

TPI – Seguridad en los Sistemas de Información
Valentino Terreno

Caso de estudio:

Starwood / Marriott

Brecha masiva de datos: 2014 - 2020

starwood
*
Hotels and
Resorts



ÍNDICE

1 Contexto del caso de estudio

2 Cronología del incidente

3 Impacto reportado

4 MITRE ATT&CK y STRIDE

5 Gestión de riesgos

6 Respuesta al incidente y
pericias forenses

Contexto del caso de estudio



Empresa multinacional estadounidense

Cadena hotelera más grande del mundo

Ingresos anuales de \$26.186 millones de dólares

Controla **más de 30 marcas**
distintas de hoteles

Cuenta con **más de 9,400 propiedades**
distribuidas en unos **144 países**

Famoso programa de fidelización, **uno de**
los más grandes de la industria turística.

Contexto del caso de estudio

Empresa multinacional estadounidense

Competencia directa de Marriott

starwood
*
Hotels and
Resorts

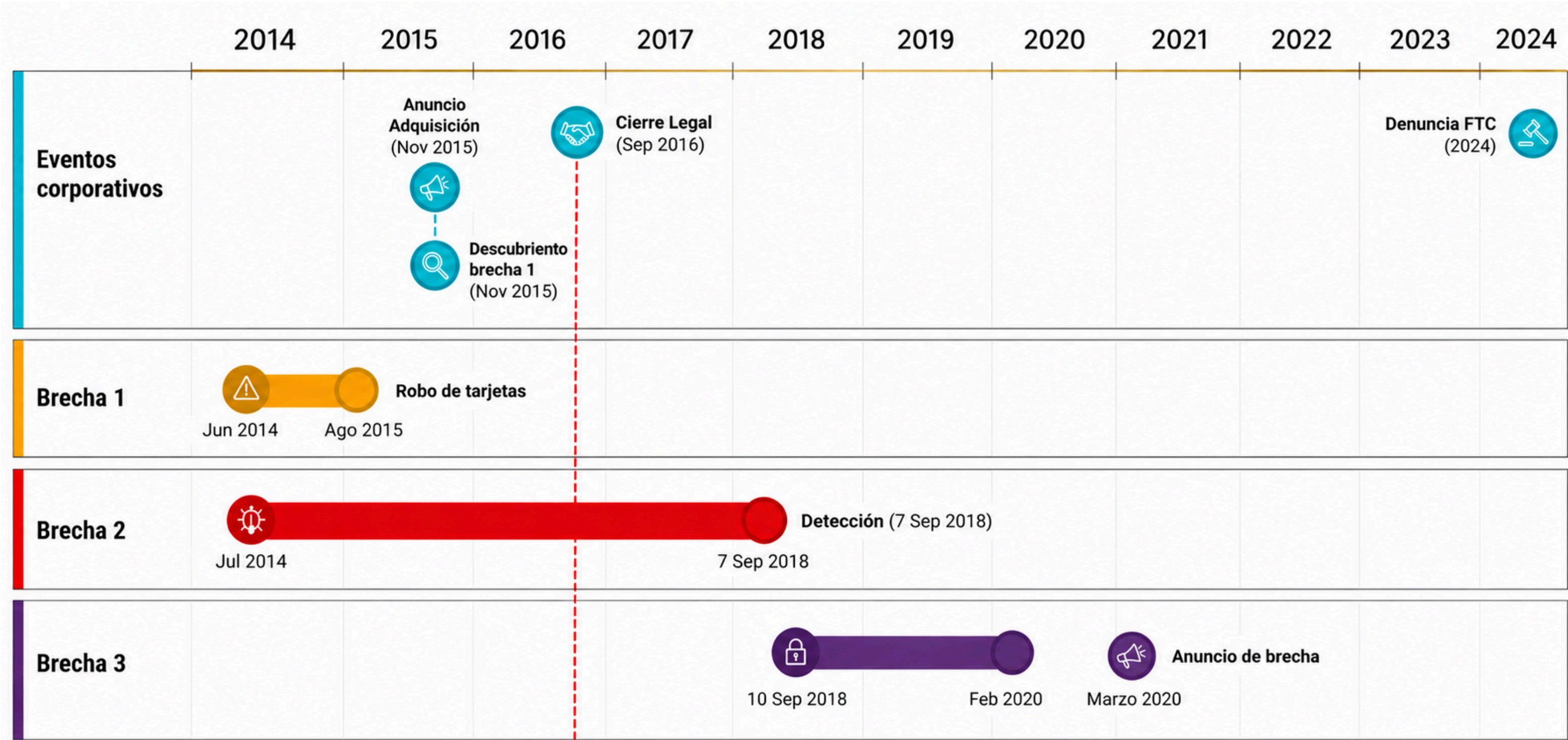


Marcas de **hoteles premium y de lujo** como Sheraton

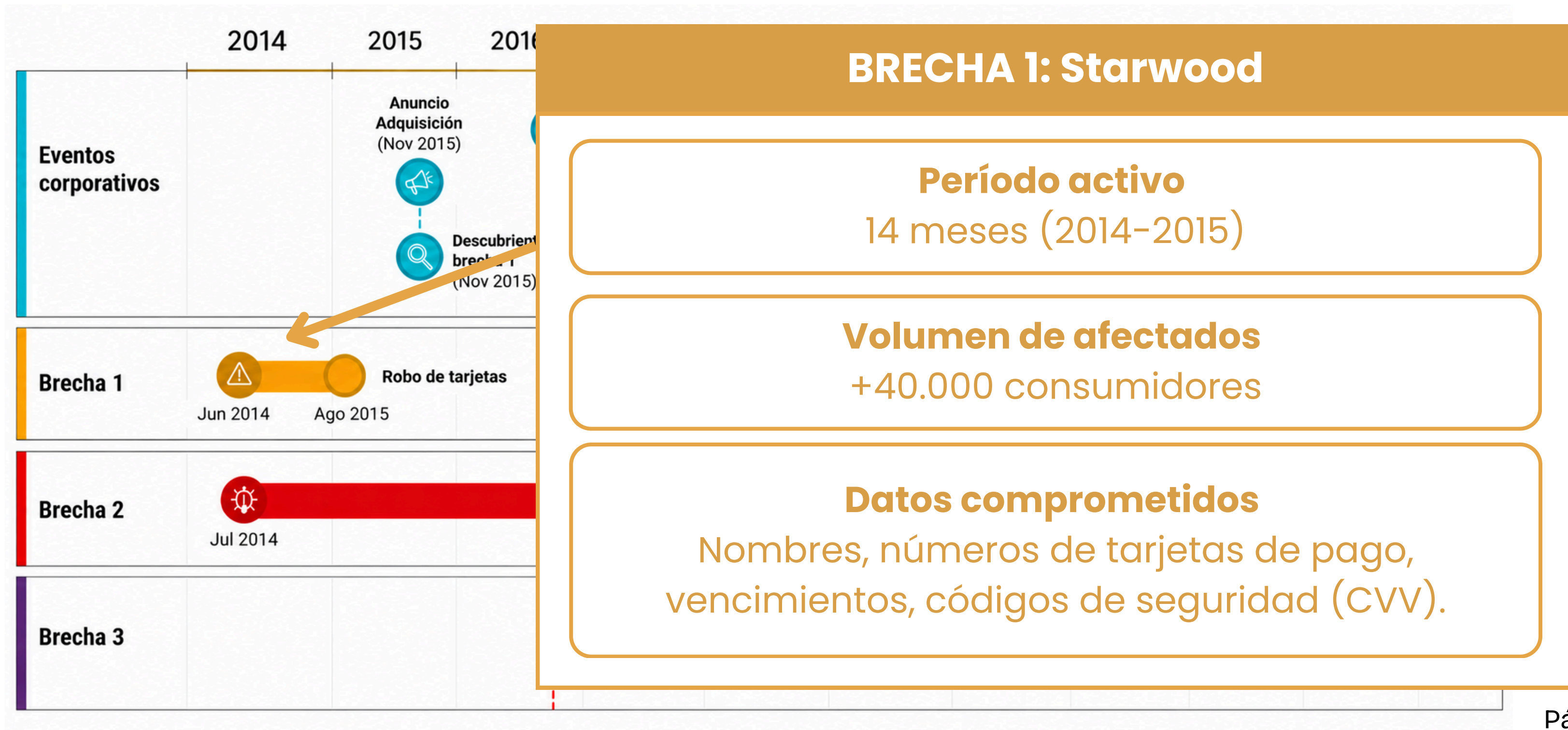
Gestionaba **más de 1,200 propiedades** en aproximadamente **100 países**

Adquirida por Marriot en sept. 2016

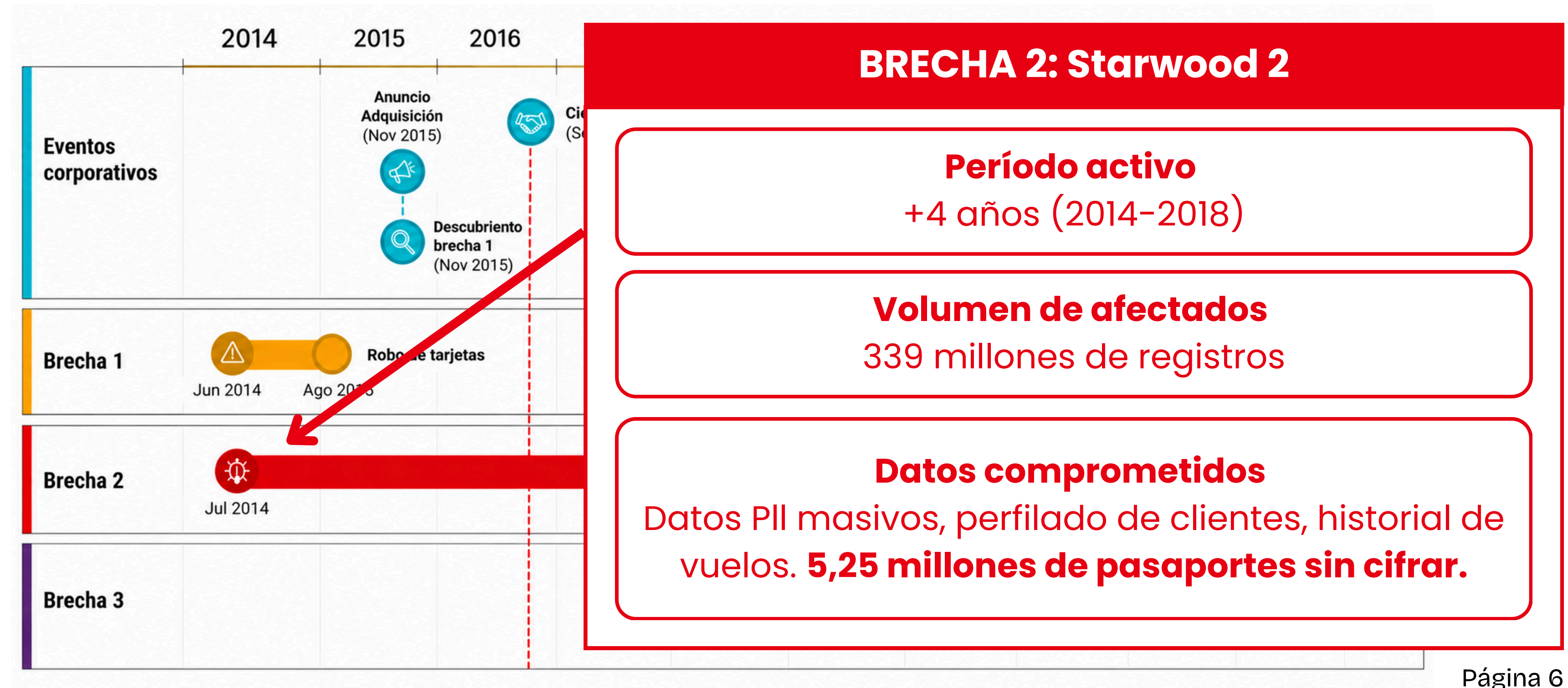
Cronología del incidente



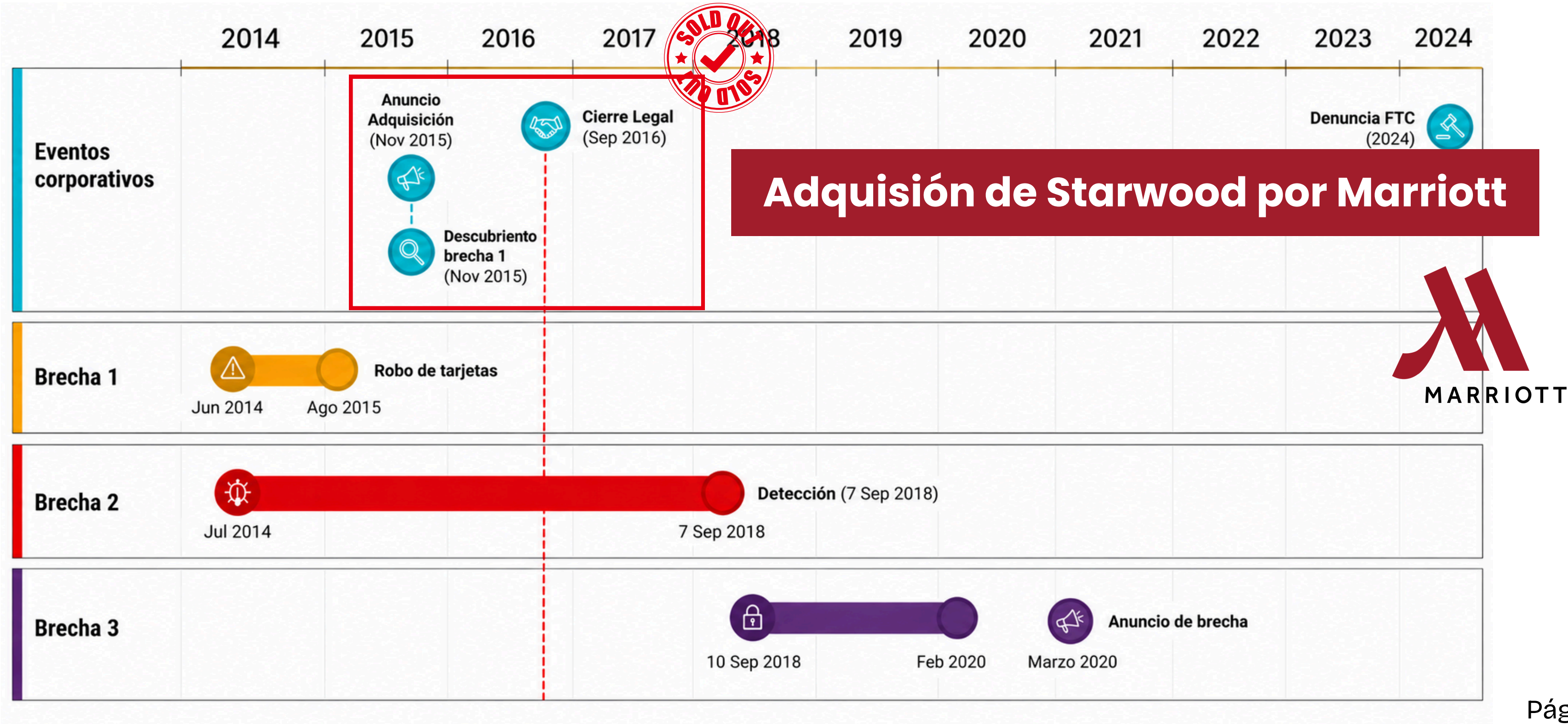
Cronología del incidente



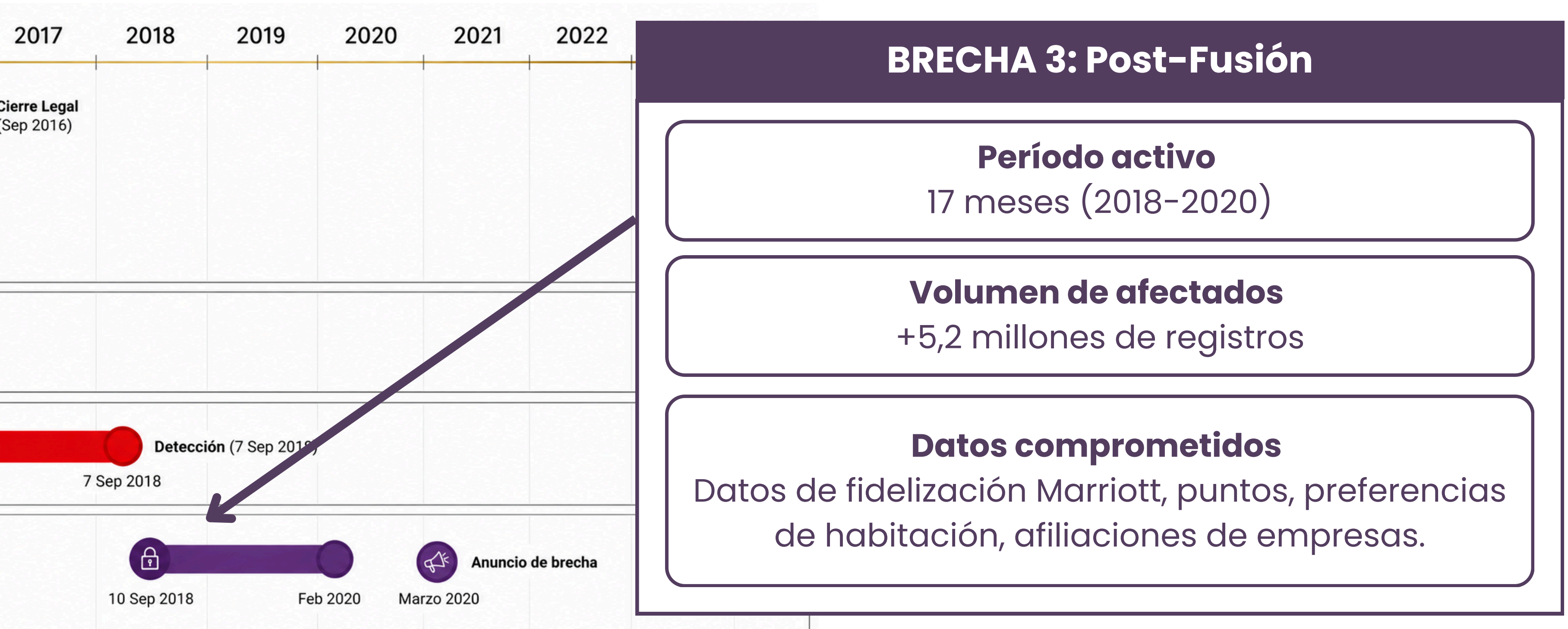
Cronología del incidente



Cronología del incidente



Cronología del incidente



Impacto reportado – Tríada CIA

C – CONFIDENCIALIDAD

339M registros de huéspedes
expuestos

5,25M pasaportes en texto plano

Tarjetas de pago sin controles
criptográficos

Perfilado detallado: viajes,
preferencias, acompañantes

I – INTEGRIDAD

Malware instalado en 480+
sistemas (keyloggers, RATs)

Cuentas privilegiadas
comprometidas

Fraude en puntos de fidelización
(Brecha 3)

Alteración del entorno de control

A – DISPONIBILIDAD

Riesgo potencial de interrupción de
reservas

Fraude en programas de beneficios

Acceso legítimo comprometido

Impacto reportado

Multas regulatorias

ICO (UK): £99M → reducida a £18,4M.
FTC (EEUU): proc. formales por U\$D52M.

Daño reputacional

Sector hotelero premium donde
privacidad y confianza son factores clave.

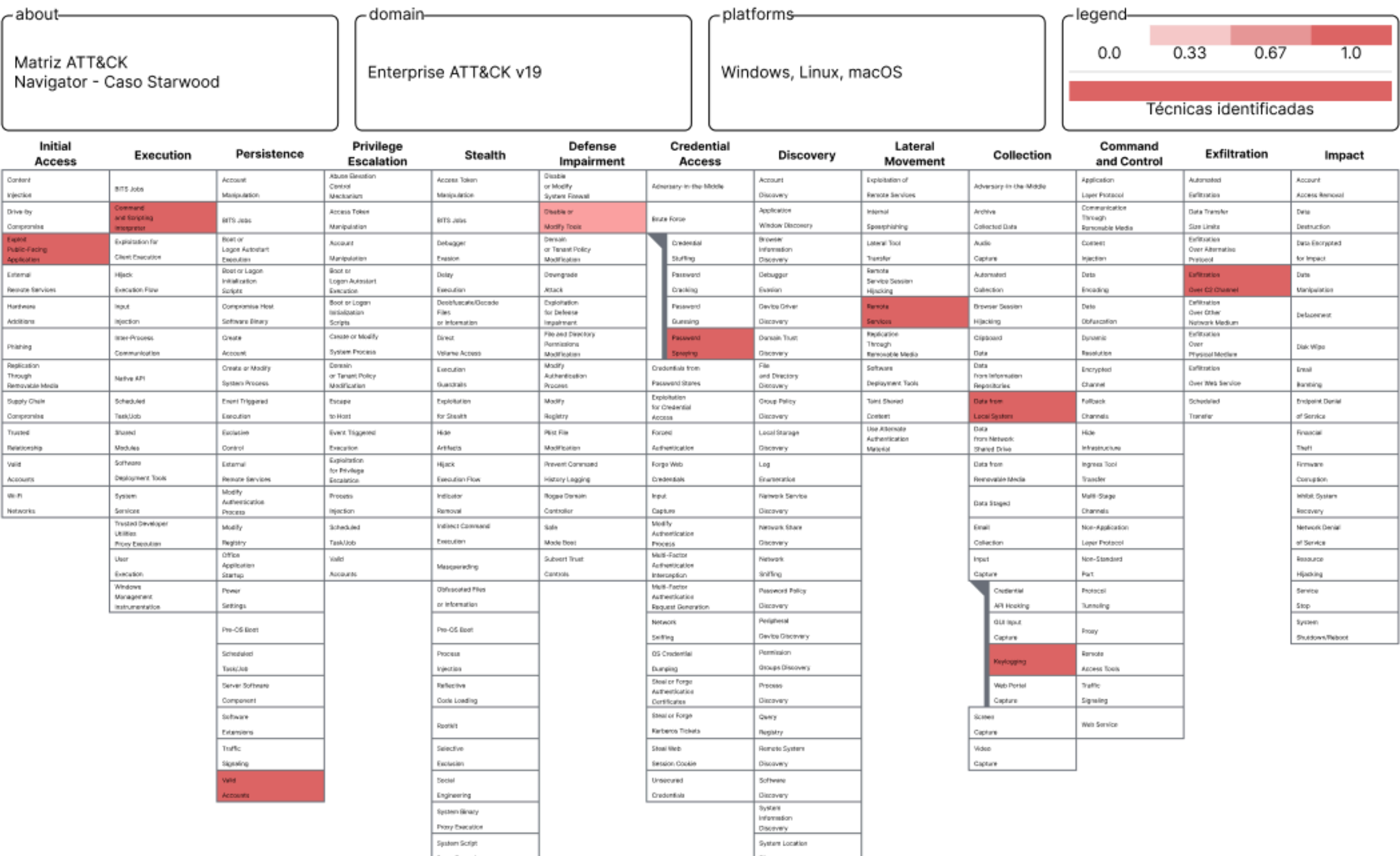
Riesgo para consumidores

Robo de identidad, fraude en puntos de
lealtad, campañas de phishing dirigidas.

Costos de remediación

Notificaciones masivas, monitoreo de
crédito, honorarios legales y forenses.

MITRE ATT&CK



MITRE ATT&CK

T1190**Exploit Public-Facing App***Initial Access*

Compromiso del servidor web externo de Starwood (Jul 2014)

T1078**Valid Accounts***Persistence*

Credenciales admin robadas para movimiento lateral durante 4 años

T1110.003**Password Spraying***Credential
Access*

Contraseñas débiles o por defecto sin controles adecuados

MITRE ATT&CK

T1056.001

Keylogging

Collection

Keyloggers en 480+ sistemas, 58 ubicaciones Starwood

T1059

Command & Scripting

Execution

RATs y malware de scraping instalados en sistemas comprometidos

T1041

Exfiltration Over C2

Exfiltration

Exportación de datos vía canales C&C detectada en Sep 2018

MITRE ATT&CK

T1685

Disable/Modify Tools

*Defense
Impairment*

Monitoreo y logging insuficiente
permitió operación sin detección

T1021

Remote Services

*Lateral
Movement*

Credenciales robadas para moverse
entre sistemas hoteleros

STRIDE



Spoofting

Credenciales robadas de empleados y administradores.
Cuentas de exempleados no desactivadas agravaron el vector.



Tampering

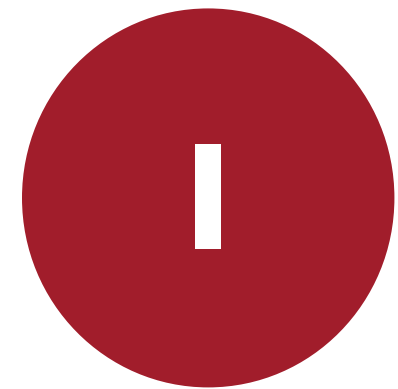
Malware (keyloggers, RATs, memory-scrapers) en 480+ sistemas alteró el comportamiento esperado y el ambiente de control.



Repudiation

Logging insuficiente impidió la trazabilidad durante años. No fue posible determinar con precisión toda la información exfiltrada.

STRIDE



Information Disclosure

Vector central: 339M registros (pasaportes, tarjetas, datos biométricos y de comportamiento) expuestos sin cifrado.



Denial of Service

Persistencia en sistemas de reservas implicó riesgo de interrupción. Brecha 3 buscó canjear puntos de lealtad fraudulentamente.



Elevation of Privilege

Escalamiento sistemático: acceso inicial en servidor web → cuentas admin → movimiento lateral → instalación de malware.

Gestión de riesgos

Controles mapeados a NIST SP 800-53 y CIS Controls v8

Riesgo = Probabilidad x Impacto (escala 1-5)

Explotación de credenciales débiles o por defecto

Score 25 – Crítico

Control fallido: NIST IA-2 / CIS 6
Falta de Autenticación Multifactor – MFA

Monitoreo, visibilidad y logging insuficiente

Score 25 – Crítico

Control fallido: NIST AU-6 / CIS 8
Inexistencia de recolección y análisis de Logs/SIEM

Gestión de riesgos

Controles mapeados a NIST SP 800-53 y CIS Controls v8

Riesgo = Probabilidad x Impacto (escala 1-5)

**Sistemas y software
desactualizados**

Score 25 – Crítico

Control fallido: NIST SI-2 / CIS 7
Aplicación de parches de seguridad

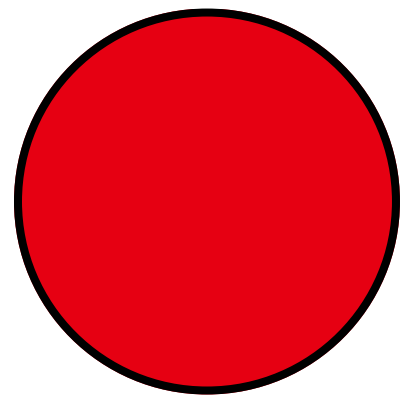
**Segmentación de red
inadecuada**

Score 20 – Crítico

Control fallido: NIST SC-7 / CIS 12
Segmentación de la red y aislamiento

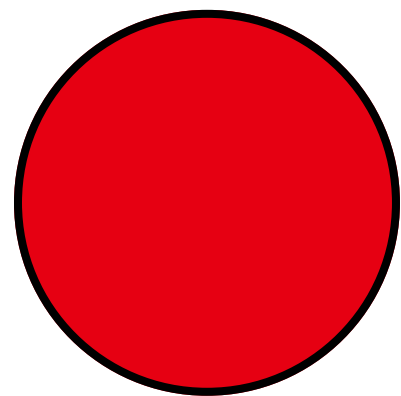
Respuesta al incidente y pericias forenses

Evaluación de la respuesta de la organización



1 – Preparación: DEFICIENTE

Heredaron una postura crítica. Controles preventivos ausentes (Sin MFA, software desactualizado, red plana). No se remedió tras la compra.

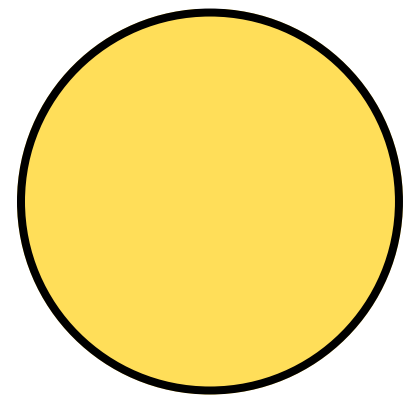


2 – Detección y análisis: DEFICIENTE

Brecha 2 no detectada por +4 años (2 años bajo control de Marriott). Detección tardía y accidental por alerta de exportación de base de datos.

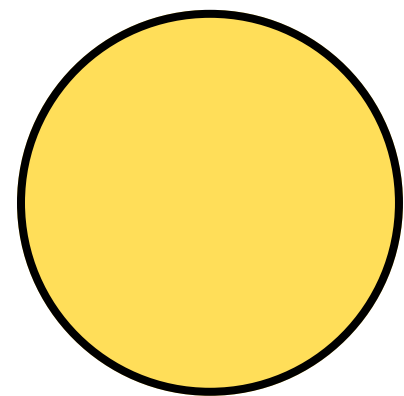
Respuesta al incidente y pericias forenses

Evaluación de la respuesta de la organización



3 – Contención y erradicación: PARCIAL

Se contrataron peritos forenses tras la detección, pero las fallas en la erradicación permitieron que la Brecha 3 iniciara y se superpusiera con la respuesta.



4 – Actividad Post-Incidente PARCIAL

Notificación regulatoria ejecutada y multas asumidas (FTC, ICO), pero las lecciones iniciales no evitaron intrusiones subsecuentes.

Respuesta al incidente y pericias forenses

Artefactos forenses

Registros de sistemas (Logs)

Apache/IIS
Active Directory
Oracle/SQL
Event Logs

Imágenes de disco (Bit-a-bit)

dd o FTK Imager
Keyloggers y RATs
Análisis de malware y
extracción de IPs C2

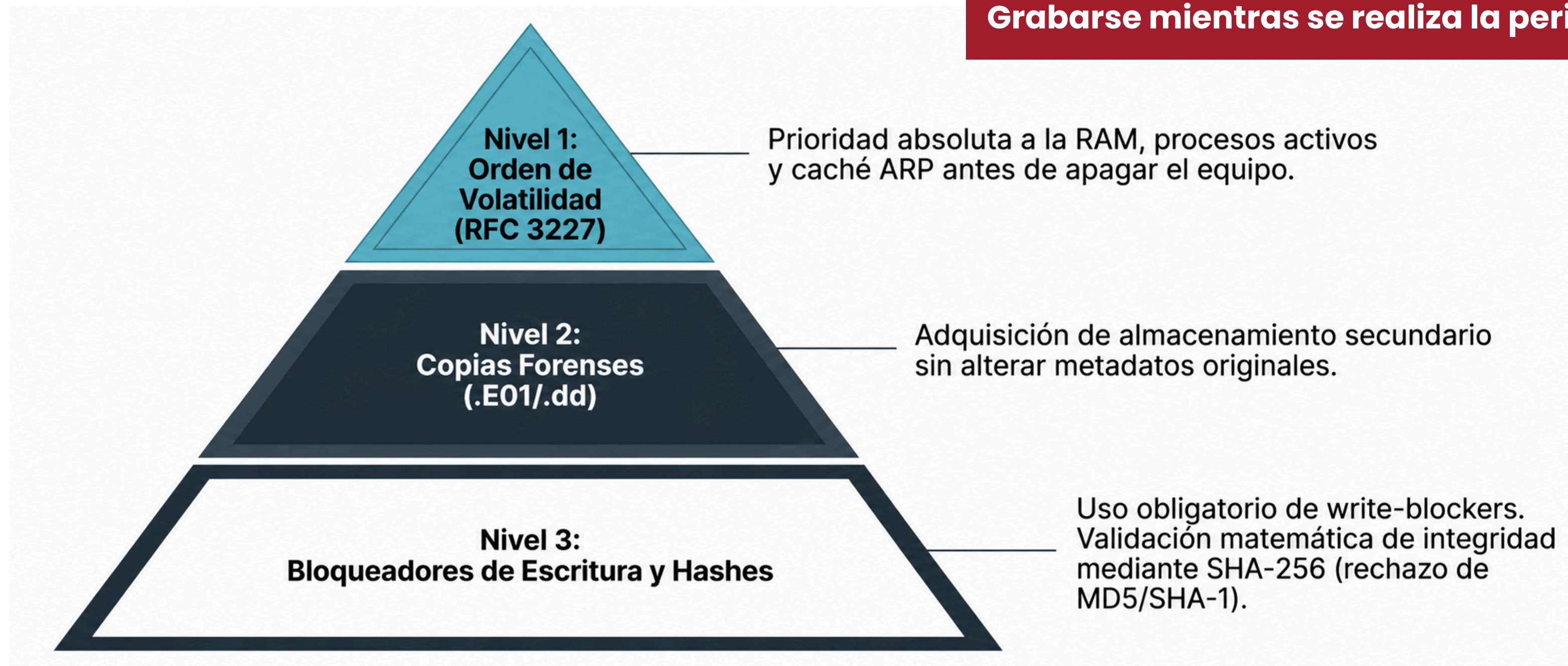
Tráfico de red (PCAP)

Capturas de paquetes de
Comando y Control
Análisis de registros para
identificar transferencias
hacia el exterior.

Respuesta al incidente y pericias forenses

Artefactos forenses

Grabarse mientras se realiza la pericia



Conclusión

Heredar una red significa heredar sus brechas. El fallo más costoso de Marriott no fue técnico, fue de gestión.

Durante una adquisición de USD 12.200 millones, Marriott falló en ejecutar el Control CIS 15 (Evaluación de seguridad de terceros).

Hoy en día, el análisis de riesgos digitales pesa tanto como el balance financiero de una organización.

¡Muchas gracias!