

Práctica: Auditoría de Seguridad y Cumplimiento Normativo

Contexto de la práctica

- Eres del equipo de ciberseguridad de "Calasanz TechHealth Solutions", una startup española que ha desarrollado una aplicación web para gestión de citas médicas online.
- El equipo de desarrollo os ha proporcionado documentación del sistema actual para que realicéis una auditoría de cumplimiento normativo:
- **Funcionalidades del sistema:**
 - Registro de pacientes con formulario web
 - Gestión de citas médicas online
 - Almacenamiento de historial médico básico
 - Pasarela de pago para consultas privadas
 - Panel de administración para clínicas
- **Arquitectura técnica actual:**
 - Frontend: Vue.js
 - Backend: Spring Boot
 - Base de datos: MySQL (sin cifrado)
 - Hosting: Servidor dedicado en España
 - Conexión: HTTP (no HTTPS)
 - Backups: Manuales, cada 15 días
 - Sin logs de auditoría implementados
 - **Autenticación:**
 - Contraseñas guardadas en MD5 (sin salt)
 - No hay doble factor de autenticación
 - Las contraseñas se pueden recuperar por email (se envía la contraseña original)
 - No hay límite de intentos de login
- **Datos que Recoge el Formulario de Registro.** Al registrarse, el paciente debe introducir:
 - Nombre completo*
 - DNI*
 - Fecha de nacimiento*
 - Género*
 - Dirección postal completa*
 - Teléfono móvil*
 - Email*
 - Teléfono fijo (opcional)
 - Profesión (opcional)
 - Nivel de estudios (opcional)
 - Número de tarjeta sanitaria*
 - Historial de enfermedades previas*
 - Medicación actual

- Alergias conocidas
- Nombre y teléfono de contacto de emergencia*
- Compañía de seguros médicos (opcional)
- Número de tarjeta de crédito* (se guarda completo en BD)
- Preferencias de idioma
- Preferencias de notificaciones (email/SMS)
- **Política de Privacidad Actual.** El sistema muestra en letra pequeña al final del formulario:

"Al registrarte aceptas nuestra política de privacidad y el tratamiento de tus datos. Usaremos tu información para gestionar tus citas y enviarte ofertas comerciales de nuestros partners. Tus datos se conservarán indefinidamente."

- La casilla viene premarcada por defecto.
- **Roles y permisos implementados:**
 - Paciente: Ver sus propias citas, Modificar cualquier campo de su perfil, Cancelar citas
 - Médico: Ver datos completos de TODOS los pacientes de la BD, Modificar historiales médicos, Acceder a datos de pago
 - Admin Clínica: Acceso total a la base de datos, Gestión de usuarios, Exportar datos a Excel sin restricciones
 - Desarrollador: Acceso SSH a producción con usuario root, Acceso directo a MySQL de producción, Sin restricción horaria
- **Incidentes recientes:**
 - Un médico accedió desde una red WiFi pública sin VPN
 - Un desarrollador borró accidentalmente 200 registros en producción (no se pudieron recuperar)
 - Se detectó que un paciente podía ver citas de otros pacientes cambiando el parámetro `id=` en la URL ?
 - El servidor estuvo caído 4 horas por saturación (sin plan de contingencia)
 - Un email de phishing comprometió las credenciales de un administrador
 - No se ha notificado ningún incidente a la AEPD (Agencia Española de Protección de Datos)

Parte 1 - Categorización y Clasificación de Datos

Parte 1.1. Inventario de Datos

- Identifica y clasifica todos los tipos de datos que maneja la aplicación según su sensibilidad (Públicos, Internos, Confidenciales, Críticos).
- Debes crear una tabla con al menos 15 tipos de datos diferentes, indicando:
 - Tipo de dato
 - Nivel de clasificación
- Por ejemplo:

Tipo de dato	Nivel de clasificación	Justificación de la clasificación	¿Es necesario recogerlo?
Grupo Sanguíneo	Confidencial	Es un dato sensible del paciente, y puede causar daños significantes si se compromete, pero no llega a ser tan crítico como otros datos médicos	Si, para que quede reflejado en el historial del paciente

Parte 1.2. Categorización ENS

- Determina la categoría ENS del sistema evaluando el impacto en las tres dimensiones (Disponibilidad, Integridad, Confidencialidad).
- Tienes que indicar la categoría asignada a cada dimensión CIA (BAJO/MEDIO/ALTO), su justificación y la categoría final del sistema.

Parte 2: Análisis de Cumplimiento RGPD

- Analiza en una tabla el cumplimiento de los 6 principios del RGPD vistos en clase. Por ejemplo:

Principio RGPD	¿Cumple?	Evidencia/Problema	Acción correctiva
Minimización de daños	NO	Se pide profesión y nivel de estudios sin justificación	Eliminar campos innecesarios

- Analiza la política de privacidad actual. ¿Crees que han incumplido el RGPD? Si es así, ¿por qué? ¿Que incumplimientos detectas?
- El RGPD otorgaba una serie de derechos a los usuarios. ¿Como los implementarías en esta aplicación? Por ejemplo, para el derecho a la limitación del tratamiento el sistema podría tener un botón que permitiera al usuario desactivar su cuenta del sistema, los datos quedaría pero no se estarían usando hasta que quiera volver a activar su cuenta.

Parte 3: Análisis de vulnerabilidades

Parte 3.1. Análisis de Incidentes Reales

- Analiza cada uno de los 5 incidentes descritos en la documentación completando esta tabla:

Incidente	Principio CIA Vulnerado	Causa	Impacto	Medida necesaria
Médico en WIFI publica	Confidencialidad	Falta de VPN obligatoria	Media	Implementar VPN corporativa + política de uso

Parte 3.2. Evaluación de seguridad técnica

- Identificad todos los problemas de seguridad en la arquitectura técnica actual, con la siguiente tabla:

Problema	Riesgo CIA	Prioridad	Solución técnica
Un paciente puede ver las citas médicas de otro paciente cambiando el id de la URL	Confidencialidad	ALTA	Implementar medidas de seguridad en los roles para que solo puedan ver sus citas

Parte 4: Análisis de Riesgos

- Completa una tabla de riesgos para 5 amenazas:

Riesgo	Vulnerabilidad	Impacto	Nivel	Posible solución
Inyección SQL	Atacante externo	Alto	Critico	Validación de los campos del formulario para prevenir estos ataques

Evaluación

- Entrega un documento con las preguntas respondidas
- Práctica relacionada con el RA5
- Cada falta de ortografía resta -0.25, hasta un máximo de 2

Criterio	Excelente	Bien	Suficiente	Insuficiente
Inventario de Datos (1 punto)	Tabla completa con 15+ datos correctamente clasificados. Justificaciones técnicas sólidas basadas en normativa. Evaluación crítica de necesidad de cada dato. (1)	Tabla con 15 datos, mayoría bien clasificados. Justificaciones correctas pero genéricas. Evalúa necesidad de datos principales. (0,7)	Tabla con 12-14 datos. Algunas clasificaciones incorrectas. Justificaciones superficiales. Evaluación limitada de necesidad. (0,3)	Menos de 12 datos o clasificaciones mayoritariamente incorrectas. Sin justificaciones o erróneas. (0)

Criterio	Excelente	Bien	Suficiente	Insuficiente
Categorización ENS (1 punto)	Las 3 dimensiones correctamente evaluadas con justificación detallada del impacto. Categoría final correcta (ALTA). Menciona consecuencias legales/sanitarias.(1)	Las 3 dimensiones evaluadas correctamente. Justificación adecuada. Categoría final correcta. (0,7)	2 dimensiones correctas. Justificación básica. Puede haber error en categoría final por falta de comprensión. (0,3)	1 o ninguna dimensión correcta. Sin justificación o errónea. Categoría final incorrecta. (0)
Evaluación de los 6 Principios RGPD (1,5 puntos)	Los 6 principios evaluados correctamente. Identifica todos los incumplimientos con evidencias específicas del caso. Acciones correctivas concretas y aplicables. (1.5)	5-6 principios correctos. Identifica incumplimientos principales. Acciones correctivas adecuadas pero genéricas. (1 punto)	4 principios correctos. Identifica algunos incumplimientos. Acciones correctivas superficiales. (0,5 puntos)	Menos de 4 principios o evaluaciones incorrectas. No identifica incumplimientos clave. (0)
Análisis de Política de Privacidad (0,75)	Identifica 4+ incumplimientos graves: casilla premarcada, falta de base legal clara, finalidades mezcladas, conservación indefinida. Cita artículos RGPD vulnerados. (0,75)	Identifica 3 incumplimientos principales. Menciona normativa general. (0,5)	Identifica 1-2 incumplimientos. Sin referencias normativas específicas. (0.25)	No identifica incumplimientos o son incorrectos. (0)
Implementación de Derechos de Usuarios (0,75)	Propone implementación técnica para 5+ derechos. Describe proceso completo (verificación identidad, plazos, formatos). Soluciones viables técnicamente. (0.75)	Propone implementación para 3-4 derechos. Proceso descrito adecuadamente. Soluciones razonables. (0,5)	Propone 2 derechos. Descripción básica. Soluciones genéricas. (0,25)	1 derecho o propuestas inviables técnicamente. (0)

Criterio	Excelente	Bien	Suficiente	Insuficiente
Análisis de Incidentes Reales (1,25)	Los 5 incidentes analizados correctamente. Principio CIA correcto en todos. Identifica causa raíz real. Impacto evaluado adecuadamente. Medidas preventivas específicas y técnicas. (1,25)	4--5 incidentes correctos. Principio CIA correcto. Causas e impacto identificados. Medidas preventivas adecuadas. (0,8)	3 incidentes correctos. Algunos errores en principio CIA. Causas superficiales. Medidas genéricas. (0,4)	Menos de 3 correctos. Errores en principio CIA. Sin análisis de causa. Medidas irrelevantes. (0)
Evaluación de Seguridad Técnica (1,25 puntos)	Identifica 8+ problemas técnicos graves. Priorización correcta. Soluciones técnicas específicas y viables.(1,25)	Identifica 6-7 problemas. Priorización razonable. Soluciones técnicas adecuadas.(0,8)	Identifica 4-5 problemas. Priorización básica. Soluciones genéricas pero correctas.(0,4)	Menos de 4 problemas o identificaciones incorrectas. Sin priorización lógica. Soluciones inviables.(0)
Matriz de Riesgos (2 puntos)	Identifica 5 amenazas relevantes y reales. Vulnerabilidades específicas del sistema. Evaluación de impacto coherente (considera datos médicos, RGPD, disponibilidad). Nivel de riesgo calculado correctamente. Soluciones concretas y priorizadas. (2)	5 amenazas identificadas. Vulnerabilidades adecuadas. Impacto evaluado correctamente. Nivel coherente. Soluciones razonables. (1,4)	4 amenazas. Vulnerabilidades genéricas. Impacto básico. Algunas soluciones correctas. (0,6)	Menos de 4 amenazas o irrelevantes. Vulnerabilidades incorrectas. Sin evaluación de impacto. Soluciones no aplicables. (0)
Presentación y Formato (0,5 pts)	Documento profesional, bien estructurado. Tablas completas y legibles. Redacción clara y técnica. (0,5)	Documento ordenado. Tablas correctas. Redacción adecuada. (0,3)	Documento básico. Tablas incompletas. Redacción mejorable. (0,1)	Documento desorganizado. Tablas confusas o incompletas.(0)