Nadia Arellano G.
Ingeniera en Informática

Actividad – Sesión 3 – Análisis de Casos de Cumplimiento Normativo en la Nube

Escenario 1: Una empresa europea de e-commerce maneja información sensible de sus clientes en un servicio de almacenamiento en la nube. Por un error, algunos datos no se cifran. ¿Qué normativa aplica aquí? Explica qué consecuencias podría enfrentar la empresa.

(R). La normativa que aplica es el GDPR (Reglamento General de Protección de Datos), porque corresponde a una empresa europea que maneja información sensible de sus clientes. Uno de sus principios es la confidencialidad de los datos, por lo que se debe aplicar medidas de seguridad como el cifrado para evitar accesos no autorizados. Las consecuencias que puede enfrentar la empresa serian sanciones que incluyen multas de hasta el 4% de la facturación anual global o 20 millones de euros, el valor que sea mayor.

Escenario 2: Una clínica en EE. UU. utiliza servicios en la nube para almacenar información de pacientes sin implementar un acuerdo con el proveedor de la nube. ¿Qué normativa debería seguir para cumplir con las regulaciones? Fundamenta tu respuesta.

(R). La normativa que debería seguir esta clínica en EE. UU. es HIPAA (Health Insurance Portability and Accountability Act), ya que regula el manejo y la protección de la información médica personal (PHI) en ese país. Para cumplir con HIPAA, es obligatorio establecer un acuerdo de socio comercial (Business Associate Agreement - BAA) con cualquier proveedor de servicios en la nube que tenga acceso a datos de pacientes. Si la clínica no implementa este acuerdo estaría incumplimiento la normativa, lo que puede derivar en multas federales e investigaciones.

Escenario 3: Un startup que procesa pagos en línea no implementa controles de acceso seguros para los datos de tarjetas de crédito. ¿Qué estándar es el más relevante y qué requisitos específicos podría estar incumpliendo?

(R). El estándar más relevante para aplicar en este caso es el PCI-DSS (Payment Card Industry Data Security Standard), ya que regula la protección de los datos de tarjetas de crédito y débito para cualquier organización que los procese, almacene o transmita. Esta empresa emergente podría estar incumpliendo varios requisitos específicos principalmente la confidencialidad al no proteger los datos correctamente. Esto a través de controles de accesos no limitados y configuraciones no seguras ya que no aplica una autenticación robusta.