ISO 27002 - 8.25 - 8.34

8.25 Ciclo de Vida de desenvolvimento seguro

Controle: Convém que regras para o desenvolvimento seguro de software e sistemas sejam estabelecidas e aplicadas.

Propósito: Assegurar que a segurança da informação seja projetada e implementada dentro do ciclo de vida de desenvolvimento seguro de software e sistemas.

Orientação: O desenvolvimento seguro é um requisito para construir serviço, arquitetura, software e sistema seguros. Para isso, convém que sejam considerados os seguintes aspectos:

8.25 Ciclo de Vida de desenvolvimento seguro

- Separação dos ambientes de desenvolvimento, teste e produção;
- Orientação sobre a segurança no ciclo de vida do desenvolvimento de software:
  - Segurança na metodologia de desenvolvimento de software
  - Diretrizes de codificação seguras para cada linguagem de programação utilizada
- Requisitos de segurança na fase de especificação e design

8.26 Requisitos de segurança da aplicação

Controle: Convém que os requisitos de segurança da informação sejam identificados, especificados e aprovados ao desenvolver ou adquirir aplicações.

Propósito: Assegurar que todos os requisitos de segurança da informação sejam identificados e abordados ao desenvolver ou adquirir aplicações.

Orientação Geral: Convém que os requisitos de segurança de aplicações sejam identificados e especificados. Esses requisitos geralmente são determinados por meio de uma avaliação de risco. Convém que os requisitos sejam desenvolvidos com o apoio de especialistas em segurança da informação.

8.26 Requisitos de segurança da aplicação

- Nível de confiança na identidade das entidades;
- Identificação do tipo de informação e do nível de classificação a serem tratados pela aplicação;
- Necessidade de criptografar com segurança as comunicações entre todas as partes envolvidas;

Orientação Serviços Transacionais: Além disso, para aplicações que oferecem serviços transacionais entre a organização e um parceiro, convém que o seguinte seja considerado ao se identificarem requisitos de segurança da informação.

8.26 Requisitos de segurança da aplicação

- Nível de confiança que cada parte requer em cada identidade declarada pela outra parte;
- Processos de autorização associados a quem pode aprovar conteúdos, emitir ou assinar documentos transacionais importantes;
- Confidencialidade e integridade de quaisquer transações (por exemplo, pedidos, detalhes do endereço de entrega e confirmação de recibos);

Orientação Pedidos eletrônicos e aplicações de pagamentos: Além disso, para aplicações envolvendo pedidos eletrônicos e pagamento, convém que o seguinte seja considerado.

8.26 Requisitos de segurança da aplicação

- Requisitos para manter a confidencialidade e integridade das informações das ordens de pagamento;
- Armazenamento de detalhes de transações fora de qualquer ambiente acessível ao público (por exemplo, em uma plataforma de armazenamento existente na intranet organizacional, e não retido e exposto em mídia de armazenamento eletrônico diretamente acessível da internet);
- Evitamento de perdas ou duplicação de informações de transação;

8.27 Princípios de arquitetura e engenharia de sistemas seguros

Controle: Convém que princípios de engenharia para sistemas de segurança sejam estabelecidos, documentados, mantidos e aplicados a qualquer atividade de desenvolvimento de sistemas.

Propósito: Assegurar que os sistemas de informação sejam projetados, implementados e operados com segurança dentro do ciclo de vida de desenvolvimento.

Orientação: Convém que a segurança seja projetada em todas as camadas de arquitetura (negócios, dados, aplicações e tecnologia). Convém que os princípios de engenharia de sistemas seguros incluam a análise de:

8.27 Princípios de arquitetura e engenharia de sistemas seguros

- Toda a gama de controles de segurança necessários para proteger as informações e os sistemas contra ameaças identificadas;
- Capacidades dos controles de segurança para prevenir, detectar ou responder a eventos de segurança;
- Controles de segurança específicos requeridos por determinados processos de negócios (por exemplo, criptografia de informações sensíveis, verificação de integridade e assinatura digital de informações);

8.27 Princípios de arquitetura e engenharia de sistemas seguros

Convém que os princípios de engenharia de segurança levem em conta:

- Necessidade de se integrar com uma arquitetura de segurança;
- Capacidade da organização para desenvolver e apoiar a tecnologia escolhida;
- Custo, tempo e complexidade para atender aos requisitos de segurança;

Convém que a engenharia segura do sistema envolva:

- Uma análise crítica de design orientada à segurança para ajudar a identificar vulnerabilidades de segurança da informação e assegurar que os controles de segurança sejam especificados e atendam aos requisitos de segurança;

8.27 Princípios de arquitetura e engenharia de sistemas seguros

Convém que a engenharia segura do sistema envolva:

- Uma análise crítica de design orientada à segurança para ajudar a identificar vulnerabilidades de segurança da informação e assegurar que os controles de segurança sejam especificados e atendam aos requisitos de segurança;
- Documentação e reconhecimento formal de controles de segurança que não atendem totalmente aos requisitos (por exemplo, devido aos requisitos de segurança sobrepostos);

8.27 Princípios de arquitetura e engenharia de sistemas seguros

Convém que a organização considere os princípios de “confiança zero”, como:

- Assumir que os sistemas de informação da organização já estão violados e, portanto, não depender apenas da segurança do perímetro de rede;
- Empregar uma abordagem “nunca confie e sempre verifique” para o acesso aos sistemas de informação;
- Verificar cada solicitação a um sistema de informações, como se tivesse se originado de uma rede aberta e externa, mesmo que essas solicitações se originem internamente à organização(ou seja, não confiar automaticamente em nada dentro ou fora de seus perímetros)

8.28 Codificação Segura

Controle: Convém que princípios de codificação segura sejam aplicados ao desenvolvimento de software.

Propósito: Assegurar que o software seja escrito com segurança, reduzindo assim o número de potenciais vulnerabilidades de segurança da informação no software.

Orientação Geral: Convém que a organização estabeleça processos em toda a organização para fornecer uma boa governança para uma codificação segura. Convém que uma linha de base segura mínima seja estabelecida e aplicada.

8.28 Codificação Segura

Planejamento e antes da codificação: Convém que princípios de codificação segura sejam usados tanto em novos desenvolvimentos quanto em cenários de reutilização. Convém que estes princípios sejam aplicados às atividades de desenvolvimento tanto dentro da organização quanto em produtos e serviços fornecidos por ela a terceiros. Convém que o planejamento e os pré-requisitos antes da codificação incluam:

- Configuração de ferramentas de desenvolvimento, como ambientes integrados de desenvolvimento (IDE), para ajudar a impor a criação de código seguro;
- Padrões de codificação seguros e, quando relevante, obrigando seu uso;

8.28 Codificação Segura

Durante a codificação:

- Práticas de codificação seguras específicas das linguagens e técnicas de programação que estão sendo utilizadas;
- Utilização de técnicas seguras de programação, como programação em duplas, refactoring, revisão por pares.

Análise crítica e manutenção(Após operar o código):

- Selecionar, autorizar e reutilizar componentes bem avaliados, particularmente autenticação e componentes criptográficos**;**
- Utilizar licença, segurança e histórico dos componentes externos;

8.28 Codificação Segura

Se forem usadas ferramentas externas e bibliotecas, convém que as organizações considerem:

- Assegurar que as bibliotecas externas sejam gerenciadas e atualizadas regularmente;
- Assegurar que o software seja mantido, rastreado e originário de fontes comprovadas e respeitáveis;
- Selecionar, autorizar e reutilizar componentes bem avaliados, particularmente autenticação e componentes criptográficos

8.28 Codificação Segura

Quando um pacote de software precisar ser modifcado, convém que sejam considerados os seguintes pontos:

- O risco de controles incorporados e processos de integridade serem comprometidos;
- Impacto se a organização se tornar responsável pela manutenção futura do software como resultado de mudanças;
- Compatibilidade com outros softwares em uso.

8.29 Testes de segurança em desenvolvimento e aceitação

Controle: Convém que os processos de teste de segurança sejam definidos e implementados no ciclo de vida do desenvolvimento.

Propósito Validar se os requisitos de segurança da informação são atendidos quando as aplicações ou códigos são implantados no ambiente de produção.

Orientação: Convém que novos sistemas de informação, upgrades e novas versões sejam exaustivamente testados e verificados durante os processos de desenvolvimento. Convém que os testes de segurança sejam parte integrante dos testes para sistemas ou seus componentes.

8.29 Testes de segurança em desenvolvimento e aceitação

- Funções de segurança por exemplo, autenticação do usuário, restrição de acesso e uso de criptografia ;
- Codificação segura;
- Configurações seguras, incluindo a de sistemas operacionais, firewalls e outros componentes de segurança.

8.29 Testes de segurança em desenvolvimento e aceitação

- Cronograma detalhado de atividades e testes;
- Entradas e saídas esperadas sob uma série de condições;
- Critérios para avaliar os resultados;
- Decisão para outras ações, conforme necessário.

8.30 Desenvolvimento terceirizado

Controle: Convém que a organização dirija, monitore e analise criticamente as atividades relacionadas à terceirização de desenvolvimento de sistemas.

Propósito Assegurar que as medidas de segurança da informação requeridas pela organização sejam implementadas na terceirização do desenvolvimento de sistemas.

Orientação: Quando o desenvolvimento do sistema é terceirizado, convém que a organização comunique e concorde com requisitos e expectativas, monitore e analise criticamente de forma contínua se a entrega de trabalhos terceirizados atende a essas expectativas.

8.30 Desenvolvimento terceirizado

- contratos de licenciamento, propriedade de código e direitos de propriedade intelectual relacionados com o conteúdo de terceiros;
- requisitos contratuais para práticas seguras de projeto, codificação e teste.
- provisão do modelo de ameaça a ser considerado por desenvolvedores externos;
- teste de aceitação para a qualidade e precisão dos produtos;
- provisão de evidências de que níveis mínimos aceitáveis de segurança e capacidades de privacidade estão estabelecidos (por exemplo, relatórios de garantia)

8.31 Separação dos ambientes de desenvolvimento, teste e produção

Controle: Convém que ambientes de desenvolvimento, testes e produção sejam separados e protegidos.

Propósito: Proteger o ambiente de produção e os dados de comprometimento por meio de atividades de desenvolvimento e teste.

Orientação: Convém que o nível de separação entre ambientes de produção, testes e desenvolvimento necessários para evitar problemas de produção seja identificado e implementado

8.31 Separação dos ambientes de desenvolvimento, teste e produção

- separar adequadamente os sistemas de desenvolvimento e produção e operação deles em diferentes domínios (por exemplo, em ambientes virtuais ou físicos separados);
- definir, documentar e implementar regras e autorização para a implantação de software do desenvolvimento ao status de produção;
- testar alterações nos sistemas de produção e aplicações em um ambiente de teste ou preparação antes de serem aplicados aos sistemas de produção;

8.32 Gestão de mudanças

Controle: Convém que mudanças nos recursos de tratamento de informações e sistemas de informação estejam sujeitas a procedimentos de gestão de mudanças.

Propósito Preservar a segurança da informação ao executar mudanças.

Orientação: Convém que a introdução de novos sistemas e grandes mudanças nos sistemas existentes sigam as regras acordadas e um processo formal de documentação, especificação, testes, controle de qualidade e implementação gerenciada.

8.32 Gestão de mudanças

- planejamento e avaliação do impacto potencial das mudanças, considerando todas as dependências.
- autorização de mudanças;
- comunicação de mudanças às partes interessadas pertinentes;
- testes e aceitação de testes para as mudanças
- implementação de mudanças, incluindo planos de implantação;

8.33 Informações de teste

Controle: Convém que as informações de teste sejam adequadamente selecionadas, protegidas e gerenciadas.

Propósito Assegurar a relevância dos testes e a proteção das informações operacionais utilizadas para testes.

Orientação: Convém que as informações de teste sejam selecionadas para assegurar a confiabilidade dos resultados dos testes e a confidencialidade das informações operacionais relevantes.

8.33 Informações de teste

Controle: Convém que as informações de teste sejam adequadamente selecionadas, protegidas e gerenciadas.

Propósito Assegurar a relevância dos testes e a proteção das informações operacionais utilizadas para testes.

Orientação: Convém que as informações de teste sejam selecionadas para assegurar a confiabilidade dos resultados dos testes e a confidencialidade das informações operacionais relevantes.

8.34 Proteção de sistemas de informação durante os testes de auditoria

Controle: Convém que testes de auditoria e outras atividades de garantia envolvendo a avaliação de sistemas operacionais sejam planejados e acordados entre o testador e a gestão apropriada.

Propósito Minimizar o impacto da auditoria e outras atividades de garantia em sistemas operacionais e processos de negócio.

Orientação: Minimizar o impacto da auditoria e outras atividades de garantia em sistemas operacionais e processos de negócio.

8.34 Proteção de sistemas de informação durante os testes de auditoria

- acordar pedidos de acesso da auditoria a sistemas e dados com a gestão apropriada;
- acordar e controlar o escopo dos testes de auditoria técnica;
- imitar testes de auditoria a acesso somente para leitura de software e dados. Se o acesso somente para leitura não estiver disponível para obter as informações necessárias, executar o teste por um administrador experiente que tenha os direitos de acesso necessários em nome do auditor
- e o acesso for concedido, estabelecer e verificar os requisitos de segurança (por exemplo, antivírus e patches) dos dispositivos utilizados para acessar os sistemas (por exemplo, laptops ou tablets) antes de permitir o acesso;

Leituras interessantes