Riesgos para las operaciones globales de UNICEF

---

1. Inventario de activos con cantidades y ubicaciones específicas

1.1 Activos de hardware

- **Portátiles y ordenadores de sobremesa**:
- **Serie Dell Latitude (5000, 7000, 9000)** y **Serie XPS**:
  - **Cantidad**: ~12.000 unidades.
  - **Uso principal**: Personal administrativo, operaciones de oficina, funciones generales de los empleados.
  - **Distribución geográfica**:
    - **Sede**: **Nueva York**, **Ginebra**, **Nairobi**, **Bangkok**, **El Cairo**
    - **Oficinas Regionales**: En lugares clave como **Ciudad de México**, **Abuja (Nigeria)**, **Bangladés**, **Zimbabue**, y **Sudáfrica**.
    - **Otras ubicaciones**: Oficinas de país en Asia, Europa y América Latina.
- **HP EliteBook** y **HP ProBook**:
  - **Cantidad**: ~10.000 unidades.
  - **Uso principal**: Personal de campo, personal operativo en zonas de alto riesgo, trabajadores de salud, educación y respuesta a emergencias.
  - **Distribución geográfica**:
    - **Zonas de conflicto**: **Sudán del Sur**, **Siria**, **Afganistán**, **Yemen**, **Haití**, **Colombia**.
    - ** Regiones en desarrollo **: **Bangladés**, **Etiopía**, **Nigeria**.
    - **Operaciones de campo**: En áreas volátiles o remotas con necesidades urgentes de ejecución de programas.
- **Apple MacBook Pro**:
  - **Cantidad**: ~3.000 unidades.
  - **Uso principal**: Alta dirección, desarrolladores de TI, equipos especializados (investigación, análisis de salud, gestión de crisis).
  - **Distribución geográfica**: **Nueva York**, **Ginebra**, **Singapur**, y **Sede (oficinas regionales)**.
- **Lenovo ThinkPad**:
  - **Cantidad**: ~2.000 unidades.
  - **Uso principal**: Trabajo basado en proyectos en oficinas de campo desafiantes con un enfoque en operaciones remotas y temporales.
  - **Distribución geográfica**: Principalmente en **África**, **Asia**, y **América Latina**.

Total de computadoras portátiles/de escritorio: ~25.000 unidades.

1.2 Dispositivos móviles

- **Apple iPhone 12, 13, 14 Pro Max**:
- **Cantidad**: ~5.000 unidades.
- **Uso principal**: Dispositivos móviles esenciales para el personal de campo en zonas remotas o de alto riesgo que requieren comunicación segura en tiempo real.
- **Distribución geográfica**: **Sudán del Sur**, **Siria**, **Afganistán**, **Colombia**, **Yemen**.

- **Samsung Galaxy S20/S21**:
- **Cantidad**: ~8.000 unidades.
- **Uso principal**: Comunicación móvil para operaciones en regiones en desarrollo y entornos de emergencia.
- **Distribución geográfica**: **Bangladés**, **Sudáfrica**, **Nepal**, **India**, **Zambia**.
- **Apple iPad (modelos 10.2 y Pro)**:
- **Cantidad**: ~7.500 unidades.
- **Uso principal**: Recopilación de datos y prestación de servicios en educación, salud y protección infantil.
- **Distribución geográfica**: **Bangladés**, **Uganda**, **Haití**, **India**, **Siria**.

Total de dispositivos móviles: ~20.500 unidades.

1.3 Dispositivos externos (unidades USB, discos duros externos)

- **Unidades flash USB (32 GB - 512 GB)** y **Discos duros externos (1TB - 5TB)**:
- **Cantidad**: ~20.000 unidades.
- **Uso principal**: Almacenamiento y transferencia de datos operativos, de salud y de respuesta a emergencias confidenciales donde la conectividad a Internet no es confiable.
- **Distribución geográfica**: Utilizado principalmente en **Sudán del Sur**, **Siria**, **Yemen**, **RDC**, y **Haití**.
- **Dispositivos de almacenamiento conectados a la red (NAS)**:
- **Cantidad**: ~500 TB de almacenamiento.
- **Uso principal**: Respaldos de datos para operaciones de campo, salvaguardando información crítica durante crisis regionales.
- **Distribución geográfica**: Principalmente en **Nairobi**, **Bangkok**, **Ginebra**y otras oficinas regionales.

Total de dispositivos externos: ~20.000 unidades.

1.4 Centros de datos y servidores

- **Centros de datos físicos**:
- **Nueva York, EE.UU.**:
  - **Servidores**: 3 servidores físicos, capacidad total de almacenamiento de **20TB**.
  - **Uso principal**: Almacenamiento y alojamiento de datos operativos para sistemas financieros, datos operativos regionales para América del Norte.
- **Ginebra, Suiza**:
  - **Servidores**: 2 servidores físicos, capacidad total de almacenamiento de **15TB**.
  - **Uso principal**: Almacenamiento de datos sanitarios y humanitarios, gestión de programas europeos y de Oriente Medio.
- **Nairobi, Kenia**:
  - **Servidores**: 2 servidores físicos, capacidad total de almacenamiento de **10TB**.

    - **Uso principal**: Operaciones en África Oriental, incluidos programas de protección, salud y educación infantil.
- **Bangkok, Tailandia**:
    - **Servidores**: 2 servidores físicos, capacidad total de almacenamiento de **10TB**.
    - **Uso principal**: Programas de respuesta a emergencias de Asia y el Pacífico, operaciones de socorro y almacenamiento de datos para programas regionales.

Total de servidores físicos: 9 servidores con **55TB** de datos almacenados.

1.5 Infraestructura basada en la nube

- **Servicios web de Amazon (AWS)**:
- **500 instancias EC2**: Activo para necesidades de procesamiento y computación de datos en operaciones globales.
- **Almacenamiento S3 de 250 TB**: Para almacenar datos operativos, información de donantes, datos de salud infantil y materiales educativos.
- **75 bases de datos RDS**: Se utiliza a nivel mundial para gestionar los sistemas operativos de UNICEF (sistemas financieros, programáticos y de recursos humanos).
- **MicrosoftAzure**:
- **25.000 usuarios activos**: Gestionado a través de Azure Active Directory, representando al personal de UNICEF en todo el mundo.
- **30 bases de datos SQL**: Para alojar sistemas operativos críticos, incluidos recursos humanos, finanzas y aplicaciones programáticas.
- **Almacenamiento de blobs de 50 TB**: Se utiliza para la recuperación ante desastres y para almacenar datos confidenciales del programa, incluidos registros de respuesta a emergencias y datos de bienestar infantil.
- **Google Nube**:
- **Almacenamiento en la nube de 100 TB**: Para investigación y almacenamiento de datos, particularmente para datos de educación y salud infantil en todo **Asia-Pacífico**.

---

2. Activos de software

2.1 Aplicaciones desarrolladas por UNICEF

- **Informe U**:
- **Usuarios activos**: ~200.000 usuarios.
- **Uso principal**: Una herramienta para involucrar a los jóvenes y recopilar datos críticos en tiempo real de más **50 países** en África, Asia y América Latina.
- **Cuidado de comunicaciones**:
- **Usuarios activos**: ~15.000 usuarios.

- **Uso principal**: Aplicación móvil utilizada en **30+ países** para la recopilación de datos en programas de salud, educación y bienestar infantil.
- **fuerza de ventas**:
- **Usuarios activos**: ~2.500 usuarios.
- **Uso principal**: Para relaciones con donantes, recaudación de fondos y comunicación, particularmente en grandes campañas de recaudación de fondos como **Martes de donaciones**.
- **Salvia intacta**:
- **Usuarios activos**: ~1.000 usuarios.
- **Uso principal**: Gestión e informes financieros para el seguimiento de donaciones, subvenciones y financiación gubernamental.
- **Prometido**:
- **Usuarios activos**: ~500 usuarios.
- **Uso principal**: Sistema de gestión de activos y logística, utilizado globalmente por el personal de campo para gestionar suministros.

---

3. Activos de datos

3.1 Datos personales sensibles

- **Datos de niños**:
- **~10 millones de registros** de datos confidenciales sobre niños, familias y comunidades, que abarcan datos de salud, educación y asistencia de emergencia.
- **Ubicaciones de almacenamiento principales**: AWS, Azure y Google Cloud, con una infraestructura distribuida en oficinas globales.

3.2 Datos de investigación

- **Datos de investigación anuales**:
- Recogido de **5 millones de niños** anualmente en áreas como salud, educación, pobreza y desarrollo.
- Los datos informan **Informes sobre el estado mundial de la infancia**, anual **evaluaciones educativas**y otras investigaciones humanitarias globales.

3.3 Datos financieros

- **Donaciones anuales**:
- **~$6 mil millones** rastreado globalmente usando **fuerza de ventas** y **Salvia intacta**.
- **Usuarios financieros globales**: ~1.000 usuarios financieros en varias oficinas de UNICEF en los países.

---

4. Personal y socios externos

4.1 Empleados

- **Empleados totales**: 15.000 empleados repartidos en **190 oficinas en los países** mundial.
- **Áreas clave de trabajo**: Operaciones de campo, logística, salud, educación, protección infantil, respuesta a emergencias y desarrollo de políticas.

- **Riesgos de ciberseguridad**: Empleados en regiones remotas o de alto riesgo como **Sudán del Sur**, **Siria**, y **Venezuela** pueden ser más vulnerables a ataques de phishing o ingeniería social.

4.2 Socios y proveedores externos

- **Contratistas externos**:
- Miles de contratistas que trabajan en zonas de conflicto y poscrisis, incluidas **Sudán del Sur**, **Siria**, **Afganistán**, y **Yemen**.
- Las tareas incluyen la coordinación de la respuesta a emergencias, el apoyo logístico y los servicios de TI.
- **Proveedores de servicios de TI**:
- Servicios de TI gestionados proporcionados por **AWS**, **Microsoft**, **fuerza de ventas**, y **Google**.

---

5. Identificación de amenazas y análisis de impacto

5.1 Amenazas externas

- **Amenazas de ciberseguridad**:
- **Suplantación de identidad**: Alto

probabilidad de intentos de phishing, especialmente dirigidos al personal con acceso a bases de datos y sistemas operativos de donantes.

- **ransomware**: Mayor riesgo de ataques de cifrado de datos, especialmente en datos financieros relacionados con donantes o datos de campo (salud, educación).
- **Ataques DDoS**: Riesgo potencial para las plataformas de recaudación de fondos en línea durante los períodos de máxima donación, como **Martes de donaciones** o campañas navideñas.
- **Violación de datos**: Alto riesgo en zonas de conflicto, donde la infraestructura digital puede verse comprometida.
- **Desastres naturales**:
- **Inundaciones, terremotos, huracanes** que afectan a los centros de datos y las oficinas de campo, especialmente en áreas como **Asia del Sur**, **América Latina**, y **Caribe**.

5.2 Amenazas internas

- **Amenazas internas**: Riesgo de personal interno o contratistas que pueden hacer un mal uso o filtrar datos confidenciales, particularmente en entornos de crisis o de alto estrés.
- **Error humano**: Pérdida o eliminación accidental de datos, particularmente en respuesta a emergencias u operaciones de campo donde el manejo de datos es manual y urgente.

---

6. Evaluación de riesgos y priorización

| **Riesgo** | **Probabilidad** | **Impacto** | **Calificación de riesgo** | **Detalles** | |----------|----------- ------|----------|----------|----------- -| | **Ataques de phishing** | Alto | Alto | **Alto** | Los ataques de phishing son una de las amenazas de ciberseguridad más frecuentes a las que se enfrentan organizaciones internacionales como UNICEF. Estos ataques aprovechan el error humano para obtener acceso a información confidencial a través de correos electrónicos engañosos o sitios web falsos. La estructura descentralizada de UNICEF, con un gran número de oficinas sobre el terreno en zonas de conflicto y áreas de alto riesgo, lo convierte en un objetivo principal para los ciberdelincuentes. Las campañas de phishing se han vuelto más sofisticadas y utilizan tácticas personalizadas, como el phishing selectivo y el compromiso del correo electrónico empresarial (BEC), dirigidas a altos ejecutivos, personal de campo y socios. Las consecuencias pueden incluir pérdidas financieras, exposición de datos confidenciales (por ejemplo, información de donantes, planes de respuesta a emergencias) y daños a la reputación de la organización. UNICEF debe actualizar continuamente sus sistemas de capacitación, sensibilización y detección. | | **Ransomware/ataques cibernéticos externos** | Medio | Alto | **Alto** | La creciente dependencia de UNICEF de plataformas en la nube (por ejemplo, AWS, Azure) y de contratistas externos aumenta el riesgo de ataques de ransomware. Estos ataques pueden paralizar la infraestructura crítica, comprometer datos confidenciales y provocar interrupciones operativas importantes. Las aplicaciones basadas en la nube utilizadas por UNICEF para gestionar grandes conjuntos de datos (por ejemplo, datos de protección infantil, programas educativos, bases de datos de ayuda de emergencia) corren un alto riesgo, particularmente porque los atacantes a menudo apuntan a las debilidades de terceros proveedores o proveedores de servicios. Este riesgo se ve agravado aún más por la amenaza de ataques de denegación de servicio distribuido (DDoS), que pueden interrumpir los servicios en línea y la disponibilidad de datos. En las zonas de conflicto, donde la infraestructura de datos de UNICEF es menos resistente, los ataques cibernéticos podrían retrasar o detener las operaciones humanitarias, lo que las convierte en una máxima prioridad para la mitigación. | | **Violación de datos** | Alto | Muy Alto | **Alto** | Las filtraciones de datos son una preocupación crítica debido a la naturaleza delicada del trabajo de UNICEF. La organización recopila una amplia gama de información confidencial, incluidos datos de salud, registros financieros y datos de protección infantil, que es un objetivo principal para los actores maliciosos. Una infracción podría dar lugar a la divulgación no autorizada de información de identificación personal (PII), poniendo en riesgo a las poblaciones vulnerables y potencialmente violando normas de privacidad como el GDPR (Reglamento General de Protección de Datos). El uso cada vez mayor de contratistas, socios y oficinas de campo externos aumenta la cantidad de puntos de acceso para posibles infracciones, especialmente en áreas con mala higiene cibernética. En caso de incumplimiento, la confianza entre UNICEF, los donantes y los beneficiarios podría verse gravemente comprometida, lo que provocaría daños a la reputación y pérdida de financiación. | | **Desastres naturales (inundaciones, terremotos)** | Medio | Muy Alto | **Alto** | Los desastres naturales, como inundaciones, terremotos y huracanes, tienen un impacto enorme en las operaciones de UNICEF, especialmente en regiones vulnerables y de baja resiliencia como Filipinas, Haití y partes de África y Asia. Estos eventos pueden alterar las cadenas de suministro, destruir la infraestructura física (por ejemplo, oficinas, almacenes) y desplazar a millones de personas, creando un aumento en la demanda de los servicios de emergencia de UNICEF. Los desastres naturales también plantean riesgos de pérdida de datos o tiempo de inactividad del sistema si se dañan el hardware o los servidores críticos. El personal de campo que trabaja en zonas propensas a desastres enfrenta desafíos adicionales de comunicación y movilidad, lo que complica aún más los esfuerzos humanitarios. A pesar de las estrategias de preparación para desastres de la organización, la imprevisibilidad y magnitud de tales eventos requieren una inversión continua en medidas de mitigación para garantizar la continuidad del negocio durante y después de los desastres. | | **Robo/Pérdida de Dispositivos** | Medio | Alto | **Alto** | Con más de 10.000 empleados en más de 190 países, el riesgo de robo o pérdida de dispositivos (por ejemplo, computadoras portátiles, teléfonos móviles, unidades USB) es una amenaza

constante. Esto es particularmente problemático en regiones con altas tasas de criminalidad o durante el transporte de personal o materiales a zonas de conflicto y entornos humanitarios. Un dispositivo perdido o robado podría provocar la exposición de datos altamente confidenciales, incluidos registros de donantes, datos de salud e información de seguridad. El uso de dispositivos no seguros o la falta de implementación de medidas de seguridad adecuadas (por ejemplo, protección con contraseña, cifrado de dispositivos) aumenta este riesgo. En el pasado ya se han informado de ejemplos específicos de incidentes, como el robo de computadoras portátiles que contienen datos confidenciales en las oficinas sobre el terreno o la pérdida de dispositivos durante emergencias. Por lo tanto, son necesarias políticas estrictas con respecto a la administración de dispositivos, protocolos de seguridad y capacidades de borrado remoto. | | **Amenaza interna** | Bajo | Muy Alto | **Medio** | Las amenazas internas, si bien son menos comunes, conllevan riesgos sustanciales debido a la sensibilidad de los datos que manejan los empleados y contratistas de UNICEF. La organización depende de una fuerza laboral numerosa y diversa, incluidos empleados en regiones de alto riesgo. Las amenazas internas pueden incluir acciones maliciosas (por ejemplo, robo de datos, sabotaje) o mal manejo inadvertido de información confidencial (por ejemplo, no seguir los protocolos de acceso a datos). Aunque el riesgo es relativamente bajo, las consecuencias pueden ser devastadoras, especialmente para el personal que trabaja en zonas de conflicto con acceso a datos sensibles sobre protección infantil y salud. Las amenazas internas también pueden extenderse a contratistas, socios o proveedores que tienen acceso a sistemas de datos críticos. La supervisión periódica, los controles de acceso sólidos y las auditorías internas son esenciales para minimizar el riesgo de amenazas internas. | | **Error humano (pérdida de datos)** | Alto | Medio | **Medio** | El error humano es una de las causas más comunes de pérdida o exposición de datos en las organizaciones globales. Las operaciones globales de UNICEF, combinadas con la diversidad de idiomas, culturas y niveles de alfabetización tecnológica entre el personal, aumentan la probabilidad de cometer errores como la eliminación accidental de datos, el intercambio inadecuado de archivos o el incumplimiento de las políticas de seguridad de datos. En las oficinas de campo, donde el personal está bajo presión para brindar respuestas rápidas, el error humano puede provocar la exposición accidental o la pérdida de información crítica. El uso de procesos manuales o sistemas obsoletos en determinadas regiones puede exacerbar aún más la probabilidad de errores. Se necesitan capacitación, políticas claras de gestión de datos y sistemas automatizados de respaldo de datos para minimizar el error humano. |

---

7. Estrategias de mitigación

1. Campaña de concientización sobre phishing

- **Acción**:
- Implementar un sistema global **programa de concientización sobre phishing** que se adapte a los contextos regionales y las amenazas locales. El programa incluirá **sesiones de entrenamiento interactivas**, **ejercicios de phishing simulados**, y **evaluaciones en curso** para evaluar la preparación del personal.
- Comprometer **expertos externos en ciberseguridad** para realizar simulaciones de phishing en profundidad y proporcionar a las oficinas regionales pautas específicas basadas en los tipos de ataques más comunes en su geografía.
- Educar al personal sobre **banderas rojas** como remitentes desconocidos, archivos adjuntos sospechosos y enlaces no solicitados en correos electrónicos, con especial atención a **phishing** y **fraude del director general** que a menudo apuntan a altos líderes.

- Colabore con servicios globales de filtrado de correo electrónico y garantice **bloqueo automático** de correos electrónicos relacionados con phishing y archivos adjuntos maliciosos.
- **Cronología**:
- Formación inmediata para **regiones de alto riesgo** (por ejemplo, zonas de conflicto, mercados emergentes) dentro **1 mes**.
- Implementación completa del programa global dentro **3 meses**, con regularidad **cursos bianuales de actualización**.
- **Impacto**:
- Reducción significativa de incidentes relacionados con phishing y un personal más informado capaz de reconocer y prevenir intentos de phishing. Resiliencia mejorada a los ataques de ingeniería social.

2. Cifrado de datos

- **Acción**:
- Asegurar **cifrado de extremo a extremo** se aplica en todos los dispositivos móviles, computadoras portátiles y servicios basados en la nube (por ejemplo, AWS, Azure) para proteger los datos durante la transmisión y el almacenamiento.
- Integre soluciones de cifrado que cumplan con **RGPD** y otras leyes regionales de protección de datos, garantizando que todos los datos confidenciales, incluidos los registros médicos y de protección infantil, estén cifrados tanto en tránsito como en reposo.
- Implementar **cifrado basado en hardware** soluciones para dispositivos del personal de campo, con cifrado automático activado al iniciar.
- Actualizar periódicamente los estándares de cifrado y evaluar su eficacia para contrarrestar las amenazas emergentes (por ejemplo, la computación cuántica).
- **Cronología**:
- **Implementación de cifrado inmediata** para operaciones de campo de alto riesgo y sistemas críticos (por ejemplo, datos de donantes, registros de protección infantil).
- **Implementación completa** globalmente dentro **6 meses**, con periódico **auditorías anuales**.
- **Impacto**:
- Los datos permanecen seguros incluso en caso de robo o violación del dispositivo, lo que reduce significativamente el riesgo de acceso no autorizado a información confidencial.

3. Autenticación multifactor (MFA)

- **Acción**:
- Exija MFA a todos los empleados y contratistas que accedan a sistemas críticos (por ejemplo, servicios en la nube, datos financieros, bases de datos internas) para evitar el acceso no autorizado, incluso si las credenciales están comprometidas.
- Proporcionar apoyo para **autenticación biométrica** o **fichas de hardware** para personal de alto rango y aquellos que trabajan en regiones sensibles o en proyectos de alto riesgo.
- Integrar MFA con **VPN** y garantizar el acceso seguro a sistemas remotos para el personal de campo.
- **Cronología**:
- Implementar MFA para **sistemas críticos** dentro **2 meses** (por ejemplo, AWS, Salesforce y plataformas de donantes).
- Lleno **MFA para toda la organización** implementación en todos los sistemas dentro **4 meses**.
- **Impacto**:

- Reduce drásticamente las posibilidades de acceso no autorizado a sistemas sensibles, especialmente en caso de phishing o robo de credenciales.

4. Planes de respaldo y recuperación ante desastres

- **Acción**:
- Crear **centros regionales de recuperación de desastres** para garantizar que los datos se puedan recuperar rápidamente incluso en regiones propensas a desastres naturales o conflictos. Los sistemas de respaldo deben diversificarse en ubicaciones físicas y en la nube.
- Conducta **simulacros bianuales de recuperación de desastres** para probar la resiliencia del sistema y la preparación del personal de campo para recuperar datos de forma remota o en persona.
- Mejorar **redundancia de datos**, asegurando que los datos clave (como registros de donantes, datos de salud y planes de proyectos) estén respaldados en múltiples geografías, minimizando el riesgo de pérdida de datos.
- **Cronología**:
- **Revisión de 1 mes** de las capacidades actuales de recuperación ante desastres, seguidas por **mejoras inmediatas**.
- Lleno **pruebas e implementación** de redundancias de respaldo físico y basado en la nube dentro **6 meses**.
- **Impacto**:
- Reduce la pérdida de datos en caso de desastres o ataques de ransomware, lo que garantiza que las operaciones críticas de UNICEF puedan continuar incluso ante interrupciones.

5. Control de acceso a datos

- **Acción**:
- Hacer cumplir **Control de acceso basado en roles (RBAC)** que todos los sistemas limiten el acceso a datos confidenciales en función del rol, las responsabilidades y la necesidad de conocimiento del individuo.
- Implementar **auditorías frecuentes** de registros de acceso para detectar intentos no autorizados y anomalías, y realizar **revisiones trimestrales** de los derechos de acceso de los usuarios.
- Establecer **acceso con privilegios mínimos** protocolos y garantizar que los empleados solo tengan acceso a los datos necesarios para realizar sus funciones laborales.
- Implementar **revisiones de acceso automatizado** para contratistas y proveedores externos con acceso a sistemas y datos críticos.
- **Cronología**:
- **Implementación en curso**, con una revisión inicial dentro **3 meses** para garantizar que el modelo RBAC esté funcionando en todos los sistemas principales.
- **Impacto**:
- Control mejorado sobre datos confidenciales, con riesgos reducidos de amenazas internas o exposición accidental de datos a través de derechos de acceso que se alinean con las necesidades laborales.