IEC 62443-4-1:2018 Ciclo de vida de desenvolvimento seguro de produtos para automação industrial

Ciclo de vida de desenvolvimento seguro, oito práticas

47 requisitos. Esta norma é certificável por um organismo acreditado. Versão de 07/2026.

A norma IEC 62443-4-1 permite certificação, mas o objeto é invulgar: o que é certificado é o processo de desenvolvimento de uma organização de desenvolvimento concreta, ou seja, uma versão documentada e concreta do ciclo de vida seguro. Não é certificado nem um produto nem uma pessoa. As vias são o ISASecure SDLA e o IECEE CB Scheme. Tal como as coisas estão hoje, esse certificado não gera uma presunção de conformidade com o Regulamento de Ciber-resiliência da UE (Cyber Resilience Act). Não deve ser confundida com a IEC 62443-4-2, que estabelece requisitos sobre o próprio componente. Esta lista é um auxiliar de trabalho para autoavaliação, não uma prova.

Empresa	Data	Elaborado por

5 Prática 1: Gestão da Segurança (SM) 13

SM-1 **Existe um ciclo de vida de desenvolvimento de produto definido, que mantém a segurança presente em todas as fases, desde o conceito inicial até à retirada de serviço do produto, e este ciclo de vida é o que é efetivamente seguido na prática.** Documento

Como se comprova: Descrição do processo ou instrução de trabalho que enumere as fases, os entregáveis por fase e os pontos de transição, juntamente com evidência de um projeto em curso que mostre que as fases foram efetivamente percorridas. Uma organização pequena pode gerir-se com uma página por fase mais uma lista de verificação no sistema de tickets; o que importa é que o processo documentado e a prática diária coincidam.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

SM-2 **Cada tarefa do ciclo de vida de desenvolvimento seguro tem um responsável atribuído, e essa atribuição é conhecida pelas pessoas envolvidas.** Documento

Como se comprova: Matriz de funções e responsabilidades que associa cada passo do processo a uma função nomeada, complementada com a atribuição atual de pessoas a essas funções. Com apenas um pequeno grupo de pessoas basta uma tabela com função, tarefa e pessoa; o importante é a regra de substituição para férias e baixas por doença.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

SM-3 **Está definido de forma rastreável quais os produtos, variantes, versões e componentes que estão sujeitos ao ciclo de vida de desenvolvimento seguro e quais não estão.** Documento

Como se comprova: Lista dos produtos e estados de versão incluídos no âmbito, com a justificação das inclusões e exclusões, atualizada a cada nova versão. Na prática, funciona bem uma coluna no resumo de produtos com um sim ou um não por linha mais uma frase de justificação.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

SM-4 **As pessoas que assumem tarefas de segurança possuem a competência técnica necessária para tal, e essa competência é desenvolvida e atualizada de forma deliberada.**

Como se comprova: Perfil de competências por função de segurança, registos de qualificação, plano de formação e registos de presença, complementados com um resumo das lacunas detetadas. As organizações pequenas evidenciam isto através de certificados, participação em conferências ou webinars e uma breve revisão anual de quem fecha qual lacuna e até quando, recorrendo a competência externa quando necessário.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

SM-5 **O âmbito do ciclo de vida de desenvolvimento seguro está delimitado e identifica os locais, unidades organizacionais, contribuições de fornecedores e ambientes de desenvolvimento envolvidos, juntamente com os limites desse âmbito.** Documento

Como se comprova: Declaração de âmbito que abrange locais, equipas, partes subcontratadas e sistemas, mais um esquema das interfaces externas. Quem desenvolve num único local documenta isto em poucas frases e identifica explicitamente o que fica de fora, como conjuntos desenvolvidos externamente ou alojamento por terceiros.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SM-6 **Para cada elemento entregue aos utilizadores, software, firmware, configurações e ficheiros anexos, é possível realizar uma verificação de integridade, de modo a que os destinatários possam detetar uma modificação não assinalada.**

Como se comprova: Assinaturas ou somas de verificação publicadas por pacote de entrega, uma descrição do método e um exemplo de uma versão real, juntamente com instruções para o cliente sobre como realizar a verificação. Para equipas pequenas, basta um ficheiro de soma de verificação assinado junto ao descarregamento mais um parágrafo nas notas de versão.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SM-7 **Os ambientes utilizados para desenvolvimento, compilação e testes estão protegidos contra acessos não autorizados e contra manipulações do código-fonte, das ferramentas de compilação e dos artefactos.**

Como se comprova: Conceito de controlo de acesso para o repositório, o servidor de compilação e os sistemas de teste, listas de acesso com a data da última revisão, registos de alterações relevantes para a segurança e evidência de que o acesso de produção e o de desenvolvimento estão separados. Sem um departamento de TI próprio, basta a autenticação com dois fatores, um ramo principal protegido com revisão obrigatória e uma revisão semestral de quem ainda tem acesso.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SM-8 **As chaves privadas utilizadas para assinar as entregas estão protegidas contra divulgação e uso indevido, e a sua utilização está restringida a pessoas e sistemas autorizados.**

Como se comprova: Descrição do armazenamento, acesso, renovação e revogação das chaves, evidência de um armazenamento protegido, como um token de hardware ou um serviço de gestão de chaves, mais registos das operações de assinatura. Uma organização pequena guarda a chave de assinatura num token de hardware, documenta as duas pessoas com acesso e mantém um procedimento pronto para o caso de perda.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SM-9 **Para os componentes comprados ou adotados, incluindo software de código aberto, estão definidas as expectativas de segurança em relação ao fornecedor, e estas são aplicadas durante a seleção.** Documento

Como se comprova: Requisitos de segurança nas especificações ou contratos com fornecedores, critérios de seleção para componentes de terceiros, um inventário de todos os componentes de terceiros com versão e origem, mais a avaliação de se o fornecedor cumpre as expectativas. Sem um departamento de compras, basta uma lista de componentes mantida com uma coluna que registe se as atualizações de segurança e os canais de comunicação do fornecedor foram verificados.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SM-10 **Os componentes desenvolvidos por encomenda por um terceiro estão sujeitos aos mesmos requisitos de segurança que o desenvolvimento interno, e o seu cumprimento é verificado.**

Como se comprova: Encomenda de compra ou documentos contratuais que indiquem as obrigações de segurança exigidas, evidência do fornecedor sobre as práticas aplicadas, registos de aceitação e resultados das verificações próprias sobre o trabalho entregue. Sem orçamento para auditorias, bastam uma garantia contratual, a entrega dos resultados de teste do fornecedor e uma verificação por amostragem própria antes da aceitação.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SM-11 **Os achados relacionados com a segurança provenientes de todas as fontes, testes, revisões, relatos de utilizadores e notificações de terceiros, são registados, o seu impacto é avaliado, é-lhes atribuído um responsável e uma data-limite, e são acompanhados até ao fecho.** Documento

Como se comprova: Sistema de defeitos ou tickets com uma marca específica para temas de segurança, e por cada entrada a avaliação de impacto, o responsável, a data-limite e a nota de fecho, mais um relatório dos pontos em aberto. Uma equipa pequena usa uma etiqueta no sistema de tickets existente e um ponto fixo na agenda da reunião semanal.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SM-12 **Antes de um produto ser lançado, é verificado e evidenciado que os passos previstos do ciclo de vida de desenvolvimento seguro foram efetivamente realizados e que os registos correspondentes foram produzidos.** Documento

Como se comprova: Revisão de lançamento por cada versão, comparando com os passos do processo, com referências aos registos correspondentes e uma decisão de lançamento documentada com data e assinatura. Na prática, funciona bem uma lista de verificação de lançamento que não permite o envio sem todas as caixas assinaladas; os pontos em aberto são justificados e recebem uma data.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SM-13 **O próprio ciclo de vida de desenvolvimento seguro é questionado e melhorado regularmente, a partir dos conhecimentos obtidos de incidentes, resultados de testes, retorno de clientes e da evolução do panorama de ameaças.**

Como se comprova: Registos da revisão do processo, por exemplo uma revisão de gestão ou uma retrospetiva, com as alterações de processo desencadeadas, o seu estado de implementação e uma referência à causa raiz. Quem utiliza os níveis de maturidade da norma regista o estado atual e o objetivo por cada prática; o nível de maturidade 4 exige precisamente esta evidência de melhoria contínua. Para uma organização pequena, basta uma reunião por ano com ata e três melhorias concretas.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

6 Prática 2: Especificação dos Requisitos de Segurança (SR) 5

SR-1 **É descrito o contexto de utilização previsto do produto: ambiente operacional esperado, medidas de segurança que se assume serem fornecidas por esse ambiente, grupos de utilizadores e funções previstos, limites de confiança assumidos, e as utilizações para as quais o produto explicitamente não se destina.** Documento

Como se comprova: Uma descrição do contexto de segurança do produto, seja como documento independente ou como secção fixa da especificação do produto, que abranja o ambiente de rede, as proteções externas assumidas, como uma firewall ou controlo de acesso físico, uma lista de funções e uma lista explícita de utilizações fora do âmbito. Uma organização pequena limita isto a duas páginas, junta um esquema simples do ambiente de fábrica, e faz com que o responsável do produto date e aprove o documento.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR-2 **Existe um modelo de ameaças para o produto que representa os fluxos de dados, as interfaces, os limites de confiança e as vias de ataque, identifica as ameaças resultantes e o seu possível impacto, e atribui contramedidas. É revisto e atualizado perante alterações relevantes e pelo menos uma vez por cada versão do produto, e os pontos em aberto são acompanhados até ao fecho.** Documento

Como se comprova: Modelo de ameaças com um diagrama de fluxo de dados, uma lista de ameaças por interface, contramedidas atribuídas e o estado dos pontos em aberto, mais um histórico de revisões com data e autor. Uma organização pequena pode trabalhar com uma tabela por interface, com colunas para o que poderia correr mal ali, quão grave seria, o que se faz a esse respeito e quem revê.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR-3 **Os requisitos de segurança do produto estão definidos e documentados. Abrangem os resultados do modelo de ameaças, o contexto de segurança do produto descrito, as obrigações legais e contratuais aplicáveis e o nível de segurança-alvo, e incluem as capacidades de segurança que o próprio produto tem de fornecer.** Documento

Como se comprova: Lista de requisitos ou ferramenta de gestão de requisitos com um identificador único por requisito, a origem de cada entrada, como uma ameaça, um contrato com o cliente ou uma obrigação legal, e o nível de segurança-alvo. Uma organização pequena gere isto como uma única tabela com uma coluna de ID fixa à qual a verificação e os testes se associam mais tarde.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

SR-4 **Cada requisito de segurança individual é redigido de forma inequívoca, sem contradições, testável e rastreável até a uma função ou interface concreta do produto, e contém a informação necessária para o verificar mais tarde sem esclarecimentos adicionais.**

Como se comprova: Uma amostra da lista de requisitos que mostre, para cada requisito, um critério de aceitação mensurável e a função ou interface afetada, juntamente com a correspondência entre requisito e caso de teste. Uma organização pequena verifica isto com um modelo de redação fixo e a pergunta de controlo sobre se é possível escrever um caso de teste a partir do requisito sem necessidade de voltar a perguntar.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

SR-5 **Os requisitos de segurança são revistos antes de serem utilizados na conceção e implementação, com a participação das partes afetadas, como o desenvolvimento, os testes, a propriedade do produto e, quando útil, as vendas ou o cliente. A revisão abrange a completude face ao modelo de ameaças e ao contexto de segurança do produto, a correção e a testabilidade. Os achados são registados e acompanhados até ao fecho.**

Como se comprova: Registo de revisão com data, participantes e as suas funções, a versão revista dos requisitos, uma lista de achados com responsável e estado de fecho, e uma nota de aprovação. Uma organização pequena trata isto como uma revisão entre duas pessoas, desenvolvimento e testes, com um registo breve e uma linha de aprovação na lista de requisitos.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

7 Prática 3: Segurança desde a Conceção (SD) 4

SD-1 **Cada produto possui uma descrição de conceção que capta os aspetos relevantes para a segurança da arquitetura: quais os componentes existentes, como comunicam entre si, onde correm os limites de confiança, quais as interfaces externas expostas e com que mecanismos os requisitos de segurança previamente definidos são concretizados na conceção.** Documento

Como se comprova: Documento de arquitetura ou especificação de conceção que contenha um diagrama que mostre os componentes, os fluxos de dados e os limites de confiança, mais uma tabela de correspondência entre cada requisito de segurança e o elemento de conceção que o implementa. A um fornecedor pequeno basta um diagrama mantido mais duas ou três páginas de explicação; o importante é que esteja sob controlo de versões no repositório e seja atualizado sempre que a arquitetura muda.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

SD-2 **A conceção é analisada sistematicamente à procura de ameaças. A análise identifica os objetivos do atacante, os limites de confiança e as interfaces afetadas, as ameaças resultantes juntamente com a sua classificação, e as contramedidas adotadas na conceção. É repetida sempre que a arquitetura ou o ambiente mudam de forma significativa, e as ameaças identificadas são acompanhadas até que tenha sido tomada uma decisão sobre cada uma delas.** Documento

Como se comprova: Modelo de ameaças por produto ou por cada versão principal, por exemplo uma tabela com colunas para ameaça, interface afetada, classificação, contramedida e estado, juntamente com a ata da sessão de modelação com participantes e data. Uma equipa pequena modela de forma pragmática numa sessão de duas a três horas seguindo o diagrama de arquitetura e regista os pontos em aberto como tickets, de modo que a evidência de acompanhamento surge sem esforço adicional.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

SD-3 **A conceção segue de forma demonstrável princípios de conceção segura reconhecidos, entre eles o privilégio mínimo, a superfície de ataque mínima, a defesa em profundidade, os valores predefinidos seguros, o comportamento seguro perante falhas e mecanismos de segurança tão simples e verificáveis quanto possível. A aplicação destes princípios é visível na conceção e está justificada.**

Como se comprova: Uma secção na descrição de conceção ou uma diretriz de conceção própria que identifique os princípios, mais evidência concreta por princípio no produto, como a matriz de privilégios dos serviços, a lista de portas abertas com a respetiva justificação, os valores predefinidos de entrega ou o comportamento documentado perante erros. Um fornecedor pequeno utiliza uma breve lista de verificação destes princípios como ponto fixo na revisão de conceção e arquiva a folha preenchida junto com a conceção.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SD-4 **A conceção é revista por pares qualificados antes de a implementação começar. A revisão abrange a completude face aos requisitos de segurança, a correção e eficácia dos mecanismos de segurança e os resultados da análise de ameaças. Participam pessoas com competência suficiente em segurança, os achados são registados e acompanhados até ao fecho.** Documento

Como se comprova: Registo de revisão com data, item em revisão incluindo a sua versão, participantes e as suas funções, lista de achados com estado e a decisão de aprovação. Uma equipa pequena anexa a revisão ao pull request dos documentos de conceção e deixa os achados como comentários com uma nota de fecho, o que evidencia o acompanhamento sem ferramentas adicionais. Quando falta competência de segurança internamente, contratar um revisor externo por horas para as conceções críticas é a via pragmática.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

8 Prática 4: Implementação Segura (SI) 2

SI-1 **Existe um processo definido para verificar a implementação real face à conceção segura: a revisão confirma que as medidas de proteção previstas na conceção estão realmente presentes e são eficazes no código, que a defesa em profundidade se mantém, e que não foram introduzidas novas vulnerabilidades durante a implementação. A revisão é realizada por pessoal devidamente qualificado, e qualquer desvio encontrado é registado e acompanhado até ao fecho.**

Como se comprova: Um procedimento escrito para a revisão de implementação, juntamente com registos de revisão por componente ou versão: o módulo revisto, a referência ao documento de conceção, a data, o revisor, os achados e o respetivo estado de resolução. Como evidência adequada servem as revisões de pull request com uma lista de verificação de segurança obrigatória, os resultados da análise estática de código com uma avaliação documentada de cada ocorrência, e as atas das sessões de revisão. Uma equipa pequena cobre isto com o princípio das quatro vistas, um modelo de revisão guardado no repositório em que cada medida de conceção é assinalada individualmente, e um ticket por cada achado em aberto. O ponto essencial é que o autor do código nunca seja o revisor desse mesmo código.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SI-2 **Aplicam-se regras vinculativas de codificação segura a todo o trabalho de desenvolvimento relacionado com a segurança, abrangendo pelo menos a prevenção de construções e funções inseguras conhecidas, o tratamento de entradas e erros, a gestão de memória e recursos, e a utilização de código de segurança já validado em vez de implementações próprias. As regras aplicam-se por cada linguagem de programação utilizada, são conhecidas por todos os programadores e são atualizadas quando necessário, por exemplo quando surgem novos padrões de ataque ou novas ferramentas.** Documento

Como se comprova: Um padrão de codificação segura aprovado com estado de versão, âmbito por linguagem e data de aprovação, complementado com evidência de que se aplica no trabalho diário: a configuração de linters e ferramentas de análise no repositório, uma regra de compilação que assinala infrações, e a lista de presenças na sessão informativa. As organizações pequenas não escrevem um padrão de raiz; declaram vinculativo um conjunto de regras públicas já estabelecido, acrescentam uma breve lista de regras próprias adicionais e ancoram a verificação no pipeline, de modo que o cumprimento é demonstrado automaticamente.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

9 Prática 5: Verificação e Validação da Segurança através de Testes (SVV) 5

SVV-1 **Cada requisito de produto relacionado com a segurança tem pelo menos um caso de teste atribuído, que demonstra que a função de proteção funciona conforme previsto em funcionamento normal, que se comporta conforme especificado perante entradas inválidas ou uso indevido, e que as configurações predefinidas de entrega do produto correspondem ao estado seguro. A execução e o resultado são registados para cada versão de software testada.** Documento

Como se comprova: Uma matriz de rastreabilidade que liga requisito, caso de teste e resultado, mais registos de teste que mostrem a data, a versão ou build testada e o nome da pessoa que realizou o teste. Um fornecedor pequeno limita-se a acrescentar uma coluna de ID de caso de teste à sua lista de requisitos e arquiva o registo de saída da execução de testes automatizados do pipeline de compilação como ficheiro anexo à respetiva versão.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SVV-2 **As contramedidas derivadas do modelo de ameaças são testadas especificamente para confirmar que efetivamente fecham a via de ataque assumida. Os testes são realizados face às ameaças identificadas, não apenas face a uma utilização conforme, e os pontos em aberto são incorporados no processo de gestão de defeitos.**

Como se comprova: Casos de teste que referenciam diretamente as entradas do modelo de ameaças, por exemplo um caso de abuso por cada ID de ameaça com o comportamento defensivo esperado, juntamente com os registos dessas execuções. Sem necessidade de maquinaria pesada, basta acrescentar ao modelo de ameaças uma coluna que referencie o caso de teste e a data da última verificação bem sucedida.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SVV-3 **O produto é examinado sistematicamente à procura de vulnerabilidades antes do lançamento. O âmbito abrange pelo menos: o exame das interfaces e serviços acessíveis externamente, testes com entradas malformadas e mutadas de forma aleatória, a revisão dos componentes de terceiros utilizados face a vulnerabilidades conhecidas e reportadas, e uma verificação de classes de fragilidade conhecidas no código próprio do fornecedor. Os achados são registados juntamente com a respetiva avaliação.** Documento

Como se comprova: Relatórios das ferramentas utilizadas, indicando nome da ferramenta, versão e o estado dos dados da base de vulnerabilidades, registos de fuzzing, uma lista de componentes de terceiros com a data da última comparação, e a lista de achados com avaliação e decisão. Um fornecedor pequeno combina ferramentas padrão gratuitas, uma verificação de dependências e uma verificação de portas e serviços contra o produto instalado, e arquiva os resultados por versão numa pasta.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SVV-4 **O candidato a lançamento é submetido a uma tentativa de ataque em condições realistas que tenta ativamente contornar os mecanismos de proteção, em vez de se limitar a consultá-los. O âmbito, as condições de contorno e os limites do teste são acordados previamente, e as fragilidades encontradas são geridas e acompanhadas como defeitos.**

Como se comprova: A encomenda ou ordem de teste que indique o âmbito e o ambiente de teste, um relatório que abranja a abordagem, as fragilidades exploradas e a respetiva avaliação, mais as entradas no sistema de defeitos ou tickets com evidência da correção ou de uma aceitação de risco justificada. Os fornecedores pequenos costumam contratar este teste externamente com um orçamento de tempo limitado, ou encarregam uma pessoa que não desenvolveu o produto.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SVV-5 **A independência do pessoal de testes está definida e é adequada ao nível de maturidade previsto. Quem desenvolve um componente não o lança apenas com base nos seus próprios testes, e à medida que o nível de maturidade aumenta, os testes ficam a cargo de uma unidade organizacionalmente separada ou de um terceiro externo. A atribuição real é rastreável para cada teste.**

Como se comprova: Uma definição de funções dentro do processo de desenvolvimento que mostre a separação entre criação e testes, mais, para cada execução ou relatório de teste, o nome e a função registados da pessoa que realizou o teste. Um negócio de duas pessoas gere isto através de revisão mútua com uma nota documentada de quatro vistas, e recorre a uma pessoa externa para os testes de segurança em profundidade.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

10 Prática 6: Gestão de Defeitos de Segurança (DM) 6

DM-1 **Existe um canal definido através do qual são recebidos e registados relatos de fragilidades de segurança no produto vindos de todas as direções: da própria equipa de desenvolvimento, de testes e revisões, de clientes e integradores, de relatores externos, e de avisos sobre componentes de terceiros e de código aberto utilizados. O canal de comunicação é localizável por terceiros, e cada relato é registado com a respetiva data de receção e origem.** Documento

Como se comprova: Uma descrição do canal de comunicação, o ponto de contacto publicamente acessível (uma página de segurança, um ficheiro security.txt, ou uma caixa de correio como security@), e o registo de entrada com data, origem e uma breve descrição por cada relato. Uma organização pequena pode trabalhar com uma caixa de correio partilhada e uma única folha de cálculo ou etiqueta de ticket, desde que todos os relatos acabem ali, incluindo os levantados no chat interno de programadores.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

DM-2 **Cada relato recebido é triado e examinado para determinar se é relevante para a segurança e a que produtos, versões e componentes afeta. Os relatos que se revelem não relevantes para a segurança, ou não aplicáveis, também são fechados com o motivo indicado, em vez de descartados silenciosamente.**

Como se comprova: Uma nota de triagem por cada relato que indique o resultado (relevante para a segurança, sim ou não), as versões afetadas e o motivo de rejeição quando aplicável, visível no ticket ou na lista de entrada. As equipas com um volume baixo de relatos podem realizar a triagem numa breve sessão periódica e registar o resultado em duas frases por entrada.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

DM-3 **Os defeitos de segurança confirmados são avaliados com um método coerente: causa raiz, versões e configurações afetadas, impacto potencial na operação e na segurança, explorabilidade e gravidade face a uma escala definida. O resultado da avaliação é registado e rastreável.** Documento

Como se comprova: Um registo de avaliação ou um conjunto de campos de ticket para cada defeito que abranja a causa raiz, a gravidade e a escala aplicada (por exemplo um sistema de pontuação comum com um vetor documentado), juntamente com a lista de versões afetadas. As equipas pequenas podem apoiar-se num modelo de campos fixo no sistema de tickets mais meia página que descreva a escala e os limiares que desencadeiam uma ação imediata.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

DM-4 **Para cada defeito de segurança avaliado é tomada uma decisão sobre como será tratado: correção, medida compensatória ou uma aceitação justificada do risco. A decisão decorre da gravidade, é atribuída a uma pessoa responsável e a uma data-limite, e o defeito é acompanhado até ao fecho.** Documento

Como se comprova: Uma lista de ações ou o estado do ticket que mostre o responsável, a data-alvo, o tipo de medida e uma nota de fecho, associada à linha de base do código ou à versão em que a correção entra em vigor. Os riscos residuais aceites necessitam de uma breve justificação por escrito aprovada pela propriedade do produto. Uma organização pequena pode gerir isto num quadro de tickets com datas-limite, sem ferramentas adicionais.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

DM-5 **Os utilizadores afetados, os integradores e outras partes interessadas são informados sobre os defeitos de segurança assim que a avaliação o exigir, indicando as versões afetadas, o impacto e a correção ou medida compensatória disponível. Os prazos e o âmbito de destinatários dessa divulgação estão definidos previamente, tal como a abordagem para os relatos de terceiros que chegam com o seu próprio prazo de divulgação.**

Como se comprova: Avisos ou boletins de segurança publicados com data e referência de versão, a lista de distribuição ou o canal de subscritores, e a regra escrita sobre prazos e divulgação coordenada. Os fornecedores com poucos clientes podem usar um único envio a uma lista de clientes mantida mais uma página de avisos datada cujas alterações são versionadas.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

DM-6 **O tratamento dos defeitos de segurança é revisto a intervalos fixos. A revisão analisa os casos em aberto e em atraso, o tempo decorrido entre o relato e a correção, as causas raiz recorrentes e a eficácia das medidas adotadas. As melhorias do processo resultantes da revisão são implementadas e a sua implementação é acompanhada.** Documento

Como se comprova: Ata da revisão periódica com data, participantes, números de casos em aberto e em atraso, e uma lista de melhorias acordadas com responsável e data-limite. Uma organização pequena pode acrescentar este ponto a uma reunião trimestral já existente e manter os números e decisões numa única página.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

11 Prática 7: Gestão de Atualizações de Segurança (SUM) 5

SUM-1 **Cada atualização de segurança do produto é verificada face às versões de produto e ambientes operacionais suportados antes de ser lançada aos clientes, e existe um registo que mostra que a atualização fecha a vulnerabilidade sem alterar a função prevista do produto.** Documento

Como se comprova: Registo de testes por cada correção que abranja a versão de produto testada, a plataforma, os casos de teste (eficácia face à vulnerabilidade mais a regressão de funções principais) e a aprovação de lançamento. Um fornecedor pequeno pode trabalhar com uma breve entrada de aprovação de correção no ticket: ID do ticket, verificado por, verificado em, resultado, com o registo da execução de testes automatizados anexado.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SUM-2 **Para todos os componentes do produto que não foram desenvolvidos internamente (bibliotecas de terceiros, sistema operativo, ambientes de execução), está definido e evidenciado como as respetivas atualizações de segurança são avaliadas e adotadas no produto ou rejeitadas com uma justificação documentada.** Documento

Como se comprova: Inventário de componentes das partes de terceiros com versão e origem, mais uma entrada de avaliação por cada vulnerabilidade de terceiros reportada, indicando a decisão (adotar, não afetado, coberto por medida compensatória) e a justificação. As equipas pequenas executam uma verificação automatizada de dependências na compilação e mantêm as decisões como comentários sobre o resultado da verificação ou numa lista de exceções simples.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SUM-3 **Para cada atualização de segurança lançada, os utilizadores recebem informação complementar compreensível: quais as versões de produto afetadas, qual a vulnerabilidade corrigida, qual a sua gravidade, se há efeitos secundários ou medidas compensatórias a observar, e como se instala a atualização.** Documento

Como se comprova: Avisos de segurança ou notas de versão publicados que indiquem o identificador da vulnerabilidade, as versões afetadas, a classificação de gravidade, os passos de instalação e orientação para reverter ao estado anterior. Os fornecedores pequenos mantêm uma única página pública com uma lista cronológica de avisos de segurança e ligam a ela a partir do próprio produto.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SUM-4 **Existe uma via definida e protegida contra manipulações através da qual os utilizadores obtêm as atualizações de segurança, e a autenticidade e integridade de uma atualização podem ser verificadas do lado do utilizador antes da instalação.**

Como se comprova: Descrição do canal de entrega (área de descarregamento, servidor de atualizações, suporte físico) juntamente com as respetivas medidas de proteção, mais a assinatura digital ou soma de verificação por pacote e instruções que indiquem ao utilizador como a verificar. Os fornecedores pequenos conseguem isto assinando no servidor de compilação, publicando a soma de verificação junto ao descarregamento e designando um local claro onde a chave pública é guardada.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SUM-5 **Existem objetivos de tempo definidos para disponibilizar as atualizações de segurança, graduados consoante a gravidade da vulnerabilidade; os tempos efetivamente alcançados são acompanhados, e qualquer objetivo não cumprido é justificado e apoiado por uma medida provisória para os utilizadores.** Documento

Como se comprova: Especificação interna com uma janela de tempo por categoria de gravidade (por exemplo crítica <= 30 dias, alta <= 90 dias) e uma avaliação por vulnerabilidade: data do relato, data de lançamento da correção, dias decorridos, motivo do desvio. Os fornecedores pequenos mantêm isto como dois campos de data no ticket de vulnerabilidade e revêem a lista uma vez por trimestre em vez de montar um sistema de métricas dedicado.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

12 Prática 8: Diretrizes de Segurança para a Implementação e Operação do Produto (SG) 7

SG-1 **Cada produto vem acompanhado de uma descrição da sua estratégia de defesa em profundidade: identifica as camadas de proteção incorporadas no próprio produto, associa-as às ameaças que contrariam, e mostra que efeito protetor só surge da interação entre várias camadas.** Documento

Como se comprova: Uma secção na documentação de produto entregue, ou um conceito de segurança independente, que indique para cada camada de proteção o mecanismo, a ameaça coberta e os limites do seu efeito. Uma organização pequena mantém isto como uma tabela de duas páginas: coluna camada de proteção, coluna ameaça retirada do seu próprio modelo de ameaças, coluna risco residual. Basta uma referência cruzada ao modelo de ameaças de SR-2, o conteúdo não tem de ser mantido em duplicado.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SG-2 **A documentação identifica as medidas de segurança que o produto não fornece por si mesmo mas que espera do ambiente de implementação, por exemplo a segmentação de rede, firewalls a montante, controlo de acesso físico ou um serviço de hora externo, e deixa claro que o nível de segurança assegurado não é alcançado sem essas medidas.** Documento

Como se comprova: Um capítulo de pré-requisitos de implementação no manual, ou um desenho de arquitetura de referência com zonas e condutas em que estão explicitamente assinaladas as medidas a fornecer pelo proprietário do ativo. Na prática, revelou-se útil uma lista de pressupostos sobre o ambiente, derivada diretamente do contexto de segurança do produto e revista em cada versão do produto.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SG-3 **Existe um guia de configuração base segura que enumera todas as definições, serviços, portas e interfaces relevantes para a segurança, indica o estado recomendado de entrega e descreve o impacto de se desviar dessa recomendação.** Documento

Como se comprova: Guia de reforço com uma tabela de definições: parâmetro, valor recomendado, efeito, efeito secundário ao desviar-se. Mais a lista de serviços e portas ativos na configuração predefinida com a justificação de por que permanecem ativados. Uma equipa pequena mantém esta tabela mesmo junto ao ficheiro de configuração no repositório e exporta-a para a documentação de entrega, de modo que se mantém alinhada com o produto.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SG-4 **Para a operação contínua existe um guia que descreve como o produto é operado de forma segura, monitorizado e mantido no seu estado seguro, incluindo cópia de segurança e restauro, registo de eventos e o tratamento das mensagens de eventos relevantes para a segurança.** Documento

Como se comprova: Guia de operação com secções sobre registo de eventos, cópias de segurança, reinício e mensagens de eventos. Como evidência adicional, uma lista das mensagens relevantes para a segurança que o produto emite, cada uma com uma breve ação recomendada, de modo que o proprietário do ativo não tenha de as interpretar sozinho.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SG-5 **A documentação explica como as contas de utilizador, funções e permissões do produto são configuradas e mantidas, em particular a separação de funções, a alteração das credenciais predefinidas e a remoção de contas que já não são necessárias.** Documento

Como se comprova: Um capítulo de gestão de contas com uma visão geral das funções e das permissões atribuídas a cada função, mais uma nota explícita sobre as credenciais predefinidas e a sua alteração na colocação em serviço. Na prática, funciona bem uma breve lista de verificação de colocação em serviço no manual, que o proprietário do ativo possa assinalar e arquivar.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SG-6 **Existe um guia para a retirada de serviço segura que descreve a remoção completa de dados sensíveis do produto, como credenciais, chaves, dados de configuração e registos, antes de o dispositivo ser entregue a um terceiro, reutilizado ou eliminado.** Documento

Como se comprova: Uma secção de retirada de serviço que enumere cada local de armazenamento de dados sensíveis dentro do produto e o respetivo procedimento de eliminação, incluindo os casos em que a eliminação é tecnicamente impossível e o hardware tem de ser fisicamente destruído. Aqui ajuda uma lista do armazenamento persistente retirada da descrição de arquitetura, pois evita que se esqueça algum local de armazenamento.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SG-7 **A documentação de segurança entregue aos utilizadores é revista antes do lançamento: é tecnicamente correta, coerente com a versão de produto entregue, completa face ao conteúdo previsto e compreensível para o público a que se destina, e é atualizada sempre que o produto muda.**

Como se comprova: Um registo de revisão por documento e versão de produto com revisor, data, achados e o respetivo fecho, associado à aprovação de lançamento. Uma organização pequena resolve isto com o princípio das quatro vistas no pull request da documentação: um programador revê o conteúdo técnico, uma segunda pessoa revê a compreensibilidade, e a aprovação é registada no ticket. Uma versão só pode ser lançada depois de a revisão estar documentada.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação