Alcance del Sistema de Gestión de Seguridad de la Información (SGSI) de UNICEF

---

1. Identificar activos de información (alcance global)

1.1 Inventario de Activos de Información

Computadoras y dispositivos

- **Portátiles y ordenadores de sobremesa**:
- **Serie Dell Latitude**, **Serie HP EliteBook**, **Apple MacBook Pro/iMac** (utilizado por personal superior).
- **Sistemas operativos**:
  - **Windows 10/11**: Sistema operativo principal a nivel mundial.
  - **macOS**: Para directivos superiores y personal especializado (por ejemplo, directores de programas).
  - **Linux (Ubuntu)**: Utilizado por algunos equipos técnicos en regiones con necesidades de procesamiento de datos a gran escala.
- **Herramienta de gestión**: Los dispositivos se administran y rastrean mediante **Microsoft Intune** para la seguridad, el inventario y el cumplimiento de los dispositivos.

Dispositivos móviles

- **Teléfonos inteligentes**:
- **Modelos Apple iPhone 12/13/14** para el personal del programa en países clave como **India**, **Nigeria**, **Siria**, y **Sudán del Sur**.
- **Dispositivos Samsung Galaxy** para regiones de América Latina y países con infraestructura móvil orientada a Android.
- **Gestión Móvil**: Dispositivos registrados y asegurados mediante **VMware AirWatch** para cifrado, borrado remoto y acceso seguro a los sistemas de UNICEF.

Servidores y bases de datos

- **Centros de datos globales**:
- **Nueva York (sede)**: Centro de datos primario para operaciones globales internas.
- **Ginebra (Europa)**: Gestiona las operaciones y el almacenamiento de datos para las operaciones europeas, MENA y algunas de Asia y el Pacífico.
- **Oficinas Regionales** (p.ej., **Bangkok**, **Nairobi**, **San José**): Para necesidades de gestión de datos locales y recuperación ante desastres.
- **Infraestructura en la nube**:
- **AWS (servicios web de Amazon)**:
  - **instancias EC2** (Máquinas virtuales): alberga operaciones globales y sistemas de respuesta a emergencias.

    - **T3** (Servicio de almacenamiento simple): almacena grandes conjuntos de datos para programas de ayuda de emergencia, salud infantil y educación a nivel mundial.
    - **RDS** (Servicio de base de datos relacional): aloja bases de datos de misión crítica como **Bases de datos de donantes, educación y salud de UNICEF**.

- **MicrosoftAzure**:
- **Almacenamiento de blobs de Azure**: Se utiliza para almacenar datos financieros y de donantes confidenciales.
- **Azure AD** (Active Directory): Gestión centralizada de identidades y accesos para todos los usuarios a nivel global.

Aplicaciones y software

- **Informe U**: Una herramienta de mensajería social para la participación de los jóvenes en más de 50 países (incluidos **Kenia**, **Nigeria**, **Indonesia**).
- **Cuidado de comunicaciones**: Una aplicación móvil para la recopilación de datos de campo, utilizada en emergencias (p. ej., **Yemen**, **Sudán del Sur**).
- **Salesforce CRM**: Para gestionar donaciones globales y relaciones con los donantes.
- **Salvia intacta**: Sistema financiero para seguimiento de presupuestos y donaciones en todo el mundo.

---

2. Definir límites físicos

2.1 Ubicaciones físicas incluidas en el SGSI

- **Sede de UNICEF**:
- **Nueva York, EE.UU.**: La oficina principal donde se toman las decisiones estratégicas, financieras y operativas globales.
- **Oficinas Regionales**:
- **Ginebra, Suiza**: El centro de operaciones europeo, que cubre Europa, Oriente Medio y Asia Central.
- **Bangkok, Tailandia**: Gestiona las operaciones para la región de Asia Pacífico.
- **Nairobi, Kenia**: Maneja las operaciones para África Oriental.
- **San José, Costa Rica**: Responsable de programas de América Latina y el Caribe.
- **Oficinas de país**:
- **India**: Almacenamiento seguro de datos y operaciones para el sur de Asia (salud, educación, programas WASH).
- **Nigeria**: Centros de datos en **Abuja**, gestionando datos para África Occidental.
- **Siria**: Datos críticos almacenados localmente bajo protocolos de alta seguridad debido a un conflicto en curso.

2.2 Áreas Restringidas

- **Salas de servidores**: Ubicado en oficinas regionales y centros de datos nacionales (p. ej., **Bangkok**, **Ginebra**, **Nairobi**) con acceso restringido y vigilancia. La entrada está autorizada sólo para administradores del sistema.

---

3. Definir límites virtuales

3.1 Seguridad de la red

- **WAN global de UNICEF**: Red de área amplia segura que conecta oficinas regionales, servicios en la nube y centros de datos en todo el mundo.
- **Redes de área local (LAN)**: En oficinas regionales como **Bangkok** y **Nairobi** para garantizar la protección local de datos confidenciales.

3.2 Entornos de nube

- **Servicios web de Amazon (AWS)**:
- **Región**: Virginia del Norte (EE.UU.), Irlanda (Europa), Singapur (Asia), Sydney (Australia).
- **Servicios utilizados**: EC2, S3, Lambda, CloudFront para aplicaciones en la nube escalables.
- **MicrosoftAzure**:
- **Región**: Países Bajos, Irlanda y América del Norte.
- **Servicios**: Azure Blob Storage para datos financieros y confidenciales, Microsoft Teams y Office 365 para colaboración y gestión de documentos.

3.3 Sistemas de Seguridad

- **Cortafuegos**: Firewalls de nivel empresarial de **Fortinet** y **Cisco** para proteger el tráfico de red interno y externo.
- **VPN**: **Cisco AnyConnect** Servicio VPN para acceso remoto seguro a los sistemas de UNICEF en todo el mundo.

---

4. Identificación de partes interesadas

4.1 Partes interesadas clave

- **Gestión Ejecutiva**:

- **Sede de UNICEF en Nueva York**: Garantiza la alineación con los objetivos organizacionales y prioriza la seguridad de la información en todas las regiones.

- **Equipo de TI global**:

- Con base en **Nueva York**, responsable de supervisar todas las políticas de ciberseguridad, evaluaciones de riesgos y monitoreo del cumplimiento de estándares globales como **ISO 27001**.

- **Equipos regionales de TI**:

- **Ginebra**, **Bangkok**, **Nairobi**, **Amán**, y **San José**: Los equipos específicos de la región gestionan implementaciones locales, capacitación del personal y generación de informes.
- **Proveedores externos**:
- **AWS**, **MicrosoftAzure**, **Google Nube**: Administrar la infraestructura de la nube.
- **Consultores de seguridad**: Trabajar con **KPMG**, **Deloitte** para pruebas de penetración y auditorías.

---

5. Cronograma de implementación del SGSI

5.1 Fase 1: Planificación y evaluación de riesgos (1 a 3 meses)

- **Tareas**:
- Complete una evaluación de riesgos integral de los sistemas, la infraestructura y los datos existentes.
- Identificar activos de información clave, clasificándolos según **confidencialidad**, **integridad**, y **disponibilidad**.
- Diseñar la arquitectura ISMS en alineación con **ISO 27001** estándares.
- **Productos clave**:
- Informe inicial de evaluación de riesgos.
- Alcance documentado del SGSI.
- Roles y responsabilidades asignados para la ejecución del SGSI.

5.2 Fase 2: Desarrollo de políticas e implementación de controles (3 a 6 meses)

- **Tareas**:
- Desarrollar e implementar políticas de seguridad de la información que cubran control de acceso, protección de datos, respuesta a incidentes y recuperación ante desastres.
- Configurar soluciones de seguridad como **protección de terminales (CrowdStrike)**, **cortafuegos (Fortinet)**, y **autenticación multifactor**.
- Crear pautas para el acceso al trabajo remoto y las operaciones de campo (por ejemplo, usando **Reloj aéreo** para la gestión de dispositivos).
- **Productos clave**:
- Políticas de seguridad publicadas.
- Sistemas de seguridad configurados.
- Programas de sensibilización al personal sobre procedimientos de seguridad.

5.3 Fase 3: Capacitación y concientización (6 a 9 meses)

- **Tareas**:
- Llevar a cabo sesiones obligatorias de capacitación en seguridad para todo el personal en **phishing**, **gestión de contraseñas**, y **reporte de incidentes**.
- Actualice periódicamente la capacitación en función de las amenazas emergentes (por ejemplo, seminarios web de seguridad trimestrales).
- Pruebe la concienciación del personal con campañas de phishing simuladas.
- **Productos clave**:
- Módulos de capacitación completados para todo el personal.
- Informes de simulación y resultados de evaluación.

5.4 Fase 4: Auditorías de seguridad y respuesta a incidentes (9 a 12 meses)

- **Tareas**:
- Realice evaluaciones periódicas de vulnerabilidades y pruebas de penetración con proveedores de seguridad externos.
- Implementar un sistema centralizado **Información de seguridad y gestión de eventos (SIEM)** sistema como **Splunk** para monitorear registros y detectar amenazas de seguridad en tiempo real.
- Pruebe los planes de respuesta a incidentes simulando ciberataques o filtraciones de datos.
- **Productos clave**:
- Informes de auditoría finalizados.
- Procedimientos de respuesta a incidentes.
- Sistema SIEM configurado y activo.

5.5 Fase 5: Mejora continua y seguimiento (en curso)

- **Tareas**:
- Actualice periódicamente las políticas de SGSI y las medidas de seguridad para reflejar nuevas amenazas.
- Monitoreo continuo con **Splunk**, **Ataque multitudinario**y evaluaciones periódicas de vulnerabilidad.
- Revisión y ajustes anuales del SGSI.
- **Productos clave**:
- Documentación SGSI actualizada.
- Informes anuales de auditoría y actualizaciones sobre cumplimiento.
- Programas continuos de formación y sensibilización del personal.

---

6. Cumplimiento y consideraciones legales

- **ISO 27001**: El SGSI se adherirá a **ISO 27001** estándares para establecer, mantener y mejorar el sistema de gestión de seguridad de la información.
- **RGPD**: Cumplimiento de las **Reglamento General de Protección de Datos (GDPR)** para cualquier operación que implique datos de ciudadanos de la UE.
- **Otras regulaciones locales**: Cumplimiento de las leyes locales de protección de datos en regiones como **África (NDPR de Nigeria)**, **América Latina (LGPD de Brasil)**, y **Asia (PDPB de la India)**.