Título: Estrategias de Seguridad Futura para CliniNova S.A.S.

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