Actividad grupal: Sin seguridad no hay privacidad

Objetivos

* Entender que los tratamientos de datos pueden poner en riesgo a las personas y que, junto con otras medidas técnicas y organizativas establecidas en el RGPD, la seguridad de los datos es fundamental a la hora de abordar estos riesgos.
* Aprender a aplicar criterios clave para dimensionar la severidad de una brecha de seguridad en el marco de la protección de datos.

Pautas de elaboración

En esta actividad pondrás en práctica tus conocimientos del RGPD en relación con una de las novedades que este incorporaba: violaciones de seguridad y obligación de su notificación a las autoridades de control e incluso a los afectados. Además, podrás verificar los potenciales efectos negativos que puede tener un incidente de seguridad sobre las personas cuando se tratan datos de carácter personal.

La actividad contempla el análisis de un caso real publicado en los medios de comunicación, sobre el que investigarás para entender el alcance del incidente y sus implicaciones en las personas afectadas. También aplicarás los conocimientos sobre notificaciones a la autoridad de control en el caso de violaciones de seguridad.

El caso sobre el que trabajarás parte de la siguiente noticia:

Ingram, M. (19 de agosto de 2015). Will the media name Ashley Madison users? It may not matter — we’re all the media now. *Fortune.*

<https://fortune.com/2015/08/19/ashley-madison-media/>

En 2015 saltó a los medios una noticia que no dejó indiferente al mundo, no solo por la empresa que se había visto sometida a un ataque, sino también por el impacto que tuvo sobre los afectados. Dada la repercusión que la noticia alcanzó, parece interesante que profundicemos en el caso desde la perspectiva del RGPD.

Para ello se requiere lo siguiente:

1. Investigar en la red, a través de contenidos en otros medios de comunicación que profundicen en la noticia, para elaborar un resumen sobre lo que sucedió, cómo se materializó el ataque, por qué tuvo éxito y cuáles fueron las consecuencias sobre los afectados.
2. Justificar si, atendiendo a lo sucedido, estamos ante una violación de seguridad tal y como se define en el RGPD.
3. Evaluar si, tal y como establece el RGPD, en este caso habría sido obligatoria la notificación del incidente a la autoridad de control correspondiente ([Information Commissioner’s Office](https://ico.org.uk/)) y a los afectados. En tal caso, ¿piensas que los afectados habrían podido protegerse del impacto negativo de la divulgación de la información?

Para la resolución del caso se puede recurrir a:

* El Reglamento General de Protección de Datos.
* La guía para la gestión y notificación de brechas de seguridad de la AEPD (por ejemplo, su anexo III).

Accede a la guía desde la siguiente dirección web: <https://www.aepd.es/media/guias/guia-brechas-seguridad.pdf>

Extensión y formato

La concreción es una virtud, por lo que consideramos un espacio razonable para la resolución de la actividad de un máximo de 4 páginas; fuente Georgia 11 e interlineado 1,5.

Rúbrica

|  |  |  |  |
| --- | --- | --- | --- |
| Sin seguridad no hay privacidad | Descripción | Puntuación máxima  (puntos) | Peso  % |
| Criterio 1 | Conocimientos de conceptos y principios de la normativa. | 3,4 | 34 % |
| Criterio 2 | Aplicación práctica de los conocimientos. | 3,3 | 33 % |
| Criterio 3 | Solvencia de argumentos, concreción y claridad de exposición. | 3,3 | 33 % |
|  |  | **10** | **100 %** |

Un paquete de 9.7 gigabytes de datos fueron publicados en la web oscura utilizando una dirección de Onion accesible solo a través del navegador Tor. Los archivos incluyen detalles de cuentas e inicios de sesión de unos 32 millones de usuarios del sitio de redes sociales, siete años de tarjetas de crédito y otros detalles de transacciones de pago también forman parte de la base de datos del portal de citas.

El portal ofrece la posibilidad de agendar citas para parejas infieles y citas matrimoniales, su logo describe la frase “Tenga una aventura hoy en Ashley Madison”, lo cual hace atractivo a miles de esposos y esposas infieles alrededor del mundo.

Algunos de los datos sensibles como las contraseñas publicadas en el lote de datos fueron codificadas mediante el algoritmo “*bycypt*” de PHP el cual a pesar de ser una de las formas más seguras para almacenar contraseñas, no es un gran desafío para los hackers informáticos lograr descifrar los hash o códigos cifrados mediante el algoritmo, lo cual pone en peligro información privada asociada a las cuentas de usuario de la plataforma web o aplicación. Cabe mencionar que otros portales en algunas ocasiones nunca se molestan o implementan algún control de seguridad de cifrado de información sensible o confidencial como las contraseñas.

<https://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/>