Hardening en base de datos documentales

Grupo 23
Agustín Sánchez
Lucía Rotela

Contenido

- Introducción y Motivación
- Vulnerabilidades
- Caso de estudio
- Recomendaciones
- Conclusiones y Trabajo futuro

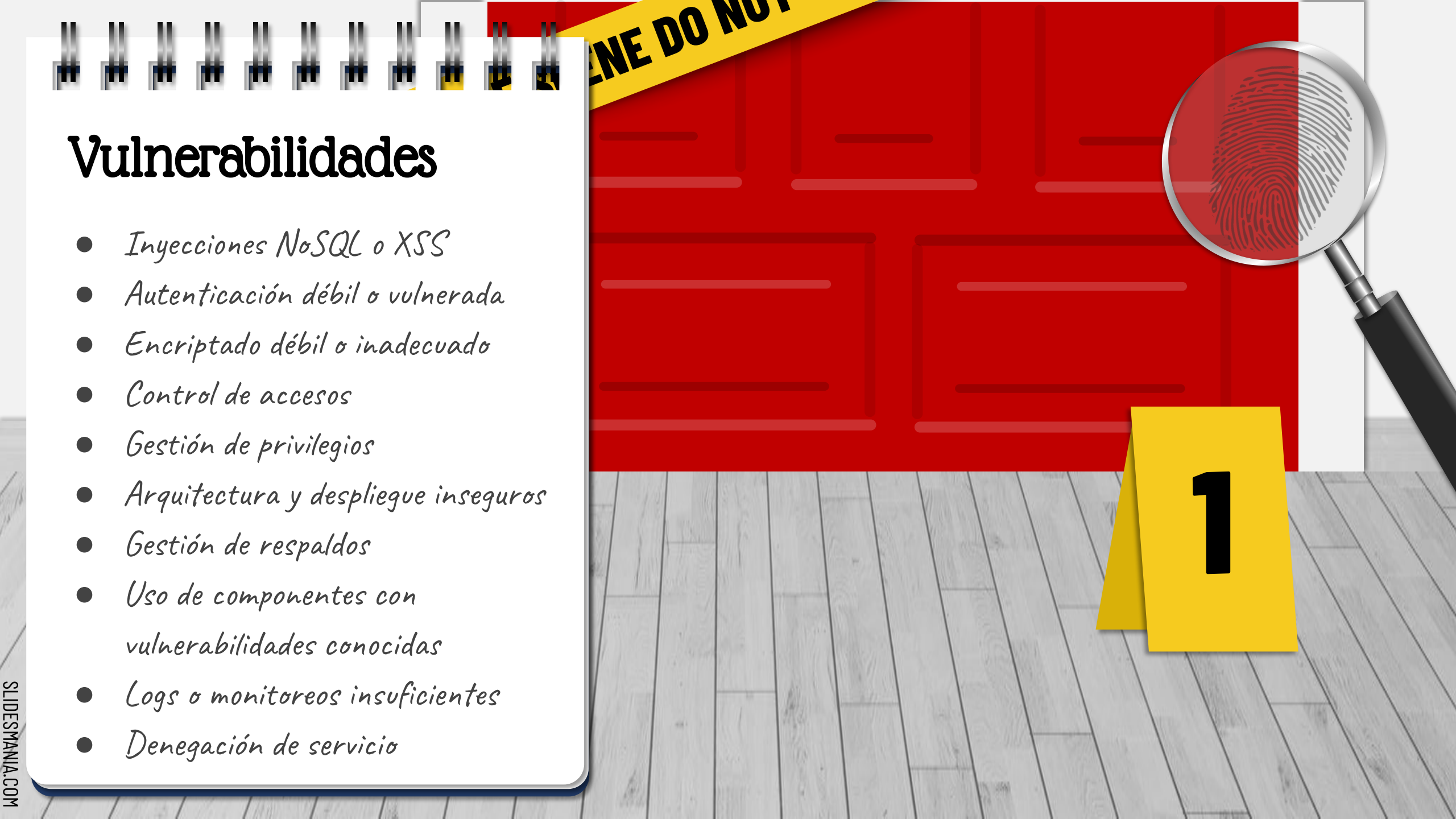
Introducción y Motivación

- Eficiencia ✓
- Escalabilidad ✓
- Seguridad ✗

- Ataque Meow (2020)
- 29000 bases sin autenticación (2021)
- Medicare (2019)

Vulnerabilidades

- Inyecciones NoSQL o XSS
- Autenticación débil o vulnerada
- Encriptado débil o inadecuado
- Control de accesos
- Gestión de privilegios
- Arquitectura y despliegue inseguros
- Gestión de respaldos
- Uso de componentes con vulnerabilidades conocidas
- Logs o monitoreos insuficientes
- Denegación de servicio



Caso de Estudio

Medicare, seguros de salud que mejor se adapte

Expuso **5 millones** de registros

Contienen **información personal**

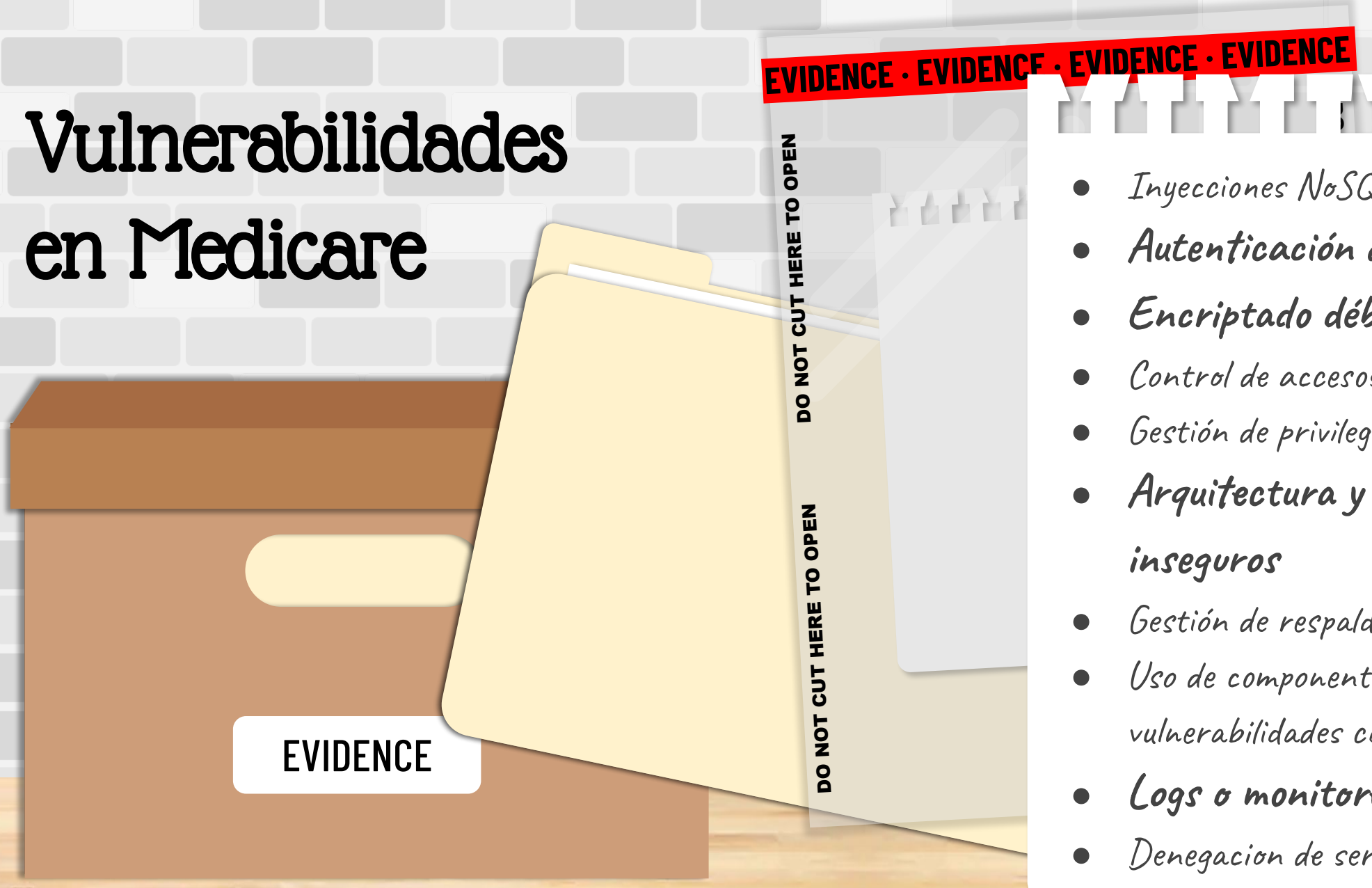
Nombre, dirección, número de celular, fecha de nacimiento, género, direccion IP

Acceso abierto a todo **público**!

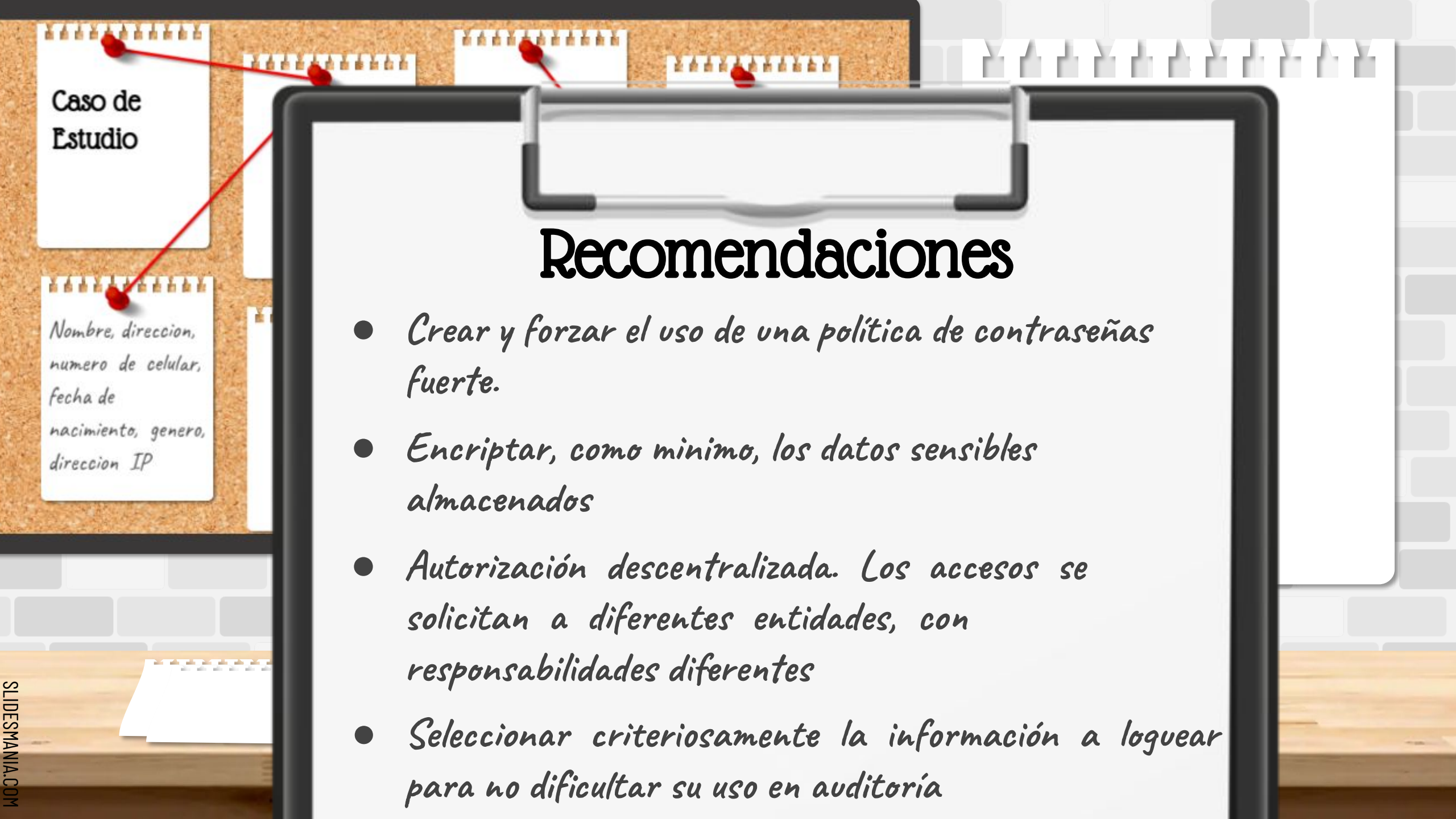
No se sabe quiénes han accedido

Víctimas de fraude, spam y phishing dirigido

Vulnerabilidades en Medicare



- Inyecciones NoSQL o XSS
- **Autenticación débil o vulnerada**
- **Encriptado débil o inadecuado**
- Control de accesos
- Gestión de privilegios
- **Arquitectura y despliegue inseguros**
- Gestión de respaldos
- Uso de componentes con vulnerabilidades conocidas
- **Logs o monitoreos insuficientes**
- Denegacion de servicio



Recomendaciones

- Crear y forzar el uso de una política de contraseñas fuerte.
- Encriptar, como minimo, los datos sensibles almacenados
- Autorización descentralizada. Los accesos se solicitan a diferentes entidades, con responsabilidades diferentes
- Seleccionar criteriosamente la información a loguear para no dificultar su uso en auditoría

Conclusiones y Trabajo futuro

- Prevenir falencias graves de seguridad que, por desconocimiento, terminan siendo la puerta de entrada de usuarios malintencionados

---

- Obtener la aprobación de la sociedad científica
- Desarrollo de un toolkit que incorpore herramientas con capacidad para auditar las recomendaciones

Gracias, Preguntas?