Datos del estudiante

**Nombre y apellidos**

**Fecha de entrega**

Actividad grupal: Sin seguridad no hay privacidad

Objetivos de la actividad

* Comprender cómo los tratamientos de datos personales pueden representar riesgos para la privacidad de las personas y la importancia de garantizar la seguridad de los datos en el marco del RGPD.
* Desarrollar habilidades para analizar y evaluar casos reales de violaciones de seguridad y determinar si es necesario notificar a las autoridades y a los afectados según la normativa vigente.
* Aprender a identificar los principales riesgos asociados al manejo de datos personales y proponer medidas preventivas para minimizar posibles violaciones de seguridad.
* Aplicar criterios clave para evaluar la severidad de una brecha de seguridad en el contexto de la protección de datos y sus posibles efectos negativos sobre los individuos.

Pautas de elaboración

Esta actividad grupal está diseñada para que los estudiantes apliquen de manera práctica sus conocimientos sobre la seguridad y privacidad de los datos personales, conforme al Reglamento General de Protección de Datos (RGPD). A través de la investigación y el análisis de casos reales, los participantes podrán explorar las implicaciones legales y éticas que tiene la protección de los datos en la sociedad digital actual.

El propósito de esta actividad es que los estudiantes comprendan cómo las violaciones de seguridad pueden comprometer la privacidad de las personas y cuáles son las medidas que pueden tomarse para prevenir y mitigar dichos riesgos. Para su desarrollo, se requiere que los participantes seleccionen datos y ejemplos reales que consideren pertinentes y que investiguen en fuentes disponibles en la web. Aunque tendrán libertad para elegir las fuentes de información, es esencial que los datos utilizados estén alineados con los objetivos y requerimientos de la actividad.

Este enfoque les permitirá no solo entender el marco teórico del RGPD, sino también evaluar cómo se aplica en situaciones reales y cómo las empresas y organizaciones deben responder ante incidentes de seguridad. Los estudiantes podrán analizar las implicaciones de estas violaciones en la privacidad de los usuarios y proponer soluciones basadas en buenas prácticas de seguridad de datos.

El trabajo colaborativo será clave para intercambiar perspectivas y reforzar la comprensión de los desafíos y responsabilidades inherentes a la protección de datos en un mundo cada vez más interconectado.

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.

Parte I

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:

Welivesecurity. (2015, Agosto 31). *Caso Ashley Madison: la cronología de los hechos*. <https://www.welivesecurity.com/la-es/2015/08/31/caso-ashley-madison-cronologia/>

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:

* 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.
* Justificar si, atendiendo a lo sucedido, estamos ante una violación de seguridad, tal y como se define en el RGPD.
* Evaluar si, tal y como establece el RGPD, en este caso habría sido obligatoria la notificación del incidente a la autoridad de control correspondiente y a los afectados. En tal caso, ¿piensas que los afectados habrían podido protegerse del impacto negativo de la divulgación de la información?

Parte II

Desarrollar una Guía de buenas prácticas de privacidad para una aplicación móvil de turismo.

Contexto

En el ámbito del turismo, las aplicaciones móviles juegan un papel crucial en la mejora de la experiencia del viajero, ofreciendo desde recomendaciones personalizadas hasta reservas instantáneas. Sin embargo, estas aplicaciones manejan una gran cantidad de datos personales, lo que plantea importantes desafíos de privacidad y protección de datos.

Objetivo

Crear una guía de buenas prácticas de privacidad para el desarrollo y manejo de una aplicación móvil de turismo, asegurando que se respeten y protejan los datos personales de los usuarios conforme a la legislación vigente (como el GDPR en la Unión Europea).

Pasos a seguir:

Paso 1: Investigación y Análisis.

* Investigar sobre las leyes de protección de datos aplicables (ejemplo: GDPR, CCPA).
* Analizar los tipos de datos personales que suelen recopilar las aplicaciones de turismo.

Paso 2: Identificación de Riesgos. Identificar los riesgos potenciales para la privacidad asociados con el tratamiento de datos en aplicaciones de turismo.

Paso 3: Desarrollo de la Guía.

* Transparencia: instrucciones sobre cómo proporcionar información clara y accesible a los usuarios sobre qué datos se recopilan, con qué fin y cómo pueden gestionar su privacidad.
* Minimización de datos: principios para asegurar que solo se recolecten los datos estrictamente necesarios para la prestación del servicio.
* Consentimiento informado: directrices para obtener el consentimiento explícito de los usuarios de manera clara y sin ambigüedades.
* Seguridad de datos: medidas recomendadas para garantizar la seguridad de los datos recopilados, incluyendo cifrado, acceso seguro y protocolos de respuesta ante brechas de seguridad.
* Derechos de los usuarios: procedimientos para permitir que los usuarios ejerzan sus derechos, como el acceso a sus datos, rectificación, eliminación y portabilidad.
* Evaluación de Impacto sobre la Protección de Datos (EIPD): guía para realizar evaluaciones de impacto cuando se introduzcan nuevas tecnologías o se realicen cambios significativos en la aplicación.

Paso 4: Recomendaciones Prácticas.

* Incluir ejemplos prácticos de cómo implementar estas buenas prácticas en el ciclo de vida del desarrollo de la aplicación.
* Recomendaciones sobre herramientas y tecnologías que pueden ayudar a cumplir con los principios de protección de datos.

Para la resolución de ambas partes 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).

AEPD. (2021). *Guía para la notificación de brechas de datos personales*. <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 8 páginas (una página de portada, una página de índice, cuatro páginas Parte I y dos páginas Parte II); fuente Georgia 11 e interlineado 1,5.

Al finalizar la actividad grupal, **todos los miembros del equipo harán la entrega del mismo informe final** a través del apartado «Envío de actividades» del aula virtual.

Se debe indicar en el informe y en el script el nombre de todos los componentes del equipo. En el informe, además, se adjuntará cumplimentada la siguiente tabla de valoración individual.

Tabla

Descripción generada automáticamente

Figura 1. Fuente: elaboración propia.