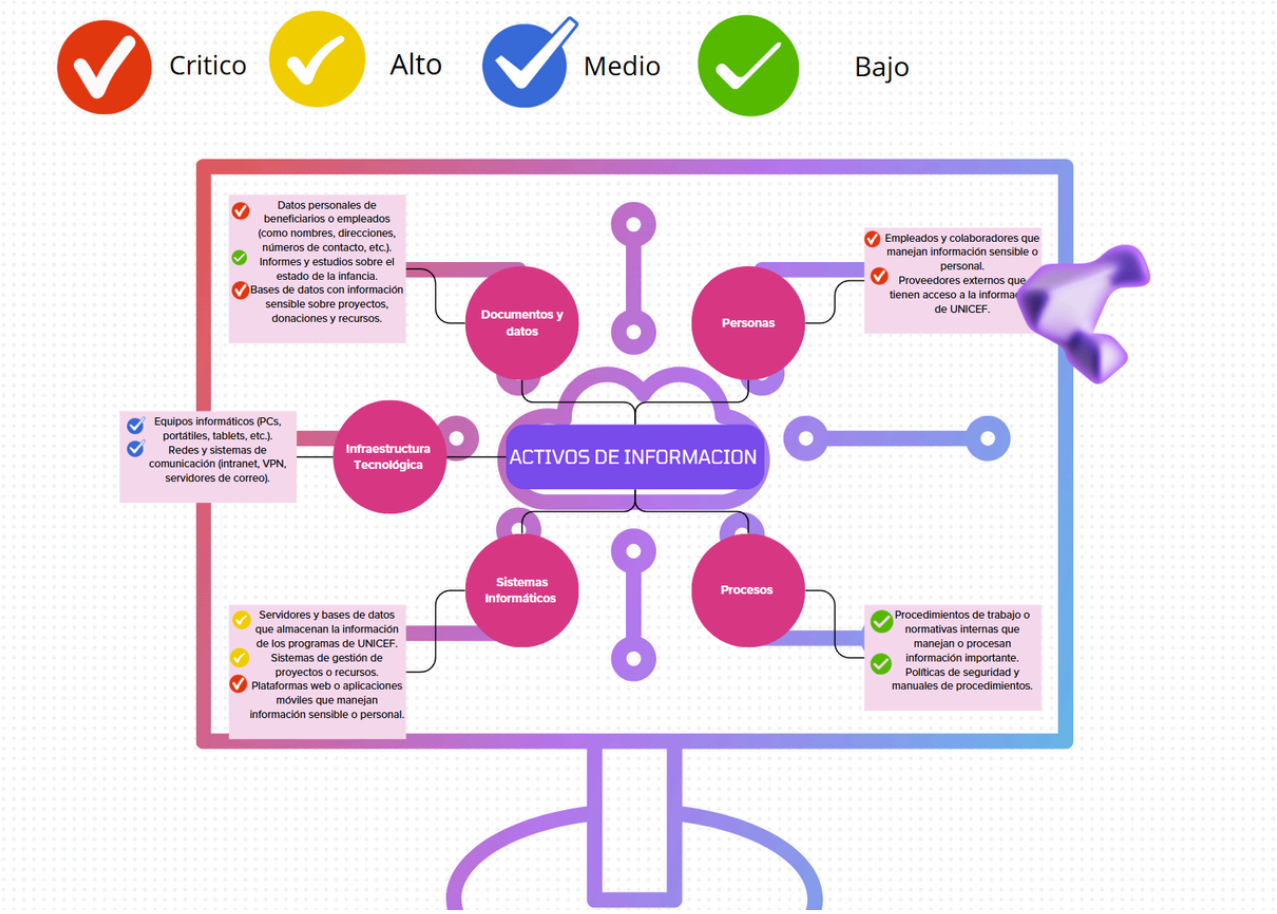
EVALUACIÓN DE RIESGOS



Inventario

Hardware	Software	Datos	Personal
x140 HP Slim Desktop S01-pF2044ns Intel Core i3-12100/8GB/256GB SSD	Microsoft 365 (Office)	Donantes	Alta Dirección (Directores)
x140 Monitor MSI PRO MP225 21.5" LED IPS FullHD 100Hz	Google Workspace	Finanzas	Personal IT
x4 Lenovo ThinkSystem ST250 V2 (7D8FA01YEA)	Microsoft Azure	Beneficiarios	Equipo de Proyectos
6TP-Link Archer AX12 Router AX1500 Wi-Fi 6 Dual Band	Fortinet	Empleados	Personal de Recursos Humanos
x4 TP-Link TL-SG116 Gigabit Ethernet de 16 Puertos (Conmutador no Gestionado, Plug and Play, Metal, Escritorio, Montaje en Bastidor, sin Ventilador, Vida ÚTI Limitada)	Adobe Acrobat Pro	Proyectos	Personal de Comunicación
x2 DIGITUS Armario de red - rack de 19 pulgadas - 7 U - montaje en la pared - profundidad 450 mm - capacidad de carga 60 kg - serie	VeraCrypt	Comunicación	Voluntarios

Dynamic Basic - Negro			
x12 HP Color LaserJet Pro MFP 3302sdw Multifunción Láser Color WiFi Dúplex	Wazuh	Auditorias y cumplimiento normativo	
	Wireshark	Datos médicos	
	Windows 11 Pro		
	Windows Server		

Vulnerabilidades identificadas

1. **Falta de cifrado de datos sensibles**
   - **Activos afectados**: Datos de donantes, alta dirección, finanzas, beneficiarios, comunicación, datos médicos.
   - **Descripción**: Si los datos confidenciales almacenados en sistemas o servicios no están cifrados (como los datos médicos, donantes o información financiera), podrían ser accesibles en caso de una violación de seguridad.
   - **Impacto potencial**:
     - **Pérdida financiera**: Compromiso de datos de donantes o transacciones financieras.
     - **Daño reputacional**: La exposición de datos de beneficiarios o personal clave podría dañar la imagen pública de UNICEF.
     - **Compromiso de datos sensibles**: Pérdida de confianza de las partes interesadas.
2. **Contraseñas débiles o sin política de autenticación robusta**
   - **Activos afectados**: Microsoft 365, Google Workspace, Fortinet, VeraCrypt, servidores Windows.
   - **Descripción**: Si no se usan contraseñas fuertes o autenticación multifactor (MFA) en sistemas críticos como los servicios de colaboración en la nube (Microsoft 365, Google Workspace), redes (Fortinet) o sistemas de cifrado (VeraCrypt), los atacantes podrían acceder a datos confidenciales.
   - **Impacto potencial**:
     - **Acceso no autorizado**: Un atacante podría obtener acceso a redes, archivos cifrados, o bases de datos internas.
     - **Interrupción operativa**: Pérdida de control sobre las infraestructuras críticas, lo que interrumpe operaciones y comunicaciones.
     - **Daño reputacional y sanciones**: Si se expone información confidencial de terceros (donantes, beneficiarios), la organización podría enfrentar consecuencias legales y perder la confianza pública.
3. **Sistemas desactualizados o sin parches de seguridad**
   - **Activos afectados**: Windows 11 Pro, Windows Server, routers TP-Link Archer AX12, switches TP-Link TL-SG116, hardware HP.

- **Descripción**: Si los sistemas no reciben actualizaciones y parches de seguridad regularmente, pueden ser vulnerables a exploits y malware.
- **Impacto potencial**:
  - **Compromiso de la red**: Malware o ransomware podría propagarse por la red interna, afectando operaciones críticas.
  - **Pérdida de disponibilidad**: Los servidores podrían ser vulnerables a ataques de denegación de servicio (DoS), interrumpiendo el acceso a servicios clave.
  - **Pérdida de datos**: Los sistemas infectados podrían provocar la pérdida de datos sensibles si no están correctamente respaldados.

4. **Falta de segmentación de red**
   - **Activos afectados**: TP-Link routers y switches, servidores Lenovo ThinkSystem, armarios de red.
   - **Descripción**: Si no se segmenta adecuadamente la red, una vulnerabilidad en un área (por ejemplo, un servidor comprometido) podría propagarse fácilmente a otros sistemas o redes críticas.
   - **Impacto potencial**:
     - **Compromiso total de la infraestructura**: Un fallo en la segmentación permitiría a los atacantes moverse lateralmente a través de la red, comprometiendo múltiples activos.
     - **Daño operacional**: Si se comprometen múltiples sistemas, la recuperación será más compleja y costosa.
5. **Mal uso o configuración incorrecta de herramientas de seguridad**
   - **Activos afectados**: Fortinet, VeraCrypt, Wazuh, Wireshark.
   - **Descripción**: Si las herramientas de seguridad no están configuradas correctamente (por ejemplo, Wazuh para auditorías y cumplimiento normativo), no ofrecerán la protección adecuada o incluso podrían abrir nuevas vulnerabilidades.
   - **Impacto potencial**:
     - **Falsa sensación de seguridad**: La organización podría creer que está protegida, pero las configuraciones deficientes podrían dejar expuestos datos o sistemas.
     - **Incumplimiento de normativas**: Si no se configuran adecuadamente las herramientas de cumplimiento (como Wazuh), la organización podría no cumplir con las normativas de seguridad de datos, lo que conlleva sanciones.

Evaluación del Impacto Potencial en la Organización

1. **Pérdida financiera**:
   - Exposición de datos financieros o compromisos con donantes puede derivar en pérdida de fondos, fraudes o transacciones no autorizadas. La interrupción operativa por ataques también podría generar costos significativos para la recuperación.
2. **Daño a la reputación**:
   - UNICEF maneja información crítica de donantes, beneficiarios y socios. Si estos datos se ven comprometidos, la confianza de las partes interesadas se verá gravemente afectada, poniendo en peligro futuras colaboraciones y donaciones.
3. **Compromiso de datos sensibles**:
   - La exposición de información personal de beneficiarios, como datos médicos o financieros, puede tener graves repercusiones, tanto para las personas involucradas como para la organización, lo que podría derivar en acciones legales.

4. **Interrupción operativa**:
    - Un ataque a la infraestructura o a los servidores de proyectos clave podría paralizar operaciones importantes, afectando las misiones humanitarias y la prestación de servicios, lo que genera un impacto directo en las personas que dependen de las acciones de UNICEF.
5. **Sanciones regulatorias**:
    - Si los datos sensibles no se protegen adecuadamente, la organización podría enfrentar sanciones legales, especialmente en contextos con regulaciones estrictas como el RGPD (Reglamento General de Protección de Datos) en Europa o leyes de privacidad en otras regiones.