1. Falla de Sony PlayStation Network (abril de 2011)

¿Qué información se expuso?
Se expusieron datos personales de aproximadamente 77 millones de usuarios, incluyendo nombres, direcciones físicas, direcciones de correo electrónico, fechas de nacimiento, nombres de usuario, contraseñas y posiblemente información financiera como números de tarjetas de crédito y débito.

¿Cómo afectó la filtración a la empresa y a sus clientes?
Sony tuvo que suspender el servicio de PlayStation Network durante casi un mes, lo que afectó a millones de jugadores. La empresa enfrentó críticas por la demora en informar a los usuarios y sufrió una pérdida de confianza significativa.

¿Qué impacto tuvo la pérdida de datos?
Además de las implicaciones legales y financieras, la reputación de Sony se vio gravemente afectada. La empresa enfrentó demandas colectivas y tuvo que invertir en mejorar su infraestructura de seguridad.

¿Qué se podía hacer para evitar tales fallas en los datos?
Implementar medidas de seguridad más robustas, como cifrado de datos sensibles, monitoreo constante de la red y protocolos de respuesta rápida ante incidentes de seguridad.

2. Dropbox (agosto de 2012)

¿Qué información se expuso?
Se filtraron direcciones de correo electrónico y contraseñas cifradas (hashed y salted) de aproximadamente 68 millones de cuentas de usuarios.

¿Cómo afectó la filtración a la empresa y a sus clientes?
Aunque las contraseñas estaban cifradas, la filtración generó preocupaciones sobre la seguridad de la plataforma. Dropbox tuvo que reforzar sus medidas de seguridad y recomendar a los usuarios cambiar sus contraseñas.

¿Qué impacto tuvo la pérdida de datos?
La confianza de los usuarios se vio comprometida, y la empresa enfrentó críticas por no haber detectado la brecha antes.

¿Qué se podía hacer para evitar tales fallas en los datos?
Adoptar autenticación de dos factores, realizar auditorías de seguridad periódicas y educar a los usuarios sobre la importancia de contraseñas únicas y seguras.

3. Ashley Madison (2015)

¿Qué información se expuso?
Se filtraron datos personales de más de 36 millones de usuarios, incluyendo nombres, direcciones, números de teléfono, correos electrónicos, detalles de tarjetas de crédito y mensajes privados.

¿Cómo afectó la filtración a la empresa y a sus clientes?
La exposición de información sensible tuvo consecuencias devastadoras para muchos usuarios, incluyendo casos de extorsión y suicidios. La empresa enfrentó múltiples demandas y su reputación quedó gravemente dañada.

¿Qué impacto tuvo la pérdida de datos?
Además del daño a los usuarios, la empresa tuvo que pagar un acuerdo de $11.2 millones para resolver demandas colectivas y perdió una parte significativa de su base de usuarios.

¿Qué se podía hacer para evitar tales fallas en los datos?
Implementar políticas de eliminación segura de datos, mejorar la infraestructura de seguridad y ser transparente con los usuarios sobre las prácticas de protección de datos.

4. UIDAI (Aadhaar)

¿Qué información se expuso?
Se filtraron datos personales de aproximadamente 815 millones de ciudadanos indios, incluyendo nombres, direcciones, números de teléfono, números de Aadhaar y posiblemente datos biométricos.

¿Cómo afectó la filtración a la empresa y a sus clientes?
La filtración generó preocupaciones sobre la privacidad y seguridad de los datos personales en India. La confianza en el sistema Aadhaar se vio comprometida.

¿Qué impacto tuvo la pérdida de datos?
El acceso no autorizado a datos sensibles facilitó actividades fraudulentas y suplantación de identidad, afectando la seguridad financiera y personal de millones de ciudadanos.

¿Qué se podía hacer para evitar tales fallas en los datos?
Implementar controles de acceso más estrictos, cifrado de datos sensibles y monitoreo constante de posibles vulnerabilidades en el sistema.