OMAR BECERRA

Msc Ciberseguridad
Services Director

CASOS DE INTERÉS

“Samsung Electronics Co. prohibió a su personal el uso de populares herramientas de inteligencia artificial generativa como ChatGPT después de descubrir que empleados subieron un código confidencial a la plataforma, lo que supuso un revés para la difusión de dicha tecnología en el lugar de trabajo.”

Fuente: El Tiempo

“La empresa china de IA DeepSeek ha arreglado una base de datos de fondo expuesta que tiraba información delicada, incluidas los historiales de chat de usuarios y las claves del API, en Internet abierto. La base de datos DeepSeek no estaba protegida con una contraseña, cosa que permitía a cualquier persona en Internet acceder además de un millón de registros sin cifrar.”

Fuente: El Nacional

En Colombia, muchas empresas aún no han implementado normativas internas para regular el uso de herramientas como ChatGPT, lo que aumenta el riesgo de fugas de datos. Solo el 27% de las empresas que han adoptado estas herramientas aseguran tener políticas claras y cumplirlas.

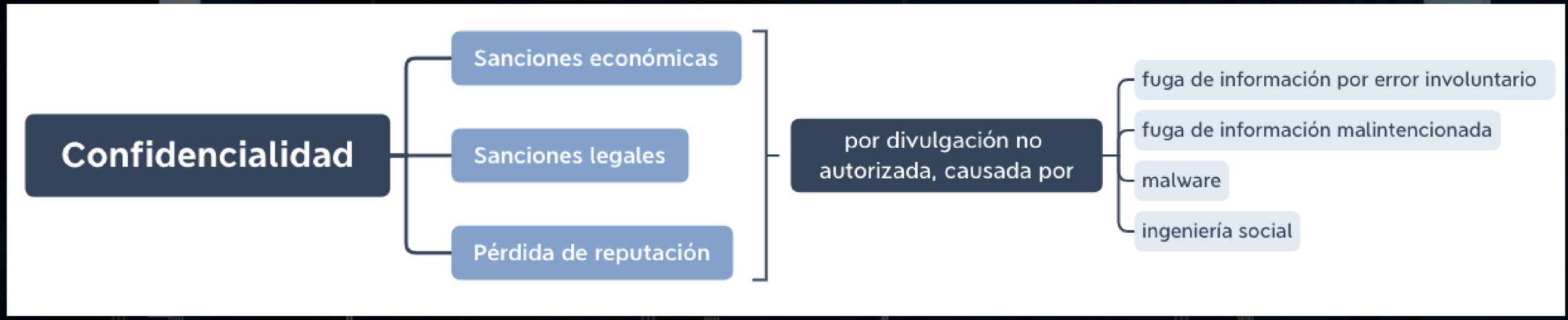
Fuente: Deloitte

30 AÑOS

Globaltek

Retos - IA generativa

Redacción de un riesgo



Afectación legal debido a compromiso de datos personales por uso indebido de IA generativa causada por ausencia de controles de prevención de fuga de datos

Afectación: Legal (multas y sanciones por incumplimiento de normativas como la Ley 1581 de 2012, GDPR entre otros).

Amenaza: Fuga de información por uso indebido de IA generativa.

Vulnerabilidad: Ausencia de controles de prevención de fuga de datos.

Controles: Gobierno, sensibilización, y controles de fuga de información, DSPM (Data Securtiy Posture Management).

30 AÑOS

Globaltek

Afectación estratégica debido a fuga de información privilegiada por uso indebido de plataformas de IA generativa causada por ausencia de políticas de uso aceptable.

Afectación: Estratégica (pérdida de información sensible y ventaja competitiva).

Amenaza: Fuga de información.

Vulnerabilidad: Ausencia de políticas de uso aceptable y concientización sobre el uso de IA generativa.

Controles: Gobierno y sensibilización, protección de fuga de información (DSPM, DLP), web security.

30 AÑOS

Globaltek

DEMO

30 AÑOS

Globaltek

Efecto favorable en la estrategia debido a la adopción de IA generativa, aprovechando su potencial para mejorar la productividad y la creatividad en la organización

Afectación: Afectación estratégica positiva

Oportunidad: adopción de IA generativa.

Vulnerabilidad: mejorar la productividad y la creatividad.

30 AÑOS

Globaltek

¿ Implementa su empresa políticas y controles específicos para prevenir la fuga de información a través del uso de inteligencia artificial (IA) ?

30 AÑOS

Globaltek

¡REGÍSTRATE Y PARTICIPA EN NUESTRA RIFA!

ARMANDO CARVAJAL

Msc Ciberseguridad
Innovation Director

¿Su empresa ha pensado usar o usa la IA Generativa para extraer datos de documentos no estructurados?

30 AÑOS

Globaltek

¡REGÍSTRATE Y PARTICIPA EN NUESTRA RIFA!

LIKE COMENTA COMPARTE

Globaltek

Página Web
www.globaltek.co

LinkedIn
Globaltek

Instagram
@globaltek.co

Youtube
Globaltek Security