12ª EDICIÓN

Pronóstico de la Industria de Brechas de Datos 2025

Resumen Ejecutivo

Las brechas de datos globales no muestran signos de desaceleración. De hecho, según el Informe de Investigaciones de Brechas de Datos de Verizon 2024, han habido 10,626 compromisos de datos en los primeros tres trimestres de 2024, más del doble del total del año pasado de 5,199. Experian ha apoyado más de 4,000 brechas de datos de clientes en los primeros tres trimestres de 2024. Según nuestros análisis internos, más de 66 millones de consumidores a nivel mundial se vieron afectados por estas brechas de datos de nuestra base de clientes en 2024, un aumento del 13% respecto al año pasado.

Ninguna organización es inmune a los ataques impulsados por inteligencia artificial de los sofisticados estafadores de hoy en día. Desde la filtración de mensajes de Slack de Disney en julio hasta Ticketmaster y BBC en mayo, las marcas más grandes son susceptibles.

Un problema crítico para las empresas es el aumento de los costos de las brechas de datos. Según el Informe de Costos de una Brecha de Datos de IBM 2024, el costo promedio global de una brecha aumentó un 10% desde 2023, alcanzando los 4.88 millones de dólares, el mayor aumento desde la pandemia. A esto se suman los costos adicionales de demandas, como el acuerdo de 30 millones de dólares en septiembre contra la empresa de pruebas de ADN 23andMe por una brecha de datos genéticos que expuso la información personal de 6.4 millones de clientes en 2023.

Reflexionando sobre las predicciones del año pasado, la brecha de datos de AT&T que involucró a su proveedor de servicios en la nube, Snowflake, y el robo de datos sensibles de más de 70 millones de clientes inalámbricos de AT&T es un ejemplo de nuestra predicción de "Seis Grados de Separación". La brecha de datos de Life360, donde los hackers explotaron una vulnerabilidad en su integración de back-end con herramientas de aplicación de la ley, es otro ejemplo. Destacando nuestra predicción de "Poco a poco se hace mucho", la brecha de Holograph Crypto Exchange en junio involucró una pequeña falla en el código del contrato inteligente de Holograph que permitió a los hackers desviar 26 millones de dólares en Bitcoin y Ether.

En nuestro 12º Pronóstico Anual de la Industria de Brechas de Datos, nuestro enfoque abarca una amplia gama de ataques desde los personales (explotación de adolescentes), corporativos (aumento del fraude interno), nacionales (uso de identificación dinámica como defensa contra el fraude) y globales (actores maliciosos persiguiendo centros de datos). Todas estas predicciones están impulsadas por la velocidad y escala dramáticamente aceleradas de los ciberataques habilitados por IA. Las predicciones de este año provienen de la larga historia de Experian ayudando a las empresas a navegar por las brechas durante los últimos 22 años. Las siguientes predicciones representan lo que vemos en el horizonte en el mundo de los incidentes de seguridad de datos en 2025.

El Pronóstico de la Industria de Brechas de Datos de Experian es un intento de prever y proporcionar predicciones de ciberseguridad para el futuro. Las predicciones no están garantizadas y no deben considerarse como asesoramiento formal, sino con fines educativos.

Contribuyentes

Michael Bruemmer

Vicepresidente de Resolución de Brechas de Datos Globales

Michael Bruemmer es Vicepresidente de Resolución de Brechas de Datos Globales y Protección al Consumidor en Experian. El grupo es líder en ayudar a las empresas a prepararse para una brecha de datos, gestionar programas de respuesta a crisis de consumidores y mitigar el riesgo para los consumidores tras los incidentes.

Con más de 25 años en la industria, Michael aporta una gran cantidad de conocimientos relacionados con la gestión de respuesta a crisis, desde el descubrimiento hasta la gestión posterior al incidente. Ha manejado algunas de las mayores brechas de datos del país durante su mandato en Experian, con más de 60,000 hasta la fecha. Michael ha educado a empresas de todos los tamaños y sectores sobre la planificación y ejecución de respuestas a brechas de datos. Esto abarca desde cómo notificar a los consumidores afectados, hasta la configuración de centros de llamadas e incluso cómo implementar servicios de protección contra el robo de identidad.

Es un orador respetado y presenta a organizaciones de la industria en todo el país. Ha proporcionado información a muchos medios comerciales y de negocios, incluyendo Dark Reading, IT Business, CIO, Info Security, Security Week, Health IT Security, Wall Street Journal y American Banker, entre otros. Ha sido columnista invitado para SecurityInfoWatch y ha aparecido en canales de televisión como Fox Business.

Actualmente, reside en la Junta de Gestión Responsable de la Información (RIM) de Ponemon y en la Junta Asesora de NetDiligence.

Tiene una Licenciatura en Artes en Economía Laboral de la Universidad de Wisconsin-Madison.

Jim Steven

Jefe de Servicios de Respuesta a Crisis y Brechas de Datos, Reino Unido

Jim Steven es el jefe de Servicios de Respuesta a Crisis y Brechas de Datos para Experian UK, aprovechando el conocimiento, la experiencia y el éxito de la oferta global de resolución de brechas de datos de Experian.

Su equipo trabaja con empresas para ayudarlas a gestionar y proporcionar recursos para respuestas a crisis masivas de consumidores, incluyendo la notificación a clientes, centros de contacto y servicios de monitoreo de crédito/identidad para clientes/empleados afectados por un evento de crisis. También apoyan a los clientes en la preparación y práctica de planes de preparación para posibles incidentes para mitigar el impacto y acelerar la recuperación.

Antes de unirse a Experian, Jim trabajó en la industria de la seguridad y la gestión de riesgos, proporcionando experiencia en soluciones de gestión de riesgos de seguridad, gestión de riesgos de viaje, seguridad en la aviación y seguridad corporativa para algunas de las mayores empresas de seguridad del mundo.

01

Huele a Secreto Adolescente

Según el **FBI** la edad promedio de una persona arrestada por ciberdelito es de 19 años, en comparación con 37 años para cualquier otro delito. Los **hallazgos** de la Escuela de Educación de Harvard indican que la mitad (51%) de los jóvenes de entre 14 y 22 años reportaron usar IA generativa, y el 31% dijo que la usan para **"hacer imágenes o fotos"**. **Hoy en día, el mundo del ciberhackeo no está confinado a los adultos, ni sus consecuencias.**

En un escenario, los adolescentes comunes ahora son el objetivo de contenido emocional y dañino para su reputación por parte de actores maliciosos que buscan acosarlos, humillarlos o manipularlos para que realicen actividades inapropiadas o ilegales. Muchos de estos actores maliciosos son adolescentes que utilizan herramientas de IA generativa ampliamente disponibles para producir sus deepfakes. También vemos a muchos adolescentes entrando en el mundo del ciberdelito por diversión o ganancia monetaria. **"En todo el país estamos viendo ciberdelitos cada vez más sofisticados llevados a cabo por personas cada vez más jóvenes",** dijo William McKeen, un agente especial supervisor de la División Cibernética del FBI, en una historia del **Wall Street Journal.**De hecho, los cibercriminales adolescentes, como los del grupo Lapsus$ y el Com junto con su derivado Scattered Spider, han ganado notoriedad significativa en los últimos años.

Lamentablemente, muchos de ellos habrán sido reclutados en el "negocio" por estafadores más sofisticados, que los contactan a través de juegos en línea, chats y redes sociales. A medida que más estados aprueban leyes contra la pornografía vengativa, el ciberacoso y otras formas de ataques fraudulentos en línea, **el futuro cercano podría ver un aumento dramático en el número de adolescentes procesados por hackeo y fraude.**

02

El Enemigo Interno: Aumento del Fraude Interno

Según PwC, el 57% del fraude es cometido por empleados internos o una combinación de internos y externos, y los internos están detrás del 43% de los casos de fraude que implican más de 100 millones de dólares en pérdidas. Lo preocupante es que este nivel de fraude interno ocurrió antes de la llegada de la IA generativa. Un informe de principios de 2024 del **Grupo Adecco** revela una asombrosa tasa de adopción del **70% de la IA en el lugar de trabajo.** El mismo informe indica que solo el 43% de los ejecutivos de nivel C creen que el equipo de liderazgo de su empresa tiene suficientes habilidades y conocimientos en IA para comprender los riesgos y oportunidades que ofrece la tecnología. Eso es mucho riesgo.

A medida que más empresas continúan capacitando a sus empleados en el uso responsable de la IA, podríamos ver un aumento significativo en el uso de esa educación en IA por parte de esos mismos empleados para el robo interno, la obtención de información sensible y mucho más. El próximo año podría ver al menos una marca global afectada por el fraude perpetrado por un empleado interno al que se le proporcionó capacitación educativa en IA.

03

Depredadores se Convierten en Presas

Una historia reciente sobre hackers de OnlyFans siendo engañados por malware sofisticado de un hacker más malicioso y perdiendo sus fondos apunta a una tendencia de rápido crecimiento en el mundo del cibercrimen de alto riesgo: los depredadores se convierten en presas. Hackers aspirantes de servicios de streaming y redes sociales están sucumbiendo a publicaciones en foros de hackers que, al abrirse, inician cargas útiles dañinas, incluyendo ataques a sus billeteras de criptomonedas.

De manera similar a cómo los miembros ucranianos del grupo de ransomware como servicio Conti dejaron esa organización durante la guerra ruso-ucraniana y **eventualmente derribaron a la banda de cibercrimen rusa BlackCat.** El próximo año podría ver un aumento marcado en los ataques de hacker contra hacker, ya sea por razones políticas o monetarias. Estos incidentes destacan cómo los límites entre depredador y presa en el mundo digital son cada vez más difusos.

04

La Identificación Dinámica es la Próxima Defensa Contra el Fraude

La encriptación normal de 256 bits se está volviendo obsoleta, y el fraude impulsado por IA está aumentando en sofisticación tan rápidamente que los estafadores pronto podrán crear documentos de prueba de vida virtualmente indiscernibles que engañarán incluso al ojo o sistema de identificación más estricto. Para combatir esta realidad en evolución, los estados-nación y las agencias gubernamentales podrían pasar a la identificación dinámica que reemplazará las licencias de conducir estáticas y las tarjetas de seguridad social con información personal identificable (PII) dinámica que cambia continuamente, como un código de barras 3D en línea utilizado para boletos de eventos.

Como resultado, incluso si una organización es hackeada y se roban el nombre y número de seguridad social de sus clientes o miembros, los consumidores podrían restablecer sus números como contraseñas y usar códigos de barras 3D que rotan constantemente en su dispositivo móvil para identificación. Considera que muchos expertos en ciberseguridad creen que el número de identificación de cada estadounidense ha sido filtrado al menos una vez en la dark web, y este enfoque puede no ser tan descabellado como se podría pensar.

05

Centros de Datos Hambrientos de Energía como Objetivo Favorito

Los ciberatacantes globales han tenido en la mira a los grandes centros de datos durante años, pero un vector de ataque claro ha surgido con el crecimiento exponencial del uso de IA generativa por parte de consumidores y empresas: la energía. **Según Goldman Sachs**, en promedio, una sola consulta de ChatGPT utiliza casi 10 veces más electricidad para procesarse que una búsqueda estándar en Google. Esta banca de inversión también informa que la demanda de energía de los centros de datos crecerá un 160% para 2030.

En noticias relacionadas, después de reunirse con ejecutivos de empresas de hiperescala, compañías de IA, operadores de centros de datos y empresas de servicios públicos a principios de septiembre, la Casa Blanca **anunció** un nuevo grupo de trabajo para abordar las crecientes necesidades de construcción y mantenimiento de la infraestructura de IA de Estados Unidos. Todas estas entidades representan nuevas superficies de ataque que pueden ser interrumpidas por actores maliciosos. A nivel mundial, el problema se agrava. La infraestructura en la nube y la tecnología y seguridad de los centros de datos varían enormemente de un país a otro. **En el próximo año, los ciberatacantes podrían poner en peligro con éxito la infraestructura en la nube de un Estado-nación a través de un ataque a la energía necesaria para operarla.**

Resolución de Brechas de Datos de Experian® en Cifras

Cobertura
Más de 100 países

2,808
Total de brechas hasta la fecha en 2024, hasta el tercer trimestre.

77M
Notificaciones de brechas enviadas en 2024.

8
Mega brechas en 2024

TOTAL DE BRECHAS POR SECTOR

- Salud: 36%
- Sector Público: 19%
- Servicios Financieros: 16%
- Retail: 13%
- Educación: 10%
- Otros: 6%

LOS 5 PAÍSES MÁS AFECTADOS


Estados Unidos


Reino Unido


Canadá


Australia


México

Consumidores Afectados

24% Menores de edad

76% Adultos

41% de todas las brechas en 2024 fueron brechas de la cadena de suministro.

Mejores Resultados, Valor Inigualable

Confía en la resolución de brechas de datos de Experian para obtener la mejor asociación, soluciones y rendimiento, creando el mejor resultado posible. Obtén control y confianza con el valor que solo las Soluciones para Socios de Experian pueden proporcionar.

Contáctanos

Pagina Web

https://www.experian.com/careers/locations-teams/latin-america?fbclid=PAZXh0bgNhZW0CMTEAAaZdgkYsZUJKdtC9XoqPPBlCzm_dhhkX_GRL22feWmmltBu72zzjS2fNbhl_aem_cZCSgFVpBE_177PxtR8LCg

LinkedIn

https://www.linkedin.com/company/experian-spanish-latam/

Instagram

https://www.instagram.com/experian_spanishlatam?utm_source=ig_web_button_share_sheet&igsh=ZDNlZDc0MzIxNw==