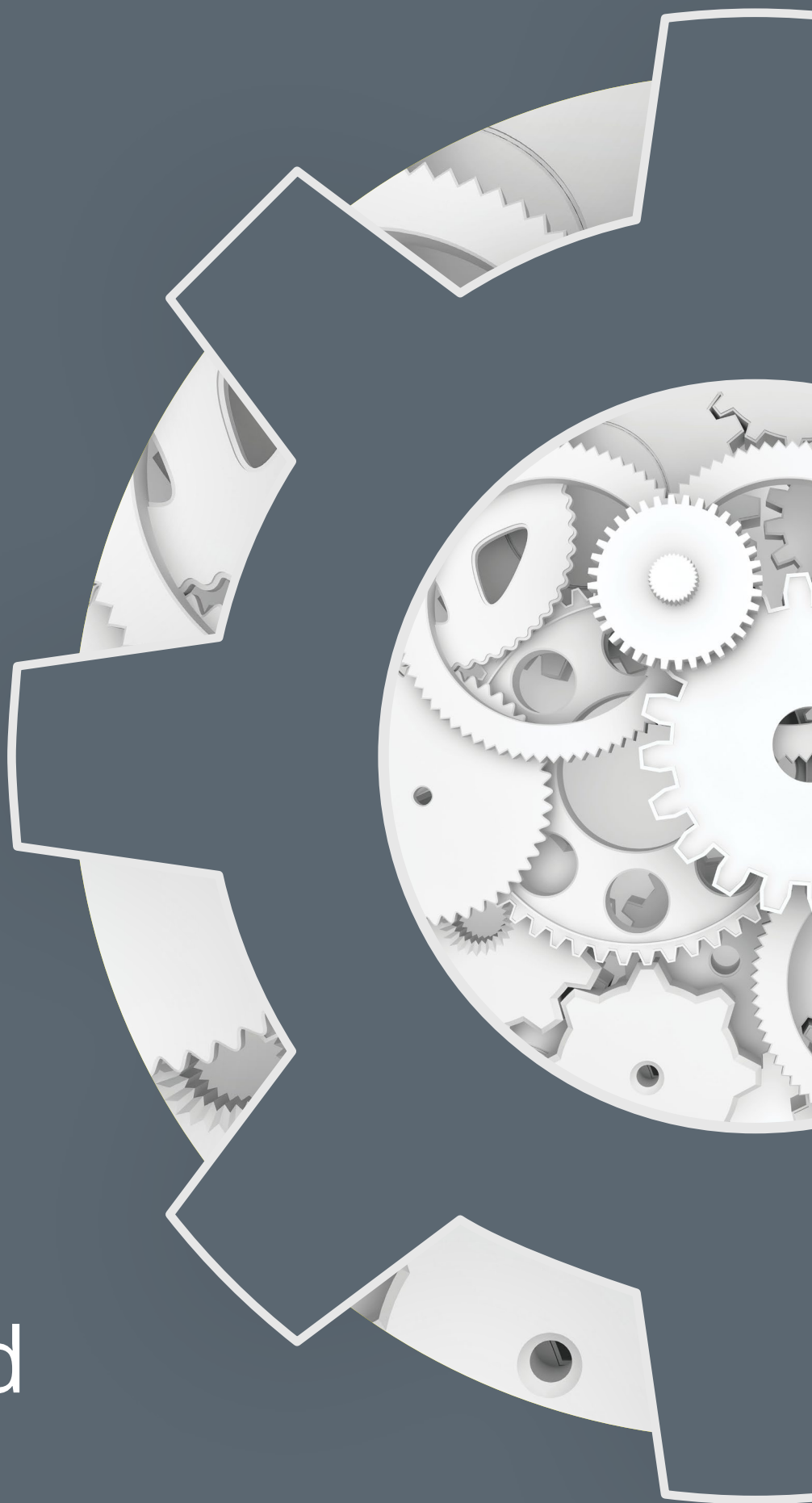




Informe anual de seguridad de 2022

Tabla de Contenidos

- 2** Carta del CEO Mark W. Begor
- 3** Carta del CISO Jamil Farshchi
- 4** Según los números
Ciberseguridad en Equifax
- 5** Estado de las cosas
Cybersécurité en 2022
- 6** Nuestras acciones
Iniciativas y resultados de seguridad de Equifax en el 2022
- 8** Dando forma al futuro
Duplicando la colaboración y la transparencia
- 9** Evaluación comparativa independiente
- 10** Resumen de resultados
- 12** Nuestras prioridades en el 2023

El siguiente nivel de ciberseguridad

El 2022 fue un año sólido para la Nueva Equifax, ya que pasamos de una era de construcción de la Equifax Cloud™ a aprovechar la nube de manera segura para la innovación, nuevos productos y el crecimiento. Realmente nos hemos convertido en una compañía diversificada de datos, análisis y tecnología que se ha extendido mucho más allá de un buró de crédito tradicional en los 24 mercados a los que prestamos servicios en todo el mundo. Y, a medida que hemos crecido e innovado para satisfacer las necesidades cambiantes de los consumidores y clientes globales, también nos hemos comprometido a asociarnos con ellos de nuevas maneras.

La ciberseguridad es fundamental para esta asociación.

Cuando me incorporé a la compañía en el 2018, asumí el compromiso personal de establecer a Equifax como líder de la industria en seguridad de datos y de crear una cultura donde la seguridad sea parte del ADN de nuestro equipo global, donde todos juegan parte. Hemos transformado nuestra organización en todos los niveles para cumplir esa promesa. Desde el compromiso de nuestros colaboradores, la infraestructura tecnológica, la estructura de datos y el desarrollo de productos, hasta nuestras estrategias de M&A, la seguridad se ha incorporado en todo lo que hacemos.

Durante los últimos cinco años, hemos construido uno de los programas de ciberseguridad más avanzados y efectivos del mundo. Nuestro nivel de madurez ha superado todos los principales puntos de referencia de la industria, y nuestra posición se ha clasificado en el 1 % superior de las empresas de tecnología y el 3 % superior de las empresas de servicios financieros analizadas, durante tres años consecutivos.

La transparencia ha sido fundamental para el crecimiento y la fortaleza de nuestro programa de seguridad. Creemos que más comunicación, más colaboración y más transparencia equivalen a una seguridad más sólida. Compartir activamente las buenas prácticas que hemos obtenido a medida que trabajamos para implementar el cambio es el motivo por el que desarrollamos este informe y por el cual continuamos interactuando activamente con los clientes, reguladores y otras organizaciones, con respecto a los desafíos y oportunidades en ciberseguridad a diario durante el transcurso del último año.

El 2022 vio una serie de nuevas amenazas a la infraestructura global de ciberseguridad. Equifax respondió, defendiéndose contra 39 millones de amenazas a la ciberseguridad cada día mientras realizaba más de 374.000 simulaciones para probar nuestra fuerza laboral global y prepararnos para lo que está por venir.

Si bien estoy motivado por nuestro progreso, no hemos terminado. El siguiente nivel de seguridad de Equifax es uno que viene con evolución continua y un compromiso inquebrantable para ayudar a nuestros clientes, socios y consumidores a fortalecer sus propias posturas de ciberseguridad para el beneficio de la industria en general a medida que Equifax impulsa el liderazgo en la industria en seguridad.



Mark W. Begor
Director Ejecutivo (CEO)
Equifax

Dando forma al futuro

Media década. Se siente como un parpadeo y una eternidad al mismo tiempo. Me uní a Equifax hace cinco años y establecí una “estrategia MinMax” para nuestro programa de seguridad, minimizando los riesgos cibernéticos y maximizando el crecimiento del negocio. Esta estrategia tuvo tres actos: Construir > Madurar > Liderar.

Ha funcionado. Hemos alcanzado el liderazgo en seguridad, y este informe lo demuestra. Todavía tenemos riesgo cibernético (siempre existirá), pero ahora está siendo administrado por talento de primer nivel, armado con tecnología de última generación y supervisado por la mejor gobernanza de su clase. Igualmente importante, lo hemos hecho mientras respaldamos el período de crecimiento más significativo de Equifax en nuestros 124 años de historia. ¡La buena seguridad ES buena para los resultados finales!

Entonces ¿qué sigue? ¿Qué viene después de “Liderar”? Dos palabras: **Dar forma**.

Estamos trabajando activamente para ayudar a dar forma a comportamientos, tecnologías y prácticas de seguridad más allá de nuestras cuatro paredes. ¿Por qué? Porque todos estamos fuertemente interconectados y dependemos unos de otros. El viejo axioma de “solo es tan fuerte como su eslabón más débil” es más cierto hoy que nunca. Simplemente no es suficientemente bueno que Equifax sea un líder en seguridad, **todos** debemos serlo.

El panorama de amenazas de 2022 destacó este imperativo. Infraestructuras vulnerables. Una carrera acelerada de armas cibernéticas. Estados nacionales envalentonados. Más del 50 % de los incidentes de seguridad se atribuyen a violaciones de la cadena de suministro. Estos son desafíos que ninguno de nosotros puede resolver solo.

Nuestra respuesta a esto es la asociación. Establecimos una visión audaz para abordar algunos de los desafíos más intrincados de la seguridad, y trabajamos cooperativamente para eliminarlos.

Contratamos proveedores de seguridad a fin de crear nuestros diseños para la capacitación de última generación, la cadena de suministro y las tecnologías de identidad en la nube. Nos asociamos con el FBI para mejorar la asociación público-privada. Compartimos nuestro plan de asociación con la junta directiva para promover las buenas prácticas de gobernanza corporativa. Nos unimos a líderes empresariales, gubernamentales y sin fines de lucro para educar a stakeholders globales sobre los principales riesgos cibernéticos. Y esto es solo el principio.

Esta es la forma. La cooperación es el multiplicador de fuerza que nos permite a todos ganar la carrera de armas cibernéticas. Nos lo debemos unos a otros, se lo debemos a nuestros países y a nuestras comunidades.

El 2022 fue un año desafiante en ciberseguridad, y el 2023 ciertamente nos traerá sorpresas. Pero juntos podemos ganar esta lucha. Avancemos con un compromiso compartido de marcar la diferencia.



A handwritten signature in black ink, appearing to read 'Jamil Farshchi', written over a light blue grid background.

Jamil Farshchi
Director de seguridad
de la información (CISO)
Equifax

Nuestro impacto

+ 39M

de amenazas cibernéticas defendidas
en promedio cada día

+ 374.000

simulaciones lanzadas para probar la
fuerza laboral global en seguridad

+ 23.000

empleados y contratistas
recibieron capacitación
personalizada en seguridad

+ 2.700

cuestionarios y auditorías completados
en nombre de los clientes de Equifax
para garantizar el cumplimiento

+ 750

análisis de riesgos profundos sobre
proveedores externos de riesgo crítico

+ 600

profesionales de ciberseguridad que
protegen los datos de los consumidores

+ 280

clientes incorporados al panel de
visibilidad de seguridad en la nube
en tiempo real

+ 160

comprobaciones automatizadas de
seguridad en la nube monitoreadas
en tiempo real

+ 110

productos nuevos de Equifax lanzados
al mercado de manera segura

+ 40

foros de la industria participaron
para abordar los desafíos
cibernéticos globales

38

certificaciones y autorizaciones
obtenidas de auditores externos

38

evaluaciones de seguridad física
completadas, validando los
controles adecuados

14

ejercicios prácticos realizados como
preparación para situaciones de crisis

4

nuevas adquisiciones evaluadas
a través de sólidas evaluaciones
de riesgos

3

años consecutivos logrando un puntaje
de Madurez de Seguridad que supera
a todos los principales puntos de
referencia de la industria

Estado de las cosas

Los temas a los que se hace referencia a continuación encapsulan las principales amenazas macro de conciencia situacional que presenciamos en el 2022.

Ataques a gran escala a los países

Albania. Australia. Costa Rica. Estonia. Finlandia. Montenegro. País tras país sintió la amenaza de los ataques a su infraestructura. Esta realidad muestra cuán descarados se han vuelto los delincuentes: atacan a gobiernos enteros y dañan los servicios públicos, el comercio y la atención médica. Pero nada parecía mayor que el ataque cibernético a Ucrania que desplegó todo, desde ataques de eliminación de datos hasta la piratería de dispositivos periféricos.

Vulnerabilidades de la cadena de suministro

La mayoría de las empresas tienen cientos de socios digitales en su cadena de suministro. Y el año pasado vio un enorme aumento en los ataques de terceros, lo que finalmente afectó a más de 10 millones de personas. Esto demostró inequívocamente que, si un eslabón débil se ve comprometido, las consecuencias pueden repercutir en muchas organizaciones integradas.

Ataques de evasión de MFA

La autenticación multifactor (Multi-Factor Authentication, MFA) ha sido durante mucho tiempo un control de referencia en los arsenales de los defensores. Últimamente, se están probando sus límites. Ya sea a través de trucos de ingeniería social o agotamiento por fuerza bruta, los ciberdelincuentes han encontrado formas de eludir la MFA.

Escasez de talento

Con una escasez global de más de tres millones de trabajadores de seguridad cibernética, los defensores se encontraron superados en 2022. Esta escasez de talento se complicó por el aumento en el área de superficie para proteger debido al aumento de la digitalización. Como nota positiva, este enigma impulsó los centros de operaciones de ciberseguridad para lograr avances en eficiencia, aprovechando la inteligencia artificial y la automatización para combatir los ataques en lugar de personal adicional.

El panorama de seguridad continúa evolucionando a un ritmo vertiginoso.

Nos mantenemos a la vanguardia con un marco de condiciones de amenaza de Equifax. Nuestro equipo se mantiene actualizado sobre la escena de ciberseguridad que cambia rápidamente, teniendo en cuenta estos eventos del mundo real en la calibración de nuestro nivel de amenaza empresarial.

Marco de condiciones de amenaza de Equifax

Seguridad de Equifax administra nuestro Nivel de amenaza empresarial que se ajusta en función de una variedad de factores, como la tasa a la que otras empresas de tecnología se ven comprometidas. Para cada nivel de amenaza: Protegido, Elevado, Alto, Grave, tenemos una serie de procesos predefinidos que activan varias acciones de nuestro equipo. Nuestro nivel de amenaza empresarial se informa regularmente al equipo de liderazgo sénior y a la junta directiva de la compañía y ha permanecido protegido durante todo el 2022.

- | | |
|---|---|
|  Grave |  Elevado |
|  Alto |  Protegido |

Nuestras acciones



Ampliamos nuestra seguridad en la nube

Continuamos fortaleciendo la postura de seguridad del Equifax Cloud, logrando la paridad de seguridad del entorno multi nube y mejorando la seguridad de los contenedores de software.

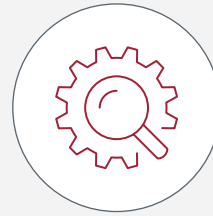
También diseñamos una pila de seguridad de red global (Global Network Security Stack, GNSS), que establece un diseño de seguridad de red estandarizado y permite una incorporación de aplicaciones más rápida y tiempo de respuesta del cliente para aplicaciones críticas en la nube.



Mayor concientización sobre la seguridad en los colaboradores

Ampliamos nuestras tarjetas de puntuación de seguridad para incluir a los contratistas de Equifax, lo que garantiza los mismos altos estándares en toda nuestra fuerza laboral. Nos asociamos con nuestro proveedor de servicios de capacitación para desarrollar conjuntamente nuevas mediciones dirigidas de comportamientos clave.

Como un ejemplo de la mayor conciencia de ciberseguridad de nuestra fuerza laboral, los empleados cada vez evitan más hacer clic en los correos electrónicos de simulación de phishing que enviamos, al mismo tiempo que los informan a una tasa más alta (y, por lo tanto, también informan más correos electrónicos de phishing reales).

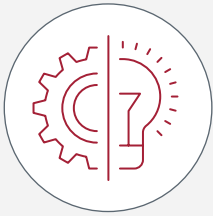


Optimización de nuestra canalización de M&A

Equifax continúa reinvertiendo nuestro sólido desempeño en adquisiciones estratégicas y complementarias para fortalecer nuestra compañía e impulsar el crecimiento futuro no hipotecario.

El equipo de seguridad ha mejorado nuestros procesos de adquisición al establecer una prioridad de control por niveles, un subconjunto de controles clave e informes basados en riesgos. Para garantizar que las empresas recién adquiridas se alineen con nuestros rigurosos estándares, completamos la alineación de controles para 15 adquisiciones.

Nuestras acciones continúan



Modernizamos y conectamos nuestras herramientas de seguridad

Para aumentar el apalancamiento operativo de nuestro equipo, elevamos nuestro conjunto de herramientas de seguridad en las áreas de protección de puntos finales, gestión de acceso, registro y reconocimiento de imágenes. El resultado es una mejor gobernanza, un menor riesgo y menos fricción para el negocio.

Gran parte de este aumento se logró a través de la asociación con proveedores de tecnología para diseñar conjuntamente soluciones que ahora están disponibles para el mercado en general, fortaleciendo la seguridad en todo el ecosistema comercial más amplio.



Crecimiento comercial habilitado

Incorporamos más de 280 clientes en CloudControl, un panel diseñado para nuestros clientes que proporciona información en tiempo real sobre la postura de seguridad de los productos y servicios basados en la nube de Equifax que utilizan.

Además, obtuvimos nuevas certificaciones que crean oportunidades para el negocio, incluida la obtención del cumplimiento de la Ley de Portabilidad y Responsabilidad de los Seguros Médicos (HIPAA) de los EE. UU. para dos entornos clave y la obtención de la autorización de seguridad de las instalaciones secretas del gobierno de Canadá.



Transparencia y colaboración avanzadas

Desarrollamos nuestro compromiso continuo con las partes interesadas de todo el mundo y priorizamos los temas y las oportunidades de asociación que tienen el mayor impacto en el avance de la ciberseguridad.

Esto incluyó compartir nuestra experiencia en la creación de asociaciones efectivas con la junta directiva/CISO y facilitar el diálogo efectivo entre organizaciones públicas y privadas, asociarnos con organizaciones como el Centro de Políticas Bipartidistas, el Instituto Cibernético Suizo y la Asociación Nacional de Directores Corporativos.

Duplicamos
la colaboración y
la transparencia

Dando forma al futuro

La seguridad a escala requiere trabajo en equipo. En el 2022, colaboramos externamente desde múltiples ángulos.

Teníamos una visión estratégica para nuestro programa y seguridad en general, pero no existían productos para dar vida a esta visión. Esto no nos detuvo. **Llevamos las relaciones con nuestros proveedores de transaccionales a transformadoras**, trabajando codo a codo para llevar soluciones de última generación al mercado. Más allá de dar forma a nuestras capacidades líderes, estas asociaciones impulsan a toda la industria hacia adelante.

- Buscamos un mecanismo positivo y motivador para orientar, educar, medir e incentivar un compendio de **comportamientos seguros de los empleados**. Nos asociamos con nuestro proveedor de capacitación para mejorar la profundidad y amplitud de su oferta, incluida la medición integral y la retroalimentación en tiempo real.
- Ningún producto respondía a nuestra visión de cómo debe hacerse la **seguridad de la cadena de suministro**. Así que ayudamos a crear uno nos asociándonos con un proveedor líder de software de seguridad para transformar un producto incipiente en una innovadora herramienta en la nube para clientes totalmente operativa.
- Queríamos una solución unificada de **administración y gobernanza de identidad (IGA) basada en la nube y gestión de acceso privilegiado (PAM)**. No existía ninguna. Así que seleccionamos un socio de diseño para ofrecer una solución, ayudando a garantizar capacidades integradas, de próxima generación y centradas en la nube, no solo para nosotros, sino para todos los demás en el mercado a partir de entonces.
- Trabajamos con el equipo de ingeniería de Ping Identity para automatizar nuestras **capacidades de autenticación** y fuimos reconocidos con su premio Cloud Identity Champion por nuestro “trabajo que impulsa nuestra industria hacia el futuro”.

Para ayudar a los directores a mejorar el diálogo con los CISO y comprender mejor los riesgos cibernéticos **compartimos nuestro plan de asociación con la junta:**

Asociación Nacional de Directores Corporativos	Consejo Asesor de la Junta de la Bolsa de Valores de Nueva York (NYSE)	Perspectiva de los inversionistas de Glass Lewis	Gestión de seguridad y riesgos de Gartner	Red del Comité de Auditoría de EY
--	---	--	---	-----------------------------------

He interactuamos con legisladores, agencias gubernamentales, ONG y reguladores:

- El CISO de Equifax fue nombrado **por el FBI como Asesor de Compromiso Estratégico**.
- Nos asociamos con el **Centro de Políticas Bipartidistas** para destacar los principales riesgos en ciberseguridad para empresas, el gobierno y la sociedad en el 2023.
- Nos asociamos con el **Grupo de Seguridad Cibernética de Costa Rica** para fomentar la asociación público-privada entre el Ministerio de Ciencia y Tecnología, la Cámara de Industrias de Costa Rica, universidades y otros negocios.
- Nos asociamos con la **Alianza Chilena de Ciberseguridad** para contribuir a las políticas de ciberseguridad en Chile.
- Apoyamos la resiliencia cibernética de Australia y Nueva Zelanda a través de **CISOLens**.

Ciber Gobernanza

Un mayor enfoque regulatorio en la gobernanza cibernética está convirtiendo la seguridad en una responsabilidad central de la junta directiva y el equipo de gestión.

Y dado que ya tenemos una sólida asociación con nuestra alta gerencia y la Junta Directiva, compartimos nuestros aprendizajes ganados con tanto esfuerzo, tanto para ayudar a dar forma a las regulaciones como para ayudar a las organizaciones a cumplir.

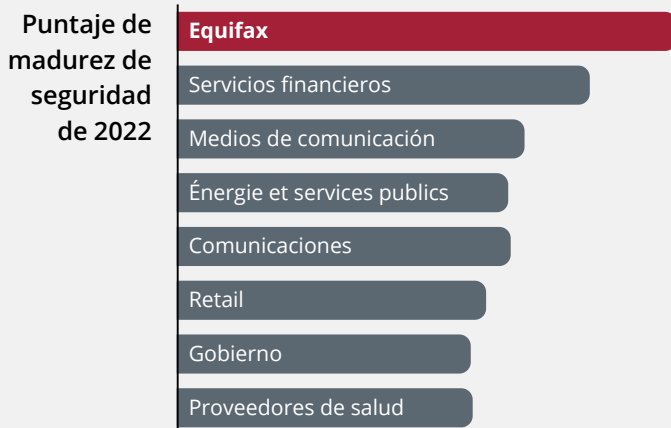
Conforme a la regulación más reciente del Departamento de Servicios Financieros del Estado de Nueva York (NYDFS), **el CEO y el CISO deben firmar conjuntamente un certificado anual de cumplimiento de las normas de seguridad**, y el consejo de administración debe:

- Tener conocimientos y experiencia significativos en riesgos cibernéticos para una supervisión eficaz
- Aprobar las políticas, los procedimientos y la evaluación de riesgos de seguridad de una empresa
- Recibir informes del CISO, al menos una vez al año
- Revisar cualquier problema sustancial que surja de las evaluaciones de vulnerabilidad y las pruebas de penetración

Glass Lewis, líder de servicios de asesoramiento para inversionistas, proclamó que nuestra transparencia es “**singular y extraordinaria**”.

Madurez de la seguridad

Una firma líder mundial de investigación y asesoramiento lleva a cabo un análisis anual en profundidad de la madurez de todo nuestro programa de seguridad.



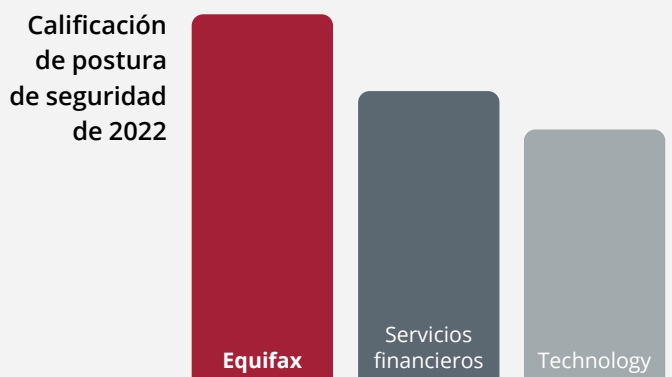
¿Qué es la madurez de la seguridad?

La madurez de la seguridad de una organización representa qué tan bien puede adaptarse a las amenazas cibernéticas y gestionar el riesgo con el tiempo.

A fines de 2022, la madurez de nuestro programa de ciberseguridad superó todos los principales puntos de referencia de la industria por tercer año consecutivo.

Postura 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 cadena de suministro.



¿Qué es la postura de seguridad?

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

A fines de 2022, nuestras capacidades de seguridad se clasificaron en el 1 % superior de las empresas de tecnología y en el 3 % superior de las empresas de servicios financieros analizadas.

Resumen de resultados

Madurez y postura de seguridad

- Optimizamos el gasto en ciberseguridad en un 9,2 % del presupuesto de TI, por debajo del promedio de la industria del 9,9 %
- Logramos un puntaje de Madurez de seguridad que superó todos los principales puntos de referencia de la industria por tercer año consecutivo.
- Logramos una calificación de Postura de seguridad que se ubicó en el 1 % superior de las empresas de tecnología y en el 3 % superior de las empresas de servicios financieros analizadas

Ciberseguridad

- Implementamos 349 comprobaciones automatizadas de seguridad en la nube monitoreadas en tiempo real
- Sólida mejora en la seguridad de las aplicaciones; el 96 % de las aplicaciones verificadas se inscribieron en el escaneo automatizado para fines de 2022 (frente al 69 % en agosto)
- Se aplicó la autenticación multifactor (MFA) para el 100 % del acceso remoto a nuestra red
- Se actualizó a herramientas de próxima generación en protección de puntos finales, gestión de acceso, registro y reconocimiento de imágenes

Compliance

- Obtuvimos 38 certificaciones de auditores externos (un aumento del 45 % con respecto al 2021) que validan nuestro cumplimiento con los requisitos comerciales, legales, contractuales y reglamentarios.
- Equifax Canadá obtuvo la autorización de seguridad de instalaciones secretas del gobierno de Canadá
- Logramos el cumplimiento de la HIPAA para dos entornos clave: Kount (nuestra plataforma de protección contra fraudes) y nuestro negocio de Servicios de filtraciones de datos

M&A

- Realizamos una sólida diligencia debida sobre las cuatro adquisiciones completadas en el 2022, incluido el escaneo integral de vulnerabilidades, la revisión de códigos, la evaluación de compromisos y las revisiones de control clave antes del cierre.
- Desarrollamos una nueva estrategia de integración de seguridad de tres niveles, asegurando que las nuevas entidades estén alineadas con los controles de Equifax sin demora
- Completamos la alineación de control de seguridad para 15 adquisiciones de Equifax

Gestión del riesgo

- Desarrollamos análisis de riesgo profundos en el 100 % de los proveedores externos de riesgo crítico de nuestra compañía (más de 750)
- Incorporamos más de 280 clientes a CloudControl, una plataforma líder en la industria que ofrece a los clientes visibilidad en tiempo real de la seguridad de los productos y servicios de Equifax Cloud que utilizan

Manejo de crisis

- Desarrollamos 14 ejercicios prácticos y simulaciones de crisis en tiempo real con las partes interesadas de la compañía. Las partes interesadas clave incluyeron:
 - Junta directiva
 - CEO y equipo ejecutivo
 - 12 equipos de crisis regionales y de unidades de negocios

Privacidad

- Se implementó Google Workspace Client-Side Encryption para cifrar los datos confidenciales almacenados en Google Workspace

Resumen de resultados continúan

Capacitación en seguridad	• Realizamos 15 simulaciones globales y 18 simulaciones dirigidas para probar nuestra fuerza laboral en seguridad • Expandimos nuestro “Security Snapshot” a 23.500 colaboradores y contratistas de Equifax • Mantuvimos un puntaje de seguridad global líder en el mercado de 91, superando a todos los principales puntos de referencia de la industria • Se redujo la tasa promedio de clics de simulación de phishing de los empleados al 4,2 % (mejora del 10 % frente al 2021) • Se introdujeron nuevos comportamientos basados en roles en la tarjeta de puntuación de seguridad de los colaboradores, incluida la navegación segura y el manejo de datos confidenciales
Servicios de filtración de datos	• Apoyamos a 716 organizaciones y a sus clientes, ayudándoles a responder y recuperarse de incidentes cibernéticos
Participación de clientes	• Se completaron más de 2.700 cuestionarios y auditorías en nombre de los clientes de Equifax para garantizar el cumplimiento
Productos y servicios	• Lanzamos al mercado de manera segura 113 nuevos productos para nuestros clientes • Se incorporó una sólida habilitación de seguridad de productos en la etapa de diseño del ciclo de desarrollo, asesorando a los equipos de productos y empoderando a los desarrolladores con una herramienta de autoservicio para encontrar y corregir vulnerabilidades
Fraude	• Se introdujeron capacidades antifraude de vanguardia que incorporan machine learning, inteligencia artificial y entradas mejoradas de proveedores, al tiempo que se minimiza la fricción del consumidor
Investigaciones y seguridad física	• Se completaron 12 pruebas de penetración física para identificar áreas de mejora continua en la prevención del acceso no autorizado a las instalaciones • Se realizaron 38 evaluaciones de seguridad física que validan los controles adecuados para proteger a los empleados, los datos y los activos. • A través de procesos mejorados y automatización, nuestro Centro de Operaciones de Seguridad Física reforzó nuestro tiempo de respuesta para: – Alarmas locales de alta prioridad: dentro de los 3:21 minutos (respuesta un 16 % más rápida que en el 2021) – Informes de inteligencia entrantes: dentro de los 2:07 minutos (respuesta un 58 % más rápida que en el 2021)
Talento y diversidad	Continuamos aumentando la diversidad entre nuestra fuerza laboral: • 13 % de los miembros del equipo de seguridad de raza negra en los EE. UU. (frente al 9 % del promedio de la industria) • 27 % de los miembros del equipo de seguridad en los EE. UU. se identifican como mujeres (frente al 24 % del promedio de la industria)
Defensa y asociación	• Participamos en más de 40 foros para promover una ciberseguridad más sólida para el negocio, el gobierno y la sociedad • Nos asociamos con el Centro de Políticas Bipartidistas para destacar los principales riesgos en ciberseguridad para empresas, el gobierno y la sociedad en el 2023 • El CISO fue nombrado por el FBI como Asesor de Compromiso Estratégico para promover la relación del FBI con el sector privado

No nos detenemos



Optimización de nuestras herramientas y procesos

Tenemos políticas y métricas clave establecidas y documentadas. Las prácticas de seguridad están estandarizadas e incorporadas en la estrategia comercial general de Equifax. Hemos llegado a una etapa de nuestro viaje de madurez en la que es hora de enfocarnos en la optimización.

Perfeccionaremos nuestras herramientas, datos y personal con el fin de reforzar nuestro dispositivo de seguridad. Esto nos permitirá contrarrestar eficazmente las amenazas en evolución y mantenernos a la vanguardia de la carrera de las armas cibernéticas.



Aceleración de la seguridad sin fricción

Las personas harán su trabajo, sin importar lo que pase. Si los controles son engorrosos, los omitirán (creando riesgo), cometerán errores (creando riesgo) o lograrán menos (y, en consecuencia, rechazarán las medidas de seguridad). La seguridad sin fricción ayuda a reducir el riesgo y mejorar la productividad de la fuerza laboral.

Aunque hemos logrado un progreso significativo al incorporar el autoservicio y la automatización en todo nuestro negocio, no hemos terminado. Perfeccionaremos y escalaremos las capacidades que introdujimos en el 2022, moldeando la experiencia de cada usuario para facilitar que todos los stakeholders hagan lo correcto.



Refuerzo de la seguridad de la identidad

“Confianza cero” es un término usado en exceso. Pero los principios que apoya, evitar suposiciones, monitorear continuamente y basarse en la verificación, son primordiales.

Si bien ya estamos haciendo cumplir el acceso Justo a tiempo y Con tiempo limitado para recursos privilegiados, no escatimaremos esfuerzos en nuestra búsqueda para proteger la privacidad de los consumidores y minimizar la superficie de ataque a través de la seguridad en capas.



equifax.com