Desarrollo de un Sistema Básico de Gestión de Seguridad de la Información (SGSI) para una Organización Pública.

Organización Mundial de la Salud.

El alcance del SGSI de la OMS incluye varios elementos clave:

1. **Tipos de Información**: Abarca toda la información manejada por la OMS, incluyendo datos de salud pública, información personal de pacientes, investigaciones, y documentación administrativa.
2. **Actividades y Procesos**: Incluye todos los procesos que gestionan información, desde la recolección y almacenamiento hasta la distribución y eliminación de datos.
3. **Infraestructura**: Considera los sistemas tecnológicos, redes y recursos humanos involucrados en el manejo de la información.
4. **Cumplimiento Normativo**: Se asegura de que se cumplan todas las leyes y regulaciones pertinentes, así como las políticas internas de la OMS.

Identificación de Activos de Información.

Datos de Salud	Información sobre enfermedades, brotes, estadísticas de salud pública y datos epidemiológicos.
Registros de Pacientes	Información personal y clínica relacionada con individuos, especialmente en el contexto de estudios y programas de salud.
Documentación de Políticas	Guías, protocolos y normativas que rigen la salud pública y la práctica médica.
Investigaciones	Estudios, informes y publicaciones científicas que contribuyen al conocimiento y las mejores prácticas en salud.
Sistemas de Información	Plataformas y aplicaciones utilizadas para recopilar, almacenar y analizar datos de salud.
Recursos Humanos	Información sobre el personal, incluyendo credenciales, formación y habilidades.

Redes y Comunicaciones	Infraestructura de TI que permite la comunicación interna y externa, así como la transmisión de datos.
Propiedad Intelectual	Patentes, derechos de autor y otros derechos relacionados con investigaciones y desarrollos en salud.
Auditorías y Evaluaciones	Documentos y datos relacionados con la evaluación de programas y el cumplimiento normativo.

Las ubicaciones físicas incluidas en el Sistema de Gestión de la Seguridad de la Información (SGSI) de la OMS abarcan varias áreas clave, que pueden incluir:

Oficinas Centrales: La sede principal de la OMS, donde se gestionan operaciones y toma de decisiones.

Oficinas Regionales: Sedes en diferentes regiones del mundo que coordinan actividades específicas de salud pública.

Centros de Investigación: Instalaciones dedicadas a la investigación y análisis de datos de salud.

Centros de Datos: Lugares donde se almacenan y procesan grandes volúmenes de información.

Instalaciones de Capacitación: Espacios donde se realizan entrenamientos y capacitaciones para el personal.

Ubicaciones de Colaboración: Espacios donde se llevan a cabo reuniones y proyectos conjuntos con socios externos y gobiernos.

Instalaciones de Respuesta a Emergencias: Lugares designados para coordinar respuestas rápidas a crisis de salud pública.

Nodos de Comunicaciones: Puntos clave en la infraestructura de TI que facilitan la comunicación interna y externa.

El Sistema de Gestión de Seguridad de la Información (SGSI) de la OMS incluye varias redes, entornos en la nube y máquinas virtuales para garantizar la seguridad de la información y los datos. Aunque no pude acceder a información específica actualizada, en general, estos pueden incluir:

1. **Redes Seguras**: Redes internas protegidas con cortafuegos y sistemas de detección de intrusos. VPNs (Redes Privadas Virtuales) para acceso seguro a datos sensibles.
2. **Entornos en la Nube**: Servicios en la nube pública y privada, que pueden incluir plataformas como AWS, Azure o Google Cloud. Almacenamiento en la nube para datos de investigación y operativos, con cifrado y controles de acceso.
3. **Máquinas Virtuales**: Infraestructura virtualizada para ejecutar aplicaciones y almacenar datos de manera aislada. Contenedores y orquestadores como Docker y Kubernetes para gestión de aplicaciones y microservicios.

En el marco del Sistema de Gestión de Seguridad de la Información (SGSI) de la OMS, se manejan varios sistemas y tipos de datos. Estos pueden incluir:

Sistemas bajo el control del SGSI:

Sistemas de Información de Salud: Sistemas de gestión de datos clínicos y epidemiológicos.

Sistemas de Comunicación: Herramientas de colaboración interna, como correos electrónicos y plataformas de mensajería.

Bases de Datos: Bases de datos que almacenan información sobre investigaciones, estudios de salud y estadísticas.

Infraestructura de TI: Servidores, redes y dispositivos de almacenamiento que soportan operaciones y servicios.

Sistemas de Gestión de Proyectos: Herramientas para el seguimiento de proyectos y colaboraciones internacionales.

Tipos de datos bajo control:

1. **Datos Personales**:
    a. Información de identificación personal (PII) de empleados, colaboradores y participantes en estudios de salud.
2. **Datos de Salud**:
    a. Registros clínicos, resultados de pruebas y datos de pacientes.
3. **Datos Financieros**:
    a. Información relacionada con presupuestos, gastos y financiamiento de proyectos.
4. **Datos de Investigación**:

    a. Resultados de estudios y ensayos clínicos, así como datos recopilados en investigaciones.
5. **Datos de Seguridad**:
    a. Información sobre incidentes de seguridad, auditorías y evaluaciones de riesgo.
6. **Documentación Operativa**:
    a. Políticas, procedimientos y protocolos relacionados con la gestión de la seguridad de la información.

Identificación de las partes clave y a su vez le asignamos responsabilidades para actividades de la información.

- **Equipo de TI**
  Responsabilidades:
    - Implementar y mantener las infraestructuras de seguridad (firewalls, sistemas de detección de intrusos).
    - Realizar auditorías de seguridad y evaluaciones de riesgos.
    - Gestionar el acceso a sistemas y datos sensibles.
- **Gestión**
  Responsabilidades:
    - Establecer políticas de seguridad de la información.
    - Aprobar presupuestos y recursos para iniciativas de seguridad.
    - Promover una cultura de seguridad dentro de la organización.
- **Empleados**
  Responsabilidades:
    - Cumplir con las políticas y procedimientos de seguridad establecidos.
    - Reportar incidentes de seguridad o vulnerabilidades.
    - Participar en capacitaciones y sesiones informativas sobre seguridad de la información.
- **Ciudadanos/Estudiantes/Pacientes**
  Responsabilidades:
    - Proporcionar datos personales e información de salud de manera segura y consciente.
    - Ser conscientes de sus derechos en relación con la privacidad y la protección de datos.
    - Informar sobre cualquier posible violación de la seguridad de la información que puedan observar.
- **Proveedores de Servicios Externos**
  Responsabilidades:

    - Cumplir con los acuerdos de nivel de servicio (SLA) en materia de seguridad.
    - Implementar medidas de seguridad adecuadas en sus sistemas que interactúan con la OMS.
    - Participar en auditorías y revisiones de seguridad según sea necesario.
- **Comités de Ética y Gobernanza**
  Responsabilidades:
    - Supervisar el cumplimiento de las políticas de privacidad y ética en el manejo de datos.
    - Evaluar el impacto de la seguridad de la información en la investigación y la salud pública.
    - Proporcionar orientación sobre la gestión ética de los datos personales.

Propósito del SGSI

El propósito del SGSI de la OMS es garantizar la confidencialidad, integridad y disponibilidad de la información, protegiendo los datos sensibles y cumpliendo con normativas internacionales, para respaldar la misión de la organización en la promoción de la salud pública y la gestión de crisis sanitarias.

Alcance

El SGSI abarca:

Datos y sistemas que recopila los datos personales y de salud, procesados y almacenados por la OMS, también sistemas de información y tecnología utilizados para la gestión de datos. Por otra parte, abarca sistemas y plataformas en la nube utilizadas para la gestión de datos.

Metas

1. **Proteger la Información**:

   Implementar medidas de seguridad efectivas para proteger la información contra accesos no autorizados y pérdidas.

2. **Cumplimiento Normativo**:

Asegurar el cumplimiento de leyes y regulaciones internacionales sobre privacidad y protección de datos.

3. **Concienciación**:

   Fomentar una cultura de seguridad de la información entre todos los empleados y partes interesadas.

Objetivos

1. **Evaluación de Riesgos**:

   Realizar evaluaciones de riesgos periódicas para identificar y mitigar vulnerabilidades.

2. **Capacitación**:

   Proporcionar formación continua sobre seguridad de la información a todo el personal.

3. **Gestión de Incidentes**:

   Establecer un protocolo para la gestión de incidentes de seguridad, asegurando una respuesta rápida y efectiva.

4. **Auditoría y Mejora Continua**:

   Implementar un sistema de auditoría y revisión regular para evaluar la eficacia del SGSI y realizar mejoras.

Limitaciones y Exclusiones

1. **Alcance Geográfico**:

   El SGSI se aplica a las operaciones de la OMS, pero puede no abarcar actividades específicas de los Estados miembros o de otras organizaciones asociadas.

2. **Datos No Sensibles**:

Información que no se considera sensible, como datos públicos, puede no estar bajo el mismo nivel de control o protección.

3. **Recursos Limitados**:

   La implementación de todas las medidas de seguridad puede verse limitada por factores como presupuesto, recursos humanos y tecnología disponible.

4. **Dependencias Externas**:

   El SGSI depende de la cooperación y cumplimiento de los proveedores de servicios externos y otras partes interesadas, lo que puede limitar su efectividad.

Evaluación de Riesgo.

Lista de todos los activos.

HARDWARE	
Servidores	• Servidores de bases de datos • Servidores de aplicaciones • Servidores de correo electrónico • Servidores web
Dispositivos de red	• Firewalls • Routers y switches • Balanceadores de carga • Sistemas de detección/previsión de intrusiones (IDS/IPS)
Dispositivos de almacenamiento	NAS/SAN (Almacenamiento en red) • Discos duros externos y unidades flash USB
Equipos de usuarios finales	• Computadoras de escritorio y portátiles • Tablets y teléfonos móviles
Equipos de seguridad física	• Cámaras de vigilancia • Sistemas de control de acceso físico

	• Sensores y alarmas

SOFTWARE	
Sistemas operativos	• Windows Server, Linux, macOS • Sistemas operativos móviles (Android, iOS)
Software de gestión de bases de datos	MySQL, PostgreSQL, Oracle DB
Aplicaciones de gestión de recursos empresariales.	• ERP (SAP, Oracle ERP) • CRM (Salesforce) • Sistemas de gestión de salud y emergencias (que podrían ser específicos de la OMS)
Software específico de la OMS	• Herramientas de gestión de proyectos y colaboración para misiones humanitarias • Aplicaciones para el seguimiento de brotes de enfermedades • Sistemas de gestión de datos médicos • Sistemas de información geográfica (GIS)
Herramientas de ciberseguridad	• Antivirus y antimalware • Firewalls de aplicaciones web (WAF) • Sistemas de gestión de eventos de seguridad (SIEM)
Aplicaciones de comunicación	• Correo electrónico (Outlook, Gmail) • Herramientas de mensajería instantánea (Teams, Zoom)

DATOS	
Datos personales	• Información de identificación personal (PII) de empleados, colaboradores y pacientes • Registros médicos
Datos sensibles	• Informes sobre brotes de enfermedades y pandemias

	• Datos de investigación médica y científica • Información confidencial sobre suministros médicos y logística
Datos operacionales	• Planes estratégicos y operacionales de la OMS • Información sobre las operaciones humanitarias • Registros financieros y contables • Registros de acceso a sistemas y auditorías de seguridad
Backups de datos	• Copias de seguridad almacenadas localmente o en la nube • Planes de recuperación ante desastres

PERSONAL	
Empleados	• Personal administrativo y de soporte • Personal técnico (ingenieros de sistemas, especialistas en ciberseguridad) • Investigadores médicos y científicos • Personal de atención de salud en misiones humanitarias
Consultores y contratistas	• Especialistas externos en seguridad • Proveedores de soluciones tecnológicas
Colaboradores internacionales	• Equipos de respuesta rápida en situaciones de emergencia • Representantes de otros organismos de salud pública • Voluntarios y trabajadores de campo.
Usuarios con acceso privilegiado	• Administradores de sistemas y bases de datos • Responsables de seguridad de la información • Gestores de redes y servicios críticos.

Identificación de posibles amenazas que pueden afectar activos ya mencionados.

1. Activos Humanos (Empleados, Personal Médico y de TI).

Acceso no autorizado: Los empleados con privilegios excesivos o credenciales comprometidas podrían acceder a información confidencial de salud o información personal de pacientes.

Errores humanos: El personal puede cometer errores, como eliminar o modificar datos accidentalmente, o caer en ataques de phishing.

Insider threats (amenazas internas): Empleados descontentos o infiltrados pueden dañar o robar información confidencial de la OMS.

2. Activos de Información (Datos de Salud, Información Personal, Estudios Médicos).

Violación de datos: El acceso no autorizado a la información de pacientes, investigaciones sensibles o datos médicos puede exponer la privacidad de personas y comprometer proyectos importantes.

Pérdida de datos: Los datos pueden ser eliminados accidentalmente o por fallos en los sistemas de almacenamiento sin un sistema de respaldo adecuado.

Modificación no autorizada: Cambios no autorizados en datos críticos de salud, lo que podría comprometer investigaciones o diagnósticos médicos.

3. Infraestructura Tecnológica (Sistemas de TI, Redes, Servidores, Bases de Datos)

Malware y ransomware: Los sistemas pueden ser comprometidos por software malicioso, que puede cifrar datos importantes o hacer que el sistema sea inaccesible hasta que se pague un rescate.
Ataques de denegación de servicio (DDoS): Los atacantes pueden saturar los servidores con tráfico para interrumpir los servicios críticos, afectando operaciones importantes en la OMS.

Acceso no autorizado a servidores: Hackers pueden explotar vulnerabilidades en sistemas mal configurados o desactualizados para acceder a información crítica.

4. Aplicaciones Críticas (Software Médico, Plataformas de Gestión de Pacientes).

Vulnerabilidades en el software: Las aplicaciones pueden contener errores o puertas traseras que los atacantes pueden explotar para comprometer la información sensible.

Fallo de integridad en los datos: Cambios en los datos de pacientes o en los resultados médicos debido a fallos en las aplicaciones puede generar diagnósticos erróneos.

Acceso no autorizado a las aplicaciones: Si las aplicaciones no están adecuadamente protegidas, los atacantes podrían explotar credenciales débiles o vulnerabilidades para acceder a la información.

5. Infraestructura Física (Edificios, Centros de Datos, Equipos de Comunicación).

Desastres naturales: Inundaciones, terremotos o incendios pueden dañar tanto la infraestructura física como los sistemas de almacenamiento de datos.

Fallo de energía: Una interrupción eléctrica prolongada puede afectar las operaciones y provocar la pérdida de datos o la caída de servicios críticos.

Acceso físico no autorizado: Intrusos pueden acceder físicamente a áreas restringidas o equipos de TI sensibles, lo que facilita el robo o la alteración de datos.

Robo de hardware: Equipos críticos (como servidores, estaciones de trabajo o dispositivos médicos) pueden ser robados, comprometiendo la seguridad de la información.

6. Cumplimiento y Regulaciones (Leyes de Privacidad, Normativas Internacionales)

No conformidad: El incumplimiento de las regulaciones de privacidad y seguridad de los datos (como el RGPD o normativas específicas de la OMS) puede resultar en sanciones legales y pérdida de confianza pública.

Auditorías fallidas: La falta de controles o procesos de seguridad adecuados puede hacer que la OMS no pase auditorías de seguridad o normativas, lo que afectaría su reputación y operación.

Resumen de Evaluación de Probabilidad e Impacto:

Riesgo	Probabilidad	Impacto
Acceso no autorizado y amenazas internas	Media	Alto
Errores humanos y phishing	Alta	Medio
Violación de datos	Media-Alta	Alto
Malware, ransomware	Alta	Alto
Ataques DDoS	Media	Medio
Vulnerabilidades en el software	Media	Medio-Alto
Desastres naturales o fallos de infraestructura	Baja	Alto
Vulnerabilidades en proveedores externos	Media	Medio-Alto
Robo o sabotaje de dispositivos médicos	Baja-Media	Alto
Incumplimiento de regulaciones	Media	Alto

La **probabilidad alta** de que ocurran amenazas como errores humanos, ataques de phishing y ransomware sugiere la necesidad de controles fuertes y capacitación continua del personal. Las amenazas con **impacto alto** (como violaciones de datos, sabotaje de dispositivos médicos y ataques a la infraestructura) requieren estrategias de mitigación robustas, ya que un evento de este tipo podría tener graves repercusiones financieras, legales y reputacionales para la OMS.

Para seleccionar los controles de seguridad apropiados para mitigar los riesgos identificados en un Sistema de Gestión de Seguridad de la Información (SGSI) en una organización como la Organización Mundial de la Salud (OMS), es fundamental seguir un enfoque sistemático. Aquí se proporciona un enfoque basado en la norma ISO/IEC 27001, que es la norma reconocida internacionalmente para la gestión de la seguridad de la información. Los controles pueden agruparse en varias categorías clave:

1. Políticas y Procedimientos de Seguridad

- **Control**: Crear políticas y procedimientos de seguridad claros y actualizados para gestionar riesgos.
- **Justificación**: La OMS, como organismo internacional, maneja datos críticos de salud pública. Una política clara asegura que todos los empleados conozcan los protocolos de seguridad.

2. Controles Técnicos

- **Control de acceso**: Implementar un sistema de control de acceso basado en roles (RBAC) y autenticación multifactor (MFA) para garantizar que solo el personal autorizado acceda a los datos críticos.
  - **Justificación**: Evita accesos no autorizados a datos confidenciales, que podrían poner en riesgo la privacidad de los datos de salud.

3. Controles Administrativos

- **Gestión de incidentes**: Desarrollar un plan de respuesta a incidentes y de recuperación ante desastres.
  - **Justificación**: Permite a la OMS reaccionar rápida y eficazmente ante violaciones de seguridad, reduciendo el impacto de los ataques.
- **Evaluación de riesgos**: Realizar evaluaciones regulares de riesgos y auditorías de seguridad para identificar vulnerabilidades.

4. Gestión de Proveedores

- **Seguridad de proveedores**: Asegurarse de que los proveedores externos que manejan datos o sistemas críticos para la OMS cumplan con los requisitos de seguridad de la información.
  - **Justificación**: Los proveedores pueden ser una vía de entrada para ataques, por lo que es importante que estén alineados con las políticas de seguridad.

5. Gestión de Continuidad del Negocio

- **Plan de recuperación ante desastres (DRP)**: Implementar y probar regularmente un plan de recuperación que permita a la OMS continuar operando tras un ataque o desastre.

- **Justificación**: Garantiza la resiliencia de los servicios críticos y la minimización de interrupciones en situaciones de crisis.

6. Protección de la Privacidad

- **Cumplimiento de GDPR/Normas de privacidad**: Asegurar que el tratamiento de los datos personales cumpla con regulaciones internacionales como el GDPR.
  - **Justificación**: La OMS maneja datos personales sensibles de pacientes y ciudadanos de todo el mundo, por lo que debe cumplir con las normativas de privacidad más estrictas.

Redacción de una Política de Seguridad de alto nivel para la OMS.

La Organización Mundial de la Salud (OMS) reconoce la importancia crítica de proteger la confidencialidad, integridad y disponibilidad de la información. Esta política establece el marco general para garantizar la seguridad de la información en toda la organización, alineada con los más altos estándares internacionales.

Principios Fundamentales.

- **Confidencialidad:** La información de la OMS se mantendrá confidencial y se protegerá contra el acceso no autorizado.
- **Integridad:** La información de la OMS se mantendrá precisa, completa y confiable.
- **Disponibilidad:** Los recursos de información de la OMS estarán disponibles para los usuarios autorizados cuando se necesiten.

La OMS se compromete a:

Implementar un sistema de gestión de seguridad de la información.	Basado en normas internacionales reconocidas, como ISO/IEC 27001.
Proteger la información personal.	Cumpliendo con las leyes y regulaciones aplicables en materia de protección de datos.
Realizar evaluaciones de riesgos.	Identificando y gestionando de manera proactiva las amenazas a la seguridad de la información.
Proporcionar capacitación.	A todos los empleados sobre seguridad de la información, sensibilizándolos sobre las mejores prácticas.
Investigar y responder a incidentes de seguridad.	De manera oportuna y efectiva.
Mantener la continuidad del negocio.	Garantizando la disponibilidad de los servicios de información esenciales.

Alcance de la Política.

Esta política abarca, pero no se limita a:

- Sistemas de información.
- Redes de comunicaciones.
- Dispositivos móviles.
- Información almacenada en cualquier formato (digital o físico).

Control de Acceso a Usuarios.

Un control de acceso a usuarios es un conjunto de medidas y políticas que determinan quién puede acceder a qué recursos de información y cuándo.

Concesión	Modificación	Revocación
• **Solicitud formal:** Todo nuevo usuario debe realizar una solicitud formal, especificando los recursos a los que necesita acceder y justificando la necesidad. • **Evaluación de riesgos:** Se realizará una	• **Solicitud formal:** Cualquier modificación en los permisos de acceso debe ser solicitada formalmente. • **Reevaluación:** Se realizará una nueva evaluación de riesgos para verificar que la modificación no	• **Causas:** La revocación del acceso puede deberse a la terminación del empleo, cambio de rol, incumplimiento de las políticas de seguridad o cualquier otra razón justificada.

evaluación para determinar si el nivel de acceso solicitado es adecuado y si el usuario cumple con los requisitos de seguridad. • **Aprobación:** La concesión del acceso será aprobada por un supervisor o administrador de seguridad. • **Creación de cuentas:** Una vez aprobada, se creará una cuenta de usuario con los permisos asignados.	comprometa la seguridad. • **Aprobación:** La modificación será aprobada por un supervisor o administrador de seguridad.	• **Procedimiento:** Se realizará un procedimiento formal para revocar el acceso, incluyendo la desactivación de cuentas y la eliminación de permisos.

Las contraseñas son una de las primeras líneas de defensa en la seguridad de la información. La OMS debería establecer políticas de contraseñas robustas que incluyan:

- **Complejidad:**
  - Combinación de mayúsculas, minúsculas, números y caracteres especiales.
  - Longitud mínima de 12 caracteres.
  - Prohibición de utilizar información personal fácilmente adivinable (nombres, fechas de nacimiento, etc.).
- **Rotación:**
  - Cambio obligatorio de contraseña cada [número] de días.
  - Impedir el uso de contraseñas anteriores durante un período determinado.
- **Almacenamiento:**
  - Las contraseñas deben almacenarse de forma segura, utilizando algoritmos de cifrado fuertes y evitando el almacenamiento en texto plano.
- **Autenticación de dos factores:**

- Implementar la autenticación de dos factores para un nivel adicional de seguridad.

Plan de respuestas a Incidentes.

Un **incidente de seguridad** se define como cualquier evento o acción que comprometa o ponga en riesgo la confidencialidad, integridad o disponibilidad de los sistemas, datos o recursos de la OMS. Esto incluye, pero no se limita a:

- **Intentos no autorizados de acceso:** Logins fallidos, escaneos de puertos, intentos de intrusión.
- **Pérdida o robo de dispositivos:** Equipos portátiles, dispositivos de almacenamiento.
- **Descubrimiento de vulnerabilidades:** Software, hardware, configuraciones.
- **Ataques cibernéticos:** Malware, ransomware, phishing, DDoS.
- **Divulgación accidental de información confidencial:** Errores humanos, configuración incorrecta.

Procedimiento paso a paso:

Detección y Reporte.	• **Detección:** Los incidentes pueden ser detectados por sistemas de detección de intrusos (IDS), sistemas de prevención de intrusiones (IPS), registros de seguridad, o por usuarios finales que notifiquen actividades sospechosas. • **Reporte:** Cualquier persona que detecte un incidente debe informarlo inmediatamente al equipo de respuesta a incidentes (CSIRT) o a su supervisor. • **Recopilación de Evidencia:** El equipo CSIRT debe recopilar toda la evidencia posible, como registros de sistema, capturas de pantalla, y cualquier otra información relevante.

Evaluación y Clasificación.	• **Evaluación:** El equipo CSIRT evalúa la naturaleza y gravedad del incidente. • **Clasificación:** El incidente se clasifica según su impacto potencial (bajo, medio, alto) y su urgencia (baja, media, alta).
Contiene el Incidente.	• **Aislamiento:** Se aísla el sistema o red afectado para evitar la propagación del incidente. • **Contención:** Se implementan medidas para contener el incidente, como el bloqueo de cuentas, el cierre de puertos o la desconexión de dispositivos.
Erradicación.	• **Eliminación de la Causa:** Se identifica y elimina la causa raíz del incidente. • **Recuperación de Datos:** Se recuperan los datos afectados, si es posible.
Recuperación.	• **Restauración de los Sistemas:** Se restauran los sistemas a un estado operativo seguro. • **Actualización de Sistemas:** Se aplican parches y actualizaciones de seguridad.
Análisis Post-Incidente	• **Análisis:** Se realiza un análisis detallado del incidente para identificar las lecciones aprendidas. • **Documentación:** Se documenta el incidente y las acciones tomadas. • **Mejora Continua:** Se implementan medidas correctivas para prevenir incidentes similares en el futuro.

Roles y Responsabilidades

- **Equipo CSIRT:** Responsable de la detección, respuesta, y recuperación de incidentes de seguridad.
- **Administradores de Sistemas:** Responsables de la configuración y mantenimiento de los sistemas de información.
- **Usuarios Finales:** Responsables de reportar actividades sospechosas y seguir las políticas de seguridad.
- **Gerencia:** Responsable de proporcionar los recursos necesarios y de garantizar el cumplimiento de las políticas de seguridad.

Copia de Seguridad y Recuperación de Datos.

Procedimientos para Copias de Seguridad Regulares de Datos.

1. Definición de Datos a Resguardar:

- **Clasificación de Datos:** Se clasificarán los datos en función de su criticidad para la organización (alta, media, baja).
- **Identificación de Datos:** Se realizará un inventario detallado de todos los datos que deben ser respaldados, incluyendo sistemas operativos, aplicaciones, bases de datos, archivos de configuración y datos de usuario.

2. Frecuencia de Copias de Seguridad:

- **Datos Críticos:** Copias de seguridad diarias o incluso más frecuentes.
- **Datos Importantes:** Copias de seguridad semanales.
- **Datos Menores:** Copias de seguridad mensuales.

3. Medios de Almacenamiento:

- **Local:** Discos duros externos, cintas magnéticas.
- **Remoto:** Nube (AWS, Azure, Google Cloud), almacenamiento en otro sitio físico.
- **Combinación:** Se recomienda una combinación de ambos para mayor seguridad y redundancia.

4. Procedimientos de Copia de Seguridad:

- **Automatización:** Implementar herramientas de software para automatizar el proceso de copia de seguridad.
- **Verificación:** Verificar la integridad de las copias de seguridad de manera periódica.
- **Rotulación y Almacenamiento:** Rotular correctamente los medios de almacenamiento y almacenarlos en un lugar seguro y de fácil acceso.

5. Pruebas de Recuperación:

- **Periodicidad:** Realizar pruebas de recuperación de forma regular (mensual, trimestral).
- **Simulación:** Simular escenarios de desastre para verificar la capacidad de restaurar los datos.
- **Documentación:** Documentar los resultados de las pruebas y las acciones correctivas necesarias.

Roles y Responsabilidades

- **Administrador de Sistemas:**

    - Configurar y mantener los sistemas de respaldo.
    - Ejecutar las copias de seguridad de acuerdo con el cronograma establecido.
    - Verificar la integridad de las copias de seguridad.
- **Equipo de Seguridad:**
    - Desarrollar las políticas y procedimientos de respaldo.
    - Realizar auditorías de los sistemas de respaldo.
- **Equipo de TI:**
    - Asistir al administrador de sistemas en caso de problemas.
- **Usuarios:**
    - Realizar copias de seguridad locales de sus archivos importantes.

Ejemplo de un Plan de Copias de Seguridad:

Tipo de Datos	Tipo de Datos	Medio de Almacenamiento	Ubicación	Verificación
Datos Críticos	Diaria	Nube, Disco Local	Sitio Remoto y Local	Diaria
Datos Importantes	Semanal	Nube, Cinta	Sitio Remoto	Semanal
Datos Menores	Mensual	Disco Local	Sitio Local	Mensual

Concienciación y capacitación de los empleados.

Dotar a todos los empleados de la OMS de los conocimientos y habilidades necesarias para comprender y cumplir con las políticas de seguridad de la información, garantizando así la protección de los datos sensibles de la organización.

Objetivos Específicos

- Concientizar a los empleados sobre la importancia de la seguridad de la información y su papel en la protección de los datos de la OMS.
- Capacitar a los empleados en la identificación de amenazas comunes a la seguridad de la información.
- Instruir a los empleados sobre las políticas y procedimientos de seguridad de la OMS.
- Fomentar una cultura de seguridad de la información en toda la organización.

Contenido del Programa de Capacitación.

Módulo	Contenido	Duración estimada	Metodología
Módulo 1: Fundamentos de la Seguridad de la Información	Conceptos básicos de ciberseguridad, amenazas comunes (phishing, malware, ingeniería social), vulnerabilidades comunes (errores humanos, contraseñas débiles)	2 horas	Presentación, discusión grupal, video explicativo
Módulo 2: Políticas de Seguridad de la OMS	Política de uso aceptable de los recursos informáticos, política de contraseñas, política de protección de datos personales, política de incidentes de seguridad	1.5 horas	Presentación, preguntas y respuestas
Módulo 3: Buenas Prácticas de Seguridad	Manejo seguro de dispositivos móviles, navegación segura en internet, protección de contraseñas, identificación y reporte de actividades sospechosas	2 horas	Taller práctico, simulación de escenarios
Módulo 4: Simulaciones y Ejercicios Prácticos	Ejercicios de phishing, simulaciones de ataques cibernéticos	1.5 horas	Simulación en línea, análisis de casos reales

Metodología de Capacitación.

- **Capacitación en línea:** Módulos interactivos y autoguiados disponibles en cualquier momento y lugar.
- **Talleres presenciales:** Sesiones interactivas con instructores para resolver dudas y realizar ejercicios prácticos.
- **Webinars:** Transmisiones en vivo para llegar a un gran número de empleados.
- **Material impreso:** Guías de referencia rápida y carteles informativos.