Manual del Sistema de Gestión de Seguridad de la Información

Viviana Mendoza

Índice

Manual del Sistema de Gestión de Seguridad de la Información

1. Introducción

1.1. Manual SGSI

El Sistema de Gestión de Seguridad de la Información (SGSI) tiene como objetivo garantizar la confidencialidad, integridad y disponibilidad de la información crítica utilizada por la empresa en sus operaciones.

Este propósito se alinea con el cumplimiento de normativas internacionales como ISO 27001 y regulaciones locales.

El SGSI busca gestionar los riesgos de seguridad de manera efectiva mediante un enfoque estructurado y colaborativo, proporcionando un marco que promueve la mejora continua y protege los activos de información de amenazas internas y externas.

1.2. Metas y Objetivos

Identificar y tratar los riesgos de forma sistemática, tanto internos como externos. De manera que se puedan conseguir las siguientes metas:

- Proteger la información sensible de la organización de accesos no autorizados.
- Cumplir con la legislación, normativas estatales y normativas internas. (ISO 27001, reglamentos internos de la compañía)
- Asegurar la continuidad de los servicios operativos.
- Fomentar cultura de ciberseguridad entre los miembros de la organización y por extensión a la sociedad.

1.3. Objetivos Específicos:

- Identificar y gestionar los riesgos relacionados con la seguridad de la información.
- Asegurar la implementación de controles adecuados para garantizar la confidencialidad, integridad y disponibilidad de la información.
- Monitorear continuamente el cumplimiento de políticas y regulaciones.
- Proveer capacitación continua a todos los niveles de la organización para fortalecer la conciencia sobre ciberseguridad.

- Facilitar la respuesta oportuna a incidentes de seguridad mediante un sistema de comunicación y coordinación eficiente

2. Alcance del SGSI

El SGSI abarca los siguientes elementos:

2.1. Activos de información:

Documentos administrativos, operativos, información sobre personal, información de clientes/proveedores, información sensible económica…

Infraestructura tecnológica:
Servidores virtuales, redes cableadas e inalámbricas, entornos en la nube, dispositivos para el usuario final (ordenadores de sobremesa, portátiles).

2.2. Límites físicos:

Organización en la que se encuentra el sistema operativo Debian.

2.3. Límites virtuales:

Redes internas (LAN), redes perimetrales (DMZ), redes inalámbricas (Wi-Fi), servicios en la nube utilizados oficialmente (servidores, almacenamiento), así como sistemas y aplicaciones internas (correo interno).

Redes:

Redes Internas: Todas las redes internas de la organización utilizadas para la comunicación entre servidores, estaciones de trabajo y dispositivos internos.
Redes Inalámbricas (Wi-Fi): Redes usadas para dispositivos portátiles.

Entornos en la Nube

Proveedores de Servicios en la Nube:
- Microsoft Azure o Amazon Web Services (AWS) para almacenamiento de datos e infraestructura virtual.
- Google Cloud para colaboración en línea y almacenamiento.

Aplicaciones en la Nube:
- Plataformas de gestión académica y administración como sistemas ERP (Enterprise Resource Planning).
- Herramientas colaborativas (Google Workspace, Microsoft 365).

Almacenamiento en la Nube:
- Servicios utilizados para respaldo y recuperación ante desastres.
- Bases de datos alojadas en servicios en la nube para proyectos de investigación.

Sistemas:

Sistema Debian

2.4. Partes interesadas: Roles y responsabilidades

Gestión (Directivos y administración), Dirección de IT (equipo de ciberseguridad), empleados (usuarios del sistema).

Gestión (Directivos y Administración)

La dirección de la organización desempeña un papel fundamental en el éxito del Sistema de Gestión de Seguridad de la información. Este compromiso se manifiesta mediante el cumplimiento de las siguientes responsabilidades y aspectos clave.

Responsabilidades:

- **Definición de Políticas:**
  - Aprobar políticas de seguridad de la información y alinear estas con los objetivos estratégicos de la organización.
- **Supervisión y Gobernanza:**
  - Garantizar el cumplimiento de normativas, como ISO 27001y otras regulaciones. Participar activamente en iniciativas de seguridad, demostrando un compromiso claro con la protección de activos.
- **Asignación de Recursos:**
  - Proporcionar recursos financieros y humanos necesarios para implementar medidas de seguridad. Estos deben ser suficientes para poder implementar y mantener el SGSI.
- **Monitoreo de Riesgos:**
  - Revisar regularmente las evaluaciones de riesgos y aprobar planes de tratamiento. Comprobar la efectividad de los programas, controles y planes implementados.
- **Comunicaciones Estratégicas:**
  - Informar a las partes interesadas clave (como ciudadanos y socios) sobre las medidas de seguridad adoptadas.
- **Apoyo a la cultura de la seguridad:**
  - Fomentar que la cultura de la seguridad sea una prioridad para todos los miembros de la organización.

Equipo de IT

Responsabilidades:

- **Gestión de Infraestructura:**
  - Configuración, mantenimiento y monitoreo de servidores, redes y dispositivos.

- **Seguridad Cibernética:**
  - Implementar herramientas de monitoreo de amenazas, firewalls y sistemas de detección de intrusos.
  - Realizar análisis de vulnerabilidades y pruebas de penetración.
- **Respuesta a Incidentes:**
  - Gestionar la respuesta a incidentes de seguridad, incluyendo análisis forense digital.
  - Coordinar la recuperación de sistemas afectados por ataques cibernéticos.
- **Capacitación Interna:**
  - Proporcionar formación continua a empleados sobre prácticas seguras de manejo de datos.
- **Auditorías Técnicas:**
  - Realizar auditorías internas y apoyar auditorías externas relacionadas con la seguridad.

CISO (Chief Information Security Officer)

Responsabilidades:

- **Gestión Integral de Seguridad:**
  - Supervisar la implementación del SGSI en la organización.
- **Evaluación de Riesgos:**
  - Realizar evaluaciones periódicas de riesgos a nivel del sistema y proponer planes de mitigación.
- **Respuesta a Emergencias:**
  - Coordinar la respuesta a incidentes críticos en toda la organización.
- **Colaboración:**
  - Trabajar con otras partes interesadas, incluidos proveedores y autoridades, para reforzar la seguridad.
- **Actualización de Políticas:**
  - Revisar y actualizar las políticas de seguridad según los avances tecnológicos y regulatorios.

Cybersecurity Operations Team

Responsabilidades:

- **Monitoreo Continuo:**
  - Gestionar herramientas de detección de amenazas, firewalls, y sistemas de respuesta ante incidentes.
- **Gestión de Vulnerabilidades:**
  - Realizar análisis periódicos para identificar y remediar vulnerabilidades en la infraestructura.

- **Respuestas a Incidentes:**
  - Actuar como primer nivel de respuesta en eventos de seguridad, incluyendo análisis forense.
- **Pruebas de Seguridad:**
  - Llevar a cabo pruebas de penetración y ejercicios de simulación.
- **Soporte Técnico:**
  - Proveer asistencia a otros equipos en la implementación de controles técnicos.

Empleados

Responsabilidades:

- **Cumplimiento de Políticas:**
  - Seguir las políticas y procedimientos relacionados con la seguridad de la información.
- **Manejo Seguro de Datos:**
  - Proteger los datos confidenciales a los que tengan acceso, evitar el uso indebido y reportar anomalías.
- **Participación en Capacitación:**
  - Completar cursos de concienciación sobre ciberseguridad y manejo de datos sensibles.
- **Prevención de Amenazas:**
  - Identificar y reportar correos de phishing, accesos no autorizados o cualquier actividad sospechosa.
- **Colaboración:**
  - Trabajar con los equipos de IT y gestión para mejorar las prácticas de seguridad.

Proveedores Externos y Afiliados

Responsabilidades:

- **Cumplimiento Contractual:**
  - Seguir los acuerdos de seguridad estipulados en los contratos y garantizar que sus sistemas cumplen con las normativas de seguridad aplicables.
- **Gestión de Accesos:**
  - Limitar el acceso a los sistemas y datos de la organización al personal autorizado y relevante.
- **Monitoreo y Auditorías:**
  - Permitir auditorías periódicas y colaborar en la evaluación de riesgos.
- **Notificación de Incidentes:**
  - Informar inmediatamente sobre cualquier incidente de seguridad que pueda afectar a los datos o sistemas de la organización.

2.5. Exclusiones / Limitaciones.

Se excluyen los siguientes componentes del SGSI por motivos de priorización de recursos y bajo nivel de criticidad percibida:

- Infraestructuras que no manejen datos sensibles.
- Infraestructuras ajenas a la organización que mantengan relación, pero no manejen datos o activos relacionados directamente con ella.
- Sistemas personales de los miembros de la organización no conectado a las redes de la organización
- Equipos no gestionados directamente por la organización, a menos que interactúen con estructuras o datos críticos/sensibles.

3. Metodología de Evaluación de Riesgos

3.1. Proceso

- Identificación y clasificación de activos.

Se realiza un listado exhaustivo de los activos de la organización, clasificándolos por tipo e importancia en los servicios prestados por la organización.
Plantilla Utilizada ejemplo:

Activo	Clasificación	Descripción
Servidores físicos	Crítico	Alojamiento de sistemas esenciales y datos sensibles

- Identificación de amenazas y vulnerabilidades.

Se identifican las posibles amenazas y vulnerabilidades específicas para cada tipo de activo y si están pueden venir desde la propia organización (Internas) o desde fuera (Externas)

Plantilla utilizada ejemplo:

Categoría	Amenaza	Interna/Externa	Probabilidad	Impacto
Hardware	Acceso físico no autorizado (robo, daño)	Externa	Media	Alto

- Análisis de probabilidad e impacto.

Se evalúa la probabilidad de que ocurran esas amenazas y el potencial impacto de cada una de ellas.

A la plantilla anterior se la añaden probabilidad e impacto en este punto del análisis.

  - Probabilidad: Baja, Media, Alta.
  - Impacto: Bajo, Medio, Alto.

- Priorización de Riesgos: Se clasifican los riesgos en base a su probabilidad e impacto.

IMPACTO	ALTA PROBABILIDAD	MEDIA PROBABILIDAD	BAJA PROBABILIDAD
ALTO	Alto (Crítico)	Medio	Medio
MEDIO	Medio	Medio	Bajo
BAJO	Medio	Bajo	Bajo

  - **Alto** (Crítico): Situaciones que tienen tanto alta probabilidad como alto impacto. Requieren acción inmediata para mitigar el riesgo.
  - **Medio**: Riesgos con probabilidad media/alta o impacto medio. Se deben tratar con prioridad, pero no necesariamente de forma inmediata.
  - **Bajo**: Riesgos con baja probabilidad o bajo impacto. Pueden manejarse a largo plazo o monitorearse regularmente.

- Definición de planes de tratamiento (selección de controles).

En esta fase seleccionamos controles y medidas para reducir los riesgos que hemos priorizado antes.

- Revisión y Monitoreo continuo:

Se debe mantener el inventario de activos actualizado, de manera que se puedan descubrir posibles nuevas amenazas a tiempo e implementar los controles adecuados.

También se realizarán evaluaciones periódicas para revisar la efectividad de los controles y estrategias implementadas y ajustarlas en caso de nuevos riesgos o ineficacia.

3.2. Inventario de activos:

Resultados de la Evaluación de Riesgos

Para poder realizar la evaluación de riesgo seguiremos los siguientes pasos:

1. **Listado de Activos y Clasificación**

Activo	Clasificación	Descripción
Servidores web	Crítico	Alojamiento de sistemas esenciales y datos institucionales sensibles.
Routers, switches y firewalls	Alto	Elementos esenciales para la conectividad y la seguridad de la red.
Ordenadores de escritorio y portátiles	Medio	Dispositivos para el trabajo del personal.
Google Workspace y Microsoft 365	Alto	Comunicación y colaboración entre personal/proveedores
Antivirus y herramientas EDR y Firewalls	Crítico	Protección contra amenazas y ataques dirigidos a los sistemas.
Plataformas de almacenamiento en la nube	Medio	Almacenamiento y colaboración de archivos institucionales.
Software de recuperación ante desastres	Crítico	Garantiza la continuidad operativa mediante la restauración de sistemas y datos críticos tras un incidente.
Software de monitoreo	Crítico	Supervisa el estado y rendimiento de los sistemas para detectar y responder a amenazas o fallos de manera oportuna.

Datos

Activo	Clasificación	Descripción
Registros de empleados	Crítico	Información confidencial relacionada con salarios y contratos.
Propiedad intelectual	Alto	Datos generados en proyectos científicos / investigaciones/ patentes
Copias de seguridad en la nube	Alto	Respaldo de información crítica almacenada en servicios externos.
Logs de de seguridad	Medio	Registros de actividades y accesos para cumplimiento normativo.
Datos financieros	Crítico	Información clave para planificación y asignación de recursos, así como datos sensibles frente al fraude o acceso no autorizado.

Personal

Activo	Clasificación	Descripción
Dirección ejecutiva	Crítico	Responsables de decisiones estratégicas de la organización.
Equipo de ciberseguridad	Crítico	Encargados de proteger y gestionar la seguridad de la información.
Proveedores y colaboradores	Alto	Personal externo que interactúa con la organización y puede tener acceso a información sensible.

2. Principales Amenazas y Vulnerabilidades 3. probabilidad e Impacto

Categoría	Amenaza	Interna/Externa	Probabilidad	Impacto
Hardware	Acceso físico no autorizado(robo, daño intencional, sabotaje)	Externa	Media	Alto
	Uso indebido	Interna	Media	Medio
	Corte de electricidad	Externa	Alta	Alto
	Negligencia - daños accidentales	Interna	Alta	Medio
	Daño por desastres naturales	Externa	Media	Alto
Software	Malware y ransomware	Externa	Alta	Alto
	Configuraciones inseguras	Interna	Media	Alto
	Software desactualizado	Interna	Alta	Alto
	Phishing	Externa	Alta	Alto
	Uso no autorizado de software	Interna	Media	Medio
	Explotación de vulnerabilidades	Externa	Alta	Alto
	Instalación de software no autorizado	Interna		Alto
Datos	Acceso no autorizado a datos	Externa	Alta	Alto
	Robo de datos	Interna	Alta	Alto
	Errores humanos (borrado/modificación)	Interna	Alta	Alto
	Intercepción de datos en tránsito	Externa	Media	Alto
	Falta de cifrado en datos sensibilidad.	Interna	Alta	Alto
Personal	Ingeniería social	Externa	Alta	Alto
	Descontento interno	Interna	Media	Alto

	Falta de capacitación en ciberseguridad	Interna	Alta	Alto
	Brechas de seguridad en sistemas de proveedores	Externa	Alta	Alto
Redes	Ataques DDoS	Externa	Media	Alto
	Escaneo y explotación de servicios	Externa	Alta	Alto
	Uso indebido de redes internas	Interna	Media	Medio

3.3. Controles seleccionados:

Lista de Controles Seleccionados

Controles de Seguridad Basados en Normas Relevantes para Mitigar los Riesgos Identificados

En este análisis, se seleccionan controles de seguridad apropiados de normas como **ISO/IEC 27001**, además de considerar regulaciones específicas locales. Los controles se alinean con los riesgos críticos con alta probabilidad y alto impacto, que se han identificado previamente.

	Riesgo Mitigado	**Control**	**Descripción**	**Prioridad**	Roles y responsabilidades
Hardware	Cortes de electricidad.	**Disponibilidad de sistemas críticos**	Implementar sistemas de alimentación y generadores para soportar sistemas y operaciones durante fallos eléctricos.	Alta	Equipo de Infraestructura: Instalar y mantener sistemas y generadores.
Software	Malware, ransomware	**Antivirus y EDR (Endpoint Detection)**	Implantar software de protección y monitoreo para detectar amenazas en dispositivos finales.	Alta	Equipo de Ciberseguridad: Configurar herramientas EDR. Usuarios: Reportar actividades sospechosas. CISO: Revisar eficacia de las soluciones implementadas.
	Vulnerabilidades: desactualización u obsolescencia.	**Parches y Actualizaciones**	Políticas y procedimientos para mantener apps, software y sistemas actualizados de manera automatizada.	Alta	Equipo de TI: Configurar herramientas de gestión de parches.

			Monitorización constante		
	Phishing	**Concienciación y capacitación**	Implementar programas y políticas de capacitación en ciberseguridad para empleados, incluir simulaciones. Entrenamiento obligatorio.	Alta	Equipo de Capacitación: Desarrollar simulaciones y cursos. Usuarios: Participar activamente en las capacitaciones. CISO: Supervisar efectividad.
			Uso de herramientas avanzadas para detectar correos maliciosos.		Equipo de Ciberseguridad: Configurar y monitorear herramientas.
	Instalación de software no autorizado	**Gestión de instalación de software. Restricciones. Gestión de privilegios. Inventario y control de software.**	Establecer políticas estrictas que prohíban la instalación de software no autorizado. Limitar privilegios de instalación solo a usuarios autorizados. Configurar controles para limitar permisos de administrador en los dispositivos.	Alta	Equipo de TI: Configurar políticas de control de software. CISO: Supervisar auditorías regulares. Usuarios: Cumplir con las políticas.
Datos	Acceso no autorizado, contraseñas débiles	**Control de Acceso**	Implementación de autenticación multifactor y gestión de identidades centralizada.	Alta	IT: Configuraciones. CISO: supervisión. Usuarios: seguir las recomendaciones.
			Contraseñas complejas, de longitud adecuada, con caracteres especiales, de rotación periódica y verificación de contraseñas (listas de contraseñas comprometidas). 2FA		Usuarios: cumplir los requisitos de las contraseñas.
			Implementar herramientas para gestionar accesos y sesiones de usuarios, controles de privilegios, eliminación de usuarios inactivos junto a revisión continua de privilegios.		IT: monitorear y auditar privilegios.
	Robo de información	**Cifrado de Datos**	Uso de cifrado para proteger datos sensibles (VPN, SSL/TLS).	Alta	Equipo de TI: Configurar sistemas de cifrado. CISO:

					Asegurar cumplimiento de políticas de cifrado.
	Pérdida de datos, desastres naturales	**Gestión de Backups y Recuperación**	Definición de políticas para copias de seguridad y pruebas de restauración, tanto en entornos locales como en la nube.	Media	Equipo de Infraestructura: Configurar backups locales y en la nube. CISO: Validar políticas de recuperación.
	Intrusiones avanzadas, actividad sospechosa	**Monitoreo y Registro (SIEM)**	Implementación de un sistema de monitoreo y correlación de eventos de seguridad para alertas tempranas.	Media	Equipo de Ciberseguridad: Configurar y monitorear el SIEM. CISO: Revisar informes generados por el SIEM.
	Errores humanos, uso indebido de privilegios	**Plan de Concienciación y Capacitación**	Formación y simulacros de phishing, entrega de materiales informativos sobre seguridad de la información.	Alta	Equipo de Capacitación: Diseñar simulacros y contenidos formativos. Supervisores: Asegurar asistencia de su equipo.
	Acceso no autorizado físico	**Control Físico de Acceso**	Uso de tarjetas de identificación, cerraduras electrónicas y CCTV en zonas restringidas (salas de servidores, laboratorios de alta seguridad).	Baja	Equipo de Infraestructura: Configurar cerraduras y CCTV. CISO: Aprobar controles físicos en áreas críticas.
	Fugas de datos a terceros	**Control de Proveedores y Contratistas**	Evaluación de seguridad para proveedores externos que manejan datos de la Organización.	Baja	Equipo Legal: Incluir cláusulas de seguridad en contratos. CISO: Asegurar evaluación de proveedores críticos.
Redes	Intrusiones, Malware	**Seguridad en la Red y Segmentación**	Segmentación de redes internas y uso de firewalls para aislar sistemas críticos.	Alta	IT: configuración, implementación, supervisión.
Personal	Ingeniería social	**Concienciación y capacitación en seguridad y sobre amenazas**	Realizar simulacros, proporcionar capacitación sobre técnicas de ingeniería social, crear campañas personalizadas para cada rol de la organización.	Alta	CISO: diseñar y supervisar los programas. Equipo de capacitación: ejecutar el programa. Usuarios: Participar y poner en práctica

	Brechas de seguridad en sistemas de proveedores o 3º	**Gestión de relaciones con terceros**	Establecer requisitos de seguridad en los contratos con proveedores, incluir auditorias y evaluaciones periódicas.	Alta	Legal: redactar contratos. CISO: Autorizar contratos. IT: monitorear cumplimiento
			Realizar evaluaciones iniciales de seguridad de los sistemas de proveedores y monitorear su cumplimiento.		Auditores: evaluaciones iniciales

Planificación de la Implementación:

La implementación dependerá en gran medida de la probabilidad de que se produzcan y del posible impacto que tengan en el buen funcionamiento de la Organización, esto determinará que controles abordar primero y el margen de tiempo ideal para su implementación.

1. Prioridad Alta: Controles que mitigan riesgos críticos con alta probabilidad e impacto directo en la continuidad operativa o en la confidencialidad, integridad y disponibilidad de los datos. Estos controles se planifican para los primeros 1-3 meses.
2. Prioridad Media: Controles que mitigan riesgos moderados, pero no de manera inmediata. Se implementan en un período de 3-6 meses.
3. Prioridad Baja: Controles enfocados en prevenir riesgos con baja probabilidad o impacto limitado, pero que contribuyen a la mejora general de la seguridad. Se implementan en 6 meses o más.

Independientemente de la prioridad, todos los controles a implementar requieren de un análisis para la gestión de un presupuesto adecuado y las acciones necesarias.

- Establecer un inventario de los sistemas, software, hardware y personal disponible. Este sería el primer paso, independientemente de la prioridad. De esta manera se podrá planificar mejor cualquier paso siguiente.

Como segunda fase del cronograma se procedería a la implementación de los controles:

Hardware y redes:

Los controles relacionados con el hardware requieren identificar sistemas críticos que necesiten soporte eléctrico, lo que supondría el uso la adquisición de generadores y su instalación.

Estos controles deben tener métricas de éxito: como disminución de interrupciones por corte eléctrico.

Software y datos:

El departamento de IT y el equipo de ciberseguridad deben trabajar en conjunto para realizar una auditoría e inventario del software disponible, adaptar su configuración y uso y elegir el software adicional necesario para que los controles puedan implementarse. Lo que incluye revisión de configuraciones, cifrado, sistemas de autenticación…

Métricas de éxito: porcentaje de usuarios con contraseñas seguras, porcentaje de datos cifrados. Software de auditoría que nos indique que el sistema es más seguro que en la evaluación inicial.

Personal:

Se debe crear una política de seguridad, que incluya manuales, simulaciones, prácticas que ayuden y capaciten a los usuarios para que tengan herramientas para detectar, hacer frente o denunciar estos posibles ataques.

Métricas de éxito: aumento de denuncias de correos sospechosos o incidentes de ingeniería social, tasas de éxito en simulaciones de phishing.

3.3.1. Cronograma:

Mes	Riesgos Tratados	Acciones Clave
1	Planificación e inventario	Reunión inicial, validación de riesgos, priorización.
2	Sistemas desactualizados, contraseñas débiles	Implementación de parches, MFA, políticas de contraseñas.
3	Cifrado, cortafuegos mal configurados, tráfico no cifrado	HTTPS, segmentación, VPN.
4	Capacitación, ingeniería social, accesos mal gestionados	Simulaciones de phishing, auditorías de accesos.
5	Acceso físico no autorizado, copias de seguridad	Controles de acceso físico, cifrado de respaldos.
6	Evaluación de proveedores, privilegios excesivos	Evaluaciones iniciales de seguridad, ajuste de privilegios.
7+	Seguimiento y auditorías	Auditorías trimestrales, monitoreo de KPIs.

4. Políticas y Procedimientos de Seguridad de la información:

La Organización está comprometida con la protección de su información y activos, de manera que se pueda garantizar la confidencialidad, integridad y disponibilidad de estos. Esta política establecerá los principios, responsabilidades y objetivos fundamentales para buenas prácticas de seguridad en toda la organización.

- **Ámbito**

  Aplica a todo el personal, contratistas y socios externos que accedan, procesen, almacenen, transmitan o manipulen información relacionada con la Organización. También cubre todos los sistemas, dispositivos y redes que interactúan con los activos digitales de la organización.

- **Principios Clave**

  Confidencialidad: La Organización protegerá la información contra el acceso no autorizado para prevenir la divulgación, uso indebido o perdida de datos confidenciales, incluida información personal, financiera y de investigación.
  Integridad: Se implementarán controles para garantizar la exactitud, consistencia y validez de la información en todos los sistemas. Los datos deben estar protegidos contra manipulación, corrupción o modificación no autorizada.
  Disponibilidad: Se asegurará que los sistemas de información y los datos estén disponibles para los usuarios autorizados en el momento en que los necesiten, minimizando interrupciones y asegurando la continuidad operativa.

- **Objetivos**
  - **Cumplimiento normativo:** Garantizar que se cumpla con todas las leyes, normativas y estándares aplicables.
  - **Protección de la información:** Proteger los activos de la información frente a riesgos internos y externos.
  - **Gestión de riesgos:** Implementar un programa de gestión de riesgos que identifique, evalúe y mitigue las amenazas a la seguridad de la información.
  - **Respuesta a incidentes:** Establecer y mantener un plan de respuesta a incidentes para detectar, responder y recuperarse de eventos de seguridad de manera efectiva.
  - **Educación y Concienciación:** Proporcionar capacitación de manera regular para garantizar que todos los miembros de la comunidad comprendan sus responsabilidades en materia de seguridad.

4.1. Control de acceso de usuarios:

Fundamental para proteger los recursos digitales de la Organización. Ya sea de manera física o digital.

- **Procedimiento de Alta y Baja de Usuarios (área de IT)**
  - El acceso a los sistemas y datos serán concedidos según el principio de menor privilegio y con la aprobación previa de él/los responsables de área correspondientes.

- Los diferentes departamentos notificarán del ingreso de nuevos empleados y se les asignarán credenciales para poder acceder a los recursos, físicos y tecnológicos.
- También notificarán si tienen roles adicionales para poder concederles los privilegios de usuario correspondientes (Investigadores, acceso a zonas restringidas…)
- RR.HH. notificará sobre la incorporación o cese de empleados o colaboradores.
- Las áreas de recursos notificarán de la incorporación de nuevos proveedores y la baja de aquellos que lleven más de 3 meses sin utilizarse a menos que se indique lo contrario.
- Cuando un usuario cambie de función o abandone la organizacion, sus privilegios deberán ser revisados y si corresponde, revocados de manera inmediata. Esto supondrá:
    - Deshabilitar las cuentas de usuario.
    - Revocar acceso a sistemas y recursos.
    - Recuperar dispositivos físicos asignados (tarjetas de acceso, ordenadores, dispositivos móviles…)

➢ **Política de Contraseñas**

Las contraseñas utilizadas deberán cumplir con los siguientes requisitos de complejidad:

- Se asignará de manera automática una contraseña aleatoria al usuario al inscribirse.
- Se le solicitará un cambio obligatorio de contraseña la primera vez que ingrese al sistema.
- Debe tener mínimo 12 caracteres.
- Debe incluir al menos una letra mayúscula, una letra minúscula, un número y un símbolo especial.
- No pueden utilizarse nombres de usuarios o contraseñas fácilmente identificables (contraseña, 123456, qwerty…)
- Deben cambiarse las contraseñas de manera obligatoria cada 90 días, llegará un aviso a la cuenta a modo de recordatorio.
- Bloqueo del usuario tras 5 intentos fallidos, tras lo que se deberá acudir a IT para el desbloqueo.
- No se podrán utilizar las últimas 5 contraseñas.

➢ **Autenticación Multifactor**

Todos los sistemas críticos y el acceso remoto requerirán el uso de un doble factor de autenticación y el uso de VPN.

- **Control de Acceso físico**
  En instituciones y salas que manejen información crítica se utilizarán controles de acceso físico, como tornos, lectores de huellas o lectores de identificaciones.

- **Protección de datos**
  La información confidencial deberá cifrarse tanto en reposo como en tránsito.
  Se realizarán respaldos regulares de los datos críticos y se probará su recuperación de manera periódica.

- **Monitoreo y Auditoría**
  La actividad en los sistemas será monitoreada para detectar accesos no autorizados o actividades sospechosas.
  Se realizarán auditorias de manera regular para asegurar cumplimiento de las políticas.

4.2. Plan de respuesta a incidentes

Definimos un incidente de seguridad a cualquier evento que comprometa la confidencialidad, integridad o disponibilidad de los activos de información de la Organización. A continuación, se detalla el procedimiento de gestión de incidentes:

- **Identificación del Incidente**
  - Monitorización de sistemas: El monitoreo continuo y automático de los sistemas permitirá detectar actividades sospechosas o no autorizadas.
  - Denuncia de usuarios: cualquier usuario que identifique un posible incidente debe reportarlo de inmediato, mediante el envío de correo electrónico al departamento de IT.
  - Alertas de proveedores o terceros.

- **Clasificación del Incidente**
  Se evaluará la severidad del incidente para su clasificación según su impacto: Crítico, Alto, Medio, Bajo.
  - **Crítico:** Impacto inmediato en datos sensibles u operaciones críticas.
  - **Alto:** Pérdida o acceso no autorizado a información relevante.
  - **Medio:** Evento con potencial de impacto limitado.
  - **Bajo:** Eventos menores o de bajo riesgo.

- **Notificación**
  - Notificación al equipo de respuesta a incidentes: Se informará a las partes responsables, para que se tomen las medidas oportunas. Según el nivel del incidente, se deberá escalar la notificación hasta el más alto nivel
  - Comunicar a los usuarios afectados sobre posibles impactos.
  - Comunicar a las autoridades en caso de que la normativa legal lo exija.

- **Contención y erradicación**

  Implementar medidas para limitar el alcance del incidente:
  - Aislar los sistemas afectados. Desconectar dispositivos comprometidos, revocar accesos temporalmente…
  - Implementar medidas de contención: Bloquear direcciones IP o usuarios maliciosos. Actualizar reglas de cortafuegos o aplicar parches urgentes.

- **Erradicación:**
  - Identificar y eliminar la causa raíz del incidente.
  - Reparar vulnerabilidades.
  - Aplicar parches, desinstalar software malicioso o realizar cambios en la configuración de seguridad.
  - Implementar controles adicionales si es necesario.

- **Recuperación**
  - Restaurar los sistemas afectados a su estado operativo normal.
  - Verificar que los sistemas restaurados no presenten vulnerabilidades.
  - Comprobar la integridad de los datos restaurados.

- **Análisis posterior al incidente**
  - Documentar el incidente y cada paso de las acciones tomadas. Logs, capturas de pantalla, reportes de vulnerabilidades.
  - Documentar lo aprendido del incidente
  - Actualizar las políticas y procedimientos para que el incidente no se vuelva a producir o disminuir su impacto.
- **Roles y responsabilidades**
  - CISO (Chief Information Security Officer): responsable de desarrollar, implementar y supervisar el programa de seguridad de la información. Realizar evaluaciones periódicas de riesgos.
  - Departamentos de IT y Ciberseguridad de las facultades, hospitales, laboratorios y edificios anexos: Asegurar la implementación de controles técnicos y operativos adecuados en toda la infraestructura de IT.
  - Usuarios finales: cumplir con las políticas y procedimientos de seguridad, reportar incidentes y proteger la información que manejen.

4.3. Copia de seguridad y recuperación de datos

La Organización tiene en custodia información que puede llegar a ser considerada extremadamente sensible. Lo que supone seguir una serie de procedimientos para garantizar su confidencialidad, integridad y disponibilidad:

- **Copias de seguridad:**
  - Identificación de Datos: Se identificarán bases de datos, sistemas y archivos críticos para la operación de la organización.
  - Realizar copias de seguridad: dependerán de la criticidad de los datos.
    - **Datos críticos:** Respaldos diarios.
    - **Datos no críticos:** Respaldos semanales.
    - **Datos de archivo:** Respaldos mensuales.
  - Configuración de herramientas de copias de seguridad automáticas. Que realicen estas tareas de manera automática en la frecuencia definida.
  - Ubicación de los respaldos: múltiples ubicaciones.
    - Localmente: Centros de datos seguros.
    - Remoto: Servicios en la nube.
  - Cifrar los respaldos: Todas las copias de seguridad deberán estar cifrados con AES-256 tanto en tránsito como en reposo.
  - Comprimir las copias de seguridad para reducir el espacio utilizado.
  - Política de conservación:
    - **Respaldos diarios:** Mantener durante 30 días.
    - **Respaldos semanales:** Mantener durante 90 días.
    - **Respaldos mensuales:** Mantener durante 1 año.
  - Pruebas de recuperación y verificación: se deben realizar pruebas de recuperación completas al menos trimestralmente para garantizar la integridad de los respaldos y que estos continúen estando completos. Deben ser pruebas de todas las situaciones posibles, restaurar archivos concretos o sistemas completos.
  - Documentar las pruebas. Documentar los tiempos de recuperación y si se han realizado correctamente. Así como cualquier paso que permita mejorar el proceso.
  - Monitorización y notificación: Habilitar alertas automáticas para respaldos éxitos o fallidos.

- **Recuperación de datos**
  - Identificación del incidente. Determinar el sistema y datos afectados, así como la fecha del incidente. Revisar los logs de respaldos e identificar la copia de seguridad más reciente.
  - Planificar la recuperación: Alcance e infraestructura.
    Cantidad de archivos a recuperar:
    - Recuperación parcial: archivos específicos.
    - Recuperación total: El sistema completo.

Infraestructura, para asegurarnos de que el sistema afectado está listo para recibir los datos restaurados.

- Ejecución de recuperación. Restaurar los datos desde las copias de seguridad locales o remotas según sea necesario.
- Validar recuperación: comprobar que los datos restaurados son completos y funcionales antes de reactivar los sistemas.
- Seguimiento y documentación: documentar el proceso de recuperación, las acciones realizadas y los resultados obtenidos.
- Mejorar el procedimiento: Identificar cualquier posible mejora que se pueda integrar en la política de seguridad.

4.4. Concienciación y capacitación de empleados

Se debe garantizar que todos los usuarios de la Organización al completo comprenda las políticas de seguridad, sus responsabilidades y las mejores prácticas para protegerse y proteger los activos de la organización. Se debe crear una cultura de la seguridad.

➢ **Objetivos:**

- **Cumplimiento de políticas.** Garantizar que las políticas sean comprendidas y aplicadas correctamente.
- **Prevención de incidentes.** Reducir el número de incidentes relacionados con errores humanos, como ataques de phishing o uso inadecuado de credenciales.
- **Incrementar conciencia de seguridad y cultura de seguridad.** Asegurar que todos los usuarios conozcan los riesgos de seguridad cibernética y como evitarlos. Así como fomentar un enfoque proactivo hacia la seguridad de todas las áreas de la organización.

➢ **Plan de capacitación:**

Capacitación general

- Obligatoria para todos los empleados al menos una vez al año.
- Todos los empleados nuevos deben tener su capacitación dentro de los primeros 30 días en el puesto.
- Se colocarán carteles o se enviará material gráfico con carteles o presentaciones con recordatorios de las capacitaciones en los boletines internos.
- Temario:
    - Políticas de seguridad de la información.
    - Gestión de contraseñas
    - Identificación de correos phishing y otras amenazas.
    - Uso seguro de dispositivos personales y acceso remoto.

- Uso seguro de redes Wi-Fi y protección de datos
- Procedimientos para reportar incidentes de seguridad.

Capacitación específica

La capacitación a recibir varía de un usuario a otro, dependiendo de los roles específicos que tengan los usuarios o de la información sensible a la que puedan acceder.
Adicionalmente a la capacitación general:

- Personal administrativo: con acceso a información sensible como nombres, números de identificación, direcciones, información contable, financiera,
  - Formación en protección de datos
  - Buenas prácticas de uso del sistema correspondiente y aplicaciones internas específicas de su área.
- Equipo de IT y ciberseguridad: Gestión de incidentes, análisis forense, actualización de herramientas de seguridad, buenas prácticas de uso, monitorización.
- Dirección: Cifrado y protección de datos sensibles para la organización. Gestión de riesgos, supervisión de políticas.

Prácticas

- Simulaciones de Phishing: Envío de correos simulados para medir la capacidad de los empleados para identificar amenazas.
- Simulacros de incidentes: como ransomware o robo de datos.
- Simulacros de ingeniería social: Conseguir credenciales, acceso a instalaciones bajo pretextos, conexiones a sistemas…
- Evaluaciones: cuestionarios tras capacitación.

5. Monitoreo y Medición del SGSI

Aunque se ha incluido la monitorización y evaluación continua a lo largo del plan en necesario resaltar su importancia para la efectividad del SGSI, ya que es lo que asegura el cumplimiento de los objetivos establecido y permite la mejora continua.

Cómo se realizará el monitoreo

Sistemas de Detección y Monitoreo Automático:

- Implementación de herramientas SIEM para recopilar, correlacionar y analizar eventos de seguridad en tiempo real.

- Supervisión continua de accesos, actividades sospechosas, y comportamiento anómalo en redes, sistemas y datos.

Auditorías Periódicas:

- Revisiones programadas del cumplimiento normativo y de las políticas de seguridad (ISO 27001).
- Auditorías técnicas de vulnerabilidades, configuraciones y actualizaciones.

Reportes de Incidentes y Anomalías:

- Registro centralizado de incidentes de seguridad, reportes de phishing y accesos no autorizados.
- Sistema de notificación automática para alertar sobre incidentes críticos.

Pruebas y Simulaciones:

- Ejercicios de simulación de ataques (como simulacros de ransomware y phishing).
- Evaluación de tiempos de respuesta y efectividad del equipo de ciberseguridad.

Seguimiento de Acciones Correctivas:

- Control del cumplimiento de las recomendaciones tras auditorías e incidentes.
- Evaluación de la efectividad de las acciones tomadas.

Indicadores Clave de Rendimiento para Seguridad de la Información

1. **Monitoreo de Incidentes de Seguridad**:
   - **Número de incidentes detectados y resueltos**: Incidentes identificados por el SIEM o reportados manualmente.
   - **Tiempo promedio de detección**: Tiempo desde la ocurrencia del incidente hasta su detección.
   - **Tiempo promedio de respuesta**: Tiempo necesario para mitigar y resolver un incidente.
2. **Estado de los Controles Técnicos**:
   - **Porcentaje de sistemas actualizados**: Evaluación de parches aplicados en servidores, software y dispositivos.
   - **Porcentaje de datos críticos cifrados**: Información cifrada tanto en reposo como en tránsito.

- **Tasa de detección de intentos de acceso no autorizado**: Porcentaje de accesos bloqueados por sistemas de control de acceso.

3. **Cumplimiento Normativo**:
   - **Porcentaje de auditorías superadas sin no conformidades**.
   - **Cumplimiento de políticas de contraseñas**: Proporción de usuarios que cumplen con los requisitos de complejidad y rotación.
4. **Cultura de Ciberseguridad**:
   - **Porcentaje de participación en programas de capacitación**: Asistencia en cursos obligatorios y simulacros.
   - **Tasa de éxito en simulaciones de phishing**: Proporción de empleados que no caen en intentos simulados de phishing.
5. **Eficiencia en Respaldo y Recuperación**:
   - **Frecuencia de respaldos exitosos**: Porcentaje de respaldos realizados conforme a la política.
   - **Tiempo promedio de restauración de datos**: Tiempo necesario para recuperar datos desde respaldos en caso de incidentes.
6. **Monitoreo del Rendimiento del Sistema**:
   - **Disponibilidad del sistema**: Tiempo de actividad de los sistemas críticos.
   - **Número de vulnerabilidades abiertas**: Vulnerabilidades identificadas y pendientes de resolución tras análisis de seguridad.

Mecanismos de Reporte y Análisis

- **Informes Periódicos**: Generación de reportes mensuales y trimestrales con métricas clave y análisis de tendencias.
- **Panel de Control**: Plataforma centralizada para visualizar el estado de KPIs en tiempo real.
- **Revisión Anual del SGSI**: Evaluación global del desempeño del SGSI y actualización de objetivos.

6. Aprobación y revisión de documentos

La organización establece un procedimiento claro y estructurado para garantizar que todas las políticas, procedimientos y documentos relacionados con la seguridad sean revisados y aprobados por la dirección.
Además, se asegura que los documentos se mantengan actualizados y alineados con las necesidades operativas, normativas y tecnologías.

- Elaboración: Las políticas e informes se elaborarán por el responsable de cada área utilizando plantillas estándar para asegurar la uniformidad en formato y contenido.
- Revisión interna: Se revisará por equipo técnico para verificar que se ajuste a la normativa, políticas existentes y otros detalles técnicos.
- Aprobación de la dirección: El documento se revisará por el comité de seguridad y al CISO para su validación y a continuación será aprobado por la dirección para pasar a formar parte de las políticas y normativas de la organización.
- Comunicación: Una vez aprobado, el documento se hará llegar a las partes interesadas a través de correos electrónicos oficiales o publicaciones en los boletines internos de la organización
- Revisión y actualización: Cada política, plan o procedimiento debe revisarse al menos una vez al año o tras incidentes de seguridad relevantes. También deberán revisarse tras cambios significativos en la infraestructura tecnológica.
- Auditorías internas también pueden provocar cambios en las normativas.
- Cada cambio será documentado y registrado.