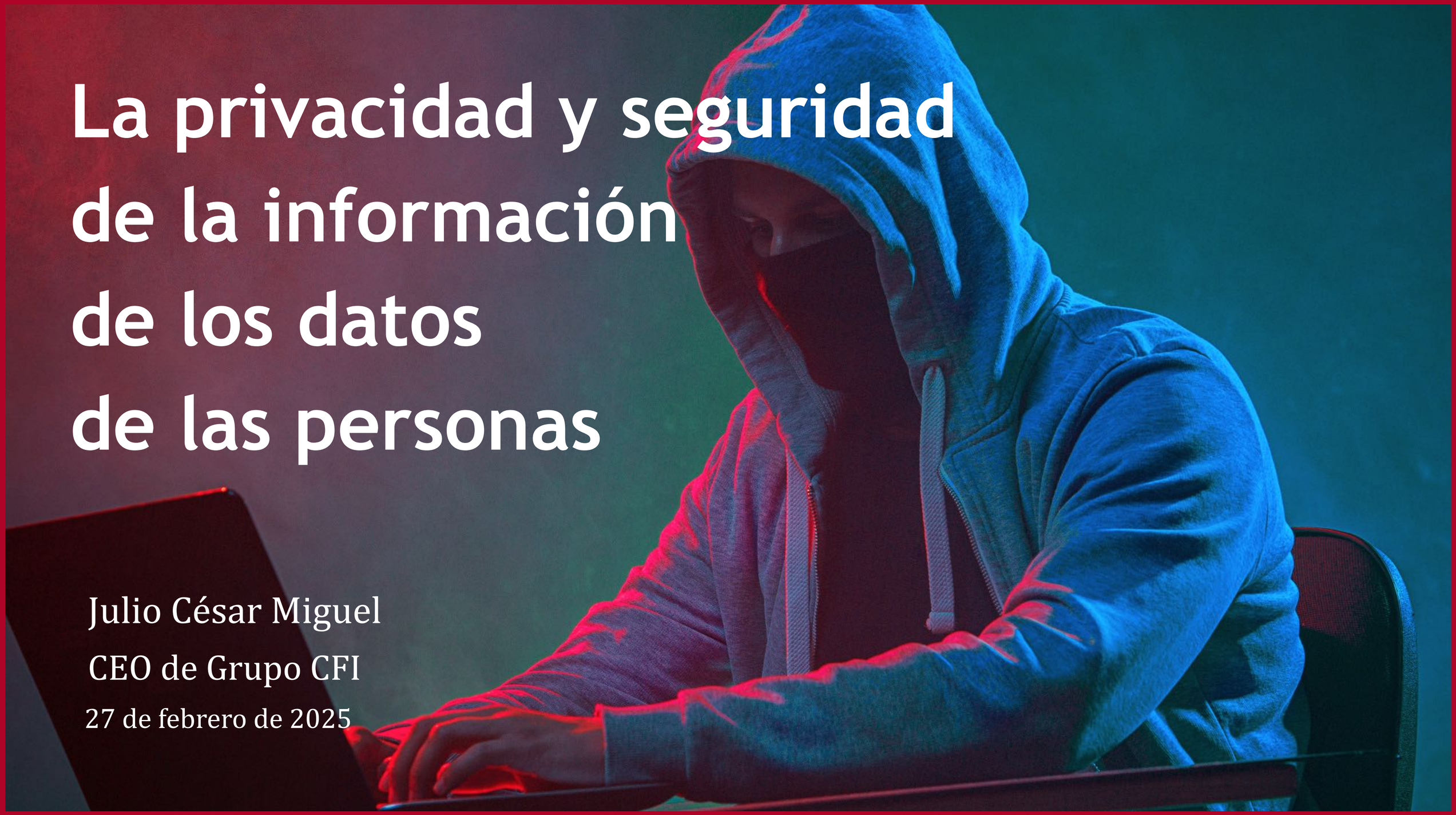
La privacidad y seguridad de la información de los datos de las personas



Julio César Miguel
CEO de Grupo CFI
27 de febrero de 2025

Importancia de la seguridad en sociosanitario

- **Sensibilidad de los datos personales y de salud**
- **Impacto de las filtraciones: daño reputacional, a los pacientes, legal y económico**
- **Es uno de los sectores más ciberatacados**

El sector sanitario, principal víctima de ciberataques en España en 2024

Los ataques de bloqueo de sistemas fueron los más habituales en España y Portugal en la primera mitad del año

Te puede interesar

Los TCAE van a la huelga en Cataluña por la reclasificación y el sueldo

Las aseguradoras, ante el nuevo plazo

Características del sector en ciberseguridad

- **Alta criticidad de los servicios, principalmente los asistenciales**
- **Alto valor de los datos que gestionan (un historial tiene un precio de entre 30 y 1.000€)**
- **Heterogeneidad e hiperconectividad de sistemas y dispositivos**
- **Aumento del volumen y flujos de datos entre sistemas**

Principales riesgos de ciberseguridad

- Ciberataques (ransomware, phishing, acceso no autorizado)
- Errores humanos (envío de información por error, contraseñas débiles)
- Fugas de información interna (mal uso de los datos por empleados)
- Riesgos en la nube y proveedores externos

Normativas y regulaciones

Principales regulaciones en el ámbito de la seguridad de la información de los pacientes y usuarios:

- **RGPD**
- **LOPDGDD**
- **ENS**
- **NIS2**

Buenas prácticas en ciberseguridad

Medidas esenciales:

- **Control de accesos (2FA, permisos mínimos)**
- **Gestión de vulnerabilidades**
- **Cifrado de datos sensibles**
- **Auditorías y monitorización**
- **Formacion y concienciación**

Estrategia para gestionar la ciberseguridad

Estrategia 360º:

- **Prevención: políticas de seguridad, formación y concienciación**
- **Proteccion: cifrado, antimalware, firewalls, vulnerabilidades, etc.**
- **Detección: monitorización y detección de anomalías**
- **Respuesta: plan continuidad**

05/03/2023

Ciberataque ransomware paraliza actividad del Hospital Clínic de Barcelona

Fecha de publicación 13/03/2023
05/03/2023

El Hospital Clínic de Barcelona ha sido víctima de un ataque informático de tipo *ransomware*, tal y como notificó la institución sanitaria a la Agencia de Ciberseguridad de Cataluña. El incidente afectó al normal funcionamiento del servicio de urgencias, laboratorio y farmacia, obligando a realizar los trámites informáticos a mano.

Los responsables del ciberataque han solicitado un rescate de 4,5 millones de dólares por la información cifrada, que constituye cerca de 4,5 TB, pero el Govern ha declarado en uno de sus comunicados que no realizará dicho pago.

El hospital ha recuperado gradualmente su actividad, restableciendo hasta el momento el 40% de la actividad quirúrgica y el 70% de las consultas externas.

04/07/2023

CATALUÑA • 'Dark web'

Nueva filtración de los datos robados en el ciberataque al Hospital Clínic de Barcelona por los piratas informáticos RansomHouse

GERARD MELGAR
Barcelona

Actualizado Martes, 4 julio 2023 - **23:05**

Comentar

Es la cuarta exposición de la información sustraída en marzo por el grupo de ciberdelincuentes

07/11/2024

CIBERATAQUES >

La Generalitat concluye que el Clínic no tenía medidas de seguridad “mínimas” para contener el ciberataque de 2023

Los delincuentes filtraron 4,5 terabytes de información identificativa y la Autoridad Catalana de Protección de Datos considera que el centro barcelonés no realizó un “análisis de riesgo”

¿Por dónde empiezo?

Evaluar los riesgos y su tratamiento

- **Identificar los activos primarios de información**
- **Identificar activos de soporte, amenazas y vulnerabilidades**
- **Evaluar los riesgos (ISO 27005 u otras)**

		PROBABILIDAD				
		Muy baja	**Baja**	**Media**	**Alta**	**Muy alta**
IMPACTO	**Muy bajo**	Muy bajo	Bajo	Bajo	Medio	Medio
	Bajo	Bajo	Bajo	Medio	Medio	Alto
	Medio	Bajo	Medio	Medio	Alto	Alto
	Alto	Medio	Medio	Alto	Alto	Muy alto
	Muy alto	Medio	Alto	Alto	Muy alto	Muy alto

Riesgo = Impacto x Probabilidad

Probabilidad = F. Amenaza x G. Vulnerabilidad

Plan de seguridad de la información

Formular un plan de tratamiento de los riesgos de seguridad de la información

Debe incluir medidas organizativas, técnicas y físicas

Resultado: Plan de seguridad de la información

Conclusiones

Conclusiones

- **Gestionar la ciberseguridad es clave para proteger la información de los pacientes (políticas, medidas técnicas, buenas prácticas, etc.)**
- **La formacion y concienciación del personal es imprescindible**
- **Cumplir con las regulaciones evita sanciones y mejora la confianza**

¡MUCHAS GRACIAS!

Contacto:

- **Julio César Miguel**
- **Email: jcmiguel@grupocfi.es**
- **Twitter: @juliocesarlopd**
- **LinkedIn: es.linkedin.com/in/juliocesarlopd**

¿Preguntas?