Actividad 1

Análisis de casos destacados en brechas de seguridad

Existen algunos ejemplos de cómo corporaciones han tenido dificultades cumpliendo las normatividades de manejo de datos y las consecuencias. Para ello en grupos discutan los siguientes casos. En cada caso los estudiantes deben consultar los valores estimados de las multas impuestas y el daño que los usuarios sufrieron por culpa de las fallas en la protección de la información.

Equifax: Una de las mayores agencias de informes crediticios de Estados Unidos sufrió una brecha de datos en 2017 que expuso la información personal de más de 147 millones de consumidores. Las consecuencias incluyeron multas millonarias, pérdida de confianza de los consumidores y un daño significativo a la reputación de la empresa.

Respuesta: En 2017, Equifax, una de las principales agencias de informes crediticios de EE.UU., sufrió una violación de datos que afectó a más de 147 millones de personas, exponiendo información sensible como números de Seguro Social y direcciones. Las consecuencias fueron graves: la empresa recibió una multa de hasta **$700 millones** por parte de la FTC y otros reguladores. Además, los usuarios afectados enfrentaron riesgos de robo de identidad y fraudes financieros, lo que generó una pérdida masiva de confianza en la compañía. Este caso demostró la importancia de fortalecer los sistemas de ciberseguridad para proteger datos críticos.

Cambridge Analytica: Esta empresa consultora política utilizó los datos de millones de usuarios de Facebook sin su consentimiento para influir en las elecciones presidenciales de Estados Unidos en 2016. Este escándalo desencadenó una serie de investigaciones y cambios regulatorios en todo el mundo, y generó un debate sobre la privacidad en la era digital.

Respuesta: Cambridge Analytica recolectó datos de 87 millones de usuarios de Facebook sin su consentimiento, utilizándolos para manipular campañas políticas,

incluyendo las elecciones presidenciales de EE.UU. en 2016. El escándalo llevó a una multa de $5 mil millones a Facebook por la FTC y provocó cambios globales en regulaciones de privacidad, como el GDPR en Europa. Los usuarios afectados vieron vulnerada su privacidad, y el caso generó un debate sobre el uso ético de los datos en redes sociales.

Marriott International: En 2018, Marriott International reveló que los datos de hasta 500 millones de huéspedes de sus hoteles habían sido expuestos en una brecha de seguridad. La compañía enfrentó multas y demandas por parte de los reguladores y los consumidores afectados.

Respuesta: En 2018, Marriott informó que una brecha de seguridad expuso datos de 500 millones de huéspedes, incluyendo pasaportes y números de tarjetas de crédito. La multa impuesta por la UE bajo el GDPR fue de £18.4 millones, y la empresa enfrentó múltiples demandas. Los afectados tuvieron que lidiar con posibles fraudes, mientras que Marriott sufrió un fuerte daño reputacional. Este incidente resaltó la necesidad de proteger bases de datos en la industria hotelera.

Yahoo: En 2013, Yahoo sufrió una de las mayores brechas de datos de la historia, en la que se vio comprometida la información de más de mil millones de usuarios. La compañía fue adquirida por Verizon por un precio significativamente inferior al inicialmente acordado debido a esta brecha.

Respuesta: Yahoo experimentó en 2013 una violación masiva que comprometió datos de **mil millones de usuarios**, aunque se reveló años después. Esto redujo el valor de la compañía, llevando a Verizon a comprarla por **$350 millones menos** de lo pactado inicialmente. La FTC multó a Yahoo con **$35 millones**, pero el mayor perjuicio fue para los usuarios, cuyas contraseñas e información personal quedaron expuestas, aumentando riesgos de ciberataques. Este caso subraya la importancia de la transparencia y la respuesta inmediata ante brechas de seguridad.