Políticas y procedimientos de seguridad de UNICEF

Tabla de contenido

1. **Introducción al marco de seguridad de UNICEF**

El **Marco de Prácticas de Seguridad de la Información de UNICEF** está diseñado para garantizar que la infraestructura digital, los datos confidenciales y los recursos de UNICEF estén protegidos eficazmente contra amenazas y riesgos, incluidos ataques cibernéticos, filtraciones de datos, desastres naturales y errores humanos. Dada su presencia global en protección infantil, salud, educación y esfuerzos humanitarios, UNICEF requiere medidas de seguridad sólidas e integrales.

- **Visión**: Proteger los datos confidenciales de UNICEF, apoyar las operaciones globales, garantizar la seguridad de los niños en todo el mundo y mantener la confianza de las partes interesadas.
- **Elementos principales**:
  - **Privacidad de datos**: Cumplimiento de los estándares globales de privacidad de datos (GDPR, HIPAA, etc.).
  - **Respuesta a incidentes**: Establecer procesos claros y organizados para detectar, gestionar y mitigar incidentes.
  - **Continuidad del negocio**: Garantizar una interrupción mínima de las operaciones de misión crítica de UNICEF durante una crisis.
  - **Conciencia de seguridad**: capacitación continua para reducir los errores humanos y mantener una fuerza laboral alerta y bien informada.

2. **Gobernanza y cumplimiento**

2.1 Regulaciones clave y marcos de cumplimiento

UNICEF opera en diversas regiones y jurisdicciones, cada una con sus propias leyes de protección de datos y normas de ciberseguridad. La organización alinea sus prácticas de seguridad con los siguientes estándares clave:

- **ISO/IEC 27001**: este estándar describe las mejores prácticas para un **Sistema de gestión de seguridad de la información (SGSI)**. UNICEF garantiza que el marco proporcione controles de seguridad sólidos, desde la identificación de riesgos hasta la implementación de mitigaciones.
- **Reglamento General de Protección de Datos (GDPR)**: El cumplimiento del RGPD es obligatorio para el tratamiento de datos personales de ciudadanos de la UE. Los procesos de UNICEF están diseñados para defender derechos como la minimización de datos, la transparencia y la rendición de cuentas.
    - Ejemplo: UNICEF proporciona a las personas formularios de consentimiento claros y derechos para acceder y eliminar sus datos, de acuerdo con los requisitos del RGPD.
- **NIST SP 800-53**: Estándar federal de EE. UU. que proporciona un catálogo de controles de seguridad para sistemas de información federales, garantizando el cumplimiento de los requisitos de ciberseguridad.
- **Controles de seguridad críticos del CIS**: un conjunto de mejores prácticas de ciberseguridad priorizadas que sigue UNICEF para proteger sus sistemas contra vulnerabilidades y amenazas comunes.
- **Ley de Responsabilidad y Portabilidad del Seguro Médico (HIPAA)**: Aplicable al manejo de datos médicos de UNICEF en contextos humanitarios específicos (por ejemplo, la prestación de servicios de salud a niños), que requieren protecciones estrictas para la información de salud.

2.2 Estructura de gobernanza de la seguridad

La **Estructura de Gobernanza de la Seguridad** dentro de UNICEF es un enfoque integral y multifacético diseñado para garantizar que la seguridad de la información esté integrada en todos los niveles de la organización. Esta estructura proporciona liderazgo, supervisión y rendición de cuentas para las decisiones de seguridad, y garantiza que los esfuerzos de seguridad de UNICEF se alineen con sus objetivos organizacionales y requisitos regulatorios globales. Los siguientes componentes definen este marco de gobernanza:

CISO (Director de Seguridad de la Información)

El **Jefe de Seguridad de la Información (CISO)** tiene la responsabilidad final de la estrategia general de seguridad, el liderazgo y la ejecución de las iniciativas de seguridad en todo UNICEF. El CISO es responsable de garantizar que todos los aspectos de la seguridad de la información, desde la gestión de amenazas hasta el cumplimiento de los estándares internacionales, estén cubiertos e implementados de manera efectiva.

Responsabilidades clave:

- **Supervisión estratégica**: el CISO garantiza que el programa de seguridad de la información se alinee con la misión y las necesidades operativas de UNICEF. Desarrollan estrategias de seguridad a largo

plazo, garantizando que los recursos se asignen de manera efectiva y los riesgos se gestionen de manera proactiva.
- **Gestión de riesgos**: el CISO evalúa los riesgos y vulnerabilidades relacionados con los activos físicos y digitales de UNICEF, incluidos datos, redes y propiedad intelectual. Crean y actualizan estrategias de mitigación de riesgos y son responsables de tomar decisiones sobre niveles aceptables de riesgo.
- **Cumplimiento y regulaciones**: el CISO garantiza que UNICEF cumpla con estándares globales como **GDPR**, **ISO/IEC 27001**, **NIST SP 800-53** y **HIPAA** (cuando corresponda), garantizando al mismo tiempo el cumplimiento de las leyes de seguridad y privacidad de datos de varios países en los que opera UNICEF.
- **Informes al liderazgo ejecutivo**: el CISO proporciona informes de seguridad periódicos al liderazgo ejecutivo y a la Junta Directiva de UNICEF, incluidas actualizaciones sobre riesgos de seguridad, incidentes e iniciativas estratégicas.

Integración al Comité de Gestión de Riesgos:

El CISO es un miembro clave del **Comité de Gestión de Riesgos** de UNICEF. Este comité es responsable de las decisiones estratégicas sobre riesgo organizacional, ciberseguridad y privacidad de datos, integrando la seguridad en el marco general de gestión de riesgos de la organización. El Comité de Gestión de Riesgos se reúne periódicamente para discutir las amenazas emergentes, los cambios regulatorios y la preparación de la organización para manejar los riesgos.

Centro de operaciones de seguridad (SOC)

El **Centro de Operaciones de Seguridad (SOC)** es la columna vertebral de las operaciones de seguridad de UNICEF y tiene la tarea de monitorear y responder a incidentes de seguridad en tiempo real. El equipo SOC opera las 24 horas del día, los 7 días de la semana, empleando herramientas y tecnologías de última generación para monitorear todos los sistemas e infraestructuras críticos.

Funciones clave:

- **Detección de amenazas en tiempo real**: el SOC utiliza herramientas de seguridad avanzadas como **Splunk** para la agregación y el análisis de registros, **CrowdStrike** para la protección de endpoints y **AWS GuardDuty** para la inteligencia de amenazas en la nube. . Estas herramientas monitorean continuamente eventos de seguridad, detectan actividades anormales y emiten alertas para una acción inmediata.
    - **Splunk**: ayuda en la **Gestión de eventos e información de seguridad (SIEM)**, agregando datos de múltiples fuentes (servidores, puntos finales, aplicaciones) para identificar posibles incidentes de seguridad como violaciones de datos y ataques de denegación de servicio. o amenazas internas.
    - **CrowdStrike Falcon**: una herramienta clave para la seguridad de terminales que proporciona monitoreo en tiempo real de los dispositivos utilizados por el personal, como computadoras portátiles y teléfonos móviles, para detectar y mitigar malware, ransomware y otras amenazas a terminales.
- **Detección y respuesta a incidentes**: el SOC detecta actividades sospechosas, analiza amenazas potenciales y se coordina con el Equipo de respuesta a incidentes (IRT) para contener, mitigar y resolver incidentes con prontitud.

    - Ejemplo: si el SOC detecta un intento inusual de exfiltración de datos a través del monitoreo de la red, el equipo alerta instantáneamente al IRT para que tome medidas, como aislar el sistema afectado y bloquear futuras transferencias de datos.
- **Inteligencia sobre amenazas**: el SOC integra continuamente fuentes de inteligencia sobre amenazas de proveedores de seguridad globales y fuentes internas para anticipar amenazas emergentes. Herramientas como **FireEye** y **ThreatConnect** se utilizan para recopilar y analizar información sobre nuevas amenazas dirigidas a organizaciones como UNICEF.
- **Monitoreo y búsqueda proactivos**: además del monitoreo reactivo, el SOC busca de manera proactiva posibles vulnerabilidades y signos de compromiso, utilizando técnicas como ejercicios de **Caza de amenazas** y **Red Teaming** para probar y mejorar la seguridad. defensas.

Dotación de personal del SOC:

El SOC está compuesto por **Analistas de seguridad**, **Responsadores de incidentes**, **Especialistas en inteligencia de amenazas** y **Expertos forenses** que trabajan juntos para garantizar la disponibilidad, integridad y confidencialidad de los datos y sistemas.

Comité de Seguridad TI

El **Comité de Seguridad de TI** es un grupo multifuncional formado por profesionales superiores de TI y seguridad dentro de UNICEF. La responsabilidad principal del comité es supervisar la formulación, implementación y revisión de la estrategia, las políticas y los planes operativos de seguridad de la organización.

Responsabilidades clave:

- **Planificación estratégica**: El Comité de Seguridad de TI trabaja con el CISO para definir y actualizar la estrategia de seguridad de la organización, identificando áreas clave de mejora y garantizando la alineación con los objetivos más amplios de la organización.
- **Desarrollo de políticas de seguridad**: el comité desempeña un papel crucial en la redacción y revisión de políticas de seguridad, incluida la protección de datos, estándares de cifrado, controles de acceso de usuarios y protocolos de gestión de incidentes de seguridad.
- **Presupuesto de seguridad y asignación de recursos**: El comité decide sobre las inversiones relacionadas con la seguridad, evaluando el financiamiento para las herramientas, capacitación y operaciones de seguridad necesarias. Priorizan la asignación presupuestaria para garantizar que los recursos se dirijan a iniciativas de alta prioridad, como actualizaciones de infraestructura o nuevas herramientas de seguridad.
- **Evaluación y mitigación de riesgos**: el comité evalúa la eficacia de los esfuerzos de gestión de riesgos de la organización, considerando el panorama cambiante de las amenazas a la ciberseguridad, los cambios regulatorios y la exposición al riesgo operativo de UNICEF.
- **Evaluación de la postura de seguridad**: El Comité de Seguridad de TI trabaja con auditores externos para revisar la postura de seguridad actual de la organización, garantizando que los sistemas críticos estén protegidos contra posibles vulnerabilidades y amenazas.

Partes interesadas clave en el Comité de Seguridad de TI:

- **CTO (director de tecnología)**: trabaja en estrecha colaboración con el CISO para alinear la infraestructura técnica y las innovaciones con las necesidades de seguridad.
- **Oficiales legales y de cumplimiento**: garantizar que las iniciativas de seguridad cumplan con las leyes internacionales y las regulaciones de la industria, como GDPR e ISO/IEC.
- **Equipo de gestión de riesgos**: colabora con el comité para identificar y abordar los riesgos emergentes para los activos de información de la organización.
- **Expertos externos**: Ocasionalmente, el comité consulta con expertos externos como **consultores de seguridad**, **probadores de penetración** o **auditores de cumplimiento** para evaluar y mejorar las prácticas de seguridad.

Auditores Externos

Los auditores externos desempeñan un papel integral para garantizar que las prácticas de seguridad de la información de UNICEF sigan siendo efectivas y cumplan con los más altos estándares. Aportan una perspectiva independiente e imparcial a la gobernanza de la seguridad y son fundamentales para identificar brechas y vulnerabilidades.

Funciones y responsabilidades clave:

- **Auditorías de cumplimiento**: UNICEF colabora con auditores externos como **KPMG**, **PwC** y **Deloitte** para realizar auditorías periódicas y evaluar el cumplimiento de la organización con los principales marcos y regulaciones de seguridad, como como **ISO 27001**, **SOC 2**, **GDPR** y **NIST SP 800-53**.
    - Ejemplo: Una **auditoría de PwC** de la postura de seguridad en la nube de UNICEF evalúa si las configuraciones de la nube de la organización cumplen con las mejores prácticas y los estándares regulatorios para la protección de datos.
- **Evaluaciones de vulnerabilidad y pruebas de penetración**: los auditores externos a menudo tienen la tarea de realizar evaluaciones de seguridad integrales, que incluyen **pruebas de penetración**, **escaneo de vulnerabilidades** y **revisión de código**. Estas evaluaciones ayudan a UNICEF a identificar posibles debilidades en su infraestructura digital.
    - Ejemplo: Una **prueba de penetración** podría descubrir brechas de seguridad en la aplicación móvil o los portales web de UNICEF, lo que llevaría a recomendaciones para mecanismos de autenticación y cifrado más sólidos.
- **Análisis de brechas**: Después de completar sus evaluaciones, los auditores externos realizan informes de análisis de brechas, destacando áreas de vulnerabilidad y asesorando sobre las mejoras o acciones correctivas necesarias.
    - Ejemplo: Los auditores pueden identificar que es necesario fortalecer las medidas de protección de terminales de UNICEF para tener en cuenta el uso cada vez mayor de **dispositivos móviles** para operaciones remotas en el campo.
- **Reportes al Directorio**: Los auditores externos brindan informes independientes sobre la efectividad del programa de seguridad de la información, ofreciendo recomendaciones para la mejora continua. Estos informes a menudo se presentan directamente a la alta dirección y a la junta directiva de UNICEF.

Beneficios de las auditorías externas:

- **Verificación independiente**: Las auditorías externas proporcionan una revisión neutral de terceros de los controles y prácticas de seguridad de UNICEF, lo que ayuda a garantizar que los sistemas de la

organización sean seguros y cumplan con las normas.
- **Garantía regulatoria**: la interacción regular con los auditores ayuda a UNICEF a demostrar su compromiso con el cumplimiento de las leyes internacionales de protección de datos y los estándares de la industria.
- **Mejoras de seguridad continuas**: los hallazgos de las auditorías externas se incorporan directamente al ciclo de mejora continua de UNICEF, mejorando la postura de seguridad con el tiempo.

Integración con otras estructuras de gobernanza

Además de estas funciones específicas, el marco de gobernanza de la seguridad de UNICEF está integrado con estructuras organizativas más amplias, lo que garantiza que se incorporen consideraciones de ciberseguridad en todos los procesos de toma de decisiones. La estructura de **Gobierno de tecnología de la información (TI)** trabaja en estrecha colaboración con los equipos de seguridad para garantizar que las nuevas tecnologías y sistemas se evalúen en busca de riesgos de seguridad antes de implementarlos.

---

3. Política de seguridad de la información

3.1 Propósito y Alcance

La **Política de Seguridad de la Información** define el enfoque integral de UNICEF para salvaguardar sus activos de información y tecnología. Esta política garantiza la confidencialidad, integridad y disponibilidad de la información y los sistemas de la organización, al tiempo que cumple con las regulaciones globales de cumplimiento y privacidad. La política se aplica a:

- **Empleados**: Esto incluye a todos los empleados de tiempo completo, contratistas, trabajadores temporales, pasantes y proveedores de servicios externos que tienen acceso a los sistemas de información de UNICEF. Todos los miembros del personal deben familiarizarse con la política y seguir los procedimientos de seguridad.
    - **Ejemplo**: un contratista que trabaja en un proyecto para UNICEF debe cumplir con los mismos protocolos de seguridad que el personal de tiempo completo, incluidas medidas de control de acceso y requisitos de notificación de incidentes.
- **Sistemas**: todos los sistemas operados o de propiedad de UNICEF, incluidos:
    - **Infraestructura de TI**: servidores internos, dispositivos de red, firewalls y sistemas de almacenamiento de datos.
    - **Sistemas en la nube**: cualquier servicio alojado en plataformas en la nube como **Amazon Web Services (AWS)**, **Microsoft Azure** y **Google Cloud Platform (GCP)**, donde las aplicaciones críticas de UNICEF y se almacenan los datos.
    - **Puntos finales**: todos los dispositivos, como computadoras portátiles, de escritorio, tabletas, teléfonos inteligentes y otros equipos conectados que pueden acceder a las redes y servicios internos de UNICEF.
    - **Redes**: todas las redes de comunicación internas y externas, incluidas las redes privadas virtuales (VPN) utilizadas por el personal de UNICEF para el trabajo remoto y el acceso seguro.
- **Datos**: La política cubre todo tipo de datos manejados por UNICEF, incluyendo:

- **Datos Personales**: Datos sujetos a regulaciones de privacidad como el **Reglamento General de Protección de Datos (GDPR)**, que cubre datos personales relacionados con donantes, empleados y beneficiarios de UNICEF.
- **Datos Operativos**: Incluye datos del proyecto, comunicaciones internas e información de investigación.
- **Información financiera confidencial**: todos los registros financieros, presupuestos, datos de nómina y otros detalles financieros confidenciales.
- **Propiedad Intelectual**: Documentos, diseños, software y otros materiales desarrollados por UNICEF.

3.2 Objetivos de seguridad

La política de seguridad de la información está diseñada para alcanzar los siguientes objetivos de seguridad:

Confidencialidad

La confidencialidad garantiza que solo aquellos con acceso autorizado puedan acceder a la información confidencial, lo que reduce el riesgo de divulgación no autorizada. UNICEF emplea un **enfoque de seguridad de múltiples niveles** para hacer cumplir la confidencialidad en todos los niveles de su ecosistema de información.

- **Cifrado de datos**: todos los datos personales confidenciales y la información operativa se cifran en reposo y en tránsito mediante protocolos de cifrado sólidos.
  - **Ejemplo**: los datos personales, como la información de los donantes y los registros de los beneficiarios, se cifran en reposo mediante **AWS Key Management Service (KMS)** con cifrado **AES-256**. Los datos en tránsito se cifran mediante **Seguridad de la capa de transporte (TLS)**.
- **Control de acceso**: el acceso se otorga según el **principio de privilegio mínimo**, lo que garantiza que los empleados solo tengan acceso a los datos necesarios para sus funciones específicas.
  - **Ejemplo**: los empleados del departamento de finanzas solo pueden acceder a los registros financieros, mientras que el personal de Recursos Humanos puede acceder a los datos de los empleados pero no a los datos financieros. Los derechos de acceso se gestionan a través de **Okta** y se revisan periódicamente.
- **Enmascaramiento y redacción de datos**: para determinadas operaciones confidenciales (por ejemplo, informes públicos, datos compartidos con socios), los campos confidenciales se enmascaran o se redactan para evitar el acceso no autorizado.
  - **Ejemplo**: la información de los donantes en los informes compartidos con socios externos está enmascarada para proteger las identidades personales.

Integridad

La integridad garantiza que la información sea precisa, coherente y confiable durante todo su ciclo de vida. Para proteger la integridad de los datos, UNICEF emplea varias medidas:

- **Validación de datos y sumas de verificación**: para verificar la autenticidad de los datos críticos, UNICEF utiliza hashes criptográficos (por ejemplo, **SHA-256**) y sumas de verificación durante las transferencias o el procesamiento de datos.

    - **Ejemplo**: al transferir grandes conjuntos de datos entre plataformas o realizar copias de seguridad de datos, UNICEF genera hashes criptográficos para verificar que los datos no hayan sido manipulados durante la transmisión.
- **Control de versiones**: los cambios en documentos, bases de código y datos críticos se rastrean mediante sistemas de control de versiones como **GitHub** para código y **SharePoint** para documentos.
    - **Ejemplo**: se registra un cambio en el pronóstico financiero interno de UNICEF y cualquier discrepancia se marca para su revisión.

Disponibilidad

La disponibilidad garantiza que la información y los sistemas sean accesibles para los usuarios autorizados cuando sea necesario, minimizando el tiempo de inactividad y las interrupciones del servicio.

- **Sistemas de alta disponibilidad**: UNICEF implementa configuraciones de alta disponibilidad para sistemas de misión crítica, garantizando un tiempo de inactividad mínimo en caso de falla. Por ejemplo, **SAP** y **Salesforce** se implementan en la infraestructura de **AWS** mediante implementaciones de zona de disponibilidad múltiple (AZ), lo que garantiza capacidades de redundancia y conmutación por error.
    - **Ejemplo**: si falla un AWS AZ, el tráfico se redirige automáticamente a otra zona disponible dentro de la región, lo que garantiza la disponibilidad continua del servicio.
- **Recuperación ante desastres**: existe un sólido plan de recuperación ante desastres, con copias de seguridad frecuentes de datos y sistemas críticos para garantizar que los objetivos de recuperación se cumplan dentro de plazos aceptables (Objetivos de tiempo de recuperación - RTO) y se minimice la pérdida de datos (Punto de recuperación). Objetivos - RPO).
    - **Ejemplo**: UNICEF realiza copias de seguridad diarias de datos y sistemas utilizando **Veeam Backup** para replicar datos en depósitos de **AWS S3** y **AWS Glacier** para almacenamiento a largo plazo. Estas copias de seguridad se prueban periódicamente para comprobar la integridad y restauración de los datos.

No repudio

El no repudio garantiza que las acciones realizadas en los sistemas y los datos sean rastreables, proporcionando responsabilidad y evitando que los usuarios nieguen sus acciones.

- **Seguimientos de auditoría**: se registran todas las interacciones del usuario con sistemas y datos confidenciales. Los registros se agregan y almacenan de forma segura para realizar análisis forenses si es necesario. Herramientas como **Splunk** se utilizan para monitorear y analizar las actividades de los usuarios, generando alertas ante cualquier acción anómala o sospechosa.
    - **Ejemplo**: si un empleado accede a los datos financieros de un donante, se crea una entrada en el registro de **Splunk**, que captura la identidad del usuario, la hora y el tipo de acción realizada (por ejemplo, leer, escribir, actualizar).
- **Firmas digitales**: los documentos y transacciones que requieren firmas se firman digitalmente para garantizar la autenticidad y evitar manipulaciones. Esto incluye acuerdos, contratos y comunicaciones clave.
    - **Ejemplo**: UNICEF utiliza **DocuSign** para firmar documentos oficiales, lo que garantiza que cada documento tenga una firma digital cifrada que no pueda modificarse.

3.3 Evaluación y gestión de riesgos

- **Evaluación continua de riesgos**: UNICEF lleva a cabo evaluaciones de riesgos continuas para identificar posibles amenazas a la seguridad de sus sistemas y datos. Estas evaluaciones están diseñadas para priorizar las vulnerabilidades en función del impacto potencial en la organización y la probabilidad de que ocurran.
    - **Ejemplo**: Cada año, UNICEF realiza una **evaluación de riesgos** que incluye análisis de vulnerabilidades utilizando herramientas como **Qualys** y **Tenable.io**, seguido de una **penetración en profundidad. probar** el compromiso con una empresa de seguridad externa como **KPMG**.
- **Auditorías de seguridad**: se realizan auditorías de seguridad internas y externas periódicas para garantizar el cumplimiento de los estándares de la industria y las políticas organizacionales.
    - **Ejemplo**: **PwC** realiza una auditoría de seguridad anual de la infraestructura de TI de UNICEF para garantizar el cumplimiento de los estándares **ISO 27001** y **SOC 2**.
- **Gestión de vulnerabilidades**: las vulnerabilidades identificadas durante los análisis o auditorías se priorizan y se solucionan de manera oportuna. Las vulnerabilidades críticas que suponen un riesgo importante para los sistemas se solucionan en **24 horas**.
    - **Ejemplo**: si se identifica una vulnerabilidad crítica en **SAP** durante una auditoría, el equipo de gestión de vulnerabilidades trabaja para parchearla dentro del cronograma definido para mitigar el riesgo potencial.

3.4 Cumplimiento de empleados y contratistas

Todos los empleados, contratistas y proveedores externos de UNICEF deben cumplir con la **Política de seguridad de la información**. Esto incluye el cumplimiento de:

- **Programas de capacitación**: todos los empleados reciben capacitación anual sobre concientización sobre seguridad a través de plataformas como **KnowBe4**, enfocándose en identificar phishing, comprender la seguridad de las contraseñas e informar posibles incidentes de seguridad.
    - **Ejemplo**: Cada nuevo empleado debe completar un curso de incorporación de seguridad dentro del primer mes de empleo, que incluye módulos sobre políticas de uso aceptable, protección de datos y control de acceso al sistema.
- **Gestión de terceros**: los contratistas y proveedores externos deben firmar acuerdos de confidencialidad, someterse a controles de seguridad y cumplir con las políticas de seguridad de UNICEF cuando trabajan con datos confidenciales.
    - **Ejemplo**: antes de que un proveedor externo tenga acceso a los datos de UNICEF, se realiza una **evaluación de riesgos de terceros** para evaluar su postura de seguridad y garantizar que cumplan con los estándares de seguridad de la información de UNICEF.

3.5 Aplicación de políticas e infracciones

- **Cumplimiento**: El **CISO** y el **Comité de Seguridad de TI** son responsables de hacer cumplir la Política de Seguridad de la Información. Cualquier violación de la política puede dar lugar a medidas disciplinarias, incluido el despido, acciones legales o sanciones financieras.
    - **Ejemplo**: Si se descubre que un empleado ha violado los controles de acceso a datos al compartir indebidamente datos confidenciales, puede estar sujeto a una investigación formal y a

un posible despido.

- **Monitoreo e informes**: UNICEF monitorea continuamente sus sistemas para verificar el cumplimiento de la política utilizando herramientas automatizadas como **Splunk** y auditorías manuales. Se anima a los empleados a denunciar cualquier actividad sospechosa o infracción a través de los canales de denuncia designados.
    - **Ejemplo**: los empleados pueden informar un presunto intento de phishing a través del correo electrónico de seguridad de la empresa o un sistema de tickets interno, lo que desencadenará una investigación.

3.6 Revisión y actualizaciones de políticas

- **Revisión periódica**: la Política de seguridad de la información se revisa anualmente y se actualiza según sea necesario para abordar amenazas emergentes, nuevos requisitos de cumplimiento y avances en tecnología.
    - **Ejemplo**: Después de un evento importante de ciberseguridad global como el **ataque de SolarWinds**, las políticas de seguridad de UNICEF se revisan y actualizan para garantizar que la organización esté protegida contra tipos de ataques similares.
- **Mecanismo de retroalimentación**: Se alienta a los empleados, contratistas y auditores externos a brindar retroalimentación sobre la política y sugerir mejoras, que se consideran durante la revisión anual.
    - **Ejemplo**: después de una campaña de ataque de phishing, el **CISO** lleva a cabo una sesión de comentarios con empleados clave para analizar qué salió mal y cómo se puede actualizar la política para mejorar la concientización sobre la seguridad.

---

4. Control de acceso y autenticación de usuarios

4.1 Gestión de identidad y acceso (IAM)

UNICEF adopta un marco sólido y centralizado de **Gestión de identidad y acceso (IAM)** para gestionar las identidades de los usuarios, la autenticación y los controles de acceso en todos los sistemas y aplicaciones. El sistema IAM garantiza que solo las personas autorizadas tengan acceso a información y recursos confidenciales, según sus funciones y responsabilidades dentro de la organización. Ayuda a mitigar el riesgo de acceso no autorizado, violaciones de datos y amenazas internas.

Okta - Plataforma IAM centralizada

UNICEF aprovecha **Okta** como su principal solución IAM, que se integra con una variedad de sistemas empresariales, garantizando una autenticación segura y fluida para los usuarios en todas las plataformas y servicios. Okta proporciona **Inicio de sesión único (SSO)** y **Autenticación multifactor (MFA)**, lo que permite a los usuarios acceder de forma segura a múltiples sistemas sin necesidad de contraseñas separadas para cada uno.

- **Inicio de sesión único (SSO)**: la funcionalidad SSO de Okta permite a los usuarios iniciar sesión una vez y obtener acceso a una amplia gama de aplicaciones, minimizando la necesidad de recordar múltiples nombres de usuario y contraseñas.

    - **Ejemplo**: un empleado de UNICEF puede iniciar sesión en Okta usando sus credenciales y acceder a un conjunto de herramientas como **Workday** para tareas de recursos humanos, **Salesforce** para gestión de donantes y **Slack** para equipo. comunicación, sin necesidad de introducir credenciales separadas para cada uno.
    - **Beneficio**: esto mejora la experiencia del usuario, reduce la fatiga del inicio de sesión y aumenta la seguridad al minimizar las vulnerabilidades relacionadas con las contraseñas.

- **Autenticación multifactor (MFA)**: MFA se aplica a todos los usuarios que acceden a sistemas confidenciales. MFA requiere que los usuarios proporcionen dos o más factores de verificación, lo que agrega una capa adicional de seguridad. Esto puede incluir una combinación de algo que el usuario sabe (contraseña), algo que tiene (dispositivo móvil o token de seguridad) o algo que es (datos biométricos como huellas dactilares o reconocimiento facial).

    - **Ejemplo**: cuando un empleado de UNICEF accede a su sistema de nómina a través de **Workday**, se le solicita que ingrese su contraseña y luego se autentique mediante un método MFA, como un código enviado a su teléfono mediante SMS o una aplicación. como **Google Authenticator**.
    - **Beneficio**: MFA reduce significativamente el riesgo de acceso no autorizado, incluso si un atacante adquiere la contraseña de un usuario.

Control de acceso basado en roles (RBAC)

UNICEF emplea **Control de acceso basado en roles (RBAC)** para garantizar que los usuarios tengan acceso solo a los recursos y datos necesarios para sus funciones laborales específicas. RBAC minimiza el riesgo de fuga de datos o acceso no autorizado al limitar lo que los usuarios pueden ver y hacer según su función dentro de la organización.

- **Definiciones granulares de roles**: los roles se definen cuidadosamente dentro del sistema IAM para reflejar diversas funciones laborales, departamentos y requisitos de seguridad. Los roles se asignan a aplicaciones y permisos específicos, lo que garantiza que los usuarios solo puedan acceder a los datos y funciones relevantes para su rol.

    - **Ejemplo**: un **Gerente de Recursos Humanos** podría tener acceso a los registros de los empleados y a los datos de nómina, pero no podrá ver los informes financieros, que están restringidos al **Equipo de Finanzas**.
    - **Ejemplo**: un **Administrador de TI** tiene amplio acceso a los ajustes y configuraciones del sistema, pero no tendrá acceso a los sistemas de recursos humanos o de nómina, que no forman parte de sus responsabilidades laborales.

- **Principio de privilegio mínimo**: los derechos de acceso se proporcionan según el principio de **privilegio mínimo**, lo que significa que a los usuarios se les otorga solo el nivel mínimo de acceso necesario para realizar sus funciones laborales. Los niveles de acceso se revisan y ajustan periódicamente para garantizar que sigan siendo apropiados.

    - **Ejemplo**: un contratista contratado para un proyecto a corto plazo tendrá acceso limitado a los archivos del proyecto en **SharePoint**, sin acceso a la red más amplia de la organización ni a los sistemas financieros confidenciales.

Gestión de identidades federadas

Además de Okta, UNICEF también utiliza **Gestión de identidad federada** para un acceso seguro a servicios externos, lo que permite a los empleados utilizar sus credenciales corporativas para acceder a plataformas de terceros sin crear cuentas separadas.

- **Ejemplo**: los empleados de UNICEF pueden acceder a plataformas basadas en la nube como **AWS** o **Google Cloud Platform (GCP)** utilizando sus credenciales de Okta, lo que agiliza el acceso y garantiza la gestión centralizada de los permisos.

4.2 Políticas de administración de contraseñas

La gestión eficaz de contraseñas es fundamental para proteger las cuentas y los sistemas de los usuarios del acceso no autorizado. UNICEF aplica políticas de contraseñas sólidas para garantizar que las contraseñas sean complejas y seguras, al tiempo que proporciona un proceso eficiente para que los usuarios administren sus credenciales.

Requisitos de complejidad de la contraseña

UNICEF exige que las contraseñas cumplan estrictos requisitos de complejidad para garantizar la solidez frente a ataques comunes de adivinación de contraseñas (por ejemplo, ataques de fuerza bruta y de diccionario).

- **Longitud de la contraseña y diversidad de caracteres**: todas las contraseñas deben tener al menos **12 caracteres** e incluir una combinación de:
    - Letras mayúsculas y minúsculas
    - Números (al menos uno)
    - Caracteres especiales (por ejemplo, @, #, $, %, &, etc.)
    - **Ejemplo**: Una contraseña como "UNICEF$2024!Secure" cumple con estos requisitos y ofrece un alto nivel de complejidad para resistir ataques comunes.
- **Listas negras de contraseñas**: UNICEF emplea una lista negra de contraseñas para evitar que los usuarios seleccionen contraseñas débiles o de uso común que sean fáciles de adivinar. El sistema marca y rechaza automáticamente las contraseñas comunes como "contraseña123" o "qwerty".
    - **Ejemplo**: si un usuario intenta establecer su contraseña como “12345678”, el sistema le impedirá hacerlo y le pedirá que seleccione una contraseña más segura.

Caducidad y rotación de contraseña

Para proteger aún más las cuentas del acceso no autorizado debido al robo o compromiso de contraseñas, UNICEF exige la caducidad periódica de las contraseñas.

- **Intervalo de caducidad de contraseña**: todas las contraseñas de usuario caducan cada **90 días** para garantizar que las contraseñas antiguas no queden vulnerables indefinidamente. Los usuarios son notificados 10 días antes del vencimiento de la contraseña y deben actualizar sus contraseñas dentro de este período.
    - **Ejemplo**: **Okta** notifica a un usuario por correo electrónico y recordatorios en la aplicación que su contraseña vencerá en 10 días. Se les solicita que elijan una nueva contraseña que cumpla

con los requisitos de complejidad.

- **Historial de contraseñas**: los usuarios tienen prohibido reutilizar la misma contraseña dentro de una cierta cantidad de cambios de contraseña (por ejemplo, 5 contraseñas anteriores) para evitar el reciclaje de contraseñas inseguras.
    - **Ejemplo**: después de que un usuario restablece su contraseña, no se le permite volver a una contraseña utilizada anteriormente, lo que promueve la creación de contraseñas nuevas y seguras.

Proceso de recuperación de contraseña

Para garantizar que los usuarios puedan recuperar de forma segura el acceso a sus cuentas sin comprometer la seguridad, UNICEF emplea un sólido proceso de **recuperación de contraseña** que incorpora **Autenticación multifactor (MFA)**.

- **Método de recuperación**: si un usuario olvida su contraseña, puede utilizar el **portal de autoservicio de Okta** para iniciar el proceso de recuperación de contraseña. El usuario debe autenticarse utilizando un segundo factor, como un código de verificación enviado a su número de teléfono registrado o correo electrónico.
    - **Ejemplo**: A un usuario que olvida su contraseña se le solicita que ingrese su dirección de correo electrónico. Recibirán un código de autenticación por **SMS** o **correo electrónico**, que deberán ingresar para restablecer su contraseña de forma segura.
- **Tokens de recuperación basados en el tiempo**: el proceso de recuperación utiliza **contraseñas de un solo uso basadas en el tiempo (TOTP)**, lo que garantiza que cualquier token de recuperación enviado a los usuarios sea válido solo durante un período corto, lo que mejora aún más la seguridad.
    - **Ejemplo**: un usuario que solicite un restablecimiento de contraseña recibirá un TOTP de 6 dígitos que caduca en 10 minutos, lo que evitará que un atacante intercepte y reutilice el código.

Herramientas de administración de contraseñas

UNICEF también fomenta el uso de **Administradores de contraseñas** para que los usuarios almacenen y administren de forma segura sus contraseñas complejas. Herramientas como **1Password** o **LastPass** pueden ayudar a los usuarios a mantener contraseñas seguras y únicas para cada aplicación sin el riesgo de olvidarlas.

- **Ejemplo**: un usuario accede a su cuenta de **Salesforce** y utiliza un administrador de contraseñas para generar una contraseña única, que se almacena de forma segura y se completa automáticamente para futuros inicios de sesión.

4.3 Auditoría y monitoreo de acceso

El monitoreo y la auditoría regulares de las actividades de acceso de los usuarios ayudan a garantizar que los usuarios cumplan con las políticas de seguridad y permiten la detección de posibles incidentes de seguridad, como accesos no autorizados o comportamientos sospechosos.

- **Registros de auditoría**: Okta mantiene **registros de auditoría** detallados para todas las actividades de acceso y autenticación de usuarios, que se almacenan y analizan de forma centralizada en busca de anomalías. Estos registros incluyen información como intentos de inicio de sesión, intentos fallidos de inicio de sesión, direcciones IP y marcas de tiempo.
    - **Ejemplo**: si un usuario accede a un sistema confidencial como **SAP**, el sistema registra cada acción realizada por el usuario. Si se detecta una cantidad inusual de intentos fallidos de inicio de sesión, se activa una **alerta de seguridad** para su revisión.
- **Monitoreo en tiempo real**: la integración con herramientas como **Splunk** o **CrowdStrike** permite el monitoreo en tiempo real del acceso de los usuarios en todos los sistemas. Las alertas se activan automáticamente cuando se detectan patrones de acceso sospechosos (por ejemplo, múltiples inicios de sesión fallidos, acceso desde IP inusuales).
    - **Ejemplo**: si un empleado inicia sesión desde una ubicación o dispositivo desconocido, el sistema marca esta actividad y solicita una verificación adicional a través de **Okta MFA** antes de otorgarle acceso.
- **Revisiones periódicas de acceso**: las **revisiones periódicas de acceso** garantizan que los usuarios mantengan los derechos de acceso adecuados según sus funciones y responsabilidades actuales. El equipo de seguridad y los jefes de departamento revisan periódicamente el acceso a los sistemas y datos críticos.
    - **Ejemplo**: cada trimestre, el **departamento de recursos humanos** revisa los privilegios de acceso de todos los empleados, garantizando que a los usuarios que cambiaron de rol o abandonaron la organización se les revoque el acceso de inmediato.

---

5. Plan de respuesta a incidentes (IRP)

5.1 Ciclo de vida de la gestión de incidentes con cronogramas

| **Tipo de incidente** | **Herramientas de detección** | **Comportamiento** | **Próximos pasos** | **Planificación previa al incidente** | **Cronograma de respuesta** | |----------|--- ---------- ----------- ----|---------- ---------- --------|---------- ---------- ---------- ----------|---------- ----------| | **Acceso no autorizado** (fuerza bruta, compromiso de cuenta) | - **Okta**: Intentos de inicio de sesión fallidos.
- **CrowdStrike**: Actividad inusual.
- **AWS GuardDuty**: Detección de anomalías. | - Bloquear la cuenta afectada.
- Activar **restablecimiento de contraseña forzado**.
- Aislar los sistemas comprometidos. | - Análisis forense de registros para identificar movimiento lateral.
- Notificar a los usuarios afectados. | - Aplicar **MFA**.
- Implementar **detección de inicio de sesión avanzada**. | **Inmediata (5-15 minutos)** para detección.
30 minutos para contención.
1-2 horas para erradicación.
4-12 horas ** para recuperación.| | **Infección de malware (ransomware, troyanos) | - **CrowdStrike Falcon**: Detección de endpoints.

- **Splunk**: Tráfico anormal.
- **AWS GuardDuty**: Actividad sospechosa. | - Aislar el dispositivo afectado.
- Ejecutar **análisis completo de malware**.
- Analizar los registros del sistema en busca de comportamiento de malware. | - **Volver a crear imágenes** de las máquinas afectadas.
- Notificar a las partes interesadas internas.
- Remediar la causa raíz. | - Implementar **ATP**.
- **Copias de seguridad fuera de línea** periódicas.
- **Segmentación de red**. | **Inmediata (5-15 minutos)** para detección.
30-60 minutos para contención.
1-4 horas para erradicación.
4-12 horas para recuperación. | | **Ataque de phishing** (recolección de credenciales) | - **Mimecast**: filtro de correo electrónico malicioso.
- **Splunk**: correlación de tráfico de red anormal.
- **Proofpoint**: detección de phishing. | - Poner en cuarentena el correo electrónico malicioso.
- Activar el restablecimiento de contraseña para los usuarios afectados.
- Revisar el origen del correo electrónico y los registros DNS. | - Ejecute un barrido de seguridad de los dispositivos afectados.
- Notifique a otros usuarios que tengan cuidado.
- Analice e informe intentos de phishing. | - Implementar **soluciones de filtrado de correo electrónico**.
- Realizar **capacitación para concientizar sobre phishing**. | **Inmediata (5-15 minutos)** para detección.
30-60 minutos para contención.
1-2 horas para erradicación.
2-4 horas para recuperación. | | **Ataque DDoS** (Denegación de servicio distribuida) | - **AWS Shield**, **Cloudflare**: protección DDoS.
- **Splunk**: análisis de tráfico.
- **Akamai**: monitoreo de tráfico. | - Activar protección DDoS.
- Implementar **limitación de velocidad**.
- Aplicar **bloqueo geográfico** si es necesario. | - Redirigir el tráfico a regiones alternativas.
- Monitorear ataques en curso usando **CloudWatch**.
- Análisis forense posterior al incidente. | - Configurar **equilibrio de carga**.
- Implementar **infraestructura escalable** con protección **Cloudflare/AWS Shield**. | **Inmediata (5-15 minutos)** para detección.
30-60 minutos para contención.
1-2 horas para erradicación.
4-12 horas para recuperación. |

5.2 Fases de respuesta a incidentes y cronograma

| **Fase** | **Acción** | **Periodo de tiempo** | **Parte responsable** | |---------- ---------- ---------- ---------- | | **Detección** | Detección inicial mediante herramientas de seguimiento y alertas. | **Inmediato (5-15 minutos)** | Analistas de SOC | | **Triaje** | Clasificación de incidentes según gravedad (Crítico, Alto, Medio, Bajo). | **15-30 minutos** | Líder de respuesta a incidentes, analistas de SOC | | **Contención** | Aislar los sistemas afectados para limitar la propagación. | **30-60 minutos** | Ingenieros TI, Analistas SOC | | **Erradicación** | Elimine la causa raíz (por ejemplo, malware, acceso no autorizado). | **1-4 horas** | Ingenieros TI, Analistas de Seguridad | |

Recuperación | Restaurar sistemas desde copias de seguridad o entornos alternativos. | **4-12 horas** | Soporte TI, Continuidad del Negocio | | **Revisión posterior al incidente**| Revisar el incidente para mejorar futuros procesos de respuesta. | **24-48 horas después de la resolución**| Líder de respuesta a incidentes, CISO |

5.3 Escenarios de incidentes detallados con cronogramas

1. Acceso no autorizado (fuerza bruta/relleno de credenciales)

Detección:

- **Okta** detecta múltiples intentos fallidos de inicio de sesión en un corto período de tiempo.
- **CrowdStrike** identifica patrones de acceso inusuales (por ejemplo, iniciar sesión desde un país desconocido).

Comportamiento:

- Bloquee la cuenta afectada y realice un **restablecimiento de contraseña**.
- Aislar los sistemas y restringir el acceso a recursos sensibles.
- Activar **MFA** para evitar más accesos no autorizados.

Cronología:

- **Detección**: **Inmediata (5-15 minutos)**
- **Contención**: **30-60 minutos**
- **Erradicación**: **1-2 horas** (análisis de causa raíz y remediación)
- **Recuperación**: **4-12 horas** (restaurar y monitorear)

Planificación previa al incidente:

- Aplicar **MFA** para todos los sistemas críticos.
- Implementar **políticas de bloqueo de cuenta** después de repetidos intentos fallidos de inicio de sesión.

---

2. Infección de malware (ransomware)

Detección:

- **CrowdStrike Falcon** detecta firmas de malware o actividad inusual de archivos.
- **Splunk** correlaciona el tráfico de red anormal indicativo de una violación de datos.

Comportamiento:

- Aislar inmediatamente la máquina infectada de la red.
- Ejecute **análisis antivirus** o utilice **CrowdStrike Falcon** para la detección de malware.
- Bloquear todas las comunicaciones salientes para evitar una mayor filtración de datos.

Cronología:

- **Detección**: **Inmediata (5-15 minutos)**

- **Contención**: **30-60 minutos**
- **Erradicación**: **1-4 horas** (eliminación de malware y corrección)
- **Recuperación**: **4-12 horas** (nueva imagen de los sistemas y restauración de datos)

Planificación previa al incidente:

- Implementar **ATP** en todos los dispositivos.
- Mantener **copias de seguridad fuera de línea** para sistemas críticos.

---

3. Ataque de phishing

Detección:

- **Mimecast** marca enlaces o archivos adjuntos de correo electrónico maliciosos.
- **Proofpoint** detecta sitios de phishing conocidos o comportamientos inusuales en el correo electrónico.

Comportamiento:

- Poner en cuarentena el correo electrónico de phishing para evitar que se propague.
- Realice **restablecimiento de contraseña** para todas las cuentas afectadas.
- Activar un **barrido de seguridad** de los dispositivos afectados.

Cronología:

- **Detección**: **Inmediata (5-15 minutos)**
- **Contención**: **30-60 minutos**
- **Erradicación**: **1-2 horas** (eliminación de enlaces o archivos maliciosos)
- **Recuperación**: **2-4 horas** (restauración de servicios de correo electrónico y revisión de la configuración de seguridad)

Planificación previa al incidente:

- Implementar **soluciones de filtrado de correo electrónico** para la detección de phishing.
- Llevar a cabo **formación sobre concientización sobre phishing** para evitar errores del usuario.

---

4. Ataque DDoS

Detección:

- **AWS Shield** detecta picos de tráfico típicos de un ataque DDoS.
- **Akamai** o **Cloudflare** identifican patrones de tráfico anormales o anomalías en las solicitudes HTTP.

Comportamiento:

- Utilice servicios de mitigación de DDoS como **AWS Shield** o **Cloudflare** para absorber el tráfico.
- Implementar **limitación de velocidad** y **bloqueo geográfico** para evitar la amplificación del ataque.
- Redirigir el tráfico a servidores de respaldo o utilizar **equilibrio de carga** para mitigar la tensión en los sistemas primarios.

Cronología:

- **Detección**: **Inmediata (5-15 minutos)**
- **Contención**: **30-60 minutos** (Activar protección DDoS, limitación de velocidad)
- **Erradicación**: **1-2 horas** (gestión y filtrado del tráfico)
- **Recuperación**: **4-12 horas** (restablecer acceso y servicio normal)

Planificación previa al incidente:

- Utilice **equilibrio de carga** para distribuir el tráfico de red de manera uniforme.
- Implementar **infraestructura de nube escalable** que pueda manejar picos de tráfico.

5.4 Plan de comunicación con cronogramas

| **Acción** | **Descripción** | **Parte responsable** | **Cronología** | |----------|---------- ---------- ---------- --|----------|----------| | **Notificación interna** | Notificar a la alta dirección, al CISO y a los equipos de respuesta a incidentes. | Líder de SOC, Líder de respuesta a incidentes | **Inmediato (0-15 minutos)** | | **Notificación externa** | Notificar a los usuarios, clientes y organismos reguladores afectados según sea necesario (por ejemplo, notificación de incumplimiento del RGPD). | Equipo de relaciones públicas, Legal, Líder de respuesta a incidentes | **Dentro de 1 hora de la contención** | | **Divulgación pública** | Anuncie cualquier problema de interés público (solo si es necesario). | CISO, equipo de relaciones públicas | **Post-resolución** | | **Actualizaciones de las partes interesadas** | Proporcionar actualizaciones periódicas a las partes interesadas (incluidos los usuarios afectados) hasta la resolución. | Líder de respuesta a incidentes, CISO | **En curso (cada 1-2 horas)** | | **Informes posteriores al incidente** | Documente el cronograma completo y las acciones tomadas, incluidas las fallas y mejoras. | Líder de respuesta a incidentes, CISO | **Dentro de 24-48 horas** |

5.5 Revisión posterior al incidente

| **Acción** | **Descripción** | **Parte responsable** | **Cronología** | |----------|---------- ---------- ----------|---- ----------|---------- ---| | **Informe de incidente** | Cree un informe de incidente detallado que describa lo que ocurrió, cómo se manejó y su impacto. | Líder de respuesta a incidentes, CISO | **Dentro de 24 horas** | | **Sesión de lecciones aprendidas** | Llevar a cabo una reunión con todas las partes interesadas relevantes para revisar el incidente y derivar acciones de mejora. | CISO, líder de respuesta a incidentes | **Dentro de 48 horas** | | **Actualizar procedimientos de respuesta** | Revisar el plan de respuesta a incidentes en función de las lecciones aprendidas. | Líder de respuesta a incidentes | **Dentro de 72 horas** | | **Capacitación de seguimiento** | Realizar cursos de actualización y simulacros a los empleados sobre los protocolos de seguridad mejorados. | RRHH, equipo de seguridad | **En curso** |

---

6. Copia de seguridad, recuperación y continuidad del negocio de datos

---

6.1 Estrategia de respaldo: la regla 3-2-1

Componentes de respaldo:

Componente de respaldo	**Descripción**	**Herramientas/Sistemas utilizados**	**Implementación en el mundo real**	**Planificación previa al incidente**	**Cronograma de respuesta**		---	---	---	---	---	---
3 copias de datos	Mantenga tres copias de datos: la copia primaria (en vivo), una copia de respaldo almacenada localmente y una copia de respaldo externa.	- **Datos primarios**: sistemas activos. - **Copia de seguridad 1**: copia de seguridad in situ con **Veeam Backup**. - **Copia de seguridad 2**: copia de seguridad externa con ** AWS S3** o **Azure Blob Storage**.	**Copia principal**: sistemas activos, incluidos entornos de producción como **SAP**, **Salesforce**, **Microsoft 365** y datos operativos críticos. **Copia de seguridad 1**: **Veeam Backup** en el sitio **NAS (NetApp)** ubicado en **UNICEF Geneva Data Center (Suiza)**. **Copia de seguridad 2**: almacenamiento en la nube en **AWS S3** y **Azure Blob Storage** (Irlanda para Europa y Singapur para Asia-Pacífico).	- Trabajos de respaldo configurados con frecuencia **cada hora** para sistemas críticos (por ejemplo, sistemas de nómina, finanzas y recursos humanos). - Configuración de **Almacenamiento en la nube** para incluir **redundancia geográfica**.	**Frecuencia de respaldo**: **Cada hora** para todos los sistemas críticos. - **Comprobaciones de integridad de las copias de seguridad**: **Semanal** para copias de seguridad en el sitio (NAS) y **mensual** para copias de seguridad en la nube (AWS S3, Azure Blob).
2 medios diferentes	Utilice dos tipos diferentes de medios para garantizar la redundancia en caso de que falle un medio.	- **Copia de seguridad in situ**: **NAS (almacenamiento conectado en red)** para almacenamiento local. - **Copia de seguridad externa**: almacenamiento en la nube (por ejemplo, **AWS S3** o **Azure Blob Storage **).	**Copia de seguridad in situ**: Dispositivo **NetApp NAS** de 10 TB de capacidad en **Ginebra (Suiza)**, conectado a sistemas internos. **Copia de seguridad externa**: **AWS S3** en **UE-Irlanda** y **Asia-Pacífico-Singapur**, con datos de copia de seguridad replicados entre múltiples regiones para recuperación ante desastres.	- Los dispositivos NAS en el sitio están **replicados** para garantizar la **redundancia** dentro del centro de datos de Ginebra. - **La replicación de respaldo en la nube** garantiza que los datos en **Irlanda** y **Singapur** estén activos -al día con la última copia de seguridad por hora.	**Frecuencia de respaldo**: **Actualizaciones cada hora**. - **Verificación de respaldo en la nube**: Pruebas de verificación mensuales utilizando AWS y Azure para garantizar la disponibilidad e integridad de los datos.
1 ubicación fuera del sitio	Almacene al menos una copia de seguridad fuera del sitio, preferiblemente en ubicaciones geográficamente separadas para mitigar desastres regionales.	- **Copia de seguridad externa**: almacenamiento en la nube en **AWS S3** o **Azure Blob Storage**.	**Copia de seguridad externa**: **AWS S3** en **Irlanda (UE)** para operaciones europeas, región de **Singapur** para Asia-Pacífico. Utilice **redundancia geográfica de AWS S3** para replicar copias de seguridad en diferentes zonas y regiones de disponibilidad para mayor resiliencia.	- Asegúrese de que el **almacenamiento en la nube con redundancia geográfica** esté configurado para garantizar que las copias de seguridad estén separadas geográficamente. - **Mecanismos de conmutación por error automática** implementados para restaurar las operaciones desde la ubicación secundaria.	**Frecuencia de respaldo**: **Cada hora**. - **Simulación de recuperación ante desastres**: Simulación anual del proceso de conmutación por error en la nube para validación de redundancia geográfica.

Implementación detallada de la estrategia de respaldo en el mundo real:

- **Frecuencia de respaldo**:
  Los sistemas críticos reciben copias de seguridad cada hora. Esto incluye:
    - **Sistemas financieros (SAP)**
    - **Sistemas de RRHH (Workday, bases de datos de nómina)**
    - **Gestión de relaciones con clientes (Salesforce)**
    - **Datos de infraestructura básica de UNICEF** Estas copias de seguridad se realizan con **Veeam Backup & Replication**, almacenando los datos en **NetApp NAS** en el sitio y en **AWS S3** fuera del sitio.

- **Pruebas de respaldo e integridad**:
  Las copias de seguridad se someten a verificación cada semana para garantizar la coherencia. Si se encuentra algún problema, se soluciona de inmediato y se restaura la copia de seguridad exitosa más reciente para garantizar la preparación en caso de desastre.

6.2 Objetivo de punto de recuperación (RPO) y objetivo de tiempo de recuperación (RTO)

Objetivo de punto de recuperación (RPO)

RPO define cuánta pérdida de datos es aceptable en caso de un incidente, especificando con qué frecuencia se deben realizar las copias de seguridad. Para UNICEF, el **RPO es de 1 hora**, lo que significa que las copias de seguridad de los datos deben realizarse al menos cada hora para garantizar que, en el peor de los casos, no se pierdan más de una hora de datos durante una falla.

| **Métrico** | **Valor** | **Descripción** | **Herramientas/Sistemas utilizados** | **Implementación en el mundo real** | **Cronograma de respuesta** | |----------|----------|----------- ---------- ----- |---------- ----|---------- ----------|----------| | **RPO** | **1 hora** | Pérdida de datos máxima permitida durante un incidente (la pérdida de datos se limita a una hora de datos). | - **Veeam Backup** (copias de seguridad in situ cada hora).
- **AWS S3** (copias de seguridad externas cada hora). | **Frecuencia de copia de seguridad**: Se realiza una copia de seguridad de los datos cada **hora** para sistemas críticos utilizando **Veeam Backup** (local) y **AWS S3** (en la nube). Todas las copias de seguridad se validan y verifican su integridad para garantizar una restauración precisa. | **Frecuencia de respaldo**: **Cada hora**.
Verificación de respaldo: Semanal para respaldos locales y mensual para respaldos en la nube. |

Implementación de RPO en el mundo real:

- **Copias de seguridad automatizadas**:
  Los sistemas críticos como **SAP** y **Salesforce** reciben copias de seguridad automáticamente cada hora. Esto minimiza el riesgo de pérdida de datos y garantiza que la copia de seguridad más reciente contenga registros actualizados.

- **Estrategia de copia de seguridad incremental**:
  Para mejorar la eficiencia, solo se guardan los cambios en los datos (copias de seguridad incrementales) después de la copia de seguridad completa inicial, lo que reduce el tiempo de copia de seguridad y los requisitos de almacenamiento.

Objetivo de tiempo de recuperación (RTO)

RTO se refiere al tiempo máximo permitido para restaurar sistemas y datos después de una interrupción. El **RTO de UNICEF es de 4 horas**, lo que significa que la organización pretende restaurar servicios y datos críticos dentro de las **4 horas** de una interrupción.

| **Métrico** | **Valor** | **Descripción** | **Herramientas/Sistemas utilizados** | **Implementación en el mundo real** | **Cronograma de respuesta** | |----------|----------|---------- ---------- ----- |---------- ----|---------- ----------|----------| | **RTO** | **4 horas** | Tiempo de inactividad máximo permitido para sistemas críticos (los sistemas deben estar operativos dentro de 4 horas). | - **Veeam Backup**: Restauración de copias de seguridad in situ.
- **AWS S3**: Restauración basada en la nube. | **Restauración de sistemas críticos**: la restauración de sistemas esenciales (p. ej., **SAP**, **Salesforce**, **Workday**) debe completarse en un plazo de 4 horas. Los sistemas de respaldo se restauran desde **Veeam Backup** (in situ) o **AWS S3** (nube), según sea necesario. | **Tiempo de restauración**: Dentro de **4 horas** para los sistemas principales. |

Implementación de RTO en el mundo real:

- **Recuperación priorizada**:
  SAP (ERP), **Salesforce** (CRM) y **Workday** (HR) son las principales prioridades para la restauración. Estos sistemas son fundamentales para las operaciones diarias de UNICEF. Después de un incidente, estos sistemas deben restaurarse primero, dentro de las 4 horas posteriores a la detección.

- **Redundancia para sistemas críticos**:
  Existen sistemas redundantes para garantizar que estas aplicaciones estén disponibles dentro de la ventana de recuperación. Por ejemplo, se realiza una copia de seguridad de **SAP** tanto en el sitio como en la nube (a través de **AWS S3**), lo que permite una restauración flexible.

6.3 Planificación de la continuidad del negocio (BCP)

BCP garantiza que UNICEF pueda continuar con sus funciones esenciales durante y después de un incidente. Así es como UNICEF ha implementado su BCP:

| **Componente BCP** | **Descripción** | **Herramientas/Sistemas utilizados** | **Implementación en el mundo real** | **Planificación previa al incidente** | **Cronograma de respuesta** | |---------- ---------- ------- |---------- ---------- |---------- ---------- ---------- |---------- ---------- | | **Identificación del sistema crítico** | Identificar sistemas críticos para priorización en recuperación. | - **SAP**, **Salesforce**, **Veeam Backup**, **AWS S3** | **Sistemas críticos**: **Salesforce**, **SAP**, **Workday** figuran como los más críticos.
Primero se restauran, seguidos de los sistemas secundarios, como servidores de correo electrónico y herramientas de colaboración interna. | - El **Plan de continuidad del negocio** prioriza los **sistemas críticos**.
- Cada aplicación crítica tiene un propietario de recuperación designado. | **Identificación Inmediata**: 0-15 minutos después de la detección del incidente. | | **Activación de sitio alternativo** | Establezca entornos de nube alternativos para garantizar la continuidad durante una interrupción. | - **AWS EC2**, **Microsoft Azure** | La conmutación por error se produce en **AWS EC2** (Irlanda) o **Azure** (Singapur) para servicios críticos.
Si el centro de datos de Ginebra deja de estar disponible, la conmutación por error en la nube se activa automáticamente. | - Las configuraciones de conmutación por error en la nube y **configuraciones de sitios**

alternativos están preestablecidas.
Las aplicaciones basadas en la nube (por ejemplo, Salesforce) se reflejan continuamente. | **Activación inmediata de conmutación por error (en 1 hora)** si los sistemas principales no funcionan. | | **Acceso a datos y comunicación** | Asegúrese de que los empleados puedan acceder de forma segura a datos críticos de forma remota y comunicarse durante un incidente. | - **Equipos de Microsoft**, **Slack**, **AWS WorkDocs** | **Microsoft Teams** y **Slack** sirven como herramientas de colaboración.
El acceso remoto se habilita a través de **VPN** para un acceso seguro a los datos. **AWS WorkDocs** se utiliza para compartir documentos en caso de fallas del sistema local. | - **VPN** preconfiguradas para personal remoto.
Las herramientas de **colaboración en la nube** como **Microsoft Teams** y **Slack** se prueban periódicamente. | **Acceso a comunicación inmediata**: dentro de los **30 minutos** posteriores al fallo. |

6.4 Pruebas y cronograma de continuidad del negocio

| **Acción** | **Descripción** | **Parte responsable** | **Cronología** | |----------|-----
---------- --------|----------|---
---------- --------| |
Verificación de respaldo | Pruebe los sistemas de respaldo con regularidad para verificar la integridad de los datos y restaurar los procesos. | Soporte de TI, Líder de respuesta a incidentes | **Semanalmente para copias de seguridad en el sitio**.
Mensualmente para copias de seguridad en la nube | | **Simulacros de recuperación de desastres** | Pruebas de recuperación a gran escala para simular diferentes escenarios de desastre y garantizar que se cumpla el RTO. | Soporte de TI, CISO | **Trimestral** | | **Prueba de continuidad del negocio** | Pruebe los protocolos de continuidad del negocio para sistemas críticos, incluida la conmutación por error de los sistemas a ubicaciones alternativas. | Líder de respuesta a incidentes, CISO | **Anualmente** | | **Revisión posterior al incidente y lecciones aprendidas**| Después de un incidente, realice una revisión para identificar áreas de mejora y garantizar una preparación continua. | Líder de respuesta a incidentes, CISO | **Dentro de las 48 horas posteriores a la resolución del incidente** |

---

7. Seguridad de terminales

La estrategia de seguridad de terminales de UNICEF es esencial para salvaguardar todos los dispositivos utilizados por empleados, contratistas y personal remoto. Esto incluye computadoras de escritorio, portátiles, dispositivos móviles y otros tipos de puntos finales. El propósito de esta política es garantizar que todos los puntos finales estén protegidos contra amenazas de seguridad, vulnerabilidades y accesos no autorizados, minimizando el riesgo de violaciones de datos y garantizando el cumplimiento de los requisitos de seguridad legales y organizacionales.

7.1 Herramientas para la protección de endpoints

UNICEF implementa un conjunto integral de herramientas para la protección de terminales, proporcionando una estrategia de defensa en capas para proteger contra las cambiantes amenazas a la ciberseguridad. Estas herramientas se implementan globalmente en todas las ubicaciones de UNICEF para garantizar que se mantengan estándares de seguridad uniformes.

| **Herramienta de seguridad** | **Descripción** | **Implementación** | **Ubicaciones de implementación** | |---------- ----------|---------- ---------- ---------- ----------|------ ---------- ---------- ----------| | **Halcón CrowdStrike** | Una plataforma avanzada de protección de endpoints que ofrece detección de amenazas en tiempo real, respuesta automatizada e investigación de incidentes. | Todos los dispositivos se monitorean continuamente para detectar posibles riesgos de seguridad, como malware, ransomware y APT. | **Todas las oficinas y ubicaciones sobre el terreno de UNICEF en todo el mundo**, incluidas **Ginebra**, **Bangkok**, **Nueva York**, **Bangladesh** y **Sudán del Sur**. | | **Microsoft Defender para punto final** | Proporciona protección integral para terminales basados en **Windows** contra malware, ransomware y exploits. | Defender ofrece protección en tiempo real, gestión de vulnerabilidades y corrección automatizada para todos los dispositivos Windows. | **Computadoras portátiles y de escritorio con Windows** en todas las ubicaciones de UNICEF. | | **VMware AirWatch (MDM)** | Una solución de administración de dispositivos móviles que administra y protege los dispositivos móviles como teléfonos inteligentes y tabletas utilizados por los empleados. | Aplica políticas de seguridad como cifrado de dispositivos, inclusión en listas blancas de aplicaciones y borrado remoto en caso de robo o pérdida. | Implementado en todos los dispositivos móviles a nivel mundial, especialmente para trabajadores de campo en regiones como **Uganda**, **México**, **Afganistán**, **Siria**. | | **Sophos Antivirus** | Una solución que brinda protección avanzada contra malware, ransomware y otras actividades maliciosas en dispositivos macOS. | Proporciona detección en tiempo real de amenazas en puntos finales basados en macOS. | Implementado en todos los **dispositivos macOS** utilizados por el personal en **Europa**, **Asia** y **América**. | | **BitLocker (Windows)** | Software de cifrado de disco completo para computadoras portátiles y de escritorio **Windows** para proteger los datos almacenados en el dispositivo en caso de robo o acceso no autorizado. | Cifra automáticamente todos los dispositivos para garantizar que la información confidencial permanezca segura. | Se aplica a todas las **computadoras portátiles** y de escritorio con Windows en **operaciones globales**. | | **FileVault (macOS)** | Cifrado de disco completo para dispositivos **macOS** que garantiza que todos los datos estén cifrados y protegidos contra el acceso no autorizado. | Se aplica a todas las computadoras portátiles y tabletas **macOS** utilizadas por el personal y el personal de campo. | Se aplica a nivel mundial, especialmente para operaciones de campo en **Siria**, **Líbano** y **Sudán del Sur**. | | **Locker de aplicaciones (Windows)** | Herramienta de lista blanca de aplicaciones que controla qué aplicaciones se pueden ejecutar en dispositivos **Windows**, minimizando el riesgo de aplicaciones no aprobadas o malware. | Configurado para bloquear la ejecución de aplicaciones no autorizadas en todos los dispositivos **Windows**. | Se aplica en todas las **computadoras portátiles** y **computadoras de escritorio** con Windows en **Europa**, **África** y **América**. | | **Copia de seguridad y replicación de Veeam** | Solución de copia de seguridad de datos que garantiza que se realice una copia de seguridad periódica de todos los datos de los terminales en una ubicación externa segura, lo que permite una recuperación rápida en caso de pérdida de datos o falla del dispositivo. | Copias de seguridad periódicas de los datos de los terminales para garantizar una recuperación rápida en caso de un incidente. | Implementado en **oficinas de UNICEF** y **ubicaciones sobre el terreno**, con énfasis en **África**, **Asia** y **Medio Oriente**. | | **Empresa Splunk** | Gestión de registros centralizada y plataforma SIEM (gestión de eventos e información de seguridad) utilizada para monitorear las actividades de los terminales e identificar posibles amenazas a la seguridad. | Agrega registros de seguridad de puntos finales en todas las ubicaciones para análisis de amenazas, detección de anomalías y fines de auditoría. | Se aplica globalmente en todas las **oficinas de UNICEF** y **operaciones remotas sobre el terreno**. |

7.2 Política de protección de terminales

UNICEF aplica una estricta **Política de protección de terminales** que garantiza que todos los dispositivos cumplan con estándares de seguridad predefinidos. Esta política se aplica a todos los empleados,

contratistas y personal remoto que utilizan cualquier punto final para acceder a la red, los datos y los sistemas de UNICEF.

| **Componente de política** | **Detalles de la política** | **Mecanismos de aplicación** | **Ubicaciones de implementación** | |---|---|---|---| | **Antivirus y antimalware** | Todos los puntos finales deben tener software antivirus y antimalware instalado, configurado y actualizado periódicamente. | **Windows Defender** (para **Windows**), **Sophos Antivirus** (para **macOS**), **CrowdStrike Falcon** (para todos los dispositivos). | Se aplica globalmente en **Windows**, **macOS** y dispositivos móviles en **Nueva York**, **Ginebra**, **Bangladesh**, **Siria** y otras oficinas de campo. | | **Actualizaciones automáticas** | El software antivirus debe configurarse para que se actualice automáticamente para recibir protección en tiempo real contra amenazas nuevas y emergentes. | Gestionado a través de **Sistemas de gestión centralizados** como **Splunk** y **CrowdStrike**. Las actualizaciones automáticas se programan diariamente. | Garantizado en todas las **oficinas de UNICEF** y **ubicaciones remotas** en **África**, **Asia**, **América**. | | **Cifrado de disco completo (FDE)** | Todos los dispositivos deben utilizar cifrado de disco completo para garantizar que los datos estén protegidos del acceso no autorizado en caso de pérdida o robo. | **BitLocker** (para **Windows**) y **FileVault** (para **macOS**) son obligatorios y se aplican en todos los dispositivos. | Se aplica a todas las **computadoras portátiles Windows**, **computadoras portátiles macOS** y **dispositivos de campo** a nivel mundial, especialmente para el personal de **África** y **Medio Oriente**. | | **Política de contraseñas** | Se aplican políticas de contraseñas seguras en todos los dispositivos para evitar el acceso no autorizado a los puntos finales. Se requiere una complejidad mínima y cambios periódicos. | **Okta** para autenticación centralizada y **Active Directory** para aplicar políticas de cambio y seguridad de contraseña. | Se aplica globalmente para todos los **empleados de UNICEF** en todas las ubicaciones. | | **Lista blanca de aplicaciones** | Solo se permite ejecutar aplicaciones aprobadas en los dispositivos para reducir el riesgo de malware o ejecución de software no autorizado. | **AppLocker** para **Windows** y **Administración de aplicaciones móviles** a través de **AirWatch**. | Se aplica a todas las **computadoras portátiles Windows** y **dispositivos móviles** en **Europa**, **Medio Oriente**, **Asia**, **África** y **América**. | | **Administración de dispositivos móviles (MDM)** | Todos los dispositivos móviles utilizados para acceder a los sistemas de **UNICEF** deben ser administrados por un sistema MDM para aplicar políticas de seguridad como cifrado, listas blancas de aplicaciones y borrado remoto. | Administrado a través de **VMware AirWatch**, que aplica la configuración de seguridad para dispositivos móviles. | Aplicado globalmente para todos los dispositivos móviles en **Sudán del Sur**, **Líbano**, **Pakistán** y **México**. | | **Borrado remoto** | En caso de pérdida o robo, los dispositivos deben borrarse de forma remota para garantizar que los datos confidenciales no queden expuestos. | Las políticas de **borrado remoto** están integradas en **AirWatch**, **BitLocker** y **FileVault** para dispositivos móviles y no móviles. | Se aplica a nivel mundial, especialmente en regiones de **alto riesgo** como **Siria**, **Sudán del Sur**, **Uganda** y **Honduras**. | | **Reporte de incidentes** | Cualquier actividad sospechosa o incidente de seguridad debe informarse inmediatamente al Centro de Operaciones de Seguridad (SOC) a través de la plataforma **ServiceNow**. | **SOC** responde a incidentes con investigación y remediación inmediata, utilizando herramientas como **Splunk** y **CrowdStrike**. | Aplicado en **todas las oficinas** en **Nueva York**, **Ginebra**, **Bangladesh**, **Sudán del Sur**, **Siria**, **México** y ** Líbano**. |

7.3 Monitoreo y respuesta

UNICEF emplea un monitoreo continuo de puntos finales, utilizando tecnologías de detección avanzadas y sistemas centralizados de gestión de incidentes para garantizar una respuesta rápida a posibles incidentes de seguridad. El monitoreo y la respuesta son cruciales para mantener la seguridad de los terminales,

particularmente para detectar y mitigar cualquier amenaza que pueda comprometer la integridad de los datos confidenciales.

| **Herramienta de seguimiento** | **Descripción** | **Objetivo** | **Mecanismo de respuesta** | |---|---|---|---| | **Splunk** | Gestión de registros centralizada y plataforma SIEM (gestión de eventos e información de seguridad) para monitoreo de terminales en tiempo real. | Proporciona una vista global de la actividad de los terminales, detectando amenazas y comportamientos sospechosos en todos los dispositivos. | Alertas inmediatas de actividad sospechosa. Se notifica a los equipos de seguridad y se inicia una investigación. | | **Halcón CrowdStrike** | Herramienta de detección y respuesta de endpoints (EDR) para monitoreo de amenazas en tiempo real y respuesta automatizada. | Supervisa todos los puntos finales en busca de amenazas como malware, acceso no autorizado y vulnerabilidades del sistema. | Cuarentena automatizada de dispositivos infectados. Los equipos de respuesta a incidentes toman medidas según la gravedad. | | **VMware AirWatch** | Herramienta de administración de dispositivos móviles que proporciona monitoreo en tiempo real de dispositivos móviles y aplica políticas de seguridad. | Detecta y reporta incidentes de seguridad que involucran dispositivos móviles. | Alertas automáticas activadas para dispositivos no compatibles. Si es necesario, se aplica el borrado remoto o el bloqueo. | | **Microsoft Defender para punto final** | Proporciona gestión integral de amenazas y vulnerabilidades para dispositivos Windows, incluidas capacidades de detección y corrección. | Detecta y corrige amenazas en puntos finales basados en **Windows**. | Detección inmediata y aislamiento automatizado de puntos finales comprometidos. Investigación de seguimiento y remediación. | | **Detección y respuesta de terminales (EDR)** | Conjunto de herramientas integrado que combina **CrowdStrike**, **Microsoft Defender** y **Splunk** para monitorear, detectar y responder a incidentes de seguridad en todos los puntos finales. | Combina monitoreo en tiempo real, análisis de amenazas y respuesta automatizada para garantizar que los puntos finales estén protegidos. | Se aíslan los dispositivos, se identifica la fuente de la amenaza y se aplican acciones correctivas. |

Al implementar estas herramientas y hacer cumplir las políticas descritas anteriormente, UNICEF mantiene un entorno seguro para todos los puntos finales y garantiza que todos los empleados, contratistas y personal de campo cumplan con los estándares de ciberseguridad de la organización.

---

8. Seguridad de red y protección de la nube

Descripción general

La estrategia de **Seguridad de la red y protección de la nube** de UNICEF es fundamental para salvaguardar su infraestructura digital crítica, garantizando que la organización pueda gestionar de forma segura información confidencial y operar globalmente sin interrupciones. Con la creciente dependencia de los servicios en la nube y una red descentralizada de personal y socios, la implementación de herramientas avanzadas de seguridad en la red y en la nube es crucial. A continuación se describen las medidas de seguridad de la red y las herramientas de protección de la nube implementadas en toda la infraestructura de UNICEF.

8.1 Herramientas de seguridad de red

El objetivo principal de la seguridad de la red es garantizar que la red interna y los activos digitales de UNICEF estén protegidos contra accesos no autorizados, filtraciones de datos y amenazas persistentes

avanzadas (APT). UNICEF emplea un enfoque de múltiples capas para la defensa de la red que integra tecnologías avanzadas como firewalls, sistemas de detección de intrusiones, soluciones VPN y análisis de red impulsados por inteligencia artificial.

1. Palo Alto Networks NGFW (firewall de próxima generación)

Palo Alto Networks Los NGFW se implementan en todos los puntos perimetrales de la red en las oficinas y centros de datos globales de UNICEF, incluidas la **sede**, las **oficinas regionales** y los **entornos de nube**. Estos firewalls protegen contra amenazas externas e internas, ofreciendo seguridad a nivel de aplicación e integración con fuentes de inteligencia de amenazas globales.

- **Características clave**:
    - **Inspección profunda de paquetes (DPI)**: analiza el tráfico entrante y saliente en la capa de aplicación para evitar ataques como **inyección SQL**, **scripting entre sitios (XSS)** y otros ataques a aplicaciones web.
    - **Inteligencia sobre amenazas**: integra fuentes de inteligencia sobre amenazas en tiempo real para bloquear el acceso a direcciones IP, dominios y URL maliciosos asociados con amenazas conocidas (por ejemplo, ransomware, phishing).
    - **Descifrado SSL**: garantiza que el tráfico cifrado (SSL/TLS) se inspeccione en busca de amenazas ocultas, lo que garantiza la seguridad de un extremo a otro.
- **Implementación**:
    - **Cobertura global**: Implementado en **centros de datos de UNICEF** en **Nueva York (este de EE. UU.)**, **Bruselas (Europa)**, **Singapur (APAC)**, **Kenia (África)** y **Sídney (Australia)**.
    - **Entornos de nube**: integrado con servicios de nube de AWS y **Azure**, asegurando **VPC (nubes privadas virtuales)** y protegiendo las aplicaciones internas implementadas en múltiples regiones.

2. Snort IDS/IPS (Sistema de prevención/detección de intrusiones)

Snort sirve como el principal sistema de prevención y detección de intrusiones (IDS/IPS) de UNICEF para detectar y bloquear el tráfico sospechoso basándose en firmas predefinidas. Analiza el tráfico de red interno y externo, proporcionando **monitoreo en tiempo real** y detección de amenazas.

- **Características clave**:
    - **Detección basada en firmas**: detecta patrones de ataque conocidos, como **desbordamientos de búfer**, **intentos de inicio de sesión por fuerza bruta** y **exploits de día cero**.
    - **Análisis de protocolo**: garantiza que protocolos como **HTTP**, **FTP**, **SMTP** y otros se utilicen de forma segura y libre de exploits.
    - **Alertas**: envía alertas en tiempo real al **Centro de operaciones de seguridad (SOC)**, lo que permite una investigación y respuesta rápidas.
- **Implementación**:
    - Instalado en segmentos críticos de la red interna, incluidas estaciones de trabajo de empleados, servidores de datos y entornos de nube, que abarcan **Norteamérica**, **Europa** y **África**.

- Implementado tanto en la **infraestructura local** como en la **infraestructura en la nube** de UNICEF para monitorear el tráfico de la red interna en **AWS** y **Microsoft Azure**.

3. VPN de Palo Alto Networks (GlobalProtect)

Palo Alto Networks GlobalProtect proporciona acceso remoto seguro para los empleados, contratistas y personal de campo de UNICEF que operan en todo el mundo. La solución VPN garantiza que los datos confidenciales permanezcan cifrados mientras están en tránsito y que los usuarios no autorizados no puedan acceder a la red interna.

- **Características clave**:
  - **Cifrado SSL**: utiliza **Cifrado SSL/TLS** para proteger los intercambios de datos a través de Internet y evitar la interceptación no autorizada.
  - **Autenticación multifactor (MFA)**: garantiza que solo el personal autorizado pueda acceder a los recursos internos al requerir factores de autenticación adicionales.
  - **Seguridad del lado del cliente**: los dispositivos deben cumplir con los criterios de seguridad (por ejemplo, antivirus actualizado, cifrado) antes de otorgar acceso a la red.
- **Implementación**:
  - Los clientes VPN se implementan globalmente, con **prioridad para oficinas remotas** y operaciones de campo en regiones como **Sudán del Sur**, **Siria** y **Brasil** donde la seguridad de Internet es crucial.
  - También lo utilizan empleados corporativos y equipos administrativos que acceden a aplicaciones y archivos internos de forma remota desde oficinas en **Nueva York**, **Londres**, **Ginebra** y otros.

4. Darktrace AI para análisis de tráfico de red

Darktrace es una solución impulsada por IA implementada para analizar y monitorear la actividad de la red en todos los niveles de la organización. Utiliza **aprendizaje automático** para adaptarse continuamente a los cambios en el comportamiento de la red e identificar posibles amenazas a la seguridad que, de otro modo, podrían pasar desapercibidas con los métodos tradicionales.

- **Características clave**:
  - **Detección de anomalías**: detecta patrones inusuales de actividad que indican una posible infracción, como **movimiento lateral** dentro de la red o acceso inusual a datos confidenciales.
  - **Capacidad de autoaprendizaje**: aprende y se adapta continuamente al comportamiento normal de la red, lo que reduce los falsos positivos y permite una detección de amenazas más precisa.
  - **Respuesta autónoma**: puede realizar acciones automatizadas, como poner en cuarentena dispositivos sospechosos o bloquear el tráfico asociado con actividades maliciosas.
- **Implementación**:
  - Implementado a nivel mundial, abarcando todas las oficinas de UNICEF, entornos de nube y redes de socios externos. Crítico en regiones con exposición de alto riesgo a amenazas cibernéticas como **África Oriental** y **América del Sur**.

8.2 Seguridad en la nube

Dado el uso que hace UNICEF de plataformas en la nube como **AWS**, **Microsoft Azure** y **Google Cloud**, proteger estos entornos es primordial. Las siguientes herramientas y estrategias garantizan la protección de datos, el cumplimiento y la mitigación de amenazas dentro de los sistemas basados en la nube.

1. Prisma Cloud de Palo Alto Networks

Prisma Cloud proporciona seguridad de extremo a extremo para cargas de trabajo en los entornos de nube de UNICEF, incluidos **AWS**, **Azure** y **Google Cloud**. La plataforma garantiza el cumplimiento de las normativas globales de protección de datos, como **GDPR**, y analiza los entornos de nube en busca de vulnerabilidades y configuraciones incorrectas.

- **Características clave**:
    - **Gestión de la postura de seguridad en la nube (CSPM)**: supervisa continuamente los entornos de la nube en busca de configuraciones erróneas, lo que garantiza que los recursos estén configurados de forma segura y cumplan con las normas.
    - **Análisis de vulnerabilidades**: analiza contenedores, máquinas virtuales (VM) y otros recursos en busca de vulnerabilidades conocidas.
    - **Monitoreo de cumplimiento**: evalúa las configuraciones de la nube frente a marcos como **ISO 27001**, **NIST** y **GDPR** para garantizar el cumplimiento de los estándares de seguridad.
- **Implementación**:
    - Implementado en las plataformas **AWS** (Irlanda, Singapur, Este de EE. UU.), **Microsoft Azure** (Europa, Norteamérica) y **Google Cloud** de UNICEF donde residen los datos críticos de la organización.
    - Supervisa específicamente **aplicaciones nativas de la nube**, **funciones sin servidor** y **almacenamiento de datos** (por ejemplo, **depósitos S3**, **Azure Blob Storage**) para detectar accesos o datos no autorizados. fuga.

2. Netskope CASB (Agente de seguridad de acceso a la nube)

Netskope proporciona visibilidad y control sobre las aplicaciones en la nube, lo que garantiza que se acceda de forma segura a los datos almacenados en plataformas SaaS como **Google Workspace**, **Salesforce** y **Dropbox**. Ayuda a prevenir **fugas de datos** y aplica políticas de **prevención de pérdida de datos (DLP)**.

- **Características clave**:
    - **Control de acceso a datos en tiempo real**: monitorea todas las interacciones de datos con aplicaciones en la nube para garantizar que los datos confidenciales no queden expuestos ni descargados a usuarios no autorizados.
    - **Shadow IT Discovery**: Identifica aplicaciones en la nube no autorizadas (Shadow IT) utilizadas por empleados y socios para almacenar o compartir información confidencial.
    - **Protección contra amenazas**: detecta y previene malware, ransomware e intentos de phishing en entornos de nube.
- **Implementación**:

- Implementado en **aplicaciones SaaS** utilizadas por UNICEF a nivel mundial, como **Google Workspace** (Documentos, Hojas de cálculo), **Dropbox** y **Salesforce** para CRM y gestión de donantes.
- Cubre la **presencia global** de la organización, incluidas áreas de alto riesgo como **Europa del Este**, **América Latina** y **Sudeste Asiático**.

3. AWS Cloud Trail

AWS CloudTrail se utiliza para registrar cada llamada API realizada dentro de los servicios de AWS, lo que garantiza la visibilidad de todas las interacciones con el entorno de la nube. CloudTrail proporciona registros detallados de **quién accedió a qué recursos**, **cuándo** y **qué acciones se realizaron**.

- **Características clave**:
  - **Registro de actividad de API**: captura cada acción realizada en AWS, incluido quién inició la solicitud, qué se cambió y el resultado.
  - **Pistas de auditoría**: ayuda a los equipos forenses a investigar actividades sospechosas y proporciona evidencia para auditorías de cumplimiento.
  - **Soporte multiregión**: garantiza que los registros de CloudTrail se recopilen y almacenen en múltiples regiones para evitar la pérdida de datos en caso de una interrupción del servicio regional.
- **Implementación**:
  - Activo en todas las **regiones de AWS** de UNICEF, incluidas **Irlanda**, **Singapur** y **Este de EE. UU.**, donde se almacenan datos confidenciales como información de donantes, registros financieros y datos de programas.
  - Garantiza que los registros estén disponibles para las auditorías de seguridad, lo que ayuda a UNICEF a mantener el cumplimiento de regulaciones globales como **GDPR** y **FISMA**.

4. Centro de seguridad de Azure

Azure Security Center ofrece un sistema de administración de seguridad de infraestructura unificada que brinda protección contra amenazas en Microsoft Azure. Ayuda a UNICEF a monitorear y administrar las políticas de seguridad en todos sus recursos de Azure para evitar el acceso no autorizado, las violaciones de datos y la desviación de la configuración.

- **Características clave**:
  - **Supervisión del cumplimiento normativo**: evalúa continuamente las configuraciones de seguridad según estándares como **ISO 27001**, directrices **NIST** y **GDPR** para garantizar que los recursos sigan cumpliendo.
  - **Detección y mitigación de amenazas**: se integra con otros servicios de Azure como **Azure Sentinel** para detectar vulnerabilidades, malware y **amenazas persistentes avanzadas (APT)**.
- **Implementación**:
  - Implementado en todos los **servicios en la nube Azure** de UNICEF que respaldan operaciones de misión crítica, incluidos sistemas de gestión de datos de personal, **aplicaciones SAP** y plataformas de gestión financiera alojadas en **Alemania**, **América del Norte**. y **Asia-Pacífico**.

Respuesta a incidentes para la seguridad de la red y la nube

El plan de respuesta a incidentes de UNICEF para la seguridad de la red y la nube está estructurado para identificar, contener y mitigar rápidamente posibles violaciones de seguridad. El proceso garantiza que cada incidente se resuelva rápidamente,

minimizando los daños y asegurando el cumplimiento de la normativa de protección de datos.

| **Fase** | **Acción** | **Periodo de tiempo** | **Parte responsable** | |---------------------|-------------------------- ---------- ------------------------|--------- --------------------|---------------------- ------| | **Detección** | Las alertas de **Palo Alto NGFW**, **Snort** y **Prisma Cloud** indican posibles violaciones de seguridad. | Inmediato (en cuestión de minutos) | Equipo SOC, Analistas de Seguridad | | **Triaje** | Evaluar el alcance y el impacto potencial del incidente, priorizando los esfuerzos de respuesta en función de la gravedad. | 10-30 minutos | Líder de respuesta a incidentes, equipo SOC| | **Contención** | Aislar sistemas o recursos de la nube comprometidos mediante **firewalls** y **grupos de seguridad**. | 30-60 minutos | Operaciones de TI, Analistas de Seguridad | | **Erradicación** | Identificar procesos maliciosos o usuarios no autorizados y eliminarlos del entorno. | 1-2 horas | Soporte de TI, Analistas de seguridad | | **Recuperación** | Restaurar servicios a partir de copias de seguridad (p. ej., **AWS S3**, **Azure Recovery**) y verificar que los sistemas sean seguros. | 2-4 horas | Soporte de TI, equipos de infraestructura en la nube | | **Revisión posterior al incidente** | Análisis de causa raíz, evaluación de impacto y lecciones aprendidas para mejorar la respuesta y la prevención futuras. | 24-48 horas post-resolución | CISO, líder de respuesta a incidentes |

---

9. Concientización y capacitación de los empleados

9.1 Capacitación en concientización sobre seguridad

Los programas de concientización y capacitación de los empleados de UNICEF están diseñados para mejorar continuamente la cultura de seguridad dentro de la organización. La capacitación se centra en escenarios prácticos y amenazas cibernéticas críticas, con un fuerte énfasis en pruebas prácticas mediante ejercicios simulados.

Plataformas y herramientas de formación

1. **KnowBe4**:
    - **Plataforma de simulación de phishing y capacitación**: UNICEF utiliza **KnowBe4** como plataforma principal para brindar contenido de capacitación y realizar simulaciones de phishing. Esta plataforma ofrece módulos de capacitación interactivos sobre una amplia gama de temas de ciberseguridad.
    - **Herramienta de simulación de phishing**: **KnowBe4** envía correos electrónicos de phishing simulados a los empleados para evaluar su capacidad para reconocer correos electrónicos maliciosos. Estos correos electrónicos están diseñados para reflejar vectores de ataque del mundo real relevantes para las operaciones de UNICEF.
2. **Centro de concientización sobre ciberseguridad**:
    - **Base de conocimientos interna**: además de **KnowBe4**, UNICEF mantiene un centro interno de recursos de seguridad, que incluye guías, preguntas frecuentes y tutoriales en vídeo sobre

cómo manejar datos de forma segura, evitar la ingeniería social y utilizar herramientas internas (como **Slack**, **Workday** y **Salesforce**) de forma segura.
- **Capacitación de actualización de seguridad obligatoria**: trimestralmente, todos los empleados deben revisar los conceptos básicos de seguridad a través de cursos de capacitación de actualización obligatorios, que incluyen la revisión de patrones recientes de ataques de phishing, consejos de ciberseguridad y mejores prácticas para el manejo de datos.

Temas de capacitación

1. **Phishing e ingeniería social**:
   - **Objetivo**: Dotar a los empleados de las habilidades para reconocer intentos de phishing comunes y tácticas de ingeniería social diseñadas para robar datos confidenciales.
   - **Duración de la formación**: 1,5 horas (inicial) / 30 minutos de repaso (trimestralmente).
   - **Entrega**: curso interactivo en línea con simulaciones de correo electrónico de phishing del mundo real.
   - **Ejemplo**: Los empleados encontrarán un correo electrónico de phishing simulado que pretende ser del departamento de recursos humanos de UNICEF solicitándoles que hagan clic en un enlace para verificar sus datos bancarios. La capacitación brinda consejos para identificar dichos correos electrónicos, incluidos enlaces sospechosos y errores ortográficos.
2. **Protección de Datos y Manejo Seguro**:
   - **Objetivo**: Garantizar que los empleados comprendan la importancia de la protección de datos, cómo almacenar y compartir información confidencial de forma segura y cómo cumplir con regulaciones como GDPR y las políticas de privacidad internas de UNICEF.
   - **Duración del entrenamiento**: 1 hora.
   - **Frecuencia**: Anual.
   - **Ejemplo**: la capacitación incluye pautas sobre el uso de **Microsoft Teams** para mensajería segura, cifrado de datos confidenciales usando **PGP** (Pretty Good Privacy) y cómo usar **SharePoint** y ** OneDrive** de forma segura para almacenar archivos.
3. **Gestión de contraseñas**:
   - **Objetivo**: Alentar a los empleados a utilizar contraseñas seguras y autenticación multifactor (MFA) para proteger sus cuentas.
   - **Duración del entrenamiento**: 45 minutos.
   - **Frecuencia**: Anual.
   - **Ejemplo**: se muestra a los empleados cómo usar **LastPass** para generar y almacenar contraseñas complejas y cómo configurar MFA para sistemas esenciales como **Workday** y **SAP**. La capacitación también incluye un segmento sobre los peligros de la reutilización de contraseñas y consejos sobre cómo crear frases de contraseña.
4. **Seguridad del dispositivo móvil**:
   - **Objetivo**: Educar a los empleados sobre cómo proteger los dispositivos móviles, incluidos teléfonos inteligentes, computadoras portátiles y tabletas, particularmente para quienes trabajan en entornos remotos y de campo.
   - **Duración del entrenamiento**: 1 hora.

- **Frecuencia**: Anual (con recordatorio trimestral opcional).
- **Ejemplo**: instrucciones sobre cómo usar **VMware AirWatch** para la administración de dispositivos, aplicar el cifrado completo del disco, configurar VPN y configurar el borrado remoto de dispositivos perdidos o robados.

5. **Reporte y respuesta a incidentes**:

   - **Objetivo**: Proporcionar a los empleados una comprensión clara de cómo informar incidentes de seguridad y su papel en el plan más amplio de respuesta a incidentes de la organización.
   - **Duración del entrenamiento**: 45 minutos.
   - **Frecuencia**: Semestral.
   - **Ejemplo**: los empleados están capacitados para reconocer posibles incidentes de seguridad, como violaciones de datos, correos electrónicos de phishing e intentos de acceso no autorizados, y reciben pautas específicas sobre cómo informar incidentes a través de la plataforma **ServiceNow**.

9.2 Simulaciones y pruebas de phishing

UNICEF aprovecha **KnowBe4** para realizar simulaciones de phishing mensuales para evaluar las capacidades de los empleados para identificar intentos de phishing. Estas simulaciones están diseñadas específicamente para imitar tácticas de ataque del mundo real y probar la preparación general de los empleados.

Proceso de simulación de phishing

1. **Campañas mensuales**:

   - **Personalización**: cada simulación de phishing está diseñada a medida para reflejar las amenazas cibernéticas actuales y los entornos específicos de UNICEF (por ejemplo, centrándose en correos electrónicos que afirman ser de donantes o socios de UNICEF).
   - **Tipos de ataques**:
   - **Spear Phishing**: correos electrónicos personalizados dirigidos a personas o departamentos específicos, como el de finanzas, con solicitudes para procesar pagos urgentes.
   - **Caza de ballenas**: ataques de phishing de alto nivel dirigidos a altos ejecutivos, a menudo haciéndose pasar por otros ejecutivos o miembros del personal de alto nivel.
   - **Recolección de credenciales**: correos electrónicos simulados que solicitan a los empleados que hagan clic en un enlace e inicien sesión en una página de inicio de sesión falsa de **Workday** o **Salesforce** para robar credenciales.

2. **Monitoreo y retroalimentación en tiempo real**:

   - **Comentarios inmediatos**: cuando un empleado hace clic en un enlace de phishing o envía información personal, recibe comentarios inmediatos de **KnowBe4**, que incluye una breve sesión de capacitación para educarlos sobre cómo detectar ataques de phishing.
   - **Capacitación de seguimiento específica**: los empleados que caen repetidamente en simulaciones de phishing se inscriben en sesiones de capacitación adicionales específicas centradas en phishing e ingeniería social.

3. **Informes y seguimiento**:
    - **Informes mensuales**: al final de cada campaña de simulación, los resultados se agregan en informes detallados que muestran cuántos empleados hicieron clic en enlaces maliciosos, qué tan rápido informaron el intento de phishing y qué empleados requieren capacitación adicional.
    - **Análisis de tendencias**: los informes permiten al equipo de seguridad de UNICEF identificar tendencias a lo largo del tiempo. Por ejemplo, si un departamento específico es atacado constantemente o un vector de ataque en particular tiene éxito, se programarán sesiones de capacitación adicionales.

9.3 Capacitación especializada y basada en roles

Ciertos roles dentro de UNICEF, como el personal de TI, los administradores de sistemas y la alta dirección, requieren una capacitación especializada y profunda en ciberseguridad. Estos programas de capacitación se centran en amenazas avanzadas y responsabilidades de seguridad operativa.

Programas de capacitación para roles específicos

1. **Administradores de TI e ingenieros de sistemas**:
    - **Enfoque de la capacitación**: Técnicas avanzadas de seguridad de red, evaluaciones de vulnerabilidad, administración de parches, protocolos de respuesta a incidentes y configuración segura del sistema.
    - **Herramientas cubiertas**: **Splunk**, **CrowdStrike**, **Palo Alto Networks** y **AWS CloudTrail**.
    - **Frecuencia**: Trimestral.
    - **Duración**: 3 horas por sesión.
2. **Equipo de seguridad y personal de respuesta a incidentes**:
    - **Enfoque de la capacitación**: procedimientos de respuesta a incidentes, análisis forense digital, gestión de una infracción y coordinación con las fuerzas del orden si es necesario.
    - **Frecuencia**: Simulaciones trimestrales, como ejercicios prácticos y simulacros de respuesta a incidentes del mundo real.
    - **Duración**: 4-5 horas por sesión.
3. **Alta Gerencia y Ejecutivos**:
    - **Enfoque de la capacitación**: comprender los riesgos de seguridad a nivel empresarial, proteger los datos críticos para el negocio y respaldar las estrategias de ciberseguridad.
    - **Temas**: Gestión de crisis durante filtraciones de datos, comunicación a nivel ejecutivo y gestión de riesgos cibernéticos.
    - **Frecuencia**: Anual.
    - **Duración**: 2 horas por sesión.

9.4 Calendario y cronograma de capacitación

Para garantizar que los empleados reciban capacitación periódica y relevante en materia de ciberseguridad, UNICEF cumple con el siguiente **Cronograma de capacitación y concientización**. Este cronograma se

integra en los planes anuales de desarrollo de los empleados, siendo de participación obligatoria para todo el personal relevante.

| **Mes** | **Actividad** | **Público objetivo** | **Duración** | **Frecuencia** | |----------|---------- ----------|----------|----------| | **Enero** | **Inicio de la concientización sobre la seguridad de Año Nuevo** | Todos los empleados | 1 hora | Anual | | **febrero** | **Simulación de phishing** | Todos los empleados | 15 minutos | Mensual | | **Marzo** | **Administración de contraseñas y capacitación MFA** | Todos los empleados | 1 hora | Anual | | **Abril** | **Capacitación en seguridad para administradores/TI** | Personal de TI, administradores de sistemas | 3 horas | Trimestral | | **Puede** | **Seguridad del dispositivo móvil** | Trabajadores remotos, personal de campo | 1 hora | Anual | | **Junio** | **Protección de datos y manejo de información sensible** | Todos los empleados | 1,5 horas | Anual | | **Julio** | **Capacitación en respuesta a incidentes** (Respuesta a incidentes simulada) | Equipo de seguridad, personal de respuesta a incidentes | 4 horas | Trimestral | | **Agosto** | **Simulación de phishing** | Todos los empleados | 15 minutos | Mensual | | **septiembre**| **Seguridad Avanzada para Ejecutivos** | Ejecutivos, alta dirección | 2 horas | Anual | | **Octubre** | **Conceptos básicos de seguridad para trabajadores remotos** | Trabajadores remotos, personal de campo | 1 hora | Anual | | **Noviembre** | **Simulación de phishing** | Todos los empleados | 15 minutos | Mensual | | **Diciembre** | **Revisión y concientización sobre seguridad de fin de año** | Todos los empleados | 1 hora | Anual |

9.5 Medición de la eficacia de la capacitación

La eficacia de la formación se evalúa utilizando múltiples métricas para garantizar que el programa de seguridad evolucione y cumpla sus objetivos.

1

. **Tasas de clics de phishing**: supervise la frecuencia con la que los empleados hacen clic en enlaces de phishing en simulaciones mensuales. Con el tiempo, estas tasas deberían disminuir, lo que indica que la fuerza laboral se está volviendo más vigilante. 2. **Evaluaciones de conocimientos**: Los cuestionarios al final de las sesiones de capacitación evalúan la comprensión de los empleados. Los empleados que obtienen una puntuación por debajo de un determinado umbral son marcados para recibir formación de seguimiento. 3. **Métricas de respuesta a incidentes**: evalúe qué tan bien responden los empleados a incidentes de seguridad reales, particularmente en términos de informes oportunos, cumplimiento de los procedimientos y participación en los esfuerzos de mitigación. 4. **Métricas de la cultura de concientización sobre la seguridad**: las encuestas y los comentarios de los empleados ayudan a medir la efectividad de los programas de capacitación e identificar las áreas que requieren mejora.

9.6 Mejora continua

El programa de capacitación siempre está evolucionando en función de los comentarios, las tendencias de la industria y las amenazas emergentes.

- **Revisiones trimestrales**: reuniones periódicas con TI, RR.HH. y el equipo de seguridad para revisar los últimos resultados de simulaciones de phishing, informes de incidentes y comentarios sobre capacitación.
- **Amenazas emergentes**: se desarrolla nuevo contenido de capacitación a medida que surgen nuevas amenazas, lo que garantiza que los empleados estén siempre equipados para defenderse contra los

últimos métodos de ataque.
- **Bucle de retroalimentación continua**: se anima a los empleados a brindar comentarios sobre la experiencia de capacitación y sugerir áreas de mejora, asegurando que la capacitación siga siendo relevante, atractiva y efectiva.

Aquí hay una presentación **detallada, ampliada** y **realista** de las medidas de seguridad de UNICEF para **Seguridad física**, **Seguridad de proveedores y terceros**, **Auditorías y monitoreo de seguridad** y procesos asociados, completos con **cronogramas procesables** y formato **claro y estructurado**.

---

10. Seguridad Física

UNICEF emplea una estrategia integral de seguridad física para salvaguardar sus datos, infraestructura y personal en todas sus operaciones globales. El enfoque incluye control de acceso avanzado, vigilancia y monitoreo ambiental para garantizar que las instalaciones críticas estén seguras contra amenazas internas y externas.

10.1 Seguridad del centro de datos

Los centros de datos de UNICEF son activos críticos que albergan datos y sistemas confidenciales esenciales para las operaciones de la organización en todo el mundo. Es primordial proteger estos activos de amenazas a la seguridad física, como acceso no autorizado, robo, vandalismo y peligros ambientales (por ejemplo, incendios, inundaciones).

Medidas de seguridad:

- **Control de Acceso Biométrico**:
    - **Objetivo**: Garantizar que solo el personal autorizado pueda acceder a áreas de alta seguridad dentro del centro de datos, como salas de servidores, infraestructura de red y otras ubicaciones sensibles.
    - **Proceso**: UNICEF emplea **controles de acceso biométricos** (por ejemplo, **escáneres de huellas dactilares**, **escáneres de retina** y **reconocimiento facial**) en todas las áreas de alta seguridad dentro de sus datos. centros. Estos sistemas registran cada entrada y salida, lo cual se rastrea y revisa periódicamente para garantizar que solo las personas autorizadas tengan acceso.
    - **Cronograma**: Los sistemas de acceso biométrico se someten a una **revisión anual** para comprobar su eficiencia y precisión. Además, los permisos de acceso se actualizan **trimestralmente** para reflejar los cambios en las funciones y responsabilidades del personal. Por ejemplo, el personal de TI puede tener privilegios de acceso más amplios, que se actualizan según sea necesario.
        - **Ejemplo**: En el **Centro de datos de Ginebra**, los sistemas biométricos garantizan que solo un grupo selecto de personal de TI tenga acceso a la infraestructura central. El personal de seguridad realiza revisiones mensuales de los registros para identificar

irregularidades o intentos de acceso no autorizados, garantizando el cumplimiento de los protocolos internos de seguridad.

- **Sistemas de Vigilancia**:
  - **Objetivo**: Monitorear continuamente las instalaciones para detectar cualquier acceso físico no autorizado o actividad sospechosa.
  - **Proceso**: Se instalan cámaras CCTV de alta definición en todos los centros de datos, con **capacidades de visión nocturna infrarroja y diurna** para monitoreo las 24 horas, los 7 días de la semana. Estas cámaras están integradas en un avanzado **sistema de gestión de vigilancia**, que proporciona **alertas en tiempo real** ante cualquier actividad inusual. Las transmisiones de vigilancia son monitoreadas constantemente por el **Centro de Operaciones de Seguridad Global (GSOC)**, que es responsable de la coordinación de la respuesta a incidentes.
  - **Cronología**: las cámaras CCTV se **inspeccionan semanalmente** para garantizar su correcto funcionamiento. Existe un **ciclo de mantenimiento mensual** para calibrar las cámaras y verificar si hay algún mal funcionamiento del sistema. El sistema almacena imágenes de vigilancia durante **30 días**, después de lo cual se archiva para conservarlas a largo plazo. Cualquier actividad sospechosa registrada es revisada por agentes de seguridad dentro de **24 horas**.
    - **Ejemplo**: El **Centro de datos de Nueva York** está equipado con más de **300 cámaras de alta definición**, con **sensores de movimiento** que pueden detectar movimiento en tiempo real. En caso de cualquier movimiento sospechoso, el sistema envía una notificación instantánea al **equipo de seguridad**, quien puede tomar medidas inmediatas. Anomalías como un intento de eludir las puertas de seguridad o acceder a zonas restringidas se marcan y se derivan para una mayor investigación.
- **Controles ambientales**:
  - **Objetivo**: Proteger la infraestructura de TI crítica de daños causados por peligros ambientales, como incendios, inundaciones y fluctuaciones de temperatura.
  - **Proceso**: Todos los centros de datos están equipados con **controles ambientales** de última generación, incluidos **sistemas de extinción de incendios** (por ejemplo, **gas halón**), **detección de inundaciones. sensores** y **controles de temperatura y humedad** (sistemas HVAC). Los sistemas de extinción de incendios están diseñados para evitar la propagación del fuego sin dañar los equipos electrónicos sensibles. Se realizan **simulacros de peligros ambientales** y **simulacros** regulares para garantizar que los sistemas funcionen según lo previsto durante las emergencias.
  - **Cronograma**: Los sistemas ambientales se someten a **verificaciones de diagnóstico mensuales** por parte de equipos internos y contratistas externos. Además, se realizan **auditorías anuales de seguridad contra incendios e inundaciones** para garantizar el cumplimiento de las normas de seguridad y la preparación operativa.
    - **Ejemplo**: en **Singapur**, el centro de datos tiene **sensores de detección de inundaciones** que alertan inmediatamente a los equipos de seguridad si los niveles de

agua superan un determinado umbral. En caso de incendio, el **sistema de supresión de halones** se activa automáticamente. Un contratista externo realiza una verificación de diagnóstico de rutina cada **primer lunes del mes** para garantizar que toda la infraestructura esté en pleno funcionamiento.

10.2 Seguridad de la oficina

Las instalaciones de oficinas de UNICEF son otro aspecto crucial de su infraestructura de seguridad física. Estas oficinas albergan a empleados, contratistas y visitantes, y es imperativo mantener estrictos protocolos de seguridad para proteger tanto al personal como a la información confidencial.

Medidas de seguridad:

- **Acceso con tarjeta inteligente**:
    - **Objetivo**: Regular y controlar el acceso a áreas seguras dentro de la oficina, asegurando que solo el personal autorizado pueda ingresar a lugares sensibles como salas de reuniones, laboratorios y salas de servidores.
    - **Proceso**: UNICEF utiliza **tecnología de tarjetas inteligentes** para el control de acceso. Cada empleado, contratista y visitante recibe una **tarjeta inteligente** que brinda acceso a áreas específicas dentro de la oficina. Las tarjetas inteligentes están integradas con **autenticación por código PIN** y cada intento de acceso se registra. El equipo de seguridad revisa periódicamente estos registros para garantizar el cumplimiento.
    - **Cronograma**: los registros de acceso se revisan **mensualmente** y cualquier discrepancia se deriva al equipo de seguridad para una investigación inmediata. Además, se realizan **actualizaciones trimestrales** en el sistema de tarjetas inteligentes para garantizar que los permisos de acceso reflejen las funciones y niveles de autorización actuales de los empleados.
        - **Ejemplo**: En la **sede de UNICEF en Nueva York**, el **edificio principal, las salas de servidores y los laboratorios de investigación** están protegidos con acceso con tarjeta inteligente. Cuando el rol de un empleado cambia (por ejemplo, ascenso, transferencia), sus privilegios de acceso se actualizan dentro de **24 horas** para garantizar que solo el personal autorizado pueda acceder a áreas sensibles.
- **Sistema de Gestión de Visitantes**:
    - **Objetivo**: Garantizar que todos los visitantes a las oficinas de UNICEF sean identificados, rastreados y acompañados adecuadamente en áreas sensibles.
    - **Proceso**: Todos los visitantes deben **registrarse** en el mostrador de recepción a su llegada. Se les solicita que proporcionen una **identificación con fotografía** válida e indiquen el propósito de su visita. Los visitantes reciben una **insignia de visitante** que es válida durante la duración de su visita. A los visitantes que acceden a áreas sensibles se les asigna un escolta de un empleado, que garantiza que permanezcan en las zonas autorizadas.
    - **Cronograma**: los registros de visitantes se revisan **trimestralmente** para garantizar que el sistema funcione de manera eficiente. Cualquier tendencia o problema de seguridad (como

intentos de acceso no autorizados o visitas sin acompañamiento) se aborda de inmediato y los protocolos de seguridad se ajustan en consecuencia.

- **Ejemplo**: En la **Oficina de Ginebra de UNICEF**, los visitantes de áreas de alta seguridad como los laboratorios de investigación y los centros de datos deben usar **insignias de visitante con seguimiento** y estar acompañados por un empleado en todo momento. El sistema también registra la hora exacta de entrada y salida, proporcionando un historial detallado de todas las visitas para auditorías de seguridad.

Resumen y mejora continua

La estrategia de **Seguridad física** de UNICEF está diseñada para proteger sus datos e infraestructura críticos de amenazas tanto internas como externas. A través de un estricto control de acceso, vigilancia y monitoreo ambiental, la organización garantiza que todas sus instalaciones sean seguras y cumplan con los estándares de seguridad globales. Se realizan auditorías y revisiones periódicas para mejorar continuamente los sistemas, y todas las medidas de seguridad se integran con **Centros de operaciones de seguridad global (GSOC)** para garantizar el monitoreo en tiempo real y la respuesta a incidentes.

Cronograma para la revisión y las mejoras de seguridad:

- **Mensual**: Verificación de sistemas de vigilancia, auditorías de acceso a tarjetas inteligentes, revisión de registros de visitantes.
- **Trimestral**: actualizaciones de permisos de acceso, auditoría del sistema de visitantes, ajustes de protocolos de seguridad.
- **Anualmente**: revisión integral de sistemas biométricos, sistemas de extinción de incendios y auditorías de seguridad ambiental proporcionadas por los proveedores.

Aquí hay una versión ampliada y más detallada de la sección **Seguridad de proveedores y terceros**, que incorpora procesos operativos, cronogramas y ejemplos del mundo real más completos:

---

11. Seguridad de proveedores y terceros

Dada la naturaleza crítica de los servicios de terceros para apoyar las operaciones de UNICEF, garantizar la seguridad y el cumplimiento de estos socios externos es vital. UNICEF se adhiere a prácticas rigurosas de gestión de riesgos de proveedores y realiza evaluaciones de seguridad exhaustivas para mitigar los riesgos asociados con proveedores externos.

11.1 Gestión de riesgos de proveedores

Antes de incorporar cualquier proveedor o servicio de terceros, UNICEF garantiza que la postura de seguridad del proveedor cumpla o supere los estándares de la industria y cumpla con las regulaciones pertinentes. Esto incluye una revisión exhaustiva del manejo de datos, los protocolos de seguridad y el cumplimiento legal del proveedor.

Evaluación de seguridad e incorporación:

- **Evaluaciones de seguridad**:
    - **Objetivo**: Garantizar que los proveedores se alineen con las políticas de protección de datos, las medidas de seguridad de la red y los requisitos normativos internacionales de UNICEF.
    - **Proceso**: todos los proveedores potenciales se someten a una **evaluación de seguridad** inicial antes de ser incorporados. Esta evaluación cubre una variedad de factores, que incluyen:
        - **Políticas de protección de datos**: ¿Tiene el proveedor medidas adecuadas para el cifrado de datos, el almacenamiento seguro y la transmisión segura de información confidencial?
        - **Cumplimiento de los estándares regulatorios**: ¿Cumple el proveedor las leyes internacionales como los estándares **GDPR**, **HIPAA** e **ISO 27001**?
        - **Protocolos de seguridad de red**: ¿El proveedor implementa cortafuegos, sistemas de detección de intrusiones (IDS) y protección de terminales eficaces para proteger sus sistemas?
    - **Cronograma**: el proceso de evaluación de seguridad generalmente se completa **dentro de los 30 días** de iniciar una relación con el proveedor. Después de la incorporación, UNICEF realiza **revisiones bianuales** para garantizar el cumplimiento continuo de los protocolos de seguridad.
        - **Ejemplo**: al seleccionar un **proveedor de almacenamiento en la nube**, UNICEF exige que el proveedor presente un informe detallado sobre sus **estándares de cifrado de datos**, incluido el uso de **cifrado de extremo a extremo* y autenticación multifactor para acceder a archivos confidenciales. Este informe es revisado por el equipo de seguridad de UNICEF y auditores externos, garantizando la alineación con el estándar de cumplimiento **ISO 27001**.
- **Protección de datos y cumplimiento**:
    - **Objetivo**: Garantizar que todos los proveedores manejen datos personales y confidenciales de conformidad con las leyes globales de protección de datos.
    - **Proceso**: todos los proveedores deben firmar un **Acuerdo de procesamiento de datos (DPA)** que describe las expectativas para el manejo, almacenamiento y protección de datos, en particular para la **información de identificación personal (PII)**. Además, se espera que los proveedores proporcionen **evaluaciones de cumplimiento anuales** o informes que demuestren el cumplimiento de las normas de protección de datos como **GDPR**, **HIPAA** y **CCPA**.
    - **Cronograma**: el **DPA** se revisa y firma durante la fase de negociación del contrato, con **revisiones anuales** programadas para coincidir con el período de renovación del contrato. Los proveedores deben presentar **informes trimestrales de cumplimiento de seguridad**, para garantizar que estén continuamente en línea con los requisitos reglamentarios.
        - **Ejemplo**: el **proveedor externo de servicios en la nube** de UNICEF debe someterse a una **auditoría trimestral de protección de datos**, centrándose en el cifrado de datos, las políticas de retención de datos y los controles de acceso de los usuarios. El proveedor debe enviar un informe de cumplimiento actualizado cada trimestre para confirmar el

cumplimiento del **GDPR** y las leyes de protección de datos. El incumplimiento de los requisitos de auditoría puede dar lugar a una revisión o rescisión del contrato.

11.2 Auditorías de seguridad de terceros

Las auditorías de seguridad anuales son esenciales para verificar el cumplimiento por parte del proveedor de las estrictas políticas de seguridad de UNICEF. Estas auditorías, realizadas por organizaciones independientes de terceros, evalúan los controles internos de los proveedores, las medidas de protección de datos y el cumplimiento de los estándares de la industria.

Proceso de auditorías de seguridad:

- **Auditorías de Seguridad Anuales**:
    - **Objetivo**: Realizar una revisión integral de la postura de seguridad del proveedor, centrándose en áreas como gestión de riesgos, cifrado de datos, control de acceso, respuesta a incidentes y gestión de vulnerabilidades.
    - **Proceso**: UNICEF emplea auditores externos acreditados como **KPMG**, **PwC** y **Deloitte** para realizar **auditorías de seguridad anuales**. Estas auditorías evalúan el cumplimiento por parte del proveedor de las mejores prácticas en ciberseguridad y protección de datos, que incluyen:
        - **Análisis de vulnerabilidades**: identificación de posibles debilidades en la infraestructura de red y las configuraciones del sistema del proveedor.
        - **Verificación de cumplimiento**: garantizar que el proveedor cumpla con los estándares regulatorios globales (por ejemplo, **ISO 27001**, **GDPR**, **NIST**).
        - **Preparación para la respuesta a incidentes**: evaluación de la capacidad del proveedor para detectar, responder y recuperarse de incidentes de seguridad, como violaciones de datos o compromisos del sistema.
    - **Cronograma**: estas auditorías se realizan **anualmente** y los hallazgos se informan dentro de los **30 días** posteriores a la finalización de la auditoría. Si se identifica una vulnerabilidad importante o un problema de incumplimiento, se programan auditorías de seguimiento antes.
        - **Ejemplo**: una **auditoría anual** de un **proveedor de servicios de TI administrados** puede descubrir varios sistemas de software obsoletos con vulnerabilidades conocidas. El equipo de auditoría proporcionará un **plan de acción correctiva de 30 días** para que el proveedor aborde estos problemas y actualice sus sistemas.
- **Seguimiento de los hallazgos de la auditoría**:
    - **Objetivo**: Garantizar que el proveedor aborde de inmediato cualquier vulnerabilidad o falla de cumplimiento identificada durante una auditoría para mitigar los posibles riesgos de seguridad.
    - **Proceso**: Después de cada auditoría, UNICEF programa una **reunión de seguimiento** con el proveedor para discutir los hallazgos y acordar un **plan de acción correctiva (CAP)**. Este plan describe los pasos de remediación específicos, los plazos para su finalización y las responsabilidades asignadas a ambas partes.

- **Cronograma**: las acciones correctivas para **vulnerabilidades críticas** (por ejemplo, fallas de seguridad sin parches o acceso no autorizado) deben implementarse **dentro de los 30 días**. Para **hallazgos no críticos**, como mejoras menores de procedimiento, el proveedor tiene hasta **90 días** para implementar los cambios necesarios. UNICEF monitorea el progreso de estas acciones a través de reuniones y actualizaciones periódicas.

    - **Ejemplo**: después de una auditoría de un **proveedor de almacenamiento en la nube** externo, se descubrió que sus controles de acceso a ciertos repositorios de datos no estaban adecuadamente protegidos. UNICEF emitió un **plan de acción correctiva de 30 días**, exigiendo al proveedor mejorar su cifrado e implementar medidas de autenticación de usuarios más sólidas. El proveedor actualizó con éxito sus protocolos dentro del plazo asignado.

11.3 Baja de proveedores y eliminación de datos

Cuando se termina una relación con un proveedor, UNICEF garantiza que se revoque todo acceso a los proveedores y que los datos confidenciales se devuelvan o destruyan de forma segura.

Medidas de seguridad:

- **Terminación del acceso**: al finalizar el contrato del proveedor, todas las credenciales y cuentas de acceso se desactivan inmediatamente, y todos los dispositivos o sistemas proporcionados al proveedor se devuelven o se borran de forma segura.
- **Destrucción de datos**: todos los datos almacenados por el proveedor se devuelven a UNICEF o se destruyen de forma segura, siguiendo las mejores prácticas de la industria para **desinfección de datos**.
- **Cronograma**: la destrucción de datos se produce dentro de los **30 días** posteriores a la terminación del contrato, con un certificado firmado por el proveedor que confirma la finalización del proceso.
    - **Ejemplo**: cuando UNICEF finaliza un contrato con un **proveedor de análisis de datos**, el proveedor debe presentar un **Certificado de destrucción de datos** dentro de **30 días**, confirmando que todos los datos almacenados por UNICEF en sus sistemas se ha eliminado y borrado de forma segura de todos los dispositivos.

Resumen y seguimiento continuo

Las prácticas de **Seguridad de proveedores y terceros** de UNICEF garantizan que los proveedores cumplan estándares rigurosos de protección de datos, cumplimiento y gestión de riesgos. Al realizar **evaluaciones de seguridad**, **auditorías** y **monitoreo continuo**, UNICEF mantiene una cadena de suministro segura y garantiza que los datos confidenciales estén protegidos en todas las etapas de la relación con los proveedores.

Cronograma para la gestión de seguridad de proveedores:

- **Evaluación inicial**: completada dentro de los **30 días** posteriores a la contratación del proveedor.
- **Revisión semestral de proveedores**: se realiza cada **6 meses**.

- **Auditorías de seguridad anuales**: se realizan una vez al año, con acciones de seguimiento completadas dentro de **30-90 días** dependiendo de la gravedad de los hallazgos.
- **Desincorporación y eliminación de datos**: finalizada dentro de los **30 días** posteriores a la terminación del contrato.

---

12. Auditorías y monitoreo de seguridad

12.1 Monitoreo continuo

El seguimiento continuo es un componente esencial de la estrategia de ciberseguridad de UNICEF. Implica el seguimiento en tiempo real de sistemas, tráfico de red y puntos finales para detectar amenazas y responder rápidamente a incidentes de seguridad. Las herramientas de monitoreo son fundamentales para garantizar que las posibles vulnerabilidades o ataques se identifiquen temprano, lo que permite una rápida mitigación.

Herramientas de monitoreo:

- **Splunk**:
    - **Objetivo**: Splunk sirve como una plataforma de **administración de registros centralizada** y de **análisis en tiempo real** para monitorear todos los sistemas y redes críticos. La herramienta agrega datos de múltiples fuentes, incluidos servidores, dispositivos de red, plataformas en la nube, firewalls y puntos finales, para proporcionar información detallada sobre la postura general de seguridad.
    - **Proceso**: los datos se recopilan, normalizan y analizan para generar **alertas en tiempo real** sobre anomalías que podrían indicar amenazas potenciales, como intentos de acceso no autorizados, actividad sospechosa de los usuarios o errores de configuración. Esto permite que el **Centro de operaciones de seguridad (SOC)** identifique y responda rápidamente a incidentes de seguridad.
    - **Cronograma**: el monitoreo continuo está activo **24 horas al día, 7 días a la semana**, con evaluaciones mensuales de los procesos de agregación y alertas para garantizar que no haya brechas en la recopilación de datos. El equipo SOC revisa los registros de seguridad en tiempo real y realiza **auditorías mensuales** para garantizar la precisión e integridad de los datos. **Trimestralmente** se realizan actualizaciones periódicas de las reglas de monitoreo y de los feeds de inteligencia sobre amenazas para adaptarse a las amenazas emergentes.
        - **Acciones clave**:
        - **Generación de alertas en tiempo real** cuando se detecta actividad inusual en la red o inicios de sesión no autorizados.
        - **Análisis detallado** e investigación de todos los incidentes marcados por Splunk, lo que permite una rápida identificación de posibles infracciones.
- **Halcón CrowdStrike**:
    - **Objetivo**: CrowdStrike proporciona **protección de endpoints** mediante el monitoreo en tiempo real de todos los dispositivos, detectando malware, ransomware y comportamientos anormales indicativos de un ciberataque.

- **Proceso**: la herramienta monitorea continuamente los puntos finales (servidores, computadoras portátiles, dispositivos móviles, etc.) en busca de actividades inusuales como modificaciones de archivos, acceso no autorizado a datos confidenciales o la ejecución de malware conocido. Al detectar cualquier amenaza, CrowdStrike aísla el punto final afectado, evitando la propagación de la amenaza y enviando una alerta al equipo SOC.

- **Cronología**: la supervisión se ejecuta **24 horas al día, 7 días a la semana**, con **actualizaciones semanales** y parches para garantizar que los puntos finales estén protegidos de las últimas amenazas. El equipo SOC recibe alertas en tiempo real, con revisiones diarias del estado de los puntos finales en toda la organización.

    - **Acciones clave**:
    - **Aislamiento de malware o ransomware**: cuando se detecta actividad maliciosa, CrowdStrike aísla el punto final para evitar una mayor propagación.
    - **Alertas de incidentes en tiempo real** enviadas al SOC, lo que permite una respuesta inmediata para evitar daños.

- **Herramientas de análisis de tráfico de red (por ejemplo, Darktrace)**:

    - **Objetivo**: Darktrace utiliza **inteligencia artificial (IA)** y aprendizaje automático para detectar **comportamientos anómalos de la red** que pueden indicar una amenaza a la ciberseguridad, incluida la exfiltración de datos, el movimiento lateral no autorizado o patrones de acceso anormales.

    - **Proceso**: Darktrace utiliza IA para establecer una línea de base del comportamiento normal del tráfico de red. Una vez que se establecen los patrones de referencia, detecta automáticamente desviaciones que pueden sugerir un ataque en curso. El sistema envía alertas al SOC cuando se identifican patrones sospechosos, como acceso no autorizado a datos confidenciales, tráfico saliente inusual o intentos de eludir los controles de seguridad de la red.

    - **Cronología**: se realiza un monitoreo continuo y en tiempo real, con **evaluaciones trimestrales** de las capacidades de detección de amenazas y políticas de análisis del tráfico de red. Se realizan actualizaciones periódicas de los modelos de IA para mantenerse al día con las técnicas de ataque emergentes.

        - **Acciones clave**:
        - **Detección de anomalías basada en IA** para identificar posibles amenazas internas o cuentas comprometidas.
        - **Alertas en tiempo real** y notificaciones cuando se detecta tráfico anormal o actividades sospechosas.

12.2 Auditorías Externas

Las auditorías externas desempeñan un papel fundamental para garantizar que la infraestructura de seguridad de UNICEF cumpla con las regulaciones y estándares globales pertinentes. Estas auditorías ayudan a garantizar que la organización mantenga altos estándares de seguridad y se alinee con las mejores prácticas para la gestión de riesgos, la protección de datos y los controles del sistema.

Proceso de auditoría:

- **Auditorías de Cumplimiento ISO 27001 y GDPR**:
    - **Objetivo**: Evaluar la eficacia del Sistema de Gestión de Seguridad de la Información (SGSI) de UNICEF de acuerdo con **ISO 27001** y verificar el cumplimiento de las leyes globales de protección de datos, como el **Reglamento General de Protección de Datos (GDPR) **.
    - **Proceso**: UNICEF contrata auditores externos independientes para realizar revisiones integrales de su marco de seguridad y prácticas de protección de datos. Los auditores evalúan diversos aspectos, entre ellos:
        - **Procesos de gestión de riesgos**: Evaluar cómo se identifican, evalúan y mitigan los riesgos en toda la organización.
        - **Medidas de Protección de Datos**: Revisión del cifrado de datos, controles de acceso y mecanismos de cumplimiento del RGPD.
        - **Procedimientos de respuesta a incidentes**: probar la preparación y eficacia de la respuesta a violaciones de datos o incidentes de seguridad.
        - **Controles de acceso**: garantizar que solo las personas autorizadas puedan acceder a datos y sistemas confidenciales.
    - **Cronograma**: **Se realizan auditorías anuales**, generalmente a partir del **1T**, y los informes se entregan dentro de los **30 a 45 días** posteriores a la finalización de la auditoría. Los hallazgos se utilizan para informar acciones correctivas y mejoras de procesos. Cualquier problema inmediato se aborda y resuelve en un plazo de **30 días**.
        - **Acciones clave**:
        - **Auditoría ISO 27001**: Evaluación de políticas y controles generales de SGSI para garantizar que cumplan con los estándares internacionales.
        - **Verificación de cumplimiento del RGPD**: Revisión de prácticas para garantizar que los datos personales se procesen y protejan de acuerdo con la regulación.
        - **Acciones correctivas de seguimiento**: Pronta implementación de cualquier acción correctiva identificada durante la auditoría.
- **Seguimiento de los hallazgos de la auditoría**:
    - **Objetivo**: Garantizar que las vulnerabilidades identificadas o los problemas de cumplimiento se aborden de manera rápida y efectiva.
    - **Proceso**: Después de cada auditoría, se lleva a cabo una reunión de seguimiento entre el equipo de seguridad de UNICEF, los auditores externos y las partes interesadas relevantes. Se crea un plan de acción correctiva (CAP) para abordar los hallazgos. UNICEF trabaja en estrecha colaboración con auditores externos y equipos internos para resolver problemas de manera rápida y eficiente.
    - **Cronograma**: las acciones correctivas generalmente se completan dentro de **30 días** para problemas de alta prioridad (por ejemplo, vulnerabilidades de seguridad o incumplimiento de regulaciones críticas). Los problemas menos críticos se solucionan en un plazo de **60 a 90 días**.
        - **Acciones clave**:
        - **Remediación inmediata** de vulnerabilidades de alta prioridad.

        - **Documentación de las acciones correctivas** tomadas y verificación de que los problemas han sido resueltos.
        - **Seguimiento de avances** a través de reuniones de seguimiento y auditorías internas.

- **Auditorías de Vigilancia ISO 27001**:

    - **Objetivo**: Garantizar que el SGSI de UNICEF siga cumpliendo con los estándares ISO 27001 y que las medidas de seguridad se mejoren continuamente.
    - **Proceso**: Las auditorías de vigilancia ISO 27001 se realizan anualmente y evalúan la capacidad de la organización para mantener y mejorar su SGSI. La auditoría incluye una revisión de la efectividad de las estrategias de gestión de riesgos, las prácticas de manejo de información, los procedimientos de respuesta a incidentes y el conocimiento de los empleados sobre los protocolos de seguridad.
    - **Cronograma**: estas auditorías se realizan **anualmente** y la organización debe realizar mejoras en función de los hallazgos de la auditoría. El proceso generalmente comienza en el **T2** con una auditoría de seguimiento realizada al final del año para verificar la implementación de acciones correctivas.

12.3 Integración de auditoría y respuesta a incidentes

Integrar auditorías de seguridad con protocolos de respuesta a incidentes es crucial para garantizar que los problemas de seguridad se resuelvan de manera eficiente y que la organización aprenda de incidentes pasados para mejorar sus defensas.

Integración de gestión de incidentes:

- **Objetivo**: Garantizar que los resultados de las auditorías y las herramientas de monitoreo continuo respalden acciones de respuesta a incidentes rápidas y efectivas.

- **Proceso**: cuando se detecta un incidente de seguridad, el equipo SOC colabora con los equipos de TI, legales y de cumplimiento para evaluar el alcance del incidente. Se revisan los resultados de la auditoría y los datos de herramientas de monitoreo como Splunk, CrowdStrike y Darktrace para comprender cómo ocurrió la infracción, qué sistemas se vieron afectados y cómo se podría mejorar la respuesta en el futuro.

- **Cronograma**: la respuesta a incidentes comienza inmediatamente después de la detección de una amenaza, y la contención y el análisis iniciales se llevan a cabo en **minutos u horas**, dependiendo de la gravedad del incidente. Las revisiones posteriores al incidente se llevan a cabo **dentro de los 7 días** para evaluar la efectividad de la respuesta e integrar las lecciones aprendidas en futuras estrategias de seguridad.

    - **Acciones clave**:
    - **Revisión post-incidente** para identificar brechas en los controles de seguridad.
    - **Colaboración con auditores externos** para evaluar el impacto del incidente y garantizar que todos los hallazgos de la auditoría se incorporen al plan de respuesta.
    - **Mejora de los planes de respuesta a incidentes** basado en comentarios de auditoría.

Resumen y cronograma para auditorías y monitoreo de seguridad:

- **El monitoreo continuo** con herramientas como Splunk, CrowdStrike y Darktrace está operativo **24 horas al día, 7 días a la semana** con alertas en tiempo real y actualizaciones semanales para mantener una protección óptima del sistema.
- Las **Auditorías anuales** (ISO 27001, GDPR, etc.) las completan auditores externos y generalmente se realizan dentro de **30 a 45 días** de la finalización de la auditoría, seguidas de acciones correctivas inmediatas si es necesario.
- Las **Revisiones posteriores al incidente** se integran con herramientas de monitoreo y comentarios de auditoría, y las acciones correctivas se inician **dentro de los 30 días** para problemas críticos y **90 días** para hallazgos menos graves.

---

13. Ciclo de control y revisión de documentos

Para garantizar la eficacia y relevancia continuas de las políticas, procedimientos y controles de seguridad, UNICEF emplea un **Ciclo de revisión y control de documentos** formal. Este ciclo garantiza que toda la documentación relacionada con la seguridad se evalúe, actualice y mantenga continuamente en consonancia con la evolución de las amenazas, los requisitos normativos y los cambios organizativos.

13.1 Revisión de políticas

El proceso de revisión de políticas es fundamental para garantizar que las políticas de seguridad de UNICEF se mantengan actualizadas con los riesgos, estándares legales y mejores prácticas actuales.

- **Objetivo**: Evaluar y actualizar periódicamente las políticas y prácticas de seguridad en respuesta a las amenazas de seguridad cambiantes, los avances tecnológicos y los requisitos normativos.
- **Cronograma**: las políticas de seguridad se revisan **anualmente** para garantizar que sigan siendo efectivas y relevantes. En casos de una violación de seguridad o un cambio regulatorio significativo, se activa una revisión de la política de inmediato y las actualizaciones se realizan dentro de **30 días**.

Proceso de revisión:

1. **Revisión anual**:
    - Cada año, se revisan exhaustivamente todas las políticas y directrices de seguridad. Esto garantiza que todos los procedimientos reflejen las mejores prácticas más recientes y cumplan con los estándares de la industria y los requisitos legales.
    - Durante la revisión se tienen en cuenta todos los cambios internos, como actualizaciones del sistema, modificaciones de políticas o cambios operativos.
2. **Revisión posterior al incidente**:
    - Si ocurre un incidente de seguridad, se lleva a cabo una revisión inmediata de las políticas relevantes para determinar su efectividad para mitigar la amenaza. Después de la revisión, se realizan las actualizaciones necesarias para evitar incidentes futuros. Estas actualizaciones deben implementarse dentro de **30 días**.
3. **Revisiones ad hoc**:
    - En respuesta a nuevos riesgos emergentes, cambios regulatorios o avances tecnológicos, las políticas pueden revisarse fuera del ciclo de revisión programado. Estas revisiones se inician de

inmediato y las actualizaciones se realizan dentro de los **30 días** posteriores a la identificación.

13.2 Control de documentos

El control de documentos garantiza que las políticas de seguridad, los procedimientos y los documentos relacionados se mantengan, actualicen y almacenen adecuadamente de forma segura y accesible.

- **Objetivo**: Garantizar que toda la documentación de seguridad tenga versiones controladas, se almacene de forma segura y solo sea accesible para el personal autorizado.
- **Proceso**:
    1. **Repositorio centralizado**: todos los documentos relacionados con la seguridad se almacenan en un repositorio centralizado y seguro. El acceso a este repositorio está estrictamente controlado y sólo el personal autorizado puede modificar o aprobar documentos.
    2. **Control de versiones**: se emplea un estricto mecanismo de control de versiones para garantizar que se conserven las versiones históricas de los documentos mientras solo se utiliza activamente la última versión. Cualquier cambio en los documentos se rastrea con un historial de versiones detallado, incluidas las fechas de modificación y los motivos de los cambios.
    3. **Proceso de aprobación**: antes de finalizar o actualizar un documento, debe pasar por un proceso de aprobación formal. Este proceso garantiza que las partes interesadas relevantes, incluidos los equipos legales, de seguridad y de cumplimiento, revisen y aprueben los cambios antes de su adopción.
- **Cronología**:
    - **Auditorías mensuales de documentos**: todos los documentos de seguridad se auditan mensualmente para garantizar que estén actualizados, sean relevantes y estén alineados con las regulaciones más recientes.
    - **Ciclo de revisión trimestral**: además de las auditorías mensuales, trimestralmente se realiza una revisión más completa de todos los documentos de seguridad. Este proceso garantiza que la documentación sea completa y esté alineada con la estrategia de seguridad actual.

13.3 Comunicación y capacitación de documentos

La comunicación y la capacitación efectivas garantizan que todos los empleados y partes interesadas relevantes comprendan y cumplan con las políticas de seguridad actualizadas.

- **Objetivo**: Garantizar que las actualizaciones de las políticas de seguridad se comuniquen de manera efectiva a todas las partes relevantes y que los miembros del personal estén capacitados para implementar medidas de seguridad nuevas o revisadas.
- **Proceso**:
    1. **Comunicación de cambios de políticas**: Todos los cambios de políticas se comunican a los empleados y partes interesadas a través de canales de comunicación internos, como correo electrónico, publicaciones en intranet o boletines de seguridad. Esto garantiza que todos estén informados sobre las actualizaciones y comprendan sus responsabilidades.
    2. **Capacitación sobre políticas actualizadas**: los empleados deben completar sesiones de capacitación sobre políticas nuevas o actualizadas. Esto garantiza que todos los miembros del

personal estén equipados con los conocimientos y habilidades necesarios para cumplir con las medidas de seguridad actualizadas.
3. **Seguimiento del cumplimiento**: El cumplimiento de los requisitos de capacitación se rastrea a través de un sistema de certificación. Los registros de finalización de la capacitación se almacenan y revisan durante las auditorías para garantizar que todo el personal relevante esté actualizado sobre los protocolos de seguridad.

- **Cronología**:
  - **Capacitación Bianual**: La capacitación sobre políticas de seguridad se realiza al menos dos veces al año. Se programan sesiones de capacitación adicionales según sea necesario luego de cambios importantes en las políticas o incidentes de seguridad.

13.4 Auditoría y revisión de cumplimiento

Para garantizar que el proceso de control de documentos se siga correctamente, se realizan auditorías y revisiones de cumplimiento periódicas.

- **Objetivo**: Verificar que todas las políticas y documentos de seguridad se estén revisando, actualizando y siguiendo de acuerdo con los procedimientos internos y los requisitos regulatorios externos.

- **Proceso**:

1. **Auditorías internas**: Se realizan auditorías internas periódicamente para evaluar el cumplimiento de los procedimientos de control de documentos. Estas auditorías evalúan si las políticas se están revisando y actualizando de acuerdo con los cronogramas establecidos y si se están implementando todos los cambios necesarios.
2. **Auditorías de cumplimiento**: se realizan auditorías de cumplimiento anuales para verificar que el proceso de control de documentos se alinea con los requisitos reglamentarios como **ISO 27001**, **GDPR** y otros estándares relevantes. Estas auditorías también evalúan la eficacia de la documentación de seguridad para cumplir con los objetivos generales de seguridad de la organización.

- **Cronología**:
  - **Auditorías Internas**: Realizadas trimestralmente para asegurar la efectividad del ciclo de control y revisión de documentos.
  - **Auditorías de Cumplimiento**: Se realizan anualmente para evaluar el cumplimiento de los estándares de la industria y los requisitos reglamentarios.

13.5 Elementos clave del ciclo de revisión y control de documentos

- **Revisiones periódicas**: las políticas de seguridad se revisan anualmente y se actualizan según sea necesario. Las revisiones inmediatas se producen después de incidentes o cambios regulatorios importantes.
- **Control de versiones**: Los documentos se mantienen con un estricto control de versiones para garantizar la trazabilidad de los cambios.
- **Aprobación y capacitación**: las políticas de seguridad se someten a un proceso de aprobación formal y van seguidas de capacitación para todas las partes interesadas relevantes.

- **Auditorías de cumplimiento**: Tanto las auditorías internas como las externas garantizan el cumplimiento del proceso de control de documentos y el cumplimiento general de los estándares de seguridad.

---

14. Mejora Continua

La mejora continua es un componente fundamental de la estrategia de ciberseguridad de UNICEF. Este proceso garantiza que las medidas de seguridad estén siempre evolucionando en respuesta a amenazas emergentes, nuevos desarrollos tecnológicos y lecciones aprendidas de incidentes de seguridad anteriores. UNICEF tiene como objetivo mantener una postura de seguridad proactiva y adaptable para salvaguardar su infraestructura, datos y operaciones.

14.1 Marco para la mejora continua

El marco de mejora continua sigue un enfoque estructurado de varios pasos para mejorar las prácticas de seguridad a lo largo del tiempo. Este proceso está diseñado para abordar las brechas de seguridad actuales, integrar nuevas tecnologías y garantizar el cumplimiento de los últimos estándares y regulaciones.

Componentes clave:

- **Adaptación**: responder a nuevos riesgos de seguridad, tácticas de actores de amenazas y cambios regulatorios.
- **Eficiencia**: Agilizar procesos y eliminar ineficiencias en la detección, prevención y respuesta a amenazas.
- **Innovación**: adoptar tecnologías y metodologías avanzadas para mantenerse a la vanguardia de las ciberamenazas en evolución.
- **Resiliencia**: Fortalecer la capacidad de la organización para prevenir, detectar y recuperarse de incidentes de seguridad.

14.2 Bucles de retroalimentación de seguridad

Los circuitos de retroalimentación de seguridad son vitales para el proceso de mejora continua. Estos bucles capturan información de diversas fuentes, como evaluaciones internas, revisiones de incidentes, comentarios de los empleados e inteligencia sobre amenazas de la industria. Son fundamentales para perfeccionar las políticas, los procedimientos y las herramientas de seguridad.

Fuentes de comentarios:

- **Revisiones de incidentes**: después de cualquier incidente de seguridad importante, se realiza un análisis post-mortem para identificar las causas fundamentales y las áreas de mejora en las prácticas de seguridad. Estos hallazgos informan directamente las revisiones de las políticas de seguridad.
    - **Cronograma**: las revisiones posteriores al incidente se llevan a cabo dentro de las **48 horas** de un evento y los planes de acción para mejorar se crean dentro de los **30 días**.
- **Comentarios de los empleados**: se utilizan encuestas periódicas y debates internos para recopilar comentarios del personal sobre la eficacia de los programas de capacitación en seguridad, las herramientas y la concienciación general sobre la seguridad.

    - **Cronograma**: los comentarios se recopilan cada dos años y se toman medidas inmediatas para los problemas urgentes identificados en las encuestas.

- **Inteligencia sobre amenazas**: UNICEF aprovecha la inteligencia sobre amenazas compartida por socios externos, organismos gubernamentales y grupos industriales para obtener información sobre las amenazas emergentes y las tácticas utilizadas por los ciberdelincuentes. Esta información se utiliza para ajustar las medidas de seguridad internas en consecuencia.

    - **Cronología**: la inteligencia sobre amenazas se monitorea e integra continuamente en el marco de seguridad de la organización.

14.3 Evaluaciones y auditorías de seguridad

Las evaluaciones y auditorías de seguridad periódicas son esenciales para identificar vulnerabilidades, medir la eficacia de las medidas de seguridad actuales y garantizar el cumplimiento de las regulaciones de la industria. Estas evaluaciones ayudan a identificar brechas en los controles de seguridad y brindan una base para priorizar las mejoras.

Tipos de evaluaciones de seguridad:

- **Análisis de vulnerabilidades y pruebas de penetración**: se realizan análisis de vulnerabilidades y pruebas de penetración periódicamente para simular ataques e identificar debilidades en el sistema.

    - **Cronograma**: las evaluaciones de vulnerabilidad se llevan a cabo **trimestralmente**, con solución inmediata de los problemas críticos identificados. Las pruebas de penetración se realizan **anualmente** o después de cambios significativos en el sistema.

- **Auditorías de cumplimiento**: para garantizar el cumplimiento de estándares regulatorios como GDPR, ISO 27001 y otros marcos relevantes, UNICEF se somete a auditorías internas y externas periódicas.

    - **Cronograma**: Las auditorías de cumplimiento se realizan **anualmente**, con un seguimiento continuo para un cumplimiento continuo durante todo el año.

- **Auditorías de terceros**: se contratan empresas de seguridad externas para auditar las prácticas de seguridad de proveedores y contratistas externos, garantizando que cumplan con los estándares de seguridad y privacidad de UNICEF.

    - **Cronograma**: Se realizan auditorías de terceros anualmente y se requieren evaluaciones de seguimiento si se identifica alguna brecha de seguridad.

14.4 Adopción e integración de tecnología

La adopción de nuevas tecnologías es una estrategia clave para mejorar la postura de seguridad de UNICEF. La evaluación continua de las herramientas y técnicas emergentes garantiza que la organización se mantenga a la vanguardia de las nuevas amenazas y cumpla con las regulaciones en evolución.

Áreas clave de enfoque:

- **Automatización y orquestación**: la automatización de la detección de amenazas, la respuesta a incidentes y los flujos de trabajo de seguridad ayuda a reducir los errores humanos, aumentar la eficiencia operativa y acelerar los tiempos de respuesta.
    - **Cronograma**: Las tecnologías de automatización se evalúan para su integración **cada seis meses**. Se implementan nuevas herramientas de automatización en función de la efectividad y las necesidades organizacionales.
- **Inteligencia artificial (IA) y aprendizaje automático (ML)**: la IA y el ML se integran en los sistemas de detección de amenazas para mejorar la precisión y la velocidad en la identificación de amenazas potenciales. Estas tecnologías ayudan a identificar patrones que serían difíciles de detectar para los analistas humanos.
    - **Cronograma**: las herramientas de IA y ML se revisan para su integración **trimestralmente**, con capacitación continua de estos sistemas para mejorar las capacidades de detección.
- **Herramientas de seguridad de próxima generación**: UNICEF revisa periódicamente su uso de firewalls, protección de terminales y herramientas de monitoreo de red de próxima generación. El objetivo es garantizar que se utilicen las herramientas más recientes, que incorporan inteligencia avanzada sobre amenazas y análisis de comportamiento, para proteger la organización.
    - **Cronología**: se realiza una revisión de las herramientas y sistemas de seguridad **cada dos años** y las actualizaciones se programan en función de los cambios en el panorama de amenazas y los avances tecnológicos.

14.5 Capacitación y concientización de los empleados

La sensibilización de los empleados es un elemento fundamental de la estrategia de mejora continua de UNICEF. Como el elemento humano suele ser el eslabón más débil de la ciberseguridad, se diseñan programas de formación y concientización continua para garantizar que los empleados estén preparados para reconocer y responder a amenazas potenciales.

Programas de formación:

- **Capacitación continua en seguridad**: todos los empleados reciben capacitación en concientización sobre seguridad que se actualiza periódicamente para reflejar las últimas amenazas y mejores prácticas. Esto incluye capacitación sobre phishing, administración de contraseñas, manejo seguro de datos y notificación de incidentes.
    - **Cronograma**: la capacitación en seguridad se lleva a cabo **trimestralmente**, con cursos de actualización obligatorios para los empleados que no hayan completado la capacitación en los últimos seis meses.
- **Simulaciones de phishing**: los ataques de phishing simulados se llevan a cabo periódicamente para probar el conocimiento y la preparación de los empleados para identificar intentos de phishing. Los resultados de estas simulaciones guían futuras mejoras en la capacitación.
    - **Cronograma**: las simulaciones de phishing se llevan a cabo **cada dos años** y se brinda capacitación de seguimiento específica a los empleados que no pasan las pruebas.

- **Programa de Campeones de Seguridad**: Ciertos empleados son designados como campeones de seguridad dentro de sus equipos. Estos campeones promueven las mejores prácticas de seguridad, fomentan la concientización y actúan como enlace entre sus equipos y el departamento de seguridad.
    - **Cronología**: los campeones de seguridad se seleccionan **anualmente**, con controles y evaluaciones periódicas sobre su eficacia a la hora de promover la seguridad dentro de sus equipos.

14.6 Indicadores clave de rendimiento (KPI)

Para medir la eficacia de los esfuerzos de mejora continua, UNICEF utiliza indicadores clave de rendimiento (KPI). Estos KPI ayudan a realizar un seguimiento del progreso, identificar áreas de mejora y evaluar el impacto de los cambios realizados en los protocolos y herramientas de seguridad.

Los KPI clave incluyen:

- **Tiempo de detección de incidentes**: el tiempo promedio que se tarda en detectar un incidente de seguridad desde el punto de ocurrencia.
- **Tiempo de respuesta**: El tiempo necesario para contener y resolver un incidente de seguridad una vez detectado.
- **Tasa de corrección de vulnerabilidades**: el porcentaje de vulnerabilidades identificadas que se abordan dentro de plazos específicos.
- **Eficacia de la formación**: Medida por la tasa de finalización de las sesiones de formación y la tasa de éxito en simulaciones de phishing.
- **Estado de cumplimiento**: el nivel de cumplimiento de las políticas de seguridad internas, así como de las regulaciones externas (por ejemplo, GDPR, ISO 27001).

14.7 Informes y documentación

Todos los esfuerzos de mejora continua están documentados para mantener la responsabilidad y brindar transparencia a las partes interesadas internas y externas. Los informes periódicos sobre el progreso de las iniciativas de mejora, los hallazgos de las auditorías, las actividades de capacitación y la gestión de vulnerabilidades se comparten con la alta dirección y, cuando es necesario, con los auditores externos.

Documentación:

- **Informes trimestrales**: informes detallados sobre el estado de las iniciativas de mejora de la seguridad en curso, incluidas evaluaciones, auditorías y métricas de respuesta a incidentes.
    - **Cronograma**: los informes se envían **trimestralmente**, con una revisión anual integral que resume las actividades, mejoras y resultados del año.
- **Revisión anual de seguridad**: una revisión integral de la postura de seguridad de la organización, incluida la efectividad de las políticas, tecnologías y programas de capacitación, así como la respuesta de la organización a nuevas amenazas y cambios regulatorios.
    - **Cronograma**: la revisión de seguridad anual se completa **al final de cada año fiscal**, centrándose en establecer objetivos para el año siguiente.

14.8 Gobernanza y supervisión

El proceso de mejora continua es supervisado por la alta dirección de UNICEF, y se proporcionan actualizaciones periódicas a la junta directiva y a las partes interesadas pertinentes. Esto garantiza que la seguridad siga siendo una prioridad en todos los niveles de la organización y que se asignen recursos para mejorar los controles de seguridad.

Gobernanza:

- **Comité directivo de seguridad**: un comité interdisciplinario formado por altos directivos, departamentos legales, de seguridad de TI, de cumplimiento y otros departamentos relevantes se reúne periódicamente para revisar el desempeño de la seguridad y guiar los esfuerzos de mejora.
    - **Cronograma**: el Comité Directivo de Seguridad se reúne **trimestralmente** para revisar el progreso y ajustar la estrategia de seguridad de la organización según sea necesario.

---

15. Amenazas emergentes y tendencias de seguridad futuras

UNICEF se compromete a adelantarse a los cambiantes desafíos de seguridad para proteger sus datos, infraestructura y operaciones confidenciales. Este enfoque prospectivo implica prepararse para las amenazas emergentes y adoptar tecnologías de vanguardia que puedan ayudar a mitigar los riesgos y mejorar la resiliencia general de la ciberseguridad.

15.1 Ransomware y protección de datos

El ransomware sigue siendo una de las amenazas cibernéticas más importantes para las organizaciones de todo el mundo, incluidas aquellas de los sectores humanitarios y de desarrollo internacional como UNICEF. A medida que los ciberdelincuentes desarrollan variedades de ransomware más sofisticadas, es esencial fortalecer las defensas y las capacidades de respuesta.

Estrategias de mitigación de ransomware:

- **Estrategias de respaldo**: UNICEF mejora continuamente sus estrategias de respaldo para garantizar que los datos críticos se almacenen de forma segura y puedan restaurarse rápidamente en caso de un ataque de ransomware. Se realizan **pruebas de respaldo** periódicas para verificar los procedimientos de recuperación y garantizar la integridad de los datos.
    - **Cronograma**: los sistemas de respaldo se prueban trimestralmente y se realizan ejercicios de restauración completos **anualmente** para validar los procesos de recuperación de datos.
- **Protección de terminales**: utilizando **herramientas avanzadas de protección de terminales**, como **CrowdStrike Falcon**, UNICEF trabaja para evitar que el ransomware llegue a los terminales mediante análisis de comportamiento, detección de anomalías y respuesta en tiempo real.
    - **Cronología**: las herramientas de protección de endpoints se actualizan continuamente con la última información sobre amenazas para mantenerse a la vanguardia de la evolución de las tácticas de ransomware. Se realizan actualizaciones mensuales para las bases de datos de firmas y las reglas de detección.
- **Planes de respuesta a incidentes**: para minimizar el impacto de los ataques de ransomware, el **plan de respuesta a incidentes (IR)** de UNICEF incorpora procedimientos detallados de contención,

comunicación y recuperación. El plan se prueba y actualiza periódicamente.

    - **Cronograma**: el plan IR se revisa y actualiza **anualmente**. Cada dos años se realizan simulaciones de respuesta específicas de ransomware y ejercicios prácticos.

- **Capacitación para empleados**: el phishing sigue siendo un vector principal de infecciones de ransomware, por lo que se llevan a cabo simulaciones de phishing y concientización continua sobre la seguridad para garantizar que los empleados estén preparados para identificar correos electrónicos sospechosos.

    - **Cronograma**: la capacitación sobre concientización sobre phishing se lleva a cabo trimestralmente y los ataques de phishing simulados se ejecutan **cada dos años** para evaluar la preparación de los empleados.

15.2 Inteligencia artificial y aprendizaje automático en seguridad

La Inteligencia Artificial (IA) y el Aprendizaje Automático (ML) están desempeñando un papel cada vez más importante en la ciberseguridad al mejorar la detección y la respuesta a las amenazas a la seguridad. Estas tecnologías pueden ayudar a UNICEF a identificar amenazas emergentes, predecir vulnerabilidades potenciales y automatizar respuestas a incidentes.

Integración de IA y ML:

- **Detección y análisis de amenazas**: UNICEF está invirtiendo en tecnologías de IA/ML para mejorar la detección de amenazas persistentes avanzadas (APT), amenazas internas y vulnerabilidades de día cero. Al analizar grandes volúmenes de datos, los sistemas de inteligencia artificial pueden identificar patrones y anomalías que podrían pasar desapercibidas para los sistemas tradicionales.

    - **Cronología**: las herramientas de IA/ML se evalúan y perfeccionan continuamente para adaptarse a nuevas amenazas. **Anualmente** se realiza una evaluación exhaustiva de las herramientas de detección de amenazas basadas en IA.

- **Análisis de comportamiento**: se utilizan algoritmos de aprendizaje automático para monitorear el comportamiento de los usuarios y dispositivos en la red, creando perfiles de referencia. Cualquier desviación de la línea de base puede activar alertas, lo que permite una identificación más rápida de amenazas potenciales.

    - **Cronología**: las herramientas de análisis de comportamiento se actualizan y calibran **trimestralmente** para mejorar la precisión de la detección y minimizar los falsos positivos.

- **Respuesta automatizada a incidentes**: AI/ML también se utiliza para automatizar ciertos aspectos del proceso de respuesta a incidentes, como bloquear el tráfico malicioso, aislar sistemas comprometidos y aplicar parches de seguridad. Esto reduce el tiempo de respuesta y ayuda a contener las amenazas de forma más eficaz.

    - **Cronograma**: los procesos de respuesta automatizados se evalúan cada seis meses y se implementan actualizaciones según sea necesario en función de la nueva inteligencia sobre amenazas.

15.3 Arquitectura de confianza cero (ZTA)

A medida que las organizaciones continúan enfrentando riesgos de seguridad en evolución, el modelo de seguridad tradicional basado en perímetros se vuelve cada vez más ineficaz. UNICEF está haciendo la transición a una **Arquitectura de Confianza Cero (ZTA)**, que supone que no se puede confiar en ningún usuario o dispositivo, ya sea dentro o fuera de la red, de forma predeterminada.

Implementación de confianza cero:

- **Gestión de identidad y acceso (IAM)**: la base de ZTA es el principio de privilegio mínimo, lo que significa que los usuarios solo tienen acceso a los recursos específicos que necesitan para realizar sus tareas. **La autenticación multifactor (MFA)** y estrictos **controles de acceso** se aplican a todos los usuarios, dispositivos y aplicaciones.
    - **Cronograma**: la implementación de ZTA está en curso. Se requiere MFA para todos los sistemas críticos, con auditorías periódicas de los controles de acceso realizadas cada 6 meses para garantizar el cumplimiento del modelo Zero Trust.
- **Microsegmentación**: para evitar el movimiento lateral en caso de una infracción, UNICEF está implementando **microsegmentación** en toda su red. Esto implica segmentar la red en partes más pequeñas y aisladas, de modo que incluso si un segmento se ve comprometido, el atacante no pueda moverse libremente por toda la red.
    - **Cronograma**: la segmentación de la red y la implementación de ZTA están en fases, y se espera un progreso significativo para fines de **2025**. Los hitos clave incluyen completar la implementación de la microsegmentación en zonas críticas de la red en **12 meses**.
- **Autenticación y monitoreo continuos**: en un entorno Zero Trust, la autenticación es continua y todo el tráfico se monitorea para detectar comportamientos inusuales. Esto incluye evaluar la confiabilidad de los dispositivos y usuarios en cada etapa de la interacción, independientemente de su ubicación.
    - **Cronograma**: los mecanismos de autenticación continua se están implementando de manera incremental y se espera que la implementación inicial se realice en el **segundo trimestre de 2025**. Se realizan controles y ajustes continuos a medida que el sistema madura.

15.4 Seguridad en la nube y el cambio a la nube primero

A medida que más servicios y aplicaciones se trasladan a la nube, proteger los entornos de nube es una prioridad cada vez mayor. La estrategia de UNICEF incluye adoptar un **enfoque que dé prioridad a la nube**, garantizando al mismo tiempo que los servicios en la nube cumplan con rigurosos estándares de seguridad y cumplan con las regulaciones pertinentes de protección de datos.

Medidas de seguridad en la nube:

- **Agentes de seguridad de acceso a la nube (CASB)**: UNICEF utiliza **CASB** para monitorear y controlar el movimiento de datos a través de varias plataformas en la nube, garantizando que el acceso a los datos se gobierne adecuadamente y que las políticas de seguridad se apliquen de manera consistente.
    - **Cronograma**: las soluciones CASB se implementarán en todas las principales plataformas en la nube para **mediados de 2025**, con monitoreo y ajuste continuos según las necesidades de seguridad en evolución.

- **Cifrado en la nube**: todos los datos confidenciales almacenados en la nube se cifran tanto en tránsito como en reposo. Las claves de cifrado se gestionan a través de un sistema seguro para evitar el acceso no autorizado.
    - **Cronograma**: las estrategias de cifrado en la nube se revisan **anualmente** para garantizar que se alineen con los estándares de cifrado en evolución y los requisitos de cumplimiento.
- **Gestión de riesgos de proveedores**: a medida que UNICEF continúa colaborando con proveedores externos de servicios en la nube, las prácticas de gestión de riesgos de los proveedores garantizan que estos proveedores cumplan con los estándares de seguridad, las regulaciones de protección de datos y las políticas internas.
    - **Cronograma**: las auditorías de seguridad de los proveedores se realizan **anualmente**, y se activan evaluaciones adicionales después de cualquier actualización importante del contrato o cambio en el servicio de nube.

15.5 Colaboración e intercambio de inteligencia sobre amenazas

Ante las amenazas que evolucionan rápidamente, la ciberseguridad se está volviendo cada vez más colaborativa. UNICEF participa activamente en iniciativas de intercambio de información y colabora con otras organizaciones, líderes industriales y entidades gubernamentales para intercambiar inteligencia sobre amenazas.

Esfuerzos de colaboración:

- **Asociaciones público-privadas**: UNICEF colabora con agencias gubernamentales, organizaciones no gubernamentales (ONG) y empresas de ciberseguridad del sector privado para mantenerse informado sobre nuevas amenazas y compartir mejores prácticas.
    - **Cronología**: las asociaciones se revisan y actualizan **anualmente**, y se realizan intercambios periódicos de inteligencia sobre amenazas a medida que hay nueva información disponible.
- **Grupos y foros industriales**: UNICEF es un miembro activo de varios foros y grupos industriales de ciberseguridad, donde se comparte inteligencia sobre amenazas y se discuten medidas de defensa conjuntas.
    - **Cronología**: La participación en grupos de la industria se produce de forma continua, con actualizaciones trimestrales sobre inteligencia de amenazas y nuevas técnicas de ciberdefensa.

15.6 Inteligencia artificial y sistemas de seguridad autónomos

Como parte de su estrategia de futuro, UNICEF está explorando el uso de **sistemas de seguridad autónomos** impulsados por IA para monitorear, detectar y responder de manera proactiva a las amenazas cibernéticas sin intervención humana directa. Estos sistemas utilizarán algoritmos de aprendizaje automático para analizar grandes cantidades de datos de red y tomar decisiones de seguridad en tiempo real.

Planes de implementación:

- **Detección de amenazas impulsada por IA**: se desarrollarán modelos avanzados de aprendizaje automático para detectar tipos nuevos y desconocidos de amenazas cibernéticas mediante el análisis

de patrones de tráfico de red, comportamientos de los usuarios y anomalías del sistema.

    - **Cronograma**: se espera que la fase piloto de detección de amenazas basada en IA comience a **finales de 2025**, y la implementación completa está programada para **2027**.

- **Sistemas de respuesta autónomos**: a medida que las tecnologías de inteligencia artificial maduren, UNICEF planea integrar capacidades de respuesta de seguridad autónomas, donde el sistema pueda tomar medidas (por ejemplo, bloquear el tráfico malicioso, aislar puntos finales infectados) sin requerir intervención manual.

    - **Cronograma**: La implementación completa de los sistemas de respuesta autónomos está prevista para **2027**, y la implementación gradual comenzará en **2026**.

15.7 Computación cuántica y criptografía poscuántica

Se espera que la computación cuántica revolucione el campo de la ciberseguridad, con el potencial de romper los esquemas de cifrado actuales y la capacidad de ofrecer modelos de cifrado más sólidos. UNICEF está monitoreando activamente los avances en la **criptografía poscuántica (PQC)**, asegurándose de que esté preparado para la transición a métodos criptográficos resistentes a los cuánticos.

Estrategia PQC:

- **Seguimiento de los avances cuánticos**: UNICEF está siguiendo los avances en la computación cuántica y la criptografía poscuántica para anticipar la necesidad de un cambio hacia protocolos de cifrado cuánticos seguros.
    - **Cronograma**: se está desarrollando una estrategia formal para la transición a la criptografía poscuántica, con la investigación y preparación iniciales programadas para **2026**.