Gestión y cumplimiento básico

CÓRDOBA CREA FUTURO

Introducción

En la era digital, las pequeñas y medianas empresas (pymes) enfrentan cada vez más exigencias para gestionar la seguridad de su información y cumplir con estándares básicos de ciberseguridad. Este módulo aborda dos aspectos importantes: por un lado, las políticas mínimas de seguridad que toda organización debería establecer; por otro, una introducción al estándar internacional ISO 27001 como marco de gestión de la seguridad de la información. Aunque las pymes suelen disponer de recursos limitados, adoptar políticas claras y procesos de cumplimiento puede marcar la diferencia entre prevenir incidentes o sufrir brechas costosas.

La creciente exposición de las pymes a amenazas informáticas refuerza esta necesidad. Según un informe de Kaspersky divulgado en 2025, el 43 % de las pymes de América Latina fue víctima de ataques de *phishing* durante el año anterior. Además, se estima que en 2024 se registraron más de 1,18 millones de ciberataques en la región; en países como Argentina, las pymes fueron blanco frecuente de ataques de *ransomware* y robo de credenciales. Estos datos evidencian la urgencia de adoptar medidas de protección que no dependan únicamente de soluciones técnicas, sino también de la concientización del personal y de políticas de seguridad claras.

Este módulo busca brindar fundamentos prácticos para que una organización establezca políticas básicas de seguridad —sobre uso de sistemas, contraseñas, dispositivos móviles y copias de seguridad— y comprenda cómo un SGSI basado en ISO 27001 ayuda a gestionar la seguridad de forma sistemática.

Al finalizar este módulo, sabremos cómo redactar e implementar políticas sencillas pero eficaces, fomentar hábitos seguros en el equipo y dar los primeros pasos hacia el cumplimiento de estándares reconocidos. La seguridad no es solo un asunto técnico: es una cultura organizacional que comienza con reglas claras, apoyo de la dirección y educación continua de todos los miembros de la empresa.

CONTINUAR

Unidad 1. Políticas mínimas

En esta unidad exploraremos las políticas básicas de seguridad que una pyme debería establecer para proteger sus activos. Las políticas son directrices escritas que definen «qué se debe hacer» en distintos aspectos de la seguridad. Funcionan como reglas del juego que todos en la empresa deben seguir para reducir riesgos.

A continuación, se describen cuatro políticas mínimas que pueden implementarse en organizaciones pequeñas o medianas: uso aceptable, contraseñas/MFA, BYOD (*trae tu propio dispositivo*) y copias de seguridad/retención de datos.

Cada política se presenta con su propósito, recomendaciones clave y ejemplos prácticos para su aplicación. Es importante recordar que estas políticas deben adaptarse a la realidad de cada empresa, comunicarse claramente a todo el personal y revisarse periódicamente para asegurar su vigencia.

Uso aceptable

La política de uso aceptable establece qué usos de los recursos informáticos de la empresa se consideran permitidos o prohibidos. Su objetivo es que el personal sepa con claridad cómo utilizar las herramientas tecnológicas —como computadoras,

teléfonos móviles, redes, internet o correo electrónico— de forma segura y responsable. En otras palabras, define las reglas del juego para prevenir abusos o prácticas inseguras que puedan comprometer los sistemas corporativos.

¿Qué incluye una política de uso aceptable?

Su contenido suele abarcar varios aspectos. Por ejemplo, puede restringir la navegación a sitios web peligrosos o inapropiados, prohibir la descarga de software no autorizado y regular el uso del correo electrónico corporativo. También suele indicar que los dispositivos de la empresa deben usarse con fines laborales (limitando un uso personal excesivo) y que está prohibido realizar actividades ilegales, discriminatorias o que violen la confidencialidad de la organización desde los sistemas corporativos. En esencia, delimita qué está permitido y qué no al utilizar los activos de tecnologías de la información de la empresa.

¿Por qué es importante?

En primer lugar, porque reduce riesgos de seguridad y legales. Si el personal conoce las reglas, es menos probable que lleve a cabo acciones que introduzcan *malware* —como conectar dispositivos USB desconocidos o instalar aplicaciones no autorizadas— o que expongan información sensible, por ejemplo, al subir datos de la empresa a servicios en la nube sin autorización. En segundo lugar, porque mejora la productividad: evita que los recursos de la organización se utilicen en actividades ajenas al trabajo durante la jornada laboral. En tercer lugar, porque establece con claridad las expectativas de comportamiento y las posibles sanciones ante el incumplimiento, lo que contribuye a mantener la disciplina y la equidad.

Un uso aceptable de los recursos garantiza la protección de la red y los dispositivos corporativos. Por ejemplo, la política debe indicar que no se tolera el uso de internet para descargar contenido malicioso, visitar páginas de riesgo o realizar actividades ilegales. Asimismo, puede contemplar el uso adecuado del correo electrónico (evitando el envío de correos personales masivos, no compartiendo contraseñas por ese medio, entre otras prácticas), el manejo responsable de equipos portátiles (no dejarlos desatendidos y

mantenerlos cifrados si se trasladan fuera de la oficina) y el uso de redes sociales (aclarando si se permite el acceso desde el entorno laboral y recordando que no debe publicarse información confidencial de la empresa).

Implementación práctica

Al redactar esta política, es importante involucrar a las áreas de sistemas y de recursos humanos. Debe formularse en un lenguaje claro y difundirse de manera amplia. Es recomendable que cada persona firme una copia al ingresar a la empresa, dejando constancia de que entiende y acepta las normas.

El documento debe incluir ejemplos concretos. Por ejemplo: «No está permitido conectar a la red corporativa dispositivos externos sin autorización del departamento de TI». Además, es útil ofrecer alternativas seguras: si se prohíbe el uso de servicios de almacenamiento en la nube no autorizados, la política puede especificar cuáles están aprobados para uso empresarial.

Por último, se debe revisar esta política de forma periódica, con el fin de adaptarla a nuevas tecnologías o riesgos emergentes, como el uso de aplicaciones de mensajería o herramientas de videoconferencia.

Buenas prácticas en la política de uso aceptable

A continuación, se enumeran algunas recomendaciones habituales que refuerzan el cumplimiento de esta política en el entorno laboral:

- **No instalar *software* no autorizado**. Todos los programas deben estar licenciados y contar con la aprobación del área de TI.
- **Navegación segura**: está prohibido visitar sitios de descargas ilegales, apuestas, pornografía u otras páginas de alto riesgo. El filtrado web puede respaldar esta medida.

- **Correo electrónico corporativo**: debe usarse de forma responsable, sin reenviar cadenas ni adjuntos sospechosos. No se debe emplear para registrarse en servicios personales de dudosa fiabilidad.
- **Uso de dispositivos**: no se deben conectar dispositivos de almacenamiento externos de origen desconocido. Es necesario bloquear la computadora al ausentarse del puesto y evitar compartir el equipo corporativo con personas ajenas al entorno laboral.
- **Redes sociales y mensajería**: no divulgar información interna en redes sociales y evitar mantener conversaciones informales sobre datos de la empresa en aplicaciones no autorizadas.

En resumen, la política de uso aceptable funciona como un código de conducta digital. Todo el personal debe conocerla y comprender que su cumplimiento protege tanto a la organización como a cada uno de sus integrantes. Una recomendación final: complementar la política con instancias de capacitación y recordatorios periódicos. Por ejemplo, realizar sesiones breves de sensibilización, en las que se analicen casos reales de mal uso —como empleados que infectaron la red al descargar juegos— puede ayudar a contextualizar y reforzar su importancia.

Contraseñas y MFA (autenticación multifactor)

Una política de contraseñas constituye otro pilar de la ciberseguridad básica. Las contraseñas siguen siendo la llave de acceso a la mayoría de los sistemas, pero con frecuencia representan el eslabón más débil debido a malas prácticas por parte de los usuarios. Esta política establece los requisitos que deben cumplir las contraseñas utilizadas en la organización y promueve el uso de autenticación multifactor (MFA) como una capa adicional de protección.

Según un estudio reciente del Instituto Nacional de Ciberseguridad (INCIBE), el 90% de las contraseñas son vulnerables. Sin embargo, la implementación de MFA puede

reducir el riesgo de accesos no autorizados hasta en un 99 %.

A continuación, se detallan los puntos esenciales que esta política debe contemplar.

REQUISITOS DE CONTRASEÑAS SEGURAS	GESTIÓN DE CONTRASEÑAS	AUTENTICACIÓN MULTIFACTOR (MFA)	EDUCACIÓN SOBRE CONTRASEÑAS

La política debe establecer criterios mínimos de complejidad y gestión de contraseñas. Por ejemplo, suele requerirse una longitud mínima —al menos 12 caracteres— y la combinación de letras mayúsculas, minúsculas, números y símbolos. También se recomienda no utilizar datos personales obvios, como nombres propios, números de documento, fechas de cumpleaños o referencias a la empresa.

Otra regla habitual es prohibir el uso de contraseñas corporativas en servicios externos, así como la reutilización de contraseñas antiguas. Además, conviene establecer el cambio periódico de contraseñas sensibles. Aunque las tendencias actuales destacan la importancia de la longitud y la unicidad por sobre la frecuencia de cambio, en entornos empresariales todavía es común exigir su renovación cada 90 días.

REQUISITOS DE CONTRASEÑAS SEGURAS	GESTIÓN DE CONTRASEÑAS	AUTENTICACIÓN MULTIFACTOR (MFA)	EDUCACIÓN SOBRE CONTRASEÑAS

Dado que recordar contraseñas complejas y únicas para cada cuenta puede resultar difícil, la política puede fomentar el uso de gestores de contraseñas confiables. Estas herramientas permiten generar claves aleatorias robustas y almacenarlas de forma cifrada, lo que elimina la necesidad de memorizarlas una por una. Su uso contribuye a evitar prácticas inseguras, como anotar contraseñas en papel o reutilizar la misma clave en múltiples servicios —una conducta riesgosa, ya que si una contraseña se ve comprometida, puede poner en peligro todas las cuentas asociadas.

En caso de utilizar un gestor, la contraseña maestra debe ser especialmente fuerte y mantenerse en absoluta confidencialidad. La política debe dejar en claro que compartir contraseñas está estrictamente prohibido: las credenciales son personales e intransferibles. Ningún integrante del equipo debe comunicar su contraseña a colegas, personal técnico o terceros, ni siquiera por teléfono. En lugar de compartir cuentas, deben establecerse accesos individuales con los permisos adecuados para cada usuario.

Más allá de las contraseñas, la política debe fomentar el uso de autenticación multifactor (MFA) siempre que sea posible. Este mecanismo consiste en añadir al menos un factor adicional a la contraseña, normalmente algo que el usuario posee —como un código temporal en su teléfono móvil, una aplicación autenticadora o un dispositivo físico— o algo que el usuario es, como una huella dactilar o el reconocimiento facial. De este modo, aunque una contraseña se vea comprometida, el atacante no podrá acceder sin ese segundo factor.

Un ejemplo práctico es la activación de MFA en el correo corporativo (como Office 365 o Google Workspace): al iniciar sesión, el usuario debe ingresar su contraseña y, además, un código generado en su teléfono. Solo con ambos elementos se permite el acceso. Este método ha demostrado frenar la mayoría de los intentos de intrusión automatizados. Diversos organismos de ciberseguridad señalan que implementar MFA permite bloquear hasta el 99 % de los ataques por fuerza bruta o robo de credenciales.

La política puede especificar qué sistemas internos requieren MFA obligatorio —como la red privada virtual (VPN) de la empresa, paneles de administración de servidores o cuentas de administrador de red—. En los servicios que aún no soporten MFA, se recomienda migrar a plataformas que sí lo permitan o aplicar controles compensatorios, como cofres de contraseñas de un solo uso.

Por último, debe indicarse el método preferido de autenticación. Idealmente, se recomienda el uso de aplicaciones autenticadoras —como Google Authenticator, Microsoft Authenticator o Authy— en lugar de mensajes SMS, ya que estos últimos son menos seguros. No obstante, los SMS pueden considerarse una medida inicial válida cuando no existan otras alternativas disponibles.

La política de contraseñas debe venir acompañada de acciones de concientización. Muchos usuarios subestiman la importancia de una buena contraseña. Podemos compartir con ellos ejemplos de contraseñas débiles típicas —como «123456», «contraseña» o el nombre de la empresa seguido del año— y explicar por qué son riesgosas. También es útil mencionar incidentes conocidos: «El 81 % de las filtraciones de datos se deben a contraseñas robadas o débiles» (estadística global repetidamente citada).

Podemos capacitar en cómo crear frases de contraseña fáciles de recordar, pero robustas —por ejemplo, una combinación de tres o cuatro palabras aleatorias con espacios o símbolos—. Y, sobre todo, debemos promover el uso de MFA como hábito: aunque pueda parecer engorroso, vale la pena ese segundo adicional para verificar en el teléfono, ya que impide que un ciberdelincuente utilice una contraseña robada desde otro país.

Buenas prácticas de la política de contraseñas y MFA

A continuación, se enumeran algunas prácticas recomendadas que debemos considerar al implementar esta política:

- **Longitud y complejidad**. Establecer un mínimo de 12 caracteres, combinar diferentes tipos de caracteres y evitar palabras completas del diccionario.

- **Unicidad**: utilizar una contraseña distinta para cada cuenta. Si un servicio sufre una brecha y la contraseña se filtra, no debe permitir el acceso a ningún otro sistema.
- **Prohibido compartir**: ninguna contraseña corporativa debe compartirse por correo electrónico, mensajería o notas. Si una persona se ausenta, existen procedimientos formales para el acceso de emergencia sin violar esta regla.
- **Almacenamiento seguro**: utilizar un gestor de contraseñas en lugar de anotarlas en papel o guardarlas en archivos de texto.
- **MFA obligatorio**: habilitar MFA en cuentas corporativas críticas —correo electrónico, VPN, sistemas en la nube, banca en línea, entre otros—. Incluso se puede considerar el uso de MFA interno para accesos administrativos a servidores.
- **Cambio de contraseñas**: cambiar de inmediato cualquier contraseña que se sospeche haya sido comprometida. También es necesario reemplazar las contraseñas por defecto en dispositivos —como *routers* o cámaras IP— antes de ponerlos en producción.
- **Bloqueo tras intentos fallidos**: configurar los sistemas para que bloqueen la cuenta o aumenten los retardos tras varios intentos incorrectos, a fin de mitigar ataques por fuerza bruta.

En síntesis, la combinación de contraseñas robustas y autenticación multifactor representa hoy la medida más eficaz para una autenticación segura. La política debe reflejar una postura estricta al respecto, ya que los ataques por robo de credenciales —*phishing*, *malware* especializado o filtraciones masivas— son una amenaza constante. Al adoptar estas prácticas, protegemos a la empresa frente a una de las vías de ataque más comunes.

«Bring your own device» (BYOD) o «trae tu propio dispositivo» y móviles

El término *bring your own device* (BYOD) hace referencia a la práctica de permitir que el personal utilice sus dispositivos personales —computadoras portátiles, teléfonos móviles, tabletas— para acceder a recursos corporativos. Esta modalidad puede mejorar la

productividad y la comodidad, pero también introduce riesgos de seguridad si no se gestiona adecuadamente.

Una política de BYOD y móviles establece las condiciones y controles para el uso de dispositivos personales en el trabajo, así como las normas aplicables a los dispositivos móviles provistos por la empresa. En una pyme, es común que no todas las personas cuenten con equipos corporativos, por lo que regular el uso de BYOD resulta clave para prevenir brechas de seguridad.

Aspectos clave de la política BYOD

En primer lugar, es necesario definir qué tipos de dispositivos están permitidos y con qué requisitos mínimos. Por ejemplo, se puede autorizar solo el uso de teléfonos móviles y computadoras portátiles con sistemas operativos actualizados —según una versión mínima definida— y con el cifrado de disco habilitado.

En segundo lugar, se deben establecer medidas de seguridad obligatorias en los dispositivos personales. Para poder conectarse a la red de la empresa, el empleado debe cumplir condiciones como mantener un antivirus actualizado, contar con un PIN o contraseña de desbloqueo, y tener habilitada la función de borrado remoto en caso de pérdida. También puede requerirse la instalación de una aplicación de gestión de dispositivos móviles (*MDM*) de la empresa, que permita separar los datos personales de los corporativos y aplicar configuraciones de seguridad específicas. Por ejemplo, en caso de desvinculación o extravío, la empresa podría borrar únicamente los datos laborales sin afectar la información personal del dispositivo.

La política también debe contemplar las condiciones de conexión a la red interna. Según el nivel de riesgo, puede limitarse el uso de BYOD a redes wifi de invitados o segmentadas. Si los dispositivos personales acceden a información sensible —como correo corporativo o documentos de negocio—, deben aplicarse controles de acceso equivalentes a los de un equipo corporativo. Por ejemplo, se puede exigir el uso de una VPN para acceder a recursos internos desde una computadora personal o, al menos, autenticación multifactor para ingresar a los servicios en la nube de la empresa.

Uso aceptable en BYOD

Es importante recordar que, incluso cuando se utiliza un dispositivo personal, al conectarse a la red o a los datos de la empresa, aplican las mismas reglas de uso aceptable. No por tratarse de un teléfono particular se puede instalar una aplicación insegura que interactúe con sistemas corporativos.
La política debe dejar en claro que la empresa se reserva cierto derecho de auditoría o monitoreo sobre la actividad relacionada con sus datos en dispositivos personales. Este suele ser un punto sensible, pero puede gestionarse adecuadamente si se especifica, por ejemplo, que mediante la solución MDM la empresa solo tiene visibilidad sobre la partición de datos corporativos, respetando la privacidad del resto del dispositivo.

Protección de datos móviles

Los dispositivos móviles —ya sean personales o provistos por la empresa— suelen salir del entorno laboral con frecuencia y son propensos a extravíos o robos. La política debe exigir el cifrado de los datos. La mayoría de los teléfonos inteligentes modernos ya cifran el almacenamiento de forma nativa si tienen un PIN o un sistema biométrico activado.

También deben establecerse medidas como el autobloqueo tras un período breve de inactividad y la activación de funciones de localización o borrado remoto. Un caso común: un empleado pierde un teléfono que tenía acceso al correo corporativo. Si el dispositivo contaba con un PIN robusto y la empresa logró eliminar la cuenta de forma remota, el incidente queda mitigado. De lo contrario, alguien con malas intenciones podría acceder al correo y, desde allí, restablecer otras contraseñas, generando un efecto dominó.

El correo electrónico corporativo en un dispositivo móvil debe contar con el mismo nivel de protección que en una computadora. Si nuestra organización utiliza MFA para el acceso vía web, debemos configurarlo también en el cliente móvil.

Por último, la política de BYOD debe abordar la separación entre datos personales y corporativos. Idealmente, la información de la empresa no debería mezclarse sin control con los datos personales en un mismo dispositivo. Algunas formas de lograrlo incluyen el uso de

aplicaciones oficiales —por ejemplo, una aplicación corporativa que contenga los archivos de trabajo y requiera autenticación adicional— o, al menos, la instrucción clara de que no se debe almacenar documentación interna en aplicaciones personales (por ejemplo, subir archivos de la empresa a una cuenta personal de Google Drive).

Varias soluciones de MDM permiten crear contenedores cifrados para los datos corporativos dentro del dispositivo. Si la pyme no cuenta con este tipo de herramientas, debe reforzarse la concientización: educar al personal para que maneje la información empresarial con cuidado, evite respaldarla en servicios personales en la nube, y utilice únicamente medios autorizados.

Resumen de requisitos en la política BYOD/móviles —

Para implementar una política de BYOD efectiva, es necesario establecer una serie de requisitos básicos que deben cumplir los dispositivos personales y móviles utilizados con fines laborales. Entre ellos, se destacan los siguientes:

- Dispositivo con sistema operativo actualizado y sin *jailbreak* o *root*.
- Bloqueo de pantalla seguro obligatorio (PIN complejo, huella digital, etc.), con intentos fallidos limitados.
- Cifrado del dispositivo activo.
- Antivirus actualizado (en computadoras portátiles y, en Android, si se considera necesario).
- Prohibido conectar a la red interna dispositivos no autorizados o de terceros que no cumplan con la política.
- La empresa puede revocar el acceso o eliminar los datos corporativos si detecta incumplimientos (por ejemplo, un dispositivo comprometido con *malware*).
- Uso de la red: conexión mediante VPN para acceder remotamente a recursos internos; en la oficina, uso de redes wifi segmentadas si así lo establece la política.

- Notificación obligatoria: se debe reportar de inmediato la pérdida o el robo de un dispositivo con datos de la empresa, para poder tomar medidas como el cambio de contraseñas, la anulación de sesiones o el borrado remoto.

Implementar BYOD de forma segura representa un desafío, pero con una política clara y herramientas de gestión adecuadas, es posible lograr un equilibrio. Muchas pymes optan por esta modalidad para reducir costos en equipamiento; si ese es nuestro caso, debemos asegurarnos de formalizar estas reglas y de que cada persona comprenda que conectar su dispositivo personal al trabajo implica una responsabilidad adicional.

Una recomendación útil es ofrecer apoyo: por ejemplo, ayudar al personal a instalar aplicaciones de seguridad o proporcionar licencias de antivirus para sus computadoras personales. De este modo, todos ganamos en tranquilidad.

En 2025, las amenazas móviles —como *malware* en Android o iOS y *phishing* a través de WhatsApp o SMS— siguen en aumento. Una buena política de BYOD, acompañada de capacitación, puede reducir significativamente la superficie de ataque de la organización al cubrir estos eslabones sueltos. Recordemos: un dispositivo desprotegido es una puerta de entrada que los atacantes no dudarán en aprovechar.

Copias y retención —

La última política mínima que abordamos es la de copias de seguridad (*backups*) y retención de datos. Esta política busca garantizar que la empresa realice respaldos periódicos de su información crítica y defina por cuánto tiempo conservar determinados datos, cumpliendo tanto con requisitos operativos como legales.

En muchas pymes, las copias de seguridad suelen dejarse de lado —«¿para qué, si nunca pasa nada?»— hasta que ocurre un incidente devastador: una falla de disco, un ataque de *ransomware* que cifra toda la información o, simplemente, el borrado accidental de un documento vital.

Una política de *backups* y retención permite prevenir estos escenarios mediante un esquema claro para el resguardo de la información.

Estrategia de *backup* 3-2-1

Un principio ampliamente recomendado para la protección de datos es la regla 3-2-1. Esta sugiere:

- mantener tres copias de los datos, la original y al menos dos copias de respaldo;
- Utilizar dos tipos de medios diferentes, por ejemplo, disco local y almacenamiento en la nube, o disco y cinta;
- conservar al menos una copia fuera del sitio principal (*off-site*).

La política debe establecer qué datos se respaldan, con qué frecuencia y cómo se almacenan esas copias. Por ejemplo: «Se realizará diariamente una copia de seguridad incremental de la base de datos de clientes en el servidor NAS local, y semanalmente se transferirá una copia completa cifrada a un servicio en la nube confiable».

También es recomendable designar a una persona o área responsable —como el administrador de sistemas o una empresa tercerizada de IT— e incluir procedimientos para probar regularmente la restauración de los respaldos.

Alcance de los *backups*

Debemos identificar cuáles son los activos de información críticos para la organización. En una pyme, esto puede incluir documentos contables, listas de clientes, bases de datos de ventas, correos electrónicos, proyectos en curso, entre otros. La política debe enumerar qué conjuntos de datos forman parte del plan de respaldo.

No todo requiere ser respaldado —por ejemplo, puede que no sea necesario copiar por completo cada computadora individual si los archivos importantes están centralizados—, pero todo lo relevante debe estar cubierto.

Además, la política debe definir los *retention points*, es decir, cuántas versiones históricas se conservarán. Por ejemplo, se podrían guardar respaldos diarios de la última semana, semanales del último mes y luego mensuales durante un año. Esto permite recuperar un archivo tal como estaba en una fecha anterior o revertir modificaciones realizadas por error tiempo atrás.

Retención y cumplimiento legal

La política de retención define por cuánto tiempo deben conservarse ciertos datos antes de su eliminación segura. Este período suele estar determinado por normativas legales o por las propias necesidades del negocio. Por ejemplo, las leyes fiscales pueden exigir la conservación de comprobantes y documentación contable durante cinco o diez años. En otros casos, los datos personales de clientes deben eliminarse una vez finalizado el servicio, en cumplimiento de normativas de privacidad como el Reglamento General de Protección de Datos (GDPR).

La política debe establecer lineamientos claros. Por ejemplo, «los respaldos se almacenarán por un período de un año, tras el cual serán eliminados de forma segura, excepto aquellos que contengan registros contables, los cuales se conservarán durante cinco años conforme a la legislación vigente». También pueden aplicarse esquemas escalonados, como «los respaldos diarios se conservarán durante un mes y los respaldos de fin de mes se mantendrán durante un año». Esta práctica evita la acumulación innecesaria de copias antiguas y facilita la gestión eficiente del almacenamiento.

Seguridad de las copias

Es fundamental que las copias de seguridad sean seguras por sí mismas. Esto implica proteger los respaldos con el mismo nivel de cuidado que los datos originales. La política debe exigir que las copias estén cifradas, especialmente cuando se almacenan fuera de la empresa —por ejemplo, si se suben a la nube o se guardan en cintas o discos externos transportados a otra ubicación—.

También se debe controlar su acceso: solo el personal autorizado puede manipular los respaldos. Además, es indispensable probar periódicamente la restauración de las copias para confirmar que funcionan correctamente. No sirve de nada realizar respaldos de forma diligente si, al momento de necesitarlos, descubrimos que los archivos están corruptos o que nadie sabe cómo recuperarlos. Un buen hábito consiste en realizar simulacros de restauración con regularidad, como recuperar un archivo aleatorio de un respaldo antiguo cada trimestre y verificar su integridad.

Esta política de respaldos suele incluir también un procedimiento para incidentes. En caso de pérdida masiva de datos, debe detallarse cómo proceder con la recuperación. Por ejemplo: «En caso de desastre en el servidor principal, el responsable de IT iniciará la restauración desde la copia externa más reciente; prioridad 1: base de datos de ventas (máximo 4 horas de RTO), prioridad 2: archivos compartidos (RTO de 8 horas)».

Conceptos como RTO (*Recovery Time Objective*) y RPO (*Recovery Point Objective*) pueden estar reflejados en la política. Se refieren, respectivamente, al tiempo máximo de interrupción aceptable y a la cantidad de datos que se puede tolerar perder. Aunque muchas pymes no los formalizan, es importante que la política los contemple de manera implícita para garantizar una recuperación eficaz.

Por ejemplo, una organización que tolere hasta 24 horas de datos potencialmente perdidos (RPO = 24 h) deberá realizar respaldos al menos una vez por día. Si además puede tolerar hasta dos días de interrupción total (RTO = 48 h), será necesario contar con hardware de reemplazo disponible para restablecer los servicios críticos dentro de ese plazo.

Retención de registros y datos sensibles

Además de los respaldos, esta política puede incluir directrices sobre la retención de distintos tipos de información. Por ejemplo, ¿los correos electrónicos se conservan indefinidamente o se eliminan después de cierto tiempo? ¿Los archivos de proyectos finalizados permanecen en los servidores activos o se archivan o eliminan

tras un período determinado? ¿Qué sucede con los documentos en papel, si aún existen: cuánto tiempo se conservan y cómo se destruyen luego?

Todas estas decisiones suelen estar vinculadas al cumplimiento normativo. Si nuestro sector está regulado —como salud, finanzas o servicios legales—, debemos asegurarnos de incorporar los requisitos específicos. Si no existen exigencias legales concretas, al menos debemos definir un criterio de buena práctica que evite conservar datos innecesarios de forma indefinida, ya que eso también representa un riesgo para la seguridad.

BUENAS PRÁCTICAS DE BACKUPS Y RETENCIÓN

A continuación, se enumeran algunas buenas prácticas que debemos considerar al implementar esta política:

- **Automatización**. Utilizar *software* de respaldo automatizado en lugar de depender de copias manuales. Esto reduce el riesgo de error humano, como olvidar realizar el respaldo.
- **Diversificación de medios**: combinar, por ejemplo, un respaldo local rápido (en un NAS o servidor interno) con otro externo o en la nube. De este modo, cubrimos eventos como incendios o robos manteniendo una copia fuera del sitio principal.
- **Cifrado y protección**: cifrar las copias externas con contraseñas robustas y restringir el acceso a las claves de cifrado únicamente al personal autorizado.
- **Versionado**: conservar múltiples versiones de los archivos. Esto permite recuperar información anterior a un ataque de *ransomware*, evitando que se sobrescriba la única copia disponible.
- **Documentar y probar**: además de establecer la política por escrito, debemos realizar pruebas de restauración al menos cada seis meses. Es fundamental documentar los

resultados y aplicar los ajustes necesarios.

En síntesis, la política de copias de seguridad y retención busca prepararnos para el peor escenario y cumplir con las obligaciones de archivo. Una pyme no puede darse el lujo de perder sus datos críticos, ya que esto podría representar desde un impacto financiero hasta el cierre definitivo del negocio.

Con una política bien definida, construimos un colchón de seguridad: ante cualquier eventualidad —un ataque de *ransomware*, un incendio o el robo de un equipo portátil— los datos seguirán resguardados en otro lugar. Además, al establecer criterios de retención, garantizamos que se conserven únicamente los datos necesarios y se elimine lo que ya no es útil, reduciendo la exposición a riesgos innecesarios.

De hecho, muchas normas y estándares —incluida la norma ISO 27001, que abordaremos en la unidad 2— exigen contar con copias de respaldo y procedimientos de restauración. No se trata de una opción: es un componente esencial de la resiliencia de la organización.

CONTINUAR

Unidad 2. ISO 27001

En esta unidad nos adentramos en el estándar internacional ISO/IEC 27001, que establece un marco para gestionar la seguridad de la información en una organización a través de un sistema de gestión de seguridad de la información (SGSI). Veremos cómo ISO 27001 se apoya en el ciclo de mejora continua PDCA (plan-do-check-act), y exploraremos algunos componentes clave como el contexto y liderazgo dentro de la empresa, la gestión de riesgos, la concientización y controles de seguridad, y la definición de roles y responsabilidades (por ejemplo, mediante matrices RACI). Aunque suene muy corporativo, incluso las pymes pueden beneficiarse de los principios de ISO 27001, adaptándolos a su escala. Esta unidad no busca que memoricemos la norma, sino comprender sus conceptos básicos y cómo aplicarlos de forma pragmática para elevar el nivel de seguridad y cumplimiento en un negocio.

¿Por qué ISO 27001?

Porque proporciona una guía estructurada para proteger la confidencialidad, integridad y disponibilidad de la información. Es un estándar reconocido internacionalmente; obtener su certificación demuestra a clientes y aliados que tomamos en serio la ciberseguridad. Sin embargo, más allá del certificado, aplicar ISO 27001 nos obliga a reflexionar sobre qué riesgos amenazan nuestra información y qué controles debemos implementar para mitigarlos.

Para una pyme, adoptar ISO 27001 puede parecer abrumador, pero es posible hacerlo de forma gradual y proporcionada. En esta unidad comenzaremos por sus fundamentos.

La serie de normas ISO/IEC 27000 está compuesta por estándares internacionales de seguridad publicados por la Organización Internacional de Normalización (ISO, International Organization for Standardization) y la Comisión Electrotécnica Internacional (IEC, *International Electrotechnical Commission*).

Esta serie recoge las mejores prácticas recomendadas en seguridad de la información para desarrollar, implementar y mantener un sistema de gestión de seguridad de la información (SGSI). Un SGSI abarca todos los controles administrativos, técnicos y operativos necesarios para proteger la información dentro de una organización.

Tomando como referencia la versión 2013, se definieron doce dominios independientes que representaban los componentes del estándar ISO/IEC 27000. Aunque en la versión más reciente esta estructura ha cambiado, estos doce dominios siguen siendo útiles para comprender los fundamentos de la norma, ya que permiten organizar —a un nivel general— las principales áreas que abarca la seguridad de la información.

Figura 1. Domicilios de la serie ISO/TEC 27000

Fuente: Velandia et al., 2023, https://goo.su/BIcnj

Para diseñar un sistema de administración de seguridad informática, debemos tener en cuenta lo siguiente:

- **El estándar ISO/IEC 27001 define los objetivos de control.**
- **El estándar ISO/IEC 27002 define los controles.**
- **Los controles son más detallados que los objetivos.**
- **Los objetivos de control indican lo que la organización debe lograr.**
- **Los controles especifican cómo alcanzar esos objetivos.**

Por ejemplo, consideremos el siguiente objetivo de control: controlar el acceso a las redes mediante mecanismos de autenticación adecuados para los usuarios y los

equipos.

Un control asociado podría ser el siguiente: «Utilizar contraseñas seguras. Una contraseña segura debe tener al menos ocho caracteres e incluir una combinación de letras, números y símbolos (@, #, $, %, etc.), si están permitidos. Debe distinguir entre mayúsculas y minúsculas, por lo que es recomendable incluir ambos tipos de letras».

La mayoría de las organizaciones genera un documento llamado **declaración de aplicabilidad** (*statement of applicability*, SOA), en el cual se definen los objetivos de control que la organización ha decidido implementar.

Algunos principios ampliamente reconocidos en ciberseguridad sobre los controles incluyen:

- los controles no son obligatorios, pero sí están ampliamente aceptados y adoptados;
- deben mantener la neutralidad frente a proveedores, para evitar la percepción de que se respalda un producto o empresa específica;
- funcionan como pautas: existen múltiples formas válidas de cumplir con un mismo objetivo de control.

Figura 2. Principios de la ciberseguridad

Fuente: Velandia et al., 2023, https://goo.su/BIcnj

Los controles establecidos por la norma ISO abordan específicamente los objetivos de seguridad de los datos en cada uno de sus tres estados: en tránsito, en uso y en reposo. Para ello, los representantes de cada grupo de trabajo colaboran en la identificación de los controles aplicables y en la determinación de su prioridad según el área:

- El representante del grupo de seguridad de red identifica los controles que garantizan la confidencialidad, integridad y disponibilidad de los datos mientras se transmiten.
- El representante del grupo de desarrollo y el personal encargado del ingreso de datos determina los controles necesarios para proteger la confidencialidad, integridad y disponibilidad de los datos durante su procesamiento.

- El representante del grupo de soporte de hardware y servidores identifica los controles que resguardan la confidencialidad, integridad y disponibilidad de los datos almacenados.

La familia ISO/IEC 27000 comprende una amplia gama de normas que abordan, de manera integral, los distintos aspectos de la seguridad de la información. A continuación, se describen algunas de las más relevantes.

- **ISO/IEC 27000**: ofrece un vocabulario estándar para el SGSI. Sirve como introducción y base para el resto de las normas.
- **ISO/IEC 27001**: es la norma certificable que deben cumplir las organizaciones. Especifica los requisitos para la implantación de un SGSI, adopta un enfoque basado en la gestión de riesgos y promueve la mejora continua. Es la norma central de la serie.
- **ISO/IEC 27002**: *Information security, cybersecurity and privacy protection — Information security controls*. Anteriormente conocida como BS 7799 parte 1 y luego como ISO/IEC 17799. Es un código de buenas prácticas para la gestión de la seguridad de la información.
- **ISO/IEC 27003**: proporciona directrices para la implementación de un SGSI. Complementa la norma ISO/IEC 27001.
- **ISO/IEC 27004**: establece métricas para la gestión de la seguridad de la información. Indica quién, cuándo y cómo realizar mediciones.
- **ISO/IEC 27005**: aborda la gestión de riesgos en seguridad de la información, con métodos y técnicas para su evaluación, en apoyo a la ISO/IEC 27001.

- **ISO/IEC 27006**: define los requisitos para la acreditación de organizaciones que certifican SGSI, y se utiliza junto con la norma ISO/IEC 17021-1.
- **ISO/IEC 27007**: guía para la auditoría de un SGSI.
- **ISO/IEC 27008**: guía para auditar los controles implementados en un SGSI.
- **ISO/IEC 27009**: especifica cómo adaptar ISO/IEC 27001 a distintos sectores o ámbitos.
- **ISO/IEC 27010**: orientada a la gestión de la seguridad de la información compartida entre organizaciones, aplicable a cualquier tipo de intercambio.
- **ISO/IEC 27011**: guía de interpretación específica para el sector de telecomunicaciones.
- **ISO/IEC 27014**: trata el gobierno corporativo de la seguridad de la información.
- **ISO/IEC 27015**: orientada a organizaciones del sector financiero y de seguros.
- **ISO/IEC 27016**: se enfoca en el análisis financiero y económico de las inversiones en seguridad.
- **ISO/IEC 27017**: guía de seguridad para servicios de computación en la nube (*cloud computing*).
- **ISO/IEC 27018**: orientada a la protección de datos personales en servicios de nube pública.
- **ISO/IEC 27019**: guía para sistemas de control industrial en el sector energético.
- **ISO/IEC 27031**: guía para la preparación de tecnologías de la información y comunicación ante interrupciones.
- **ISO/IEC 27032**: establece directrices generales para fortalecer la ciberseguridad en las organizaciones.
- **ISO/IEC 27033**: ofrece una guía detallada sobre la seguridad en redes.
- **ISO/IEC 27034**: se centra en la seguridad de las aplicaciones dentro del ámbito de tecnologías de la información.

- **ISO/IEC 27035:2011**: aborda la gestión de incidentes de seguridad, incluyendo detección, notificación y análisis.
- **ISO/IEC 27036**: trata la seguridad en las relaciones con proveedores.
- **ISO/IEC 27038**: especifica directrices para la seguridad en la redacción digital.
- **ISO/IEC 27039**: orientada a la selección, despliegue y operación de sistemas de detección y prevención de intrusiones.
- **ISO/IEC 27040**: guía para la seguridad en medios de almacenamiento.
- **ISO/IEC 27041**: directrices para evaluar la idoneidad de métodos de investigación en seguridad digital.
- **ISO/IEC 27042**: guía para el análisis e interpretación de evidencias digitales.
- **ISO/IEC 27043**: desarrolla principios de investigación digital para la recopilación de evidencias.
- **ISO/IEC 27050**: serie de normas sobre el tratamiento de información almacenada en dispositivos electrónicos.
- **ISO/IEC 27103:2018**: proporciona orientación para aplicar normas existentes dentro de un marco de ciberseguridad.
- **ISO/IEC 27799:2008**: guía para implementar ISO/IEC 27002 en el sector salud.

Un SGSI es un conjunto de políticas, procesos y controles interrelacionados que se implementan en una organización para gestionar la seguridad de la información de manera sistemática. A diferencia de medidas aisladas o reactivas, un SGSI propone un enfoque integral y continuo: planificar la seguridad, implementarla, evaluarla regularmente y mejorar

lo necesario. ISO/IEC 27001 especifica los requisitos para establecer, mantener y mejorar un SGSI efectivo.

El **ciclo PDCA** (planificar – hacer – verificar – actuar) es la espina dorsal de cualquier sistema de gestión ISO, incluido el SGSI. También conocido como círculo de Deming, el ciclo PDCA promueve la mejora continua: siempre existen oportunidades para ajustar procesos y controles; nunca se alcanza una seguridad «perfecta» o estática. Veamos cómo se aplica este ciclo en ISO/IEC 27001:

- *Plan* **(planificar)**

  En esta fase se establece el SGSI. Implica definir el alcance —qué partes de la organización y qué información protegerá el SGSI—, comprender el contexto y las partes interesadas, establecer la política de seguridad de la información, identificar riesgos y planificar cómo tratarlos.
  En ISO/IEC 27001, esta etapa se desarrolla en varios capítulos de la norma:

  - ➔ 4. Contexto de la organización
  - ➔ 5. Liderazgo
  - ➔ 6. Planificación
  - ➔ 7. Soporte

  Esto significa que, al planificar, debemos analizar los factores internos y externos que afectan la seguridad (contexto), asegurar el compromiso de la dirección y definir roles (liderazgo), realizar la evaluación de riesgos y planificar los objetivos de seguridad (planificación), y asignar recursos y concienciar al personal (soporte).

  El resultado tangible de esta fase suele ser un *statement of applicability* —documento que define qué controles se aplicarán— y un plan de tratamiento de riesgos, entre otros documentos iniciales.

- *Do* **(hacer)**

En esta fase se implementan y operan los controles y procesos planificados. Es la etapa de ejecución: aplicar las políticas, poner en marcha las medidas de seguridad —tanto tecnológicas como organizativas—, realizar las capacitaciones y gestionar los riesgos según lo planificado.

En ISO/IEC 27001, esta fase corresponde principalmente al capítulo 8. Operación. Por ejemplo, si en la fase «planificar» se decidió mitigar el riesgo de *malware* mediante un antivirus centralizado, en «hacer» se procede a instalar y configurar ese antivirus en todos los equipos. Si se planificaron copias de seguridad fuera del sitio, en esta etapa se monta la infraestructura necesaria y se comienzan a realizar los respaldos. Básicamente, «hacer» representa el trabajo diario de seguridad con el sistema ya en funcionamiento.

- ***Check*** **(verificar)**

Esta fase consiste en evaluar el desempeño del SGSI y comprobar si las actividades se desarrollan según lo planificado. Incluye el monitoreo de incidentes, la realización de auditorías internas, la revisión de métricas de seguridad y la revisión por la dirección (instancia formal en la que la alta gerencia evalúa el estado del SGSI).

En ISO/IEC 27001, esta etapa corresponde al capítulo 9. Evaluación del desempeño. Por ejemplo, se verifica si los controles están funcionando (¿los parches se aplican a tiempo?, ¿los usuarios cumplen con la política de contraseñas?), se audita el cumplimiento de la documentación establecida y se miden indicadores (como el número de incidentes en el trimestre respecto al anterior, o el porcentaje de personal que completó la formación).

Esta fase genera hallazgos, no con fines punitivos, sino para identificar oportunidades de mejora. Un ejemplo de hallazgo sería el siguiente: «la auditoría interna detectó que, aunque existe un procedimiento de respaldo, en el 20 % de las computadoras no se estaba ejecutando correctamente». Ese tipo de hallazgo alimenta la siguiente fase.

- ***Act* (actuar)**

  En esta fase se corrigen las debilidades detectadas en «verificar» y se ajusta el SGSI. Se toman acciones correctivas sobre los problemas hallados y se introducen mejoras que reinician el ciclo. Esta etapa corresponde al capítulo 10. Mejora de la norma ISO/IEC 27001.

  Siguiendo el ejemplo anterior, se actuará corrigiendo el proceso de respaldo (ajustar la configuración en esas computadoras y, quizá, establecer una comprobación mensual de los *backups*). Otras acciones pueden incluir la actualización de una política, la incorporación de un nuevo control si surge un riesgo no contemplado, o el refuerzo de la capacitación en un área donde se hayan producido incidentes.

  «Actuar» cierra el ciclo y da inicio a un nuevo «planificar»: se vuelve a evaluar el contexto si hubo cambios, se reconsideran los riesgos y se continúa iterando de forma continua.

Un SGSI basado en el ciclo PDCA garantiza que la seguridad no sea un proyecto de «una sola vez», sino un proceso continuo. Para ilustrar su funcionamiento, se puede considerar el siguiente caso aplicado a una pyme. Supongamos que la empresa ha implementado su SGSI e identificado un riesgo alto de *phishing*. En la fase de planificación, se decide mitigar este riesgo mediante acciones como la capacitación del personal, la implementación de autenticación multifactor (MFA) y la configuración de filtros *antiphishing*. En la fase de ejecución, se dictan los talleres, se habilita MFA en las cuentas corporativas y se configuran los filtros en el correo electrónico.

Tiempo después, en la fase de verificación, se observa que algunos usuarios aún hicieron clic en correos de prueba de phishing interno, y se detecta que dos cuentas no tenían MFA activo, a pesar de la política establecida. Ante estos hallazgos, en la fase de mejora se decide reforzar la capacitación con un módulo específico para quienes fallaron y se configura desde el área de TI la activación obligatoria de MFA en las cuentas rezagadas. Además, se actualiza la política para aclarar que ninguna cuenta puede quedar exceptuada de este requisito. Con estas medidas, se inicia un nuevo ciclo, ahora más ajustado a la realidad detectada.

La estructura de la norma ISO/IEC 27001 refleja directamente el ciclo PDCA. Los capítulos 4 al 10 se organizan según las fases del ciclo: contexto de la organización, liderazgo, planificación y soporte (planificar); operación (hacer); evaluación del desempeño (verificar); y mejora continua (actuar). Además, incorpora un anexo (Anexo A) que reúne una lista de controles de seguridad —como políticas, controles de acceso, cifrado o antivirus— que deben analizarse en función de los riesgos identificados y aplicarse según corresponda. Aun así, el foco principal de la norma está en el SGSI: disponer de un sistema formal para gestionar estos controles de forma coherente y sostenible.

En una pyme, quizás no se implemente cada formalidad de la norma, pero comprender el ciclo PDCA resulta valioso. Podemos aplicar este enfoque a nuestro propio plan de seguridad, incluso sin buscar la certificación. Por ejemplo, cada año (planificar) revisamos qué nuevos riesgos han surgido (nuevos ataques, cambios en el negocio) y ajustamos nuestros planes; ejecutamos las medidas de seguridad (hacer) durante el año; al finalizar, evaluamos los incidentes y el cumplimiento (verificar); y corregimos las fallas detectadas (actuar) preparando el siguiente ciclo. De este modo, evitamos la lógica de «poner parches solo cuando hay incendios» y adoptamos una mejora continua.

En resumen, un SGSI basado en PDCA nos ofrece una estructura para organizar la seguridad. Desde los aspectos técnicos hasta los organizativos, todo queda abarcado y se revisa periódicamente. ISO/IEC 27001 nos indica qué elementos debemos considerar —riesgos, políticas, activos, controles, auditorías, entre otros—, mientras que PDCA es la brújula que permite abordarlos con constancia. Como señala la norma, el objetivo final es «establecer, implementar, mantener y mejorar continuamente» la seguridad de la información: justamente lo que promueve este ciclo.

Registro de riesgos. Concientización y controles —

Contexto y liderazgo

Dos componentes iniciales en la implementación de ISO/IEC 27001 (fase planificar) son el contexto de la organización y el liderazgo de la dirección. Ambos establecen la base sobre la cual se diseña el SGSI, garantizando que esté alineado con la realidad y los objetivos del negocio, y que cuente con el respaldo firme de la alta gerencia.

Contexto de la organización

Antes de implementar controles, ISO/IEC 27001 exige entender la organización y su contexto (cláusula 4.1). Esto implica analizar factores internos y externos que afectan la seguridad de la información. Entre los factores internos se incluyen: el tamaño de la empresa, el tipo de datos que maneja, su cultura organizacional, las tecnologías utilizadas y la infraestructura de TI (¿todo en la nube?, ¿infraestructura propia?). Entre los factores externos: el sector en el que opera (no es lo mismo una clínica que una tienda minorista), los requisitos legales aplicables (leyes de protección de datos, regulaciones sectoriales), las amenazas del entorno (¿opera en una zona con alta ciberdelincuencia?, ¿tiene proveedores tecnológicos con riesgos?), o el estado general de la ciberseguridad en el país.

También se deben identificar las partes interesadas (cláusula 4.2): ¿quiénes tienen interés en la seguridad de la información? Clientes, socios, reguladores, empleados, propietarios. Cada uno puede tener expectativas o requisitos específicos (por ejemplo, un cliente podría exigir ciertos controles si se manejan sus datos).

Con esta información, se define el alcance del SGSI (cláusula 4.3): qué áreas de la empresa y qué sistemas quedan incluidos. En una pyme podría ser «todo el departamento de operaciones y sus sistemas de información» o «la empresa completa» si es pequeña. Definir el alcance evita confusiones: se sabe hasta dónde aplican las políticas y procesos del SGSI.

Entender el contexto es fundamental para que el SGSI sea pertinente y efectivo. Por ejemplo, si se identifica que el principal riesgo externo es el cumplimiento de la ley de protección de datos personales, el SGSI deberá enfocarse en controles de privacidad, concientización y respuesta a incidentes. O si internamente hay escaso personal de TI, la estrategia deberá apoyarse más en automatización o servicios tercerizados. En resumen, el contexto define las condiciones iniciales. Un SGSI que no lo tenga en cuenta puede fracasar,

ya sea por aplicar controles innecesarios que dificulten el negocio o por ignorar amenazas reales.

Liderazgo y compromiso de la dirección —

ISO/IEC 27001 enfatiza que la alta dirección (gerentes, dueños) debe demostrar liderazgo en el SGSI (cláusula 5.1). Esto no es un simple formalismo: significa que la cúpula de la empresa apoya abiertamente la iniciativa de seguridad, asigna recursos y se involucra en las decisiones clave. Deben aprobar y difundir la política de seguridad de la información (cláusula 5.2), que es un documento marco donde declaramos nuestro compromiso de proteger la información, cumplir las leyes, gestionar riesgos, etc. Además, se espera que se asignen claramente los roles y responsabilidades para el SGSI (cláusula 5.3); por ejemplo, nombrar un responsable de seguridad de la información (que en una pyme podría ser el encargado de sistemas, o un consultor externo) y otros responsables para acciones específicas.

¿Por qué es tan importante el liderazgo? Porque ningún proyecto de seguridad prospera sin apoyo gerencial. Imaginemos intentar imponer políticas y cambios de hábitos sin el respaldo de los jefes: los empleados podrían no tomarlo en serio («esto no le importa al jefe, ¿por qué me va a importar a mí?»). Por el contrario, cuando la dirección da el ejemplo —por ejemplo, el gerente general toma el curso de concientización igual que todos, o envía comunicaciones subrayando la prioridad de la ciberseguridad— la cultura organizacional se alinea más fácilmente. Además, muchas iniciativas requieren inversión (comprar un *firewall*, contratar capacitación, etc.): solo la dirección puede aprobar presupuesto. Su compromiso se ve en hechos: asignar fondos, participar en las revisiones del SGSI, exigir reportes periódicos sobre el estado de la seguridad y, sobre todo, cumplir también ellos las políticas (¡un mal ejemplo sería que la gerencia se excluya de seguir las reglas!).

En ISO/IEC 27001, la alta dirección también debe realizar la **revisión por la dirección** (cláusula 9.3), que consiste, básicamente, en reunirse —al menos una vez al año— para evaluar el desempeño del SGSI: revisar los resultados de auditorías, incidentes ocurridos, logros frente a los objetivos establecidos, y a partir de ello emitir directrices para mejoras.

Esta instancia cierra el ciclo de liderazgo continuo. En una pyme, esta reunión puede ser breve, pero no debería omitirse: es la oportunidad para que los responsables del negocio verifiquen si la inversión en seguridad está dando resultados y qué ajustes pueden ser necesarios.

Podemos afirmar que el contexto y el liderazgo sientan las bases del SGSI: sabemos dónde estamos y contamos con un compromiso claro de hacia dónde queremos ir. Por ejemplo, supongamos que somos una pyme de desarrollo de *software* que decide implementar un SGSI. En el análisis de contexto detectamos que el mayor riesgo es la protección de la propiedad intelectual del código y los datos de clientes almacenados en la nube. Identificamos nuestras partes interesadas: clientes internacionales preocupados por la seguridad, entes reguladores de datos personales, entre otros. Establecemos el alcance del SGSI en todo el proceso de desarrollo y los servicios en la nube. Con este diagnóstico claro, la dirección (CEO y CTO) se compromete a liderar con el ejemplo: aprueba la política, designa al CTO como responsable del SGSI, asigna presupuesto para capacitar al equipo en seguridad durante el desarrollo, y solicita reportes mensuales sobre los avances. Este arranque sólido incrementa notablemente las probabilidades de éxito del SGSI.

Por el contrario, si la alta dirección se ausenta o muestra apatía («ocúpense ustedes de seguridad, yo no me meto»), es muy probable que el SGSI se convierta en un simple documento archivado. ISO/IEC 27001 exige formalmente ese respaldo, pero más allá de la obligación, se trata de una buena práctica fundamental para que la seguridad se integre verdaderamente en la cultura organizacional.

Rol de la política de seguridad —

Vale la pena destacar el papel central que tiene la política de seguridad de la información, la cual debe ser establecida y aprobada por la alta dirección. Este documento, habitualmente de una o dos páginas, enuncia nuestros compromisos generales: proteger los activos de información, cumplir con las leyes aplicables, gestionar los riesgos, fomentar la mejora continua, asignar responsabilidades, entre otros aspectos clave. Su función es ser la carta de

presentación del enfoque organizacional frente a la seguridad, tanto para nuestro personal como para terceros. Todos en la organización deberían conocerla.

En algunos casos, esta política se complementa con un manual más extenso, pero la política en sí es la declaración formal de alto nivel. Un ejemplo de frase habitual podría ser «la Gerencia se compromete a proporcionar los recursos necesarios para implantar las medidas de seguridad que protejan la confidencialidad, integridad y disponibilidad de la información de la empresa, acorde con los riesgos identificados, y a revisar periódicamente la eficacia del Sistema de Gestión de Seguridad de la Información». Esta formulación permite dejar claramente expresado el liderazgo y compromiso institucional.

En resumen, el contexto y el liderazgo constituyen los cimientos del SGSI: nos permiten diseñar un sistema de seguridad ajustado a nuestro entorno y asegurar que toda la organización —comenzando desde la dirección— reme en la misma dirección. Sin estos elementos, cualquier esfuerzo en seguridad podría ser descoordinado o carecer de respaldo. Con ellos, tenemos un norte claro —sabemos qué debemos proteger y por qué— y un liderazgo firme que impulsa la seguridad como una prioridad estratégica, no solo técnica.

Registro de riesgos

La gestión de riesgos es el corazón de ISO/IEC 27001. Identificar y manejar los riesgos relacionados con la seguridad de la información nos permite enfocar los recursos en proteger lo que realmente importa frente a las amenazas más probables y con mayor impacto. El registro de riesgos —también conocido como matriz de riesgos— es una herramienta clave en este proceso, ya que documenta los riesgos identificados, su evaluación y las decisiones sobre su tratamiento. En esta sección abordamos cómo llevamos a cabo este proceso en un entorno básico.

¿Qué entendemos por riesgo de seguridad? Es la combinación de una amenaza y una vulnerabilidad que, al materializarse, puede generar un impacto sobre un activo de información. Por ejemplo, amenaza = ransomware; vulnerabilidad = ausencia de copias de seguridad actualizadas; activo afectado = base de datos de clientes; impacto = pérdida de datos y paralización de las operaciones. En el registro, esto se expresaría como «existe el

riesgo de que un *ransomware* infecte la red y cifre la base de datos de clientes, provocando su indisponibilidad y posible pérdida permanente de información».

Identificación de riesgos —

Según ISO/IEC 27001 (cláusula 6.1.2), debemos identificar los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de nuestros activos de información. Esta etapa implica listar situaciones no deseadas, que van desde ataques cibernéticos —como *malware*, *phishing* o ataques de denegación de servicio (DDoS)— hasta fallos de equipamiento, errores humanos (como eliminaciones accidentales o configuraciones incorrectas), desastres naturales (por ejemplo, una inundación que afecte servidores), robos internos o accesos no autorizados. Para cada riesgo se deben identificar las fuentes de amenaza, las vulnerabilidades que podrían ser explotadas y los activos que se verían afectados. Esta información se documenta en el registro de riesgos (*risk register*), que será la base para el análisis y tratamiento posterior.

Análisis y evaluación

Una vez identificados, analizamos cada riesgo considerando su probabilidad de ocurrencia y el impacto que tendría si se materializa. Para ello, se asignan niveles cualitativos (por ejemplo, baja, media o alta) o valores numéricos. Luego, se calcula el nivel de riesgo —por ejemplo, combinando probabilidad e impacto mediante una multiplicación o una matriz— que nos indica su criticidad.

Por ejemplo, el riesgo de «robo de un portátil con datos sensibles» podría tener una probabilidad media (suele ocurrir en el sector) y un impacto alto (exposición de datos confidenciales), resultando en un riesgo alto. En cambio, un «incendio en la oficina que destruya los servidores» podría tener una probabilidad baja, pero un impacto igualmente alto; eso podría ubicarse como riesgo medio-alto, según el criterio utilizado.

Muchas organizaciones representan esta información mediante una matriz de riesgos (o *heatmap*), donde el eje X muestra la probabilidad y el eje Y el impacto. Cada riesgo se ubica

en un cuadrante: verde (tolerable), amarillo (moderado), rojo (inaceptable). Esta visualización permite priorizar el tratamiento: los riesgos en zona roja requieren acción inmediata, los amarillos deben tratarse en un plazo razonable y los verdes pueden aceptarse.

ISO/IEC 27001 permite definir un criterio de aceptación de riesgos; por ejemplo, «aceptamos los riesgos bajos, los medios y altos deben ser tratados». Además, se espera un registro documentado con la evaluación, el nivel asignado y un responsable (propietario del riesgo) para su gestión.

Tratamiento de riesgos

Para cada riesgo identificado —especialmente aquellos no aceptables— la organización debe definir una estrategia de tratamiento: mitigar, transferir, evitar o aceptar.

- **Mitigar** consiste en implementar controles que reduzcan la probabilidad de ocurrencia o el impacto del riesgo. Por ejemplo, ante un riesgo de ransomware, se puede mitigar mediante copias de seguridad, antivirus actualizados y segmentación de red.
- **Transferir** implica trasladar el riesgo a un tercero, generalmente mediante seguros o servicios externos. Por ejemplo, contratar un seguro cibernético o utilizar un proveedor *cloud* que asuma parte del riesgo.
- **Evitar** significa dejar de realizar la actividad que genera el riesgo. Por ejemplo, si un servidor antiguo sin parches expuesto a Internet representa un riesgo inaceptable, evitarlo sería apagarlo o desconectarlo definitivamente.
- **Aceptar** es asumir conscientemente las consecuencias sin aplicar medidas adicionales. Esta opción se utiliza principalmente cuando el riesgo es bajo o cuando el costo de mitigación supera el posible impacto.

Estas decisiones se documentan en el registro de riesgos o en un plan de tratamiento de riesgos. Cada riesgo debe tener una o varias acciones de control asociadas. Veamos algunos ejemplos.

- Riesgo: *phishing* dirigido a empleados.
- Tratamiento: mitigar mediante capacitación en detección de *phishing*, implementación de un filtro antispam más estricto, y activación de autenticación multifactor (MFA) para el acceso al correo electrónico.

Se asigna también un responsable y un plazo para implementar cada acción.

Registro de riesgos (*risk register*)

Este suele estructurarse como una tabla donde cada fila representa un riesgo identificado. Las columnas típicas incluyen: Identificador del riesgo, Descripción, Activos afectados, Probabilidad, Impacto, Nivel de riesgo, Controles existentes, Controles propuestos (plan de tratamiento), Propietario del riesgo y Estado (pendiente, en curso, tratado). Es un documento vivo: a medida que se implementan controles, el riesgo residual disminuye y se actualiza su estado. También sirve como base para el seguimiento en las revisiones periódicas del SGSI.

En una pyme, al comenzar, puede ser suficiente identificar entre 10 y 20 riesgos principales. No es necesario listar cientos de riesgos menores; lo importante es enfocarse en aquellos que realmente pueden materializarse y tener un impacto significativo.

Tabla 1. Ejemplo de registro de riesgos simplificado

ID	Riesgo	Prob. (valor)	Impacto (valor)	Nivel de riesgo	Tratamiento (control)	Responsable
R1	*Ransomware* cifra servidor de archivos	Media (3)	Alto (5)	15 (Alto)	Copias de seguridad diarias fuera del	Encargado de TI

	compartidos → pérdida de datos				sitio + antivirus en servidores + formación al personal (no abrir adjuntos sospechosos)	
R2	Fuga de datos de clientes por empleado deshonesto (interno)	Baja (2)	Alto (5)	10 (Medio)	Limitar acceso (principio de mínimos privilegios) + monitoreo de accesos + acuerdos de confidencialidad	Gerente de Operaciones
R3	Caída prolongada de Internet deja a la empresa sin operar (ventas en línea)	Media (3)	Media (3)	9 (Medio)	Contratar conexión redundante con otro proveedor	Dirección general / TI
R4	Robo físico de computadoras con información sensible	Media (3)	Media (3)	9 (Medio)	Cifrado de disco en portátiles + política de oficina segura (cerradura física) + inventario actualizado de equipos	Encargado de TI

R5	Incumplimiento de la Ley de Protección de Datos Personales → sanciones	Baja (2)	Alto (5)	10 (Medio)	Mitigar mediante políticas de privacidad, consentimiento informado, control de acceso a datos personales y borrado seguro al finalizar relación contractual	Dirección general / Legal

Fuente: elaboración propia.

Los controles seleccionados deben estar justificados en función del riesgo. De hecho, la norma exige elaborar una **declaración de aplicabilidad** (SoA), donde se indique qué controles del Anexo A se aplican o no, y por qué. Esta decisión debe derivarse directamente del análisis de riesgos. Por ejemplo, en el SoA puede consignarse:

- «Control A.10.1 – Cifrado de datos: Aplicado. Para mitigar el riesgo de robo de portátiles, se cifra el disco duro».
- «Control A.11.2 – Sistema de alarma contra incendios: No aplicado. Las oficinas se encuentran en un edificio con sistema central contra incendios; el riesgo es bajo y está cubierto por seguros».

Este documento conecta explícitamente la evaluación de riesgos con la selección de controles. En una pyme, quizás no se formalice todo el lenguaje de ISO, pero resulta igualmente útil contar con un registro de riesgos, aunque sea informal. Esto ofrece múltiples beneficios: permite justificar inversiones (por ejemplo, si se identifica que un ataque puede ocasionar pérdidas estimadas de $ 50.000 y el control cuesta $ 5000, la inversión es razonable), ayuda a priorizar (focalizando primero los riesgos más críticos) y permite anticiparse (si ocurre un riesgo previsto, se sabe cómo actuar o al menos no toma por sorpresa). Además, la gestión de riesgos debe ser continua: cada vez que se introduce un cambio relevante —nueva tecnología, proveedor, mercado, etc.— es necesario reevaluar los riesgos asociados.

En términos de cumplimiento básico, muchas regulaciones exigen evidencias de gestión de riesgos. Por ejemplo, algunas leyes de protección de datos requieren «evaluaciones de impacto» en privacidad, que no dejan de ser análisis de riesgos específicos de ese ámbito. La propia ISO/IEC 27001 es, esencialmente, un marco centrado en la gestión de riesgos de seguridad de la información. Además, es común que clientes corporativos pregunten «¿cómo gestionas tus riesgos de TI?». Poder presentar un registro de riesgos (o un resumen no confidencial) genera confianza y demuestra madurez organizacional.

En resumen, un registro de riesgos funciona como una lista organizada y priorizada de preocupaciones. Ayuda a no pasar por alto posibles problemas y a contar con un plan de acción frente a ellos. Es importante mantenerlo simple y claro. Involucrar a personas de distintas áreas al identificar riesgos es clave, ya que cada una conoce mejor sus procesos y vulnerabilidades. El registro debe revisarse periódicamente (por ejemplo, durante la reunión anual de revisión del SGSI).

No debe verse como un trámite burocrático: es una herramienta práctica para la toma de decisiones. Con el tiempo, la gestión de riesgos se vuelve parte de la cultura organizacional: ante cada nuevo proyecto o cambio, el equipo pensará automáticamente «¿qué riesgos hay aquí?» y «¿cómo los gestionamos?». Ese es el enfoque proactivo que se busca fomentar.

La concientización en seguridad y la implementación de controles son componentes fundamentales de un SGSI. Podemos entenderlos como los elementos «humanos» y «técnicos» que hacen operativa la gestión de la seguridad en el día a día. ISO/IEC 27001 otorga importancia a ambos: por un lado, establece que las personas deben ser conscientes de las políticas, los riesgos y su rol en el sistema (esto se aborda en los apartados de recursos, competencia y comunicación, dentro del capítulo de soporte); por otro lado, el Anexo A presenta un catálogo amplio de controles que deben evaluarse según el contexto de la organización (incluye desde gestión de accesos hasta cifrado, seguridad física, protección contra *malware*, entre otros). Veamos ambos enfoques en más detalle.

Concientización y capacitación

Las mejores políticas y tecnologías no sirven si las personas no las comprenden o, peor aún, las evitan. Muchas brechas de seguridad ocurren por error humano o descuido: hacer clic en un enlace de *phishing*, compartir contraseñas, o configurar mal un sistema por desconocimiento. Por eso, un principio fundamental es educar a todos los miembros de la organización en buenas prácticas de seguridad.

La concientización busca generar cultura: que el personal incorpore la seguridad como parte natural de su trabajo, y no como una obligación externa o molesta. ISO/IEC 27001 establece que la organización debe asegurar que sus empleados comprendan sus responsabilidades en materia de seguridad de la información y la relevancia de cumplirlas.
Un programa básico de concientización en una pyme puede incluir:

- **Inducción al ingresar**. En el proceso de *onboarding*, se explican las políticas de seguridad de la empresa al nuevo empleado. Se le entregan para su lectura (por ejemplo, política de uso aceptable) y se solicita la firma de compromiso.

- **Charlas periódicas o boletines**: por ejemplo, enviar mensualmente un consejo de seguridad por correo electrónico (cómo detectar un *phishing*, evitar conectar dispositivos USB desconocidos, etc.) o realizar reuniones breves trimestrales comentando incidentes recientes («tal empresa fue vulnerada por no usar MFA en RDP; por eso lo exigimos aquí»). Esto mantiene el tema presente en la cultura organizacional.
- **Capacitación formal anual**: muchas pymes organizan un taller anual de una hora repasando los aspectos clave o utilizan plataformas de *e-learning* con cursos básicos de ciberseguridad para empleados (hay opciones gratuitas o de bajo costo).
- **Simulaciones o pruebas internas**: por ejemplo, realizar campañas de *phishing* internas. Se envía un correo simulado a los empleados y se mide quién hace clic; luego se ofrece retroalimentación para mejorar la detección. Esta práctica mejora notablemente la atención ante correos sospechosos.
- **Pósteres o recordatorios visuales**: colocar mensajes de concientización en áreas comunes («no compartas tu contraseña», «piensa antes de hacer clic», etc.), replicando estrategias comunes de seguridad física en el entorno digital.
- **Políticas accesibles**: asegurar que las políticas estén disponibles para todos (por ejemplo, en la intranet o en tablones físicos) y promover su actualización participativa, lo que refuerza el sentido de pertenencia y compromiso.

El objetivo final es que cada persona conozca las buenas prácticas básicas: uso de contraseñas seguras, no compartir credenciales, cómo reportar incidentes o correos sospechosos, precaución con dispositivos externos, manejo adecuado de información confidencial (por ejemplo, no imprimirla y dejarla expuesta, o cifrarla si se envía por correo), entre otras. Además, deben saber qué hacer si ocurre un incidente: ¿a quién deben avisar si pierden una laptop o si detectan un comportamiento anómalo en su equipo? Un personal bien capacitado puede actuar como un «sensor» de incidentes y primera línea de defensa; por ejemplo, un empleado consciente puede detectar a tiempo un intento de fraude gracias a la capacitación recibida.

ISO/IEC 27001, en su capítulo sobre competencia y toma de conciencia, establece que la organización debe definir las competencias necesarias para los roles que afectan la seguridad, brindar capacitación cuando haya brechas y verificar su efectividad. En una pyme, este proceso suele ser más informal, pero no por ello menos relevante. Y no hay que olvidar que la alta dirección también debe ser concientizada. De hecho, en muchos casos los directivos pueden ser los más vulnerables, ya sea por exceso de confianza o por trabajar con apuro. La política de seguridad debe aplicarse también a ellos, y su liderazgo debe reflejarse en el ejemplo: no anotar contraseñas en *post-its* visibles, ni saltarse controles por conveniencia.

Hablamos aquí de las medidas —procedimientos, mecanismos, herramientas— que se implementan para proteger contra los riesgos. ISO/IEC 27001:2022 incluye 93 controles en cuatro grupos; en su versión 2013 tenía 114 controles distribuidos en 14 dominios. Algunos ejemplos de controles son los siguientes: gestión de acceso, cifrado de datos, copias de seguridad, mantenimiento de registros (*logs*), protección contra malware, seguridad física (control de acceso a oficinas o salas de servidores), seguridad en redes, gestión de vulnerabilidades (parcheo), entre otros. La norma no exige aplicar todos los controles, sino únicamente los pertinentes según el análisis de riesgos y su aplicabilidad.

En un SGSI básico para una pyme, los controles comunes podrían incluir los siguientes:

- **Control de acceso lógico**: cada persona con su cuenta individual, privilegios mínimos necesarios, uso de autenticación robusta (contraseñas fuertes + MFA). Revocación inmediata de accesos cuando alguien deja la empresa.
- **Copias de seguridad**: ya tratadas anteriormente; asegurarse de tener respaldos regulares, verificados y almacenados en lugares seguros.

- **Protección contra malware**: contar con antivirus o *antimalware* actualizado en equipos y servidores; uso de firewall —ya sea perimetral o, al menos, el firewall local habilitado en los equipos— y filtros de correo para spam y *phishing*.
- **Gestión de parches**: mantener sistemas y *software* actualizados para cerrar vulnerabilidades conocidas. Muchas infecciones ocurren por equipos desactualizados. Si la empresa no tiene personal de TI dedicado, se puede contratar un servicio o usar herramientas automáticas (como Windows Update).
- **Seguridad física**: proteger físicamente los espacios que alojan equipos críticos —como servidores o routers— mediante cerraduras y control de acceso. Evitar que personas no autorizadas ingresen sin supervisión. Para laptops, usar cables de seguridad o mantenerlas bajo vigilancia.
- **Clasificación de la información**: identificar qué información es confidencial o sensible y etiquetarla; de este modo, se controla su circulación. Por ejemplo, los documentos marcados como «Privado Empresa» no deberían enviarse sin cifrar o sin autorización gerencial.
- **Registro de eventos e incidentes**: activar *logs* en servidores y sistemas clave. Tener un proceso básico para la gestión de incidentes: cómo se reportan, registran, investigan y resuelven. En una pyme, puede llevarlo la misma persona encargada de TI, pero es útil documentar incidentes para aprender de ellos.
- **Seguridad en el desarrollo (si aplica)**: si la empresa desarrolla *software*, debe aplicar controles como revisión de código, uso de repositorios seguros, pruebas de vulnerabilidades, etc. Si no aplica, simplemente se excluye.
- **Relación con terceros**: incluir cláusulas de seguridad en los contratos con proveedores que gestionan información de la empresa. También se pueden exigir estándares mínimos (por ejemplo, que una aplicación en la nube tenga cifrado, backups, certificaciones, etc.).
- **Plan de continuidad**: aunque sea básico, debe contemplar qué hacer ante un incidente mayor. Por ejemplo, si se cae el sistema principal, ¿hay respaldo manual temporal? ¿Se

dispone de los contactos de emergencia de TI? ¿Hay contratado un seguro cibernético? Este control suele ignorarse hasta que ocurre un desastre.

Cada control implementado debe estar documentado en políticas o procedimientos. Por ejemplo, un procedimiento de gestión de cuentas debe indicar cómo se crean nuevas cuentas de usuario, quién las autoriza y cómo se eliminan cuando un empleado deja la empresa. Otro ejemplo es un procedimiento de actualizaciones que establezca que los parches críticos se aplican mensualmente, primero en un entorno de pruebas y luego en producción, dentro de una ventana horaria definida.

La documentación debe ser la mínima necesaria para operar de forma consistente. No se busca generar burocracia, sino establecer reglas claras. ISO/IEC 27001 permite a cada organización decidir qué necesita documentar, pero su principio guía es: «declarar por escrito lo que se hará y cumplirlo».

Es importante destacar que los controles reducen los riesgos, pero no los eliminan completamente. Por esta razón, deben evaluarse periódicamente dentro del ciclo PDCA. Si ocurre un incidente, este debe analizarse para identificar oportunidades de mejora.

Además, la concientización refuerza la eficacia de los controles. Por ejemplo, un sistema técnico puede filtrar correos maliciosos, pero si una persona no está adecuadamente formada, podría igualmente compartir sus credenciales ante un engaño telefónico. De manera inversa, una persona bien capacitada puede detectar una amenaza que el sistema no haya identificado. Por ello, los aspectos técnicos y humanos deben trabajar en conjunto.

En ISO/IEC 27001, al implementar controles, también se espera que se mida su efectividad. Por ejemplo, si se establece un control de «bloqueo tras cinco intentos fallidos de inicio de sesión», se puede monitorear cuántas cuentas se bloquean por esa causa; si el número es excesivo, podría indicar un ataque de fuerza bruta o usuarios que olvidan frecuentemente sus contraseñas. Si se implementa un programa de gestión de parches, resulta útil medir el porcentaje de sistemas actualizados en tiempo. Estas mediciones forman parte de la evaluación del desempeño (capítulo 9).

Para cerrar este apartado, podemos decir que la seguridad de la información requiere tanto personas capacitadas como controles bien diseñados. Ambos elementos deben funcionar en conjunto. La concientización genera una cultura organizacional donde «la seguridad es responsabilidad de todos», y cada miembro colabora activamente para no convertirse en el eslabón débil. Por su parte, los controles proporcionan barreras técnicas y organizativas en múltiples capas.

Una frase comúnmente citada es: «Los usuarios son el eslabón más débil… o la primera línea de defensa». A través de programas de concientización, ese eslabón puede convertirse en un defensor activo. Y mediante controles bien definidos, la organización no depende solo del azar o la buena voluntad, sino que establece mecanismos objetivos para reducir la probabilidad de éxito de un ataque y minimizar su impacto.

Para una pyme, invertir en ambos frentes es factible: educación continua del equipo (en muchos casos gratuita o de bajo costo), y selección estratégica de controles, priorizando aquellos más relevantes según los riesgos identificados.

Una correcta definición de roles y responsabilidades en seguridad es esencial para evitar confusiones y omisiones. Todos en la organización deben saber qué se espera de ellos en materia de seguridad —lo cual logramos en parte mediante políticas y acciones de concientización—, pero además, al implementar y operar controles o responder a incidentes, conviene asignar responsables claros para cada tarea. Aquí entra en juego la matriz RACI, una herramienta útil de gestión que aclara las responsabilidades dentro de actividades o procesos.

¿Qué es la matriz RACI?

RACI son las siglas de cuatro posibles roles que una persona o grupo puede tener respecto a una tarea o decisión: responsable, aprobador (*accountable* en inglés), consultado e informado. La matriz RACI se presenta como una tabla donde en las filas se listan tareas o entregables, y en las columnas, los roles o personas; en la intersección se marca si alguien es R, A, C o I para esa tarea. A continuación se explican los cuatro roles:

- **R = Responsable.** Quien ejecuta el trabajo necesario para completar la tarea. Puede haber varios responsables o solo uno por tarea. Son quienes realizan la acción.
- **A = Aprobador (*accountable*)**: quien tiene la última palabra y autoridad sobre la tarea, y asume la responsabilidad final de que se complete con éxito. Debe haber solo un «A» por tarea para evitar ambigüedades. Este rol puede coincidir con el «R» si la tarea es pequeña.
- **C = Consultado**: personas que deben ser consultadas antes de ejecutar la tarea, ya que su opinión o experiencia es relevante. La comunicación con ellas es bidireccional.
- **I = Informado**: personas que deben ser notificadas del avance o resultado de la tarea. No participan en la ejecución ni en la toma de decisiones. La comunicación con ellas es unilateral.

Aplicado a la seguridad y cumplimiento, una matriz RACI ayuda a clarificar quién hace qué en el SGSI o en proyectos de seguridad. Por ejemplo, supongamos la tarea «realizar evaluación de riesgos anual». En este caso, podríamos asignar «R» = analista de seguridad (porque recopila la información y llena el registro); «A» = gerente de TI (porque aprueba el informe final de riesgos); «C» = jefe de cada área (se les consulta sobre riesgos en sus procesos); «I» = director general (debe estar informado sobre los mayores riesgos identificados). De este modo, nadie se confunde: el analista sabe que debe conducir el trabajo, los jefes de área entienden que deben responder consultas, etc.

Implementación ISO 27001 con RACI

Un proyecto de implementación de ISO/IEC 27001 también puede beneficiarse del uso de una matriz RACI. Como vimos, la implantación de la norma involucra a diferentes personas con distintos roles según la etapa del proyecto. Por ejemplo, al comienzo, la alta dirección debe aprobar el proyecto, por lo que se la considera como el aprobador («A») en esa fase, mientras que un consultor o responsable de seguridad puede ser el responsable («R») de planificar. Más adelante, los jefes de departamento podrían asumir el rol de responsables o aprobadores («R» o «A») en la implementación de controles específicos dentro de sus áreas. Finalmente, una vez implementado el SGSI, el resto de la organización suele estar en el rol de informado («I»).

Una vez que la dirección ha dado luz verde al proyecto, no es necesario incluirla como aprobadora en cada tarea menor, ya que ha delegado la responsabilidad operativa en el equipo de implementación. Esto evita complejidad innecesaria en la matriz RACI y permite enfocarse en quién realmente ejecuta o participa en cada actividad concreta del sistema de gestión.

Matriz RACI de ejemplo (seguridad de la información)

Imaginemos una pequeña tabla RACI para algunas actividades recurrentes del SGSI en una pyme:

Tabla 2. Ejemplo de matriz RACI

Actividad	Responsable (R)	Aprobador (A)	Consultado (C)	Informado (I)
Definir políticas de seguridad	Encargado de Seguridad	Director general	Jefe de Sistemas, Legal	Todos los empleados (I de la política)

Gestionar copias de seguridad	Técnico de TI	Gerente de TI	Usuario clave de cada área (para priorizar datos)	Auditor Interno (quiere saber cumplimiento)
Monitorear eventos e incidentes	Analista SOC (externo)	Encargado de seguridad	Jefe de TI (si técnico externo)	Director (incidentes graves)
Auditoría interna anual SGSI	Auditor interno (externo o no)	Director general (recibe reporte)	Gerente de TI, encargado de seguridad (apoyan info)	Responsables de áreas auditadas (se les informa hallazgos)
Respuesta a incidente crítico	Equipo de respuesta (por ejemplo, CSIRT externo)	Director General (toma decisiones finales)	Gerente TI, encargado de seguridad, legal (según incidente)	Empleados (si afecta operaciones, se les informa situación)

Fuente: elaboración propia.

Este es solo un ejemplo inventado. Lo importante es asignar un «A» claro para cada tarea (es decir, quién tiene la responsabilidad última). Por ejemplo, en la gestión de respaldos, el gerente de TI sería el «A» porque debe asegurarse de que se cumplan adecuadamente, mientras que el técnico de TI sería el «R», es decir, quien los ejecuta.

Roles típicos en SGSI —

En pymes, una misma persona muchas veces desempeña varios roles. Aun así, conviene definir esos «sombreros». Por ejemplo: el rol de propietario de un activo («owner») suele asignarse a quien tiene la responsabilidad sobre la información. En una pyme, puede ocurrir que el owner de la base de datos de clientes sea el gerente comercial —porque es su información— aunque TI administre la base. TI actúa como custodio, implementa controles, pero el propietario decide quién accede, etc. Todo esto puede aclararse con una matriz RACI: por ejemplo, para el activo «BD de clientes», el gerente comercial sería «A» (responsable último), TI sería «R» (administración), Legal podría ser «C» (consultado para cumplir normativas de privacidad) y la dirección sería «I» (informada del estado).

La matriz RACI también ayuda a identificar vacíos o redundancias. Si para una tarea no hay nadie asignado como «R», esa tarea podría no realizarse porque cada quien piensa que la hace otro. Si hay dos «A» para una misma tarea, puede haber choques o demoras —es mejor que haya uno solo. Con RACI se asignan responsabilidades claras y se evitan cabos sueltos.

Aunque la norma no mencione explícitamente «matriz RACI», sí exige que las responsabilidades de seguridad estén definidas con claridad. Para cumplir ese requisito (cláusula 5.3) puede utilizarse RACI, documentando quién hace qué. Muchas implementaciones de ISO/IEC 27001 usan esta matriz como forma práctica de demostrar organización clara de roles. Incluso si no buscamos certificación, RACI resulta útil para coordinar tareas de seguridad de forma simple y efectiva.

Implementando RACI en una empresa —

El primer paso consiste en listar los procesos o tareas clave en materia de seguridad (por ejemplo: gestión de accesos, parches, incidentes, cumplimiento legal, etc.). Para cada uno, se deben asignar los roles: quién planifica, quién ejecuta, quién aprueba resultados, quién

debe ser consultado y quién debe estar informado. Es recomendable involucrar a los responsables de cada área para asegurar acuerdo y claridad. Una vez definida, la matriz debe comunicarse a todos los implicados. Esto evita situaciones como «pensaba que otra persona lo hacía» o «no sabía que era responsabilidad propia».

Un aspecto importante es evitar complicaciones innecesarias. En organizaciones pequeñas, no se requiere una matriz extensa: puede bastar con dejarlo establecido en las políticas internas o en las descripciones de roles. Por ejemplo, «el responsable de seguridad de la Información (RSI) estará a cargo de...», «la gerencia debe aprobar...», «el personal deberá...». A medida que aumentan la complejidad o los proyectos transversales, la matriz se vuelve más útil.

En conclusión, roles definidos implican responsabilidades claras. Cuando cada tarea cuenta con un responsable y un aprobador definidos, se minimizan los vacíos operativos. La matriz RACI es una herramienta eficaz para documentar esta asignación. Recordando sus siglas —R (responsable), A (aprobador), C (consultado), I (informado)—, se recomienda verificar que cada actividad crítica esté cubierta de forma adecuada. De este modo, el sistema de gestión funcionará de forma coordinada y sin solapamientos.

CONTINUAR

Referencias

INCIBE. (2019). *¿Sabías que el 90% de las contraseñas son vulnerables?* https://www.incibe.es/ciudadania/blog/sabias-que-el-90-de-las-contrasenas-son-vulnerables INCIBE

Kaspersky. (2025). *Amenaza vintage asedia a América Latina: el phishing afecta a 43 % de las pymes de la región*. Kaspersky América Latina. https://latam.kaspersky.com/about/press-releases/amenaza-vintage-asedia-a-america-latina-el-phishing-afecta-a-43-de-las-pymes-de-la-region

Organización Internacional de Normalización. (2022). *Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos (ISO/IEC 27001:2022)*. https://www.iso.org/es/norma/27001

Velandia, J. J., Liberato Robayo, N. G., Tinjaca Garzón, J. C., & Chaverra Córdoba, C. A. (2023). *Diseño de instrumentos que garanticen la calidad y mejores prácticas en el desarrollo de software para las pequeñas y medianas empresas de Bogotá* [Trabajo de pregrado, Universidad EAN]. https://repository.universidadean.edu.co/server/api/core/bitstreams/0647b1d0-47ae-47d3-b4ac-1b97deab45f7/contentf

CONTINUAR