Cebraspe
Centro Brasileiro de Pesquisa em Avaliação e Seleção e de Promoção de Eventos

CONCURSO PÚBLICO

TRIBUNAL DE CONTAS DO ESTADO DE RONDÔNIA

CARGO 1: ANALISTA DE TECNOLOGIA DA INFORMAÇÃO
ESPECIALIDADE: DESENVOLVIMENTO DE SISTEMAS

PROVA DISCURSIVA

Aplicação: 20/10/2019

PADRÃO DE RESPOSTA DEFINITIVO

1 Requisitos de segurança de sistemas de informação (objetivo, controle e diretrizes para implementação)

Na norma NBR ISO/IEC n.º 27002:2013, a segurança no desenvolvimento de sistemas é abordada no capítulo 14. O objetivo é garantir que a segurança da informação integre todo o ciclo de vida dos sistemas de informação. Propõe-se como controle que os requisitos relacionados à segurança da informação sejam incluídos nos requisitos para novos sistemas de informação ou melhorias dos sistemas de informação já existentes. As principais diretrizes para implementação desse controle são:

1. identificação dos requisitos por meio de vários métodos, como de conformidade oriundos de política e regulamentações, modelos de ameaças, análises críticas de incidentes e uso de limiares de vulnerabilidade;
2. documentação e análise crítica dos requisitos pelas partes interessadas;
3. reflexão sobre o valor da informação e o potencial impacto resultante de uma falha de segurança da informação;
4. integração da identificação, da gestão dos requisitos de segurança da informação e dos processos aos estágios iniciais dos projetos de sistemas de informação.

2 Princípios para se projetar sistemas seguros (controle e diretrizes para implementação)

A norma propõe como controle estabelecimento, documentação, manutenção e aplicação de princípios para se projetar sistemas seguros para qualquer implementação de sistemas de informação. As principais diretrizes para implementação são:

1. estabelecimento, documentação e aplicação de procedimentos para projetar sistemas de informação seguros nas atividades de engenharia de sistemas da organização, embasados em engenharia de segurança;
2. projeção da segurança em todas as camadas da arquitetura (negócios, dados, aplicações e tecnologia), com balanceamento das necessidades de segurança da informação e de acessibilidade;
3. análise de novas tecnologias quanto aos riscos de segurança e análise crítica do projeto com base em ataques conhecidos;
4. análise crítica regular dos princípios e procedimentos estabelecidos, para assegurar que estejam contribuindo para melhorar as normas de segurança, garantir atualidade contra novas ameaças e permanecer aplicáveis aos avanços das soluções e tecnologias.

3 Ambiente seguro para o desenvolvimento de sistemas (controle e diretrizes para implementação)

A norma define como controle que as organizações estabeleçam e protejam ambientes seguros de desenvolvimento que cubram todo o ciclo de vida de desenvolvimento de sistema, e indica como principais diretrizes para implementação:

1. avaliação dos riscos dos esforços de desenvolvimento de sistemas e estabelecimento de ambientes de desenvolvimento seguro, considerando-se a sensibilidade dos dados processados, armazenados e transmitidos; requisitos aplicáveis; controles de segurança já implementados; confiabilidade das pessoas do ambiente; grau de terceirização do desenvolvimento do sistema; necessidade de segregação entre os diferentes ambientes de desenvolvimento; controle de acesso ao ambiente de desenvolvimento; monitoramento de mudanças do ambiente e do código armazenado; *backups* armazenados em locais seguros externos à organização;
2. documentação dos processos correspondentes em procedimentos de desenvolvimento seguro e fornecimento desses procedimentos a todos os indivíduos que deles necessitam.

Quesito 2.1

0 – Não apresentou o objetivo, nem o controle, nem nenhuma diretriz para implementação.
1 – Apresentou o objetivo, ou o controle, ou uma diretriz para implementação.
2 – Apresentou o objetivo, o controle e uma diretriz para implementação.
3 – Apresentou o objetivo, o controle e duas diretrizes para implementação.
4 – Apresentou o objetivo, o controle e três ou mais diretrizes para implementação.

Quesito 2.2
0 – Não apresentou o controle, nem diretriz para implementação.
1 – Apresentou o controle ou uma diretriz para implementação.
2 – Apresentou o controle e uma diretriz para implementação.
3 – Apresentou o controle e duas diretrizes para implementação.
4 – Apresentou o controle e três ou mais diretrizes para implementação.

Quesito 2.3
0 – Não apresentou o controle, nem diretriz para implementação .
1 – Apresentou o controle ou uma diretriz para implementação.
2 – Apresentou o controle e uma diretriz para implementação.
3 – Apresentou o controle e duas diretrizes para implementação.