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