Análisis de una noticia sobre ataque informático

**Nicolás Aspes**

**Gustavo Camus**

Información Básica

Un ataque informático significativo ocurrió en abril de 2025 contra la [*Legal Aid Agency*](https://en.wikipedia.org/wiki/Legal_Aid_Agency) *o (LAA)* una agencia ejecutiva del Ministerio de Justicia del Reino Unido, comprometiendo datos personales sensibles de aproximadamente 2,1 millones de personas que solicitaron asistencia legal en dicha compañía desde 2010.

¿Cómo se llevó a cabo el ataque?

El 23 de abril de 2025, el Ministerio de Justicia detectó una intrusión en los sistemas de la LAA. Los detalles técnicos no se han divulgado públicamente pero se sabe que los atacantes accedieron de manera directa a los sistemas digitales de la agencia, lo que sugiere una posible explotación de vulnerabilidades en la infraestructura tecnológica. La falta de inversión en sistemas modernos y seguros pudo haber facilitado el acceso no autorizado.

Método utilizado

Hasta el momento, no se ha revelado públicamente el método técnico exacto que los atacantes usaron para vulnerar los sistemas de la Legal Aid Agency del Reino Unido. Sin embargo, expertos y medios especializados han planteado hipótesis fundamentadas sobre cómo pudo haberse realizado el ataque, basándose en el tipo de datos comprometidos y la estructura de la institución afectada.

### **Hipótesis sobre el método utilizado:**

#### **1. Explotación de vulnerabilidades Seguridad**

Posibilidad más probable, dado que se trata de una agencia pública con infraestructura tecnológica conocida por ser antigua y mal mantenida como vulnerabilidades en Apache, Servidores Windows, Key login, Descuido de empleados y correos informaticos.

#### **2. Ataque de tipo phishing dirigido (spear phishing)**

Otra vía probable es que los atacantes enviaran correos falsos a empleados clave, logrando robar credenciales de acceso, Esto explicaría cómo obtuvieron acceso a sistemas internos sin necesidad de explotar software directamente.

### Consecuencias del ataque

* **Datos comprometidos**: Información personal como nombres, direcciones, fechas de nacimiento, historiales penales, números de seguro nacional, detalles financieros y situación laboral de los solicitantes de asistencia legal.
* **Impacto en servicios**: La LAA tuvo que desconectar sus servicios en línea, lo que afectó la tramitación de casos legales y retrasó pagos a representantes legales.
* **Riesgos para los afectados**: Expertos en ciberseguridad advirtieron sobre posibles fraudes y extorsiones debido al acceso a información sensible.

Delitos cometidos

El ataque constituye una violación de la Ley de Protección de Datos del Reino Unido y del [Reglamento General de Protección de Datos (GDPR)](https://en.wikipedia.org/wiki/General_Data_Protection_Regulation) de la Unión Europea. Las acciones ilegales incluyen:

* **Acceso no autorizado a sistemas informáticos**: Infracción de leyes que protegen la integridad de los sistemas digitales gubernamentales.
* **Robo de información personal**: Obtención y posible distribución de datos personales sin consentimiento, lo que puede derivar en sanciones penales y civiles.
* **Posible extorsión**: Si se demuestra que los atacantes intentaron obtener beneficios económicos mediante amenazas relacionadas con la información robada.

Las autoridades pertinentes, incluida la [Oficina del Comisionado de Información](https://en.wikipedia.org/wiki/Information_Commissioner%27s_Office) (ICO), investigaron el incidente y podrían imponer sanciones significativas a los responsables.

Consecuencias para los involucrados

**Ciberdelincuentes:** Prisión (hasta 10 años) + multas, Por acceso ilegal, robo de datos, posible extorsión

**La Legal Aid Agency:** Multas hasta €20M + auditorías, Por mala protección de datos personales bajo el GDPR

**Para el Gobierno británico**: Obligación de reformar su infraestructura digital, Recomendaciones del ICO tras la investigación

Análisis de delitos informáticos hipotéticos en Chile

### **Delitos aplicables**

En Chile, el **Delito de acceso ilícito y robo de datos personales** está regulado principalmente por:

* **Ley Nº 21.459 (Ley de Delitos Informáticos)**: publicada en agosto de 2022.
* **Ley Nº 19.628 sobre protección de la vida privada** (en proceso de reforma para alinearse con estándares OCDE/GDPR).
* **Código Penal** (para delitos conexos como extorsión o amenazas).

**Comparativa:**

|  |  |  |
| --- | --- | --- |
| **Situación UK** | **Ley UK / GDPR** | **Equivalente en Chile** |
| **Robo de datos por hackers** | **Computer Misuse Act / GDPR** | **Ley 21.459 (Delitos Informáticos)** |
| **Mal manejo institucional** | **GDPR** | **Ley 19.628 y reforma 2025** |
| **Sanciones a los atacantes** | **Prisión y multas** | **Prisión (hasta 5 años) + multas en UTM** |
| **Sanciones a la agencia** | **Hasta €20M** | **Hasta 10.000 UTM (propuesta)** |

### 

### 

### 

### 

### 

### 

### 

### 

### 

### 

### **STRIDE**

### **1. Spoofing (Suplantación de identidad)**

**Amenaza**:

Un atacante se hace pasar por otro jugador (por ejemplo, usando credenciales robadas o manipulando paquetes).

Falsificación de identidad para acceder a cuentas premium.

***Mitigación:***

Autenticación segura (por ejemplo, tokens JWT, OAuth2).

Autenticación de dos factores (2FA).

Validación criptográfica de mensajes entre cliente y servidor.

### ***2. Tampering (Manipulación de datos)***

***Amenaza:***

Alterar paquetes enviados al servidor (por ejemplo, modificando el daño o velocidad en un shooter).

Hackers modifican el cliente para enviar información ilegal (cheats, aimbots).

***Mitigación:***

Validación estricta del lado del servidor.

Uso de canales cifrados (TLS).

Anticheat en cliente + detección en servidor de patrones anómalos.

### ***3. Repudiation (Negación de acciones)***

***Amenaza:***

Jugadores niegan haber hecho trampas, usado exploits, o enviado ciertos mensajes ofensivos.

***Mitigación:***

Logging detallado en el servidor (acciones, IP, timestamps).

Firmado de logs o eventos críticos.

### ***4. Information Disclosure (Divulgación de información)***

***Amenaza:***

Filtración de datos de usuarios (correos, contraseñas, estadísticas privadas).

Exposición de detalles técnicos del servidor que puedan usarse para ataques.

***Mitigación:***

Cifrado en tránsito y en reposo.

Control de acceso a datos sensibles.

Minimizar información expuesta en errores o APIs.

***5. Denial of Service (DoS)***

***Amenaza:***

Atacar el servidor para que deje de responder (saturación de conexiones, spam de solicitudes).

Uso excesivo de recursos por scripts maliciosos o jugadores bots.

***Mitigación:***

Firewalls y sistemas de detección de intrusos.

Rate limiting.

Balanceadores de carga y escalado automático.

### ***6. Elevation of Privilege (Elevación de privilegios)***

***Amenaza:***

Un jugador normal obtiene acceso a comandos de administración.

Vulnerabilidades que permiten cambiar estadísticas o recursos.

***Mitigación:***

Separación clara de roles (administrador, moderador, jugador).

Revisión del código para prevenir inyecciones o exploits.

Autorización estricta en cada acción.

Fuentes:

Fuentes principales:

<https://www.reuters.com/world/uk/personal-data-taken-uk-legal-aid-cyber-attack-govt-says-2025-05-19/>

otras:

<https://www.thescottishsun.co.uk/news/14811241/ministry-cyber-attack-data/>

<https://apnews.com/article/britain-cyberattack-uk-legal-aid-d0235240d360fb8926082d358e3>

[bb520](https://apnews.com/article/britain-cyberattack-uk-legal-aid-d0235240d360fb8926082d358e3)

<https://www.thetimes.com/uk/crime/article/criminal-records-cyber-attack-legal-aid-xzpbw08s3?region=global>