ISO 27001:2022

La guía definitiva para certificar tu empresa sin complicaciones

nimbus TECH

ÍNDICE

1. Introducción: Por qué ISO 27001 es clave en 2025
2. Marco legal en España: ENS, NIS2, RGPD y conexión con ISO 27001
3. Cómo implementar un SGSI paso a paso
4. Checklist de fases críticas para implantar un SGSI
5. Los 93 controles explicados con ejemplos prácticos y casos reales
6. Comparativa ISO 27001:2013 vs 2022: Cambios clave y su impacto en las empresas
7. Herramientas tecnológicas recomendadas por control
8. KPIs e indicadores clave para evaluar tu SGSI
9. Errores frecuentes al implantar y mantener un SGSI (y cómo evitarlos)
10. Cómo una empresa IT como Nimbus Tech puede ayudarte a implementar, mantener y optimizar un SGSI
11. Caso práctico: implantación y certificación ISO 27001 en una empresa española
12. Conclusiones y próximos pasos

¿Por qué ISO 27001 es clave en 2025?

Un entorno de amenazas en constante evolución

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 empresarial. En 2024, el número de ciberataques a empresas españolas creció un 38% respecto al año anterior, evidenciando una tendencia preocupante.

Marco legal cada vez más exigente

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 la pauta regulatoria que las organizaciones deben seguir.

La confianza como activo diferencial

Hoy, los clientes, socios y empleados exigen garantías de que sus datos están protegidos. La ISO 27001 actúa como un pasaporte de confianza que abre puertas en concursos públicos, colaboraciones estratégicas y acuerdos comerciales internacionales.

Teletrabajo

Nuevos riesgos asociados a entornos remotos no controlados

Cloud Computing

Superficies de ataque ampliadas en entornos multicloud

Inteligencia Artificial

Vulnerabilidades emergentes en tecnologías avanzadas

La norma ISO 27001:2022 se convierte así en una herramienta estratégica indispensable, no solo como un estándar internacional reconocido, sino como una metodología probada para gestionar la seguridad de la información de forma sistemática, alineada con los riesgos reales y con los objetivos del negocio.

nimbus TECH

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

La gestión de la seguridad de la información en España se desarrolla dentro de un complejo entramado regulatorio. Entender cómo se articulan estas normativas con la ISO 27001 es fundamental para cualquier responsable de seguridad.

Esquema Nacional de Seguridad (ENS)

Marco de referencia para garantizar la protección de la información en el ámbito de las Administraciones Públicas y empresas que prestan servicios a éstas.

Conexión con ISO 27001: Comparten principios de confidencialidad, integridad y disponibilidad. Una organización certificada en ISO 27001 tiene gran parte del camino recorrido para certificar el ENS.

Directiva NIS2

Establece nuevas obligaciones para reforzar la seguridad en sectores críticos y servicios esenciales en la UE. Afecta principalmente a empresas de energía, agua, salud, banca e infraestructuras digitales.

Exigencias: Implantación de políticas de gestión de riesgos, reporte de incidentes graves en menos de 24 horas y auditorías periódicas.

Reglamento General de Protección de Datos (RGPD)

Regula el tratamiento de datos personales dentro de la UE, exigiendo evaluaciones de impacto, notificación de brechas en 72 horas y medidas técnicas y organizativas adecuadas.

Beneficio de ISO 27001: Un SGSI bien definido permite demostrar el cumplimiento del RGPD mediante políticas claras y trazabilidad documental.

Beneficios de alinear el SGSI con las regulaciones españolas y europeas

- Evitar sanciones y responsabilidades legales que pueden llegar hasta 20 millones de euros o el 4% de la facturación global anual.
- Mejorar la reputación y credibilidad frente a clientes, socios y reguladores.
- Obtener ventaja competitiva en licitaciones públicas y contratos internacionales donde se valora la certificación.
- Simplificar auditorías regulatorias y de clientes, reduciendo costes operativos.

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 significativa en su sector.

nimbus TECH

Cómo implementar un SGSI paso a paso

La implementación de un Sistema de Gestión de Seguridad de la Información requiere un enfoque estructurado y metódico. A continuación, presentamos un método en 7 fases que garantiza una implantación exitosa, independientemente del tamaño o sector de la organización.

Diagnóstico inicial y análisis de madurez

Evaluación de la situación actual respecto a la seguridad de la información, identificando fortalezas, debilidades, riesgos potenciales y nivel de concienciación de la plantilla.

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

Definición del alcance del SGSI

Determinación de qué procesos, departamentos, servicios, sistemas de información y ubicaciones físicas o virtuales quedan dentro del SGSI.

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

Análisis de riesgos y oportunidades

Identificación de amenazas y vulnerabilidades, valoración de impacto y probabilidad, determinación del nivel de riesgo y definición de acciones para tratarlos (evitar, transferir, mitigar o aceptar).

Metodologías recomendadas: MAGERIT, ISO 31000 o combinaciones personalizadas.

Política y objetivos de seguridad

Establecimiento del pilar estratégico que guiará todas las acciones del SGSI, alineado con los objetivos de negocio, expectativas de las partes interesadas y cultura corporativa.

Fijación de objetivos SMART: específicos, medibles, alcanzables, relevantes y con límite temporal.

Implementación de controles

Selección e implementación de los controles adecuados del Anexo A de la ISO 27001 en función del análisis de riesgos previo.

Ejemplos: Doble factor de autenticación, políticas de clasificación de información, restricciones de acceso, seguridad física y cifrado de datos.

Formación y concienciación

Formación del personal en prácticas seguras, concienciación sobre la importancia de proteger la información y promoción de una cultura de seguridad proactiva.

Recomendación: Implementar programas gamificados y simulaciones de phishing para mayor efectividad.

Auditoría, revisión y mejora

Siguiendo el ciclo PDCA (Plan-Do-Check-Act), realizar auditorías internas periódicas, revisiones por parte de la dirección y corrección de desviaciones para mejorar continuamente.

Este ciclo garantiza que el SGSI evoluciona con el negocio y con el entorno de amenazas.

El tiempo estimado para implantar un SGSI varía según el tamaño de la organización: 4-6 meses para pequeñas empresas, 6-9 meses para medianas y 9-12 meses o más para grandes corporaciones, dependiendo siempre del nivel de madurez previo, el alcance definido y los recursos disponibles.

Checklist de fases críticas para implantar un SGSI

Para garantizar una implantación ordenada y sin lagunas, a continuación presentamos un checklist práctico que sirve como hoja de ruta para cualquier empresa que quiera implantar un SGSI conforme a la ISO 27001:2022.

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
2. Definir el alcance	Delimitar el perímetro del SGSI	- Definir procesos, servicios y ubicaciones incluidos - Aprobación por la dirección	Documento de Alcance del SGSI
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
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
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	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
7. Documentación	Formalizar el SGSI	- Documentar procesos y procedimientos - Establecer control documental	Manual y procedimientos del SGSI actualizados
8. Auditoría interna y revisión	Verificar el sistema	- Auditorías internas - Revisión por la dirección - Acciones correctivas	Informe de auditoría interna y revisión de dirección
9. Certificación externa	Obtener el reconocimiento formal	- Selección de certificadora acreditada - Auditoría de certificación - Corrección de desviaciones	Certificado ISO 27001 obtenido (opcional)
10. Mejora continua	Evolucionar el SGSI	- Revisión periódica de riesgos - Actualización de controles - Mejoras en procesos	SGSI actualizado y adaptado al negocio

Se recomienda revisar esta tabla cada trimestre para validar que cada fase sigue vigente y alineada con la evolución de la empresa y su entorno. Esta herramienta permite también identificar posibles retrasos o áreas de mejora durante la implantación.

Los 93 controles de ISO 27001:2022 explicados

La norma ISO 27001:2022 establece 93 controles organizados en cuatro grandes categorías. Cada control es un instrumento esencial para proteger los activos de información frente a los riesgos previamente identificados.

Controles organizativos

37 controles que establecen el marco de gobierno, políticas y procedimientos.

- Política de Seguridad de la Información
- Roles y responsabilidades
- Gestión de proveedores
- Clasificación de la información

Controles tecnológicos

34 controles enfocados en proteger redes, sistemas y aplicaciones.

- Control de acceso lógico
- Cifrado de la información
- Seguridad en la configuración
- Protección contra malware

Controles centrados en personas

8 controles diseñados para mitigar riesgos derivados del factor humano.

- Concienciación y formación
- Proceso de incorporación y desvinculación
- Compromisos de confidencialidad

Controles físicos

14 controles para proteger los activos físicos y entornos.

- Control de acceso físico
- Protección contra amenazas ambientales
- Gestión segura de equipos móviles

Priorización de controles según el tipo de empresa

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
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
Despachos profesionales	Clasificación de información, control de accesos, protección frente a fugas de información, formación en ciberhigiene

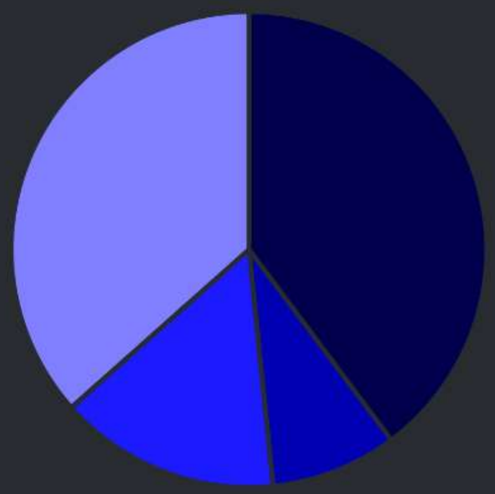
Un SGSI efectivo no depende solo de implementar controles, sino de integrarlos en la cultura y en los procesos de negocio. Solo así se garantiza la seguridad como un elemento estratégico y no como un mero cumplimiento normativo.

Comparativa ISO 27001:2013 vs 2022: Cambios clave

La actualización de la norma ISO 27001 en 2022 ha supuesto una evolución significativa que refleja la necesidad de adaptarse a un entorno digital más complejo y a las nuevas amenazas en ciberseguridad.

Reducción y reagrupación de controles

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



Este cambio no reduce la protección, sino que fusiona controles relacionados, clarifica otros y añade nuevos para abordar tecnologías y riesgos emergentes.

Controles nuevos más relevantes

Inteligencia de amenazas

Procesos para identificar y gestionar información sobre amenazas emergentes, como servicios que monitorizan fuentes OSINT y Dark Web.

Seguridad en servicios cloud

Asegurar el uso adecuado y seguro de servicios en la nube, con políticas específicas para proveedores como AWS, Azure o Google Cloud.

Prevención de fugas (DLP)

Detectar y evitar la pérdida de datos sensibles mediante soluciones específicas en correo electrónico y otros canales corporativos.

Mejora en la flexibilidad

La norma incluye ahora la atribución de controles mediante etiquetas (por ejemplo, "Cloud" o "Dispositivos móviles"), lo que facilita personalizar su aplicación según el tipo de tecnología, modelo de negocio y entorno de amenazas.

Impacto para empresas ya certificadas en 2013

Las organizaciones tienen hasta octubre de 2025 para adaptarse si quieren mantener la certificación. Esta transición implica:

- Revisión y actualización de la Declaración de Aplicabilidad (SoA) para incorporar los nuevos controles.
- Actualización del análisis de riesgos considerando las amenazas asociadas a tecnologías emergentes.
- Formación específica en los nuevos controles, especialmente para equipos IT y de seguridad.
- Adaptación documental: procedimientos, políticas y registros deben alinearse con la nueva estructura.

Se recomienda realizar un gap analysis para identificar las diferencias entre el SGSI actual y la versión 2022, incorporar herramientas tecnológicas que permitan cumplir con los nuevos controles, y aprovechar la actualización para reforzar la cultura de seguridad en toda la organización.

nimbus TECH

Herramientas tecnológicas recomendadas por control

Una implantación eficaz de ISO 27001:2022 requiere apoyarse en herramientas tecnológicas adecuadas para cada tipo de control. Estas soluciones facilitan tanto el cumplimiento como la gestión continua del SGSI.

Controles organizativos

Gestión de políticas

- Confluence / SharePoint
- PowerDMS
- PolicyKit

Gestión de riesgos

- Risk Management Studio
- ISMS.online
- eramba

Control de proveedores

- Prevalent
- OneTrust Vendor Risk
- MetricStream

Controles centrados en personas

Formación y concienciación

- KnowBe4
- Terranova Security
- Proofpoint Security Awareness

Gestión de identidades

- Okta / Azure AD
- 1Password / LastPass
- CyberArk

Controles físicos

Control de accesos físicos

- Genetec Security Center
- Paxton Net2
- Lenel OnGuard

Continuidad operativa

- Veeam Backup & Replication
- Zerto
- Acronis Cyber Protect

Controles tecnológicos

Seguridad en la configuración

- CIS-CAT
- Chef InSpec / Ansible
- Microsoft SCM

Cifrado de la información

- VeraCrypt / BitLocker
- AWS KMS / Azure Key Vault
- PGP / GPG

Monitorización y respuesta

- Splunk / IBM QRadar
- Elastic SIEM
- AlienVault USM

Herramientas transversales de apoyo al SGSI

Para una gestión integral del Sistema de Gestión de Seguridad de la Información, existen plataformas que facilitan múltiples aspectos:

- **ServiceNow GRC:** Gestión integrada de riesgos y cumplimiento con workflows automatizados.
- **MetricStream:** Plataforma completa de gobierno, riesgo y cumplimiento con gestión de políticas.
- **Power BI / Tableau:** Creación de dashboards personalizados para KPIs de seguridad y visualización de datos.
- **Microsoft Compliance Manager:** Gestión del cumplimiento normativo integrado con Microsoft 365.

La selección de herramientas debe realizarse tras analizar los requisitos específicos del negocio y los riesgos detectados, priorizando aquellas que se integren fácilmente con el ecosistema tecnológico existente y asegurando la formación adecuada del personal.

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. Los siguientes indicadores clave de rendimiento (KPIs) permiten evaluar objetivamente el funcionamiento del sistema.

95%

Riesgos tratados

Porcentaje óptimo de riesgos identificados que deben contar con un plan de tratamiento definido.

100%

Controles implementados

Objetivo para los controles definidos en la Declaración de Aplicabilidad que deben estar activos.

90%

Personal formado

Porcentaje mínimo de empleados que deben recibir formación en seguridad anualmente.

2h

Tiempo de respuesta

Objetivo de tiempo medio máximo para responder a incidentes de seguridad críticos.

Dimensiones principales para evaluar un SGSI

Gestión de riesgos

- % de riesgos identificados tratados
- % de riesgos mitigados vs aceptados
- Tiempo medio de actualización del análisis de riesgos

Controles de seguridad

- % de controles implementados sobre el total definido
- % de controles con revisiones actualizadas
- Número de vulnerabilidades detectadas por control

Concienciación y formación

- % de empleados formados en seguridad
- Tasa de éxito en simulaciones de phishing
- Número de sesiones formativas realizadas

Gestión de accesos

- % de cuentas inactivas deshabilitadas rápidamente
- Proporción de accesos con MFA activo
- Número de intentos de acceso no autorizados

Ciberseguridad

- Número de incidentes detectados por trimestre
- Tiempo medio de detección (MTTD)
- Tiempo medio de respuesta (MTTR)
- % de endpoints protegidos con EDR

Continuidad de negocio

- Tiempo estimado de recuperación (RTO)
- % de simulacros realizados según planificación
- Resultado de simulacros vs objetivos

Herramientas para monitorizar KPIs

Para una visualización efectiva y seguimiento de estos indicadores, se recomiendan soluciones como:

- **Power BI / Tableau:** Dashboards visuales que integren métricas clave con alertas automáticas.
- **ServiceNow GRC:** Gestión integral de indicadores asociados a riesgos y cumplimiento.
- **MetricStream:** Consolidación de KPIs de seguridad, cumplimiento y auditoría.
- **Microsoft 365 Compliance Manager:** Medición integrada del cumplimiento en entornos Microsoft.

Es importante adaptar estos indicadores a la realidad y objetivos específicos de cada organización, revisarlos periódicamente para evitar que se conviertan en métricas sin propósito, e implicar a la dirección en la revisión de resultados y toma de decisiones basadas en estos datos.

nimbus TECH

Errores frecuentes y cómo evitarlos

La implantación de un SGSI conforme a ISO 27001 es un proceso que exige rigor y compromiso. Sin embargo, muchas organizaciones caen en errores recurrentes que comprometen su eficacia real. Identificar estos fallos comunes nos permite prevenirlos desde el principio.

1

Enfoque centrado solo en la certificación

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

Solución: Integrar el SGSI con los procesos de negocio y alinear los objetivos de seguridad con los estratégicos de la organización, implicando a todos los niveles desde el principio.

2

Análisis de riesgos superficial

Error: Realizar un análisis genérico, sin adaptarlo al contexto específico de la empresa, dejando desprotegidos activos críticos.

Solución: Utilizar metodologías reconocidas (MAGERIT, ISO 31000), incluir a responsables de negocio en la identificación y revisar el análisis tras cada cambio significativo.

3

Controles sin indicadores de eficacia

Error: Implementar controles de seguridad sin establecer cómo se medirá si funcionan correctamente.

Solución: Asociar cada control a un KPI o métrica de seguimiento e incorporar estos indicadores en el cuadro de mando de la empresa para su revisión periódica.

1

Descuido en formación del personal

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

Solución: Establecer un plan de formación recurrente para toda la plantilla y realizar simulacros periódicos de phishing y otras amenazas para mantener la concienciación.

2

SGSI desactualizado

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

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

3

Falta de implicación directiva

Error: Delegar el SGSI exclusivamente en el departamento de IT o Seguridad, sin apoyo de la dirección.

Solución: Incluir la revisión del SGSI en las reuniones directivas y asociar la seguridad de la información con indicadores estratégicos del negocio para demostrar su valor.

Un enfoque adecuado debe considerar la seguridad de la información como un proceso continuo integrado en toda la organización, no como un proyecto puntual o una carga burocrática. La participación de la dirección es clave para asignar recursos adecuados y promover una cultura de seguridad efectiva.

Revisar periódicamente el SGSI con un enfoque crítico y constructivo permitirá identificar aspectos de mejora antes de que estos se conviertan en vulnerabilidades o incumplimientos significativos.

nimbus TECH

Cómo Nimbus Tech puede ayudarte con tu SGSI

Diagnóstico y análisis de madurez

Evaluamos el grado de cumplimiento actual respecto a ISO 27001, los riesgos críticos específicos del sector y la cultura organizacional en seguridad.

Mantenimiento y mejora

Ofrecemos revisión periódica de riesgos, actualización de controles frente a nuevas amenazas y asesoría en cambios organizativos o tecnológicos.

Auditoría interna

Realizamos auditorías previas a la certificación, con informes detallados de no conformidades y recomendaciones para el cierre de brechas.

Diseño del SGSI adaptado

Definimos el alcance más eficiente, diseñamos la arquitectura documental y asesoramos en la selección de controles adecuados para la Declaración de Aplicabilidad.

Implantación técnica

Implementamos controles como MFA, cifrado, EDR, SIEM y DLP, configuramos entornos seguros e integramos soluciones de monitorización.

Formación y concienciación

Diseñamos planes de formación adaptados a cada nivel: directivos, técnicos y toda la plantilla, incluyendo simulacros de phishing.

En Nimbus Tech ofrecemos un enfoque práctico con soluciones adaptadas al negocio, no estándares genéricos, con un equipo multidisciplinar de expertos en ciberseguridad, compliance, formación y auditoría.

nimbus TECH

Caso práctico: Implantación ISO 27001 en empresa española

Situación inicial

- Empresa SaaS con 120 empleados
- Clientes en banca, salud y administraciones públicas
- Manejo de datos sensibles en entornos cloud
- Prácticas básicas de seguridad sin sistema formalizado

Retos detectados

- Presión para cumplir RGPD y ENS
- Clientes financieros exigiendo certificación
- Entornos cloud dispersos sin políticas estandarizadas
- Necesidad de gestionar continuidad y riesgos

El diagnóstico inicial reveló políticas incompletas, ausencia de análisis de riesgos formal y controles aplicados de forma desigual, lo que requería un enfoque estructurado para la implementación del SGSI.

nimbus TECH

Proceso de implantación en el caso práctico

Definición del alcance

Se aplicó el SGSI a la infraestructura cloud para servicios SaaS, desarrollo de software y entornos de soporte y atención al cliente.

Análisis de riesgos personalizado

Identificamos riesgos asociados a fugas de información, brechas en configuración cloud, ataques de ransomware e incumplimientos regulatorios.

Implementación de controles clave

MFA en servicios críticos, EDR para protección de endpoints, DevSecOps, SIEM para monitorización centralizada y clasificación de información.

Formación y cultura de seguridad

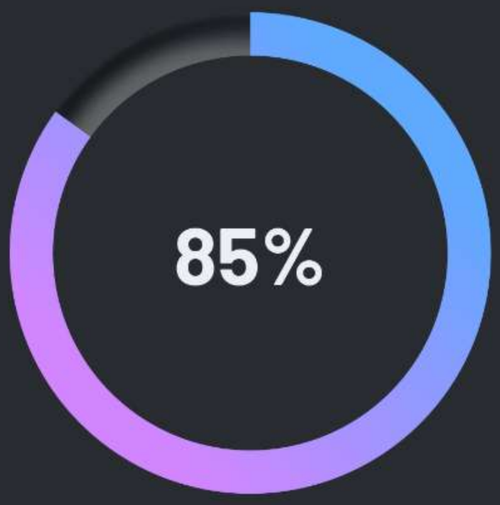
Sesiones para todos los empleados, talleres técnicos específicos y simulacros de phishing periódicos.

Auditoría y certificación

Auditoría interna completa seguida de acciones correctivas y certificación externa sin no conformidades mayores.

Meses para certificación

Tiempo total para conseguir la certificación ISO 27001:2022



Reducción de incidentes

Disminución significativa de incidentes de seguridad tras implementación

Cumplimiento ENS

Facilidad para cumplir requisitos en licitaciones públicas

nimbus TECH

Conclusiones y próximos pasos

Puntos clave

La seguridad no es un proyecto puntual, sino un proceso de mejora continua que requiere atención constante.

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

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

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

Beneficios estratégicos

- Reducción de la exposición a ciberamenazas
- Garantía de continuidad del negocio ante incidentes
- Mejora de la reputación y confianza
- Cumplimiento de RGPD, ENS y directiva NIS2
- Protección del valor estratégico de la información
- Fortalecimiento de la resiliencia empresarial

nimbus TECH

Recomendaciones según su situación actual

1	2	3
Si aún no tiene un SGSI	**Si tiene un SGSI antiguo o parcial**	**Si ya tiene certificado el SGSI**
• Realice un diagnóstico de seguridad y madurez • Defina un plan de implementación escalable • Busque acompañamiento especializado para diseñar un SGSI adaptado a su negocio	• Actualícelo a la versión 2022 de la norma • Realice un gap analysis frente a los nuevos controles • Incorpore herramientas que automaticen el cumplimiento y monitorización	• Asegúrese de aplicar la mejora continua: auditorías internas, actualización de riesgos y KPIs • Forme regularmente a toda la plantilla • Valore extender el SGSI a nuevas áreas o procesos

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

Solicite su diagnóstico o consulta sin compromiso en: https://nimbustech.es/contacto

nimbus TECH