Existen varios casos de fallas de grandes corporaciones en la protección de la información como son:

1. Falla de Sony PlayStation network (Abril de 2011)

**¿Qué sucedió?**  
Entre el 17 y 19 de abril de 2011, hackers accedieron ilegalmente a los servidores de Sony, comprometiendo la información de aproximadamente 77 millones de cuentas de PlayStation Network (PSN). [The Guardian](https://www.theguardian.com/technology/2011/apr/26/playstation-network-hackers-data?utm_source=chatgpt.com)

**¿Qué información se expuso?**

* Nombres, direcciones, correos electrónicos, fechas de nacimiento, nombres de usuario, contraseñas y preguntas de seguridad.
* Posiblemente, información de tarjetas de crédito.

**Impacto para la empresa y los clientes:**

* Cierre de PSN durante casi un mes, afectando a millones de jugadores.
* Pérdidas económicas estimadas en 171 millones de dólares.
* Daño significativo a la reputación de Sony y pérdida de confianza de los usuarios.

**¿Cómo se podía evitar?**

* Implementación de cifrado robusto para datos sensibles.
* Actualizaciones y parches de seguridad regulares.
* Monitoreo continuo de la red para detectar actividades sospechosas.

1. Drobpox (Agosto de 2012)

**¿Qué sucedió?**  
En 2012, Dropbox sufrió una brecha de seguridad que resultó en la exposición de datos de más de 68 millones de cuentas. [The Verge+2Sprintzeal.com+2cyberpolicy.com+2](https://www.sprintzeal.com/blog/dropbox-data-breach?utm_source=chatgpt.com)

**¿Qué información se expuso?**

* Direcciones de correo electrónico y contraseñas cifradas (hashed y salteadas).

**Impacto para la empresa y los clientes:**

* Riesgo de acceso no autorizado a cuentas si los usuarios reutilizaban contraseñas.
* Pérdida de confianza en la seguridad de la plataforma.

**¿Cómo se podía evitar?**

* Fomento del uso de contraseñas únicas y seguras.
* Implementación de autenticación de dos factores.
* Educación a los empleados sobre prácticas de seguridad cibernética.

1. Ashley Madison (2015)

**¿Qué sucedió?**  
En julio de 2015, un grupo de hackers llamado "The Impact Team" accedió y filtró datos de usuarios del sitio de citas Ashley Madison, que se promocionaba para facilitar relaciones extramaritales. [The Guardian+5Wikipedia+5athreon.com+5](https://en.wikipedia.org/wiki/Ashley_Madison_data_breach?utm_source=chatgpt.com)

**¿Qué información se expuso?**

* Nombres, direcciones, correos electrónicos, detalles de transacciones, y preferencias personales de aproximadamente 36 millones de usuarios.

**Impacto para la empresa y los clientes:**

* Exposición pública de usuarios, causando vergüenza, rupturas matrimoniales y, en algunos casos, suicidios.
* Demandas legales y pérdida significativa de reputación para la empresa.

**¿Cómo se podía evitar?**

* Implementación de protocolos de seguridad más estrictos, como el cifrado de datos sensibles.
* Garantizar la eliminación completa de la información de los usuarios que lo soliciten.
* Transparencia en las políticas de privacidad y seguridad.

1. UIDAI (Aadhaar)

**¿Qué sucedió?**  
Entre agosto de 2017 y enero de 2018, se descubrió que datos personales de aproximadamente 1.1 mil millones de ciudadanos indios registrados en el sistema Aadhaar estaban vulnerables y algunos fueron encontrados a la venta en la dark web. [moneylife.in](https://www.moneylife.in/article/aadhaar-data-breach-largest-in-the-world-says-wefs-global-risk-report-and-avast/56384.html?utm_source=chatgpt.com)

**¿Qué información se expuso?**

* Números de Aadhaar, nombres, direcciones, números de teléfono, correos electrónicos y datos biométricos como huellas dactilares e iris.

**Impacto para la empresa y los clientes:**

* Riesgo significativo de robo de identidad y fraudes financieros.
* Pérdida de confianza en el sistema de identificación nacional.

**¿Cómo se podía evitar?**

* Implementación de controles de acceso más estrictos.
* Monitoreo regular de la seguridad del sistema.
* Educación a los usuarios sobre la importancia de proteger su información personal.