



ACTIVIDAD 01

ANÁLISIS EN GRUPO DE UN CIBERATAQUE REAL Y SU IMPACTO EMPRESARIAL.



Jasso Dávila Pedro Damián - 176658

Moreno Solís Gisela Geraldine - 176522

Palomo Cerdá José Armando - 17593

Zarate Domínguez David - 175842

Zorrilla Rivera Eduardo - 175877

Mtro. Servando López Contreras

30 DE ENERO DE 2026
UPSLP
CNO V Seguridad Informática

Introducción.

El presente reporte documenta el ciberataque sufrido por **Equifax** en 2017, considerado uno de los incidentes de ex-filtración masiva más graves en el sector financiero. El ataque fue posible mediante la explotación de la vulnerabilidad **CVE-2017-5638** en Apache Struts, la cual permitió la ejecución remota de código (RCE) debido a la omisión de un parche de seguridad disponible meses antes del incidente.

La brecha expuso deficiencias críticas en la gestión de activos y la visibilidad operativa, destacando el vencimiento de certificados SSL que impidieron la detección del tráfico malicioso durante 76 días. Con un impacto que afectó a **147.5 millones de víctimas** y resultó en un acuerdo judicial de **\$1.4 mil millones de USD**.

Este estudio tiene el propósito de evaluar las consecuencias bajo el modelo **CIA** (Confidencialidad, Integridad y Disponibilidad) para comprender la relación entre la ciberseguridad y la sostenibilidad organizacional.

Línea de Tiempo

CRONOLOGÍA DETALLADA DE LA INVESTIGACIÓN (EXPEDIENTE EQX-2017)

Fecha	Hora	Evento
07 de marzo de 2017	10:00 hrs	El Departamento de Seguridad Nacional de EE. UU. (DHS) emite una alerta crítica sobre la vulnerabilidad CVE-2017-5638 en Apache Struts.
08 de marzo de 2017	09:00 hrs	El equipo de seguridad global de Equifax recibe la notificación oficial y clasifica el riesgo como "Inminente y Crítico".
09 de marzo de 2017	08:30 hrs	Se distribuye un correo interno a todos los administradores de sistemas ordenando la aplicación del parche en un periodo máximo de 48 horas.
10 de marzo de 2017	15:00 hrs	El equipo de TI ejecuta un escaneo de vulnerabilidades automatizado en la red externa.
10 de marzo de 2017	17:00 hrs	Fallo operativo: el escaneo no identifica el portal de disputas de consumidores como sistema vulnerable debido a una configuración de red errónea.
12 de marzo de 2017	00:00 hrs	Vence el plazo interno para el parcheo. El servidor crítico queda expuesto y sin protección en el puerto 443.
13 de mayo de 2017	21:15 hrs	Intrusión inicial: actores de amenaza detectan el vector de entrada. Se registra el primer comando de ejecución remota (RCE) exitoso.

13 de mayo de 2017	<u>23:50 hrs</u>	Los atacantes instalan una Web Shell (puerta trasera) para asegurar la persistencia en el servidor comprometido.
14 de mayo de 2017	<u>04:00 hrs</u>	Comienza el reconocimiento de la red interna. Los atacantes buscan archivos de configuración locales.
15 de mayo de 2017	<u>11:20 hrs</u>	Hallazgo de evidencia crítica: los atacantes localizan un archivo con credenciales de bases de datos en texto plano.
16 de mayo de 2017	<u>02:00 hrs</u>	Inicia el movimiento lateral. Los atacantes acceden a los servidores de bases de datos centrales.
20 de mayo de 2017	<u>14:00 hrs</u>	Los perpetradores realizan consultas de prueba para medir la velocidad de respuesta de la base de datos de crédito.
25 de mayo de 2017	<u>09:00 hrs</u>	Se establece un canal de exfiltración cifrado. La empresa no detecta el tráfico saliente porque las herramientas de inspección están inactivas.
01 de junio de 2017	<u>00:00 hrs</u>	Comienza la extracción masiva de PII (Información de Identificación Personal). Se estima la salida de 5 millones de registros por día.
10 de junio de 2017	<u>10:30 hrs</u>	Los atacantes expanden su presencia instalando más de 30 web shells adicionales en distintos servidores.
20 de junio de 2017	<u>18:00 hrs</u>	La extracción continúa sin interrupciones. El volumen de datos ex infiltrados supera los 200 GB.
01 de julio de 2017	<u>08:00 hrs</u>	El ataque se vuelve selectivo; se extraen datos específicos de tarjetas de crédito y documentos de identidad escaneados.
15 de julio de 2017	<u>23:00 hrs</u>	Se registra actividad desde direcciones IP vinculadas a infraestructuras de inteligencia extranjera.
28 de julio de 2017	<u>16:00 hrs</u>	El equipo de seguridad de red nota una anomalía en el rendimiento de un servidor durante una revisión de rutina.
29 de julio de 2017	<u>10:15 hrs</u>	Detección del incidente: se identifica tráfico sospechoso hacia una dirección IP externa no autorizada.
29 de julio de 2017	<u>11:30 hrs</u>	El equipo técnico descubre que el certificado SSL de la herramienta de monitoreo venció en septiembre de 2016.

29 de julio de 2017	<u>14:00 hrs</u>	Se bloquea el acceso al portal de disputas. Los atacantes pierden la conexión activa.
30 de julio de 2017	<u>09:00 hrs</u>	Se activa el Protocolo de Respuesta a Incidentes. Se contrata a la firma externa Mandiant para realizar el peritaje forense.
02 de agosto de 2017	<u>12:00 hrs</u>	El análisis forense confirma la exfiltración masiva. El conteo inicial es de 130 millones de víctimas.
15 de agosto de 2017	<u>17:00 hrs</u>	La alta dirección es informada de la magnitud del desastre. Se discute la estrategia de comunicación legal.
24 de agosto de 2017	<u>10:00 hrs</u>	Tres altos ejecutivos de Equifax venden acciones de la empresa por un valor de \$1.8 millones.

Análisis técnico, impacto económico y estratégico

Tras la reconstrucción de los hechos, el equipo pericial concluye que el éxito de la intrusión se debió a una pérdida de control del ciclo de vida de los activos. No se trata únicamente de un servidor olvidado; se trata de una ruptura en la Cadena de Mando de TI.

- **Omisión de Mantenimiento Crítico:** La vulnerabilidad CVE-2017-5638 fue pública y tuvo una solución técnica inmediata (parche) desde marzo. La incapacidad de Equifax para identificar qué servidores corrían dicho software demuestra una falta de inventario de activos, violando los principios básicos de marcos internacionales como ISO 27001.
- **Falla de Visibilidad Operativa:** El hecho de que un Certificado SSL estuviera vencido por 10 meses no es un error menor; es una negligencia grave. En términos policiales, es equivalente a tener cámaras de seguridad en un banco, pero no tener a nadie mirando el monitor porque el cable está desconectado. Los atacantes filtraron gigabytes de información a plena vista, protegidos por el mismo cifrado que la empresa debía supervisar.
- **Higiene de Datos Deficiente:** Una vez que el perímetro fue vulnerado, los atacantes no enfrentaron resistencia interna. El hallazgo de credenciales de bases de datos en texto plano eliminó la necesidad de realizar ataques de fuerza bruta complejos. Esto permitió que una intrusión web se transformara en un acceso total a la "joyería" de la empresa: los datos crediticios.

Tablas técnicas y de costos

Tabla Técnica del Ataque:

Elemento	Descripción
----------	-------------

Tipo de ataque	Explotación de vulnerabilidad de ejecución remota de código (RCE) y exfiltración masiva de datos.
Actor o grupo atacante	Actores vinculados a infraestructuras de inteligencia extranjera.
Vector de entrada	Portal de disputas de consumidores expuesto a través del puerto 443.
Vulnerabilidad explotada	CVE-2017-5638 en Apache Struts, con una gravedad de 10.0 (Crítico).
Etapas del ataque (MITRE ATT&CK)	<ol style="list-style-type: none"> 1. Intrusión inicial. 2. Persistencia (instalación de Web Shells). 3. Reconocimiento interno. 4. Movimiento lateral a bases de datos. 5. Exfiltración cifrada de datos.
Sistemas o servicios comprometidos	Servidor web del portal de disputas y servidores de bases de datos centrales de crédito.
Duración del incidente	76 días de actividad maliciosa activa (del 13 de mayo al 29 de julio de 2017).
Mecanismos de detección y respuesta	Identificación de tráfico sospechoso durante revisión de rutina. Bloqueo del portal, activación de protocolo de respuesta y contratación de Mandiant para peritaje forense.

Evaluación del impacto(ModeloCIA):

Principio	Descripción del impacto	Evidencia del caso
Confidencialidad	¿Qué información fue expuesta o robada?	Robo de registros de 147.5 millones de personas , incluyendo nombres, números de seguro social, fechas de nacimiento y datos de tarjetas de crédito.
Integridad	¿Qué datos o sistemas fueron alterados?	Localización de archivos con credenciales en texto plano y ejecución de "queries" de prueba para medir la respuesta de la base de datos de crédito.
Disponibilidad	¿Qué servicios se interrumpieron o paralizaron?	Bloqueo total del acceso al portal de disputas el 29 de julio y caída del sitio web de ayuda tras el anuncio público debido a la saturación.

Cálculo del costo total del ciberataque:

Tipo de cambio promedio 2017: ≈ \$18.50 MXN por 1 USD (Banxico, promedio anual aproximado)

Tipo de costo	Descripción	Estimación (MXN)
Pérdidas operativas	Interrupción de servicios, suspensión del portal de disputas, horas hombre en contención, caída de productividad interna durante respuesta al incidente. Estimado ≈ \$90 M USD en operación y respuesta inicial.	\$1,665,000,000 MXN
Daños reputacionales	Pérdida de confianza, clientes que dejaron de usar servicios, caída del valor de acciones tras el anuncio (la empresa perdió miles de millones en valor de mercado en días posteriores). Impacto reputacional estimado conservador ≈ \$4,000 M USD en valor de marca/mercado.	\$74,000,000,000 MXN
Costos técnicos	Investigación forense (Mandiant), renovación de infraestructura, monitoreo de crédito para víctimas, mejoras en ciberseguridad. Reportes estiman más de \$1,000 M USD en gastos tecnológicos y remediación.	\$18,500,000,000 MXN
Costos legales / regulatorios	Acuerdo judicial con la FTC, CFPB y estados de EE.UU. por hasta \$700 M USD inicialmente (luego aumentó con demandas adicionales).	\$12,950,000,000 MXN
Pago de rescate o extorsión	En caso de ransomware, monto pagado o solicitado. No aplicable — no fue ransomware, fue robo y exfiltración de datos.	\$0 MXN
TOTAL ESTIMADO	Suma total en pesos mexicanos (MXN)	\$107,115,000,000 MXN

Relación con marcos normativos

A continuación, se presenta el análisis de los controles de seguridad fallidos basados en los estándares ISO 27001, el Marco de Ciberseguridad del NIST (NIST CSF) y el Reglamento General de Protección de Datos (GDPR), explicando cómo su correcta implementación habría cambiado el curso del incidente

Marco Normativo	Control / Artículo Relacionado	Descripción del Fallo en Equifax	Cómo hubiera preventido o mitigado el impacto
ISO 27001:2013	A.12.6.1 Gestión de vulnerabilidades técnicas	Equifax no identificó ni parchó la vulnerabilidad CVE-2017-5638 a tiempo, a pesar de que el parche existía desde marzo.	Prevención: Si se hubiera aplicado el parche dentro de las 48 horas posteriores a la alerta, el vector de ataque RCE habría sido ineficaz en

			mayo, impidiendo la intrusión inicial.
ISO 27001:2013	A.8.1.1 Inventario de activos	La empresa no sabía que el "Portal de Disputas" ejecutaba Apache Struts, por lo que quedó fuera del alcance del mantenimiento.	Prevención: Un inventario actualizado habría alertado a los administradores de que ese servidor específico requiera atención inmediata, asegurando que no quedaran "puntos ciegos" en la red.
NIST CSF	DE.CM-1 (Detección / Monitoreo Continuo)	El tráfico malicioso no fue detectado durante 76 días debido a que el certificado SSL del dispositivo de inspección (IDS/IPS) estaba vencido.	Mitigación: Si el certificado SSL hubiera estado vigente, el sistema de inspección habría descifrado el tráfico, detectado las firmas de las Web Shells y alertado al equipo de seguridad en horas, no en meses.
NIST CSF	PR.AC-1 (Protección / Control de Acceso)	Los atacantes encontraron credenciales de bases de datos almacenadas en texto plano dentro de los servidores comprometidos.	Mitigación: Si las credenciales hubieran estado cifradas o gestionadas mediante una bóveda (PAM), el movimiento lateral hacia las bases de datos críticas habría sido extremadamente difícil, limitando el alcance del robo.
GDPR	Art. 32 Seguridad del tratamiento	Se falló en implementar medidas técnicas apropiadas (seudonimización y cifrado) para garantizar la confidencialidad de los datos personales.	Mitigación: Si la base de datos hubiera estado cifrada en reposo (Data at Rest Encryption) y separada lógicamente de la aplicación web, los datos exfiltrados habrían sido ilegibles e inútiles para los atacantes.

Conclusiones

El ciberataque a Equifax no fue el resultado de una técnica de hackeo sofisticada e inevitable, sino la consecuencia de una serie de fallas operativas y negligencias en la gestión de seguridad. A continuación, se presentan los aprendizajes clave y las acciones preventivas necesarias para cualquier organización:

- **La visibilidad es la base de la protección:** No se puede proteger lo que no se sabe que existe. El desconocimiento de que el "Portal de Disputas" utilizaba Apache Struts dejó una brecha crítica fuera del alcance de las políticas de mantenimiento.

- **Un parche omitido es una puerta abierta:** La existencia de una solución técnica (parche) desde marzo para la vulnerabilidad CVE-2017-5638 subraya que la velocidad de respuesta es tan vital como la detección misma.
- **El cifrado sin monitoreo es un punto ciego:** Contar con herramientas de inspección es inútil si no se gestionan sus componentes básicos. El vencimiento de un certificado SSL por 10 meses permitió que los atacantes exfiltraran datos masivos sin ser detectados, ocultos tras el propio cifrado de la empresa.
- **La higiene de datos interna es crítica:** Una vez superado el perímetro, la falta de seguridad interna (como credenciales en texto plano) facilitó un acceso total a la base de datos central sin necesidad de ataques complejos.

Recomendaciones estratégicas:

- **Implementar un inventario de Activos Dinámico:** Mantener un registro automatizado y actualizado de todo el software, versiones y hardware en la red para eliminar "puntos ciegos" operativos.
- **Establecer una Política de Gestión de Parches Críticos:** Definir tiempos de respuesta obligatorios (ej. 24-48 horas) para vulnerabilidades con severidad alta o crítica (CVSS 10.0), asegurando su cumplimiento en todos los niveles de la infraestructura.
- **Automatizar la Gestión de Certificados:** Utilizar herramientas que alerten y renueven automáticamente los certificados SSL/TLS para garantizar que la visibilidad y el monitoreo del tráfico (IDS/IPS) nunca se interrumpan.
- **Adoptar el Principio de Privilegio Mínimo y Cifrado de Credenciales:** Prohibir estrictamente el almacenamiento de contraseñas en texto plano y utilizar soluciones de Gestión de Acceso Privilegiado (PAM) para dificultar el movimiento lateral de un atacante.
- **Segregación y Cifrado de Datos en Reposo:** Aplicar técnicas de seudonimización y cifrado directamente en las bases de datos para que, en caso de una exfiltración exitosa, la información sea ilegible y carezca de valor para el perpetrador.

El análisis del caso Equifax revela que la magnitud de una brecha de seguridad no depende únicamente de la habilidad del atacante, sino de la madurez operativa de la organización. El incidente de 2017 dejó de ser un simple fallo técnico para convertirse en un caso de estudio sobre negligencia sistemática. La exposición de datos de 147.5 millones de personas y un costo total estimado de \$107,115,000,000 MXN demuestran que el ahorro en mantenimiento preventivo es ínfimo comparado con las pérdidas operativas, legales y reputacionales que genera un ataque exitoso. La ciberseguridad no puede gestionarse de forma aislada; debe estar integrada en la Cadena de Mando de TI.

El caso Equifax es un recordatorio de que marcos como ISO 27001 y NIST CSF no son solo requisitos de cumplimiento, sino herramientas de supervivencia. Para una organización moderna, la ciberseguridad es una responsabilidad ética y financiera: la confianza del cliente, una vez perdida por fallos evitables como la falta de un parche o un certificado vencido, es el activo más difícil y costoso de recuperar.

Glosario

FICHA TÉCNICA: CVE-2017-5638:

- Nombre Clave: Apache Struts RCE (Remote Code Execution).
- Gravedad: 10.0 Crítico (Máxima prioridad en la escala CVSS).
- Definición: Vulnerabilidad de ejecución remota de código que permite a un atacante tomar control total de un servidor web sin necesidad de usuario ni contraseña.
- Modus Operandi: El atacante envía una petición HTTP con código malicioso oculto en el encabezado. El servidor, al intentar procesar un error de este encabezado, termina ejecutando los comandos del atacante.
- Relación con Equifax: Fue la puerta de entrada principal. El parche existía desde marzo de 2017, pero Equifax no lo aplicó, dejando la vulnerabilidad expuesta durante meses.
- Impacto Legal: Su aprovechamiento permitió el robo de datos de 147.5 millones de personas, lo que constituye una falla crítica en los controles de seguridad exigidos por la ISO 27001 y el marco NIST.

Bibliografía

- U.S. Government Accountability Office (GAO): Reporte GAO-18-559, "*Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach*". Es el documento más completo que detalla los fallos de parcheo y la falta de visibilidad técnica.
- House of Representatives (Committee on Oversight and Government Reform): Reporte final de 96 páginas titulado "*The Equifax Data Breach*". Este informe concluye que el ataque fue "completamente evitable" y detalla el uso de las *web shells* y el robo de credenciales en texto plano.
- Federal Trade Commission (FTC): Documentación sobre el acuerdo judicial (settlement) y las sanciones económicas impuestas por la falta de protección de datos personales.