Título: Informe de Clausura del Proyecto de Ciberseguridad
Empresa: CliniNova S.A.S.

Ubicación: Barranquilla, Atlántico, Colombia

Fecha: Julio 2025
Versión: 1.0
Elaborado por: Coordinación de Seguridad de la Información
Supervisado por: Dirección General – Comité de Seguridad Digital

2. Introducción

Este informe representa el cierre formal del proyecto de implementación de una estrategia integral de ciberseguridad en CliniNova S.A.S., desarrollado en el periodo comprendido entre mayo y julio de 2025 como parte del Reto Macro planteado en el laboratorio técnico.

El proyecto fue concebido ante el aumento de amenazas cibernéticas en el sector salud y la necesidad de garantizar la confidencialidad, integridad y disponibilidad de la información médica. El presente documento detalla los entregables, logros, indicadores alcanzados, lecciones institucionales y el estado de cierre administrativo y operativo.

---

3. Alcance del Proyecto

Nombre del proyecto: Estrategia Integral de Ciberseguridad
Área de implementación: CliniNova S.A.S. – sede principal
Duración: 10 semanas (mayo a julio de 2025)
Ámbitos cubiertos:

- Sistemas clínicos (HCE, dispositivos médicos)
- Redes administrativas
- Usuarios internos y externos
- Infraestructura local y nube
- Procesos de respaldo y recuperación
- Cumplimiento normativo (ISO 27001, GDPR, Resolución 1995 de 1999)

---

4. Resumen de Actividades por Reto

Reto	Tema	Resultado Principal
Reto 1	Identificación de activos y evaluación de riesgos	5 activos críticos priorizados y mapa de riesgos documentado

Reto 2	Diseño de estrategia de seguridad	Plan integral alineado con ISO 27001 y NIST CSF
Reto 3	Firewalls, VPN, IDS/IPS	Implementación de reglas y configuración de túneles VPN
Reto 4	Gestión de accesos y MFA	MFA aplicado al 100% de usuarios administrativos
Reto 5	Seguridad en endpoints y gestión de parches	92% de estaciones con antivirus actualizado y políticas de actualización automática
Reto 6	Plan de respuesta a incidentes	Procedimiento probado, roles definidos, simulacro exitoso
Reto 8	Recuperación ante desastres	Política 3-2-1 implementada, recuperación verificada en entorno de prueba
Reto 9	Auditoría técnica y normativa	90% de cumplimiento en checklists ISO y regulación nacional
Reto 10	Clausura y mejora continua	Planes integrados y validados por stakeholders internos

---

5. Resultados Generales del Proyecto

Indicador	Valor Inicial	Meta	Resultado Final
Vulnerabilidades críticas	27	≤ 5	6 (reducción del 78%)
Cumplimiento ISO 27001	42%	≥ 85%	90%
Usuarios con MFA	12%	100%	100%
Tiempo medio de respuesta a incidentes	>1 hora	≤ 20 min	17 min
Participación en capacitaciones	—	≥ 90%	92%
Backups funcionales verificados	60%	100%	100%

---

6. Evaluación de Entregables

Todos los entregables establecidos en la fase de planificación fueron completados y documentados en el repositorio institucional:

Entregable	Estado	Evidencia
Política de Seguridad de la Información	Aprobado	`/documentos/politica_seguridad.pdf`
Scripts de auditoría y respaldo	Ejecutados y probados	`/scripts/`
Simulación de incidente real	Concluida con éxito	`/documentos/plan_respuesta_incidentes.pdf`
Plan de continuidad y recuperación	Validado	`/documentos/plan_recuperacion.pdf`
Plan de mejora continua	Incorporado	`/documentos/plan_mejora_continua.pdf`

---

7. Participación de Áreas Clave

La colaboración interdepartamental fue un factor decisivo. Las siguientes áreas participaron activamente:

Área	Rol
Dirección General	Aprobación estratégica y presupuesto
Tecnología e Infraestructura	Implementación técnica y configuración de sistemas
Recursos Humanos	Coordinación de capacitaciones y canal de comunicación interna
Legal y cumplimiento	Validación de políticas conforme a normativas
Áreas médicas y administrativas	Participación en talleres y pruebas funcionales

---

8. Estado de Cierre del Proyecto

Criterio de Cierre	Estado	Observaciones
Objetivos técnicos alcanzados	Cumplido	Todos los KPI superaron las metas
Documentación completa	Cumplido	100% entregada en formatos PDF y Markdown
Retroalimentación aplicada	Cumplido	Comentarios integrados en planes de mejora
Validación final por stakeholders	Aprobado	Dirección general autorizó cierre oficial
Entrega al área de continuidad operativa	Ejecutada	Transferencia de responsabilidades formalizada

---

9. Recomendaciones Finales

1. **Actualizar el plan de seguridad semestralmente**, integrando nuevos riesgos, tecnologías y aprendizajes.

2. **Consolidar el comité de seguridad digital** como organismo permanente de vigilancia y ajuste.

3. **Reforzar la formación periódica**, especialmente ante nuevas modalidades de ataque como deepfakes o IA suplantadora.

4. **Iniciar exploración de tecnologías emergentes** como EDR, SOAR o biometría conductual.

---

10. Conclusión

El proyecto de ciberseguridad ejecutado en CliniNova S.A.S. demostró que es posible transformar digitalmente una institución médica sin comprometer la confidencialidad de los datos ni la integridad de los procesos clínicos.

Al cierre del proyecto, CliniNova no solo posee mejores controles técnicos, sino también una cultura organizacional más madura en torno a la seguridad digital. La clínica se proyecta como

una institución resiliente, preparada para enfrentar las amenazas cibernéticas del presente y del futuro.

Anexo A – Cronograma Real de Ejecución

Semana	Actividad Principal	Reto Asociado
Semana 1	Evaluación de riesgos y activos críticos	Reto 1
Semana 2	Diseño de estrategia integral	Reto 2
Semana 3	Implementación de Firewalls, IDS/IPS y VPN	Reto 3
Semana 4	Gestión de accesos y MFA	Reto 4
Semana 5	Gestión de parches y seguridad en endpoints	Reto 5
Semana 6	Simulación de incidentes y plan de respuesta	Reto 6
Semana 7	Plan de recuperación ante desastres	Reto 8
Semana 8	Auditoría normativa y técnica	Reto 9
Semana 9–10	Retroalimentación, cierre y presentación final	Reto 10