Sistemas de gestión de seguridad: SGSI, ISO/IEC 27001 e ISO 28000

1 La seguridad como problema de gestión

La seguridad en los sistemas de información no se resuelve comprando tecnología, instalando un antivirus o colocando cámaras. Requiere definir políticas, asignar responsabilidades, diseñar procesos, establecer controles, medir resultados, auditar cumplimiento y mejorar continuamente.

Esta es la lógica que subyace a las normas ISO/IEC 27001 e ISO 28000: **la seguridad debe administrarse como parte del sistema organizacional**, con el mismo rigor con que se administran las finanzas, los recursos humanos o la logística.

Ambas normas son complementarias; no son opuestas ni redundantes. Cada una protege un plano diferente de la organización, y en las organizaciones modernas esos planos están profundamente conectados:

- **ISO/IEC 27001** protege la información que permite operar y decidir.
- **ISO 28000** protege los procesos y flujos que permiten que la organización siga funcionando.

Un ataque informático puede detener una cadena de suministro; una falla en la cadena de suministro puede comprometer información crítica. Gestionar solo uno de los dos planos deja expuesto al otro.

2 Fundamentos de la seguridad de la información

2.1 El SGSI como sistema de gestión, no como herramienta

Un **Sistema de Gestión de Seguridad de la Información (SGSI)** es el conjunto organizado de políticas, procesos, roles, controles, documentos, evidencias, auditorías y

acciones de mejora que una organización utiliza para proteger su información. En inglés se denomina **ISMS** (*Information Security Management System*).

La palabra **gestión** es decisiva. Un SGSI no equivale a comprar software de seguridad ni a instalar un firewall. Un antivirus, una política de contraseñas o un sistema de copias de respaldo pueden ser controles útiles, pero no constituyen un SGSI si no existe un método para identificar riesgos, aprobar accesos, revisar resultados y conservar evidencias.

Ejemplo concreto: una empresa puede exigir contraseñas complejas, pero si no tiene un procedimiento para dar de baja usuarios cuando termina su relación laboral, mantiene un riesgo relevante. El SGSI debe indicar quién informa la baja, quién desactiva la cuenta, en qué plazo, qué registro queda y cómo se verifica el cumplimiento.

La pregunta central no es si una organización "tiene seguridad", sino si puede **demostrar que la gestiona** con criterios claros, evidencia suficiente y decisiones consistentes con sus riesgos.

2.2 La tríada CIA

La seguridad de la información se estructura alrededor de tres principios conocidos como la tríada **CIA** (*Confidentiality, Integrity and Availability*):

Principio	En inglés	Qué protege	Ejemplo de incumplimiento
Confidencialidad	Confidentiality	Que la información solo sea accedida por personas o sistemas autorizados	Un empleado sin permiso consulta legajos salariales
Integridad	Integrity	Que los datos sean exactos, completos	Se modifica el CBU de un proveedor sin doble aprobación

Principio	En inglés	Qué protege	Ejemplo de incumplimiento
		y no alterados indebidamente	
Disponibilidad	Availability	Que sistemas y datos estén accesibles cuando los procesos legítimos los necesitan	El sistema de facturación cae en plena jornada comercial sin plan de contingencia

Las consecuencias de no preservar cada principio son concretas:

- Sin **confidencialidad**: pérdida de confianza, incumplimiento normativo, exposición de datos de clientes o fórmulas comerciales.
- Sin **integridad**: decisiones tomadas sobre datos incorrectos, errores contables, fraudes no detectados.
- Sin **disponibilidad**: imposibilidad de facturar, cobrar, atender clientes o cumplir obligaciones.

Un mismo incidente puede afectar una, dos o las tres dimensiones simultáneamente.

3 ISO/IEC 27001 — Seguridad de la información

3.1 Qué es y qué protege

ISO/IEC 27001 es una norma internacional que establece los requisitos para crear, implementar, mantener y mejorar un SGSI. Su versión vigente es ISO/IEC 27001:2022. Su propósito es que la organización identifique sus activos de información, analice los riesgos que los afectan, seleccione controles adecuados, mida su eficacia y mejore continuamente su gestión de seguridad.

La norma protege la información en cualquier formato:

Tipo de activo de información	Ejemplos
Datos digitales	Bases de datos, registros contables, correos electrónicos, archivos en la nube
Documentos	Contratos, expedientes, facturas, órdenes de compra
Sistemas y aplicaciones	ERP, CRM, plataformas SaaS, sistemas de facturación
Credenciales y accesos	Usuarios, contraseñas, certificados digitales, claves de API
Información estratégica	Listas de clientes, precios, fórmulas, reportes gerenciales
Código fuente	Software desarrollado por la organización
Respaldos	Copias de seguridad de datos y configuraciones

Su aplicación no se limita al área de TI: la información circula por procesos administrativos, comerciales, financieros, jurídicos, operativos y logísticos. El área técnica tiene un rol central, pero la seguridad requiere compromiso de la dirección, presupuesto, capacitación, control interno y responsabilidad de todos los usuarios.

Su enfoque es **basado en riesgos** (*risk-based approach*): no indica una única forma de proteger todos los sistemas ni exige que todas las organizaciones apliquen los mismos controles con igual intensidad. Una institución educativa, una fábrica y una empresa de servicios digitales tienen activos, amenazas y obligaciones distintas.

3.2 La estructura de la norma

Los requisitos de ISO/IEC 27001 se organizan en siete bloques:

Bloque	Contenido principal
Contexto	Comprensión de la organización y sus partes interesadas
Liderazgo	Compromiso de la alta dirección, política y roles
Planificación	Evaluación y tratamiento de riesgos, objetivos
Soporte	Recursos, competencia, conciencia, comunicación, documentación
Operación	Ejecución de procesos y controles planificados
Evaluación del desempeño	Indicadores, auditoría interna, revisión por la dirección
Mejora	No conformidades, acciones correctivas, mejora continua

3.3 El Anexo A: 93 controles en cuatro categorías

La norma incluye un Anexo A con 93 controles de referencia agrupados en cuatro categorías. Esta clasificación muestra que la seguridad no es solo técnica:

Categoría	Ejemplos de controles
Organizacionales	Política de seguridad, gestión de activos, clasificación de información, gestión de proveedores, respuesta ante incidentes

Categoría	Ejemplos de controles
Personas	Capacitación, concienciación, responsabilidades del personal, proceso de desvinculación
Físicos	Control de acceso a instalaciones, protección de equipos, escritorio limpio, destrucción segura
Tecnológicos	Autenticación, control de acceso lógico, cifrado, registro de eventos, gestión de parches, backups

Un SGSI no exige aplicar los 93 controles. Exige **justificar** cuáles aplican, cuáles no y por qué, mediante la Declaración de Aplicabilidad.

3.4 Definición del sistema: alcance, contexto y partes interesadas

3.4.1 Alcance

El **alcance** (*scope*) define los límites del SGSI: qué áreas, procesos, servicios, sedes, activos, tecnologías, datos y relaciones quedan incluidos. Es una decisión crítica porque determina qué se audita, qué se controla y qué se declara bajo gestión.

El alcance debe ser claro, justificable y considerar las **interfaces**: si un proceso incluido depende de un proveedor, una nube o un servicio compartido, esa dependencia debe identificarse. No debe dejar fuera elementos críticos necesarios para operar el proceso incluido.

Ejemplo: "El SGSI comprende los procesos de administración, soporte y operación de la plataforma de gestión de estudiantes, incluyendo servidores, bases de datos, usuarios internos, proveedores de infraestructura y procedimientos de respaldo."

3.4.2 Contexto de la organización

El contexto comprende los factores que pueden afectar el SGSI y la seguridad de la información:

Factores internos	Factores externos
Estructura y cultura de control	Regulación y obligaciones legales
Recursos, sistemas y procesos críticos	Clientes, contratos y expectativas
Competencias del personal	Amenazas digitales del entorno
Sedes, tecnología y madurez	Proveedores críticos y dependencias

Por qué importa: dos organizaciones pueden usar sistemas similares pero tener riesgos distintos. Una organización con trabajo remoto, plataformas cloud y múltiples proveedores tiene un perfil de riesgo muy diferente de una con operación presencial y sistemas internos simples.

El análisis de contexto debe documentarse y **revisarse ante cambios**: nuevas plataformas, tercerización, migración a la nube o cambios regulatorios pueden modificar riesgos y controles.

3.4.3 Partes interesadas

Las **partes interesadas** (*interested parties*) son quienes pueden afectar al SGSI, verse afectadas por él o tener requisitos relacionados con la seguridad:

Parte interesada	Necesidad o requisito típico
Clientes	Confidencialidad de sus datos y notificación de incidentes en plazo definido
Empleados	Protección de legajos, datos salariales y comunicaciones internas

Parte interesada	Necesidad o requisito típico
Proveedores	Accesos limitados, cuentas individuales y condiciones contractuales claras
Organismos reguladores	Protección de datos personales, conservación documental, reporte de incidentes
Alta dirección	Continuidad del servicio, reportes ejecutivos de riesgo y resultados auditables

Un contrato puede exigir cifrado, registros de auditoría o tiempos máximos de respuesta. Esos requisitos deben incorporarse al SGSI con procedimientos y evidencias.

3.5 Liderazgo, política y responsabilidades

3.5.1 Liderazgo y compromiso de la alta dirección

Un SGSI requiere liderazgo real. La alta dirección debe:

Acción	Qué implica
Aprobar la política de seguridad	Compromiso formal en el nivel más alto
Asignar recursos	Presupuesto, personal, herramientas y tiempo
Definir responsabilidades	Quién responde por cada control
Resolver conflictos entre seguridad y operación	Aceptar o rechazar riesgos formalmente
Revisar resultados del SGSI	Reuniones con indicadores y decisiones documentadas

Si la dirección solo toma nota de los problemas sin decidir, el SGSI pierde eficacia.

3.5.2 Política de seguridad de la información

La política de seguridad es una declaración formal de alto nivel. Debe orientar decisiones, no ser un texto decorativo. Puede establecer que los accesos se otorguen por necesidad funcional, que los datos críticos se clasifiquen, que los incidentes se reporten y que los sistemas críticos tengan respaldos probados.

La política se relaciona con un conjunto de instrumentos:

Instrumento	Qué define
Política	Qué se exige y el compromiso institucional
Normas	Reglas específicas para situaciones concretas
Procedimientos	Pasos para ejecutar cada proceso
Instructivos	Tareas concretas para usuarios o técnicos
Evidencias	Registros que demuestran cumplimiento

3.5.3 Roles, responsabilidades y autoridades

La falta de responsabilidades claras genera fallas: si nadie es dueño de una base de datos, nadie revisa accesos; si nadie aprueba cambios de configuración, las modificaciones se realizan por urgencia.

La **matriz RACI** ayuda a documentar responsabilidades:

Sigla	Rol	Descripción
R	Responsible	Quien ejecuta la tarea
A	Accountable	Quien responde en última instancia
C	Consulted	Quien debe ser consultado antes de actuar
I	Informed	Quien debe ser informado del resultado

Ejemplo aplicado a una base de nómina: RR.HH. es propietario funcional; TI es custodio técnico; Seguridad define controles; Auditoría revisa evidencias; Dirección recibe indicadores.

3.6 Gestión de riesgos: el núcleo del SGSI

3.6.1 Evaluación de riesgos

La evaluación de riesgos identifica activos, amenazas, vulnerabilidades, impactos y probabilidades. Debe basarse en una **metodología documentada y repetible**, donde el nivel de riesgo = probabilidad × impacto.

Componente	Descripción	Ejemplo
Activo	Recurso con valor para la organización	Base de datos de clientes
Amenaza	Evento potencialmente dañino	Acceso no autorizado, malware, error humano
Vulnerabilidad	Debilidad explotable	Exceso de permisos, falta de MFA
Impacto	Consecuencia si el riesgo se materializa	Exposición de datos, pérdida de confianza
Probabilidad	Posibilidad de ocurrencia	Alta si hay muchos usuarios con permisos amplios

La evaluación debe revisarse ante cambios: un nuevo sistema, un nuevo proveedor, una migración a la nube o un incidente relevante pueden modificar el nivel de riesgo.

3.6.2 Criterios de aceptación y opciones de tratamiento

No todo riesgo puede eliminarse. La organización debe definir qué nivel es tolerable y tratar cada riesgo con criterio:

Opción	En qué consiste	Ejemplo
Reducir	Implementar controles para bajar probabilidad o impacto	Activar MFA y revisar perfiles de acceso
Evitar	Dejar de realizar la actividad que genera el riesgo	No usar un módulo que recolecta datos innecesarios
Transferir	Trasladar parte del impacto mediante contrato o seguro	SLA con proveedor de nube; seguro de riesgos digitales
Aceptar	Asumir el riesgo bajo criterios aprobados y documentados	Riesgo bajo en sistema interno no crítico con monitoreo básico

Una aceptación de riesgo sin responsable ni fecha de revisión puede convertirse en descuido permanente. El **plan de tratamiento** debe indicar: riesgo, acción, responsable, plazo, recursos, control seleccionado, estado y evidencia.

3.6.3 Controles del SGSI

Los controles son medidas que modifican el riesgo. Pueden ser organizativos, técnicos, físicos, legales o relacionados con personas. La selección debe basarse en la evaluación de riesgos, no en criterios genéricos.

Tipo	Ejemplos
Preventivo	MFA, cifrado, segregación de funciones, capacitación contra phishing
Detectivo	Monitoreo de logs, alertas de acceso, auditorías, conciliaciones

Tipo	Ejemplos
Correctivo	Restauración de backups, reversión de cambios, remediación técnica
Recuperatorio	Plan de continuidad, DRP, procedimientos alternativos

3.7 La Declaración de Aplicabilidad (SoA)

La **Declaración de Aplicabilidad** (*Statement of Applicability*, **SoA**) es un documento esencial del SGSI. Responde a cuatro preguntas:

- ¿Qué controles del Anexo A se aplican?
- ¿Cuáles no se aplican y por qué?
- ¿Cuál es el estado de implementación de cada control?
- ¿Con qué riesgos y tratamientos se vinculan?

La SoA es una **pieza clave para auditoría**: demuestra coherencia entre la evaluación de riesgos, las decisiones de tratamiento y los controles implementados. Una SoA desactualizada puede dejar riesgos sin tratamiento formal, especialmente ante cambios como una migración a la nube o la incorporación de nuevos proveedores.

3.8 Operación del SGSI

La operación consiste en ejecutar los procesos planificados de manera controlada y con evidencia. No alcanza con diseñar un procedimiento: debe ejecutarse de forma consistente.

Principio fundamental: si la política dice que los usuarios desvinculados deben darse de baja el mismo día, debe existir una cadena operativa que lo garantice.

Rol	Acción
RR.HH.	Informa la baja con anticipación suficiente
TI	Desactiva usuarios dentro del plazo definido
Seguridad	Verifica cuentas críticas y privilegiadas
Auditoría	Revisa una muestra mensual

La operación debe dejar **evidencia**: ticket, reporte, log, acta, captura o informe. Sin evidencia no se puede demostrar cumplimiento.

3.9 Soporte: recursos, competencia y conciencia

Dimensión	Qué requiere	Consecuencia si falta
Recursos	Presupuesto, herramientas, tiempo, personal	El SGSI se vuelve formal, sin fuerza operativa
Competencia	Conocimientos adecuados para ejecutar tareas de seguridad	Controles mal configurados o procedimientos incumplidos
Conciencia	Que los usuarios comprendan sus responsabilidades	Incidentes no reportados, credenciales compartidas, atajos inseguros

La capacitación debe ser **planificada y medible**: inducción, cursos anuales, simulaciones de phishing, formación para administradores y ejercicios de respuesta ante incidentes.

3.10 Evaluación del desempeño

3.10.1 Indicadores del SGSI

Medir sin actuar no mejora el SGSI: los indicadores deben generar decisiones.

Indicador	Qué permite observar
Porcentaje de riesgos tratados en plazo	Eficacia del plan de tratamiento
Cantidad de no conformidades abiertas	Brechas pendientes de resolver
Tiempo promedio de baja de accesos	Eficacia del proceso de desvinculación
Tiempo promedio de respuesta ante incidentes	Capacidad de reacción y eficacia del procedimiento
Porcentaje de usuarios con MFA	Cobertura del control de autenticación
Porcentaje de backups probados exitosamente	Capacidad real de recuperación
Cantidad de incidentes por severidad	Tendencia de eventos de seguridad
Porcentaje de proveedores críticos evaluados	Gestión del riesgo de terceros
Porcentaje de usuarios capacitados	Cobertura del programa de concienciación
Vulnerabilidades críticas sin tratamiento	Exposición acumulada no gestionada
Cumplimiento de revisiones de acceso	Oportunidad de control periódico

3.10.2 Auditoría interna

La auditoría interna verifica si el SGSI cumple los requisitos definidos, si se implementó correctamente y si se mantiene de manera eficaz. No debe ser una formalidad previa a una certificación: sirve para identificar brechas, controles débiles, documentación incompleta y evidencias insuficientes.

Ejemplo sobre gestión de accesos: se revisan 30 altas, 30 bajas y 20 cambios de perfiles, verificando solicitud, aprobación, oportunidad, evidencia y consistencia con las funciones. Si aparecen usuarios desvinculados con accesos activos, se registra una no conformidad.

La auditoría debe ser objetiva: quien audita no debería auditar su propio trabajo sin independencia. En organizaciones pequeñas puede utilizarse revisión cruzada entre áreas o apoyo externo.

3.10.3 Revisión por la dirección

La revisión por la dirección es una instancia en la que la alta gerencia evalúa el estado del SGSI y toma decisiones sobre:

- Resultados de auditorías y no conformidades.
- Cambios internos y externos relevantes.
- Indicadores de desempeño.
- Incidentes y acciones correctivas.
- Recursos necesarios para el período siguiente.

La revisión debe **generar decisiones documentadas**, no solo recibir informes.

3.11 No conformidades y acciones correctivas

3.11.1 Diferencia entre corrección y acción correctiva

Concepto	Qué hace	Ejemplo
Corrección	Soluciona el problema inmediato	Desactivar la cuenta del usuario que ya no trabaja en la organización
Acción correctiva	Elimina la causa para evitar la repetición	Modificar el procedimiento para que RR.HH. informe las bajas el mismo día y TI bloquee el acceso en 4 horas

Una acción correctiva debe incluir: análisis de causa, acción definida, responsable, plazo, evidencia y verificación de eficacia. Cerrar una acción sin comprobar su resultado debilita el SGSI.

3.11.2 No conformidades frecuentes

No conformidad	Requisito incumplido
Usuarios desvinculados con accesos activos	Política de baja oportuna
Backups sin prueba de restauración	Control de respaldo y recuperación
Accesos privilegiados sin revisión periódica	Gestión de cuentas con privilegios
Incidentes críticos no registrados	Gestión de incidentes
Auditorías internas no realizadas en plazo	Programa de auditorías planificadas

3.12 El ciclo PHVA: mejora continua

El **ciclo PHVA** (*Planificar-Hacer-Verificar-Actuar*), conocido en inglés como **PDCA** (*Plan-Do-Check-Act*), es la lógica que sostiene el funcionamiento del SGSI y evita que sea un documento fijo:

Fase	En el SGSI	Ejemplo aplicado
Planificar	Definir contexto, alcance, política, metodología de riesgos, evaluación y plan de tratamiento	Se identifica el riesgo de modificación indebida de CBU en el sistema de pagos
Hacer	Implementar controles, capacitar, operar procesos,	Se implementa doble aprobación y registro

Fase	En el SGSI	Ejemplo aplicado
	gestionar incidentes y conservar evidencia	automático de cambios en datos bancarios
Verificar	Medir indicadores, auditar, revisar cumplimiento y analizar resultados	Se auditan 30 modificaciones del trimestre y se verifica su conformidad
Actuar	Tratar no conformidades, aplicar acciones correctivas, actualizar riesgos y mejorar controles	Se detecta una falla en el procedimiento y se ajusta el circuito de aprobación

3.13 Temas especiales

3.13.1 SGSI y continuidad operativa

La continuidad operativa debe integrarse al SGSI cuando los riesgos de disponibilidad son relevantes:

Concepto	Qué define	Ejemplo
RTO (*Recovery Time Objective*)	Tiempo máximo tolerable de interrupción del sistema	El sistema de facturación no puede estar caído más de 4 horas
RPO (*Recovery Point Objective*)	Máxima pérdida de información tolerable, medida en tiempo	No puede perderse más de 1 hora de transacciones

Si el sistema de facturación tiene un RTO de 4 horas y un RPO de 1 hora, pero solo existe copia de respaldo diaria, hay una **brecha de continuidad** que el SGSI debe tratar.

3.13.2 SGSI y proveedores

Los proveedores pueden alojar datos, brindar soporte, administrar infraestructura o procesar pagos. El riesgo de terceros debe evaluarse antes de contratar y durante la relación. Requisitos mínimos para proveedores con acceso a sistemas:

Requisito	Descripción
Cuentas individuales	Sin cuentas genéricas o compartidas
MFA	Autenticación multifactor obligatoria
Acceso temporal	Vigente solo durante la prestación del servicio
Registro de sesiones	Trazabilidad de lo que se hizo durante el acceso
Baja al finalizar	Revocación inmediata al terminar el contrato
Cláusulas de seguridad	Confidencialidad, notificación de incidentes, SLA y auditoría

4 ISO 28000 — Seguridad y resiliencia de la cadena de suministro

4.1 Qué es y qué protege

ISO 28000 es una norma internacional que establece requisitos para un **Sistema de Gestión de Seguridad** (*Security Management System*, SMS), con especial aplicación a organizaciones que participan en cadenas de suministro complejas.

La **cadena de suministro** (*supply chain*) comprende todos los actores, procesos, recursos, sistemas e información que permiten que un producto o servicio llegue desde su origen

hasta el usuario final: proveedores, fabricantes, depósitos, transportistas, operadores logísticos, distribuidores, plataformas tecnológicas y documentación comercial.

ISO 28000 **no debe entenderse únicamente como una norma de transporte o logística**. Sus riesgos incluyen mucho más que el robo físico de mercadería:

Riesgo cubierto	Descripción
Interrupción operativa	Fallas que detienen procesos críticos
Fraude documental	Falsificación o alteración de documentos comerciales o aduaneros
Manipulación de datos logísticos	Modificación de órdenes, cantidades, rutas o destinos
Acceso no autorizado a sistemas de proveedores	Brechas en portales o plataformas de terceros
Pérdida de trazabilidad	Imposibilidad de reconstruir el recorrido de un producto o documento
Sabotaje	Daño intencional a infraestructura, transporte o información
Incumplimiento de terceros	Proveedores que no cumplen requisitos de seguridad o continuidad
Dependencia de un único operador	Punto único de falla en la cadena

4.2 La cadena de suministro digital

La cadena de suministro actual depende de sistemas digitales que deben protegerse con la misma rigurosidad que los activos físicos:

Sistema	Función	Riesgo si se compromete
ERP	Integra compras, ventas, inventarios y contabilidad	Modificación de órdenes, precios o datos de proveedores
WMS	Gestiona almacenes, inventarios y movimientos	Alteración de ubicaciones, stocks o despachos
TMS	Planifica y monitorea operaciones de transporte	Cambio de rutas, destinos o tiempos de entrega
API	Permite el intercambio de datos entre sistemas	Exposición o modificación de datos sin controles
IoT / RFID	Rastreo de activos, productos y ubicaciones	Falsificación de trazabilidad o pérdida de señal
Portal de proveedores	Canal de comunicación y transacciones con terceros	Acceso indebido a órdenes, facturas o datos de clientes

Un error en la configuración de un portal de proveedores puede exponer órdenes de compra; una API insegura puede permitir modificar domicilios de entrega; una cuenta comprometida puede alterar cantidades, rutas o datos de facturación.

5 Integración de ISO/IEC 27001 e ISO 28000

5.1 Comparación directa entre ambas normas

Criterio	ISO/IEC 27001	ISO 28000
Objeto principal	Seguridad de la información	Seguridad y resiliencia organizacional, con foco en la cadena de suministro

Criterio	ISO/IEC 27001	ISO 28000
Sistema de gestión	SGSI / ISMS	SMS (*Security Management System*)
Activo protegido	Datos, documentos, sistemas, usuarios, procesos informacionales	Bienes, servicios, infraestructura, proveedores, transporte, continuidad operativa
Riesgo principal	Pérdida, filtración, alteración o indisponibilidad de la información	Interrupción, manipulación, robo, fraude o falla en procesos y flujos organizacionales
Área de aplicación típica	TI, compliance, administración, finanzas, RR.HH., operaciones	Logística, compras, operaciones, comercio exterior, distribución, seguridad física, continuidad
Ejemplo tecnológico	Controlar accesos al ERP y proteger la base de datos de clientes	Proteger el portal de proveedores y la trazabilidad digital de entregas
Aporte al control interno	Gobierno de datos, gestión de riesgos, cumplimiento normativo	Gestión de terceros, continuidad operativa, logística segura, resiliencia

5.2 Riesgos en la intersección

Los riesgos más graves suelen ocurrir en la intersección entre ambas normas: cuando una falla de información impacta en los procesos operativos, o cuando una falla operativa compromete información crítica.

Riesgo	Impacto sobre ISO/IEC 27001	Impacto sobre ISO 28000
Ransomware	Pérdida de disponibilidad de datos y sistemas	Paralización de entregas, almacenes o producción
Phishing	Robo de credenciales e ingreso indebido a sistemas	Acceso a portales de proveedores o instrucciones de entrega falsas
BEC (*Business Email Compromise*)	Fraude por suplantación de directivos o proveedores	Cambio de cuentas bancarias, instrucciones de pago o destinos de entrega
Supply Chain Attack	Compromiso de software o datos a través de un proveedor	Manipulación de componentes, documentos o accesos en la cadena
API insegura	Exposición de datos de clientes, precios o stock	Modificación de órdenes o despachos mediante integraciones inseguras
Mala configuración en la nube	Documentos, bases de datos o respaldos expuestos públicamente	Planes logísticos, contratos o datos de proveedores accesibles sin control

Riesgo	Impacto sobre ISO/IEC 27001	Impacto sobre ISO 28000
Pérdida de trazabilidad	Incapacidad de auditar qué ocurrió con una transacción	Imposibilidad de reconstruir el recorrido de un producto o pedido
Punto único de falla	Un único sistema o administrador concentra toda la gestión	Un único proveedor o transportista concentra la operación crítica

5.3 Controles recomendados

5.3.1 Controles para ISO/IEC 27001

Control	Descripción	Implicancia administrativa
Clasificación de activos	Identificar y valorar la información según su criticidad	No toda la información requiere el mismo nivel de protección ni el mismo costo de control
Control de accesos	Cada usuario accede solo a lo necesario (mínimo privilegio)	Reduce riesgos de errores, abusos internos y accesos indebidos
MFA	Segundo factor de autenticación para sistemas críticos	Mitiga el impacto de credenciales robadas
Gestión de incidentes	Procedimiento para detectar, reportar, contener, corregir y aprender	Una respuesta organizada reduce daños y tiempos de interrupción

Control	Descripción	Implicancia administrativa
Backups probados	Copias de seguridad verificadas periódicamente	Una copia no probada no protege; el restore debe funcionar en el tiempo requerido
Capacitación	Formación periódica y adaptada al rol del usuario	El factor humano es la fuente de riesgo más frecuente en los incidentes

5.3.2 Controles para ISO 28000

Control	Descripción	Implicancia administrativa
Mapeo de la cadena de suministro	Identificar proveedores críticos, transportistas, depósitos y dependencias tecnológicas	Sin visibilidad de la cadena no es posible gestionar sus riesgos
Evaluación de riesgos con terceros	Analizar amenazas de robo, fraude, manipulación e interrupción	El riesgo de terceros (*Third Party Risk*) es tan relevante como el riesgo interno
Contratos con requisitos de seguridad	Incluir cláusulas de confidencialidad, continuidad, niveles de servicio y auditoría	El SLA debe expresar compromisos medibles, no solo intenciones
Protección del flujo de información logística	Resguardar órdenes, remitos, facturas, datos de clientes y confirmaciones de entrega	La información logística es un activo tan crítico como los datos financieros

Control	Descripción	Implicancia administrativa
Planes de continuidad	Proveedores y rutas alternativas, procedimientos manuales de emergencia	La continuidad debe planificarse antes del incidente, no improvisarse durante

5.4 Ejemplos de aplicación por tipo de organización

5.4.1 Empresa de comercio electrónico

Plano	Foco de protección
ISO/IEC 27001	Cuentas de usuario, datos personales, información de tarjetas, bases de datos, paneles administrativos, respaldos y políticas de acceso
ISO 28000	Almacenamiento tercerizado, preparación de pedidos, trazabilidad, transportistas, integridad documental y planes ante interrupciones de entrega

5.4.2 Industria alimenticia

Plano	Foco de protección
ISO/IEC 27001	Recetas, fórmulas, datos de proveedores, registros de calidad, documentación sanitaria y sistemas de producción
ISO 28000	Cadena de frío, autenticidad de proveedores, trazabilidad de lotes,

Plano	Foco de protección
	integridad de entregas, seguridad de depósitos y transporte

Un incidente en este sector puede afectar no solo costos y tiempos, sino también la salud pública, la reputación y la continuidad del negocio.

5.4.3 Institución educativa

Plano	Foco de protección
ISO/IEC 27001	Datos de estudiantes, calificaciones, documentación académica, accesos a campus virtuales, sistemas administrativos
ISO 28000	Proveedores de plataformas educativas, servicios de nube, seguridad de sedes, disponibilidad de infraestructura durante exámenes

Si una plataforma externa falla durante un período de inscripción o evaluación, el problema no es solo técnico: es administrativo, operativo y reputacional.

5.4.4 Empresa importadora

Plano	Foco de protección
ISO/IEC 27001	Contratos, facturas, documentación de comercio exterior, claves de plataformas aduaneras, registros contables
ISO 28000	Demoras, fraude en proveedores, alteración de cargas, fallas de transporte,

Plano	Foco de protección
	interrupciones portuarias, dependencia de un único operador logístico

5.5 Indicadores para la gestión integrada

Los indicadores permiten conectar la seguridad con las decisiones administrativas: sin medición, la seguridad es solo una declaración de intención. Los indicadores de seguridad de la información se detallan en la sección de Evaluación del desempeño; los siguientes corresponden a la seguridad de la cadena de suministro.

Indicador (ISO 28000)	Qué permite observar
Cantidad de incidentes en la cadena de suministro	Frecuencia de fallas de seguridad en proveedores o transportistas
Entregas afectadas por fallas de seguridad	Impacto operativo de los incidentes
Proveedores críticos evaluados anualmente	Cobertura del programa de gestión de terceros
Tiempo de recuperación ante interrupciones	Eficacia de los planes de continuidad
Porcentaje de operadores logísticos auditados	Nivel de control sobre la cadena
Nivel de trazabilidad de entregas	Capacidad de reconstruir el recorrido de productos o documentos

5.6 Relación con el control interno y la administración

Ambas normas aportan estructura al gobierno organizacional. El control interno se beneficia porque ninguna de las dos acepta declaraciones sin evidencia: exigen registros, políticas documentadas, auditorías, indicadores y planes de acción verificables.

Aporte	ISO/IEC 27001	ISO 28000
Gobierno	Define quién es responsable de cada activo de información	Define quién es responsable de cada punto de la cadena de suministro
Riesgo	Estructura la identificación y el tratamiento de riesgos de información	Estructura la identificación y el tratamiento de riesgos operativos y de terceros
Control	Selección de controles técnicos y administrativos	Requisitos contractuales, auditorías y planes de continuidad
Mejora continua	Revisiones periódicas del SGSI	Revisiones periódicas del SMS
Evidencia	Registros, logs, pruebas de restore, reportes de incidentes	Contratos, auditorías de proveedores, reportes de trazabilidad

La diferencia entre **seguridad reactiva** y **seguridad planificada** es precisamente lo que estas normas buscan instalar. La seguridad reactiva actúa después del incidente; la seguridad planificada identifica riesgos, define controles, asigna responsables, mide resultados y mejora procesos: las cuatro funciones clásicas de la administración.

5.7 Certificación y auditoría

Tanto ISO/IEC 27001 como ISO 28000 pueden ser certificadas por organismos acreditados, con dos aclaraciones importantes:

ISO no certifica directamente a las organizaciones. La certificación la realizan entidades certificadoras que evalúan si el sistema de gestión cumple los requisitos de la norma. ISO publica los estándares; otros organismos verifican su cumplimiento.

La certificación no garantiza la ausencia de incidentes. Una organización certificada también puede sufrir fallas; la diferencia es que debería contar con un sistema más ordenado para prevenir, detectar, responder y mejorar ante ellas.

Desde la administración, la certificación debe entenderse como una herramienta de gestión. Implementada solo para exhibir un certificado, pierde valor real; implementada para ordenar procesos, reducir riesgos y mejorar la toma de decisiones, puede convertirse en una ventaja competitiva y en un argumento de confianza frente a clientes, proveedores, reguladores e inversores.

6 Beneficios y errores frecuentes

6.1 Beneficios administrativos del SGSI

Beneficio	Descripción
Ordenar responsabilidades	Cada control tiene responsable, plazo y evidencia
Reducir la improvisación	Las decisiones de seguridad siguen procesos definidos
Facilitar auditorías	La evidencia organizada responde a auditores internos y externos
Fortalecer el control interno	Los controles del SGSI se integran con los controles del negocio
Mejorar la comunicación	La seguridad se expresa en términos de procesos, riesgos e impactos
Demostrar diligencia	Ante clientes, reguladores y socios, el SGSI es evidencia de gestión responsable

6.2 Errores frecuentes en la implementación

Error	Consecuencia
Tratarlo como proyecto documental	Sin cambios reales, las políticas no se cumplen
Alcance mal definido	Lo auditado no cubre los procesos más críticos
Copiar políticas genéricas	No reflejan los riesgos ni la realidad de la organización
Evaluar riesgos sin las áreas de negocio	Los riesgos identificados no corresponden a los procesos reales
Conservar evidencias solo antes de auditorías	El resto del año los controles no se ejecutan
SoA desactualizada	Riesgos nuevos sin controles asignados
No conformidades sin análisis de causa	El problema se repite porque no se corrigió la causa
Indicadores sin acción	Medir no mejora; solo actuar sobre los resultados mejora
Proveedores sin evaluación	El riesgo de terceros queda fuera del SGSI
Backups sin prueba de restauración	El SGSI declara un control que no funciona realmente

7 Ideas clave

- La seguridad debe **administrarse**, no solo instalarse: requiere políticas, responsables, controles, mediciones, auditorías y mejora continua. Un SGSI no es

una herramienta técnica ni una colección de políticas escritas, sino un sistema de gestión que vuelve la seguridad un proceso administrable, medible y auditable.

- **ISO/IEC 27001** protege la información que sostiene las decisiones y la operación; **ISO 28000** protege los procesos y flujos que permiten que la organización siga funcionando. En las organizaciones modernas, ambos planos están interconectados.

- La **tríada CIA** —confidencialidad, integridad y disponibilidad— es el marco que orienta qué proteger. Sin confidencialidad se pierde confianza y cumplimiento; sin integridad se decide con datos incorrectos; sin disponibilidad no se puede operar.

- ISO/IEC 27001 adopta un **enfoque basado en riesgos**: no impone los mismos controles a todas las organizaciones, sino que exige identificar riesgos propios y seleccionar controles adecuados a ellos.

- La **Declaración de Aplicabilidad (SoA)** es el puente entre la evaluación de riesgos y los controles implementados: justifica qué se aplica, qué se excluye y por qué.

- La **evidencia** es una condición no negociable: sin registros, actas, reportes o logs no puede demostrarse que un control existe ni que funciona.

- El **ciclo PHVA** convierte al SGSI en un proceso que se adapta a los cambios en riesgos, sistemas y contexto, en lugar de un documento fijo.

- Las **acciones correctivas** buscan eliminar causas, no solo resolver el caso puntual; un SGSI que solo corrige síntomas repite los mismos problemas.

- La cadena de suministro actual es **digital**: depende de ERP, WMS, TMS, APIs, IoT, RFID y portales de proveedores. Protegerla implica también proteger la información que la sostiene.

- Los **riesgos más graves** ocurren en la intersección entre ambas normas: un ransomware puede paralizar entregas; una cuenta comprometida puede alterar órdenes de compra; una API insegura puede modificar datos logísticos.
- El **riesgo de terceros** (*Third Party Risk*) es tan relevante como el riesgo interno: contratos, SLA medibles y auditorías periódicas son controles administrativos esenciales, no obligaciones meramente formales.
- La **certificación ISO** no garantiza la ausencia de incidentes, sino un sistema más ordenado para gestionarlos. Su valor real está en el proceso de implementación, no en el certificado.

8 Preguntas de evaluación

- ¿Qué diferencia existe entre un SGSI y la instalación de herramientas de seguridad? Proporcione un ejemplo concreto.
- ¿Cuál es la diferencia principal entre el objeto de protección de ISO/IEC 27001 y el de ISO 28000? ¿Por qué deben entenderse como complementarias y no como alternativas?
- Explique los tres principios de la tríada CIA e identifique, para cada uno, una consecuencia concreta para la administración si ese principio se ve comprometido.
- ¿Por qué ISO/IEC 27001 utiliza un enfoque basado en riesgos en lugar de definir controles obligatorios iguales para todas las organizaciones?
- ¿Qué elementos debería incluir el alcance de un SGSI en una empresa que factura en línea, gestiona datos de clientes y usa proveedores externos de infraestructura?
- ¿Cómo influye el contexto de la organización en la seguridad de la información? ¿Qué factores cambian cuando una organización incorpora trabajo remoto?
- ¿Cuál es la diferencia entre amenaza, vulnerabilidad, impacto y riesgo? Proporcione un ejemplo de cada uno aplicado al sistema de pagos a proveedores.

- ¿Qué opciones tiene una organización para tratar un riesgo y en qué condiciones aplica cada una?
- ¿Para qué sirve la Declaración de Aplicabilidad y qué consecuencias tiene tenerla desactualizada?
- ¿Cuál es la diferencia entre corrección y acción correctiva? Analice el caso de un usuario desvinculado que conserva accesos activos.
- ¿Cómo se aplica el ciclo PHVA al proceso de implementación de MFA en cuentas administrativas?
- ¿Por qué ISO 28000 no debe entenderse únicamente como una norma de transporte o logística? ¿Qué otros riesgos organizacionales abarca?
- Analice el ejemplo de la empresa de comercio electrónico: identifique tres riesgos bajo el alcance de ISO/IEC 27001 y tres bajo el de ISO 28000. ¿Existe algún riesgo que afecte a ambos simultáneamente?
- ¿De qué manera un ataque de ransomware puede afectar simultáneamente la seguridad de la información y la cadena de suministro de una organización?
- ¿Por qué los proveedores deben incluirse en la gestión de riesgos? ¿Qué controles mínimos deberían aplicarse a un proveedor con acceso remoto a servidores?
- ¿Qué importancia tienen los contratos, los SLA y las auditorías en la gestión del riesgo de terceros? ¿Por qué no alcanza con confiar en la reputación del proveedor?
- ¿Por qué una certificación ISO no garantiza que una organización nunca sufrirá incidentes? ¿Cuál es el valor real de implementar un sistema de gestión basado en estas normas?
- ¿Qué indicadores podría usar la dirección para evaluar el estado del SGSI y la eficacia de los controles en una reunión de revisión trimestral?

¿Por qué resulta estratégicamente conveniente integrar ISO/IEC 27001 e ISO 28000 en organizaciones que operan con plataformas digitales, múltiples proveedores y procesos logísticos complejos?

9 Glosario

Término	Traducción / Explicación
Accountability	Responsabilidad final. En la matriz RACI, la persona que responde en última instancia por el resultado de una tarea o proceso.
API	*Application Programming Interface*. Interfaz de programación de aplicaciones. Permite que distintos sistemas intercambien datos o funciones; una API insegura puede exponer información sensible o permitir modificaciones no autorizadas.
Audit Log	Registro de auditoría. Registro cronológico e inmutable de las acciones realizadas en un sistema. Fundamental para demostrar cumplimiento.
Availability	Disponibilidad. Principio de la tríada CIA que garantiza que sistemas y datos estén accesibles cuando los procesos legítimos los necesitan.
Backup	Copia de respaldo. Copia de datos destinada a recuperar información ante pérdida, daño o corrupción. Solo tiene valor si puede restaurarse exitosamente.
BEC	*Business Email Compromise*. Fraude por compromiso de correo corporativo: el atacante suplanta a un directivo, proveedor o cliente para ordenar pagos, cambiar cuentas bancarias o modificar instrucciones de entrega.

Término	Traducción / Explicación
Business Continuity	Continuidad del negocio. Capacidad de la organización para seguir funcionando ante interrupciones, mediante planes, recursos alternativos y procedimientos de emergencia.
CBU	Clave Bancaria Uniforme. Identificador bancario argentino de 22 dígitos. Su modificación sin doble control es un riesgo frecuente de fraude.
CIA	*Confidentiality, Integrity and Availability*. Tríada de confidencialidad, integridad y disponibilidad. Marco fundamental de la seguridad de la información.
Cloud Misconfiguration	Mala configuración de servicios en la nube. Puede dejar expuestos documentos, bases de datos, respaldos o paneles administrativos sin controles de acceso adecuados.
Cloud services	Servicios en la nube. Servicios de computación, almacenamiento o software provistos por un tercero a través de internet.
Confidentiality	Confidencialidad. Principio de la tríada CIA: la información solo debe ser accedida por personas o sistemas autorizados.
Corrective action	Acción correctiva. Medida orientada a eliminar la causa de una no conformidad para evitar que se repita. Distinta de la corrección, que solo resuelve el caso puntual.
DRP	*Disaster Recovery Plan*. Plan de recuperación ante desastres. Plan técnico para restaurar sistemas e infraestructura luego de una interrupción grave.

Término	Traducción / Explicación
Encryption	Cifrado. Técnica criptográfica que protege la información transformándola en un formato ilegible sin la clave correspondiente.
ERP	*Enterprise Resource Planning*. Sistema de planificación de recursos empresariales. Integra compras, ventas, inventarios, contabilidad y finanzas en una única plataforma.
Firewall	Cortafuegos. Herramienta de seguridad que controla el tráfico de red según reglas definidas.
IAM	*Identity and Access Management*. Gestión de identidades y accesos. Procesos y sistemas para administrar usuarios, roles, permisos, altas, bajas y modificaciones.
IEC	*International Electrotechnical Commission*. Comisión Electrotécnica Internacional. Organismo que publica normas en tecnologías eléctricas, electrónicas y relacionadas.
Integrity	Integridad. Principio de la tríada CIA: los datos deben ser exactos, completos y no alterados indebidamente.
Interested parties	Partes interesadas. Personas u organizaciones que pueden afectar al SGSI, verse afectadas por él o tener requisitos relacionados.
IoT	*Internet of Things*. Internet de las Cosas. Dispositivos físicos conectados a internet que recopilan o transmiten datos, como sensores, lectores de temperatura o rastreadores GPS.

Término	Traducción / Explicación
ISMS	*Information Security Management System*. Denominación en inglés del Sistema de Gestión de Seguridad de la Información (SGSI).
ISO	*International Organization for Standardization*. Organización Internacional de Normalización. Desarrolla y publica normas internacionales; no certifica organizaciones directamente.
ISO/IEC 27001	Norma internacional que establece los requisitos para implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).
ISO 28000	Norma internacional que establece los requisitos para un Sistema de Gestión de Seguridad y Resiliencia, con especial aplicación a la cadena de suministro.
IT	*Information Technology*. Tecnologías de la Información (TI).
Least Privilege Principle	Principio de mínimo privilegio. Cada usuario debe acceder solo a los recursos necesarios para cumplir su función, sin permisos adicionales.
Loss of Traceability	Pérdida de trazabilidad. Situación en la que la organización no puede reconstruir qué ocurrió con un producto, documento, pedido, usuario o transacción.
MFA	*Multi-Factor Authentication*. Autenticación multifactor. Mecanismo que exige más de un factor de verificación para acceder a un sistema (por ejemplo, contraseña más código temporal).

Término	Traducción / Explicación
Nonconformity	No conformidad. Incumplimiento de un requisito de la norma, la política interna, un procedimiento o un control definido.
PDCA	*Plan-Do-Check-Act*. Ciclo Planificar-Hacer-Verificar-Actuar (PHVA). Lógica de mejora continua aplicada al SGSI.
Phishing	Técnica de engaño mediante correos, mensajes o sitios falsos para obtener credenciales o información sensible del usuario.
PHVA	Planificar-Hacer-Verificar-Actuar. Versión en español del ciclo PDCA.
RACI	*Responsible-Accountable-Consulted-Informed*. Matriz que asigna roles en cada proceso: quién ejecuta, quién responde, quién es consultado y quién es informado.
Ransomware	Software malicioso que cifra archivos o sistemas y exige un pago (rescate) para restaurar el acceso. Puede paralizar operaciones completas y destruir backups.
Resilience	Resiliencia. Capacidad de una organización para anticipar, resistir, adaptarse y recuperarse frente a incidentes, interrupciones o cambios adversos.
RFID	*Radio Frequency Identification*. Identificación por radiofrecuencia. Permite identificar objetos o activos mediante etiquetas y lectores, sin contacto físico. Usada en logística y control de inventarios.
Risk-based approach	Enfoque basado en riesgos. Criterio de ISO/IEC 27001 que exige identificar riesgos propios y seleccionar controles

Término	Traducción / Explicación
	adecuados a ellos, sin imponer un conjunto fijo para todas las organizaciones.
RPO	*Recovery Point Objective*. Objetivo de punto de recuperación. Máxima pérdida de información tolerable ante un incidente, medida en tiempo.
RTO	*Recovery Time Objective*. Objetivo de tiempo de recuperación. Tiempo máximo tolerable de interrupción de un sistema antes de generar un impacto inaceptable.
Scope	Alcance. Definición de los límites del SGSI: qué áreas, procesos, sistemas y datos quedan incluidos bajo gestión.
SGSI	Sistema de Gestión de Seguridad de la Información. Conjunto organizado de políticas, procesos, controles, evidencias y mejoras para proteger la información. Equivale al ISMS en inglés.
Single Point of Failure	Punto único de falla. Situación en que una sola persona, proveedor, sistema o infraestructura concentra una función crítica, y su caída afecta toda la operación.
SLA	*Service Level Agreement*. Acuerdo de nivel de servicio. Define compromisos medibles entre proveedor y cliente sobre disponibilidad, tiempos de respuesta y calidad.
SMS	*Security Management System*. Sistema de Gestión de Seguridad. Marco utilizado por ISO 28000 para organizar la gestión de seguridad y resiliencia.

Término	Traducción / Explicación
SoA	*Statement of Applicability*. Declaración de Aplicabilidad. Documento del SGSI que registra qué controles del Anexo A se aplican, cuáles se excluyen y con qué justificación.
Supply Chain	Cadena de suministro. Red de actores, procesos, sistemas e información que permiten producir, mover y entregar bienes o servicios desde el origen hasta el usuario final.
Supply Chain Attack	Ataque a la cadena de suministro. Ocurre cuando un atacante compromete a un proveedor para acceder a la organización principal, o altera software, documentos, componentes o procesos logísticos.
Third Party Risk	Riesgo de terceros. Riesgo generado por proveedores, contratistas, socios, plataformas externas o prestadores tecnológicos que tienen acceso a sistemas, datos o procesos de la organización.
TMS	*Transportation Management System*. Sistema de gestión de transporte. Permite planificar, controlar y monitorear operaciones de transporte y logística.
WMS	*Warehouse Management System*. Sistema de gestión de almacenes. Permite administrar inventarios, ubicaciones, entradas, salidas y movimientos internos de mercadería.