IEC 62443-4-1:2018 Ciclo de vida de desarrollo seguro de productos para automatización industrial

Ciclo de vida de desarrollo seguro, ocho prácticas

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

La norma IEC 62443-4-1 admite certificación, pero el objeto es inusual: lo que se certifica es el proceso de desarrollo de una organización de desarrollo concreta, es decir, una versión documentada y concreta del ciclo de vida seguro. No se certifica ni un producto ni una persona. Las vías son ISASecure SDLA y el IECEE CB Scheme. A día de hoy, ese certificado no genera una presunción de conformidad con el Reglamento de Ciberresiliencia de la UE (Cyber Resilience Act). No debe confundirse con IEC 62443-4-2, que establece requisitos sobre el propio componente. Esta lista es una ayuda de trabajo para la autoevaluación, no una prueba.

Empresa	Fecha	Elaborado por

5 Práctica 1: Gestión de la seguridad (SM) 13

SM-1 **Existe un ciclo de vida de desarrollo de producto definido que mantiene la seguridad en todas las fases, desde el concepto inicial hasta la retirada de servicio del producto, y este ciclo de vida es el que realmente se sigue en la práctica.** Documento

Cómo se demuestra: Descripción del proceso o instrucción de trabajo que enumere las fases, los entregables por fase y los puntos de traspaso, junto con evidencia de un proyecto en curso que muestre que las fases se recorrieron realmente. Una organización pequeña puede arreglarse con una página por fase más una lista de verificación en el sistema de tickets; lo importante es que el proceso documentado y la práctica diaria coincidan.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

SM-2 **Cada tarea del ciclo de vida de desarrollo seguro tiene un responsable asignado, y esta asignación es conocida por las personas involucradas.** Documento

Cómo se demuestra: Matriz de roles y responsabilidades que asigna cada paso del proceso a un rol con nombre, complementada con la asignación actual de personas a esos roles. Con solo un pequeño grupo de personas basta una tabla con rol, tarea y persona; lo importante es la regla de suplencia para vacaciones y bajas por enfermedad.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

SM-3 **Está definido de forma trazable qué productos, variantes, versiones y componentes están sujetos al ciclo de vida de desarrollo seguro y cuáles no.** Documento

Cómo se demuestra: Lista de los productos y estados de versión incluidos en el alcance, con la justificación de las inclusiones y exclusiones, actualizada con cada nueva versión. En la práctica funciona bien una columna en el resumen de productos con un sí o un no por fila más una frase de justificación.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

SM-4 **Las personas que asumen tareas de seguridad cuentan con la competencia técnica necesaria para ello, y esa competencia se desarrolla y actualiza de forma deliberada.**

Cómo se demuestra: Perfil de competencias por rol de seguridad, registros de cualificación, plan de formación y registros de asistencia, complementados con un resumen de las carencias detectadas. Las organizaciones pequeñas lo evidencian mediante certificados, asistencia a conferencias o seminarios web y una breve revisión anual de quién cierra qué carencia y para cuándo, recurriendo a experiencia externa cuando sea necesario.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

SM-5 **El alcance del ciclo de vida de desarrollo seguro está delimitado y nombra las sedes, unidades organizativas, contribuciones de proveedores y entornos de desarrollo implicados, junto con los límites de ese alcance.** Documento

Cómo se demuestra: Declaración de alcance que cubre sedes, equipos, partes subcontratadas y sistemas, más un esquema de las interfaces externas. Quien desarrolla en una única sede lo documenta en pocas frases y nombra explícitamente lo que queda fuera, como conjuntos desarrollados externamente o alojamiento por terceros.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SM-6 **Para cada elemento entregado a los usuarios, software, firmware, configuraciones y archivos adjuntos, es posible realizar una verificación de integridad, de modo que los destinatarios puedan detectar una modificación no advertida.**

Cómo se demuestra: Firmas o sumas de comprobación publicadas por paquete de entrega, una descripción del método y un ejemplo de una versión real, junto con instrucciones para el cliente sobre cómo realizar la verificación. Para equipos pequeños basta un archivo de suma de comprobación firmado junto a la descarga más un párrafo en las notas de la versión.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SM-7 **Los entornos utilizados para desarrollo, compilación y pruebas están protegidos frente a accesos no autorizados y frente a manipulaciones del código fuente, las herramientas de compilación y los artefactos.**

Cómo se demuestra: Concepto de control de acceso para el repositorio, el servidor de compilación y los sistemas de prueba, listas de acceso con la fecha de la última revisión, registros de cambios relevantes para la seguridad y evidencia de que el acceso de producción y el de desarrollo están separados. Sin un departamento de TI propio, basta con el inicio de sesión con doble factor, una rama principal protegida con revisión obligatoria y una revisión semestral de quién sigue teniendo acceso.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SM-8 **Las claves privadas utilizadas para firmar las entregas están protegidas frente a divulgación y uso indebido, y su uso está restringido a personas y sistemas autorizados.**

Cómo se demuestra: Descripción del almacenamiento, acceso, renovación y revocación de las claves, evidencia de un almacenamiento protegido como un token hardware o un servicio de gestión de claves, más registros de las operaciones de firma. Una organización pequeña guarda la clave de firma en un token hardware, documenta a las dos personas con acceso y mantiene un procedimiento listo para el caso de pérdida.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SM-9 **Para los componentes comprados o adoptados, incluido el software de código abierto, están definidas las expectativas de seguridad hacia el proveedor y se aplican durante la selección.** Documento

Cómo se demuestra: Requisitos de seguridad en las especificaciones o contratos con proveedores, criterios de selección para componentes de terceros, un inventario de todos los componentes de terceros con versión y origen, más la evaluación de si el proveedor cumple las expectativas. Sin un departamento de compras, basta con una lista de componentes mantenida con una columna que registre si se comprobaron las actualizaciones de seguridad y los canales de notificación del proveedor.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SM-10 **Los componentes desarrollados por encargo por un tercero están sujetos a los mismos requisitos de seguridad que el desarrollo propio, y su cumplimiento se verifica.**

Cómo se demuestra: Pedido de compra o documentos contractuales que indiquen las obligaciones de seguridad exigidas, evidencia del proveedor sobre las prácticas aplicadas, registros de aceptación y resultados de las propias verificaciones sobre el trabajo entregado. Sin presupuesto para auditorías, basta con una garantía contractual, la entrega de los resultados de prueba del proveedor y una verificación de muestra propia antes de la aceptación.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SM-11 **Los hallazgos relacionados con la seguridad procedentes de todas las fuentes, pruebas, revisiones, informes de usuarios y notificaciones de terceros, se registran, se evalúa su impacto, se les asigna un responsable y una fecha límite, y se les hace seguimiento hasta su cierre.** Documento

Cómo se demuestra: Sistema de defectos o tickets con una marca específica para temas de seguridad, y por cada entrada la evaluación de impacto, el responsable, la fecha límite y la nota de cierre, más un informe de los puntos abiertos. Un equipo pequeño usa una etiqueta en el sistema de tickets existente y un punto fijo en la agenda de la reunión semanal.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SM-12 **Antes de publicar un producto se verifica y se evidencia que los pasos previstos del ciclo de vida de desarrollo seguro se llevaron a cabo realmente y que se generaron los registros correspondientes.** Documento

Cómo se demuestra: Revisión de publicación por cada versión, comparando con los pasos del proceso, con referencias a los registros correspondientes y una decisión de publicación documentada con fecha y firma. En la práctica funciona bien una lista de verificación de publicación que no permite el envío sin todas las casillas marcadas; los puntos abiertos se justifican y se les asigna una fecha.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SM-13 **El propio ciclo de vida de desarrollo seguro se cuestiona y mejora periódicamente, a partir de los conocimientos obtenidos de incidentes, resultados de pruebas, retroalimentación de clientes y la evolución del panorama de amenazas.**

Cómo se demuestra: Registros de la revisión del proceso, por ejemplo una revisión de dirección o una retrospectiva, con los cambios de proceso desencadenados, su estado de implementación y una referencia a la causa raíz. Quien utiliza los niveles de madurez de la norma registra el estado actual y el objetivo por cada práctica; el nivel de madurez 4 exige precisamente esta evidencia de mejora continua. Para una organización pequeña basta una reunión al año con acta y tres mejoras concretas.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

6 Práctica 2: Especificación de los requisitos de seguridad (SR) 5

SR-1 **Se describe el contexto de uso previsto del producto: entorno operativo esperado, medidas de seguridad que se asume que aporta ese entorno, grupos de usuarios y roles previstos, límites de confianza asumidos, y los usos para los que el producto explícitamente no está previsto.** Documento

Cómo se demuestra: Una descripción del contexto de seguridad del producto, ya sea como documento independiente o como sección fija de la especificación del producto, que cubra el entorno de red, las protecciones externas asumidas como un firewall o control de acceso físico, una lista de roles y una lista explícita de usos fuera de alcance. Una organización pequeña lo limita a dos páginas, añade un esquema simple del entorno de planta y hace que el responsable del producto lo feche y apruebe.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR-2 **Existe un modelo de amenazas para el producto que representa los flujos de datos, las interfaces, los límites de confianza y las vías de ataque, nombra las amenazas resultantes y su posible impacto, y asigna contramedidas. Se revisa y actualiza ante cambios relevantes y al menos una vez por cada versión del producto, y los puntos abiertos se siguen hasta su cierre.** Documento

Cómo se demuestra: Modelo de amenazas con un diagrama de flujo de datos, una lista de amenazas por interfaz, contramedidas asignadas y el estado de los puntos abiertos, más un historial de revisiones con fecha y autor. Una organización pequeña puede trabajar con una tabla por interfaz, con columnas para qué podría salir mal ahí, qué tan grave sería, qué se hace al respecto y quién lo revisa.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SR-3 **Los requisitos de seguridad del producto están definidos y documentados. Cubren los resultados del modelo de amenazas, el contexto de seguridad del producto descrito, las obligaciones legales y contractuales aplicables y el nivel de seguridad objetivo, e incluyen las capacidades de seguridad que el propio producto debe aportar.** Documento

Cómo se demuestra: Lista de requisitos o herramienta de gestión de requisitos con un identificador único por requisito, el origen de cada entrada, como una amenaza, un contrato con el cliente o una obligación legal, y el nivel de seguridad objetivo. Una organización pequeña lo gestiona como una única tabla con una columna de ID fija a la que luego se enlazan la verificación y las pruebas.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

SR-4 **Cada requisito de seguridad individual está redactado de forma inequívoca, libre de contradicciones, verificable y trazable hasta una función o interfaz concreta del producto, y contiene la información necesaria para verificarlo más adelante sin aclaraciones adicionales.**

Cómo se demuestra: Una muestra de la lista de requisitos que muestre, para cada requisito, un criterio de aceptación medible y la función o interfaz afectada, junto con la relación entre requisito y caso de prueba. Una organización pequeña lo comprueba con una plantilla de redacción fija y la pregunta de control de si se puede escribir un caso de prueba a partir del requisito sin necesidad de volver a preguntar.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

SR-5 **Los requisitos de seguridad se revisan antes de utilizarse en el diseño y la implementación, con la participación de las partes afectadas, como desarrollo, pruebas, la propiedad del producto y, cuando resulte útil, ventas o el cliente. La revisión cubre la completitud frente al modelo de amenazas y el contexto de seguridad del producto, la corrección y la verificabilidad. Los hallazgos se registran y se siguen hasta su cierre.**

Cómo se demuestra: Registro de revisión con fecha, participantes y sus roles, la versión revisada de los requisitos, una lista de hallazgos con responsable y estado de cierre, y una nota de aprobación. Una organización pequeña lo gestiona como una revisión entre dos personas, desarrollo y pruebas, con un registro breve y una línea de aprobación en la lista de requisitos.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

7 Práctica 3: Seguridad desde el diseño (SD) 4

SD-1 **Cada producto cuenta con una descripción de diseño que recoge los aspectos relevantes para la seguridad de la arquitectura: qué componentes existen, cómo se comunican entre sí, dónde discurren los límites de confianza, qué interfaces externas quedan expuestas y con qué mecanismos se materializan en el diseño los requisitos de seguridad definidos previamente.** Documento

Cómo se demuestra: Documento de arquitectura o especificación de diseño que contenga un diagrama que muestre los componentes, los flujos de datos y los límites de confianza, más una tabla de correspondencia entre cada requisito de seguridad y el elemento de diseño que lo implementa. A un proveedor pequeño le basta con un diagrama mantenido más dos o tres páginas de explicación; lo importante es que esté bajo control de versiones en el repositorio y se actualice cada vez que cambia la arquitectura.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

SD-2 **El diseño se analiza sistemáticamente en busca de amenazas. El análisis nombra los objetivos del atacante, los límites de confianza y las interfaces afectadas, las amenazas resultantes junto con su valoración, y las contramedidas adoptadas en el diseño. Se repite cada vez que la arquitectura o el entorno cambian de forma significativa, y las amenazas identificadas se siguen hasta que se ha tomado una decisión sobre cada una de ellas.** Documento

Cómo se demuestra: Modelo de amenazas por producto o por cada versión mayor, por ejemplo una tabla con columnas para amenaza, interfaz afectada, valoración, contramedida y estado, junto con el acta de la sesión de modelado con participantes y fecha. Un equipo pequeño modela de forma pragmática en un taller de dos a tres horas siguiendo el diagrama de arquitectura y registra los puntos abiertos como tickets, de modo que la evidencia de seguimiento se genera sin esfuerzo adicional.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

SD-3 **El diseño sigue de forma demostrable principios de diseño seguro reconocidos, entre ellos el mínimo privilegio, la superficie de ataque mínima, la defensa en profundidad, los valores predeterminados seguros, el comportamiento seguro ante fallos y mecanismos de seguridad tan simples y verificables como sea posible. La aplicación de estos principios es visible en el diseño y está justificada.**

Cómo se demuestra: Una sección en la descripción de diseño o una guía de diseño propia que nombre los principios, más evidencia concreta por principio en el producto, como la matriz de privilegios de los servicios, la lista de puertos abiertos con su justificación, los valores predeterminados de entrega o el comportamiento documentado ante errores. Un proveedor pequeño utiliza una breve lista de verificación de estos principios como punto fijo en la revisión de diseño y archiva la hoja cumplimentada junto con el diseño.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

SD-4 **El diseño es revisado por pares cualificados antes de que comience la implementación. La revisión cubre la completitud frente a los requisitos de seguridad, la corrección y eficacia de los mecanismos de seguridad y los resultados del análisis de amenazas. Participan personas con suficiente competencia en seguridad, los hallazgos se registran y se siguen hasta su cierre.** Documento

Cómo se demuestra: Registro de revisión con fecha, elemento revisado incluida su versión, participantes y sus roles, lista de hallazgos con estado y la decisión de aprobación. Un equipo pequeño adjunta la revisión a la pull request de los documentos de diseño y deja los hallazgos como comentarios con una nota de cierre, lo que evidencia el seguimiento sin herramientas adicionales. Cuando falta competencia en seguridad dentro de la organización, contratar a un revisor externo por horas para los diseños críticos es la vía pragmática.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

8 Práctica 4: Implementación segura (SI) 2

SI-1 **Existe un proceso definido para verificar la implementación real frente al diseño seguro: la revisión confirma que las medidas de protección previstas en el diseño están realmente presentes y son eficaces en el código, que se conserva la defensa en profundidad y que no se han introducido nuevas vulnerabilidades durante la implementación. La revisión la realiza personal debidamente cualificado, y cualquier desviación encontrada se registra y se sigue hasta su cierre.**

Cómo se demuestra: Un procedimiento escrito para la revisión de la implementación junto con registros de revisión por componente o versión: el módulo revisado, la referencia al documento de diseño, la fecha, el revisor, los hallazgos y su estado de resolución. Como evidencia adecuada sirven las revisiones de pull request con una lista de verificación de seguridad obligatoria, los resultados del análisis estático de código con una evaluación documentada de cada hallazgo, y las actas de las sesiones de revisión. Un equipo pequeño lo cubre con el principio de las cuatro vistas, una plantilla de revisión guardada en el repositorio en la que se marca individualmente cada medida de diseño, y un ticket por cada hallazgo abierto. El punto esencial es que el autor del código nunca sea el revisor de ese mismo código.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

SI-2 **Se aplican reglas vinculantes de codificación segura a todo el trabajo de desarrollo relacionado con la seguridad, y cubren al menos evitar construcciones y funciones inseguras conocidas, el manejo de entradas y errores, la gestión de memoria y recursos, y el uso de código de seguridad ya verificado en lugar de implementaciones propias. Las reglas se aplican por cada lenguaje de programación utilizado, son conocidas por todos los desarrolladores y se actualizan cuando es necesario, por ejemplo cuando surgen nuevos patrones de ataque o nuevas herramientas.** Documento

Cómo se demuestra: Un estándar de codificación segura aprobado con estado de versión, alcance por lenguaje y fecha de aprobación, complementado con evidencia de que se aplica en el trabajo diario: la configuración de linters y herramientas de análisis en el repositorio, una regla de compilación que muestra las infracciones, y la lista de asistencia a la sesión informativa. Las organizaciones pequeñas no escriben un estándar desde cero; declaran vinculante un conjunto de reglas públicas ya establecido, añaden una breve lista de reglas propias adicionales y anclan la comprobación en el pipeline, de modo que el cumplimiento se demuestra automáticamente.

○ Abierto ○ En curso ○ Cumplido ○ No aplicable

Evidencia / justificación

9 Práctica 5: Verificación y validación de la seguridad mediante pruebas (SVV) 5

SVV-1 Documento

Cada requisito de producto relacionado con la seguridad tiene asignado al menos un caso de prueba, que demuestra que la función de protección funciona según lo previsto en operación normal, que se comporta según lo especificado ante entradas inválidas o uso indebido, y que la configuración predeterminada de entrega del producto corresponde al estado seguro. La ejecución y el resultado se registran para cada versión de software probada.

Cómo se demuestra: Una matriz de trazabilidad que enlaza requisito, caso de prueba y resultado, más registros de prueba que muestren la fecha, la versión o build probada y el nombre de la persona que realizó la prueba. Un proveedor pequeño simplemente añade una columna de ID de caso de prueba a su lista de requisitos y archiva el log de salida de la ejecución de pruebas automatizadas del pipeline de compilación como archivo adjunto a la versión correspondiente.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SVV-2

Las contramedidas derivadas del modelo de amenazas se prueban específicamente para confirmar que realmente cierran la vía de ataque asumida. Las pruebas se realizan frente a las amenazas identificadas, no solo frente a un uso conforme, y los puntos abiertos se incorporan al proceso de gestión de defectos.

Cómo se demuestra: Casos de prueba que referencian directamente las entradas del modelo de amenazas, por ejemplo un caso de abuso por cada ID de amenaza con el comportamiento defensivo esperado, junto con los registros de esas ejecuciones. Sin necesidad de maquinaria pesada, basta con añadir al modelo de amenazas una columna que referencie el caso de prueba y la fecha de la última comprobación exitosa.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SVV-3 Documento

El producto se examina sistemáticamente en busca de vulnerabilidades antes de su publicación. El alcance cubre al menos: el examen de las interfaces y servicios accesibles externamente, pruebas con entradas malformadas y mutadas de forma aleatoria, la revisión de los componentes de terceros utilizados frente a vulnerabilidades conocidas y notificadas, y una comprobación de clases de debilidad conocidas en el código propio del proveedor. Los hallazgos se registran junto con su evaluación.

Cómo se demuestra: Informes de las herramientas utilizadas, indicando nombre de la herramienta, versión y el estado de los datos de la base de vulnerabilidades, registros de fuzzing, una lista de componentes de terceros con la fecha de la última comparación, y la lista de hallazgos con evaluación y decisión. Un proveedor pequeño combina herramientas estándar gratuitas, un escaneo de dependencias y un escaneo de puertos y servicios contra el producto instalado, y archiva las salidas por versión en una carpeta.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SVV-4

El candidato a publicación se somete a un intento de ataque en condiciones realistas que trata activamente de eludir los mecanismos de protección, en lugar de limitarse a consultarlos. El alcance, las condiciones de contorno y los límites de la prueba se acuerdan de antemano, y las debilidades encontradas se gestionan y se siguen como defectos.

Cómo se demuestra: El encargo o la orden de prueba que indique el alcance y el entorno de prueba, un informe que cubra el enfoque, las debilidades explotadas y su evaluación, más las entradas en el sistema de defectos o tickets con evidencia de la corrección o de una aceptación de riesgo justificada. Los proveedores pequeños suelen contratar esta prueba externamente con un presupuesto de tiempo acotado, o la encargan a una persona que no desarrolló el producto.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SVV-5

La independencia del personal de pruebas está definida y es adecuada al nivel de madurez previsto. Quien desarrolla un componente no lo publica basándose únicamente en sus propias pruebas, y a medida que aumenta el nivel de madurez, las pruebas quedan a cargo de una unidad organizativamente separada o de un tercero externo. La asignación real es trazable para cada prueba.

Cómo se demuestra: Una definición de roles dentro del proceso de desarrollo que muestre la separación entre creación y pruebas, más, para cada ejecución o informe de prueba, el nombre y el rol registrado de la persona que realizó la prueba. Un negocio de dos personas lo gestiona mediante revisión mutua con una nota documentada de cuatro vistas, y recurre a una persona externa para las pruebas de seguridad en profundidad.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

10 Práctica 6: Gestión de defectos de seguridad (DM) 6

DM-1 **Existe un canal definido a través del cual se reciben y registran los informes de debilidades de seguridad en el producto desde todas las direcciones: del propio equipo de desarrollo, de pruebas y revisiones, de clientes e integradores, de notificantes externos, y de avisos sobre componentes de terceros y de código abierto utilizados. El canal de notificación es localizable por terceros, y cada informe se registra con su fecha de recepción y su origen.** Documento

Cómo se demuestra: Una descripción del canal de notificación, el punto de contacto públicamente accesible (una página de seguridad, un archivo security.txt, o un buzón como security@), y el registro de entrada con fecha, origen y una breve descripción por cada informe. Una organización pequeña puede trabajar con un buzón compartido y una única hoja de cálculo o etiqueta de ticket, siempre que todos los informes acaben ahí, incluidos los planteados en el chat interno de desarrolladores.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

DM-2 **Cada informe entrante se clasifica y examina para determinar si es relevante para la seguridad y a qué productos, versiones y componentes afecta. Los informes que resultan no ser relevantes para la seguridad, o no aplicables, también se cierran indicando el motivo, en lugar de descartarse silenciosamente.**

Cómo se demuestra: Una nota de clasificación por cada informe que indique el resultado (relevante para la seguridad, sí o no), las versiones afectadas y el motivo de rechazo cuando corresponda, visible en el ticket o en la lista de entrada. Los equipos con un volumen bajo de informes pueden realizar la clasificación en una breve sesión periódica y registrar el resultado en dos frases por entrada.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

DM-3 **Los defectos de seguridad confirmados se evalúan con un método coherente: causa raíz, versiones y configuraciones afectadas, impacto potencial en la operación y la seguridad, explotabilidad y gravedad frente a una escala definida. El resultado de la evaluación se registra y es trazable.** Documento

Cómo se demuestra: Un registro de evaluación o un conjunto de campos de ticket para cada defecto que cubra la causa raíz, la gravedad y la escala aplicada (por ejemplo un sistema de puntuación común con un vector documentado), junto con la lista de versiones afectadas. Los equipos pequeños pueden apoyarse en una plantilla de campos fija en el sistema de tickets más media página que describa la escala y los umbrales que desencadenan una acción inmediata.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

DM-4 **Para cada defecto de seguridad evaluado se toma una decisión sobre cómo se va a tratar: corrección, medida compensatoria o una aceptación justificada del riesgo. La decisión se deriva de la gravedad, se asigna a una persona responsable y a una fecha límite, y el defecto se sigue hasta su cierre.** Documento

Cómo se demuestra: Una lista de acciones o el estado del ticket que muestre responsable, fecha objetivo, tipo de medida y una nota de cierre, vinculada a la línea base del código o a la versión en la que la corrección entra en vigor. Los riesgos residuales aceptados necesitan una breve justificación por escrito aprobada por la propiedad del producto. Una organización pequeña puede gestionar esto en un tablero de tickets con fechas límite, sin herramientas adicionales.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

DM-5 **Los usuarios afectados, los integradores y otras partes interesadas son informados sobre los defectos de seguridad tan pronto como la evaluación lo requiere, indicando las versiones afectadas, el impacto y la corrección o medida compensatoria disponible. Los plazos y el alcance de destinatarios de esa divulgación están definidos de antemano, al igual que el enfoque para los informes de terceros que llegan con su propio plazo de divulgación.**

Cómo se demuestra: Avisos o boletines de seguridad publicados con fecha y referencia de versión, la lista de distribución o el canal de suscriptores, y la regla escrita sobre plazos y divulgación coordinada. Los proveedores con pocos clientes pueden usar un único envío a una lista de clientes mantenida más una página de avisos fechada cuyos cambios están versionados.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

DM-6 **El tratamiento de los defectos de seguridad se revisa a intervalos fijos. La revisión analiza los casos abiertos y vencidos, el tiempo transcurrido entre el informe y la corrección, las causas raíz recurrentes y la eficacia de las medidas adoptadas. Las mejoras del proceso que resultan de la revisión se implementan y su implementación se sigue.** Documento

Cómo se demuestra: Acta de la revisión periódica con fecha, participantes, cifras de casos abiertos y vencidos, y una lista de mejoras acordadas con responsable y fecha límite. Una organización pequeña puede añadir este punto a una reunión trimestral existente y mantener las cifras y decisiones en una sola página.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

11 Práctica 7: Gestión de actualizaciones de seguridad (SUM) 5

SUM-1 **Cada actualización de seguridad del producto se verifica frente a las versiones de producto y entornos operativos soportados antes de publicarse a los clientes, y existe un registro que muestra que la actualización cierra la vulnerabilidad sin alterar la función prevista del producto.** Documento

Cómo se demuestra: Registro de pruebas por cada parche que cubra la versión de producto probada, la plataforma, los casos de prueba (eficacia frente a la vulnerabilidad más la regresión de funciones principales) y la aprobación de publicación. Un proveedor pequeño puede trabajar con una breve entrada de aprobación de parche en el ticket: ID de ticket, verificado por, verificado el, resultado, con el log de la ejecución de pruebas automatizadas adjunto.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SUM-2 **Para todos los componentes del producto que no se desarrollaron internamente (bibliotecas de terceros, sistema operativo, entornos de ejecución), está definido y evidenciado cómo se evalúan sus actualizaciones de seguridad y cómo se adoptan en el producto o se rechazan con una justificación documentada.** Documento

Cómo se demuestra: Inventario de componentes de las partes de terceros con versión y origen, más una entrada de evaluación por cada vulnerabilidad de terceros notificada, indicando la decisión (adoptar, no afectado, cubierto por una medida compensatoria) y la justificación. Los equipos pequeños ejecutan un escaneo automatizado de dependencias en la compilación y mantienen las decisiones como comentarios sobre el resultado del escaneo o en una lista de excepciones sencilla.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SUM-3 **Para cada actualización de seguridad publicada, los usuarios reciben información complementaria comprensible: qué versiones del producto están afectadas, qué vulnerabilidad se corrige, cuál es su gravedad, si hay que tener en cuenta efectos secundarios o medidas compensatorias, y cómo se instala la actualización.** Documento

Cómo se demuestra: Avisos de seguridad o notas de la versión publicados que indiquen el identificador de la vulnerabilidad, las versiones afectadas, la valoración de gravedad, los pasos de instalación y orientación para volver al estado anterior. Los proveedores pequeños mantienen una única página pública con una lista cronológica de avisos de seguridad y la enlazan desde dentro del producto.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SUM-4 **Existe una vía definida y protegida frente a manipulaciones a través de la cual los usuarios obtienen las actualizaciones de seguridad, y la autenticidad e integridad de una actualización se pueden verificar del lado del usuario antes de instalarla.**

Cómo se demuestra: Descripción del canal de entrega (área de descarga, servidor de actualizaciones, medio físico) junto con sus medidas de protección, más la firma digital o suma de comprobación por paquete e instrucciones que indiquen al usuario cómo verificarla. Los proveedores pequeños lo consiguen firmando en el servidor de compilación, publicando la suma de comprobación junto a la descarga y designando un lugar claro donde se guarda la clave pública.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SUM-5 **Existen objetivos de tiempo definidos para poner a disposición las actualizaciones de seguridad, graduados según la gravedad de la vulnerabilidad; los tiempos realmente alcanzados se siguen, y cualquier objetivo incumplido se justifica y se respalda con una medida provisional para los usuarios.** Documento

Cómo se demuestra: Especificación interna con una ventana de tiempo por categoría de gravedad (por ejemplo crítica <= 30 días, alta <= 90 días) y una evaluación por vulnerabilidad: fecha de informe, fecha de publicación del parche, días transcurridos, motivo de la desviación. Los proveedores pequeños mantienen esto como dos campos de fecha en el ticket de vulnerabilidad y revisan la lista una vez al trimestre en lugar de montar un sistema de métricas dedicado.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

12 Práctica 8: Directrices de seguridad para el despliegue y la operación del producto (SG) 7

SG-1 **Cada producto incluye una descripción de su estrategia de defensa en profundidad: nombra las capas de protección incorporadas en el propio producto, las relaciona con las amenazas que contrarrestan, y muestra qué efecto protector solo surge de la interacción entre varias capas.** Documento

Cómo se demuestra: Una sección en la documentación de producto entregada, o un concepto de seguridad independiente, que indique para cada capa de protección el mecanismo, la amenaza cubierta y los límites de su efecto. Una organización pequeña mantiene esto como una tabla de dos páginas: columna capa de protección, columna amenaza tomada de su propio modelo de amenazas, columna riesgo residual. Basta con una referencia cruzada al modelo de amenazas de SR-2, el contenido no tiene que mantenerse por duplicado.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SG-2 **La documentación nombra las medidas de seguridad que el producto no aporta por sí mismo sino que espera del entorno de despliegue, por ejemplo la segmentación de red, cortafuegos previos, control de acceso físico o un servicio de hora externo, y deja claro que el nivel de seguridad asegurado no se alcanza sin esas medidas.** Documento

Cómo se demuestra: Un capítulo de requisitos previos de despliegue en el manual, o un plano de arquitectura de referencia con zonas y conductos en el que se marquen explícitamente las medidas que debe aportar el propietario del activo. En la práctica ha demostrado ser útil una lista de supuestos sobre el entorno, derivada directamente del contexto de seguridad del producto y revisada en cada versión del producto.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SG-3 **Existe una guía de configuración base segura que enumera todos los ajustes, servicios, puertos e interfaces relevantes para la seguridad, indica el estado recomendado de entrega y describe el impacto de desviarse de esa recomendación.** Documento

Cómo se demuestra: Guía de fortalecimiento con una tabla de ajustes: parámetro, valor recomendado, efecto, efecto secundario al desviarse. Más la lista de servicios y puertos activos en la configuración predeterminada con la justificación de por qué permanecen habilitados. Un equipo pequeño mantiene esta tabla justo junto al archivo de configuración en el repositorio y la exporta a la documentación de entrega, de modo que se mantiene alineada con el producto.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SG-4 **Para la operación continua existe una guía que describe cómo se opera el producto de forma segura, se supervisa y se mantiene en su estado seguro, incluyendo copia de seguridad y restauración, registro de eventos y el tratamiento de los mensajes de eventos relevantes para la seguridad.** Documento

Cómo se demuestra: Guía de operación con secciones sobre registro de eventos, copias de seguridad, reinicio y mensajes de eventos. Como evidencia adicional, una lista de los mensajes relevantes para la seguridad que emite el producto, cada uno con una breve acción recomendada, de modo que el propietario del activo no tenga que interpretarlos por su cuenta.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SG-5 **La documentación explica cómo se configuran y mantienen las cuentas de usuario, los roles y los permisos del producto, en particular la separación de roles, el cambio de las credenciales predeterminadas y la eliminación de cuentas que ya no son necesarias.** Documento

Cómo se demuestra: Un capítulo de gestión de cuentas con una visión general de los roles y los permisos asignados a cada rol, más una nota explícita sobre las credenciales predeterminadas y su cambio en la puesta en marcha. En la práctica funciona bien una breve lista de verificación de puesta en marcha en el manual, que el propietario del activo pueda marcar y archivar.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SG-6 **Existe una guía para la retirada de servicio segura que describe la eliminación completa de los datos sensibles del producto, como credenciales, claves, datos de configuración y registros, antes de que el dispositivo se entregue a un tercero, se reutilice o se elimine.** Documento

Cómo se demuestra: Una sección de retirada de servicio que enumere cada ubicación de almacenamiento de datos sensibles dentro del producto y el procedimiento de borrado correspondiente, incluidos los casos en los que el borrado es técnicamente imposible y el hardware debe destruirse físicamente. Aquí ayuda una lista del almacenamiento persistente tomada de la descripción de arquitectura, ya que evita que se olvide alguna ubicación de almacenamiento.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación

SG-7 **La documentación de seguridad entregada a los usuarios se revisa antes de su publicación: es técnicamente correcta, coherente con la versión de producto entregada, completa frente al contenido previsto y comprensible para el público al que va dirigida, y se actualiza cada vez que cambia el producto.**

Cómo se demuestra: Un registro de revisión por documento y versión de producto con revisor, fecha, hallazgos y su cierre, vinculado a la aprobación de publicación. Una organización pequeña resuelve esto con el principio de cuatro vistas en la pull request de la documentación: un desarrollador revisa el contenido técnico, una segunda persona revisa la comprensibilidad, y la aprobación se registra en el ticket. Una versión solo se puede publicar una vez documentada la revisión.

◯ Abierto ◯ En curso ◯ Cumplido ◯ No aplicable

Evidencia / justificación