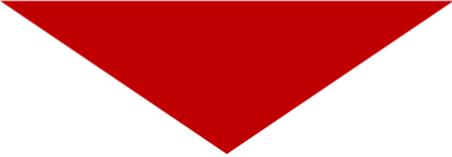


**PROYECTO**

“Implementación del Portal del Paciente”



**CURSO**

Gestión de cambios en los proyectos.

**ACTIVIDAD**

Propuesta de estrategias para cambios críticos

**PROFESOR**

Prof. Jaime Pari Tapara

**INTEGRANTES**

Melani Milagros Quenta Quispe

Stephanie Nicol Callata Candia

Dariel Moises Carpio Chura

Enmanuel Andres Choque Choque

Angelo Teofilo Yanapa Chambilla

*Viernes 24 de octubre del 2025*

*PERÚ – TACNA*



---

## ARQUITECTURA DE PLATAFORMAS Y SERVICIOS DE TECNOLOGIAS DE INFORMACION

---

### 1. Diagnóstico del cambio crítico

Durante la fase de Marcha Blanca del portal del paciente "MiSalud Conectada", un médico del grupo piloto reportó una grave falla de seguridad: al intentar descargar los resultados de laboratorio de un paciente "A", el sistema mostró brevemente la ficha médica de otro paciente "B" que no está bajo su cuidado. Aunque el error desapareció tras actualizar la página, el incidente fue registrado mediante captura de pantalla, demostrando la existencia real de la brecha.

#### **Justificación de la criticidad del cambio:**

- **Alcance:**  
El incidente afecta directamente al objetivo principal del proyecto: ofrecer un sistema seguro y confiable para la gestión de datos médicos personales. La aparición de este error compromete el alcance funcional del portal, ya que no garantiza la confidencialidad ni la correcta asignación de datos a los usuarios autorizados.
- **Tiempo:**  
El cronograma se ve impactado de forma inmediata. El lanzamiento nacional programado en 15 días debe suspenderse hasta que se identifique, corrija y valide completamente la falla. Esto representa un retraso crítico que afecta la planificación general del proyecto.
- **Costo:**  
El costo potencial de este incidente es alto. Se exponen riesgos legales significativos por violaciones a la Ley de Protección de Datos Personales, lo que podría resultar en multas millonarias. Además, los costos de remediación técnica, auditorías de seguridad, y comunicaciones de crisis se incrementarán.
- **Calidad:**  
El evento revela una falla estructural en la calidad del sistema, especialmente en la gestión de sesiones, privacidad de los datos y control de accesos. Esto pone en duda la madurez del sistema para operar a gran escala y afecta gravemente la percepción de calidad del producto final.

### 2. Estrategia general propuesta

#### Contención inmediata, análisis y re-implementación de la lógica de autorización.

Primeramente, se detendría el funcionamiento de descarga y visualización de los resultados del paciente en el sistema para evitar los riesgos de filtración de datos.

Luego se realizará un exhaustivo análisis en el código del sistema, sobre todo en los códigos de autenticación y autorización a los datos, como también en los logs de actividad para determinar la causa de la filtración de información.

Finalmente corregiremos el error agregando un parche de emergencia, poniendo a prueba la seguridad (penetration testing o stress testing) antes de reanudar las actividades.

---

**ARQUITECTURA DE PLATAFORMAS Y SERVICIOS DE TECNOLOGIAS DE INFORMACION**

---

**Justificación**

Esta estrategia es la más adecuada porque prioriza la mitigación del riesgo legal y de reputación de la empresa (detener la filtración de datos) antes que en la continuidad operativa se sigan filtrando los datos de otros pacientes de manera errónea. Un parche menor sin análisis del código ni pruebas exhaustivas es un riesgo latente ante una vulnerabilidad de datos sensibles

**3. Plan de respuesta detallado**

<b>Acción específica</b>	<b>Responsable</b>	<b>Plazo estimado</b>	<b>Recursos requeridos</b>
Investigar el incidente de brecha de seguridad	Líder técnico, jefe de proyecto, equipo de desarrollo	24 horas	Personal técnico especializado, herramientas de investigación de seguridad
Desarrollar un parche o solución para evitar el acceso no autorizado a los historiales médicos	Equipo de desarrollo, expertos en seguridad informática	48 horas	Software de desarrollo, presupuesto para pruebas de seguridad
Verificar que la solución implementada no afecte otras funciones del portal	Líder técnico, equipo de calidad, equipo de desarrollo	24 horas	Personal de pruebas, software de pruebas integradas
Realizar pruebas de penetración adicionales para asegurar que la brecha no persista	Especialistas en ciberseguridad	48 horas	Herramientas de pruebas de penetración, personal de ciberseguridad
Re-entrenar al personal sobre la importancia de la seguridad de los datos y la protección de la privacidad	Jefe de proyecto, departamento de recursos humanos	72 horas	Personal de formación, materiales de capacitación
Informar a los pacientes y médicos sobre la solución implementada y las medidas tomadas	Jefe de comunicación, jefe de proyecto	24 horas	Recursos de comunicación (email, portal web, etc.)
Preparar un informe de lecciones aprendidas y recomendaciones para evitar futuros incidentes	Líder técnico, equipo de gestión de riesgos	48 horas	Herramientas de documentación, tiempo para reuniones de análisis

---

ARQUITECTURA DE PLATAFORMAS Y SERVICIOS DE TECNOLOGIAS DE INFORMACION

---

**4. Plan de comunicación**

El presente plan de comunicación tiene como objetivo garantizar una gestión transparente, efectiva y oportuna de la información relacionada con el incidente de seguridad detectado en el portal “Mi Salud Conectada”, así como asegurar la coordinación entre todos los involucrados del proyecto durante el proceso de corrección y validación de la solución.

**4.1. Protocolo de Comunicación y Roles**

Rol	Responsable Principal	Tareas Clave y Autoridad
Líder de Comunicaciones de Crisis	Jefe de Proyecto	Único autorizado para coordinar y aprobar todos los mensajes. <b>Vocero oficial</b> ante audiencias clave (excepto prensa).
Líder Técnico de Respuesta	Líder Técnico / Especialista en Seguridad	Revisa y valida la precisión técnica de todos los mensajes. Responsable del informe técnico del incidente.
Soporte Legal y Cumplimiento	Departamento Legal	Define el contenido exacto de la notificación a las autoridades regulatorias y revisa el cumplimiento de la Ley de Protección de Datos Personales en los comunicados externos.

## ARQUITECTURA DE PLATAFORMAS Y SERVICIOS DE TECNOLOGIAS DE INFORMACION

## 4.2. Audiencias Clave, Mensajes y Canales

Audiencia (Stakeholder)	Objetivo de la comunicación	Mensaje Clave (Primeras 24 horas)	Canal y Momento
<b>Equipo del Proyecto</b>	Iniciar la corrección y garantizar discreción.	"Crítica confirmada: Falla de acceso a datos. La funcionalidad está SUSPENDIDA. Prioridad inmediata: ejecutar el parche y las pruebas de seguridad."	Reunión de emergencia (virtual).
<b>Dirección Ejecutiva/Legal</b>	Informar la crisis, el riesgo y la contención.	"Brecha de datos confirmada y contenida. Se requiere aprobación urgente para recursos de auditoría y notificación legal inmediata. El lanzamiento nacional se pospone."	Informe ejecutivo formal (email y llamada).
<b>Médicos (Piloto)</b>	Explicar la pausa operativa con confianza.	"Vulnerabilidad de acceso a resultados identificada y contenida. La descarga está inhabilitada temporalmente para garantizar la seguridad. La privacidad de los datos es nuestra prioridad."	Correo electrónico oficial.
<b>Pacientes (Piloto)</b>	Proporcionar tranquilidad y justificar la interrupción.	"Se ha detectado una anomalía en el portal. Hemos suspendido temporalmente funciones para aplicar una corrección de emergencia, priorizando su seguridad. Sus datos están protegidos."	Banner en el portal y comunicado por email.
<b>Autoridades Regulatorias</b>	Cumplir con la obligación de notificación.	"Hemos detectado y contenido una brecha de seguridad. Adjuntamos informe preliminar y el plan de mitigación para iniciar la solución permanente."	Notificación formal por escrito.