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