EQUIFAX®

Informe Anual de Seguridad

2025

Indice

Una mayor comunicación, colaboración y transparencia se traducen en una seguridad más sólida.

Un mensaje del CEO de Equifax

Mark W. Begor

Director Ejecutivo
Equifax

2025 fue un año de crecimiento e innovación. Con nuestra inversión de 3 mil millones de dólares en la transformación global de tecnología y seguridad y la creación de Equifax Cloud™ prácticamente finalizada, EFX.AI está impulsando el futuro del Nuevo Equifax. Estamos acelerando la implementación de la tecnología patentada de EFX.AI en nuestros productos, aprovechando los datos únicos y de propiedad exclusiva que distinguen a Equifax en la industria. Esto ha impulsado un número récord de Innovaciones de Nuevos Productos (NPI) que proporcionan la inteligencia necesaria para la toma de decisiones de nuestros clientes a nivel global, permitiéndoles generar nuevas oportunidades más rápido que nunca. Además, estamos ganando eficiencia aprovechando la IA internamente para dedicar menos tiempo a tareas rutinarias y poder centrarnos en los desafíos complejos, creativos y colaborativos que impulsan a nuestra compañía hacia adelante.

Nuestro compromiso con la seguridad es inquebrantable y establece una base sólida para esta innovación.

Cuando me uní a Equifax en 2018, asumí el compromiso personal de posicionar a Equifax como líder de la industria en seguridad de datos, así como de construir una cultura en la que todos en Equifax sean responsables de la seguridad. Hemos transformado cada aspecto de nuestra organización para cumplir esta promesa, haciendo que la seguridad sea parte del ADN de nuestro equipo global. Con la publicación de nuestro sexto Informe Anual de Seguridad, nuestra firme determinación en el liderazgo de seguridad se refleja con claridad: nuestro nivel de madurez de seguridad ha superado los principales puntos de referencia de la industria durante seis años consecutivos así como nuestra puntuación de postura de seguridad, que ha superado los promedios del sector de Tecnología y Servicios Financieros por quinto año consecutivo.

Al mismo tiempo, asumimos que, en lo que a seguridad se refiere, no existe una línea de meta y debemos estar en continúa evolución.

En 2025 el auge de la IA impulsó un panorama de nuevas amenazas en ciberseguridad, caracterizadas por una convergencia de volumen, velocidad y sofisticación. Fuimos conscientes de la existencia de agentes autónomos e IA industrializada que amplificaron los ataques tradicionales, aumentando el alcance de los riesgos debemos defender. Equifax estaba preparado. Guiados por nuestro enfoque en la optimización constante y maximizando nuestra infraestructura nativa en la nube, hicimos frente a más de 19,8 millones de amenazas de ciberseguridad diarias, mientras realizábamos más de 240.000 simulaciones para entrenar a nuestra plantilla a nivel global y prepararnos para los nuevos riesgos que se avecinaban.

Actualmente, se prevé que muchas empresas se vean desplazadas o pierdan su posición en el mercado debido al impacto de la IA, pero en Equifax, en cambio, estamos aprovechando para transformar la industria y consolidar nuestro liderazgo en seguridad. Estamos orgullosos de que la Inteligencia Artificial haya transformado la forma en que operamos, con casi el 90% de nuestro equipo global utilizandola durante el pasado año. Dotamos a nuestra organización de los medios necesarios para innovar utilizando la IA bajo rigurosos mecanismos de control, desde filtros automatizados de seguridad de contenido hasta marcos de desarrollo seguro.

Garantizando así que nuestros modelos sean explicables, seguros y que nuestros datos permanezcan protegidos. Continuaremos optimizando y maximizando las capacidades de la IA para fortalecer nuestras defensas, garantizar su uso de manera segura para la innovación y defendernos ante las amenazas que esta pueda generar. Es importante destacar que no solo mantendremos nuestro enfoque en la seguridad, también continuaremos ayudando a nuestros clientes, socios y consumidores a reforzar sus propias posturas de ciberseguridad en beneficio del mercado.

Un mensaje del CISO de Equifax

Jeremy Koppen

Director de Seguridad
de la Información (CISO)
Equifax

Llegué a este rol con una perspectiva distinta sobre la evolución de la seguridad en Equifax. Antes de incorporarme como Director de Seguridad de la Información en mayo de 2025, fui Director General en Mandiant, compañía en la que tuve el privilegio de trabajar junto al equipo de Equifax durante las primeras y decisivas etapas de su transformación. Durante los años siguientes, seguí de cerca y con admiración el progreso desde fuera de la organización.

Sabía que Equifax había sido reconocido como líder de la industria en seguridad. Pero cuando llegué, no encontré un equipo celebrando sus logros. Encontré un equipo con un fuerte impulso y un nivel de enfoque que destacaron desde el primer momento.

Esa intensidad es crítica porque el panorama de amenazas de 2025 estuvo marcado por una convergencia de volumen, velocidad y sofisticación. Vimos cómo los agentes autónomos y la IA industrializada amplificaron los ataques tradicionales expandiendo radicalmente el alcance de lo que debemos defender. En este entorno, simplemente redoblar esfuerzos no constituye una estrategia. Debemos evolucionar proactivamente para mantenernos a la vanguardia.

Por eso, este año nos enfocamos en **una optimización constante.**

La IA ha transformado de raíz nuestra forma de trabajar. Aprovechando nuestra infraestructura nativa de la nube, utilizamos la IA para agilizar nuestro Centro de Operaciones de Seguridad (SOC) y automatizar tareas rutinarias. De este modo, nuestros expertos pueden centrarse en las amenazas realmente críticas. También mitigamos los riesgos de la “IA adversaria”, implementando controles personalizados para bloquear inyecciones de prompt ocultos y deepfakes. Además, garantizamos el uso seguro de la IA por parte del negocio, diseñando sistemas que eliminan fricciones y estableciendo, al mismo tiempo, las salvaguardas necesarias para que el equipo aproveche las capacidades de la IA de forma rápida y responsable en todas las áreas de Equifax. Gracias a este enfoque, garantizamos que **la seguridad continúa consolidándose como un verdadero motor del crecimiento y la innovación para el negocio en Equifax.**

La prueba está en nuestros resultados. En 2025, Equifax lanzó de forma segura más de 180 Innovaciones de Nuevos Productos (NPI, por sus siglas en inglés) — nuestro sexto año consecutivo con más de 100. Esto demuestra que una seguridad robusta no es un obstáculo para la innovación, sino un motor para la innovación y el crecimiento rápido.

Pero, por encima de todo, nuestro mayor activo es que la seguridad en Equifax es una responsabilidad compartida. Vemos esto cuando nuestros equipos de Tecnología construyen una arquitectura segura por diseño, y a medida que nuestros compañeros de Finanzas y Legal analizan minuciosamente el riesgo de terceros. También lo vemos en nuestras plantilla a nivel global que actúan como nuestra primera línea de defensa, detectando intentos novedosos de phishing y reforzando nuestras defensas automatizadas con la intuición humana.

¿Estamos satisfechos? NO, absolutamente no. Aumentamos nuestra madurez de seguridad nuevamente en 2025, pero las amenazas a las que nos enfrentamos continúan evolucionando. Continuaremos adoptando nuevas tecnologías, optimizando nuestras defensas y priorizando nuestros esfuerzos basándonos en el impacto, no en la facilidad.

Estoy orgulloso de liderar un equipo como este, con la enorme ambición de superar el status quo. Nuestra búsqueda del liderazgo en seguridad no tiene límites.

Nuestro impacto:

La seguridad de Equifax en 2025

Mais de 19,8 millones
de ciberamenazas bloqueadas cada día — casi 230 intentos de ataque cada segundo, representando un aumento del 30% con respecto al año pasado.

Más de 240.000
simulaciones lanzadas para entrenar a nuestra plantilla a nivel global en diversos escenarios de seguridad.

Alrededor de 22.000
empleados y contratistas capacitados con módulos de seguridad personalizados, aumentando la dificultad de las simulaciones para reflejar el entorno de amenazas en evolución.

Más de 4.000
usuarios externos accedieron a nuestro marco de controles de seguridad y privacidad en más de 70 países.

Más de 3.700
cuestionarios de clientes y solicitudes de evidencia completados para reforzar la confianza en nuestra Postura de Seguridad.

Más de 2.280
análisis en profundidad de riesgos sobre proveedores externos críticos y de alto riesgo, identificando posibles puntos débiles de seguridad antes de que puedan ser explotadas.

Más de 400
profesionales dedicados a la ciberseguridad que protegen los datos de los consumidores las 24 horas del día.

Más de 330
controles de seguridad automatizados en la nube monitoreados en tiempo real, lo que impulsa una respuesta a las amenazas más rápida y una visibilidad casi instantánea de nuestro estado de seguridad.

Más de 180
Innovaciones de Nuevos Productos llevadas al mercado de forma segura — nuestro sexto año consecutivo con más de 100, demostrando que la velocidad y la seguridad pueden ir de la mano.

52
certificaciones y autorizaciones obtenidas de auditores externos, validando nuestra solidez y nuestro nivel de exigencia.

43
evaluaciones de seguridad física completadas para proteger a nuestra gente, datos y activos.

Más de 35
foros en los que participamos a nivel mundial para compartir conocimiento y fortalecer las defensas colaborativas.

18
ejercicios teóricos que simulan escenarios de crisis a nivel ejecutivo y regional.

6
años consecutivos logrando una puntuación de madurez de seguridad que supera a todos los principales puntos de referencia de la industria.

2
integraciones de adquisiciones completadas bajo el nuevo protocolo de seguridad ágil y simplificado.

1
minuto es el tiempo promedio de detección de ciberamenazas.

Situación actual:
Ciberseguridad en 2025

Reorientación de prioridades

En 2025, las empresas continuamos percibiendo un aumento en el volumen, frecuencia y velocidad de los ciberataques. En este contexto, los equipos con mayor madurez tecnológica adoptaron la IA para ampliar el alcance de aquello que podía neutralizarse de forma automatizada, para reducir las amenazas que requerían intervención humana. Simultáneamente, la industria perfiló su definición de riesgo. Si bien las puntuaciones de riesgo genéricas siempre han carecido de matices y contexto, el panorama de amenazas de 2025 las hizo especialmente engañosas.

Para abordar este desafío, los líderes de seguridad comenzaron a utilizar puntuaciones de riesgo personalizadas, más ajustadas a las características específicas de los entornos de sus empresas. Estas evaluaciones consideraron variables como si un sistema está expuesto a internet, si su acceso está estrictamente controlado o si maneja datos sensibles. De esta forma, los equipos pudieron descartar puntos débiles con altas puntuaciones de riesgo teórico pero bajo impacto real en su organización, y centrar sus esfuerzos en aquellas vulnerabilidades que representan una amenaza concreta para el negocio.

La evolución del riesgo de terceros

Las vulnerabilidades de la cadena de suministro han desafiado a la industria durante más de una década, pero en 2025, la estrategia cambió. Los atacantes pasaron de explotar vulnerabilidades de software a centrarse en secuestrar accesos legítimos. Al comprometer a los proveedores y robar sus credenciales, los criminales se convirtieron en "el proveedor" — utilizando conexiones autorizadas para eludir las defensas sin ser detectados.

Esta evolución transformó lo que antes se consideraba un problema en la cadena de suministro en una verdadera crisis de identidad digital, obligando a las organizaciones a verificar a sus socios y proveedores de confianza con el mismo rigor con el que evalúan las amenazas externas.

Reto de gobernanza de agentes de IA

A medida que la IA evolucionó de simples chatbots a poderosos agentes capaces de conectarse a sistemas internos para hacer tareas operativas, quedó claro que, si bien estas herramientas podían acceder a datos sensibles, carecían de los controles para mantenerlos seguros.

Esto creó una división en la industria. Algunas empresas se lanzaron, asumiendo el riesgo de usar herramientas que tal vez no podrían monitorear o detener completamente durante una emergencia. Otras organizaciones frenaron la adopción, ante el riesgo de avanzar sin la visibilidad suficiente. Pero los equipos más resolutivos encontraron una tercera vía. Construyeron sus propias verificaciones de seguridad para proteger sus datos, aprovechando los controles fundamentales que ya tenían implementados. Al mismo tiempo, colaboraron con sus proveedores para fortalecer la arquitectura y el entorno tecnológico.

El crecimiento de la superficie de ataque de la gestión de identidades y credenciales

La superficie de ataque asociada a la identidad se amplió de forma drástica en 2025, exponiendo tanto a personas como a sistemas. Los atacantes aprovecharon la IA para lanzar campañas de phishing y deepfakes hiperrealistas que, con frecuencia, lograban engañar incluso a empleados con experiencia en seguridad. Al mismo tiempo, el ecosistema de identidades de sistemas creció sin suficiente control.

A medida que las empresas aceleraron sus procesos de automatización, generaron miles de credenciales no personales (como claves API) que no contaban con los mismos niveles de supervisión y control que la que se aplica a los usuarios. Los atacantes aprovecharon estos vectores de ataque desatendidos, pero con altos niveles de acceso, demostrando que hoy proteger la identidad requiere gobernar y asegurar cada entidad que se conecta a la red, ya sea un usuario o un sistema.

Nuestras acciones:

Iniciativas y resultados de seguridad de Equifax en 2025

Evolución y fortalecimiento de la cultura de seguridad

Cada empleado y contratista reconoce que la seguridad es una parte crítica de su trabajo. Reforzamos esto introduciendo una plataforma impulsada por IA que ofrece capacitación personalizada y lúdica a toda nuestra plantilla.

Validamos su capacitación a través de más de **240.000 simulaciones de phishing a nivel global en 2025** — un 15% más que en 2024 — aumentando la dificultad para adaptarnos al panorama de amenazas actual. Y ampliamos nuestra instantánea de seguridad para incluir seis nuevos comportamientos basados en roles, impulsando una mejora del 10% en algunos comportamientos en solo cuatro meses, demostrando que dar visibilidad al usuario genera un impacto real.

Demostrando que la seguridad es una prioridad personal, los empleados utilizaron nuestras nuevas herramientas de informes de phishing para identificar 20.000 amenazas potenciales en solo seis meses, detectando así casi 1.500 indicadores maliciosos confirmados.

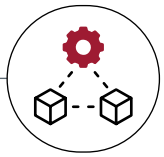
La seguridad como un factor de diferenciación en el mercado

La seguridad es un valor competitivo que permite el éxito comercial. Escalamos nuestras defensas para permitir el lanzamiento seguro de un número récord de NPI en 2025, mientras obteníamos 52 certificaciones, incluyendo autorizaciones críticas del gobierno de los EE.UU.

También implementamos una base de conocimientos de IA especializada que genera respuestas a cuestionarios de seguridad basadas únicamente en nuestra documentación de políticas de la compañía. Las métricas tempranas muestran una tasa de acierto del 67% en el primer intento, superando con creces las soluciones heredadas y permitiéndonos así **satisfacer las necesidades de los clientes con una velocidad sin precedentes**.

En 2025, una empresa líder de telecomunicaciones de la lista Fortune 50 posicionó **públicamente a Equifax como referente en el sector**. Un reconocimiento por "hacer las cosas bien en materia de seguridad", destacando nuestra transparencia como un factor determinante de su confianza en nosotros. El compromiso Equifax con la transparencia tiene un alcance global: el año pasado, más de 4.000 usuarios en 70 países accedieron a nuestro marco público de controles de seguridad para fortalecer sus propias defensas.

Seguridad e ingeniería unificadas



En 2025, **combinamos nuestras funciones de Arquitectura de Seguridad y Arquitectura Tecnológica**, uniendo desarrolladores y defensores para impulsar soluciones consistentes y automatizadas a nivel global.

A través de esta base compartida, diseñamos la arquitectura de nuestros sistemas para eliminar barreras operativas. Al proporcionar a los equipos de ingeniería una **plataforma de desarrollo ágil y automatizada** que ofrece despliegues con un solo clic y una integración fluida les dimos autonomía para **lanzar de forma segura un 50% más de cambios**, demostrando que podemos acelerar la innovación tecnológica y de productos sin comprometer la seguridad.

Esta velocidad operativa se extendió también a nuestras defensas. Con mejor visibilidad, identificamos, evaluamos y aseguramos la remediación de más de 3.700 componentes de infraestructura crítica — **un aumento del 164% en el alcance de nuestra supervisión** año tras año. A pesar de este aumento de volumen, mantuvimos un **tiempo medio de resolución menos de 24 horas**, demostrando que cuando la seguridad es colectiva, solucionamos los problemas tan rápido como los detectamos.

Co-innovamos con proveedores y socios

Equifax continúa impulsando los estándares de la industria a través de la co-innovación. Una estrategia donde **nos asociamos directamente con nuestros proveedores de seguridad para definir mejoras de productos y servicios** que aseguran no solo nuestro entorno, sino también el de otras empresas.

Ayudamos a nuestro proveedor de protección de endpoints a **eliminar puntos ciegos de visibilidad** en la infraestructura de servidores Linux, impulsamos a nuestro proveedor de nube a **desarrollar controles de acceso más granulares** para la IA generativa, presionamos por correcciones de hardware críticas y trabajamos con nuestro proveedor de gestión de identidad y acceso para **optimizar la infraestructura, reduciendo la latencia** para mejorar la productividad.

Esta colaboración también se extendió más allá de los proveedores de tecnología al sector público. Por ejemplo, nos unimos a 25 socios y a las autoridades canadienses para ayudar a **ejecutar más de 3.000 acciones contra redes de fraude**. También ampliamos nuestra asociación en América Latina, **trabajando con organismos gubernamentales en El Salvador y Costa Rica** para avanzar en la educación de seguridad de IA y dar forma a marcos de estandarización nacional.

Usando la IA para mejorar la seguridad

Aplicamos nuevas tecnologías para hacer lo que siempre hemos hecho, solo que ahora más rápido y con mayor precisión. Al implementar la IA como un potenciador estratégico de nuestras capacidades, actualizamos nuestra capacidad no solo para clasificar y remediar amenazas, sino también para acelerar las decisiones de seguridad críticas que impulsan los resultados del negocio.

Comenzamos a usar la IA agéntica para manejar alertas rutinarias, liberando a los analistas para enfocarse en amenazas complejas.

Los Centros de Operaciones de Seguridad (SOC) se enfrentan a un desafío universal: la fatiga de alertas. Una situación en la que los analistas deben revisar y filtrar miles de notificaciones diarias, muchas de ellas de bajo riesgo o irrelevantes.

Por eso, diseñamos y probamos un agente de gestión de alertas especializado con un cometido estricto: analizar alertas de baja fidelidad y solo cerrarlas si cumplen con unos rigurosos criterios de resolución.

Con la adopción completa en nuestro SOC global programada para 2026, esta herramienta ha añadido una nueva capa al conjunto de automatización que acelera el cierre de problemas mientras ayuda a los expertos a pasar menos tiempo cerrando tickets y a poder centrarse en la detección y análisis de **amenazas más sofisticadas**.

Impacto | Gestión automatizada de casi el **50%** de todos los tickets de incidentes de SOC.

Redujimos drásticamente el ciclo de validación de nuestras defensas ante nuevas amenazas.

Tradicionalmente, validar nuestras defensas contra las últimas tácticas criminales era un proceso manual. Para cuando se diseñaba una prueba, el adversario a menudo ya había evolucionado su ataque.

Para reducir esta ventana, construimos un motor impulsado por IA que lee informes de ciberamenazas no estructurados e instantáneamente los convierte en escenarios de ataque accionables. Esto nos permite simularlos y poner a prueba nuestras defensas pocos días después de que se detecten nuevas tácticas, asegurando que nuestros sistemas de protección se mantengan actualizados y alineados con las amenazas más recientes.

Impacto | **Validación de defensas** en días, no en meses, tras la detección de una amenaza.

Integramos asistentes de IA personalizados para reducir drásticamente la fricción para el negocio.

Para asegurar que nuestros procesos de seguridad respaldan la innovación rápida y el diálogo fluido con el cliente, usamos la IA para agilizar dos flujos de trabajo críticos.

Primero, un asistente de IA ayuda a los arquitectos de seguridad a analizar diseños de manera instantánea, reduciendo el tiempo de resolución de consultas de seguridad de 46 a 18 días.

Segundo, una base de conocimientos de IA acelera la respuesta a cuestionarios de seguridad de los clientes basando las respuestas en las políticas de la compañía. La herramienta alcanzó una tasa de acierto del 67% en el primer intento, lo que permitió a nuestros equipos responder a los clientes con mayor rapidez y precisión.

Impacto | Reducción de los tiempos de consulta de seguridad en un **61%** y en las respuestas a clientes.

Pasamos de detectar deficiencias a solucionarlas automáticamente.

Las herramientas de seguridad tradicionales se limitan a la detección, alertando a los desarrolladores sobre una vulnerabilidad e incluyéndola en su lista de tareas pendientes. Nosotros fuimos un paso más allá: implementamos agentes de IA capaces de, no solo identificar problemas, sino también de resolverlos automáticamente.

Usando una arquitectura de IA personalizada, nuestro sistema analiza vulnerabilidades en los contenedores y genera automáticamente la corrección de código. Posteriormente envía una "solicitud de extracción" (pull request) para que el desarrollador revise y fusione. De esta forma, la seguridad deja de ser una barrera que ralentiza el avance a un colaborador que depura el código.

Impacto | Gestión de **más de 213.000 hallazgos** anualmente sin ralentizar la entrega de productos.

Garantizando el uso seguro de la IA por parte del negocio

A medida que nuestra plantilla y desarrolladores adoptaron la IA para impulsar la innovación, nuestra prioridad ha sido asegurar que pudieran hacerlo de forma segura. Nos enfocamos en construir las barreras de protección necesarias — desde filtros de seguridad de contenido automatizados hasta marcos de codificación segura — que permitieron a nuestros equipos adoptar las poderosas nuevas herramientas sin exponer a la empresa a posibles fugas de datos o riesgos no gestionados.

Creamos modelos basados en IA más seguros para ser usados con datos de negocio

Diseñamos nuestra arquitectura para que la seguridad de nuestros datos no dependa exclusivamente de un proveedor de modelos. En su lugar, implementamos una capa de control independiente situada entre nuestros empleados y la IA.

Esta capa depura cada prompt y respuesta, detectando posibles fugas de datos sensibles o ataques de inyección maliciosos antes de que interactúen con un modelo de IA. Esto asegura que, incluso si un modelo externo se ve comprometido, nuestros datos permanecen protegidos.

Impacto | Implementación de una **capa de control unificada e independiente** para la inyección de prompt y la protección de datos personales.

Diseñamos los protocolos para que cualquier empleado pueda crear soluciones de IA.

Para escalar la IA de forma segura internamente en Equifax nos alejamos del control manual hacia la Política como Código (Policy-as-Code). Nuestros puntos de control validan automáticamente cada nuevo agente antes de su paso a producción y el monitoreo continuo detecta si un modelo comienza a desviarse o comportarse de manera impredecible.

Esto nos posiciona para cumplir con las regulaciones de IA en constante evolución asegurando que, para casos de uso de alto riesgo, se incluya la supervisión y aprobación humana en el ciclo y contemos con sistemas de desconexión automática con capacidades de reversión instantánea. Este marco nos permite democratizar las herramientas de IA con la confianza de que los controles de seguridad están siempre activos.

Impacto | Despliegue de forma segura herramientas de IA generativa a **más de 22.000 empleados y contratistas** a nivel mundial.

Eliminamos la "shadow AI" con controles específicos y un catálogo de herramientas aprobadas.

Rechazamos el enfoque de "activado por defecto" de los principales proveedores. Cuando las nuevas funcionalidades introducían riesgos potenciales para la seguridad de los datos, las pausamos selectivamente hasta que pudieran cumplir con los estándares y controles de seguridad de Equifax.

Simultáneamente, pasamos de bloquear la innovación a guiarla. Hacemos cumplir una estricta lista de denegación para modelos externos de alto riesgo, mientras proporcionamos acceso instantáneo a un catálogo de herramientas corporativas preaprobadas. Esto asegura que nuestros desarrolladores trabajen sobre una base sólida y de confianza.

Impacto | Reducción del riesgo a través de la **habilitación selectiva y regulada de funcionalidades**.

Implementamos conexiones de código seguras para agentes de IA.

A medida que la IA pasa de simples chatbots a agentes autónomos que pueden editar código, el riesgo de un agente con "privilegios excesivos" crece. Para abordar esto, definimos un marco de seguridad rígido para el Protocolo de Contexto del Modelo (MCP).

Al permitir a los desarrolladores usar servidores MCP remotos para acceder a código en vivo de forma segura, garantizamos que puedan aprovechar la última asistencia de IA sin dar acceso sin control a toda la base de códigos.

Impacto | Integración **operativa y segura entre la IA y el código.**

Defendiendo contra amenazas de IA

Siendo conscientes de que los criminales también estaban adoptando herramientas impulsadas por IA para crear suplantaciones hiperrealistas y lanzar ataques más rápidos y complejos, reajustamos nuestras defensas para detectar estas amenazas y protegernos ante ellas, asegurando que nuestros controles siguieran siendo efectivos contra una nueva generación de fraude y ciberataques impulsados por la IA.

Bloqueamos con éxito un ataque de deepfake dirigido a nuestro liderazgo.

En 2025, la amenaza teórica de la clonación de voz por IA se convirtió en una realidad. Nuestros equipos cibernéticos detectaron un ataque sofisticado de ingeniería social con una nota de voz deepfake suplantando a nuestro CEO.

No solo detuvimos el ataque, sino que lo usamos para fortalecer nuestra inmunidad. Analizamos instantáneamente los patrones lingüísticos del ataque e implementamos reglas de detección personalizadas en nuestras pasarelas de correo electrónico, blindando así a la organización contra futuros intentos de fraude generados por IA.

Impacto | Transformación de un **intento de deepfake en tiempo real** en una refuerzo permanente de nuestras defensas.

Descubrimos y bloqueamos ataques ocultos diseñados para engañar a los modelos de IA.

A medida que integramos la IA, nuestro equipo de Red Team descubrió una vulnerabilidad emergente: los ataques podían incrustar prompts ocultos, indetectables para el ojo humano, que engañan a los modelos de IA para distribuir malware.

Trasladamos con éxito este descubrimiento de un caso de prueba a un control de prevención activo. Implementamos la lógica para eliminar estos comandos ocultos antes de que lleguen a nuestro ecosistema, cerrando un punto ciego que muchas organizaciones aún no han detectado.

Impacto | Del **descubrimiento del ataque simulado al control de prevención** en tiempo récord.

Implementamos defensas adaptativas para interceptar ataques evasivos impulsados por IA.

Los atacantes están usando la IA para escribir código que se reescribe constantemente para eludir los filtros tradicionales. Estos ataques “polimórficos” están diseñados para mutar cada vez que atacan.

Como respuesta, implementamos lógica de evasión personalizada en nuestras defensas de endpoint. En lugar de buscar una firma de archivo específica, nuestras herramientas analizan el comportamiento del código, permitiéndonos detectar y bloquear malware generado por IA, independientemente de cómo se enmascare.

Impacto | Bloqueo de **malware de IA evasivo** que elude los filtros tradicionales.

Reforzamos nuestros portales de consumidores para protegerlos frente a oleadas de bots impulsados por IA.

La automatización permite a los criminales atacar a una escala que los humanos no pueden igualar, usando “enjambres” de bots para extraer datos o probar credenciales robadas contra nuestros portales de consumidores. Para proteger los datos de alto valor, implementamos perfiles avanzados de bloqueo avanzado.

Estas defensas identifican y neutralizan tácticas impulsadas por IA como “email tumbling” (una técnica que modifica rápidamente una dirección de correo para eludir filtros), asegurando que nuestros datos permanecen accesibles para las personas, pero no para los bots.

Impacto | Neutralización de **campañas sofisticadas de extracción de credenciales** en tiempo real.

Evaluaciones comparativas independientes

Madurez de Seguridad

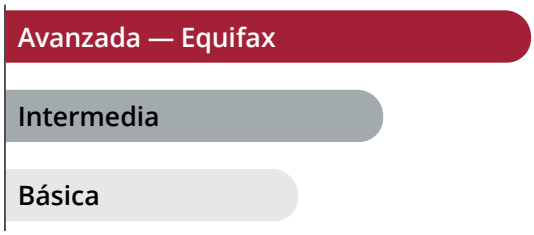
La madurez de nuestro programa de ciberseguridad, (con una puntuación de 4,4 en el Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología, NIST, de 2025) mejoró en 2025, superando a todos los principales puntos de referencia de la industria por sexto año consecutivo.

Puntuación de Madurez de Seguridad

Postura de Seguridad

Nuestra puntuación de Postura de Seguridad en 2025 superó los promedios de la industria de Tecnología y Servicios Financieros por quinto año consecutivo.

Calificación de 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 posiciona en la categoría más alta.

¿Qué es la Madurez de Seguridad?

La Madurez de Seguridad de una organización representa su capacidad para adaptarse a las ciberamenazas y gestionar el riesgo a lo largo del tiempo.

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

¿Qué es la Postura de Seguridad?

La Postura de Seguridad de una organización es su preparación y la capacidad para identificar, responder y recuperarse de amenazas y riesgos de seguridad.

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

Resumen de resultados:

La Seguridad de Equifax en 2025

Madurez y Postura de Seguridad

- Conseguimos un resultado récord en madurez de seguridad, alcanzando una puntuación de 4,4 en el Marco de Ciberseguridad del NIST (National Institute of Standards and Technology), superando los principales referentes del sector por sexto año consecutivo.
- Conseguimos una calificación de Postura de Seguridad que superó los puntos de referencia de la industria tecnológica por quinto año consecutivo — demostrando una Postura de Seguridad consistente ante clientes y reguladores.

Cumplimiento

- Obtuvimos con éxito 52 certificaciones en 2025 con una reducción del 2% año tras año en el coste por certificación y una disminución del 66% desde 2018.
- Simplificamos el cumplimiento lanzando un portal de evidencia automatizado y un nuevo tablero para mapear hallazgos directamente a controles específicos — reduciendo la carga de cumplimiento manual.

Fusiones y Adquisiciones

- Logramos la integración de dos adquisiciones anteriores utilizando nuestro marco de Fusiones y Adquisiciones repetible basado en NIST — asegurando una transición más segura.
- Aceleramos el ciclo de vida de Fusiones y Adquisiciones combinando evaluaciones de API sin agentes con IA generativa — reduciendo los plazos de diligencia debida de semanas a días mientras automatizábamos el análisis de datos para integraciones más rápidas e inteligentes.

Ciberseguridad

- Identificamos, evaluamos y aseguramos la remediación de más de 3.700 componentes de infraestructura crítica, un aumento del 164% año tras año, mientras manteníamos un tiempo de promedio de resolución menor a 24 horas — reduciendo significativamente la superficie de ataque de la organización.
- Construimos y probamos un nuevo agente de gestión de alertas de IA que ahora está ayudando a resolver de forma automática casi el 50% de todos los tickets de incidentes de SOC.
- Mantuvimos inicios de sesión sin contraseña para nuestros casi 22.000 empleados y contratistas a nivel global.
- Completamos la migración a la gestión de acceso nativa de la nube para alrededor de 2.000 aplicaciones, mejorando el control de acceso y la visibilidad.
- Implementamos IA para traducir informes de inteligencia de amenazas no estructurados en escenarios accionables de ataque simulado — permitiéndonos probar nuestras defensas contra nuevas estrategias de adversarios a los días de su descubrimiento, en lugar de meses.
- Hicimos cumplir la Autenticación Multifactor (MFA) para el 100% del acceso remoto, reduciendo los riesgos de entrada no autorizada.

Seguridad Física e Investigaciones

- Completamos 29 pruebas de penetración física, identificando áreas de mejora continua.
- Realizamos 43 evaluaciones de seguridad física para asegurar a empleados, datos y activos.

Gestión de Riesgos

- Establecimos un motor de riesgo cuantitativo como la fuente autorizada para métricas de seguridad, permitiendo la priorización de tareas de remediación de vulnerabilidades.
- Realizamos análisis de riesgo profundos en el 100% de los terceros críticos y de alto riesgo de nuestra empresa (2.289) — impulsando planes de remediación accionables donde fuera necesario.
- Completamos evaluaciones de riesgo en el 100% de las aplicaciones comerciales (4.022) para establecer una comprensión integral del riesgo de los activos.
- Continuamos incorporando cuentas estratégicas clave, incluidas algunas de las instituciones financieras más grandes del mundo, en CloudControl — proporcionando visibilidad en tiempo real de la seguridad de sus productos y servicios de Equifax.

Gestión de Crisis

- Realizamos 18 ejercicios teóricos que simulan escenarios de crisis con partes interesadas de la empresa, incluyendo:
  - Director Ejecutivo y Equipo Ejecutivo
  - Equipos de Crisis Regionales y de Unidades de Negocio
- Introdujimos nuevos ejercicios teóricos centrados en amenazas internas, modelado de IA, ransomware y escenarios de ingeniería social, equipando a los líderes para responder a amenazas avanzadas.
- Implementamos planes de crisis personalizados y facilitamos ejercicios teóricos regionales en español y portugués para asegurar la preparación del equipo local.
- Integramos la Gestión de Crisis con la Continuidad del Negocio y la Recuperación ante Desastres, formando una organización de Resiliencia Empresarial única y unificada.

Capacitación en Seguridad

- Realizamos más de 240.000 simulaciones de phishing (crecimiento del 15% año tras año), aumentando continuamente la dificultad a medida que evoluciona el panorama de riesgos y amenazas.
- Reorientamos a los empleados que se han mostrado susceptibles ante el phishing para educar sobre las técnicas comunes de los actores de amenazas.
- Aplicamos una nueva herramienta de informes de amenazas, impulsando más de 20.000 informes de phishing potencial de empleados y contratistas en solo 6 meses, casi 1.500 de los cuales se confirmó que incluían indicadores maliciosos.
- Incorporamos 6 nuevos factores en las Instantáneas de Seguridad mensuales de los empleados, incluidos comportamientos relacionados con:
  - Certificación de acceso, evaluando la recertificación oportuna del acceso de usuarios, uso de cuentas y propiedad de derechos.
  - Utilización de imágenes base, midiendo el uso de imágenes base estandarizadas en los entornos.
  - Gobernanza de problemas, calculando la puntualidad del cierre de problemas de seguridad abiertos.

Compromiso con el Cliente

- Completamos 2.599 cuestionarios de clientes, con un tiempo promedio de finalización de 1,86 días, proporcionando garantía de seguridad rápida a partes externas.
- Completamos 1.149 solicitudes de evidencia a petición de clientes de Equifax para asegurar el cumplimiento.
- Llevamos al mercado, de forma segura, más de 180 NPI — nuestro sexto año consecutivo con más de 100.

Privacidad

- Implementamos una nueva herramienta para la prevención de pérdida de datos (DLP) por correo electrónico, proporcionando mayor compatibilidad con nuestro conjunto de herramientas existente, análisis más robustos y cumplimiento global optimizado.
- Obtuvimos la recertificación del Marco de Privacidad de Datos (DPF) por segundo año, permitiendo transferencias de datos seguras de la UE/Reino Unido a los EE. UU.
- Lanzamos una nueva plataforma de gestión de consentimiento a nivel mundial para respetar las elecciones de los usuarios del sitio web.

Fraude

- Finalizamos la Estrategia de Monitoreo de Fraude Global y estandarizamos el bloqueo de cuentas fraudulentas en una sola plataforma en la nube, unificando procesos en todas las unidades de negocio.
- Bloqueamos más de 3.700 dispositivos y 2.900 direcciones IP sospechosas a través de investigaciones de fraude.
- Los incidentes de fraude que involucran la exposición de datos sensibles cayeron un 18% año tras año, destacando nuestra capacidad para detener la actividad sospechosa antes de que escale.
- Establecimos un nuevo equipo de fraude en India, proporcionando cobertura de fraude global extendida y capacitada a través de múltiples zonas horarias.

Desarrollo de Software Seguro

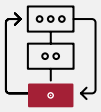
- Mejoramos la adopción de Infraestructura como Código (IaC) en un 52%, aprovechando bloques de código estandarizados para garantizar la alineación con los estándares de configuración de Equifax y eliminar configuraciones erróneas manuales.
- Lanzamos un Asistente Personal impulsado por IA para flujos de trabajo en Servicios de Asesoría de Seguridad (SAS). El cual redujo el tiempo promedio de resolución para consultas en un 61% y disminuyó las solicitudes de escalada iniciales en un 56%.
- Desarrollamos una arquitectura de IA para analizar vulnerabilidades en contenedores y generar las correcciones de código de manera automática, agilizando así la resolución de más de 213.000 hallazgos anuales.
- Presentamos el *Automated Certificate Management Toolkit* para automatizar la renovación de los certificados TLS de las aplicaciones (las credenciales digitales que cifran los datos en tránsito). Esta herramienta monitorea las fechas de vencimiento y gestiona, tanto la actualización, como la validación de los certificados sin necesidad de intervención manual.

Nuestras prioridades en 2026

Asegurando cada identidad: personas y sistemas

Al eliminar las credenciales para toda nuestra plantilla, hemos demostrado que operar sin contraseñas es posible. En 2026, estamos escalando esa revolución. Comenzaremos a implementar una opción de inicios de sesión sin contraseña para nuestros clientes B2B, neutralizando ataques de credenciales mientras eliminamos la fricción para nuestros socios comerciales.

Al mismo tiempo, nos enfocamos en el gran volumen de identidades que suelen pasar inadvertidas: cuentas no personales. A medida que nuestros agentes de IA y nuestras APIs se multiplican, estamos aplicando a los sistemas la misma verificación rigurosa que a los usuarios, asegurando que un bot no pueda ser utilizado como una puerta trasera.



Gobernanza de agentes de IA a gran escala

En 2025, construimos los protocolos para asegurar nuestra primera generación de agentes de IA. En 2026, estamos industrializando esa red de seguridad. Expandiendo nuestro marco de Política como Código (Policy-as-Code), para cubrir todos los ámbitos de la empresa, automatizando la prueba de seguridad, desviación y estricta privacidad de datos de miles de agentes. Este enfoque de gobernanza desde diseño asegura que nos mantengamos a la vanguardia del complejo panorama regulatorio de la IA.

Al escalar estos controles de protección automatizados, permitiremos que Equifax pase de probar flujos de trabajo autónomos o agénticos a ejecutarlos como un motor de negocios estándar de alto volumen, sin comprometer nunca nuestra seguridad y control.

Evolución del riesgo contextual

Cuando se trata de analizar el riesgo de seguridad, somos expertos en filtrar el ruido y tener en cuenta el contexto, incluido el valor de los activos, la exposición a Internet y los controles compensatorios. Ahora, estamos cambiando cómo vemos la señal.

En 2026, estamos rediseñando la visualización del riesgo de seguridad, convirtiendo cálculos complejos en un mapa de alta fidelidad de la exposición del negocio. También estamos estandarizando evaluaciones para casos atípicos y validando nuestro inventario de activos para asegurar una visión completa. Esta evolución convierte datos de riesgo abstractos en datos comerciales claros e innegables, haciendo que el siguiente paso sea obvio para cada tomador de decisiones.