Plan de implementación de controles de seguridad para UNICEF

1. Revisión de estándares y marcos relevantes

| **Estándar/Marco** | **Descripción general** | **Solicitud** | **Beneficios clave** | |---|---|---|---| | **ISO/IEC 27001: Sistema de Gestión de Seguridad de la Información (SGSI)** | Un estándar internacional para implementar, operar y mantener un SGSI para proteger información confidencial. | UNICEF adoptará el marco ISO/IEC 27001 para construir un SGSI integral que satisfaga las necesidades de sus operaciones a nivel mundial, abarcando registros médicos confidenciales, información de donantes y datos de protección infantil. | Crea una cultura de seguridad de la información unificada para toda la organización; reduce el riesgo de violaciones de datos e incumplimiento; mejora la confianza de las partes interesadas y la garantía global de protección de datos. | | **NIST SP 800-53: Controles de seguridad y privacidad para sistemas de información** | Un conjunto de controles federales de seguridad y privacidad diseñados para proteger los datos y sistemas de la organización durante todo su ciclo de vida. | UNICEF integrará controles NIST SP 800-53 para proteger los sistemas que administran datos confidenciales y garantizar la adopción de mejores prácticas en todas las plataformas tecnológicas, desde la seguridad de la red hasta la privacidad de los datos. | Se alinea con los estándares gubernamentales de EE. UU., proporciona pautas claras de ciberseguridad e integra la protección de la privacidad con medidas de seguridad operativas. | | **Controles CIS (Centro para la Seguridad de Internet)** | Un conjunto priorizado de mejores prácticas de ciberseguridad centrado en reducir los riesgos de los ciberataques prevalentes. | UNICEF implementará los Controles CIS 1-20, que van desde el inventario y el control de hardware y software hasta la respuesta y recuperación de incidentes, para mitigar las amenazas cibernéticas generalizadas. | Proporciona un conjunto de controles procesables y fáciles de implementar; altamente escalable para diferentes partes de la organización; promueve la resiliencia frente a las ciberamenazas más comunes y peligrosas. | | **RGPD (Reglamento General de Protección de Datos)** | Regulación de la UE que exige controles estrictos sobre la recopilación, el procesamiento y el almacenamiento de datos personales. | UNICEF cumplirá con las regulaciones GDPR en las regiones donde corresponda, particularmente en lo que respecta a los datos de los residentes de la UE, garantizando la transparencia, la seguridad y la responsabilidad en el manejo de datos. | Garantiza el cumplimiento legal en la UE, genera confianza con los donantes y las partes interesadas y evita multas elevadas mediante prácticas estrictas de protección de datos. |

---

2. Controles de seguridad detallados

| **Control** | **Riesgo abordado** | **Detalles de control** | **Estándares relevantes** | **Funciones y responsabilidades** | **Cronología** | |---|---|---|---|---|---|---| | **Autenticación multifactor (MFA)** | Acceso no autorizado debido a credenciales

comprometidas. | - Aplicar MFA en todos los sistemas críticos (por ejemplo, el sistema financiero global de UNICEF, portales de gestión de recursos humanos, registros de protección infantil).
- Factores requeridos: contraseña + OTP (a través de teléfono inteligente o token de hardware).
- Métodos de respaldo como el correo electrónico Se integrarán preguntas de verificación o seguridad para la recuperación. | ISO/IEC 27001 A.9.4.2, NIST 800-53 AC-2, Control CIS 16 | **Equipo de seguridad de TI**: Implementar y monitorear MFA.
Departamento de Recursos Humanos: Garantizar el cumplimiento de los empleados.
Operaciones de seguridad: Auditar la eficacia de la MFA y responder a los problemas. | Fase 1: Configuración de la solución (1 mes)
Fase 2: Implementación de MFA en toda la organización (2 meses)
Fase 3: Pruebas y ajustes (1 mes) | | **Cifrado de datos (en reposo y en tránsito)** | Violaciones de datos mediante acceso no autorizado o interceptación durante la transmisión/almacenamiento. | - Todos los datos confidenciales (registros médicos, datos de donantes, datos personales de los empleados) se cifrarán mediante cifrado AES-256 (en reposo) y cifrado TLS 1.2/1.3 (en tránsito).
- El sistema de gestión de claves (KMS) se cifrará de forma segura. Manejar claves de cifrado durante todo su ciclo de vida. | ISO/IEC 27001 A.10.1.1, NIST 800-53 SC-12, Artículo 32 del RGPD | **Equipo de seguridad de TI**: Implementar cifrado.
Equipos legales y de cumplimiento: Asegúrese de que los métodos de cifrado se ajusten al RGPD.
Equipo de operaciones: Audite periódicamente el estado de cifrado y la gestión de claves. | Fase 1: Selección de herramientas (1 mes)
Fase 2: Implementación (3 meses)
Fase 3: Implementación de gestión de claves (1 mes) | | **Firewalls y sistemas de detección/prevención de intrusiones (IDS/IPS)** | Amenazas basadas en la red, incluido el acceso no autorizado, malware y ataques DoS/DDoS. | - Implemente firewalls de próxima generación (NGFW) en los puntos de entrada de la red.
- Implemente IDS/IPS para detectar y prevenir intrusiones en tiempo real.
- Integre fuentes de inteligencia sobre amenazas para la detección proactiva de ataques. | NIST 800-53 AC-4, Control CIS 9, ISO/IEC 27001 A.13.1.1 | **Equipo de seguridad de red**: Configurar firewalls e IDS/IPS.
SOC: Supervise el tráfico de la red e identifique amenazas.
Administradores del sistema: Asegúrese de que los firewalls e IPS estén configurados y probados correctamente. | Fase 1: Instalación inicial (2 meses)
Fase 2: Actualizaciones periódicas y optimización del rendimiento (en curso) | | **Control de acceso basado en roles (RBAC)** | Acceso no autorizado debido a que no se aplica el control de acceso con privilegios mínimos. | - Implemente RBAC para todos los sistemas, garantizando que los usuarios tengan acceso solo a los datos necesarios para sus funciones.
- Aproveche Active Directory o LDAP para el control de acceso centralizado.
- Auditorías periódicas para garantizar que el acceso se mantenga en línea con las responsabilidades laborales. | NIST 800-53 AC-3, ISO/IEC 27001 A.9.1.1 | **Administradores del sistema**: Implementar políticas RBAC.
Departamento de Recursos Humanos: Comunicar cambios de roles de los empleados.
Equipo de seguridad: Audite los registros de acceso periódicamente para detectar accesos no autorizados. | Fase 1: Desarrollo de políticas (1 mes)
Fase 2: Implementación (2 meses)
Fase 3: Revisiones periódicas de acceso (Trimestralmente) | | **Copia de seguridad y recuperación ante desastres (DR)** | Pérdida de datos, tiempo de inactividad del sistema y tiempos de recuperación prolongados debido a incidentes como ciberataques, desastres naturales o fallas de hardware. | - Implemente copias de seguridad diarias automatizadas para el almacenamiento de datos tanto en el sitio como fuera del sitio.

- Diseñe y pruebe un Plan de recuperación ante desastres (DRP) integral, que garantice que los datos y sistemas de misión crítica se puedan restaurar en 4 horas (RTO).).
- Las pruebas de respaldo se realizarán trimestralmente. | ISO/IEC 27001 A.17.1.2, NIST 800-53 CP-9 |
Operaciones de TI: Administre sistemas de respaldo y garantice la disponibilidad.
Gestión de riesgos: Supervisar las pruebas de DRP.
Equipos de continuidad del negocio: Garantizar que DRP se alinee con las prioridades de la organización. | Fase 1: Evaluación de la solución de respaldo (1 mes)
Fase 2: Implementación (2 meses)
Fase 3: Pruebas y actualizaciones de DRP (3 meses) | | **Protección de endpoints (antivirus y antimalware)** | Amenazas de malware, virus, ransomware y otro software malicioso dirigido a puntos finales. | - Implementar soluciones antivirus y antimalware en todos los dispositivos terminales (estaciones de trabajo, portátiles, dispositivos móviles).
- Actualice y supervise periódicamente los terminales en busca de actividad maliciosa.
- Implemente sistemas de detección y respuesta de terminales (EDR) para amenazas continuas. escucha. | ISO/IEC 27001 A.12.2.1, NIST 800-53 SI-3 | **Equipo de seguridad de terminales**: Administre la implementación y la configuración.
SOC: Analice alertas de terminales e investigue actividades sospechosas.
Administradores del sistema: Asegúrese de que el software del terminal esté actualizado. | Fase 1: Selección de solución (1 mes)
Fase 2: Implementación de endpoints (3 meses)
Fase 3: Configuración y monitoreo de EDR (1 mes) | | **Información de seguridad y gestión de eventos (SIEM)** | Detección y respuesta inadecuada a eventos de seguridad. | - Implementar una solución SIEM para agregar, correlacionar y analizar registros de todos los dispositivos de red, firewalls, servidores y sistemas de protección de terminales.
- El SIEM permitirá la detección proactiva de amenazas y permitirá investigaciones forenses posteriores al incidente. | NIST 800-53 AU-6, ISO/IEC 27001 A.16.1.1 | **SOC**: Supervise y administre SIEM.
Equipo de seguridad de TI: Ajuste las reglas SIEM.
Administradores del sistema: Garantizar la integración de todos los sistemas con SIEM. | Fase 1: Implementación SIEM (2 meses)
Fase 2: Integración con sistemas (3 meses)
Fase 3: Monitoreo y ajustes (en curso) |

---

3. Monitoreo Continuo y Mejora Continua

| **Control** | **Actividades de seguimiento** | **Frecuencia** | |----------|-- ---------- ---------- ---------- ----------|----------| |
Autenticación multifactor (MFA) | Revise los intentos fallidos de inicio de sesión y controle los patrones de acceso sospechosos. | **A diario** | | **Cifrado de datos** | Realice auditorías de las claves de cifrado y supervise los registros para detectar accesos no autorizados o intentos de descifrado. | **Trimestral** | | **Cortafuegos e IDS/IPS** | Revise y analice registros en busca de intentos de intrusión y eventos de seguridad. | **Tiempo real** (24/7) | | **Control de acceso basado en roles (RBAC)** | Revise periódicamente los permisos de acceso de los usuarios y realice auditorías para detectar accesos no autorizados o asignaciones erróneas. | **Mensual** | | **Copia de seguridad y recuperación ante desastres (DR)** | Verifique el éxito de las copias de seguridad, realice pruebas de restauración y simule ejercicios de recuperación ante desastres para garantizar la preparación. | **Semanalmente** | | **Protección de terminales** | Supervise las alertas de los endpoints, analice los patrones de actividad maliciosa y asegúrese de que las actualizaciones de seguridad de los endpoints se

apliquen con prontitud. | **A diario** | | **Monitoreo SIEM** | Revise registros agregados en busca de anomalías, investigue incidentes y correlacione datos en múltiples sistemas para realizar un análisis preciso. | **24 horas al día, 7 días a la semana** |

---

4. Mejora Continua

| **Actividad** | **

Descripción** | **Frecuencia** | |----------|- ---------- ---------- ---------- ---------- ----------|----------| | **Auditorías de seguridad** | Realizar auditorías de seguridad trimestrales y evaluaciones de vulnerabilidad para verificar la efectividad de las medidas de seguridad. | **Trimestral** | | **Capacitación en seguridad para empleados** | Formación semestral sobre sensibilización en ciberseguridad, prevención de phishing, gestión de contraseñas y cumplimiento del RGPD. | **Bienal** | | **Simulacros de respuesta a incidentes** | Simule escenarios de ciberataques del mundo real para evaluar la capacidad de UNICEF para responder, recuperarse y prevenir amenazas futuras. | **Anualmente** | | **Gestión de riesgos de terceros** | Evalúe y audite periódicamente a proveedores y contratistas externos para determinar el cumplimiento de la ciberseguridad y las medidas de protección de datos. | **Anualmente** | | **Fuentes de inteligencia sobre amenazas** | Incorpore fuentes de inteligencia de amenazas globales en SIEM y otros sistemas para adelantarse a las amenazas cibernéticas emergentes. | **En curso** |