Caso de Estudio 1: Gestión de Riesgos en SaludConnect Ecuador SA

# Contexto

SaludConnect Ecuador SA es una empresa que ofrece servicios de telemedicina y administración de historiales médicos electrónicos para hospitales y clínicas del país. La organización cuenta con una plataforma digital que integra datos sensibles de pacientes, información clínica, agendas médicas y resultados de solicitudes. Conscientes de la necesidad de proteger estos activos críticos, la empresa implementó un proceso de gestión de riesgos basado en metodologías internacionales (adaptadas a su realidad) que incluye la identificación de activos, evaluación de vulnerabilidades y amenazas, y la implementación de salvaguardas técnicas y administrativas. Sin embargo, debido a un rápido crecimiento y la constante evolución del entorno digital, algunos controles no se han actualizado conforme a las nuevas amenazas detectadas.

# Incidente

Durante una revisión de seguridad rutinaria, el equipo de TI detectó accesos anómalos en el módulo de autenticación de la plataforma. Se descubrió que un atacante había explotado una vulnerabilidad en el sistema de gestión de contraseñas (debido a una configuración obsoleta y la falta de actualización de ciertos parches) para acceder de forma no autorizada a la base de datos de pacientes. Como consecuencia, datos clínicos y personales fueron comprometidos, generando una grave violación de la confidencialidad. La brecha impactó la integridad de la información y puso en riesgo la reputación de la empresa, a la vez que evidenció deficiencias en la identificación y tratamiento de ciertos riesgos críticos.

# Preguntas para el análisis

* 1. - ¿Cuáles son los activos críticos involucrados en la operación de SaludConnect (por ejemplo, bases de datos de pacientes, sistemas de gestión clínica, etc.) y cómo se valoraron en términos de confidencialidad, integridad y disponibilidad?
* 2. - ¿Qué vulnerabilidades específicas en el proceso de autenticación permitieron la explotación por parte del atacante y cómo se relacionan con los controles existentes?
* 3. - Utilizando la fórmula Valor del riesgo = Probabilidad × Impacto, ¿cómo se habría podido cuantificar este riesgo antes del incidente?
* 4. - ¿Qué factores (por ejemplo, porcentaje de controles aplicados, vulnerabilidades detectadas) influyeron en la alta probabilidad y el elevado impacto del riesgo en este caso?
* 5.- ¿Qué medidas de tratamiento (mitigación, transferencia o asunción) se podrían haber implementado para reducir la probabilidad de materialización de este riesgo o su impacto?
* 6.- ¿Cómo podría haber mejorado el plan de actualización y revisión de salvaguardas técnicas y administrativas para prevenir incidentes similares?
* 7. - ¿Qué papel juega el monitoreo y la auditoría periódica en la detección temprana de vulnerabilidades, y cómo se podría integrar de forma más efectiva en el ciclo de gestión de riesgos de SaludConnect?