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