INTRODUCCIÓN

CliniNova S.A.S. es una clínica privada especializada en servicios de salud preventiva y diagnóstica en la región Caribe. Ante el creciente uso de tecnologías digitales para la atención médica, el manejo de historiales clínicos y la interconectividad de dispositivos, la alta dirección decidió implementar una estrategia integral de ciberseguridad.

Este documento consolida la presentación final del proyecto de seguridad desarrollado entre mayo y julio de 2025, como resultado del Reto Macro planteado en el marco del laboratorio de ciberseguridad. Aquí se exponen los objetivos alcanzados, métricas clave, impacto institucional y acciones recomendadas para continuidad.

3. Objetivos del Proyecto

Objetivo Estratégico	Resultado Esperado
Proteger la confidencialidad de los datos clínicos	Evitar fugas de información personal y médica
Aumentar el nivel de madurez de seguridad de la organización	Subir de Nivel 1 (Inicial) a Nivel 3 (Definido)
Cumplir normativas del sector salud y estándares ISO	Asegurar cumplimiento ISO 27001 >90%
Establecer un plan sostenible de defensa digital	Consolidar MFA, backups, auditorías y segmentación

4. Metodología Aplicada

El proyecto fue ejecutado en 10 fases, cada una correspondiente a un reto del ciclo de vida de la ciberseguridad:

- Evaluación inicial de riesgos y activos (Reto 1)
- Diseño de estrategia de seguridad (Reto 2)
- Configuración de firewalls, IDS/IPS y VPN (Reto 3)
- Gestión de accesos, cifrado y MFA (Reto 4)

- Gestión de vulnerabilidades y protección de endpoints (Reto 5)
- Plan de respuesta a incidentes (Reto 6)
- Recuperación ante desastres (Reto 8)
- Auditoría y evaluación normativa (Reto 9)
- Plan de mejora continua y presentación final (Reto 10)

5. Resultados Obtenidos

Indicador de Éxito	Resultado Alcanzado
Reducción de vulnerabilidades críticas	75%
Tasa de implementación de MFA	100% en cuentas administrativas
Tiempo promedio de respuesta ante incidentes	20 minutos
Nivel de cumplimiento con ISO 27001	90%
Participación en capacitaciones trimestrales	92% del personal operativo

6. Impacto Institucional

La implementación de esta estrategia no solo mejoró los indicadores técnicos, sino que generó un cambio cultural en la organización. Se promovió una nueva mentalidad sobre la protección de la información médica.

Además, CliniNova se posiciona ahora como una clínica tecnológicamente segura, elemento crítico ante auditorías de entes reguladores como el Ministerio de Salud y la Superintendencia de Industria y Comercio.

7. Recomendaciones Generales

Área	Recomendación
Capacitación	Continuar con programas trimestrales orientados a phishing y amenazas internas
Auditoría	Automatizar revisiones de logs y configuraciones con herramientas como `auditd`
Infraestructura	Segmentar las redes clínicas, administrativas y de invitados
Gobernanza	Integrar la ciberseguridad en el comité directivo de calidad médica

8. Conclusión

Este informe resume un hito importante para CliniNova S.A.S.: haber consolidado una estrategia de seguridad robusta, técnica, normativa y operativa. Con los resultados alcanzados y la continuidad planificada, la institución fortalece su reputación, protege la vida digital de sus pacientes y establece una base sólida para enfrentar amenazas futuras.

9. Anexos

Anexo A - Glosario de términos clave
Anexo B - Cronograma de implementación por fase
Anexo C - Lista de documentos relacionados en el repositorio GitHub