TALENTO TECH

TIC

REGIÓN 3

CAUCA – NARIÑO

LECCIÓN 2 – UNIDAD 2

Universidad Tecnológica de Pereira

faceIT

Lección 2: Normas internacionales de protección de datos

Existen varios marcos normativos que rigen la seguridad y la protección en los datos. Si bien son normas internacionales, sus usos se extienden alrededor del mundo.

GDPR o Reglamento general de protección de datos

El GDPR es una ley europea que entró en vigor en 2018 y establece un marco común para la protección de datos personales de los ciudadanos de la Unión Europea. Su objetivo principal es garantizar que los datos personales sean tratados de manera lícita, leal y transparente, y que se respeten los derechos de las personas.
En el GDPR se garantiza un marco común a toda la unión europea para el manejo de los datos. Para la norma, no importa el país en el cual se cree una aplicación sino el origen de los usuarios que proveen datos a las aplicaciones.

Cualquier aplicación que tenga usuarios de la unión europea debe cumplir con la normatividad. De esta forma se garantiza que los datos de los ciudadanos europeos estén seguros. En caso de brechas en la información la norma GDPR considera multas millonarias que incentiva a las empresas a dar cumplimiento de la norma.

Los pilares de la norma GDPR son:

Consentimiento: Las empresas deben obtener tu consentimiento explícito antes de tratar tus datos personales. Este consentimiento debe ser libre, específico, informado y unívoco.

Derechos de los interesados: Tienes derecho a acceder a tus datos, rectificarlos, suprimirlos, oponerte a su tratamiento, limitar su tratamiento y a la portabilidad de los datos.

Principios del tratamiento: Los datos deben ser tratados de manera lícita, leal y transparente, y deben ser adecuados, relevantes y limitados a lo necesario en relación con los fines para los que son tratados.

Seguridad de los datos: Las empresas deben implementar medidas técnicas y organizativas apropiadas para garantizar la seguridad de tus datos y protegerlos contra el tratamiento no autorizado o ilícito.

Notificación de brechas de datos: En caso de una brecha de seguridad, las empresas deben notificarla a la autoridad de control y, en algunos casos, a los interesados, sin demora indebida.

Responsable del tratamiento: Toda empresa que trate datos personales debe designar a un responsable del tratamiento, que será el encargado de garantizar el cumplimiento del RGPD.

Alcance global: Aunque el RGPD se aplica principalmente a las empresas establecidas en la UE, también afecta a las empresas de fuera de la UE que ofrecen bienes o servicios a ciudadanos de la UE.

Tipos de datos: El RGPD cubre una amplia gama de datos personales, desde nombres, direcciones, historiales de navegación y cualquier dato que sirva para caracterizar individuos.

Transferencias internacionales de datos: Si una empresa transfiere datos personales fuera de la UE, debe garantizar un nivel adecuado de protección de los datos.
Legitimación del tratamiento: Las empresas solo pueden tratar datos personales si existe una base legal válida, como el consentimiento, el cumplimiento de una obligación legal o los intereses legítimos del responsable. La norma no permite la recopilación de datos innecesarios con el fin de limitar los riesgos.

Gracias al GDPR es que los portales han empezado a avisar a sus usuarios sobre los datos que estos recopilan. La norma le permite al usuario saber qué información recopilan las empresas y permite que un usuario pueda pedir copias de los datos recopilados.
Los usuarios también tienen derecho a que la información errónea sea corregida y a crear solicitudes de corrección de información que deben ser atendidas.
Los usuarios tienen derecho a que la información sea eliminada por medio de una solicitud.
Los usuarios tienen derecho a oponerse al tratamiento de los datos con el fin de que las empresas no se aprovechen de los datos y los vendan o los usen con otros fines diferentes a los que el usuario aceptó al suministrar su información personal.