ISO 27001:2022: Guía de Implementación de Sistemas de Gestión de Seguridad de la Información

Publicado por: Nimbus TechWeb: https://nimbustech.es

nimbus
TECH

Índice

Introducción: Por qué ISO 27001 es clave en 2025

Vivimos en una época donde la seguridad de la información no es un valor añadido, sino una necesidad absoluta para la continuidad y el éxito de cualquier empresa. Los datos son el nuevo oro, y protegerlos va mucho más allá de instalar un antivirus o bloquear un puerto del firewall.

Cada día, las organizaciones en España y en el resto del mundo enfrentan ciberataques más sofisticados, brechas de datos que amenazan su reputación y un entorno legal cada vez más exigente.

ISO 27001: Herramienta estratégica indispensable

En este contexto, la norma ISO 27001:2022 se convierte en una herramienta estratégica indispensable. No hablamos solo de un estándar internacional reconocido: hablamos de una metodología probada para que las empresas gestionen la seguridad de su información de forma sistemática, alineada con los riesgos reales y con los objetivos del negocio.

nimbus
TECH

¿Por qué es especialmente importante en 2025?

1. La amenaza es constante y evoluciona sin pausa

Los ataques de ransomware, el espionaje industrial, el phishing o las amenazas internas no dejan de perfeccionarse. Da igual que seas una pyme, una startup o una gran empresa: si manejas datos valiosos o sistemas críticos, estás en el radar de los ciberdelincuentes.

Dato relevante: En 2024, el número de ciberataques a empresas españolas creció un 38% respecto al año anterior.

nimbus TECH

Exigencias legales en aumento

2. Las exigencias legales se multiplican

Las autoridades europeas y nacionales están endureciendo las normas en materia de protección de datos y ciberseguridad. En España, el Esquema Nacional de Seguridad (ENS), la llegada de la directiva NIS2 y la consolidación del RGPD marcan el paso.

Cumplir estos marcos regulatorios sin un sistema de gestión sólido es simplemente inviable.

La confianza como activo diferencial

3. La confianza se ha vuelto un activo diferencial

Hoy, los clientes, los socios y hasta los propios empleados exigen garantías de que sus datos están protegidos. La ISO 27001 es, en la práctica, un pasaporte de confianza que te abre puertas en concursos públicos, colaboraciones estratégicas o acuerdos comerciales internacionales.

El entorno tecnológico lo demanda

4. El entorno tecnológico lo demanda

El teletrabajo, el cloud computing, el acceso remoto, los entornos multicloud o la inteligencia artificial han ampliado la superficie de ataque de forma exponencial.

ISO 27001:2022 introduce controles específicamente adaptados a estos nuevos entornos, lo que la convierte en una herramienta actualizada para un mundo hiperconectado.

Más que un certificado: una estrategia

Certificar un SGSI bajo ISO 27001 no es simplemente colgar un diploma en la pared. Es adoptar una cultura de la seguridad que permea toda la organización.

Implica:

Formar a los equipos

Identificar los riesgos

Establecer controles adecuados

Monitorizar y mejorar continuamente

Un enfoque flexible y adaptable

Todo ello con un enfoque flexible que se adapta a las prioridades y los recursos de cada empresa.

En Nimbus Tech hemos visto cómo un SGSI bien implantado transforma la forma de trabajar de nuestros clientes, especialmente en sectores sensibles como el sanitario, el financiero o el tecnológico. No solo protegen sus activos: ganan en eficiencia, en resiliencia y en competitividad.

Un paso necesario para empresas IT y más allá.

Obligación tácita para empresas IT

En los siguientes apartados te mostraremos no solo cómo implantar la ISO 27001 paso a paso, sino cómo convertirla en un verdadero motor de valor para tu negocio, con ejemplos, herramientas y consejos prácticos basados en nuestra experiencia en Nimbus Tech.

Para las empresas IT, que gestionan infraestructuras y servicios críticos para terceros, la certificación ISO 27001 es casi una obligación tácita.

Pero incluso para sectores no tecnológicos, es la vía más eficaz para asegurar la continuidad de negocio frente a una amenaza que ya no es una posibilidad remota, sino una realidad cotidiana.

Marco legal en España: ENS, NIS2, RGPD y conexión con ISO 27001

La gestión de la seguridad de la información no ocurre en un vacío. En España, el marco legal está evolucionando rápidamente para adaptarse a los nuevos retos que plantea la ciberseguridad. Para cualquier empresa que busque proteger sus datos y garantizar el cumplimiento normativo, es fundamental conocer y entender cómo se articulan estas regulaciones.

nimbus TECH

ENS: Esquema Nacional de Seguridad

El Esquema Nacional de Seguridad (ENS) es el referente en España para garantizar la protección de la información en el ámbito de las Administraciones Públicas y de las empresas que prestan servicios a éstas.

¿A quién afecta?

- Empresas que trabajan directamente con organismos públicos
- Proveedores tecnológicos que prestan servicios a la Administración
- Empresas privadas que gestionan datos o infraestructuras críticas

nimbus TECH

Conexión entre ENS e ISO 27001

Conexión con ISO 27001

El ENS se basa en los mismos principios de la ISO 27001: la protección de la confidencialidad, integridad y disponibilidad de la información. Un SGSI certificado facilita enormemente cumplir con los requisitos del ENS.

Ventaja: Empresas con ISO 27001 tienen el camino más avanzado para certificar el ENS, ya que comparten controles y metodologías.

NIS2: Directiva Europea de Seguridad

La Directiva NIS2 reemplaza a la anterior NIS y establece nuevas obligaciones para reforzar la seguridad en sectores críticos y servicios esenciales en la Unión Europea.

¿A quién afecta en España?

- Empresas de energía, agua, salud, banca, infraestructuras digitales
- Proveedores de servicios digitales clave
- Operadores de servicios esenciales

Exigencias principales

- Implantación de políticas de gestión de riesgos
- Reporte de incidentes graves en menos de 24 horas
- Realización de auditorías periódicas

nimbus TECH

Relación entre NIS2 e ISO 27001

Relación con ISO 27001

La ISO 27001 ofrece el marco perfecto para organizar y documentar las medidas exigidas por la NIS2. Implantar un SGSI permite a las empresas anticiparse al cumplimiento de esta directiva, cuya transposición en España se consolidará en 2025.

RGPD: Reglamento General de Protección de Datos

El RGPD regula el tratamiento de datos personales dentro de la UE. Más allá de la protección legal, se trata de un compromiso ético con clientes y usuarios.

Puntos clave:

- Evaluación de Impacto en Protección de Datos (EIPD)
- Notificación de brechas de seguridad en un máximo de 72 horas
- Obligación de adoptar medidas técnicas y organizativas adecuadas

nimbus TECH

Conexión entre RGPD e ISO 27001

Conexión con ISO 27001

Un SGSI bien definido permite demostrar el cumplimiento del RGPD mediante políticas claras, trazabilidad documental y control sobre los accesos a la información.

Beneficios de alinear el SGSI con las regulaciones

- Evitas sanciones y responsabilidades legales
- Mejoras tu reputación y credibilidad
- Ganas ventaja en licitaciones públicas y contratos internacionales
- Simplificas auditorías regulatorias y de clientes

Consejo Nimbus: Las empresas que anticipen la adaptación a NIS2 y el cumplimiento del ENS mediante un SGSI basado en ISO 27001 no solo estarán cubiertas legalmente, sino que además consolidarán una ventaja competitiva en su sector.

Cómo implementar un SGSI paso a paso

Implementar un Sistema de Gestión de la Seguridad de la Información (SGSI) según ISO 27001 no es una tarea sencilla, pero con un enfoque ordenado y práctico, cualquier empresa —independientemente de su tamaño o sector— puede lograrlo con éxito.

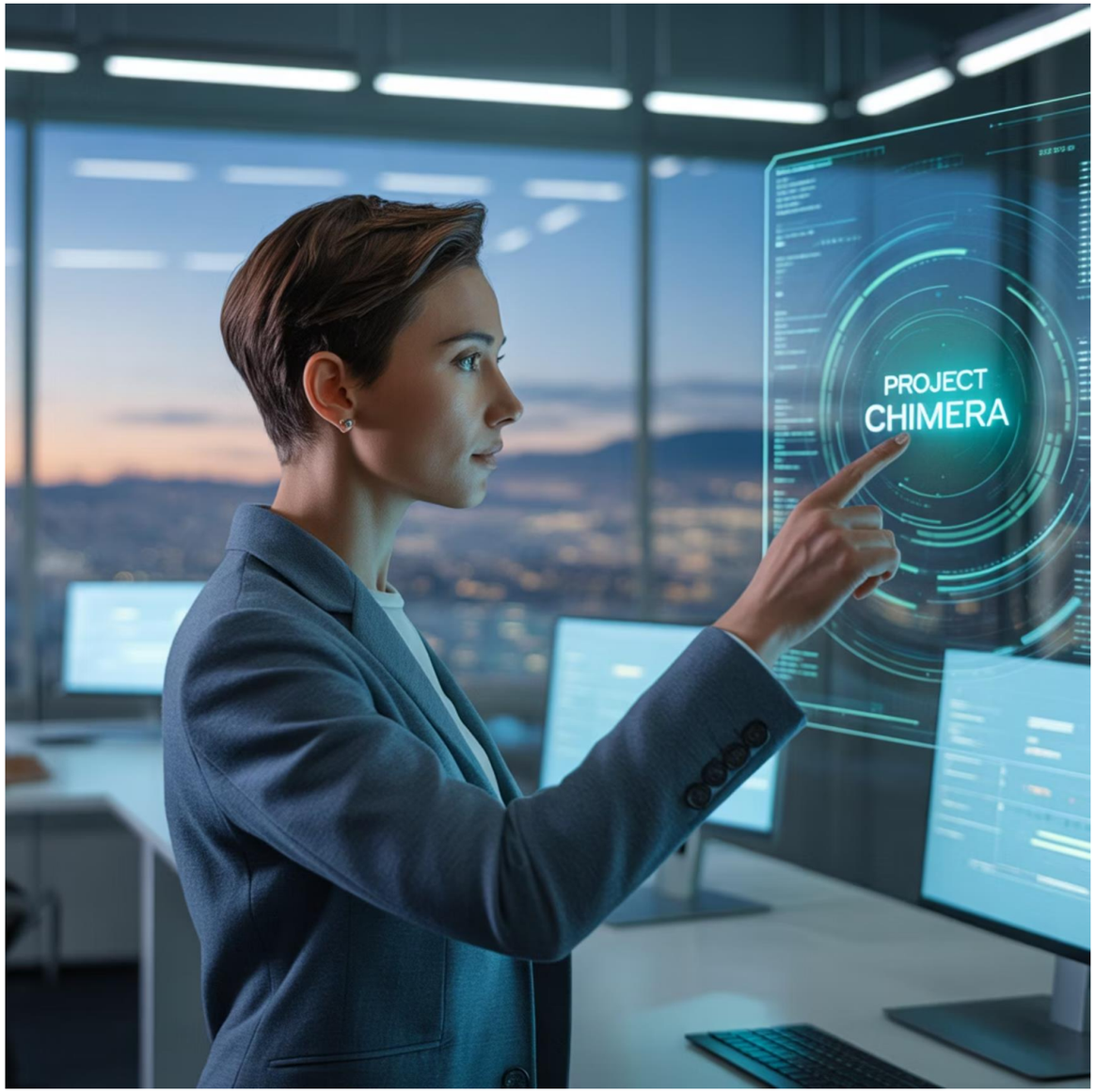
En Nimbus Tech hemos definido un método estructurado en 7 fases, que aplicamos tanto en nuestros proyectos propios como en los de clientes que nos confían la implantación de su SGSI.

nimbus TECH

Fase 1: Diagnóstico inicial y análisis de madurez

Antes de empezar, es imprescindible saber dónde estamos. Realizamos un análisis de la situación actual de la organización respecto a la seguridad de la información, para identificar:

- Fortalezas y debilidades en materia de seguridad.
- Riesgos potenciales
- Normativas que afectan al negocio (ENS, NIS2, RGPD...)
- Nivel de concienciación de la plantilla



Herramienta recomendada: Cuestionarios de madurez, entrevistas con responsables clave y análisis de documentación existente.

Fase 2: Definir el alcance del SGSI

No siempre es necesario que el SGSI abarque el 100% de la organización, aunque en muchas empresas IT es recomendable. Definir correctamente el alcance es crítico para establecer:

1. **Procesos incluidos**

   Qué procesos, departamentos o servicios están incluidos en el sistema de gestión.

2. **Sistemas críticos**

   Qué sistemas de información y activos críticos se protegerán dentro del alcance.

3. **Ubicaciones**

   Qué ubicaciones físicas o virtuales quedan dentro del SGSI y cuáles no.

Una definición clara evita ambigüedades y facilita la implantación y posterior auditoría.

nimbus TECH

Fase 3: Análisis de riesgos y oportunidades

La ISO 27001 exige un enfoque basado en riesgos. Esto implica:

Identificar amenazas y vulnerabilidades

Catalogar todas las posibles amenazas que podrían afectar a los activos de información.

Valorar impacto y probabilidad

Evaluar el impacto potencial y la probabilidad de que ocurran los eventos identificados.

Determinar nivel de riesgo

Calcular el nivel de riesgo asociado a cada activo en función del impacto y la probabilidad.

Definir acciones

Determinar cómo tratar esos riesgos: evitarlos, transferirlos, mitigarlos o aceptarlos.

Herramienta recomendada: Metodologías como MAGERIT, ISO 31000 o CRAMM. En Nimbus Tech usamos combinaciones personalizadas adaptadas al cliente.

Fase 4: Definir la política y los objetivos de seguridad

Establecer la política de seguridad de la información es el pilar estratégico que guiará todas las acciones del SGSI. Esta política debe estar alineada con:

- Los objetivos de negocio
- Las expectativas de las partes interesadas
- La cultura corporative

También se fijan los objetivos de seguridad: específicos, medibles, alcanzables, relevantes y limitados en el tiempo (SMART).

Fase 5: Implementación de controles y medidas de seguridad

Aquí es donde entra en juego el famoso Anexo A de la ISO 27001 con sus 93 controles. La empresa debe seleccionar los controles adecuados en función del análisis de riesgos previo.

Consejo práctico: No todos los controles aplican igual a todas las empresas. Una pyme tecnológica que trabaja en cloud priorizará controles distintos a una empresa industrial.

Doble factor de autenticación (MFA)

Políticas de clasificación de la información

Restricciones de acceso basadas en roles

Seguridad física en oficinas y CPDs

Cifrado de datos en tránsito y en reposo

Fase 6: Formación, concienciación y cultura de seguridad

El mejor SGSI del mundo puede fracasar si las personas no están alineadas. Por eso es clave:

- Formar al personal en prácticas seguras
- Concienciar sobre la importancia de proteger la información
- Promover una cultura de seguridad proactiva

Nimbus Tip: Programas gamificados o simulaciones de phishing son muy efectivos para sensibilizar.

Fase 7: Auditoría interna, revisión y mejora continua

La ISO 27001 sigue el ciclo PDCA (Plan-Do-Check-Act). Una vez implantado el SGSI, toca:

Realizar auditorías internas periódicas

Verificar el cumplimiento de los requisitos de la norma y la eficacia de los controles.

Revisar el sistema por parte de la dirección

Evaluar el desempeño del SGSI y tomar decisiones estratégicas.

Corregir desviaciones y mejorar procesos

Implementar acciones correctivas y oportunidades de mejora.

Este ciclo garantiza que el SGSI no se queda obsoleto, sino que evoluciona con el negocio y con el entorno de amenazas.

Tiempo estimado para implantar un SGSI

4-6

Pequeñas empresas

Meses para completar la implantación

6-9

Empresas medianas

Meses para completar la implantación

9-12+

Grandes empresas

Meses para completar la implantación

⚠ **Importante:** Esto es una referencia general. El plazo real depende del nivel de madurez previo, el alcance definido y los recursos disponibles.

Con estas fases bien estructuradas, cualquier empresa puede desplegar un SGSI sólido y alineado con la ISO 27001. En el próximo apartado, veremos un checklist práctico para que no se escape ningún paso esencial.

Checklist de fases críticas para implantar un SGSI

Para garantizar una implantación ordenada y sin lagunas, en Nimbus Tech hemos diseñado este checklist práctico en formato tabla, que sirve de hoja de ruta para cualquier empresa que quiera implantar un SGSI conforme a la ISO 27001.

nimbus TECH

Fase 1: Diagnóstico inicial

Fase	Objetivos clave	Actividades esenciales	Resultados esperados
1. Diagnóstico inicial	Evaluar la situación de partida	- Análisis de madurez- Identificación de normativas aplicables- Inventario de activos	Informe de situación inicial y riesgos preliminares

Fase 2: Definir el alcance

Fase	Objetivos clave	Actividades esenciales	Resultados esperados
2. Definir el alcance	Delimitar el perímetro del SGSI	- Definir procesos, servicios y ubicaciones incluidos- Aprobación por la dirección	Documento de Alcance del SGSI

Fase 3: Análisis de riesgos

Fase	Objetivos clave	Actividades esenciales	Resultados esperados
3. Análisis de riesgos	Identificar y tratar riesgos	- Identificación de amenazas- Valoración de impacto/probabilidad- Plan de tratamiento	Registro de riesgos y plan de tratamiento asociado

Fase 4: Políticas y objetivos

Fase	Objetivos clave	Actividades esenciales	Resultados esperados
4. Políticas y objetivos	Marcar la estrategia de seguridad	- Redacción de la política de seguridad- Definición de objetivos SMART- Comunicación interna	Política de seguridad y objetivos documentados

Fase 5: Controles y SoA

Fase	Objetivos clave	Actividades esenciales	Resultados esperados
5. Controles y SoA	Aplicar medidas de seguridad	- Selección de controles del Anexo A- Declaración de Aplicabilidad (SoA)- Implementación técnica y organizativa	Controles implementados y SoA validado

Fase 6: Formación y cultura

Fase	Objetivos clave	Actividades esenciales	Resultados esperados
6. Formación y cultura	Implicar al equipo	- Formación en buenas prácticas- Simulacros de seguridad- Evaluación de concienciación	Personal formado y concienciado

Fase 7: Documentación

Fase	Objetivos clave	Actividades esenciales	Resultados esperados
7. Documentación	Formalizar el SGSI	- Documentar procesos y procedimientos- Establecer control documental	Manual y procedimientos del SGSI actualizados

Fase 8: Auditoría interna y revisión

Fase	Objetivos clave	Actividades esenciales	Resultados esperados
8. Auditoría interna y revisión	Verificar el sistema	- Auditorías internas- Revisión por la dirección- Acciones correctivas	Informe de auditoría interna y revisión de dirección

Fase 9: Certificación externa

Fase	Objetivos clave	Actividades esenciales	Resultados esperados
9. Certificación externa	Obtener el reconocimiento formal	- Selección de certificadora acreditada- Auditoría de certificación- Corrección de desviaciones	Certificado ISO 27001 obtenido (opcional)

Fase 10: Mejora continua

Fase	Objetivos clave	Actividades esenciales	Resultados esperados
10. Mejora continua	Evolucionar el SGSI	- Revisión periódica de riesgos- Actualización de controles- Mejoras en procesos	SGSI actualizado y adaptado al negocio

Consejo Nimbus: Te recomendamos revisar esta tabla cada trimestre y validar que cada fase sigue vigente y alineada con la evolución de la empresa y su entorno.

Los 93 controles explicados con ejemplos prácticos y casos reales

La norma ISO 27001:2022 establece 93 controles de seguridad organizados en cuatro grandes categorías: controles organizativos, controles centrados en personas, controles físicos y controles tecnológicos. Cada control es un instrumento esencial para proteger los activos de información frente a los riesgos previamente identificados en el análisis de riesgos.

En Nimbus Tech, hemos implantado estos controles en empresas de diversos sectores, desde startups tecnológicas hasta grandes compañías industriales. Por ello, te explicamos cada bloque con detalle, incorporando ejemplos prácticos, buenas prácticas y recomendaciones específicas para empresas que operan en España.

Bloque 1: Controles organizativos (37 controles)

Estos controles establecen el marco de gobierno, políticas, procedimientos y directrices que rigen la seguridad de la información dentro de la organización.

Principales controles y ejemplos reales:

Política de Seguridad de la Información

Declaración formal del compromiso de la alta dirección. Por ejemplo, en una compañía de seguros con presencia nacional, ayudamos a definir una política que vinculaba la protección de datos con el cumplimiento del RGPD y la confianza del cliente.

Roles y responsabilidades

Definir qué personas o equipos son responsables de la seguridad en cada área. Un operador logístico con varios centros en España asignó responsables de seguridad locales, con coordinación centralizada desde IT.

Más controles organizativos

Gestión de proveedores

Implica la evaluación, contratación y seguimiento de los proveedores críticos. En una empresa SaaS, definimos cláusulas de seguridad en los contratos con partners cloud, incluyendo revisiones periódicas.

Clasificación de la información

Determinar qué datos son confidenciales, internos o públicos. Un bufete de abogados implementó un esquema de clasificación con etiquetas automáticas en los documentos gestionados en Microsoft 365.

Plan de continuidad de negocio

Garantizar la recuperación tras incidentes. Un banco digital estableció réplicas en la nube y simulacros anuales de recuperación ante desastres.

Bloque 2: Controles centrados en personas (8 controles)

Este bloque está diseñado para mitigar riesgos derivados del factor humano, como errores, malas prácticas o negligencias.

Controles clave y casos aplicados:

Concienciación y formación

Fundamental para que los empleados reconozcan amenazas. En una consultora tecnológica implantamos un programa de formación semestral con módulos específicos sobre ataques de ingeniería social.

Más controles centrados en personas

Proceso de incorporación y desvinculación

Incluye la asignación y retirada de permisos. Una entidad financiera automatizó la revocación de accesos en sus sistemas al notificarse la baja de empleados mediante su ERP.

Compromisos de confidencialidad

Firmar NDAs con empleados y proveedores antes de acceder a información sensible.

Control de privilegios

Asegurar que sólo el personal autorizado accede a la información que necesita. Un laboratorio farmacéutico implementó un modelo de control de accesos basado en el principio de mínimo privilegio.

Bloque 3: Controles físicos (14 controles)

Diseñados para proteger los activos físicos y los entornos donde se gestiona la información.

Ejemplos de controles físicos aplicados:

Control de acceso físico a instalaciones

Uso de tarjetas electrónicas, biometría o guardias de seguridad. Una empresa de energía restringió el acceso a sus salas de control con lectores biométricos y CCTV.

Más controles físicos

Protección contra amenazas ambientales

Sistemas antiincendios, refrigeración y alimentación eléctrica redundante. En un centro de datos en Madrid, se instalaron detectores tempranos de humo y sistemas de extinción por gas inerte.

Gestión segura de equipos móviles

Uso de fundas seguras, seguimiento por GPS o políticas de cifrado en dispositivos corporativos.

Política de puestos limpios

Garantiza que la información no quede expuesta en mesas o pantallas.

Bloque 4: Controles tecnológicos (34 controles)

El núcleo duro de la seguridad informática, enfocado en proteger redes, sistemas y aplicaciones.

Controles destacados y buenas prácticas:

Control de acceso lógico

Implementar autenticación multifactor (MFA) y políticas de contraseñas robustas. Un ecommerce nacional activó MFA en todos los accesos a su panel de gestión y backend.

nimbus TECH

Más controles tecnológicos

Cifrado de la información

Tanto en tránsito como en reposo. Un proveedor de servicios médicos cifró las historias clínicas tanto en su base de datos como en las comunicaciones mediante HTTPS.

Seguridad en la configuración

Mantener configuraciones seguras en todos los sistemas. Aplicamos las guías de configuración segura del CCN-CERT en infraestructuras públicas.

Protección contra malware

Implementación de soluciones EDR en endpoints. En un grupo hotelero, desplegamos un EDR que permitía bloquear ransomware en sus primeras fases.

Registro y monitorización

Captura de logs y supervisión continua. Una fintech implantó un SIEM para correlacionar eventos de seguridad en tiempo real.

Seguridad en el ciclo de vida del desarrollo

Integrar revisiones de seguridad en el desarrollo software (DevSecOps).

Cómo priorizar los controles según el tipo de empresa

La prioridad en la implementación de los controles varía según el sector, el tipo de información manejada y los riesgos identificados.

Tipo de empresa	Controles prioritarios
Empresas IT (SaaS, cloud)	Seguridad en el desarrollo, cifrado, control de accesos, monitorización continua, gestión de proveedores.
Industria (Manufactura, Energía)	Seguridad física, continuidad de negocio, protección contra malware, control de acceso físico y lógico.

Priorización de controles por sector (continuación)

Tipo de empresa	Controles prioritarios
Sanidad	Confidencialidad de datos, cifrado, clasificación de información, control de accesos, formación continua.
Banca y Fintech	Seguridad en transacciones, autenticación fuerte, monitorización, cifrado, respuesta ante incidentes.

Priorización de controles por sector (final)

Tipo de empresa	Controles prioritarios
Despachos profesionales	Clasificación de información, control de accesos, protección frente a fugas de información, formación en ciberhigiene.

Buenas prácticas transversales

- **Mantén una Declaración de Aplicabilidad (SoA) actualizada**
- **Asigna responsables claros para cada control**
- **Define KPIs de eficacia de los controles**
- **Realiza auditorías internas periódicas**
- **Actualiza el análisis de riesgos al menos una vez al año**

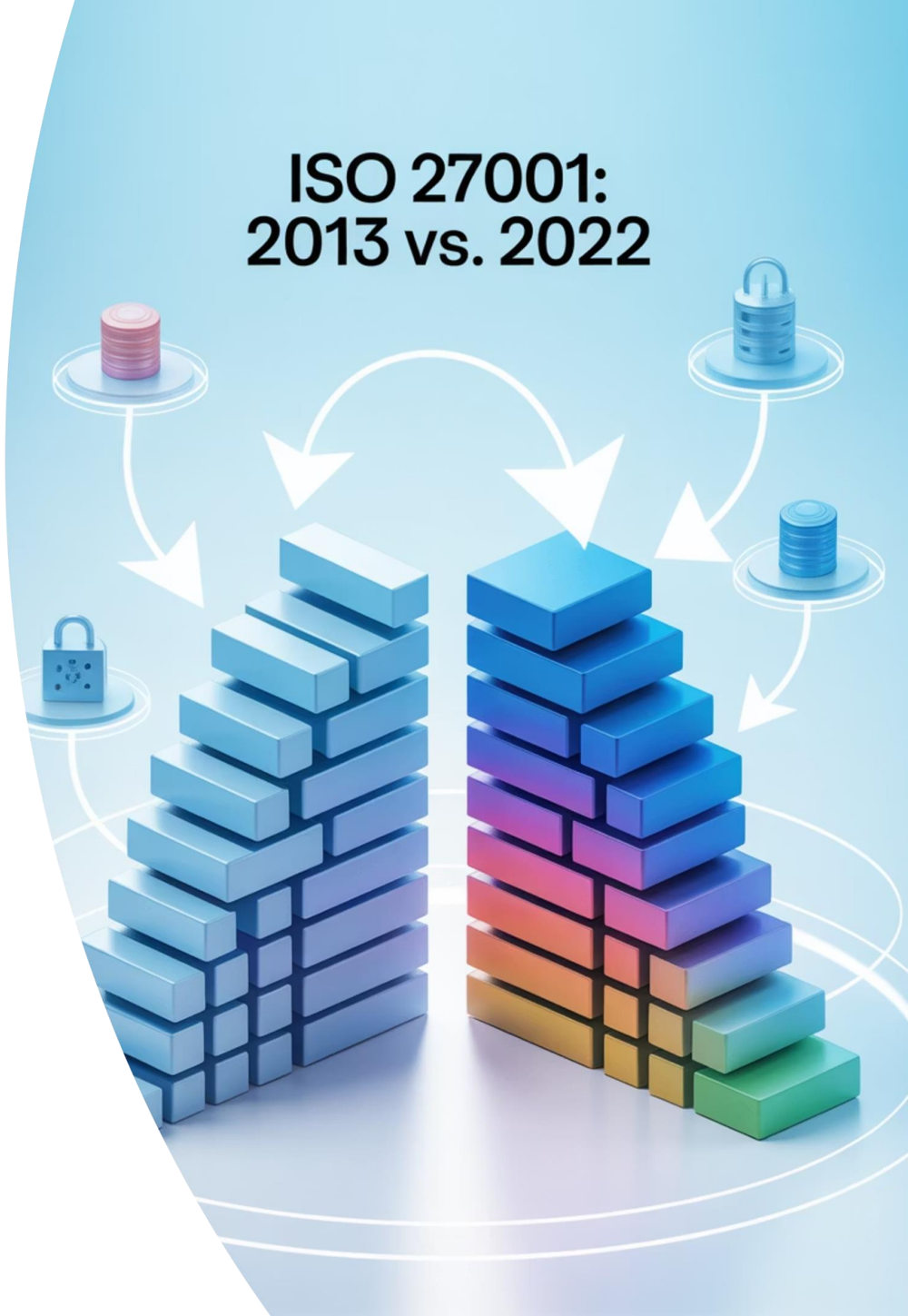
Recomendación Nimbus: Un SGSI efectivo no depende solo de implementar controles, sino de integrarlos en la cultura y en los procesos de negocio. Solo así se garantiza la seguridad como un elemento estratégico y no como un mero cumplimiento normativo.

Comparativa ISO 27001:2013 vs 2022: Cambios clave y su impacto en las empresas

La actualización de la norma ISO 27001 en 2022 ha supuesto una evolución significativa respecto a la versión de 2013. Más allá de una simple revisión, los cambios incorporados reflejan la necesidad de adaptarse a un entorno digital cada vez más complejo y a las nuevas amenazas en ciberseguridad.

En este apartado analizamos qué ha cambiado, por qué es relevante y cómo afecta a las empresas, especialmente a aquellas que ya estaban certificadas bajo la versión anterior.

Cambios estructurales en la norma



1. Reducción y reagrupación de controles

La ISO 27001:2013 contaba con 114 controles divididos en 14 dominios. La versión 2022 los reorganiza en 93 controles distribuidos en 4 categorías:

Categoría	N° de controles en 2022
Controles organizativos	37
Controles centrados en personas	8
Controles físicos	14
Controles tecnológicos	34

Este cambio no significa que se reduzca la protección, sino que algunos controles se han fusionado, otros se han clarificado y varios son completamente nuevos para abordar tecnologías y riesgos emergentes.

2. Introducción de controles nuevos

La actualización incorpora 11 controles nuevos, todos ellos diseñados para cubrir necesidades específicas derivadas de la transformación digital y las amenazas actuales.

Control nuevo	Descripción	Ejemplo práctico
Inteligencia de amenazas	Procesos para identificar y gestionar información sobre amenazas emergentes.	Implantar un servicio de threat intelligence que monitoriza fuentes OSINT y Dark Web.

Nuevos controles (continuación)

Control nuevo	Descripción	Ejemplo práctico
Seguridad en servicios en la nube	Asegurar el uso adecuado y seguro de servicios cloud.	Definir políticas para el uso de proveedores como AWS, Azure o Google Cloud.
Gestión de configuraciones	Garantizar que las configuraciones en sistemas se mantienen seguras.	Aplicar benchmarks de seguridad en servidores y dispositivos de red.

Nuevos controles (continuación)

Control nuevo	Descripción	Ejemplo práctico
Eliminación de información	Procedimientos para el borrado seguro de datos.	Uso de software certificado para eliminar datos en discos antes de su retirada o destrucción.
Prevención de fugas de información (DLP)	Detectar y evitar la pérdida de datos sensibles.	Implantar soluciones DLP en el correo electrónico corporativo.

Nuevos controles (final)

Control nuevo	Descripción	Ejemplo práctico
Actividades de monitoreo	Monitorizar continuamente la actividad de los sistemas.	Desplegar un SIEM que recoja logs y detecte patrones anómalos.
Seguridad de la información en el uso de servicios de la nube	Controlar la seguridad cuando se utilizan plataformas cloud.	Auditorías periódicas de configuración en entornos de Microsoft 365 o Google Workspace.

3. Mejora en la flexibilidad de implementación

La norma ahora incluye la atribución de controles mediante etiquetas, lo que facilita personalizar su aplicación en función de:

1. **Tipo de tecnología**

   Controles específicos para diferentes entornos tecnológicos.

2. **Modelo de negocio**

   Adaptación según las características de la organización.

3. **Entorno de amenazas**

   Focalización en las amenazas más relevantes para cada empresa.

Por ejemplo, controles etiquetados como "Cloud" o "Dispositivos móviles" permiten focalizar la implementación en entornos específicos, algo que antes requería más interpretación.

Impacto para empresas ya certificadas en 2013

¿Qué implica la transición?

Revisión y actualización de la SoA

Actualizar la Declaración de Aplicabilidad para incorporar los nuevos controles.

Actualizar el análisis de riesgos

Considerar las amenazas asociadas a tecnologías emergentes.

Formación específica

Capacitar a los equipos IT y de seguridad en los nuevos controles.

Adaptación documental

Alinear procedimientos, políticas y registros con la nueva estructura.

Plazos

La ISO permite un periodo de transición de 3 años desde la publicación, por lo que las empresas tienen hasta octubre de 2025 para adaptarse si quieren mantener la certificación.

Ventajas de la versión 2022

Adaptación a la realidad actual

Incluye controles para entornos cloud, teletrabajo y ciberamenazas modernas.

Simplicidad y claridad

Menos controles, mejor organizados.

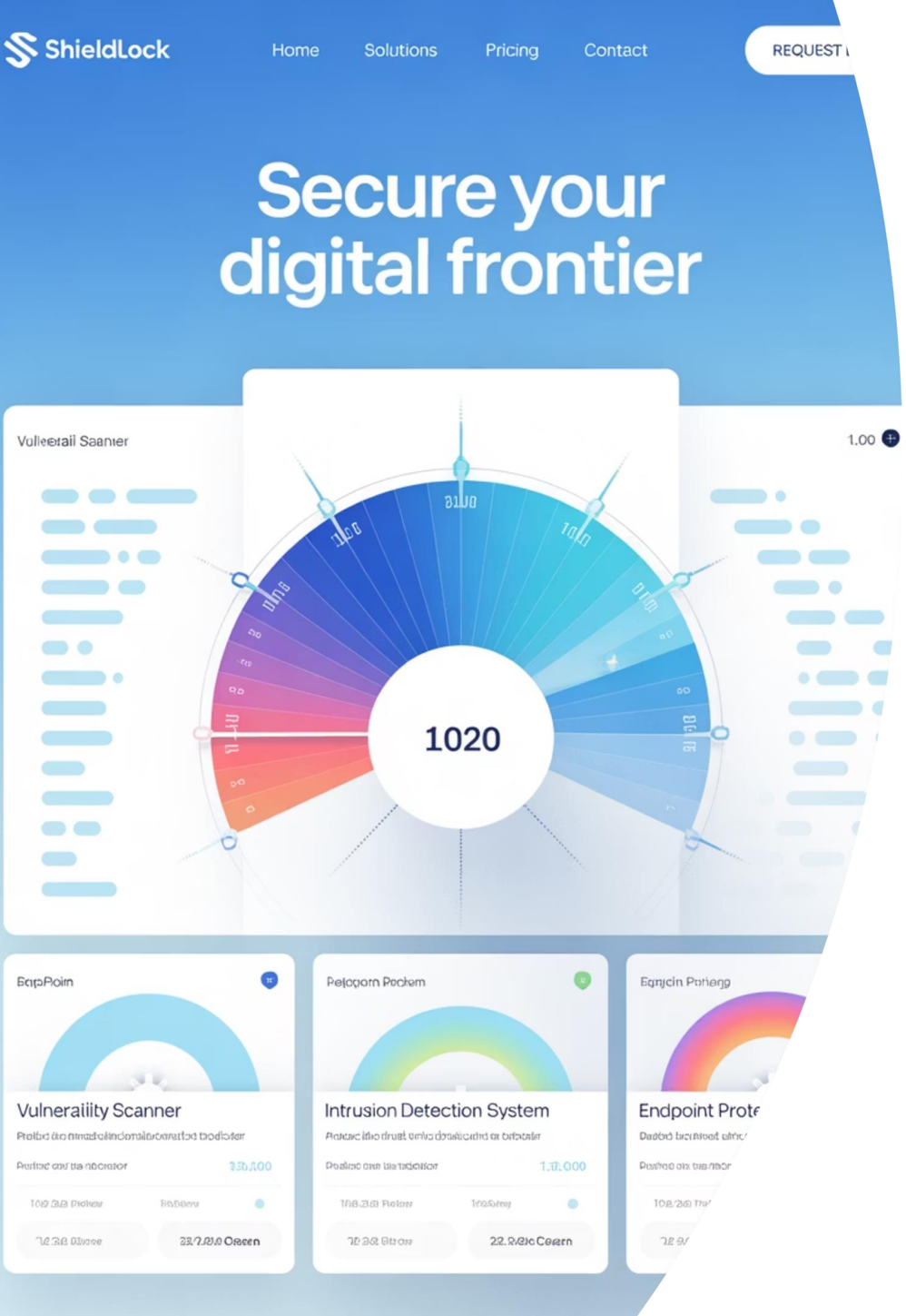
Enfoque en la mejora continua

Facilita integrar el SGSI con otros sistemas de gestión ISO.

Recomendación Nimbus

Desde Nimbus Tech, recomendamos a todas las empresas:

- Realizar un gap analysis para identificar las diferencias entre su SGSI actual y la versión 2022.
- Incorporar herramientas tecnológicas que permitan cumplir con los nuevos controles de manera eficiente.
- Aprovechar la actualización para reforzar la cultura de la seguridad en toda la organización.



Herramientas tecnológicas recomendadas por control

Una implantación eficaz de la ISO 27001:2022 no solo depende de la correcta interpretación de los controles, sino también de apoyarse en herramientas tecnológicas que faciliten su cumplimiento. A continuación, detallamos las herramientas más recomendadas agrupadas por cada tipo de control, basadas en nuestra experiencia en proyectos con clientes de diferentes sectores.

nimbus TECH

Controles organizativos

Gestión de políticas y cumplimiento

Confluence / SharePoint

Para documentar y gestionar políticas y procedimientos.

PowerDMS

Plataforma especializada en la gestión documental y control de versiones en políticas.

Gestión de riesgos y control de proveedores

Gestión de riesgos

Risk Management Studio

Software especializado para identificar, evaluar y tratar riesgos.

ISMS.online

Plataforma todo en uno para gestionar el SGSI, incluyendo el módulo de riesgos.

Control de proveedores

Prevalent / OneTrust Vendor Risk

Soluciones para evaluar y monitorizar riesgos de terceros.

Controles centrados en personas

Formación y concienciación

KnowBe4

Plataforma para formación en ciberseguridad y simulaciones de phishing.

Terranova Security

Especializada en concienciación y evaluación del nivel de ciberhigiene de los empleados.

nimbus TECH

Gestión de identidades y accesos

Okta / Azure AD

Para la gestión de identidades, accesos y políticas de single sign-on (SSO).

1Password / LastPass

Gestores de contraseñas corporativas con control centralizado.

Controles físicos

Control de accesos físicos

Genetec Security Center

Solución integral para la gestión de accesos físicos y videovigilancia.

Paxton Net2

Control de accesos por tarjeta, biometría o móvil.

Continuidad operativa y controles tecnológicos

Continuidad operativa y recuperación

Veeam Backup & Replication

Para copias de seguridad fiables y recuperación ante desastres.

Zerto

Especializada en continuidad de negocio y replicación de entornos críticos.

Control de accesos y protección

Duo Security

Doble factor de autenticación adaptable.

CyberArk

Gestión de accesos privilegiados.

Seguridad en la configuración y cifrado

Seguridad en la configuración

CIS-CAT

Herramienta gratuita para verificar configuraciones alineadas con los benchmarks CIS.

Chef InSpec / Ansible

Automatización de la configuración segura en infraestructuras.

Cifrado de la información

VeraCrypt / BitLocker

Para cifrado de discos y dispositivos.

AWS KMS / Azure Key Vault

Para la gestión de claves en entornos cloud.

Monitorización y desarrollo seguro

Monitorización y respuesta

Splunk / IBM QRadar / Elastic SIEM

Para la recolección de logs, correlación de eventos y respuesta ante incidentes.

AlienVault USM

Solución unificada para detección de amenazas y gestión de vulnerabilidades.

Seguridad en el desarrollo (DevSecOps)

Snyk / SonarQube

Detección de vulnerabilidades en el código durante el desarrollo.

GitLab CI/CD con escaneos integrados

Seguridad embebida en pipelines de desarrollo.

Prevención de fugas y herramientas transversales

Prevención de fugas de información

Symantec DLP / Forcepoint DLP

Soluciones de prevención de fuga de datos.

Herramientas transversales de apoyo al SGSI

ServiceNow GRC

Para la gestión integrada de riesgos y cumplimiento.

MetricStream

Plataforma completa de gobierno, riesgo y cumplimiento.

Power BI / Tableau

Creación de dashboards personalizados para KPIs de seguridad.

Recomendación Nimbus

Seleccionar herramientas no debe ser un proceso improvisado. En Nimbus Tech recomendamos:

Análisis de requisitos

Analizar primero los requisitos del negocio y los riesgos detectados.

Integración

Escoger herramientas que se integren fácilmente con el ecosistema tecnológico existente.

Formación

Formar al personal no solo en el uso de estas herramientas, sino en el propósito detrás de cada control.

8. KPIs e indicadores clave para evaluar tu SGSI

Una vez implementado un SGSI conforme a la ISO 27001:2022, es imprescindible medir su eficacia de forma periódica. No basta con tener controles activos: la dirección debe contar con datos objetivos que evidencien si las medidas implantadas están funcionando o si es necesario optimizar algún aspecto.

En este apartado, recopilamos los principales indicadores clave de rendimiento (KPIs) que recomendamos monitorizar desde Nimbus Tech, agrupados por dimensiones del SGSI.

KPIs por dimensión del SGSI

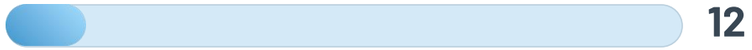
1. Gestión de riesgos

Riesgos tratados

% de riesgos identificados tratados: Proporción de riesgos detectados que ya cuentan con un plan de tratamiento.

Riesgos mitigados vs aceptados

Ayuda a entender el nivel de exposición residual.



Tiempo de actualización

Tiempo medio de actualización del análisis de riesgos: Lo ideal es revisar y actualizar el análisis al menos una vez al año o tras cambios significativos.

KPIs por dimensión del SGSI (continuación)

2. Controles de seguridad implantados

- % de controles implementados sobre el total definido en la Declaración de Aplicabilidad (SoA
- % de controles con revisiones actualizadas: Indica si los controles se mantienen vigentes y ad

3. Concienciación y formación

- % de empleados formados en seguridad de la información en el último año.
- Tasa de éxito en simulaciones de phishing: Mide el nivel de concienciación práctica.
- Número de sesiones formativas realizadas vs planificadas.

4. Gestión de accesos e identidades

- % de cuentas inactivas deshabilitadas en menos de 48 horas tras la salida de un empleado.
- Proporción de accesos con doble factor de autenticación activo.

5. Ciberseguridad y protección tecnológica

12

Incidentes trimestrales

Número de incidentes de seguridad detectados por trimestre.

4h

MTTD

Tiempo medio de detección de incidentes.

8h

MTTR

Tiempo medio de respuesta a incidentes.

95%

Endpoints protegidos

% de endpoints protegidos con soluciones EDR.

90%

Parches aplicados

% de sistemas con parches de seguridad aplicados dentro de los plazos recomendados.

KPIs de continuidad y cumplimiento

6. Continuidad de negocio

Tiempo estimado de recuperación (RTO)

Frente a incidentes críticos.

% de simulacros realizados

Según planificación.

Resultado de simulacros

Cumplimiento o no del RTO y RPO definidos.

7. Cumplimiento normativo y auditorías

No conformidades

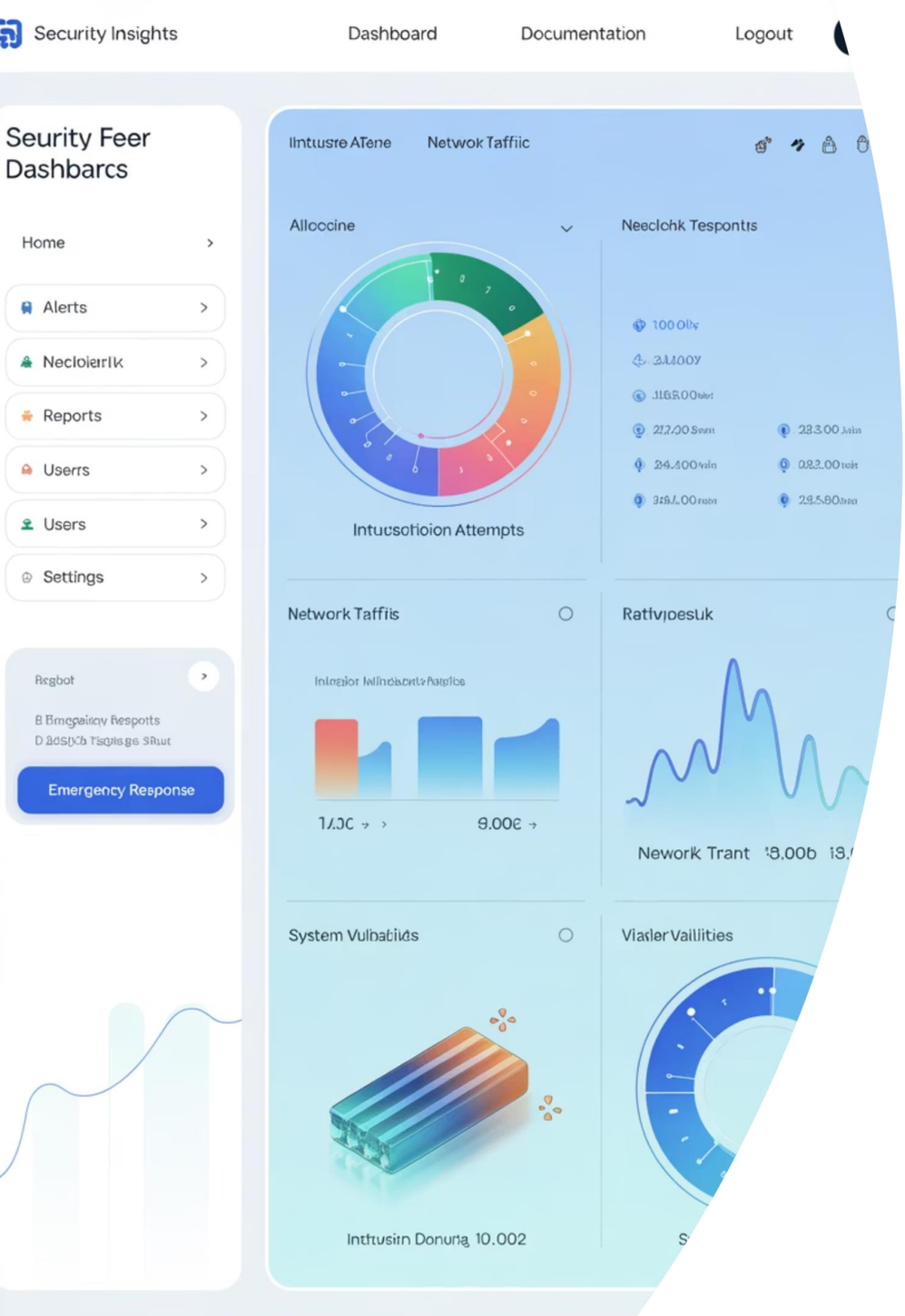
Número de no conformidades detectadas en auditorías internas.

Acciones correctivas

% de acciones correctivas cerradas dentro de los plazos comprometidos.

Resultado de auditorías externas

Número de no conformidades y observaciones.



Herramientas para monitorizar KPIs del SGSI

Power BI / Tableau

Para la creación de dashboards visuales que integren métricas clave.

ServiceNow GRC

Para la gestión integral de indicadores asociados a riesgos y cumplimiento.

MetricStream

Ideal para consolidar KPIs de seguridad, cumplimiento y auditoría.

nimbus TECH

Recomendación Nimbus

No todos los KPIs aplican por igual a todas las organizaciones. Lo importante es:

Cuadro de mando adaptado

Definir un cuadro de mando adaptado a la realidad y objetivos del negocio.

Revisión periódica

Revisar periódicamente los indicadores para evitar que se conviertan en métricas sin propósito.

Implicación directiva

Implicar a la dirección en la revisión de resultados y toma de decisiones basadas en datos.

9. Errores frecuentes al implantar y mantener un SGSI (y cómo evitarlos)

La implantación de un SGSI conforme a la ISO 27001 es un proceso que exige rigor y compromiso. Sin embargo, en Nimbus Tech hemos detectado que muchas empresas —incluso algunas certificadas— caen en errores recurrentes que comprometen la eficacia real del sistema y su sostenibilidad en el tiempo.

En este apartado, recopilamos los errores más comunes que hemos observado en proyectos de implantación o auditoría, junto a recomendaciones prácticas para evitarlos.

1. Enfocar la ISO 27001 solo como un trámite para la certificación

Error:

Implantar el SGSI únicamente para obtener el certificado, sin integrarlo realmente en la operativa y cultura de la empresa.

Consecuencia:

El sistema se convierte en una burocracia ineficiente que no protege realmente la información.

Cómo evitarlo:

- Integrar el SGSI con los procesos de negocio.
- Alinear los objetivos de seguridad con los estratégicos de la organización.
- Involucrar a la dirección y a todos los niveles de la empresa desde el principio.

2. No realizar un buen análisis de riesgos

Error:

Hacer un análisis de riesgos superficial o genérico, sin adaptarlo al contexto específico de la empresa.

Consecuencia:

Los controles seleccionados no están alineados con los riesgos reales, dejando desprotegidos activos críticos.

Cómo evitarlo:

- Utilizar metodologías reconocidas (MAGERIT, ISO 31000).
- Incluir a responsables de negocio en la identificación de riesgos.
- Revisar el análisis de riesgos tras cada cambio significativo en la organización.

3. Implementar controles sin definir indicadores de eficacia

Error:

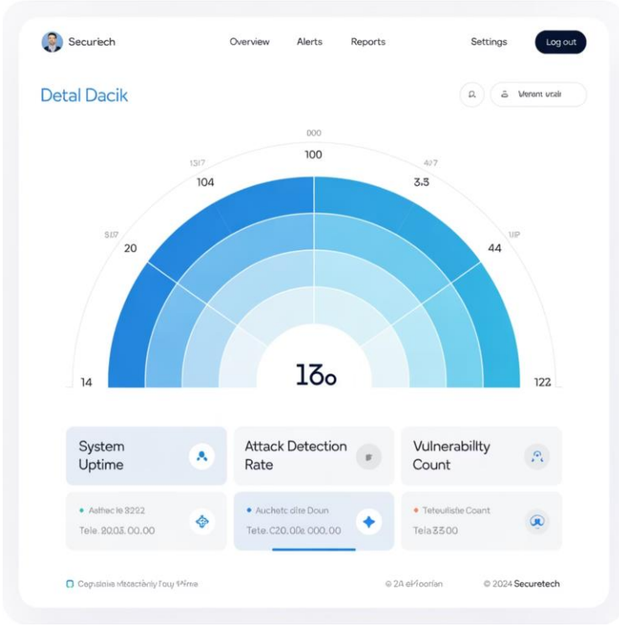
Activar controles de seguridad sin establecer cómo se va a medir si funcionan correctamente.

Consecuencia:

Es imposible demostrar la eficacia del SGSI o detectar áreas de mejora.

Cómo evitarlo:

- Asociar cada control a un KPI o métrica de seguimiento.
- Incorporar estos indicadores en el cuadro de mando de la empresa.



4. Descuidar la formación y la concienciación del personal

Error:

Pensar que con una formación inicial es suficiente o limitar la formación a perfiles técnicos.

Consecuencia:

Los empleados no son conscientes de su papel en la seguridad de la información y se convierten en el eslabón débil.

Cómo evitarlo:

- Establecer un plan de formación y concienciación recurrente para toda la plantilla.
- Realizar simulacros periódicos de phishing y otras amenazas.

5. No mantener actualizado el SGSI

Error:

Implantar el SGSI y dejar de revisarlo, actualizando solo cuando se acerca la auditoría externa.

Consecuencia:

El sistema se desactualiza respecto a los riesgos, normativas y la propia evolución de la empresa.

Cómo evitarlo:

- Aplicar el ciclo PDCA (Planificar, Hacer, Verificar, Actuar) de forma constante.
- Revisar políticas, procedimientos y controles al menos una vez al año.

6. Ignorar la seguridad en entornos cloud y remoto

Error:

Basar el SGSI en un enfoque tradicional sin contemplar las particularidades de entornos cloud, SaaS o teletrabajo.

Consecuencia:

Brechas de seguridad en entornos críticos no controlados.

Cómo evitarlo:

- Incluir controles específicos para la seguridad en la nube y el teletrabajo.
- Monitorizar configuraciones cloud con herramientas específicas.

7. No contar con un plan realista de continuidad de negocio

Error:

Disponer de un plan de continuidad solo sobre el papel, sin haberlo probado.

Consecuencia:

En caso de incidente, la empresa no sabe cómo responder realmente.

Cómo evitarlo:

- Realizar simulacros de recuperación al menos una vez al año.
- Validar que los tiempos de recuperación (RTO, RPO) son viables.

8. Falta de implicación de la dirección

Error:

Delegar el SGSI exclusivamente en el departamento de IT o Seguridad.

Consecuencia:

Falta de recursos, apoyo o integración en la estrategia global.

Cómo evitarlo:

- Incluir la revisión del SGSI en las reuniones de dirección.
- Asociar la seguridad de la información con indicadores estratégicos del negocio.

10. Cómo una empresa IT como Nimbus Tech puede ayudarte a implementar, mantener y optimizar un SGSI

En Nimbus Tech no solo implementamos Sistemas de Gestión de la Seguridad de la Información (SGSI) basados en ISO 27001:2022. Acompañamos a cada empresa en todo el ciclo de vida de la seguridad, con un enfoque práctico, adaptado al negocio y orientado a resultados reales, no solo a la certificación.

Cómo podemos ayudarte

A continuación te explicamos cómo podemos ayudarte en cada fase clave y qué valor añadido ofrecemos.

1. Diagnóstico y análisis de madurez

Antes de empezar cualquier implantación, realizamos un diagnóstico de madurez en seguridad de la información, donde analizamos:

- El grado de cumplimiento actual respecto a ISO 27001.
- Los riesgos críticos específicos del sector y del modelo de negocio.
- La cultura organizacional en torno a la seguridad.

Beneficios del diagnóstico y diseño

¿Qué obtiene la empresa?

Informe detallado

Un informe detallado con el nivel de madurez.

Roadmap estratégico

Un roadmap estratégico personalizado para alcanzar la certificación o reforzar la seguridad.

2. Diseño del SGSI adaptado al negocio

Cada empresa es única, y así debe ser su SGSI. Por eso:

- Definimos el alcance más eficiente, evitando sobrecargar el sistema con áreas que no aportan valor.
- Diseñamos la arquitectura documental: políticas, procedimientos, planes de formación, etc.
- Asesoramos en la selección de controles adecuados y en la elaboración de la Declaración de Aplicabilidad (SoA).

3. Implantación técnica de controles

Contamos con un equipo especializado en ciberseguridad que se encarga de:

Implementación de controles

Implementar controles técnicos como MFA, cifrado, EDR, SIEM, DLP, etc.

Configuración de entornos

Configurar entornos cloud y on-premises bajo estándares de seguridad.

Integración de soluciones

Integrar soluciones de monitorización y respuesta ante incidentes.

Además, trabajamos con herramientas líderes y partners estratégicos en seguridad IT.

4. Formación y concienciación del personal

Diseñamos e impartimos planes de formación adaptados a cada nivel organizativo:

Directivos

Visión estratégica y toma de decisiones en seguridad.

Técnicos

Buenas prácticas, herramientas específicas.

Toda la plantilla

Cultura de seguridad, phishing, ingeniería social.

Incluimos simulacros reales y medición de la evolución en el nivel de concienciación.

nimbus TECH

5. Auditoría interna y preparación para la certificación

Ofrecemos servicios de auditoría interna previos a la certificación, con informes detallados de:

No conformidades

Identificación detallada de incumplimientos.

Oportunidades de mejora

Áreas donde se puede optimizar el sistema.

Recomendaciones

Recomendaciones para el cierre de brechas.

Esto permite llegar a la auditoría externa con un SGSI maduro, sólido y defendible.

6. Mantenimiento y mejora continua

Una vez certificado, el SGSI requiere mantenimiento. En Nimbus Tech ofrecemos:

Revisión de riesgos

Revisión periódica del análisis de riesgos.

Asesoría

Asesoría en cambios organizativos o tecnológicos que impacten en la seguridad.

Actualización

Actualización de controles frente a nuevas amenazas.

Auditorías

Auditorías internas anuales.

Para muchas empresas actuamos como su Responsable de Seguridad de la Información externo, reduciendo costes y garantizando la continuidad y mejora del SGSI.

7. Integración con otros marcos y normativas

Además de la ISO 27001, ayudamos a las empresas a integrar el SGSI con:

Esquema Nacional de Seguridad (ENS)

Cumplimiento para administraciones públicas y proveedores.

Directiva NIS2

Para operadores de servicios esenciales.

RGPD

Protección de datos personales.

Otros estándares

ISO 22301 (Continuidad de Negocio) o ISO 27701 (Privacidad).

Beneficios de trabajar con Nimbus Tech

Enfoque práctico

Soluciones adaptadas al negocio, no estándares genéricos.

Acompañamiento completo

Desde el diagnóstico hasta el mantenimiento.

Equipo multidisciplinar

Expertos en ciberseguridad, compliance, formación y auditoría.

Ahorro de costes

Optimización de recursos sin necesidad de inflar estructuras internas.

Si estás valorando implantar, actualizar o mantener un SGSI efectivo, en Nimbus Tech podemos convertirnos en tu partner estratégico en seguridad de la información.

Contáctanos y solicita tu diagnóstico inicial sin compromiso: https://nimbustech.es/contacto

11. Caso práctico: implantación y certificación ISO 27001 en una empresa española

Para comprender el valor práctico de implementar un SGSI basado en la ISO 27001, presentamos un caso representativo de éxito en una empresa española del sector tecnológico. Si bien no compartimos el nombre concreto por motivos de confidencialidad, el proceso y los resultados reflejan una realidad aplicable a muchas organizaciones que quieren profesionalizar su seguridad de la información.

Situación inicial

Se trataba de una empresa con unos 120 empleados dedicada al desarrollo de soluciones SaaS para distintos sectores, incluyendo banca, salud y administraciones públicas. Con un crecimiento sostenido y operaciones en entornos cloud, la empresa manejaba grandes volúmenes de datos sensibles tanto propios como de clientes.

Aunque disponía de prácticas básicas de seguridad (firewalls, backups, control de accesos), no existía un Sistema de Gestión formalizado ni un enfoque basado en riesgos.

Retos y necesidades detectadas

- Cumplimiento normativo: Presión creciente para cumplir el RGPD y el Esquema Nacional de Seguridad (ENS), especialmente en contratos públicos.
- Exigencias comerciales: Varias cuentas estratégicas en el sector financiero solicitaban contar con la certificación ISO 27001.
- Entornos cloud híbridos dispersos y con falta de políticas estandarizadas.
- Necesidad de gestionar la continuidad del negocio y los riesgos cibernéticos de forma estructurada.

Proceso de implantación con la ayuda de Nimbus Tech

1. Diagnóstico inicial y análisis de brechas

Se llevó a cabo un análisis de madurez para identificar:

Políticas inexistentes o incompletas

Falta de documentación formal de seguridad.

Inexistencia de un análisis de riesgos formal

Sin metodología estructurada para identificar amenazas.

Controles de seguridad aplicados de forma desigual

Inconsistencia en la implementación de medidas.

2. Definición del alcance y análisis de riesgos

2. Definición del alcance

El SGSI se aplicó a:

- La infraestructura cloud utilizada para los servicios SaaS.
- El desarrollo de software.
- Los entornos de soporte y atención al cliente.

3. Análisis de riesgos personalizado

Identificamos riesgos asociados a:

Fugas de información confidencial

Brechas en la configuración cloud

Ataques de ransomware

Incumplimientos regulatorios

4. Diseño e implantación de controles clave

Gestión de accesos con MFA

En todos los servicios críticos.

Implementación de un EDR

Para proteger estaciones y servidores.

Seguridad en el ciclo de vida del desarrollo

DevSecOps integrado en el proceso.

SIEM para monitorización centralizada

Detección y respuesta a incidentes.

Clasificación de la información

Y control documental.

5. Formación y cultura de seguridad

Se desarrolló un plan de formación periódica que incluía:

Sesiones de formación

Para todos los empleados.

Talleres específicos

Para equipos técnicos.

Simulacros y campañas

Simulacros de phishing y campañas de concienciación.

Auditoría, certificación y resultados

6. Auditoría interna y preparación

Tras la implementación de todos los controles, se realizó una auditoría interna completa, seguida de un plan de acciones correctivas y preventivas.

7. Auditoría externa y certificación

La empresa superó la auditoría de certificación sin no conformidades mayores y con varias buenas prácticas reconocidas por el auditor externo.

Resultados obtenidos

- Certificación ISO 27001:2022 conseguida en 9 meses.
- Incorporación exitosa de la seguridad en procesos internos y desarrollo.
- Mejora de la percepción de la empresa por parte de clientes estratégicos.
- Reducción significativa de incidentes de seguridad, gracias a la combinación de medidas preventivas y reactivas.
- Facilidad para cumplir con el ENS en licitaciones públicas.

Factores clave del éxito

Compromiso de la dirección

Compromiso de la dirección y de todas las áreas.

Enfoque integral

Más allá de la certificación, orientado a proteger el negocio.

Acompañamiento especializado

Acompañamiento especializado de Nimbus Tech en cada fase.

Este caso ejemplifica que la implantación de un SGSI no solo ayuda a cumplir con requisitos legales o comerciales, sino que genera una verdadera transformación interna que protege el valor estratégico de la información y fortalece la resiliencia empresarial.

12. Conclusiones y próximos pasos

La protección de la información es hoy una necesidad crítica y estratégica para cualquier empresa, especialmente aquellas que gestionan datos sensibles, operan en entornos digitales o colaboran con el sector público.

Implementar un SGSI conforme a la ISO 27001:2022 no solo permite cumplir con normativas como el RGPD, el Esquema Nacional de Seguridad (ENS) o la directiva NIS2, sino que también ayuda a:

- Reducir la exposición a ciberamenazas.
- Garantizar la continuidad del negocio ante incidentes.
- Mejorar la reputación y la confianza de clientes, socios y administraciones.

Puntos clave que debes tener en cuenta

Proceso continuo

La seguridad no es un proyecto puntual, sino un proceso de mejora continua.

Implicación directiva

La dirección debe estar involucrada para garantizar recursos y alineación con los objetivos estratégicos.

Análisis de riesgos

La selección de controles debe basarse siempre en un análisis de riesgos sólido.

Cultura y formación

La tecnología es imprescindible, pero no sustituye la necesidad de cultura y formación.

Medición de eficacia

Medir la eficacia mediante KPIs permite evolucionar el sistema y adaptarlo a nuevos riesgos.

Próximos pasos recomendados

Si aún no tienes un SGSI:

Diagnóstico

Realiza un diagnóstico de seguridad y madurez.

Plan

Define un plan de implementación escalable.

Acompañamiento

Busca acompañamiento especializado para diseñar un SGSI adaptado a tu negocio.

Si tienes un SGSI antiguo o parcial:

Actualización

Actualízalo a la versión 2022 de la norma.

Gap Analysis

Realiza un gap analysis frente a los nuevos controles.

Automatización

Incorpora herramientas que automaticen el cumplimiento y monitorización.

Si ya tienes certificado el SGSI:

Mejora continua

Asegúrate de aplicar la mejora continua: auditorías internas, actualización de riesgos y KPIs.

Formación regular

Forma regularmente a toda la plantilla.

Extensión

Valora extender el SGSI a nuevas áreas o procesos.

¿Cómo puede ayudarte Nimbus Tech?

En Nimbus Tech te ayudamos a:

Diseño e implantación

Diseñar, implantar y mantener un SGSI desde cero.

Adaptación

Adaptar tu SGSI a la versión 2022 y a las nuevas normativas.

Controles técnicos

Implementar controles técnicos con las herramientas más eficaces.

Formación

Formar a tu equipo en buenas prácticas de seguridad.

Mejora continua

Mantener la mejora continua y preparar auditorías internas.

Solicita tu diagnóstico o consulta sin compromiso en: https://nimbustech.es/contacto

Invertir en un SGSI no es solo proteger datos: es proteger tu negocio, tu reputación y tu futuro.

Desde Nimbus Tech estaremos encantados de acompañarte en ese camino.