MANUAL DEL SGSI DEL SISTEMA DE LA UNIVERSIDAD DE CALIFORNIA

Alcance del SGSI para el Sistema de la Universidad de California

1. Identificación de Activos de Información

Inventario de activos:

- **Hardware:**
  - Computadoras personales y portátiles asignadas a personal y estudiantes.
  - Servidores físicos en centros de datos universitarios.
  - Equipos de red: routers, switches, firewalls.
  - Dispositivos de almacenamiento externo utilizados en proyectos de investigación.
- **Software:**
  - Sistemas de gestión educativa (LMS) como Canvas o Blackboard.
  - Aplicaciones administrativas y financieras, como software de nómina y presupuestos.
  - Herramientas de ciberseguridad: antivirus, sistemas de detección de intrusos (IDS/IPS).
- **Datos:**
  - Registros académicos de estudiantes.
  - Información personal de empleados y estudiantes (nombres, direcciones, números de identificación).
  - Resultados y datos de investigaciones científicas.
  - Documentación financiera y de cumplimiento normativo.
- **Personal:**
  - Profesores, investigadores y personal administrativo.
  - Estudiantes activos en todos los niveles.
  - Proveedores externos con acceso a sistemas de la universidad.

Clasificación por importancia:

- **Crítico:** Datos de investigación, registros académicos, servidores principales.
- **Alto:** Equipos de red, software administrativo y de seguridad.

- **Medio:** Computadoras de estaciones de trabajo, herramientas de colaboración.
- **Bajo:** Equipos periféricos como impresoras y dispositivos no críticos.

2. Definición de Límites Físicos

Ubicaciones incluidas:

- Todos los campus universitarios (Berkeley, UCLA, San Diego, etc.).
- Centros de datos centrales ubicados en campus estratégicos.
- Bibliotecas digitales con acceso a recursos educativos.

Áreas restringidas:

- Salas de servidores con acceso exclusivo del equipo de TI.
- Laboratorios de investigación de alto nivel que manejan datos sensibles.
- Oficinas administrativas que gestionan datos financieros y personales.

3. Definición de Límites Virtuales

Redes y sistemas virtuales:

- Redes internas de cada campus conectadas mediante redes privadas seguras.
- Entornos en la nube utilizados para almacenamiento de datos y aplicaciones educativas.
- Máquinas virtuales empleadas en proyectos de investigación y pruebas.

Tipos de datos bajo control:

- Información académica, personal y financiera almacenada en bases de datos locales y en la nube.
- Datos de investigación protegidos por acuerdos de confidencialidad.
- Comunicaciones internas gestionadas mediante sistemas de correo electrónico seguros.

4. Identificación de las Partes Interesadas

Grupos clave:

- **Equipo de TI y Ciberseguridad:** Gestión de redes, mantenimiento de servidores, supervisión de controles técnicos.
- **Docentes e Investigadores:** Uso seguro de sistemas educativos y herramientas de investigación.
- **Estudiantes:** Manejo responsable de plataformas educativas y datos personales.
- **Administración:** Cumplimiento normativo, asignación de recursos y supervisión de políticas.
- **Proveedores externos:** Aseguramiento de contratos y cumplimiento de normas de seguridad.

Asignación de responsabilidades:

- Equipo de TI: Implementar y monitorear controles de seguridad.
- Dirección administrativa: Garantizar recursos y cumplimiento de regulaciones.
- Usuarios finales: Cumplir políticas de seguridad y reportar incidentes sospechosos.

5. Documentación del Alcance del SGSI

Propósito:
Proteger los activos de información del Sistema de la Universidad de California mediante controles de seguridad adecuados que aseguren la confidencialidad, integridad y disponibilidad de los datos.

Metas y objetivos:

1. Establecer límites claros para el SGSI, abarcando activos físicos y virtuales.
2. Identificar y priorizar activos críticos para mitigar riesgos asociados.
3. Garantizar la colaboración efectiva entre todas las partes interesadas.

Limitaciones y exclusiones:

- Redes y sistemas gestionados por terceros fuera de acuerdos contractuales específicos.
- Sistemas de uso personal que no estén conectados directamente a la infraestructura universitaria.

Evaluación de Riesgos para el Sistema de la Universidad de California

1. Lista de Inventario de Activos

Categorías de activos:

- **Hardware:**
  - Servidores de bases de datos y almacenamiento en centros de datos.
  - Computadoras personales utilizadas por estudiantes, docentes y personal administrativo.
  - Equipos de red: routers, switches, firewalls.
- **Software:**
  - Sistemas de gestión académica y administrativa (Canvas, sistemas financieros).
  - Herramientas de ciberseguridad (antivirus, sistemas de detección de intrusos).
  - Aplicaciones de investigación científica.
- **Datos:**
  - Registros personales y académicos de estudiantes.
  - Datos de investigación (proyectos científicos, bases de datos sensibles).
  - Información financiera (presupuestos, nóminas, becas).
- **Personal:**
  - Equipo de TI responsable de la infraestructura tecnológica.
  - Docentes e investigadores que generan y gestionan información crítica.
  - Estudiantes y colaboradores externos que acceden a sistemas.

2. Identificación de Amenazas Potenciales

Amenazas externas:

- **Ataques cibernéticos:**
  - Phishing: Engaños para capturar credenciales de usuarios.
  - Ransomware: Bloqueo de sistemas mediante encriptación.
  - Ataques DDoS: Sobrecarga de servidores y pérdida de disponibilidad.
- **Desastres naturales:**
  - Terremotos, incendios o inundaciones que dañen infraestructura crítica.
- **Robo físico:**
  - Sustitución o extracción de dispositivos de centros de datos o campus.

Amenazas internas:

- **Errores humanos:**
  - Configuración incorrecta de sistemas o eliminación accidental de datos.
- **Acceso indebido:**
  - Abuso de privilegios por parte de empleados o estudiantes.
- **Uso no autorizado:**
  - Instalación de software no aprobado o manejo inadecuado de información.

3. Identificación de Vulnerabilidades

Vulnerabilidades detectadas:

- **Hardware:**
  - Ausencia de redundancia en sistemas críticos.
  - Falta de acceso restringido en áreas de servidores.
- **Software:**
  - Aplicaciones sin parches actualizados.
  - Ausencia de autenticación multifactor en sistemas administrativos.
- **Datos:**
  - Bases de datos sin cifrado adecuado.
  - Registro insuficiente de accesos a información sensible.

- **Personal:**
  - Falta de capacitación en ciberseguridad.
  - Políticas de acceso no revisadas periódicamente.

4. Evaluación de Probabilidad e Impacto

Riesgo	Probabilidad	Impacto	Calificación
Acceso no autorizado	Alta	Compromiso crítico	Alto
Malware en sistemas críticos	Media	Interrupción total	Alto
Desastres naturales	Baja	Daño físico	Medio
Contraseñas débiles	Alta	Violación de datos	Alto
Errores humanos	Media	Pérdida operativa	Medio

5. Priorización de Riesgos

1. **Alta prioridad:**
   - Acceso no autorizado.
   - Malware en sistemas críticos.
   - Contraseñas débiles.
2. **Media prioridad:**
   - Errores humanos.
   - Desastres naturales.
3. **Baja prioridad:**
   - Robo físico (cuando el acceso físico está asegurado con controles).

Plan de acción inicial:

1. Implementar autenticación multifactor en todos los sistemas críticos.
2. Realizar simulaciones de incidentes para capacitar al personal.
3. Desarrollar un plan de recuperación ante desastres que cubra sistemas y datos clave.

Selección de Controles de Seguridad para la Universidad de California

1. Revisión de Normas Relevantes

La selección de controles se basa en marcos de referencia ampliamente aceptados en la industria que ofrecen directrices específicas para la protección de información sensible y la mitigación de riesgos:

- **ISO/IEC 27001:**

Este estándar internacional establece los requisitos para implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI). Proporciona un enfoque sistemático para gestionar los riesgos de seguridad de la información mediante controles organizativos, técnicos y físicos. Es particularmente relevante para la UC por su enfoque integral en la gestión de riesgos y el cumplimiento normativo.

- **NIST SP 800-53:**

Este marco, desarrollado por el Instituto Nacional de Estándares y Tecnología de los Estados Unidos, ofrece un conjunto de controles de seguridad y privacidad que son altamente detallados. Entre las categorías clave están la protección contra amenazas cibernéticas, la gestión de accesos y la respuesta ante incidentes. Es adecuado para sistemas de información con altos requisitos de seguridad, como los utilizados en universidades.

- **CIS Controls:**

Una lista priorizada de acciones prácticas divididas en 18 controles fundamentales. Los controles incluyen gestión de inventario, análisis continuo de vulnerabilidades y monitoreo de actividades. Este marco es especialmente útil para identificar acciones de rápida implementación que mejoran significativamente la postura de seguridad de una organización.

- **Regulaciones sectoriales específicas:**
    - **FERPA:** Protege la privacidad de los registros educativos de los estudiantes y establece requisitos específicos sobre el acceso y manejo de esta información.
    - **HIPAA:** Garantiza la seguridad de los datos de salud, aplicable a centros médicos y sistemas de investigación médica en la UC.

2. Controles de Seguridad Seleccionados

La selección de controles se enfoca en abordar los riesgos críticos identificados mediante una combinación de controles técnicos, administrativos y físicos:

Técnicos:

- **Autenticación Multifactor (MFA):**
  - **Objetivo:** Prevenir accesos no autorizados a sistemas críticos mediante la exigencia de múltiples factores de autenticación, como contraseñas y tokens.
  - **Implementación:** Integración de herramientas MFA en sistemas administrativos, académicos y de investigación.
  - **Ventajas:** Mitiga significativamente el riesgo de acceso no autorizado, incluso si las contraseñas son comprometidas.

- **Actualizaciones automatizadas:**
  - **Objetivo:** Garantizar que los sistemas operativos y aplicaciones estén protegidos contra vulnerabilidades conocidas mediante la instalación automática de parches de seguridad.
  - **Implementación:** Configuración de servidores y estaciones de trabajo para ejecutar actualizaciones fuera de horario laboral para minimizar interrupciones.
  - **Ventajas:** Reduce la exposición a ataques de día cero y exploits conocidos.

- **Sistemas de detección de intrusiones (IDS):**
  - **Objetivo:** Identificar actividades anómalas en tiempo real y alertar sobre posibles ataques.
  - **Implementación:** Implementación en redes internas y puntos de acceso externos.
  - **Ventajas:** Proporciona visibilidad y capacidad de respuesta ante amenazas emergentes.

Administrativos:

- **Política de contraseñas robustas:**
  - **Objetivo:** Asegurar que las contraseñas utilizadas sean seguras y cambien periódicamente.
  - **Implementación:** Configuración de requisitos mínimos de longitud y complejidad en el sistema de gestión de credenciales.
  - **Ventajas:** Reduce el riesgo de accesos no autorizados debido a contraseñas débiles.

- **Capacitación periódica:**
  - **Objetivo:** Educar al personal y estudiantes sobre mejores prácticas en ciberseguridad.
  - **Implementación:** Talleres trimestrales sobre detección de phishing, uso seguro de redes y políticas internas.
  - **Ventajas:** Disminuye la probabilidad de errores humanos y fomenta una cultura de seguridad.

Físicos:

- **Control de acceso a instalaciones críticas:**
  - **Objetivo:** Proteger centros de datos, laboratorios y oficinas administrativas sensibles.
  - **Implementación:** Uso de tarjetas de identificación con autenticación biométrica para áreas restringidas.
  - **Ventajas:** Minimiza el riesgo de acceso físico no autorizado.

- **Sistemas de videovigilancia:**
  - **Objetivo:** Monitorear áreas clave para disuadir robos o accesos no autorizados.
  - **Implementación:** Instalación de cámaras con almacenamiento en servidores seguros y revisiones periódicas.
  - **Ventajas:** Aumenta la capacidad de respuesta ante incidentes físicos.

3. Documentación de la Implementación

Para cada control, se especifican los pasos de implementación, roles responsables y métricas para evaluar su eficacia:

Control Seleccionado	Pasos de Implementación	Responsable	Métrica de Éxito
Autenticación multifactor	Configurar herramientas MFA en sistemas clave, capacitar usuarios y monitorear actividad.	Equipo de TI	100% de sistemas críticos con MFA habilitado.
Actualizaciones automatizadas	Activar políticas de actualizaciones automáticas en estaciones y servidores, revisar logs mensualmente.	Equipo de TI	90% de sistemas actualizados en tiempo real.
Política de contraseñas robustas	Definir políticas en el sistema, comunicar requisitos a usuarios y realizar auditorías periódicas.	Administradores de sistemas	Reducción de incidentes relacionados con credenciales.
Capacitaciones periódicas	Diseñar contenido de talleres, realizar sesiones prácticas y medir conocimiento adquirido mediante encuestas.	Recursos Humanos y TI	80% de participantes superan evaluaciones.
Control de acceso físico	Instalar cerraduras electrónicas, configurar autenticación biométrica y realizar auditorías de acceso.	Administradores de campus	Incidentes físicos reportados reducidos a cero.

4. Planificación de la Implementación

Un plan detallado garantiza que los controles se implementen dentro de los plazos y recursos disponibles. A continuación, se describen las actividades principales:

- **Autenticación Multifactor:**
  - **Duración:** 2 meses.
  - **Requerimientos:** Tokens de seguridad, capacitación del personal.
  - **Actividades:** Configuración inicial, pruebas en entornos controlados, implementación masiva.
- **Actualizaciones Automatizadas:**
  - **Duración:** 1 mes.
  - **Requerimientos:** Software de gestión de actualizaciones.
  - **Actividades:** Instalación de sistemas automatizados, revisión de compatibilidad, monitoreo continuo.
- **Capacitaciones en Seguridad:**
  - **Duración:** 2 semanas por taller.
  - **Requerimientos:** Material educativo, presupuesto para facilitadores.
  - **Actividades:** Desarrollo de contenido, ejecución de talleres, evaluación post-taller.

Conclusión

La selección y planificación de estos controles permiten mitigar riesgos críticos en el Sistema de la Universidad de California. Este enfoque integrado asegura la protección de activos clave, fomenta una cultura de seguridad y garantiza la continuidad operativa frente a amenazas crecientes.

Documentación de Políticas y Procedimientos de Seguridad

1. Política de Seguridad

Propósito

La Universidad de California tiene como objetivo establecer un entorno seguro para proteger la información crítica y asegurar la continuidad de sus operaciones. Este propósito se basa en la adopción de estándares internacionales y mejores prácticas para la gestión de seguridad.

Principios clave

1. **Confidencialidad:**
    - Asegurar que solo las personas autorizadas tengan acceso a la información sensible.
    - Implementar controles como el cifrado de datos y políticas de acceso restringido.
2. **Integridad:**
    - Garantizar que los datos no sean alterados o manipulados de forma no autorizada.
    - Implementar sistemas de auditoría para detectar cambios no autorizados.
3. **Disponibilidad:**
    - Asegurar que la información esté accesible para los usuarios autorizados en cualquier momento.
    - Configurar sistemas de alta disponibilidad y planes de recuperación ante desastres.

Alcance

Esta política aplica a:

- **Sistemas tecnológicos:** Hardware, software y redes gestionadas por la universidad.
- **Datos:** Información académica, financiera y de investigación almacenada en sistemas internos o en la nube.
- **Usuarios:** Personal administrativo, docentes, investigadores, estudiantes y terceros autorizados.

Declaración de cumplimiento

La Universidad de California se compromete a cumplir con normativas y estándares aplicables como:

- **ISO/IEC 27001:** Gestión de seguridad de la información.
- **FERPA:** Protección de los derechos de los estudiantes.
- **HIPAA:** Seguridad de datos médicos.

2. Control de Acceso de Usuarios

Directrices generales

- **Asignación de accesos:**
  - Los permisos serán otorgados únicamente con base en la necesidad operativa y aprobados por el supervisor correspondiente.
- **Revisión de accesos:**
  - Accesos revisados trimestralmente para garantizar su adecuación al rol actual del usuario.
- **Revocación de accesos:**
  - Implementación inmediata al finalizar una relación laboral, académica o contractual.

Política de contraseñas

1. **Requisitos técnicos:**
   - Longitud mínima de 16 caracteres.
   - Incluir una combinación de letras mayúsculas, minúsculas, números y caracteres especiales.
   - Prohibido usar contraseñas basadas en información personal o palabras comunes.
2. **Gestión del ciclo de vida de contraseñas:**
   - Cambios obligatorios cada 90 días.
   - Prohibición de reutilización de contraseñas anteriores durante al menos los últimos 12 ciclos.
3. **Autenticación multifactor (MFA):**
   - Obligatoria para el acceso a sistemas críticos, implementada con tokens físicos o aplicaciones móviles de autenticación.

Gestión de privilegios

- **Principio de privilegios mínimos:**
  - Los usuarios tendrán únicamente los permisos necesarios para cumplir sus funciones.
- **Auditorías de permisos:**
  - Realización de auditorías trimestrales para identificar accesos no autorizados o excesivos.

3. Plan de Respuesta a Incidentes

Definición de incidente

Un incidente de seguridad es cualquier evento que comprometa la confidencialidad, integridad o disponibilidad de la información. Esto incluye:

- Accesos no autorizados a sistemas críticos.
- Ataques cibernéticos como ransomware, phishing o DDoS.
- Pérdida, robo o destrucción de dispositivos con información sensible.
- Configuraciones incorrectas que permitan brechas de seguridad.

Procedimiento paso a paso

1. **Identificación:**
   - Detección inicial mediante herramientas de monitoreo o reportes manuales de usuarios.
   - Clasificación del incidente según su criticidad (alto, medio, bajo).
2. **Notificación:**
   - Informar al Equipo de Respuesta a Incidentes (IRT) dentro de los primeros 15 minutos.
   - Documentar el incidente en un sistema de gestión.
3. **Contención:**
   - Aislar los sistemas afectados del resto de la red.
   - Activar medidas temporales para detener la propagación del impacto.
4. **Investigación:**
   - Realizar análisis forense para determinar la causa raíz y el alcance del daño.
   - Identificar vulnerabilidades explotadas.
5. **Mitigación:**

    - Implementar parches, ajustes de configuración o restauraciones desde copias de seguridad.
6. **Cierre:**
    - Documentar el incidente, incluyendo lecciones aprendidas.
    - Actualizar políticas y controles para evitar recurrencias.

Roles y responsabilidades

- **IRT (Equipo de Respuesta a Incidentes):**
  Responsable de la identificación, contención y mitigación.
- **Usuarios finales:**
  Obligación de informar anomalías o incidentes sospechosos.

4. Copia de Seguridad y Recuperación de Datos

Procedimientos

1. **Automatización:**
    - Implementar sistemas automáticos para copias de seguridad.
    - Configurar respaldos incrementales diarios y completos semanales.
2. **Almacenamiento externo:**
    - Mantener una copia mensual en una ubicación fuera del sitio principal.
3. **Pruebas regulares:**
    - Realizar simulaciones de recuperación semestrales para garantizar la integridad de los datos.

Roles responsables

- **Administradores de sistemas:**
    - Monitorear y verificar la realización de respaldos según lo programado.
- **Auditores internos:**
    - Revisar informes de respaldos para detectar posibles inconsistencias.

5. Concienciación y Capacitación de los Empleados

Plan de capacitación

1. **Sesiones iniciales:**
    - Formación obligatoria para nuevos empleados sobre políticas de seguridad.
2. **Actualizaciones periódicas:**
    - Talleres trimestrales sobre ciberseguridad.
3. **Simulaciones:**
    - Pruebas regulares para evaluar la preparación ante amenazas como ataques de phishing.

Materiales de concienciación

1. **Boletines informativos:**
    - Envío mensual con actualizaciones de seguridad y consejos prácticos.
2. **Carteles:**
    - Colocados en lugares estratégicos con recordatorios de mejores prácticas de seguridad.

6. Aprobación y Revisión de Documentos

Proceso de aprobación

1. **Revisión inicial:**
    - El Comité de Seguridad evalúa todas las políticas y procedimientos antes de su implementación.
2. **Aprobación final:**
    - Firmada por el director del campus o el comité de gobernanza.

Revisión periódica

1. **Frecuencia:**
    - Todas las políticas serán revisadas anualmente.
2. **Revisiones extraordinarias:**
    - Tras incidentes significativos o cambios regulatorios.

Tabla Resumen del Informe

Sección	Descripción Breve	Puntos Clave
1. Política de Seguridad	Establece el compromiso de la universidad con la protección de la información.	Confidencialidad, Integridad, Disponibilidad, Cumplimiento de normativas (FERPA, HIPAA, ISO/IEC 27001).
2. Control de Acceso	Define cómo se otorgan, modifican y revocan los accesos de los usuarios.	Privilegios mínimos, autenticación multifactor, auditorías trimestrales, política de contraseñas robustas.
3. Plan de Respuesta a Incidentes	Describe cómo gestionar incidentes de seguridad de forma estructurada.	Identificación, Notificación, Contención, Mitigación, Documentación y Roles específicos del IRT.
4. Copia de Seguridad	Procedimientos para garantizar la disponibilidad y recuperación de datos.	Respaldos diarios y semanales, pruebas semestrales, almacenamiento externo cifrado.
5. Concienciación y Capacitación	Estrategias para formar al personal y fomentar una cultura de ciberseguridad.	Talleres trimestrales, simulaciones, carteles informativos, boletines mensuales.
6. Aprobación y Revisión	Define cómo se revisan, aprueban y actualizan las políticas de seguridad.	Revisión anual obligatoria, revisiones extraordinarias tras incidentes o cambios regulatorios.

Tabla Resumen Detallada del Manual Completo SGSI

Sección	Descripción Extensa	Puntos Clave
1. Alcance del SGSI	Define los límites y la cobertura del SGSI, incluyendo activos, ubicaciones y partes interesadas.	- **Activos identificados:** - Hardware: servidores, equipos de red, computadoras personales. - Software: sistemas académicos, administrativos y herramientas de ciberseguridad. - Datos: registros de estudiantes, datos financieros, datos de investigación. - Personal: equipo de TI, docentes, estudiantes, contratistas. - **Límites físicos:** - Campus universitarios, centros de datos, bibliotecas. - Áreas restringidas: salas de servidores, laboratorios críticos. - **Límites virtuales:** - Redes internas y en la nube. - Máquinas virtuales y sistemas de correo electrónico. - **Partes interesadas:** Equipo de TI, administración, usuarios finales, contratistas.

2. Evaluación de Riesgos	Identifica y evalúa los riesgos asociados a los activos, considerando amenazas y vulnerabilidades.	- **Inventario de activos:** Clasificación en hardware, software, datos y personal. - **Amenazas potenciales:** - Externas: ransomware, phishing, desastres naturales. - Internas: errores humanos, accesos indebidos. - **Vulnerabilidades:** - Contraseñas débiles, falta de cifrado, software desactualizado. - **Evaluación de riesgos:** - Probabilidad: alta, media, baja. - Impacto: crítico, alto, moderado, bajo. - **Riesgos priorizados:** Acceso no autorizado, malware, desastres naturales, errores humanos.
3. Controles de Seguridad	Controles implementados para mitigar riesgos identificados, divididos en técnicos, administrativos y físicos.	- **Controles técnicos:** - Implementación de autenticación multifactor (MFA). - Uso de firewalls y sistemas de detección de intrusos. - Cifrado de datos sensibles. - **Controles administrativos:** - Políticas de seguridad detalladas. - Auditorías internas trimestrales. - Talleres de capacitación. - **Controles físicos:** - Acceso restringido a salas de servidores. - Videovigilancia en áreas críticas. - Supervisión de dispositivos portátiles.

4. Políticas y Procedimientos	Documentación de prácticas formales para garantizar la seguridad de la información en la organización.	- **Política de seguridad:** - Principios de confidencialidad, integridad y disponibilidad. - Compromiso con estándares internacionales como ISO/IEC 27001. - **Plan de respuesta a incidentes:** - Definición de incidentes: ataques cibernéticos, accesos no autorizados, pérdida de datos. - Procedimiento: identificación, notificación, contención, mitigación y cierre. - Roles responsables: equipo de TI, usuarios finales, administración. - **Copia de seguridad:** - Respaldos diarios y semanales. - Almacenamiento externo cifrado. - Pruebas semestrales de recuperación.
5. Capacitación y Concienciación	Estrategias para educar al personal sobre ciberseguridad y fomentar una cultura organizacional de seguridad.	- **Capacitación:** - Talleres iniciales para nuevos empleados y estudiantes. - Actualizaciones trimestrales sobre amenazas emergentes. - **Concienciación:** - Carteles y guías rápidas en espacios comunes. - Simulaciones regulares de phishing. - Boletines informativos mensuales.

6. Revisión y Aprobación	Proceso estructurado para mantener actualizadas las políticas y procedimientos de seguridad.	- **Aprobación inicial:** - Revisión por el Comité de Seguridad. - Firma final por la administración superior. - **Revisión periódica:** - Actualización obligatoria cada 12 meses. - Revisiones extraordinarias tras incidentes o cambios regulatorios. - **Documentación:** - Registros de todas las revisiones y aprobaciones.