SELECCION DE CONTROLES CRUZ ROJA

1.NORMAS RELEVANTES

Controles basados en ISO/IEC 27001

Controles Clave:

ID Control ISO 27001	Control	Aplicación en Cruz Roja
A.9.2.3	Gestión de privilegios de acceso	Implementar RBAC (Roles Based Access Control) para sistemas médicos y financieros.
A.12.4.1	Protección contra malware	Desplegar soluciones EDR (ej.: CrowdStrike) en dispositivos con datos sensibles.
A.18.1.2	Continuidad operativa (BCP)	Desarrollar un plan de recuperación ante desastres para centros de respuesta.
A.13.1.1	Cifrado de datos en tránsito/reposo	Usar TLS 1.3 y AES-256 para historiales médicos y donaciones.

Controles basados en NIST Cybersecurity Framework (CSF)

Ámbito: Protección de infraestructura crítica y gestión de Ciber RIESGOS.

Controles Clave (NIST CSF 1.1):

Categoría NIST	Control	Aplicación en Cruz Roja
PR.AC-1	Autenticación multifactor (MFA)	MFA obligatorio para acceso a sistemas de donantes y personal médico.
PR.DS-2	Respaldos automáticos	Backups diarios de bases de datos en ubicaciones seguras (ej.: AWS S3 con cifrado).
DE.CM-1	Monitoreo de redes	Implementar un SIEM (ej.: Splunk) para detectar intrusiones.

RS.RP-1	Respuesta a incidentes	Equipo CSIRT (Computer Security Incident Response Team) para ciberataques.

2. DOCUMENTAR LA IMPLEMENTACION DE CONTROLES

Tabla de Controles de Seguridad y Mitigación de Riesgos

Control	**Estándar de Referencia**	**Riesgo que Mitiga**	**Detalle de Implementación**	**Responsable**
Autenticación MFA	NIST CSF PR.AC-1 / CIS 6	Acceso no autorizado a sistemas críticos (ej.: historiales médicos).	Implementar MFA en todos los accesos remotos (ej.: Microsoft Authenticator, Duo Security). Bloqueo de cuentas tras intentos fallidos.	Equipo de Ciberseguridad
Cifrado de datos (AES-256/TLS)	ISO 27001 A.13.1.1 / NIST PR.DS-1	Robo o interceptación de datos sensibles (donantes, pacientes).	Cifrar datos en reposo (BitLocker) y en tránsito (TLS 1.3). Certificados SSL para sitios web.	TI/Infraestructura
Gestión de accesos (IAM/RBAC)	ISO 27001 A.9.2.3 / CIS 6	Privilegios excesivos o accesos obsoletos (ej.: excolaboradores).	Sistema IAM (ej.: Azure AD) con revisión trimestral de permisos. Roles basados en funciones (RBAC).	Auditoría Interna + TI
Inventario RFID de suministros	ISO 9001 / CIS 2	Pérdida o desabastecimiento de insumos médicos.	Uso de etiquetas RFID y software de tracking en tiempo real. Alertas por niveles mínimos de stock.	Logística
Protección contra malware (EDR)	ISO 27001 A.12.4.1 / CIS 8	Infecciones por ransomware o spyware.	Solución EDR (ej.: CrowdStrike) con monitoreo 24/7. Bloqueo de ejecutables no autorizados.	Ciberseguridad
Respaldos automáticos	NIST CSF PR.DS-2 / CIS 9	Pérdida de datos por ataques o desastres naturales.	Backups diarios en la nube (AWS S3) y local (discos cifrados). Pruebas de recuperación semestrales.	Operaciones TI

Plan de Continuidad (BCP)	ISO 27001 A.17.1.2 / NIST RS.RP-1	Interrupción de servicios críticos (ej.: centros de emergencia).	Documentar BCP con roles, sitios alternos y simulacros cada 6 meses.	Gerencia de Riesgos
Monitoreo con SIEM	NIST CSF DE.CM-1 / CIS 6	Detección tardía de intrusiones o anomalías.	Herramienta SIEM (ej.: Splunk) para correlacionar logs de redes y sistemas. Alertas automatizadas.	Equipo SOC
Capacitación en phishing	CIS 14 / ISO 27001 A.7.2.2	Filtración de credenciales por ingeniería social.		

3.PLANIFICACION DE LA IMPLEMENTACION

Fase	Controles Clave	Plazo	Recursos
Preparación	Gap analysis, sensibilización	Mes 1	Herramientas auditoría
Críticos	MFA, cifrado, IAM, backups	Meses 2-4	Duo/Azure AD, AWS S3
Operativos	EDR, hardening, RFID	Meses 5-8	CrowdStrike, WSUS, RFID
Monitoreo	SIEM, BCP, capacitación phishing	Meses 9-12	Splunk, simulacros, KnowBe4

Presupuesto: 120k–120k–240k EUR (software, capacitación, auditorías).

Riesgos: Presupuesto (priorizar MFA), resistencia (capacitación).

Entregables: Informes mensuales, manuales, certificaciones ISO.