Sin seguridad no hay privacidad

Gobierno del Dato y Toma de Decisiones

**Integrantes:**

Leonard Jose Cuenca Roa

Paola Michelle Figueroa Benítez

Lowenski Paredes Rosario

Carlos Damián Rodriguez Uitzil

Contents

[Parte I 1](#_Toc189846221)

[¿Qué es el Caso Ashley Madison? 2](#_Toc189846222)

[Cómo se materializó el ataque: 2](#_Toc189846223)

[Por qué tuvo éxito: 4](#_Toc189846224)

[Consecuencias para los afectados: 4](#_Toc189846225)

[Justificación: 4](#_Toc189846226)

[Evaluación: 5](#_Toc189846227)

[Parte II 6](#_Toc189846228)

Parte I

### ¿Qué es el Caso Ashley Madison?

El caso de Ashley Madison, la plataforma de citas para personas casadas es un claro ejemplo de cómo las filtraciones de datos pueden tener consecuencias devastadoras en la vida de las personas. La información personal y preferencias sexuales de 32 millones de usuarios fueron expuestas, Desde una perspectiva de ciencia de datos, este caso subraya la importancia crítica de la seguridad y privacidad en el manejo de información personal.

El portal Ashley Madison fue víctima de un ataque cibernético masivo por parte de un grupo llamado **Impact Team**. Los atacantes lograron acceder a la base de datos de la empresa y robaron información personal y financiera de millones de usuarios, así como documentos internos de la empresa.

Los datos, en este contexto, no son solo números y estadísticas, sino que representan la vida y reputación de individuos. La vulnerabilidad de Ashley Madison expone la necesidad de implementar medidas de seguridad robustas y protocolos de protección de datos efectivos.

El modelo de negocio de Ashley Madison, basado en la creación de un espacio para aventuras extramatrimoniales, fue innovador en su momento. Sin embargo, la empresa no anticipó el riesgo que representaba la filtración de datos a gran escala. La recopilación de información personal sensible, como fotos y preferencias sexuales, creó un objetivo atractivo para los hackers. Este caso nos enseña que cualquier empresa que maneje datos personales, independientemente de su naturaleza, debe priorizar la seguridad de la información.

### Cómo se materializó el ataque:

* **Vulnerabilidades de Seguridad:**
  + **Las vulnerabilidades XSS (Cross-Site Scripting) y CSRF (Cross-Site Request Forgery):** son dos de las amenazas más comunes y peligrosas en la seguridad web actual, ocurre cuando un atacante logra insertar scripts maliciosos en un sitio web legítimo y confiable. Estos scripts se ejecutan en el navegador de otros usuarios que visitan el sitio, lo que permite al atacante robar información confidencial, como cookies de sesión, datos personales o credenciales de acceso.
  + **Vulnerabilidades in-the-wild**: se refiere que está siendo **activamente explotada por atacantes reales** en situaciones reales, no solo en entornos de laboratorio o pruebas. Esto significa que ya existen ataques dirigidos que se aprovechan de esa debilidad específica.
  + **Ataques phishing**: Es un tipo de ataque de ingeniería social que busca engañar a las personas para que revelen información confidencial, como contraseñas, números de tarjetas de créditoo datos personales. Generalmente, se realiza a través de correos electrónicos, mensajes de texto o sitios web falsos que imitan a entidades legítimas
  + **Vulnerabilidades por fuga de datos**: Ocurre cuando información confidencial se expone o se divulga sin autorización. Esto puede suceder de diversas maneras, como por ejemplo: acceso no autorizado, donde un atacante logra acceder a la base de datos o a los archivos que contienen la información confidencial. Por le evidencia que dejaron los hacker **Impact Team,** también hubo esta vulnerabilidad.
  + **Ataque por La inyección SQL:** Es un tipo de ataque que se aprovecha de vulnerabilidades en las aplicaciones web que utilizan bases de datos SQL. El atacante introduce código SQL malicioso en la aplicación, lo que le permite manipular la base de datos y acceder a información confidencial, modificarla o incluso eliminarla.
  + **Ignorar las advertencias de seguridad**: La empresa matriz de Ashley Madison, Avid Life Media (ALM), tenía vulnerabilidades de seguridad conocidas en su sistema. A pesar de las advertencias internas sobre estas vulnerabilidades, no se tomaron medidas adecuadas para solucionarlas.
* **Acceso a la Base de Datos:** **Impact Team** logró explotar estas vulnerabilidades para acceder a la base de datos de ALM.
* **Extracción y Publicación de Datos:** Los atacantes extrajeron la información robada y la publicaron en línea, exponiendo los datos personales y financieros de millones de usuarios.

### Por qué tuvo éxito:

El ataque tuvo éxito debido a una combinación de factores:

* **Falta de Atención a la Seguridad:** A pesar de las advertencias internas, ALM no priorizó la seguridad de sus sistemas y no implementó medidas de protección adecuadas.
* **Vulnerabilidades Explotables:** Las vulnerabilidades de seguridad existentes en los sistemas de ALM permitieron a los atacantes acceder a la base de datos sin mayores dificultades.

### Consecuencias para los afectados:

Las consecuencias para los usuarios de Ashley Madison fueron graves:

* **Exposición de Información Personal:** La publicación de datos personales, incluyendo nombres, direcciones, preferencias sexuales y detalles de tarjetas de crédito, expuso a los usuarios a la humillación pública, el chantaje y posibles riesgos de seguridad.
* **Daño a la Reputación:** La filtración de datos tuvo un impacto negativo en la reputación de los usuarios, especialmente aquellos que buscaban mantener su participación en el sitio web en secreto.
* **Impacto Emocional:** La exposición pública de información personal y la posibilidad de enfrentar consecuencias personales y sociales causaron un gran estrés emocional a los usuarios afectados.

### Justificación:

El caso de la filtración de datos de Ashley Madison constituye una clara violación de la seguridad de datos y un incumplimiento del Reglamento General de Protección de Datos (RGPD). La exposición pública de datos sensibles de los usuarios, como sus preferencias sexuales y datos de contacto, vulnera el principio de **integridad y confidencialidad** del RGPD, que exige la protección de la información contra accesos no autorizados y divulgación.

Adicionalmente, la práctica de cobrar a los usuarios por eliminar sus perfiles y la subsiguiente retención de sus datos en el sistema contraviene los principios de **licitud, lealtad y transparencia**. El RGPD establece que los datos deben ser tratados de manera justa y transparente para el interesado, lo cual implica informar claramente sobre el tratamiento de los datos y obtener el consentimiento para ello.

Asimismo, la recopilación y almacenamiento de información adicional, como direcciones y datos bancarios, sin una justificación clara y una finalidad específica, podría infringir el principio de **limitación de la finalidad** del RGPD, que establece que los datos solo pueden ser tratados para fines determinados y legítimos.

### Evaluación:

En efecto, la notificación del incidente a la autoridad de control competente y a los afectados era obligatoria, de acuerdo con lo establecido en el RGPD. La gravedad de la filtración de datos de Ashley Madison, que incluía información sensible sobre la vida personal de los usuarios, como sus preferencias sexuales y datos de contacto, exigía el cumplimiento de esta obligación.

Es importante destacar que, si bien la notificación a los afectados es un requisito del RGPD, esto no garantiza que puedan protegerse completamente del impacto negativo de la divulgación de su información. En el caso específico de Ashley Madison, la naturaleza altamente sensible de los datos filtrados, relacionada con la infidelidad, produjo un daño emocional y social significativo para los usuarios, debido al estigma social asociado a estas conductas.

No obstante, la notificación a los afectados habría brindado a los usuarios la oportunidad de tomar medidas para mitigar los riesgos y minimizar los daños. En primer lugar, podrían haber tomado decisiones en el ámbito personal, como informar a sus parejas o buscar apoyo emocional. En segundo lugar, en lo que respecta a la información financiera, la notificación les habría permitido tomar medidas preventivas, como cancelar cuentas bancarias o bloquear tarjetas de crédito, para protegerse contra posibles fraudes o robos de identidad

Parte II