiencia del usuario como la seguridad se abordaran en cada etapa de esta transformación.

Todos nuestros trabajadores desempeñaron su papel

Cada uno de nuestros empleados y colaboradores trata la seguridad como una responsabilidad personal y su compromiso fue crucial para el éxito de esta transformación. No fueron receptores pasivos del cambio: fueron colaboradores activos en su implementación. Todos adaptaron sus flujos de trabajo diarios para integrar el nuevo sistema. Esto incluyó adaptarse a nuevos métodos de autenticación, adoptar inicios de sesión biométricos y adoptar la aplicación de autenticación móvil. Su voluntad de aceptar el cambio fue fundamental para crear una transición fluida y eficiente, ayudando a mejorar nuestra seguridad.

Esto no era “una solución única para todos”

Equifax es una empresa global y nuestros equipos regionales de Seguridad y Tecnología desempeñaron un papel fundamental no solo para ayudar a implementar nuestra nueva tecnología sin contraseña, sino también para ayudar a empoderar a toda nuestra fuerza laboral. Ofrecieron apoyo personalizado, abordaron desafíos locales únicos e impartieron programas de capacitación personalizados. Este enfoque localizado garantizó que todos los empleados, independientemente de su ubicación, se sintieran apoyados y equipados para afrontar esta transición.

Estamos encantados de mantener la colaboración en 2025 y en adelante, organizando sesiones de intercambio de conocimientos con clientes y socios que tienen como objetivo replicar nuestra transformación empresarial sin contraseñas.

Análisis comparativo independiente

Madurez de seguridad

Nos asociamos con una firma líder mundial en investigación y asesoría para realizar un análisis objetivo en profundidad de la madurez de todo nuestro programa de seguridad.

Score de madurez de seguridad



¿Qué es la madurez de la seguridad?

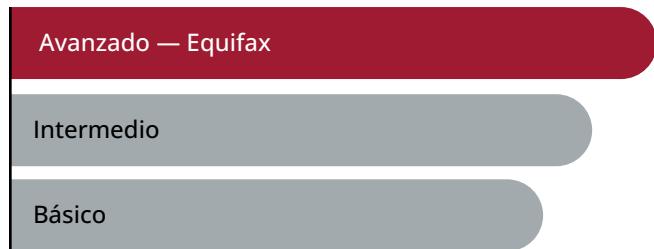
La madurez de seguridad de una organización representa la capacidad de adaptación a las amenazas ciberneticas y gestión del riesgo a lo largo del tiempo.

Mantuvimos el liderazgo con la madurez de nuestro programa de ciberseguridad en 2024, superando todos los principales puntos de referencia del sector por quinto año consecutivo.

Postura de seguridad

Un servicio líder de informes de ciberseguridad monitoriza continuamente la postura de nuestro programa de seguridad y evalúa el riesgo de la cadena de suministro de nuestro ecosistema.

Calificación de la postura de seguridad



Estas son las categorías de calificación asignadas por el servicio de informes que monitorea nuestra postura. Equifax mantiene una calificación que nos ubica en la máxima categoría.

¿Qué es la postura de seguridad?

La postura de seguridad de una organización es su disposición y capacidad para identificar, responder y recuperarse de amenazas y riesgos de seguridad.

Nuestro score de la postura de seguridad superó la media de la industria de tecnología y servicios financieros por cuarto año consecutivo.

Resumen de resultados

Seguridad Equifax 2024

Postura de seguridad y madurez

- Alcanzamos una calificación de madurez de primer nivel al implantar un programa de seguridad alineado con el Marco de Ciberseguridad (CSF) del Instituto Nacional de Estándares y Tecnología (NIST), superando todos los estándares de referencia del sector durante los últimos cinco años.
- Superamos los puntos de referencia de la industria tecnológica en calificación de Postura de Seguridad por cuarto año consecutivo.

Ciberseguridad

- Supervisamos 374 controles de seguridad en el Cloud en tiempo real, mejorando la visibilidad de nuestra postura.
- Implementamos la autenticación multifactor (MFA) obligatoria para el 100% del acceso remoto, reduciendo los riesgos de entrada no autorizada.
- Realizamos la transición a inicios de sesión sin contraseña para nuestros casi 22.000 empleados y colaboradores en todo el mundo, neutralizando las amenazas basadas en credenciales.
- Se mejoraron los tiempos de respuesta a las amenazas entre un 60 % y un 99 % año tras año, gracias a la detección basada en IA, la optimización de procesos y la inteligencia de amenazas integrada.

Cumplimiento

- Obtuvimos con éxito 51 certificaciones con una reducción de costes interanual del 6%, lo que implica un ahorro de \$500 000 solo en 2024.

Fusiones y Adquisiciones

- Integraremos dos adquisiciones anteriores hasta casi su finalización utilizando nuestro marco replicable, con el 94% de los controles alcanzando los estándares de Equifax.

Gestión de riesgos

- Realizamos análisis de riesgo detallados sobre el 100 % de terceros críticos y de alto riesgo de nuestra empresa (2.253).
- Completamos evaluaciones de riesgos en el 100 % de las aplicaciones comerciales (6.308).
- Lanzamos una versión móvil de CloudControl para una visibilidad continua de la postura de ciberseguridad.

Privacidad

- Implementamos una nueva herramienta para la prevención de pérdida de datos (DLP) de correo electrónico, mejorando la información del usuario y la protección de datos.
- Publicamos una Declaración de Privacidad global para Solicitantes de Empleo para aclarar el manejo de datos personales.
- Obtuvimos la certificación del Marco de privacidad de datos (DPF), que permite una transferencia de datos segura desde la Unión Europea o el Reino Unido a Estados Unidos.

Continuación

Seguridad Equifax 2024

Gestión de crisis

- Realizamos 15 ejercicios teóricos con simulaciones de crisis en tiempo real con stakeholders de la empresa, entre ellos:
 - CEO y equipo ejecutivo.
 - Equipos de Crisis Regionales y de Unidades de Negocio.
- Introdujimos nuevos ejercicios de simulación centrados en la seguridad laboral, la recuperación ante desastres y los escenarios del Formulario 8-K. Un Formulario 8-K es un informe que debe presentarse ante la Comisión de Bolsa y Valores de los Estados Unidos para anunciar eventos significativos.
- Implementamos planes de crisis personalizados regionales y específicos de las unidades de negocios.
- Ampliamos nuestra huella de preparación de crisis estableciendo equipos de crisis locales en nuestras operaciones en República Dominicana y Brasil.

Capacitación en seguridad

- Realizamos más de 210.000 simulaciones de phishing y logramos nuestra tasa de clics más baja hasta la fecha para intentos de phishing simulados: 2,9 %.
- Incorporamos métricas de la cadena de suministro en las Instantáneas de Seguridad mensuales de nuestros empleados, lo que enfatiza aún más la importancia de su papel en la protección de Equifax mediante una evaluación adecuada de las conexiones y relaciones con los proveedores.

Servicios de Incidentes de Seguridad

- Apoyamos a más de 700 organizaciones que respondieron a incidentes cibernéticos; en nombre de nuestros clientes, ofrecemos protección de identidad a 22 millones de víctimas de violaciones de seguridad en más de 25 países.

Customer Engagement

- Se completaron 3.551 cuestionarios y auditorías por solicitud de los clientes de Equifax para garantizar el cumplimiento.
- Llevamos de forma segura más de 100 innovaciones de nuevos productos (NPI) al mercado por quinto año consecutivo.

Fraude

- Mejoramos nuestra detección de fraude, lo que provocó un incremento del 41% de reportes de actividades sospechosas frente al 2023, lo que demuestra una mayor visibilidad y estrategias de mitigación más sólidas.

Seguridad Física e Investigaciones

- Completamos 12 tests de penetración física, identificando áreas de mejora continua.
- Realizamos 38 evaluaciones de seguridad física para proteger a los empleados, los datos y los activos.

Nuestro camino a seguir

En 2024, aprovechamos la seguridad como motor de velocidad, confianza y diferenciación en el mercado: eliminando credenciales, fusionando la IA con la detección de amenazas y las operaciones diarias y convirtiendo la adversidad en ventaja. No sólo estamos jugando a la defensiva; estamos avanzando a mayor velocidad, lanzando nuevos productos y estableciendo estándares más altos que nunca. Y aún no hemos terminado. Con la mirada puesta en 2025 y en el futuro, nos enfocamos en la innovación constante. Continuaremos abriendo nuevos caminos en seguridad y tecnología para ayudar a proteger los datos de nuestros clientes contra actores maliciosos y lo compartiremos para el beneficio de la industria en su conjunto.

1550 Peachtree Street NW, Atlanta, GA 30309 • 404.885.8000 • equifax.com