ISO/IEC 27001:2022 + Amd 1:2024 Sistemas de Gestión de la Seguridad de la Información (SGSI)

Seguridad de la información, SGSI, certificable en todo el mundo

181 requisitos. Esta norma es certificable por un organismo acreditado. Versión de 07/2026.

La norma ISO/IEC 27001 establece los requisitos para un sistema de gestión de la seguridad de la información: basado en riesgos, documentado y con eficacia demostrable. Una evaluación conforme a ella es una auditoría de certificación acreditada en dos fases (revisión documental y después revisión de eficacia in situ), seguida de auditorías de seguimiento anuales y de recertificación a los tres años.

Empresa	Fecha	Elaborado por

4 Contexto de la organización 8

4.1-1 **Se determinan y se mantienen actualizadas las cuestiones externas e internas que afectan a la capacidad de la organización para lograr los resultados previstos del SGSI.**

Cómo se demuestra: Se demuestra mediante un análisis de contexto, ya sea como documento independiente o como apartado del manual del SGSI: entorno de mercado, situación de clientes y contratos, marco legal (RGPD, NIS2), pila tecnológica, plantilla, dependencia de proveedores en la nube. Para organizaciones pequeñas basta una tabla de una página con fecha y ciclo de revisión, siempre que la revisión por la dirección demuestre que se actualiza realmente.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

4.1-2 **La organización ha determinado si el cambio climático es una cuestión relevante para ella. La determinación está justificada, tanto si la respuesta es afirmativa como negativa.**

Cómo se demuestra: Este requisito lo introdujo la Amd 1:2024 y los auditores lo piden específicamente. Mantenga una fila dedicada en el análisis de contexto: periodos de calor que afectan a las salas de servidores y a la disponibilidad, fenómenos meteorológicos extremos que afectan a los centros de datos de los proveedores en la nube, estabilidad de la red eléctrica. Un resultado justificado de no relevante es aceptable, una entrada ausente no lo es.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

4.2-1 **Se determinan las partes interesadas que son relevantes para el SGSI.**

Cómo se demuestra: Lista de partes interesadas que cubre clientes, personal, encargados y subencargados del tratamiento, autoridades de supervisión, aseguradoras, el organismo de certificación y los accionistas. En organizaciones pequeñas basta una tabla con parte interesada, expectativa y origen de la expectativa.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

4.2-2 **Se determinan los requisitos relevantes de estas partes interesadas, incluyendo cualquier requisito relacionado con el cambio climático.**

Cómo se demuestra: Para cada parte interesada indique la fuente concreta: cláusula contractual, acuerdo de tratamiento de datos, cuestionario de cliente, obligación legal. La Amd 1:2024 añade una nota según la cual las partes interesadas pueden tener requisitos relacionados con el cambio climático. No es un requisito deberá independiente, pero los auditores lo plantean con frecuencia, por ejemplo preguntas de sostenibilidad en la auditoría de proveedores de un cliente importante. Basta una fila en la tabla de partes interesadas con el resultado, incluyendo ninguno de ese tipo.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

4.2-3 **Se decide y queda trazable cuáles de estos requisitos se abordan a través del SGSI.**

Cómo se demuestra: Añada una columna a la tabla de partes interesadas que remita a la regla que aborda el requisito (política, control, anexo contractual). Esto demuestra que los requisitos no solo se recopilaron, sino que además se procesaron de verdad.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

4.3-1 **Se determina el alcance del SGSI teniendo en cuenta las cuestiones del apartado 4.1, los requisitos del apartado 4.2, así como las interfaces y dependencias con actividades realizadas por terceros.**

Cómo se demuestra: El alcance nombra sedes, unidades organizativas, productos, sistemas y límites de red. Las partes externalizadas (alojamiento, proveedores de pago, soporte) se describen como interfaces con un límite de responsabilidad claro. Un alcance recortado artificialmente que excluya procesos centrales es rechazado por los organismos de certificación.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

4.3-2 **El alcance está disponible como información documentada e indica de forma inequívoca los límites del SGSI.** Documento

Cómo se demuestra: Un documento de alcance aprobado con versión, fecha y visto bueno de la alta dirección. Su redacción exacta aparecerá después en el certificado, por lo que conviene formularlo con precisión y de forma que se pueda citar públicamente.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

4.4-1 **El SGSI, incluidos los procesos necesarios y sus interacciones, se establece, implementa, mantiene y mejora de forma continua.**

Cómo se demuestra: Un mapa de procesos o una lista de procesos que vincule la gestión de riesgos, la gestión de incidentes, la gestión de cambios, la auditoría y la revisión por la dirección con propietarios y frecuencia. La evidencia viva importa más que el diagrama: tickets, actas, entradas de calendario.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

5 Liderazgo 8

5.1-1 **La alta dirección asume la responsabilidad de la eficacia del SGSI y garantiza que la política y los objetivos se establecen y son compatibles con la dirección estratégica.**

Cómo se demuestra: La evidencia incluye aprobaciones firmadas de la política, del alcance y de la Declaración de Aplicabilidad, actas de la revisión por la dirección y decisiones presupuestarias documentadas. En organizaciones muy pequeñas, la alta dirección suele coincidir con el propietario del SGSI, lo cual es aceptable pero debe indicarse abiertamente en la definición del rol.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

5.1-2 **Los requisitos del SGSI se integran en los procesos de negocio y se comunica la importancia de una seguridad de la información eficaz.**

Cómo se demuestra: Se demuestra mejor cuando la seguridad no es una carpeta aparte: un criterio de seguridad en la definición de terminado, una comprobación de seguridad en el proceso comercial o de compras, un punto recurrente de seguridad en las actas de reunión de equipo.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

5.1-3 **La dirección proporciona los recursos necesarios, apoya a las personas que contribuyen a la eficacia del SGSI y promueve la mejora continua.**

Cómo se demuestra: Presupuesto de seguridad aprobado, tiempo asignado para formación, contratación de auditores externos o de pruebas de penetración. Un registro de mejoras o de acciones con entradas de varios trimestres demuestra continuidad y no un esfuerzo puntual.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

5.2-1 **Se establece una política de seguridad de la información apropiada al propósito de la organización que proporciona un marco para los objetivos de seguridad de la información.** Documento

Cómo se demuestra: Un documento de política breve y aprobado, con dos o tres páginas es suficiente. Nombra los objetivos de protección, el alcance, las responsabilidades y el principio del enfoque basado en riesgos. Un texto de plantilla genérico sin vínculo con el negocio real destaca negativamente en la auditoría.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

5.2-2 **La política incluye un compromiso de satisfacer los requisitos aplicables y un compromiso de mejora continua del SGSI.** Documento

Cómo se demuestra: Ambos compromisos deben aparecer como frases explícitas en la política, y se leen literalmente en la auditoría de fase 1. Además, remita a los procesos subyacentes (registro legal, registro de mejoras).

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

5.2-3 **La política se comunica dentro de la organización y está disponible para las partes interesadas según proceda.** Documento

Cómo se demuestra: Evidencia mediante una entrada en la intranet o en el wiki con obligación de lectura, una lista de comprobación de incorporación con confirmación, o un resumen publicado en el sitio web. Una lista de distribución con acuses de recibo es la prueba sólida más sencilla.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

5.3-1 **Las responsabilidades y autoridades para los roles relevantes en materia de seguridad se asignan y se comunican dentro de la organización.**

Cómo se demuestra: Una matriz de roles (RACI) que cubra al propietario del SGSI, a los propietarios de riesgos, a los propietarios de activos, al coordinador de incidentes y al contacto de protección de datos. En equipos unipersonales o muy pequeños, asigne cada rol a una persona nombrada y documente abiertamente la acumulación de roles resultante en lugar de ocultarla.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

5.3-2 **La autoridad para garantizar que el SGSI cumple con la norma y para informar del desempeño del SGSI a la alta dirección se asigna a un rol.**

Cómo se demuestra: Una carta de nombramiento o una descripción de rol para el propietario del SGSI con una línea de reporte explícita a la dirección. La línea de reporte debe quedar realmente evidenciada en las actas de la revisión por la dirección.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

6 Planificación 21

6.1.1-1 **Partiendo de las cuestiones del apartado 4.1 y de los requisitos del apartado 4.2, se determinan los riesgos y oportunidades que es necesario abordar, de modo que el SGSI logre los resultados previstos y se prevengan los efectos no deseados.**

Cómo se demuestra: Un registro que vincule las cuestiones de contexto con riesgos y oportunidades, mantenido por separado o dentro del registro de riesgos. Lo importante es la trazabilidad: cada cuestión del análisis de contexto debe conducir visiblemente a una evaluación o a una decisión justificada de no considerarla.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

6.1.1-2 **Se planifican las acciones para abordar estos riesgos y oportunidades, se integran en los procesos del SGSI y se evalúa su eficacia.**

Cómo se demuestra: Plan de acción con propietario, fecha límite y criterio de eficacia. Mantenga la evaluación de eficacia como columna propia, de lo contrario la auditoría carecerá de prueba de que la acción no solo se implementó, sino que también se verificó.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

6.1.2-1 **Se define y se aplica un proceso de evaluación de riesgos de seguridad de la información; incluye criterios de aceptación del riesgo y criterios para realizar las evaluaciones de riesgos.** Documento

Cómo se demuestra: Una política de gestión de riesgos con escalas de probabilidad e impacto, una matriz de riesgo definida y un umbral de aceptación claro. El umbral debe ser un número o una zona, no una frase como a nuestro criterio.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

6.1.2-2 **El proceso garantiza que evaluaciones de riesgos repetidas produzcan resultados coherentes, válidos y comparables.**

Cómo se demuestra: Se demuestra mediante una metodología fija con escalas definidas y comparando dos versiones de la evaluación: mismos riesgos, misma lógica de valoración, diferencias explicables. Una versión fechada del registro de riesgos del año anterior es la evidencia más sólida en este punto.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

6.1.2-3 **Se identifican los riesgos de seguridad de la información para detectar la pérdida de confidencialidad, integridad y disponibilidad dentro del alcance, y se asigna un propietario del riesgo a cada riesgo.**

Cómo se demuestra: Registro de riesgos que referencia activos o procesos, los tres objetivos de protección y un propietario del riesgo nombrado. El propietario del riesgo debe tener la autoridad para aceptarlo; en organizaciones pequeñas suele ser el gerente.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

6.1.2-4 **Se analizan los riesgos identificados: se determinan las consecuencias potenciales, la probabilidad realista y el nivel de riesgo resultante.**

Cómo se demuestra: Columnas para impacto, probabilidad y nivel de riesgo resultante, cada una con una breve justificación. Una frase de razonamiento por riesgo evita el hallazgo de auditoría más habitual, es decir, cifras sin derivación.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

6.1.2-5 **Los riesgos se comparan con los criterios de aceptación y se priorizan para su tratamiento.**

Cómo se demuestra: El registro de riesgos debe mostrar qué riesgos superan el umbral de aceptación y en qué orden se tratarán. Basta con una vista ordenada o una columna de prioridad.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

6.1.2-6 **El proceso de evaluación de riesgos está disponible como información documentada.** Documento

Cómo se demuestra: La propia metodología es un documento obligatorio, no solo su resultado. Una política aprobada con versión y fecha de aprobación, enlazada desde el índice de documentos del SGSI.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

6.1.3-1 **Para cada riesgo que supere el umbral de aceptación se selecciona una opción de tratamiento adecuada (reducir, evitar, transferir o aceptar).**

Cómo se demuestra: Una columna de opción de tratamiento en el registro de riesgos. Cuando se acepta un riesgo, registre la justificación y la aprobación formal del propietario del riesgo; cuando se transfiere, indique el contrato o la póliza de seguro.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

6.1.3-2 **Se determinan todos los controles necesarios para implementar las opciones de tratamiento de riesgos elegidas.**

Cómo se demuestra: Formule los controles de manera concreta y verificable, con propietario y fecha límite. Es válido remitir a trabajo técnico ya en marcha (implantación de MFA, prueba de copias de seguridad), siempre que apunte a un ticket o a un artefacto de configuración.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

6.1.3-3 **Los controles determinados se comparan con los controles del anexo A para verificar que no se ha pasado por alto ningún control necesario.**

Cómo se demuestra: La comparación es un paso propio y trazable, no un subproducto. Se evidencia mediante una columna de correspondencia en el registro de riesgos que referencia los números del anexo A, junto con un acta fechada de la comparación.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

6.1.3-4 **Existe una Declaración de Aplicabilidad (SoA). Evalúa individualmente los 93 controles del anexo A, indica la aplicabilidad con justificación para cada control, el estado de implementación y la justificación de cada exclusión.** Documento

Cómo se demuestra: La Declaración de Aplicabilidad es el documento obligatorio central y el mapa de toda la auditoría. Debe ser completa: los controles no aplicables también aparecen con una justificación, nunca como una línea en blanco. Columnas recomendadas: número de control, título, aplicable sí o no, justificación, estado de implementación, referencia a la política o evidencia, enlace al riesgo. La versión y la aprobación de la dirección son obligatorias, porque la Declaración de Aplicabilidad se contrasta con la realidad en cada auditoría de seguimiento.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

6.1.3-5 **Se elabora un plan de tratamiento de riesgos que reúne controles, responsabilidades, fechas límite y recursos necesarios.** Documento

Cómo se demuestra: Puede ser una pestaña en la hoja de cálculo de riesgos o un tablero de proyecto. Lo que cuenta es que las fechas sean realistas y que los plazos incumplidos se hayan replanificado de forma visible, porque eso es precisamente lo que comprueba el auditor.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

6.1.3-6 **El plan de tratamiento de riesgos es aprobado por los propietarios de los riesgos y estos aceptan formalmente los riesgos residuales restantes.** Documento

Cómo se demuestra: Firma, aprobación electrónica o una decisión fechada en un acta. Basta una línea en el acta de la revisión por la dirección que remita a la versión del registro, siempre que la versión sea inequívoca.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

6.1.3-7 **El proceso de tratamiento de riesgos está disponible como información documentada.** Documento

Cómo se demuestra: Normalmente se cubre en el mismo documento de política que la evaluación de riesgos. Debe describirse el flujo desde la evaluación, pasando por la selección de opciones, hasta la aceptación del riesgo residual.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

6.2-1 **Se establecen objetivos de seguridad de la información para las funciones y niveles relevantes, son coherentes con la política y son medibles cuando es posible.**

Cómo se demuestra: Una hoja de objetivos con entre tres y seis objetivos, cada uno con un indicador, un valor de partida, un valor meta y un plazo. Ejemplo: proporción de sistemas con MFA aumentada del 80 al 100 por ciento antes de que finalice el trimestre. Los objetivos sin cifra no cuentan como medibles.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

6.2-2 **Los objetivos tienen en cuenta los requisitos de seguridad de la información aplicables, así como los resultados de la evaluación y el tratamiento de riesgos.**

Cómo se demuestra: Añada una columna de origen a la hoja de objetivos: de qué riesgo, qué requisito de cliente o qué obligación legal procede el objetivo. Esto evita objetivos que parezcan arbitrarios.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

6.2-3 **Los objetivos se supervisan, se comunican y se actualizan cuando es necesario.**

Cómo se demuestra: Seguimiento trimestral del progreso en la hoja de objetivos, junto con la comunicación al equipo, por ejemplo una breve nota en el wiki o un punto en el orden del día de la reunión de equipo. Las versiones históricas demuestran que las actualizaciones ocurren realmente.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

6.2-4 **Los objetivos de seguridad de la información están disponibles como información documentada.** Documento

Cómo se demuestra: Basta un documento de objetivos aprobado y con fecha. Puede formar parte de la revisión por la dirección, pero debe existir allí como un apartado propio y recuperable.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

6.2-5 **Para cada objetivo se planifica qué se va a hacer, qué recursos se requieren, quién es responsable, cuándo se completará y cómo se evaluarán los resultados.**

Cómo se demuestra: Estos cinco puntos son verificables de forma individual y se preguntan de forma individual en la auditoría. Configúrelos como cinco columnas en la hoja de objetivos, así la conformidad se ve de un vistazo.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

6.3-1 **Cuando la organización determina que son necesarios cambios en el SGSI, estos cambios se llevan a cabo de forma planificada.**

Cómo se demuestra: Se evidencia mediante solicitudes de cambio, actas o tickets que muestren el desencadenante, la evaluación de impacto, la aprobación y la implementación. Desencadenantes típicos en organizaciones pequeñas: cambio de proveedor en la nube, nuevas sedes, la primera contratación.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

7 Apoyo 15

7.1-1 **Se determinan y se proporcionan los recursos necesarios para el establecimiento, la implementación, el mantenimiento y la mejora continua del SGSI.**

Cómo se demuestra: Una partida presupuestaria de seguridad, licencias de herramientas (gestor de contraseñas, MDM, plataforma de registros), días persona planificados para el mantenimiento del SGSI y servicios de auditoría externa. Una factura o una aprobación de presupuesto lo demuestra más rápido que cualquier texto.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

7.2-1 **Se determina la competencia necesaria de las personas cuyo trabajo afecta al desempeño de la seguridad de la información.**

Cómo se demuestra: Matriz de competencias o perfiles de rol que enumeren el conocimiento requerido por rol, por ejemplo desarrollo seguro para los desarrolladores, gestión de incidentes para el coordinador. En equipos muy pequeños basta una fila por persona.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

7.2-2 **La competencia se garantiza sobre la base de una educación, formación o experiencia apropiadas.**

Cómo se demuestra: Certificados, confirmaciones de cursos, currículums o experiencia práctica documentada. El autoaprendizaje es aceptable si está evidenciado, por ejemplo mediante registros de finalización de cursos en línea o pruebas de conocimiento internas superadas.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

7.2-3 **Cuando existen carencias de competencia, se han tomado medidas para cerrarlas y se ha evaluado la eficacia de esas medidas.**

Cómo se demuestra: Plan de formación con una comparación entre lo previsto y lo realizado, y una comprobación de eficacia, por ejemplo una nota de examen, una tasa de clics en una simulación de phishing o una observación en el puesto de trabajo. La comprobación de eficacia se olvida con frecuencia y es un hallazgo menor clásico.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

7.2-4 **Se dispone de información documentada apropiada como evidencia de la competencia.** Documento

Cómo se demuestra: Una carpeta de competencia o formación por persona con evidencias y fechas. En organizaciones pequeñas basta un directorio con los registros en PDF guardados más una tabla resumen.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

7.3-1 **Las personas que trabajan dentro del alcance son conscientes de la política de seguridad de la información.**

Cómo se demuestra: Confirmación en la incorporación y tras cada cambio de la política, con fecha y versión. Una función de acuse de recibo en el wiki o una lista firmada es suficiente.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

7.3-2 **Las personas conocen su propia contribución a la eficacia del SGSI y los beneficios de una mejora del desempeño de la seguridad de la información.**

Cómo se demuestra: Material de formación y listas de asistencia en las que se vea el vínculo con el propio trabajo de la persona. Los auditores entrevistan directamente al personal, por lo que conviene formar con ejemplos concretos del día a día en lugar de citas abstractas de la norma.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

7.3-3 **Las personas conocen las consecuencias de no cumplir con los requisitos del SGSI.**

Cómo se demuestra: Indique las consecuencias en las diapositivas de formación y en las instrucciones de trabajo, y vincúlelas al proceso del apartado A.6.4. Incluso las organizaciones sin personal en plantilla deben cubrir esto para contratistas y autónomos a través de sus contratos.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

7.4-1 **Se determina la comunicación interna y externa relevante para el SGSI: qué se comunica, cuándo, con quién y por qué medios.**

Cómo se demuestra: Una matriz de comunicación con filas como incidente de seguridad a clientes, notificación a la autoridad de supervisión en el plazo de 72 horas, informe mensual de estado a la dirección. Es la base de la comunicación de crisis y se revisa tras cada incidente.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

7.5.1-1 **El SGSI incluye la información documentada requerida por la norma, así como la información documentada que la organización ha determinado que es necesaria para la eficacia del SGSI.** Documento

Cómo se demuestra: Un índice de documentos que enumere cada documento del SGSI con propósito, propietario, versión y ubicación de almacenamiento. Demuestra que los documentos obligatorios están completos y es el punto de entrada más rápido para el auditor.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

7.5.2-1 **Al crear y actualizar documentos, se garantizan una identificación, un formato y un soporte apropiados, y los documentos se revisan y aprueban en cuanto a su idoneidad.**

Cómo se demuestra: Un encabezado de documento uniforme con título, versión, fecha, autor y aprobador. En entornos basados en Git, las revisiones de pull request con aprobación satisfacen el requisito de revisión y aprobación, siempre que el historial sea inmutable.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

7.5.3-1 **La información documentada está disponible y es adecuada para su uso donde y cuando se necesita.**

Cómo se demuestra: Una ubicación de almacenamiento central accesible para todas las personas autorizadas, con función de búsqueda. Se puede comprobar mediante muestreo: cualquier instrucción de trabajo dada debe poder encontrarse en menos de un minuto.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

7.5.3-2 **La información documentada está adecuadamente protegida, en particular contra la pérdida de confidencialidad, el uso indebido y la pérdida de integridad.**

Cómo se demuestra: Derechos de acceso basados en roles a los documentos del SGSI, versionado con historial, protección contra escritura para las versiones aprobadas y una copia de seguridad del repositorio de documentos. La evidencia de la copia de seguridad es la parte que más se olvida.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

7.5.3-3 **Se regulan la distribución, el acceso, la recuperación, el almacenamiento, el control de cambios, así como la conservación y disposición de la información documentada.**

Cómo se demuestra: Una breve regla de control documental con plazos de conservación y reglas de eliminación. Debe conciliarse con las obligaciones legales (derecho mercantil, derecho fiscal, RGPD) y es la base para los apartados A.5.33 y A.8.10.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

7.5.3-4 **Se identifica y controla la información documentada de origen externo que es necesaria para planificar y operar el SGSI.**

Cómo se demuestra: Una lista de documentos externos con versión y fuente: normas, textos legales, guías de bastionado de proveedores, documentación de seguridad en la nube, acuerdos de tratamiento de datos. Sin una referencia de versión no se puede demostrar el control.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

8 Operación 8

8.1-1 **Se planifican, implementan y controlan los procesos necesarios para cumplir los requisitos de seguridad de la información y para implementar las acciones del apartado 6, y se establecen criterios para dichos procesos.**

Cómo se demuestra: Un manual de operaciones o runbooks con criterios claros, por ejemplo el tiempo máximo para desplegar parches críticos, criterios de liberación para los despliegues, umbrales de alerta. Los criterios sin cifras no valen nada en la auditoría.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

8.1-2 **Se dispone de información documentada en la medida necesaria para tener confianza en que los procesos se han llevado a cabo según lo planificado.** Documento

Cómo se demuestra: Registros operativos como evidencia: historial de tickets, ejecuciones del pipeline de integración continua, informes de parches, registros de copias de seguridad, revisiones de acceso. Estos registros son la prueba real de eficacia en la auditoría de fase 2.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

8.1-3 **Se controlan los cambios planificados y se revisan las consecuencias de los cambios no previstos; cuando es necesario, se mitigan los efectos adversos.**

Cómo se demuestra: Un proceso de cambios con aprobación y una vía de reversión, vinculado al apartado A.8.32. En el caso de cambios no previstos (configuración errónea, escalada accidental de privilegios), documente el incidente y evidencie la corrección.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

8.1-4 **Se determinan y controlan los procesos, productos y servicios proporcionados externamente que son relevantes para el SGSI.**

Cómo se demuestra: Una lista de proveedores con criticidad, referencia contractual y el estado de la evidencia (el certificado ISO 27001 del proveedor, el informe SOC 2, el acuerdo de tratamiento de datos). Para las organizaciones pequeñas es la palanca más importante, porque la mayor parte de las TI se ejecuta externamente de todos modos.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

8.2-1 **Se realizan evaluaciones de riesgos a intervalos planificados y siempre que se produzcan cambios o incidentes significativos, teniendo en cuenta los criterios establecidos.**

Cómo se demuestra: Un ritmo (normalmente anual) más desencadenantes definidos para evaluaciones no programadas. Se evidencia mediante versiones fechadas del registro de riesgos y entradas en el calendario o en el sistema de tickets.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

8.2-2 **Los resultados de las evaluaciones de riesgos se conservan como información documentada.** Documento

Cómo se demuestra: Versiones históricas del registro de riesgos con fechas, no solo el estado actual. Sobrescribir el archivo hace imposible demostrar la evolución; el versionado en el sistema de archivos o en Git resuelve esto.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

8.3-1 **Se implementa el plan de tratamiento de riesgos.**

Cómo se demuestra: Compare el plan con la realidad: acciones completadas con fecha de implementación y un artefacto concreto (configuración, política, contrato). Las acciones abiertas necesitan una justificación documentada y una nueva fecha meta.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

8.3-2 **Los resultados del tratamiento de riesgos se conservan como información documentada.** Documento

Cómo se demuestra: Informes de estado o acciones cerradas con una referencia a la evidencia. Basta con el propio registro si cada fila lleva una fecha de finalización y un enlace a la evidencia.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

9 Evaluación del desempeño 21

9.1-1 **Se determina qué es necesario supervisar y medir, incluyendo los procesos y controles de seguridad de la información.**

Cómo se demuestra: Una hoja de indicadores con un número manejable de medidas sólidas: acumulación de parches pendientes, cobertura de MFA, tiempo de resolución de incidentes, resultado de la última prueba de restauración, hallazgos abiertos. Unos pocos indicadores que realmente se recopilan valen más que una lista de deseos larga.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

9.1-2 **Se definen los métodos de seguimiento, medición, análisis y evaluación, y producen resultados válidos.**

Cómo se demuestra: Documente la fuente de datos y el cálculo de cada indicador, por ejemplo una exportación del escáner de vulnerabilidades o del informe del proveedor de identidad. La trazabilidad de la fuente es el núcleo de la validez.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

9.1-3 **Se define cuándo y por quién se realizan el seguimiento y la medición, y cuándo se analizan y evalúan los resultados.**

Cómo se demuestra: Añada columnas de frecuencia y propietario a la hoja de indicadores. Una cita recurrente en el calendario para la evaluación demuestra la regularidad mejor que cualquier descripción.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

9.1-4 **Los resultados del seguimiento y la medición se conservan como información documentada.** Documento

Cómo se demuestra: Evaluaciones archivadas, paneles exportados o una hoja de indicadores mantenida como serie temporal. Una vista en vivo sin histórico no satisface el requisito.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

9.1-5 **El desempeño de la seguridad de la información y la eficacia del SGSI se evalúan sobre la base de los resultados de la medición.**

Cómo se demuestra: Una evaluación escrita, no solo cifras: tendencia, causas, necesidad de actuar. Este texto de evaluación es a la vez una entrada para la revisión por la dirección.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

9.2.1-1 **Se realizan auditorías internas a intervalos planificados y aportan información sobre si el SGSI cumple con los requisitos propios de la organización y con los requisitos de la norma, y si está implementado eficazmente.**

Cómo se demuestra: Antes de la auditoría de certificación debe completarse al menos un ciclo completo de auditoría interna que cubra todo el alcance. Sin ello, la certificación queda fuera de alcance; este es uno de los obstáculos más habituales en las primeras certificaciones.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

9.2.2-1 **Se planifica, establece y mantiene un programa de auditoría; define la frecuencia, los métodos, las responsabilidades, los requisitos de planificación y la elaboración de informes, y tiene en cuenta la importancia de los procesos en cuestión y los resultados de auditorías anteriores.**

Cómo se demuestra: Un programa de auditoría plurianual que cubra todos los apartados y todos los controles aplicables a lo largo del ciclo de certificación, con mayor frecuencia para las áreas críticas. Una simple tabla a tres años es totalmente suficiente.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

9.2.2-2 **Se definen los criterios de auditoría y el alcance de la auditoría para cada auditoría.**

Cómo se demuestra: Un plan de auditoría por fecha con los criterios (la norma, las políticas internas, los contratos) y un alcance claro. Un plan de auditoría de una página por auditoría es suficiente y sirve además como base del informe.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

9.2.2-3 **Los auditores se seleccionan y las auditorías se realizan de forma que se garanticen la objetividad y la imparcialidad. Nadie audita su propio trabajo.**

Cómo se demuestra: La independencia es el obstáculo más exigente aquí: quien redactó las políticas y configuró los sistemas no puede auditarlos. En organizaciones muy pequeñas esto casi siempre implica un auditor interno externo, por ejemplo un consultor contratado o un compañero de una empresa colaboradora; un contrato de auditoría más la declaración de independencia del auditor son la evidencia. Solo en equipos suficientemente grandes se puede rotar el rol internamente hacia una persona sin responsabilidad sobre el área auditada, y eso debe reflejarse entonces en la matriz de roles.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

9.2.2-4 **Los resultados de la auditoría se informan a la dirección pertinente.**

Cómo se demuestra: Un informe de auditoría con hallazgos, no conformidades, recomendaciones y una lista de distribución, junto con evidencia del traslado a la dirección, por ejemplo un punto en un acta o un correo fechado de traslado.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

9.2.2-5 **Se conserva información documentada sobre el programa de auditoría y los resultados de la auditoría.** Documento

Cómo se demuestra: Mantenga en un solo lugar el programa de auditoría, los planes de auditoría, los informes de auditoría y las acciones resultantes. El vínculo entre un hallazgo y una acción correctiva (apartado 10.2) debe ser visible de principio a fin.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

9.3.1-1 **La alta dirección revisa el SGSI a intervalos planificados para garantizar su continua idoneidad, adecuación y eficacia.**

Cómo se demuestra: Al menos anualmente y programada antes de la auditoría externa. Incluso en organizaciones muy pequeñas debe existir un acta fechada y firmada, incluso cuando la dirección y el propietario del SGSI son la misma persona.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

9.3.2-1 **La revisión por la dirección tiene en cuenta el estado de las acciones de revisiones por la dirección anteriores.**

Cómo se demuestra: El acta comienza con una tabla de seguimiento de las decisiones del año anterior y su estado actual. Sin esta referencia hacia atrás, la revisión se considera incompleta.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

9.3.2-2 **La revisión por la dirección tiene en cuenta los cambios en las cuestiones externas e internas que son relevantes para el SGSI, incluyendo los aspectos relevantes del cambio climático.**

Cómo se demuestra: Un punto propio del orden del día que remita al análisis de contexto actualizado. El cambio climático no se nombra explícitamente en el texto de este apartado (la Amd 1:2024 solo modifica los apartados 4.1 y 4.2), pero entra aquí a través de los cambios en las cuestiones del apartado 4.1, y los auditores lo esperan. Incluso un resultado de no relevante, sin cambios debe figurar en el acta.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

9.3.2-3 **La revisión por la dirección tiene en cuenta los cambios en las necesidades y expectativas de las partes interesadas que son relevantes para el SGSI.**

Cómo se demuestra: Nuevos requisitos de clientes procedentes de contratos y cuestionarios de seguridad, nuevas obligaciones legales, requisitos del organismo de certificación. Regístrelos como una lista con fuentes en el acta.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

9.3.2-4 **La revisión por la dirección tiene en cuenta la retroalimentación sobre el desempeño de la seguridad de la información, incluyendo las no conformidades y acciones correctivas, los resultados del seguimiento y la medición, los resultados de auditoría y el cumplimiento de los objetivos de seguridad de la información.**

Cómo se demuestra: Trate estos cuatro bloques como puntos separados del orden del día, de lo contrario alguno de ellos faltará más tarde en el acta. Adjunte la hoja de indicadores, el informe de auditoría y la hoja de objetivos como anexos.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

9.3.2-5 **La revisión por la dirección tiene en cuenta la retroalimentación de las partes interesadas.**

Cómo se demuestra: Quejas de clientes con un componente de seguridad, resultados de auditorías de clientes, informes del canal de denuncias, retroalimentación de proveedores de servicios. Regístrelo en el acta incluso cuando el hallazgo sea que no se recibió ninguna.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

9.3.2-6 **La revisión por la dirección tiene en cuenta los resultados de la evaluación de riesgos y el estado del plan de tratamiento de riesgos.**

Cómo se demuestra: Adjunte el registro de riesgos actual y el estado de implementación del plan de tratamiento, con confirmación explícita de la aceptación del riesgo residual por parte de los propietarios de los riesgos.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

9.3.2-7 **La revisión por la dirección tiene en cuenta las oportunidades de mejora continua.**

Cómo se demuestra: Un punto del orden del día con ideas de mejora concretas y una decisión sobre cada una. Las ideas aceptadas pasan al registro de mejoras como entradas con fechas límite.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

9.3.3-1 **Los resultados de la revisión por la dirección incluyen decisiones sobre oportunidades de mejora continua y sobre cualquier necesidad de cambios en el SGSI.**

Cómo se demuestra: El acta termina con un apartado de decisiones: decisión, propietario, fecha límite. Un acta sin decisiones es un hallazgo en la auditoría, porque entonces falta el efecto de liderazgo.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

9.3.3-2 **Se conserva información documentada como evidencia de los resultados de la revisión por la dirección.** Documento

Cómo se demuestra: Acta firmada con fecha, participantes, entradas, evaluación y decisiones. Es uno de los primeros documentos que pide un organismo de certificación en la fase 1.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

10 Mejora 7

10.1-1 **La idoneidad, adecuación y eficacia del SGSI se mejoran de forma continua.**

Cómo se demuestra: Un registro de mejoras alimentado por varias fuentes (auditorías, incidentes, ideas, desviaciones de indicadores) con progreso visible en el tiempo. La continuidad a lo largo de varios meses es la prueba, no el número de entradas.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

10.2-1 **Cuando se produce una no conformidad, la organización reacciona ante ella: la controla, la corrige y gestiona las consecuencias.**

Cómo se demuestra: Un informe de no conformidad con una acción inmediata y una fecha. Las fuentes son auditorías internas, auditorías externas, incidentes y observaciones de la operación diaria; todas ellas alimentan el mismo registro.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

10.2-2 **Se evalúa si es necesaria alguna acción para eliminar las causas, de modo que la no conformidad no se repita ni ocurra en otro lugar; esto incluye comprobar si existen o podrían producirse no conformidades similares.**

Cómo se demuestra: Documente el análisis de causa raíz, por ejemplo con los 5 porqués o el diagrama de Ishikawa, además de una declaración explícita sobre la transferibilidad a otros sistemas o procesos. El paso de transferibilidad es el que más se suele omitir.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

10.2-3 **Se implementan las acciones correctivas necesarias y se revisa su eficacia.**

Cómo se demuestra: Para cada acción registre la fecha de implementación, el artefacto de evidencia y una revisión de eficacia posterior con su propia fecha. Dos campos de fecha por fila son la forma más sencilla de no perder de vista la revisión de eficacia.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

10.2-4 **Cuando es necesario, se realizan cambios en el SGSI como resultado de la no conformidad.**

Cómo se demuestra: Si una no conformidad se remonta a una carencia en una política, en el registro de riesgos o en la Declaración de Aplicabilidad, el cambio debe hacerse visible allí. Una referencia desde la no conformidad hasta la versión actualizada del documento cierra la cadena.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

10.2-5 **Las acciones correctivas son apropiadas a los efectos de las no conformidades encontradas.**

Cómo se demuestra: Una calificación de gravedad en el registro de la que se desprenda la proporcionalidad de la acción. Ni trivialidades tratadas como un proyecto, ni desviaciones graves respondidas con un simple correo recordatorio.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

10.2-6 **Se conserva información documentada sobre la naturaleza de las no conformidades, las acciones tomadas en respuesta y los resultados de las acciones correctivas.** Documento

Cómo se demuestra: Un registro de no conformidades y acciones correctivas con columnas para naturaleza, causa, acción, propietario, fecha límite y el resultado de la revisión de eficacia. Es evidencia obligatoria y se solicita en cada auditoría de seguimiento.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.5 Anexo A: Controles organizativos 37

A.5.1 **Políticas de seguridad de la información: Se definen una política general de seguridad de la información y políticas específicas por tema, aprobadas por la dirección, comunicadas y revisadas a intervalos planificados y siempre que se produzcan cambios significativos.** Documento

Cómo se demuestra: Un conjunto de políticas con versión, fecha de aprobación y próxima fecha de revisión, junto con evidencia del acuse de recibo. Para organizaciones pequeñas basta una política marco y un puñado de políticas específicas (acceso, criptografía, trabajo remoto, incidentes).

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.5.2 **Roles y responsabilidades en seguridad de la información: Los roles y responsabilidades en materia de seguridad de la información se definen y se asignan según las necesidades de la organización.**

Cómo se demuestra: Una matriz de roles con nombres, suplentes y tareas. En organizaciones muy pequeñas, indique abiertamente dónde se acumulan varios roles en una sola persona y vincule esto con los controles compensatorios del apartado A.5.3.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.5.3 **Segregación de funciones: Las funciones y áreas de responsabilidad que están destinadas a controlarse mutuamente no recaen en una sola persona. El objetivo es que nadie pueda iniciar, aprobar y ocultar un cambio por su cuenta.**

Cómo se demuestra: En organizaciones pequeñas, la segregación completa es estructuralmente imposible; una afirmación genérica de conforme se derrumba de inmediato en la entrevista de auditoría. Lo que resulta sólido es un análisis honesto: qué combinaciones de funciones son críticas (desarrollar y liberar, conceder derechos y usarlos, iniciar y aprobar pagos), cuáles recaen en una sola persona, y qué controles compensatorios se aplican. Enfoques probados son los registros de auditoría inmutables accesibles para un tercero, MFA en las cuentas privilegiadas, puertas de control automatizadas en la integración continua y protección de ramas en lugar de la revisión a cuatro ojos, una revisión periódica de registros por parte de una persona externa, y una aprobación separada para los pagos. Mantenga el análisis y los controles compensatorios como un documento propio y fechado, y enlácelo desde la Declaración de Aplicabilidad.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.5.4 **Responsabilidades de la dirección: La dirección exige a todo el personal que aplique la seguridad de la información conforme a las políticas y procedimientos establecidos.**

Cómo se demuestra: Un compromiso en los contratos laborales y de contratistas, el acuse de recibo de las políticas en la incorporación, y recordatorios periódicos por parte de la dirección. Evidencia: declaraciones de compromiso firmadas y actas de reunión.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.5.5 **Contacto con las autoridades: Se mantienen contactos apropiados con las autoridades pertinentes y se puede acceder a ellos cuando es necesario.**

Cómo se demuestra: Una lista de contactos con la autoridad de protección de datos competente, la policía o la unidad de ciberdelincuencia, el punto nacional de notificación de ciberseguridad y, si procede, los canales de notificación de NIS2. Anote los plazos (como las 72 horas del RGPD) directamente en la lista.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.5.6 **Contacto con grupos de interés especial: Se mantienen contactos con grupos de interés especial, foros de seguridad y asociaciones profesionales.**

Cómo se demuestra: Membresías, boletines de alerta suscritos (CERT nacional, avisos de fabricantes), participación en grupos de interés especial. Una evidencia sencilla: una lista de suscripciones más un ejemplo de cómo un aviso derivó en una acción.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.5.7 **Inteligencia de amenazas: Se recopila y analiza información sobre amenazas a la seguridad de la información para derivar de ella las acciones apropiadas.**

Cómo se demuestra: Nuevo en la edición de 2022. Viable para organizaciones pequeñas: suscribirse a los avisos del CERT nacional y de los fabricantes, y después realizar una breve revisión mensual con una decisión de relevancia y los tickets derivados de ella. La evidencia es el análisis, no la suscripción.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.5.8 **Seguridad de la información en la gestión de proyectos: La seguridad de la información se integra en la gestión de proyectos, independientemente del tipo de proyecto.**

Cómo se demuestra: Puntos de seguridad en la lista de comprobación del proyecto: necesidades de protección, revisión de riesgos, comprobación de protección de datos, visto bueno de seguridad antes de la puesta en producción. En equipos ágiles, anclelos como puntos fijos en la definición de listo y en la definición de terminado.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.5.9 **Inventario de información y otros activos asociados: Se crea y se mantiene un inventario de la información y otros activos asociados con propietarios nombrados.**

Cómo se demuestra: Un inventario de activos que cubra hardware, software, servicios en la nube, repositorios de datos, dominios y cuentas, cada uno con un propietario y sus necesidades de protección. En organizaciones pequeñas se puede montar de forma automática a partir de una exportación de MDM, una lista de licencias y la consola de la nube; una fecha actual es obligatoria.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.5.10 **Uso aceptable de la información y otros activos asociados: Se identifican, documentan e implementan reglas para el uso aceptable y el manejo de la información y otros activos asociados.** Documento

Cómo se demuestra: Una política de uso aceptable para dispositivos, redes, cuentas en la nube y herramientas de IA, con acuse de recibo. Los dispositivos personales y los servicios de IA externos deben cubrirse de forma explícita, porque ahí es donde ocurre la mayor parte de las fugas.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.5.11 **Devolución de activos: Cuando una relación laboral finaliza o cambia, se regula y se confirma por escrito que se devuelven todos los dispositivos, llaves, cuentas y documentos entregados.**

Cómo se demuestra: Una lista de comprobación de salida con un justificante de devolución del portátil, tókenes, llaves, certificados y medios de almacenamiento, más la desactivación de cuentas el mismo día. Esto se aplica igualmente a autónomos y becarios.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.5.12 **Clasificación de la información: La información se clasifica según sus necesidades de protección en cuanto a confidencialidad, integridad, disponibilidad y requisitos legales.**

Cómo se demuestra: Un esquema sencillo con tres o cuatro niveles (pública, interna, confidencial, estrictamente confidencial) y reglas de manejo concretas por nivel. Registre la asignación en el inventario de activos o en el registro de actividades de tratamiento.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.5.13 **Etiquetado de la información: El nivel de clasificación es reconocible en el propio documento, archivo o mensaje, de modo que los destinatarios sepan cómo tratarlo sin necesidad de preguntar.**

Cómo se demuestra: Etiquetado en el encabezado del documento, en el nombre del archivo, en el asunto del correo electrónico o mediante etiquetas de sensibilidad en la suite ofimática en la nube. Evidencia mediante muestras de documentos realmente etiquetados, no solo mediante la regla.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.5.14 **Transferencia de información: Existen reglas, procedimientos y acuerdos para transferir información dentro de la organización y con terceros.**

Cómo se demuestra: Una regla que indique qué canal está permitido para cada nivel de clasificación: correo cifrado o una sala de datos para contenido confidencial, prohibición de enviar por mensajería privada. Respalde las transferencias confidenciales con acuerdos de confidencialidad.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.5.15 **Control de acceso: Se establecen e implementan reglas para controlar el acceso físico y lógico a la información y a otros activos asociados, basadas en los requisitos de negocio y de seguridad.**

Cómo se demuestra: Una política de control de acceso que siga los principios de necesidad de conocer y mínimo privilegio, con una correspondencia entre roles y derechos. Evidencia mediante la configuración real de derechos en el proveedor de identidad, no solo mediante la política.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.5.16 **Gestión de identidades: Se gestiona el ciclo de vida completo de las identidades.**

Cómo se demuestra: Un proceso desde la creación, pasando por el cambio, hasta la desactivación, idealmente centralizado en un proveedor de identidad con inicio de sesión único. Sin cuentas de grupo compartidas; cuando sea técnicamente inevitable, nombre la cuenta, justifíquela y registre su uso.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.5.17 **Información de autenticación: La asignación y gestión de la información de autenticación se controla mediante un proceso de gestión que exige a las personas manejarla correctamente.**

Cómo se demuestra: Un gestor de contraseñas como herramienta obligatoria, una política sobre la calidad de las contraseñas y la MFA, un acceso inicial seguro y un procedimiento de restablecimiento con verificación de identidad. Evidencia mediante capturas de pantalla de la configuración y el informe del gestor de contraseñas.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.5.18 **Derechos de acceso: Los derechos de acceso se aprovisionan, revisan, modifican y eliminan de acuerdo con la política de control de acceso.**

Cómo se demuestra: Una revisión periódica de acceso, al menos anual, con un resultado documentado por cuenta y evidencia de los derechos que se han eliminado. La eliminación el mismo día de la baja es un punto que a los auditores les gusta rastrear con un caso concreto.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.5.19 **Seguridad de la información en las relaciones con proveedores: Se definen e implementan procesos y procedimientos para gestionar los riesgos de seguridad derivados del uso de productos y servicios de terceros.**

Cómo se demuestra: Una lista de proveedores con un nivel de criticidad y la profundidad de la evaluación. Para los proveedores críticos, obtenga evidencias (certificado ISO 27001, informe SOC 2) en lugar de realizar auditorías propias, que es la única vía realista para organizaciones pequeñas.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.5.20 **Tratamiento de la seguridad de la información en los acuerdos con proveedores: Se acuerdan con cada proveedor los requisitos de seguridad relevantes y se recogen en los contratos.**

Cómo se demuestra: Un anexo contractual de seguridad de la información con obligaciones de notificación de incidentes, reglas sobre subencargados, obligaciones de eliminación y derechos de auditoría. Para servicios estándar, las condiciones del proveedor más un acuerdo de tratamiento de datos son suficientes, siempre que su contenido se haya revisado y documentado.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.5.21 **Gestión de la seguridad de la información en la cadena de suministro de TIC: Se definen e implementan procesos para gestionar los riesgos de seguridad en la cadena de suministro de tecnologías de la información y la comunicación.**

Cómo se demuestra: Esto cubre las dependencias de software y los propios subproveedores de los proveedores. En la práctica: una lista de materiales de software (SBOM) o lista de dependencias, comprobaciones automatizadas de paquetes vulnerables en la integración continua, y adquisición de software solo a través de canales firmados u oficiales.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.5.22 **Seguimiento, revisión y gestión de cambios de los servicios de proveedores: Los cambios en los servicios de los proveedores se supervisan, revisan y gestionan de forma regular.**

Cómo se demuestra: Una revisión anual de proveedores que analice incidentes, informes de disponibilidad y validez de certificados, más un canal para los anuncios de cambios del proveedor. Registre el resultado como una breve nota por proveedor.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.5.23 **Seguridad de la información para el uso de servicios en la nube: Se establecen procesos para adquirir, usar, gestionar y salir de los servicios en la nube conforme a los requisitos de seguridad.**

Cómo se demuestra: Nuevo en la edición de 2022 y el control central para las organizaciones pequeñas basadas en la nube. Evidencia mediante una política de nube con un proceso de aprobación para nuevos servicios, un modelo de responsabilidad compartida documentado por servicio, ajustes de bastionado, y una estrategia de salida que incluya la devolución de datos y la confirmación de eliminación.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.5.24 **Planificación y preparación de la gestión de incidentes de seguridad de la información: Se planifican y establecen procesos, roles y responsabilidades para la gestión de incidentes.** Documento

Cómo se demuestra: Un plan de respuesta a incidentes con la vía de notificación, roles, niveles de escalado, contactos fuera de horario laboral y plantillas de comunicación. Realista para equipos pequeños: una página, pero practicada.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.5.25 **Evaluación y decisión sobre los eventos de seguridad de la información: Los eventos de seguridad se evalúan y se decide si deben clasificarse como incidentes de seguridad de la información.**

Cómo se demuestra: Criterios de triaje con una matriz de gravedad y un registro de eventos en el que los eventos descartados también aparezcan con una justificación. La separación entre evento e incidente debe ser visible en el registro.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.5.26 **Respuesta a incidentes de seguridad de la información: Los incidentes se gestionan de acuerdo con los procedimientos documentados.**

Cómo se demuestra: Expedientes de incidentes con una cronología, las acciones tomadas, las personas involucradas y la decisión de cierre. Si todavía no ha habido un incidente real, un ejercicio de simulación documentado es la mejor evidencia disponible.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.5.27 **Aprendizaje de los incidentes de seguridad de la información: El conocimiento obtenido de los incidentes se utiliza para reforzar los controles de seguridad.**

Cómo se demuestra: Una revisión posterior al incidente sin buscar culpables, con análisis de causa raíz y acciones derivadas, vinculada al registro de mejoras y, cuando sea necesario, al registro de riesgos.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.5.28 **Recopilación de evidencias: Se regula cómo se identifican, aseguran y conservan los rastros relacionados con un evento de seguridad, de modo que sigan siendo utilizables más adelante.**

Cómo se demuestra: Un breve procedimiento de conservación de evidencias: no reconstruir los sistemas de forma prematura, asegurar imágenes y registros, documentar la cadena de custodia. Para organizaciones pequeñas basta con definir el nivel de gravedad a partir del cual se llama a un proveedor forense externo, junto con los datos de contacto.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.5.29 **Seguridad de la información durante la interrupción: La organización planifica cómo se mantiene la seguridad de la información en un nivel apropiado durante una interrupción.**

Cómo se demuestra: Los planes de emergencia no deben desactivar la seguridad. Documente que la MFA, el registro de actividad y las restricciones de acceso también se aplican en el modo de contingencia, y que las cuentas de emergencia (cuentas break-glass) están precintadas, documentadas y se revisan después.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.5.30 **Preparación de las TIC para la continuidad del negocio: La preparación de las TIC se planifica, implementa, mantiene y prueba sobre la base de los objetivos de continuidad del negocio y los requisitos de continuidad de las TIC.**

Cómo se demuestra: Nuevo en la edición de 2022. Evidencia mediante objetivos de tiempo de recuperación (RTO) y objetivos de punto de recuperación (RPO) definidos por sistema crítico, un procedimiento de recuperación y al menos una prueba documentada al año. Una prueba de restauración exitosa con fecha y duración es la evidencia individual más sólida.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.5.31 **Requisitos legales, estatutarios, reglamentarios y contractuales: Se identifican, documentan y mantienen actualizados los requisitos relevantes y el enfoque para cumplirlos.** Documento

Cómo se demuestra: Un registro legal que cubra el RGPD, el derecho de las telecomunicaciones, el derecho mercantil y fiscal y, cuando proceda, NIS2 o normas específicas del sector, cada uno con la regla que lo implementa y la fecha de revisión. Una revisión anual es suficiente, pero debe estar fechada.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.5.32 **Derechos de propiedad intelectual: Se implementan procedimientos apropiados para proteger los derechos de propiedad intelectual.**

Cómo se demuestra: Un inventario de licencias del software en uso, una comprobación de las licencias de código abierto en el producto (un escáner de licencias en la integración continua) y una regla para el manejo de código de terceros y código generado. Evidencia: el informe de licencias procedente de la compilación.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.5.33 **Protección de los registros: Los registros de negocio y probatorios se almacenan de modo que no puedan perderse, no puedan alterarse sin ser advertido y no puedan caer en manos equivocadas, y esto se mantiene durante todo el periodo de conservación.**

Cómo se demuestra: Un calendario de conservación con los plazos legales, almacenamiento resistente a manipulaciones, acceso restringido y copia de seguridad. Para los registros relevantes a efectos fiscales, indique explícitamente los plazos de conservación legales, ya que a los auditores les gusta comprobarlo específicamente.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.5.34 **Privacidad y protección de datos personales (PII): Se identifican y se cumplen los requisitos de privacidad y protección de la información de identificación personal (PII) conforme a la legislación aplicable.**

Cómo se demuestra: Registro de actividades de tratamiento, acuerdos de tratamiento de datos, un concepto de eliminación, un proceso para los derechos de los interesados y, cuando se requiera, una evaluación de impacto relativa a la protección de datos. Vincular esto con el SGSI mediante una lista de activos compartida evita mantenerlo todo por duplicado.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.5.35 **Revisión independiente de la seguridad de la información: El enfoque de la organización para gestionar la seguridad de la información se revisa de forma independiente a intervalos planificados y siempre que se produzcan cambios significativos.**

Cómo se demuestra: Se evidencia mediante la auditoría interna realizada por un auditor independiente, mediante pruebas de penetración externas o mediante la propia auditoría de certificación. Independiente significa que no la realiza la persona responsable del área revisada.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.5.36 **Cumplimiento de las políticas, normas y reglamentos de seguridad de la información: El cumplimiento de las propias políticas de seguridad de la organización y de las normas aplicables se revisa de forma regular.**

Cómo se demuestra: Comprobaciones de cumplimiento con fecha y resultado, por ejemplo una comprobación de configuración frente a la propia línea base de bastionado, un muestreo del etiquetado de documentos, comprobaciones automatizadas de políticas en la nube. Las desviaciones alimentan el registro de acciones correctivas.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.5.37 **Procedimientos de operación documentados: Los procedimientos de operación para los recursos de tratamiento de información se documentan y se ponen a disposición de las personas que los necesitan.** Documento

Cómo se demuestra: Runbooks para copia de seguridad y restauración, despliegue, administración de usuarios, aplicación de parches y gestión de incidentes. Breve y actualizado supera a extenso y desfasado; una fecha de última modificación por runbook es obligatoria.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.6 Anexo A: Controles relativos a las personas 8

A.6.1 **Selección: Los candidatos que van a trabajar para la organización se verifican de antemano, dentro de los límites de la ley y de forma proporcionada a las necesidades de protección; en el caso de roles sensibles, la verificación se repite durante el empleo.**

Cómo se demuestra: Sin personal en plantilla, este control puede justificarse como actualmente no aplicable, pero el procedimiento para el caso de una contratación debe seguir definido y registrado en la Declaración de Aplicabilidad como previsto. Un alcance viable: verificación de identidad, currículum y referencias, más certificados; una comprobación de antecedentes penales solo cuando las necesidades de protección lo justifiquen y la ley lo permita. Exija el mismo estándar a autónomos y contratistas a través de sus contratos, de lo contrario la brecha se abre exactamente ahí.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.6.2 **Términos y condiciones de empleo: Los acuerdos contractuales establecen las responsabilidades de seguridad de la información del personal y de la organización.**

Cómo se demuestra: Una cláusula de seguridad en el contrato laboral o de servicios que remita a las políticas aplicables. Para autónomos, la misma cláusula en el contrato de servicios, más un acuerdo de confidencialidad.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.6.3 **Concienciación, educación y formación en seguridad de la información: El personal y las partes externas relevantes reciben una concienciación y formación apropiadas, así como actualizaciones periódicas sobre las políticas de la organización.**

Cómo se demuestra: Formación anual con evidencia de asistencia y fecha, complementada con simulaciones de phishing con una tasa de clics evaluada. Incluso los autónomos sin personal necesitan evidencia de su propia formación continua, por ejemplo confirmaciones de cursos.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.6.4 **Proceso disciplinario: Existe un proceso formal y comunicado para tomar medidas contra las personas que han infringido las políticas de seguridad.**

Cómo se demuestra: Sin personal en plantilla, esto puede justificarse como actualmente no aplicable, pero el proceso debe seguir definido para el caso de una contratación; solo decae su aplicación, no la regla. Se requiere una escala de respuestas graduada y comunicada (conversación, amonestación, apercibimiento formal, despido) conforme al derecho laboral y a las normas de representación del personal. Para contratistas, refleje el nivel de sanción en el contrato, por ejemplo una penalización contractual o un derecho de rescisión.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.6.5 **Responsabilidades tras la finalización o cambio de empleo: Se definen, aplican y comunican a las personas afectadas las responsabilidades y obligaciones de seguridad que siguen vigentes tras la finalización o un cambio de rol.**

Cómo se demuestra: Una lista de comprobación de salida con eliminación de derechos, devolución de activos, traspaso de funciones y un recordatorio explícito de las obligaciones de confidencialidad que continúan. Un registro firmado de la entrevista de salida es la evidencia más sencilla.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.6.6 **Acuerdos de confidencialidad o no divulgación: Se determina quién debe firmar un acuerdo de confidencialidad. El contenido corresponde a las necesidades de protección de la información, los acuerdos se firman, se archivan y se revisan de forma regular para mantenerlos actualizados.**

Cómo se demuestra: Acuerdos de confidencialidad firmados para empleados, autónomos, proveedores de servicios y becarios, con un periodo de supervivencia. Una tabla resumen con contraparte, fecha y vigencia hace que la cartera sea auditable.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.6.7 **Trabajo remoto: Se implementan medidas de seguridad cuando las personas trabajan fuera de las instalaciones de la organización y acceden a la información de la organización mientras lo hacen.**

Cómo se demuestra: Una política de teletrabajo y trabajo remoto con requisitos sobre cifrado de disco, bloqueo de pantalla, Wi-Fi seguro, uso de VPN o acceso de confianza cero, filtros de privacidad y una prohibición de usar dispositivos personales sin aprobación. Evidencia mediante el informe de cumplimiento del MDM para los dispositivos finales.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.6.8 **Notificación de eventos de seguridad de la información: Existe un mecanismo mediante el cual las personas pueden notificar eventos de seguridad observados o sospechados de forma oportuna.**

Cómo se demuestra: Un canal de notificación comunicado con claridad (buzón de correo, canal de chat, número de teléfono) con la garantía de que no habrá sanciones por notificaciones de buena fe. Evidencia: el volumen de notificaciones en el registro de eventos; un registro permanentemente vacío es una señal de alerta en la auditoría.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.7 Anexo A: Controles físicos 14

A.7.1 **Perímetros de seguridad física: Se definen y se utilizan perímetros de seguridad para proteger las áreas que contienen información y recursos de tratamiento de información.**

Cómo se demuestra: Una descripción de los perímetros con un croquis o fotografías: edificio, oficina, armario de servidores. En una oficina en casa, el perímetro es la habitación de trabajo con llave o, en su defecto, un armario con llave; descríbalo en lugar de omitirlo.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.7.2 **Entrada física: Las áreas seguras están protegidas por controles de entrada y puntos de acceso apropiados.**

Cómo se demuestra: Un registro de llaves o tarjetas de acceso con entrega y devolución, y una regla de visitantes con acompañamiento y un registro. Si se utiliza un espacio de coworking o un centro de datos, tome como evidencia los controles de entrada del operador y asegúrelos contractualmente.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.7.3 **Seguridad de oficinas, despachos y recursos: La seguridad física de oficinas, despachos y recursos se diseña e implementa.**

Cómo se demuestra: Puertas con llave, protección de ventanas en la planta baja, ninguna pantalla confidencial visible desde el exterior, ningún letrero de empresa en áreas sensibles. Una breve descripción más una fotografía es suficiente como evidencia.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.7.4 **Supervisión de la seguridad física: Las instalaciones se supervisan de forma continua frente a accesos físicos no autorizados.**

Cómo se demuestra: Nuevo en la edición de 2022. Las opciones son un sistema de alarma, detectores de movimiento, videovigilancia o registros de entrada. La videovigilancia debe comprobarse en cuanto a su conformidad con la protección de datos; en una oficina en casa, la alternativa justificada es una combinación de sistema de alarma, habitación cerrada con llave y la constatación de que no se guardan allí servidores sensibles.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.7.5 **Protección contra amenazas físicas y ambientales: Se dispone de protección frente a amenazas físicas y ambientales, como desastres naturales y daños intencionados o no intencionados.**

Cómo se demuestra: Una revisión de incendio, agua, calor, corte de suministro eléctrico y allanamiento, junto con las medidas existentes (detectores de humo, extintores, ningún equipo bajo tuberías de agua, copia de seguridad almacenada en una ubicación diferente). Aquí es donde conecta la determinación sobre el cambio climático del apartado 4.1.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.7.6 **Trabajo en áreas seguras: Se diseñan e implementan medidas para el trabajo en áreas seguras.**

Cómo se demuestra: Reglas para la sala de servidores o áreas de alta confidencialidad: sin acceso de terceros sin supervisión, sin grabación con cámaras o dispositivos móviles, registro del trabajo realizado. Si no existen áreas seguras, esto puede justificarse remitiendo a una operación exclusivamente en la nube.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.7.7 **Escritorio despejado y pantalla despejada: Se definen y se siguen reglas para mantener despejados los escritorios en cuanto a papeles y soportes extraíbles, y para bloquear las pantallas.**

Cómo se demuestra: Esto se aplica plenamente también en la oficina en casa y, por tanto, no debe declararse no aplicable. Se evidencia mediante una breve regla (guardar los documentos bajo llave, bloqueo de pantalla tras cinco minutos, ninguna nota adhesiva con credenciales) más el bloqueo aplicado técnicamente mediante la política de dispositivos, cuya configuración puede exportarse.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.7.8 **Emplazamiento y protección de equipos: Los equipos se ubican y se protegen de forma segura.**

Cómo se demuestra: Ubicación alejada de zonas de paso y áreas públicas, sin visibilidad desde el exterior, protección frente al calor y la humedad, cables de seguridad para dispositivos móviles. Basta una breve descripción dentro de la política de oficina en casa u oficina.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.7.9 **Seguridad de los activos fuera de las instalaciones: Se protegen los activos ubicados fuera de las instalaciones.**

Cómo se demuestra: En organizaciones pequeñas se trata principalmente del portátil, el teléfono inteligente y los soportes externos, y no se puede argumentar en contra de ello. Evidencia: cifrado de disco forzado, borrado remoto activado mediante MDM, una regla contra dejar dispositivos en vehículos y contra el uso de redes públicas sin VPN, más una vía de notificación de pérdidas. El informe de cumplimiento del MDM que muestra el estado de cifrado por dispositivo es la evidencia individual más sólida.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.7.10 **Soportes de almacenamiento: Los soportes de almacenamiento se gestionan a lo largo de todo su ciclo de vida conforme al esquema de clasificación y a los requisitos de manejo, desde la adquisición, pasando por el uso y el transporte, hasta la eliminación.**

Cómo se demuestra: Esto se aplica incluso al trabajo puramente móvil, porque existen memorias USB, discos externos y soportes de copia de seguridad. Evidencia: un registro de soportes, soportes cifrados, una prohibición aplicada técnicamente de soportes extraíbles no aprobados, almacenamiento seguro en un lugar con llave, y traspaso al apartado A.7.14 al final de su vida útil.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.7.11 **Servicios de suministro: Los recursos de tratamiento de información están protegidos frente a fallos en los servicios de suministro, en particular el suministro eléctrico.**

Cómo se demuestra: Cuando los servidores se operan en las propias instalaciones, un sistema de alimentación ininterrumpida con una prueba documentada. En una configuración exclusivamente en la nube, la evidencia es la referencia a los compromisos del proveedor más una regla sobre cómo seguir trabajando durante un corte local de electricidad o internet (uso compartido de conexión móvil, ubicación alternativa).

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.7.12 **Seguridad del cableado: El cableado de energía, datos y comunicaciones está protegido frente a interceptación, interferencia y daños.**

Cómo se demuestra: Cuando el cableado es propio, protección frente a daños y frente al acceso no autorizado a los paneles de conexión. En oficinas pequeñas y oficinas en casa, la justificación es reducida, pero debe darse: el router y las tomas de red no son accesibles públicamente, los puertos no utilizados están deshabilitados.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.7.13 **Mantenimiento de equipos: Los equipos se mantienen correctamente para garantizar la disponibilidad, integridad y confidencialidad de la información.**

Cómo se demuestra: Un plan de mantenimiento o el estado de soporte del fabricante por dispositivo, y una regla para las reparaciones realizadas por terceros (retirar primero el soporte de almacenamiento o borrar los datos, y establecer un acuerdo de confidencialidad con el proveedor). Registre las fechas de fin de soporte en el inventario de activos.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.7.14 **Eliminación segura o reutilización de equipos: Antes de que un dispositivo con soporte de almacenamiento se ceda, venda o desguace, se verifica y se registra que ya no se pueden reconstruir en él datos protegidos ni software con licencia.**

Cómo se demuestra: Esto también se aplica en la oficina en casa y a los dispositivos personales retirados que se utilizaron para el trabajo. Evidencia: un registro de borrado por dispositivo con número de serie, fecha y método (borrado criptográfico en SSD cifrados, sobrescritura, destrucción física), o un certificado de destrucción de un proveedor. Para dispositivos cifrados, la destrucción documentada de la clave es suficiente, siempre que el procedimiento esté descrito.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.8 Anexo A: Controles tecnológicos 34

A.8.1 **Dispositivos finales de usuario: Se protege la información almacenada, tratada o accesible a través de dispositivos finales de usuario.**

Cómo se demuestra: Una línea base de bastionado por sistema operativo, gestión centralizada mediante MDM, cifrado de disco, actualizaciones automáticas y bloqueo de pantalla. El informe de cumplimiento del MDM con un estado por dispositivo evidencia todo esto de una sola vez.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.8.2 **Derechos de acceso privilegiado: La asignación y el uso de derechos de acceso privilegiado están restringidos y gestionados.**

Cómo se demuestra: Una lista de todas las cuentas de administrador con justificación, cuentas de administrador separadas que no se usan para el trabajo diario, MFA obligatoria, elevación limitada en el tiempo cuando sea posible, y revisión periódica. En organizaciones pequeñas, este es el control compensatorio más importante para el apartado A.5.3.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.8.3 **Restricción de acceso a la información: El acceso a la información y a otros activos asociados se restringe conforme a la política de control de acceso establecida.**

Cómo se demuestra: Un concepto de autorización basado en roles y grupos en lugar de concesiones individuales, evidenciado mediante una exportación de las pertenencias a grupos. Revise regularmente los enlaces de uso compartido público en el almacenamiento en la nube y déjelos caducar.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.8.4 **Acceso al código fuente: El acceso de lectura y escritura al código fuente, a las herramientas de desarrollo y a las bibliotecas de software se gestiona de forma apropiada.**

Cómo se demuestra: Permisos de repositorio por rol, ramas principales protegidas, revisiones obligatorias o comprobaciones de estado obligatorias, sin push directo a la rama principal. Evidencia mediante la configuración de protección de ramas y la lista de miembros de la organización.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.8.5 **Autenticación segura: Se implementan tecnologías y procedimientos de autenticación segura sobre la base de las restricciones de acceso y de la política específica por tema.**

Cómo se demuestra: MFA para todo acceso externo y todas las cuentas de administrador, métodos resistentes al phishing (llaves de acceso, FIDO2) cuando sea posible, y bloqueo tras intentos fallidos. Evidencia mediante el informe de cobertura de MFA del proveedor de identidad.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.8.6 **Gestión de la capacidad: Se supervisan el almacenamiento, la capacidad de cómputo, el ancho de banda y las licencias, y la demanda se ajusta con la antelación suficiente para que los cuellos de botella nunca comprometan la disponibilidad.**

Cómo se demuestra: Supervisión del almacenamiento, la carga de cómputo, las cuotas de licencias y los presupuestos en la nube con alertas de umbral. En organizaciones pequeñas basta una alerta sobre el uso de disco y sobre los límites de coste, más una revisión anual de la capacidad.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

A.8.7 **Protección contra malware: Las defensas técnicas contra el malware están activas y actualizadas, y las personas que usan los dispositivos están suficientemente formadas como para no debilitar esas defensas.**

Cómo se demuestra: Protección activa de endpoints con una vista de estado centralizada, un filtro de correo que inspecciona archivos adjuntos y enlaces, y una regla contra la ejecución de software no aprobado. El informe de estado fechado de la solución de protección es la evidencia directa.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

A.8.8 **Gestión de las vulnerabilidades técnicas: La organización se informa activamente sobre las vulnerabilidades de la tecnología que utiliza, decide para cada hallazgo hasta qué punto está expuesta y cierra la brecha dentro de los plazos definidos o justifica una respuesta diferente.**

Cómo se demuestra: Gestión de vulnerabilidades con una fuente (escáner, comprobación de dependencias en la integración continua, avisos de fabricantes), una calificación de gravedad y plazos definidos por nivel, por ejemplo crítico en un plazo de 7 días. Evidencia: informes de escaneo de varios momentos en el tiempo que muestren la disminución de los hallazgos abiertos.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

A.8.9 **Gestión de la configuración: Las configuraciones de hardware, software, servicios y redes, incluidas las configuraciones de seguridad, se establecen, documentan, implementan, supervisan y revisan.**

Cómo se demuestra: Nuevo en la edición de 2022. Evidencia mediante configuraciones de línea base documentadas (líneas base de bastionado) y su aplicación forzosa, idealmente como infraestructura como código en control de versiones o mediante perfiles de MDM. La detección de desviaciones y una comparación de configuración periódica lo completan.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

A.8.10 **Eliminación de información: La información almacenada en sistemas de información, en dispositivos y en soportes de almacenamiento se elimina en cuanto ya no es necesaria.**

Cómo se demuestra: Nuevo en la edición de 2022 y estrechamente vinculado con el RGPD. Evidencia mediante un concepto de eliminación con plazos de conservación por categoría de datos, políticas de retención implementadas técnicamente en servicios en la nube y bases de datos, y registros de eliminación. Las copias de seguridad y los archivos de registro también necesitan un plazo de conservación.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

A.8.11 **Enmascaramiento de datos: Se aplica el enmascaramiento de datos conforme a la política específica por tema sobre control de acceso y a los requisitos de negocio y legales.**

Cómo se demuestra: Nuevo en la edición de 2022. En la práctica: sin datos de producción en los entornos de prueba y desarrollo, sino datos anonimizados o sintéticos; seudonimización en analítica; enmascaramiento de números de cuenta y credenciales en registros e interfaces de soporte. Evidencia mediante el script o el procedimiento que genera los datos de prueba.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

A.8.12 **Prevención de fuga de datos: Se aplican medidas de prevención de fuga de datos a los sistemas, redes y dispositivos que tratan, almacenan o transmiten información sensible.**

Cómo se demuestra: Nuevo en la edición de 2022. Realista en organizaciones pequeñas: control de los enlaces de uso compartido en el almacenamiento en la nube, bloqueo de soportes extraíbles no aprobados, reglas contra el reenvío a buzones personales, comprobaciones sobre la introducción de datos confidenciales en servicios de IA externos, y detección de secretos en el código fuente. Evidencia mediante la configuración y mediante revisiones de los resultados.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.8.13 **Copia de seguridad de la información: Existen copias de seguridad de datos, software y sistemas conforme a una regla definida (alcance, frecuencia, retención, ubicación), y la restauración a partir de ellas se prueba realmente a intervalos regulares.**

Cómo se demuestra: Una política de copias de seguridad con frecuencia, retención y una copia externa siguiendo el principio 3-2-1, cifrado de las copias de seguridad, y protección frente a la sobrescritura por ransomware (copias de seguridad inmutables). Lo decisivo es la prueba de restauración documentada con fecha y resultado, porque una copia de seguridad no probada se considera inexistente en la auditoría.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.8.14 **Redundancia de los recursos de tratamiento de información: Los recursos de tratamiento de información se implementan con la redundancia suficiente para cumplir los requisitos de disponibilidad.**

Cómo se demuestra: La redundancia debe corresponder a los objetivos de disponibilidad, no al máximo posible. Evidencia mediante una descripción de arquitectura con instancias o zonas redundantes, equipos de repuesto, y una decisión justificada sobre dónde se prescinde deliberadamente de la redundancia.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.8.15 **Registro de actividad: Las actividades relevantes para la seguridad dejan un rastro. Los registros se generan, se conservan, se protegen frente a alteraciones y se analizan realmente, no solo se recopilan.**

Cómo se demuestra: Como mínimo, registre los inicios de sesión y los intentos fallidos, los cambios de permisos, las acciones administrativas y el acceso a datos confidenciales. Los registros están protegidos frente a alteraciones y tienen un plazo de conservación definido; en organizaciones pequeñas, los registros inmutables son a la vez la compensación por la falta de segregación de funciones del apartado A.5.3.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.8.16 **Actividades de supervisión: Las redes, sistemas y aplicaciones se supervisan en busca de comportamiento anómalo y se toman las medidas apropiadas para evaluar posibles incidentes de seguridad.**

Cómo se demuestra: Nuevo en la edición de 2022. Viable sin un equipo de seguridad propio: alertas del proveedor de identidad sobre desplazamientos imposibles y sobre series de intentos fallidos, alertas de la plataforma en la nube sobre gasto inusual o cambios de permisos, reenviadas a un buzón supervisado con un tiempo de respuesta definido. Evidencia mediante las reglas de alerta más ejemplos de alertas gestionadas.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.8.17 **Sincronización de relojes: Todos los sistemas que generan registros toman su hora de una fuente definida y de confianza, de modo que los eventos puedan ordenarse correctamente entre sistemas.**

Cómo se demuestra: Configuración de NTP en servidores y dispositivos finales, y una zona horaria uniforme en los registros (idealmente UTC). Sin la sincronización de la hora, la reconstrucción de un incidente conforme al apartado A.5.28 no se sostiene; un extracto de configuración es suficiente como evidencia.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.8.18 **Uso de programas de utilidad con privilegios: El uso de programas de utilidad que pueden anular las protecciones del sistema está restringido y estrechamente controlado.**

Cómo se demuestra: Una lista de herramientas de administración aprobadas, restricción de los derechos de administrador local, control de aplicaciones (listas de permitidos) cuando sea posible, y registro del uso. Evidencia: la política más la configuración de la gestión de derechos.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.8.19 **Instalación de software en sistemas operativos: Se implementan procedimientos y medidas para gestionar de forma segura la instalación de software en los sistemas operativos.**

Cómo se demuestra: Solo software aprobado procedente de fuentes de confianza, instalación mediante distribución centralizada o un gestor de paquetes, una vía de reversión y conservación de la versión anterior. Evidencia mediante la lista de aprobación y los registros de despliegue.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.8.20 **Seguridad de las redes: Las redes y los dispositivos de red activos tienen un propietario nombrado, una configuración bastionada y un conjunto de reglas trazable que define qué tráfico está permitido en absoluto.**

Cómo se demuestra: Un conjunto de reglas de cortafuegos que sigue el principio de denegación por defecto, puertos abiertos documentados con justificación, una configuración Wi-Fi segura, y credenciales por defecto cambiadas en los dispositivos de red. Evidencia mediante una exportación del conjunto de reglas y un escaneo de puertos externo.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.8.21 **Seguridad de los servicios de red: Se identifican, implementan y supervisan los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de los servicios de red.**

Cómo se demuestra: Para cada servicio de red en uso (VPN, DNS, correo, CDN), documente los compromisos de seguridad y su propia configuración, incluido el cifrado en tránsito y los compromisos de nivel de servicio del proveedor. Evidencia: una vista general de configuración más el contrato o la descripción del servicio.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.8.22 **Segregación de redes: La red se divide en zonas de modo que los servicios, grupos de usuarios y sistemas con distintas necesidades de protección no puedan alcanzarse entre sí sin filtrar.**

Cómo se demuestra: Segmentos de red o VLAN separados para invitados, administración y producción; en la nube, cuentas o redes virtuales separadas con grupos de seguridad. En una oficina en casa, la implementación viable es una red o VLAN separada para los dispositivos de trabajo, mantenida al margen de los dispositivos personales y de la domótica.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.8.23 **Filtrado web: Se gestiona el acceso a sitios web externos para reducir la exposición a contenido malicioso.**

Cómo se demuestra: Nuevo en la edición de 2022. Alcanzable con poco esfuerzo mediante un servicio de DNS con filtrado o el filtrado web incluido en la protección de endpoints, con categorías bloqueadas y registro de las solicitudes bloqueadas. Evidencia mediante la configuración del filtro y un extracto de informes.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.8.24 **Uso de criptografía: Se define de forma vinculante dónde se aplica el cifrado, con qué algoritmos, y cómo se generan, almacenan, rotan y destruyen las claves a lo largo de todo su ciclo de vida.** Documento

Cómo se demuestra: Una política de criptografía con algoritmos aprobados y longitudes de clave mínimas, cifrado en tránsito (TLS) y en reposo, más un procedimiento de gestión de claves que cubra la generación, el almacenamiento, la rotación y la destrucción. Evidencia mediante la política más la configuración del servicio de claves o del almacén de secretos.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.8.25 **Ciclo de vida de desarrollo seguro: Se establecen y aplican reglas para el desarrollo seguro de software y sistemas.**

Cómo se demuestra: Una descripción del proceso de desarrollo con puntos de control de seguridad por fase: requisitos, diseño, implementación, pruebas, liberación, operación. Para equipos pequeños, una sola página que remita a las puertas de control concretas de la integración continua y a la obligación de revisión es suficiente.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

A.8.26 **Requisitos de seguridad de las aplicaciones: Los requisitos de seguridad para las aplicaciones se identifican, especifican y aprueban durante el desarrollo y la adquisición.**

Cómo se demuestra: Requisitos de seguridad como puntos explícitos en la lista de requisitos o como una lista de comprobación reutilizable, orientada por ejemplo a estándares comunes de verificación de seguridad de aplicaciones. Evidencia mediante tickets o documentos de requisitos con un componente de seguridad.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

A.8.27 **Principios de arquitectura y ingeniería de sistemas seguros: Se establecen, documentan y aplican principios de ingeniería de sistemas seguros a las actividades de desarrollo.**

Cómo se demuestra: Principios documentados como mínimo privilegio, defensa en profundidad, configuraciones seguras por defecto, minimización de datos y un enfoque de confianza cero, junto con su aplicación visible en croquis de arquitectura o registros de decisiones.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

A.8.28 **Codificación segura: Se aplican principios de codificación segura en el desarrollo de software.**

Cómo se demuestra: Nuevo en la edición de 2022. Evidencia mediante reglas de codificación vinculantes, análisis estático de código y detección de secretos como puertas obligatorias en la integración continua, uso de bibliotecas verificadas, y revisiones de código documentadas. Cuando la segregación de funciones es imposible, las puertas automatizadas obligatorias sustituyen a la revisión a cuatro ojos; justifíquelo y evidéncielo con la configuración del pipeline.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

A.8.29 **Pruebas de seguridad en desarrollo y aceptación: Se definen e implementan procesos de pruebas de seguridad dentro del ciclo de vida de desarrollo.**

Cómo se demuestra: Pruebas de seguridad automatizadas en el pipeline (comprobaciones de dependencias, análisis estático y dinámico) más una prueba de penetración periódica cuando las necesidades de protección sean elevadas. Evidencia mediante informes de prueba fechados y el seguimiento de los hallazgos.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

A.8.30 **Desarrollo externalizado: Las actividades de desarrollo externalizadas se dirigen, supervisan y revisan.**

Cómo se demuestra: Cuando el desarrollo se externaliza, establezca los requisitos de seguridad en el contrato, asegure la titularidad del código y el derecho de revisión, y realice revisiones de código y pruebas de seguridad antes de la aceptación. Sin desarrollo externalizado, la no aplicabilidad debe justificarse de forma coherente en la Declaración de Aplicabilidad.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

A.8.31 **Separación de los entornos de desarrollo, prueba y producción: Los entornos de desarrollo, prueba y producción están separados y protegidos.**

Cómo se demuestra: Cuentas, proyectos o espacios de nombres separados, credenciales separadas y conjuntos de datos separados. En combinación con el apartado A.8.11, asegúrese de que ningún dato de producción termine en entornos que no sean de producción. Evidencia mediante la vista general de entornos y la asignación de derechos.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

A.8.32 **Gestión de cambios: Los cambios en los recursos y sistemas de tratamiento de información están sujetos a procedimientos de gestión de cambios.**

Cómo se demuestra: Un proceso de cambios con solicitud, evaluación de impacto, pruebas, aprobación, implementación y una vía de reversión. En equipos de desarrollo, un pipeline de pull requests con comprobaciones obligatorias y despliegues registrados satisface este punto, siempre que el historial sea inmutable.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.8.33 **Información de prueba: La información de prueba se selecciona, protege y gestiona de forma apropiada.**

Cómo se demuestra: El principio: sin datos personales reales en los sistemas de prueba. Cuando eso es inevitable, documente la aprobación, el enmascaramiento, la restricción de acceso y la eliminación tras la prueba. Evidencia mediante el concepto de datos de prueba y los registros de eliminación.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

A.8.34 **Protección de los sistemas de información durante las pruebas de auditoría: Las pruebas de auditoría que implican acceso a sistemas operativos se planifican y se acuerdan con la dirección para evitar interrupciones en la operación.**

Cómo se demuestra: Un acuerdo de auditoría con una ventana temporal, un alcance, acceso de solo lectura cuando sea posible, registro del acceso de auditoría y aprobación de la dirección. Esto también se aplica a las pruebas de penetración: una autorización de prueba por escrito con una ventana temporal y un contacto de emergencia es la evidencia.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación