ESTRATEGIA DE CIBERSEGURIDAD

TALENTO TECH - CIBERSEGURIDAD BÁSICO

ANDRES AGUILAR MORENO

CAMILO AGUILAR MORENO

2025

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 del la estrategía (https://github.com/camilom1dev/Estrategia_ciberseguridad/tree/main)

Anexo A – Glosario de Términos Clave

Término	Definición
Ciberseguridad	Conjunto de prácticas y tecnologías destinadas a proteger los sistemas informáticos, redes y datos frente a ataques, daños o accesos no autorizados.
MFA (Autenticación Multifactor)	Método de autenticación que requiere dos o más formas de verificación para acceder a un sistema. Ej: contraseña + código en app móvil.
VPN (Red Privada Virtual)	Tecnología que crea una conexión segura y cifrada sobre una red pública (como Internet).
IDS/IPS	Sistemas de detección y prevención de intrusos que monitorean tráfico de red y bloquean amenazas.
SIEM (Security Information and Event Management)	Herramienta para el análisis centralizado de logs y eventos de seguridad en tiempo real.
Zero Trust	Modelo de seguridad que asume que ninguna entidad (interna o externa) es de confianza por defecto. Se basa en la verificación constante.
RPO (Recovery Point Objective)	Máximo tiempo aceptable desde la última copia de seguridad hasta un posible desastre.
RTO (Recovery Time Objective)	Tiempo máximo permitido para restaurar una función o servicio después de un incidente.
Activos Críticos	Sistemas, servicios o información esenciales cuya pérdida puede afectar gravemente las operaciones.
ISO 27001	Estándar internacional que especifica los requisitos para establecer, implementar y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).

Anexo B – Cronograma de Implementación por Fase

Reto	Actividad Ejecutada	Semana	Responsable
Reto 1	Evaluación de riesgos y activos	Semana 1	CISO + Analista TI

Reto 2	Definición de estrategia integral	Semana 2	Coordinador de Seguridad
Reto 3	Configuración de Firewalls, IDS/IPS, VPN	Semana 3	Equipo Técnico
Reto 4	Gestión de accesos y MFA	Semana 4	Infraestructura TI
Reto 5	Protección de endpoints y gestión de parches	Semana 5	Help Desk
Reto 6	Plan de respuesta a incidentes	Semana 6	Comité de Incidentes
Reto 8	Plan de recuperación y continuidad	Semana 7	Área de Operaciones
Reto 9	Auditoría de seguridad y cumplimiento normativo	Semana 8	CISO + Auditor Interno
Reto 10	Presentación final y mejora continua	Semana 9-10	Dirección + Seguridad

---

Anexo C – Documentos Relacionados en el Repositorio GitHub

Repositorio: `https://github.com/[tu-usuario]/ciberseguridad_clininova_final`

Carpeta	Archivo	Descripción
`/documentos/`	`Presentacion_Final_CliniNova.pdf`	Informe ejecutivo del proyecto
	`Plan_Mejora_Continua_CliniNova.pdf`	Estrategia a largo plazo para sostenibilidad
	`Registro_Retroalimentacion_Stakeholders.pdf`	Feedback y ajustes realizados
	`Estrategias_Seguridad_Futura_CliniNova.pdf`	Políticas para enfrentar nuevas amenazas
	`Lecciones_Aprendidas_CliniNova.pdf`	Resumen reflexivo del proyecto

	Informe_Clausura_Proyecto_Ciberseguridad.pdf	Cierre formal del ciclo de implementación
/scripts/	script_auditoria.py	Script para ejecutar auditorías mensuales
	configurar_zero_trust.py	Reglas de segmentación y aislamiento de red
	respaldo_s3.shpy	Automatización de respaldos hacia AWS
/capacitacion/	Capacitaciones_Ciberseguridad_2025.xlsx	Calendario y estructura de formación interna

Título: Plan de Mejora Continua de Ciberseguridad

Empresa: CliniNova S.A.S.

Versión: 1.0
Ubicación: Barranquilla, Atlántico, Colombia
Fecha de elaboración: JULIO 2025
Elaborado por: Oficina de Seguridad de la Información – CliniNova S.A.S.

2. Introducción

La seguridad de la información en el sector salud no es un evento único, sino un proceso continuo. El presente documento forma parte del cierre del proyecto de ciberseguridad implementado en CliniNova S.A.S., como resultado del Reto Macro desarrollado en 10 fases.

Si bien se logró una reducción significativa de vulnerabilidades y se mejoraron múltiples frentes (cifrado, MFA, backups, segmentación de red), la amenaza cibernética evoluciona constantemente. Este plan tiene como objetivo garantizar que las mejoras logradas sean sostenibles, escalables y adaptables a nuevas condiciones y riesgos emergentes.

---

3. Objetivos del Plan

Objetivo Estratégico	Descripción
Sostenibilidad	Asegurar que los controles actuales se mantengan funcionales y eficaces en el tiempo.
Adaptabilidad	Preparar la clínica para responder de manera proactiva a nuevas amenazas.
Automatización	Reducir la dependencia del factor humano mediante tecnología programable.
Cultura Organizacional	Consolidar una cultura institucional orientada a la prevención digital.

---

4. Líneas de Acción Prioritarias

4.1 Automatización de Auditorías Técnicas

Descripción:
Implementación de scripts y tareas cron programadas para revisar configuraciones, detectar cambios no autorizados y generar alertas.

Herramienta sugerida: `auditd` + `cron` + envío automatizado vía email.

Ejemplo de script:

bash

CopiarEditar

```
#!/bin/bash
ausearch -m EXECVE -ts yesterday | aureport -f >
/var/log/audit/audit_report_$(date +%F).log
```

Indicador de Éxito	Meta
Informes de auditoría generados	1 por semana
Alertas proactivas de cambios críticos	> 95% detectados

4.2 Fortalecimiento del Programa de Capacitación Continua

Descripción:
Cursos trimestrales dirigidos a médicos, personal de enfermería, administrativos y técnicos, con contenidos adaptados a su rol.

Temas clave por trimestre:

Trimestre	Temas de Capacitación
Q1	Phishing avanzado, Ransomware, Buenas prácticas con contraseñas
Q2	Manejo seguro de dispositivos USB, suplantación vía IA, Wi-Fi inseguro
Q3	Ingeniería social, políticas internas, cumplimiento normativo
Q4	Simulación de ataques internos, respuesta a incidentes básicos

Métrica esperada:

- Participación: 100% del personal anual.
- Evaluación final con nota mínima de 80%.

4.3 Implementación de Modelo Zero Trust

Descripción:
Adoptar una arquitectura donde ninguna conexión es confiable por defecto, ni siquiera dentro de la red interna.

Componentes del modelo:

Componente	Implementación
Segmentación de red	VLAN separadas: clínica, administración, invitados
Control de acceso por rol	RBAC actualizado en Active Directory
Autenticación reforzada	MFA para personal interno y externo
Supervisión constante	SIEM para monitoreo en tiempo real con Splunk

---

4.4 Gestión Inteligente de Backups

Descripción:
Mejorar la estrategia de respaldo con políticas 3-2-1 (tres copias, en dos medios, una fuera del sitio).

Herramientas utilizadas:

- `rsync`, AWS S3, `cron`, `clamscan` para validación de integridad.

Tipo de backup	Frecuencia	Medio
Completo	Diario	AWS S3
Incremental	Cada hora	NAS local
Validación/restauración	Mensual	Laboratorio de pruebas

Indicadores:

Métrica	Valor Objetivo
RPO (Recovery Point Objective)	≤ 15 minutos
RTO (Recovery Time Objective)	≤ 2 horas

---

5. Calendario de Implementación

Acción	Responsable	Inicio	Periodicidad
Configurar scripts de auditoría	Líder de Infraestructura	Ago 2025	Semanal
Lanzar programa de formación	Gestión Humana + CISO	Sep 2025	Trimestral
Segmentar redes internas	Infraestructura	Oct 2025	Una vez
Validar restauración de backups	Soporte TI	Mensual	Permanente

---

6. Seguimiento y Evaluación

Se definirá un comité de mejora continua en seguridad compuesto por:

- Coordinador de Seguridad Informática
- Representante de la Dirección General
- Líder de Tecnología Médica
- Analista de Calidad

Responsabilidades del comité:

Actividad	Frecuencia
Revisión de indicadores técnicos	Mensual
Validación de logs y auditorías	Trimestral
Encuestas de concienciación	Bimestral
Actualización de políticas de seguridad	Semestral

---

7. Conclusión

Este plan de mejora continua constituye el compromiso de CliniNova S.A.S. con la resiliencia digital, la protección de sus pacientes y la preparación ante futuras amenazas.

Más allá de lo técnico, este documento consolida una cultura de seguridad institucional, empoderando al personal y fortaleciendo la confianza del público en nuestra organización como un referente en ciberseguridad dentro del sector salud.

Anexo A – Lista de Métricas de Seguimiento

Indicador	Objetivo	Herramienta
% de usuarios con MFA	100%	Azure AD, Google Workspace
% de capacitaciones completadas	≥ 90%	LMS
N° de alertas críticas auditadas	≥ 95%	Splunk
Tiempo promedio de restauración (RTO)	≤ 2 horas	Veeam, AWS
N° de intentos de acceso bloqueados	Incremento mensual de detección	Firewall, SIEM

Título: Registro de Retroalimentación de Stakeholders – Proyecto de Ciberseguridad

Empresa: CliniNova S.A.S.

Versión: 1.0

Ubicación: Barranquilla, Atlántico, Colombia
Fecha: julio 2025

2. Introducción

El éxito de un proyecto de ciberseguridad no se mide solo por las soluciones técnicas implementadas, sino también por el nivel de apropiación y aceptación de los usuarios finales y líderes organizacionales.

Durante la etapa final del proyecto de seguridad digital de CliniNova S.A.S., se llevaron a cabo reuniones de evaluación con los principales stakeholders: dirección médica, gestión humana, tecnología, operaciones clínicas y administración. Esta sección documenta los comentarios recibidos, el análisis de viabilidad y las acciones tomadas para incorporar dichos aportes al ciclo de mejora continua.

---

3. Metodología de Recopilación

Se aplicó un enfoque mixto de retroalimentación:

Método	Medio	Fecha	Participantes
Reunión sincrónica	Google Meet (grabada)	16/07/2025	Dirección, TI, Operaciones
Encuesta anónima	Google Forms	18–21/07/2025	36 empleados (muestra transversal)
Focus group	Sala de juntas CliniNova	23/07/2025	8 representantes de áreas clave
Retroalimentación directa	Canal interno en Teams	Todo julio	Abierto a todo el personal

Los datos fueron analizados mediante codificación temática y categorización de sugerencias, clasificándolas por prioridad y factibilidad.

---

4. Temas Principales Identificados

Tema Recurrente	Stakeholders que lo expresaron	Nivel de impacto	Prioridad asignada
Capacitación más práctica y específica	Personal clínico, Recursos Humanos	Medio	Alta

Ampliar MFA a contratistas externos	Área Jurídica y TI	Alto	Alta
Aumentar la frecuencia de pruebas de recuperación	Infraestructura, Dirección	Alto	Alta
Simplificar accesos a sistemas post-MFA	Personal administrativo	Bajo	Media
Crear boletines mensuales de alertas	Dirección General	Medio	Media
Mejorar respuesta ante solicitudes TI urgentes	Enfermería, Operaciones	Bajo	Baja

---

5. Sugerencias y Acciones Tomadas

Tema	Sugerencia	Acción Tomada	Estado
Capacitación	Agregar talleres prácticos de suplantación y ransomware	Incluir en Q4/2025 bajo plan formativo	Programada
MFA	Extender MFA a personal externo y contratistas	Aprobado por TI, se inicia piloto en septiembre	En curso
Backups	Realizar simulaciones trimestrales de recuperación	Se calendarizan en cronograma 2025–2026	Implementado
Comunicación	Publicar boletines mensuales de seguridad	Se delegó a TI con apoyo de Comunicaciones	Aprobado
Accesibilidad	Revisar impacto de MFA en usuarios mayores	Se ofrecerá guía impresa + asistencia presencial	En proceso

---

6. Valoración de la Retroalimentación

Se realizaron dos preguntas clave en la encuesta de percepción general:

¿Cómo calificaría la implementación del proyecto de seguridad digital en CliniNova?

- Excelente: 56%

- Buena: 36%
- Regular: 8%
- Deficiente: 0%

¿Considera que el nuevo sistema protege mejor los datos del paciente?

- Sí: 89%
- No: 5%
- No sabe / no responde: 6%

Comentarios destacados (de forma anónima):

> "Agradezco que nos capacitaron con ejemplos reales. Nunca pensé que un correo falso pudiera ser tan creíble."
>
> "Sería útil que también nos explicaran qué hacer si ocurre un incidente, no solo cómo prevenirlo."
>
> "Nos sentimos más protegidos, pero también más responsables. La seguridad ya es parte del día a día."

---

7. Plan de Integración de Mejoras Basadas en Feedback

Área	Mejora	Responsable	Fecha de Inicio	Seguimiento
Capacitación	Nuevos módulos prácticos	Seguridad + Talento Humano	Sep 2025	Evaluación Q4
Acceso	MFA para terceros	Infraestructura	Sep 2025	Informe Nov 2025
Comunicación	Boletines internos	TI + Comunicaciones	Ago 2025	Mensual
Resiliencia	Pruebas de recuperación ampliadas	Soporte TI	Ago 2025	Informe trimestral

---

8. Conclusiones

La apertura a la retroalimentación es un componente esencial de una cultura organizacional orientada a la mejora continua. Las sugerencias y observaciones recogidas en este proceso no solo reflejan una alta participación, sino también una apropiación creciente por parte del personal de CliniNova frente a la seguridad de la información.

Gracias a este proceso participativo, se fortalecen tanto la estrategia técnica como el compromiso institucional con la protección de los datos clínicos y el cumplimiento normativo.

Anexo A – Plantilla de Formulario de Retroalimentación

Nombre del instrumento: Encuesta de Satisfacción del Proyecto de Ciberseguridad
Formato: Google Forms
Campos incluidos:

1. Rol del participante
2. ¿Cómo calificaría el proyecto de ciberseguridad? (Escala 1–5)
3. ¿Se siente más seguro/a trabajando en el entorno actual?
4. ¿Qué cambiaría del sistema implementado?
5. ¿Qué sugerencia considera más urgente de atender?
6. Comentarios adicionales

Versión: 1.0

Ubicación: Barranquilla, Colombia
Fecha: JULIO 2025
Elaborado por: Coordinación de Seguridad de la Información

2. Introducción

A medida que las amenazas cibernéticas evolucionan, también deben hacerlo las defensas institucionales. Las soluciones de seguridad implementadas durante el proyecto actual han fortalecido significativamente a CliniNova S.A.S.; sin embargo, el entorno digital es dinámico y los actores maliciosos innovan constantemente.

El presente documento propone un conjunto de estrategias futuras para la protección de los activos críticos, la integridad de los datos clínicos y la continuidad operativa. Estas estrategias combinan análisis de tendencias globales, predicción de vectores emergentes y recomendaciones basadas en marcos internacionales como ISO 27001, NIST CSF y OWASP.

---

3. Análisis de Amenazas Emergentes en el Sector Salud

Amenaza	Descripción	Impacto Potencial	Tendencia
Ransomware-as-a-Service (RaaS)	Plataformas delictivas que permiten lanzar ataques sin conocimiento técnico	Alto	En aumento desde 2024
Suplantación con IA (Deepfakes)	Imitación de voz o rostro para ingeniería social avanzada	Alto	Amenaza emergente en telemedicina
Compromiso de IoMT	Hackeo de dispositivos médicos conectados (monitores, marcapasos)	Crítico	Subestimado por instituciones
Ataques a cadena de suministro digital	Brechas a través de terceros o software con malware	Medio–alto	Común en sistemas médicos integrados
Filtración vía Shadow IT	Uso de aplicaciones no autorizadas por el personal	Medio	Alta ocurrencia en entornos administrativos

---

4. Estrategias Proactivas Propuestas

4.1 Fortalecimiento del Modelo Zero Trust (ZTA)

Justificación: Ante entornos distribuidos y conectividad ubicua, se requiere un control granular de acceso por usuario, ubicación, dispositivo y contexto.

Componentes recomendados:

Elemento	Medida
Autenticación continua	Revalidación de identidad cada 30 minutos en sistemas críticos
Segmentación dinámica	VLANs por unidad clínica, bloqueando lateralidad
Autorización basada en contexto	Acceso condicional a registros clínicos fuera de horario o ubicación sospechosa
Microfirewalls internos	Control de tráfico entre estaciones médicas

---

4.2 Política de Protección de Dispositivos IoMT

Justificación: La creciente digitalización de equipos médicos representa un vector de ataque crítico, poco protegido actualmente.

Acciones estratégicas:

- Inventario digitalizado de dispositivos conectados a la red (IoMT Scanner)
- Monitoreo continuo de comportamiento anómalo (análisis de tráfico con IA)
- Parches y firmware obligatorios cada trimestre
- Cifrado en la transmisión de datos médicos

4.3 Estrategia Antiransomware de Próxima Generación

Justificación: El ransomware continúa siendo la amenaza más rentable y devastadora para el sector salud.

Componentes propuestos:

Componente	Acción
Backups inmutables	Copias no modificables en AWS S3 con retención de 90 días
Segmentación de privilegios	Revisión y minimización de privilegios de escritura

Análisis heurístico	SIEM que identifique cifrados masivos o anomalías en disco
Simulacros de ataque	Ejecución de ejercicios Red Team/Blue Team cada semestre

---

5. Nuevas Políticas de Seguridad Interna (2025–2026)

Política	Descripción	Responsable	Frecuencia de Revisión
Política de Aislamiento de Redes Críticas	Separar redes clínicas, administrativas y de visitantes	Infraestructura TI	Anual
Política de Zero Trust Extendido	Aplicación completa de principios de desconfianza continua	Comité de Seguridad	Trimestral
Política de Backups Descentralizados	Replicación cifrada en nubes híbridas (AWS y GCP)	Líder DevOps	Semestral
Política de Evaluación de Proveedores Digitales	Estándares mínimos para contratación tecnológica externa	Jurídico + TI	Anual
Política de Simulación de Ataques	Ejercicios de respuesta ante ciberataques con personal real	Coordinador de Ciberseguridad	Semestral

---

6. Adopción de Nuevas Tecnologías de Ciberdefensa

Tecnología	Aplicación en CliniNova	Estado Propuesto
EDR (Endpoint Detection & Response)	Reemplazo de antivirus tradicional en estaciones clínicas	Piloto 2025Q4
CASB (Cloud Access Security Broker)	Control de acceso a sistemas médicos en la nube	Evaluación técnica
SOAR (Security Orchestration Automation & Response)	Automatización de respuesta ante alertas	Requiere inversión 2026
Honeypots clínicos	Servidores trampa para detectar accesos no autorizados	En diseño

---

7. Medición de Efectividad y KPIs Propuestos

Indicador	Meta 2026	Herramienta
Dispositivos IoMT con firmware actualizado	100%	Sistema centralizado de gestión
Incidentes detectados y contenidos en <10 min	95%	SIEM + Alertas vía correo y Teams
Cumplimiento de simulacros semestrales	100%	Registro firmado por dirección médica
Backups inmutables verificados mensualmente	100%	AWS Snapshot Logs
MFA aplicado a cuentas de proveedores externos	100%	Azure AD / Google Workspace

---

8. Conclusión

Las amenazas del mañana requieren una visión estratégica desde hoy. Este documento sienta las bases para que CliniNova S.A.S. no solo mantenga su nivel actual de seguridad, sino que lo eleve progresivamente hacia estándares de clase mundial.

La clave estará en combinar inversión tecnológica, políticas claras, automatización e involucramiento humano, siempre bajo una lógica de mejora continua. CliniNova se proyecta así como una institución médica no solo avanzada clínicamente, sino resiliente digitalmente.

Anexo A – Cuadro Comparativo de Estrategias Actuales vs Futuras

Elemento	Implementación Actual	Mejora Futura
MFA	En personal interno	Extendido a proveedores y visitantes
Backup	Local y nube	Inmutable, cifrado, multi-nube
Segmentación	Básica por áreas	Dinámica y microsegmentación
Cifrado	Solo en bases de datos	Extendido a tráfico y almacenamiento
Simulacros	Planificados una vez al año	Establecidos como política semestral

Título: Lecciones Aprendidas del Proyecto de Ciberseguridad

Empresa: CliniNova S.A.S.

Versión: 1.0
Ubicación: Barranquilla, Atlántico, Colombia
Fecha: Julio 2025
Elaborado por: Coordinación de Seguridad de la Información

2. Introducción

Los proyectos complejos como la implementación de una estrategia de ciberseguridad institucional no solo generan resultados técnicos y cuantificables; también ofrecen valiosas enseñanzas que permiten mejorar los procesos organizacionales y anticiparse a desafíos futuros.

El presente documento recopila las **lecciones aprendidas** del proyecto ejecutado entre mayo y julio de 2025 en CliniNova S.A.S., como parte del reto macro. Estas lecciones se clasifican en áreas técnicas, humanas, organizacionales y estratégicas, con el objetivo de fortalecer la madurez institucional en futuras iniciativas.

---

3. Factores de Éxito Identificados

Área	Factor Clave	Impacto
Dirección y liderazgo	Apoyo de gerencia general desde el inicio	Facilitó priorización presupuestal y tiempo del personal
Capacitación	Enfoque práctico, segmentado por roles	Aumentó el nivel de apropiación y responsabilidad del equipo
Coordinación	Uso de metodología ágil con entregas semanales	Permitió adaptación flexible a necesidades emergentes
Tecnología	Selección de soluciones compatibles con infraestructura existente	Evitó sobrecostos y permitió implementación inmediata
Comunicación	Canales abiertos (Teams, correo, sesiones híbridas)	Generó confianza y participación activa

---

4. Obstáculos Encontrados y Cómo se Superaron

Desafío	Descripción	Solución Adoptada
Baja conciencia inicial	Personal administrativo no veía riesgo digital como propio	Sesiones interactivas con ejemplos reales de phishing
Accesos compartidos	Algunos departamentos compartían cuentas de usuario	Implementación obligatoria de usuarios únicos y MFA

Infraestructura limitada	Algunos equipos médicos antiguos no permitían cifrado	Segmentación por VLAN y monitoreo de tráfico anómalo
Resistencia al cambio	Incomodidad con MFA y nuevas reglas de acceso	Envío de manuales impresos, asistencia técnica y soporte in situ
Multiplicidad de formatos	Historias clínicas dispersas entre múltiples plataformas	Centralización progresiva en sistema único de registros (EMR)

---

5. Lecciones Aprendidas Técnicas

1. **La automatización es esencial:**
   La implementación de tareas programadas para auditorías, backups y monitoreo de logs reduce drásticamente la dependencia humana y mejora la eficiencia.

2. **El principio de menor privilegio funciona:**
   Al limitar accesos y segmentar funciones, se disminuyó el riesgo de movimiento lateral ante una posible brecha.

3. **El cifrado por defecto es una práctica obligatoria:**
   Toda la información clínica sensible debe cifrarse tanto en tránsito como en reposo, sin depender de decisiones manuales.

4. **Los dispositivos médicos requieren una estrategia propia:**
   Muchos equipos en salud no cumplen estándares de seguridad actuales y deben ser gestionados como una red especial de alto riesgo.

---

6. Lecciones Organizacionales y Humanas

1. **Capacitar al personal no técnico con ejemplos reales genera más impacto**
   El personal respondió mejor a situaciones basadas en casos reales que a teoría abstracta.

2. **La ciberseguridad debe ser parte de la cultura organizacional, no solo del área TI**
   Desde enfermería hasta recepción, todos interactúan con sistemas digitales y tienen un rol en la defensa institucional.

3. **Los líderes influyen en la adopción de buenas prácticas**
   Los jefes que promovieron el uso de MFA o el reporte de correos sospechosos

mejoraron significativamente la adherencia en sus equipos.

---

7. Recomendaciones para Proyectos Futuros

Recomendación	Motivo	Responsable Sugerido
Integrar seguridad desde la planificación de nuevos sistemas	Evita retrabajo y vulnerabilidades	Coordinador de TI
Usar simulaciones de ataque antes de lanzar proyectos	Detecta fallas no visibles en auditorías	Red Team Interno / externo
Documentar todo cambio de configuración	Facilita auditorías futuras y recuperación	Administrador de Sistemas
Mantener un comité de seguridad institucional activo	Da continuidad a políticas y estrategias	Dirección General

---

8. Impacto Cultural del Proyecto

El cambio más profundo no fue únicamente técnico: CliniNova S.A.S. logró un cambio cultural. Antes del proyecto, los temas de ciberseguridad eran vistos como responsabilidad exclusiva del área técnica. Al cierre del proyecto, el personal reconocía:

- La importancia de verificar correos antes de hacer clic.
- La utilidad de usar MFA como medida de protección personal y laboral.
- El rol que cada uno juega en proteger los datos de los pacientes.

Este cambio de percepción es una de las lecciones más valiosas del proceso.

---

9. Conclusión

Las lecciones aquí documentadas son tanto una mirada crítica como una base de construcción. Al reflexionar sobre lo que funcionó, lo que se pudo hacer mejor y lo que se descubrió en el

camino, CliniNova S.A.S. no solo culmina un proyecto exitoso, sino que fortalece su capacidad para enfrentar nuevos desafíos.

El aprendizaje continuo debe institucionalizarse como una práctica permanente en la gestión de la seguridad de la información.

Anexo A – Lista de Recomendaciones Clave

Código	Recomendación	Prioridad	Responsable
REC-01	Definir presupuesto anual exclusivo para ciberseguridad	Alta	Dirección Financiera
REC-02	Evaluar proveedores según política de seguridad digital	Media	Compras + Jurídico
REC-03	Establecer un calendario permanente de simulacros de ataque	Alta	Seguridad Informática
REC-04	Elaborar protocolo de comunicación en caso de brechas	Media	Comunicaciones Corporativas
REC-05	Monitorear IA generativa y su impacto en la suplantación	Alta	Comité de Innovación

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

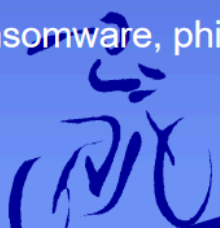
Semana	Actividad Principal	Reto Asociado
Semana 1	Evaluación de riesgos y activos críticos	Reto 1
Semana 2	Diseño de estrategia integral	Reto 2
Semana 3	Implementación de Firewalls, IDS/IPS y VPN	Reto 3
Semana 4	Gestión de accesos y MFA	Reto 4
Semana 5	Gestión de parches y seguridad en endpoints	Reto 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

DIAPOSITIVAS - ANALISIS

Objetivo del Proyecto (Reto Macro)

- Diseñar e implementar una estrategia integral de ciberseguridad para CliniNova S.A.S., simulando la protección de activos críticos en una empresa global del sector salud, bajo el enfoque de GlobalTech.

- - Protección de infraestructura TI distribuida.
- - Prevención de amenazas internas y externas.
- - Cumplimiento normativo (ISO 27001, normativas nacionales).
- - Simulación de escenarios reales (ransomware, phishing, fallas operativas).



Sesión 1 – Evaluación de Riesgos y Situación Actual

- Objetivos:
- - Comprender el entorno operativo y los activos de CliniNova.
- - Identificar amenazas y vulnerabilidades.
- - Aplicar NIST SP 800-30 y análisis FODA.

- Entregables:
- - Briefing Inicial – CliniNova.pdf
- - Inventario de Activos Críticos – CliniNova.xlsx
- - Evaluación de Riesgos – CliniNova.pdf
- - Análisis FODA – CliniNova.pdf

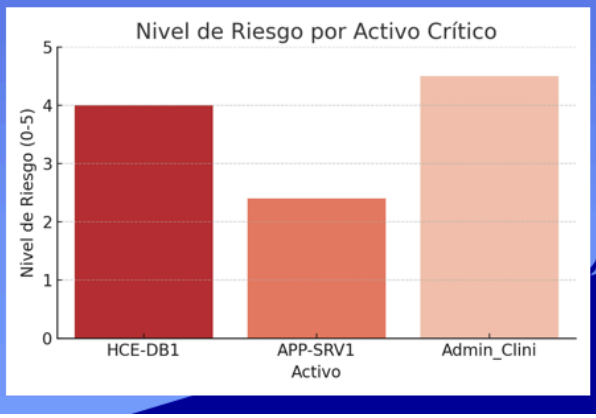
Briefing Inicial (CliniNova)

- Activos Identificados:
- - HCE-DB1 | Barranquilla | Base de datos historia clínica | Crítico
- - APP-SRV1 | Barranquilla | Aplicación de consulta externa | Crítico
- - Admin_Clini | Red interna | Cuenta administrativa TI | Crítico

- Amenazas Detectadas:
- - Ransomware dirigido a bases de datos clínicas.
- - Phishing a personal médico.
- - Accesos no autorizados por falta de MFA.

Inventario de Activos Críticos

- - HCE-DB1 | Barranquilla | Crítico | Operativo | Sin respaldo externo actualizado
- - APP-SRV1 | Barranquilla | Crítico | Activo | Software sin parches recientes
- - Admin_Clini | Red interna | Crítico | Activo | No se ha implementado MFA
- - BKP-HCE1 | Barranquilla | Alto | Obsoleto | Requiere actualización de hardware



Evaluación de Riesgos (NIST SP 800-30)

- - HCE-DB1 | Ransomware | 0.8 | 5 | 4.0 | Backup externo y pruebas de restauración
- - APP-SRV1 | Vulnerabilidad software | 0.6 | 4 | 2.4 | Aplicar parches y monitoreo continuo
- - Admin_Clini | Acceso no autorizado | 0.9 | 5 | 4.5 | Implementar MFA y monitoreo de accesos

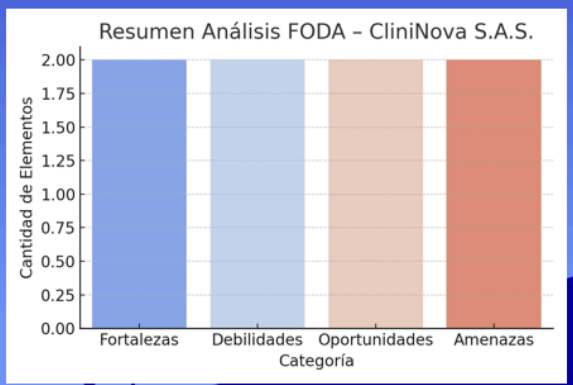
Análisis FODA – CliniNova S.A.S.

- Fortalezas:
- - Redundancia en infraestructura
- - Personal capacitado en TI

- Debilidades:
- - Falta de MFA en cuentas críticas
- - Backups incompletos

- Oportunidades:
- - Migración a Zero Trust
- - Automatización de auditorías

- Amenazas:
- - Phishing dirigido a personal clínico
- - Ransomware contra datos de pacientes



Conclusiones y Resultados Esperados

- - Identificación y clasificación de activos críticos realizada.
- - Evaluación de riesgos con NIST aplicada correctamente.
- - Recomendaciones implementables identificadas.
- - Base para definir estrategias técnicas en siguientes sesiones.

- Próximo paso: Diseñar controles y medidas con base en este diagnóstico.