ESTUDO DIRIGIDO - 29/09/2023

Confiança e Proteção de Software

INSTRUÇÕES

Com base nos conhecimentos apresentados na aula, e pesquisas relacionadas, realize os exercícios a seguir:

Após, encaminhe suas as respostas em um arquivo no **Classroom**.

DATA DE ENTREGA: **até 06/10/2023**

EXERCÍCIO 01

A) Sugira seis razões pelas quais, na maioria dos sistemas sociotécnicos, a confiança de software é importante.

- Tomada de decisão: A confiança no software é importante para que os gestores confiem nas informações fornecidas pelo sistema para fazer escolhas.
- Segurança: A confiança no software é importante para garantir a segurança dos dados e do sistema.
- Satisfação do cliente: A confiança no software é importante para o cliente decidir se continua usando e recomendando o sistema.
- Colaboração entre a equipe: A confiança no software é importante para a colaboração entre membros da equipe, quando os membros de uma equipe confiam que o software vai deixar a comunicação mais fácil, eles ficam mais tranquilos ao utilizá-lo.
- Facilidade de inovação: A confiança no software é importante para a inovação, pois quando a equipe confia no software, é mais fácil experimentar novas tecnologias.
- Longevidade: A confiança no software é importante para a longevidade, pois um software confiável tem mais chances de serem atualizados e se manterem úteis por mais tempo.

B) Quais são as dimensões mais importantes da confiança de sistema?

- A disponibilidade de um sistema é a probabilidade de ele ser capaz de prestar serviços a seus usuários quando solicitado.
- A confiabilidade é a probabilidade de os serviços de sistema serem entregues conforme especificado.
- A segurança de um sistema é um atributo que reflete a capacidade do sistema de funcionar, em condições normais ou não, sem causar danos a pessoas ou ao ambiente.
- A proteção reflete a capacidade de um sistema de se proteger contra ataques externos. Falhas de proteção podem levar a perda de disponibilidade, danos ao sistema ou aos dados, ou vazamento de informações para pessoas não autorizadas.

C) Um sistema de software crítico de segurança para o tratamento de pacientes com câncer tem dois componentes principais:

• Uma máquina de radioterapia que provê doses controladas de radiação para as regiões de tumor. Essa máquina é controlada por um sistema de software embutido.

• Um banco de dados de tratamento que inclui detalhes sobre o tratamento de cada paciente. Os requisitos de tratamento são inseridos nesse banco de dados e automaticamente transferidos para a máquina de radioterapia.

Identifique três perigos que podem surgir nesse sistema. Para cada perigo, sugira um requisito de defesa que reduzirá a probabilidade de esses perigos resultarem em um acidente. Explique por que sua defesa sugerida poderá reduzir o risco associado ao perigo.

1 - Dados corrompidos:

Solução: Backups. O backup frequente dos dados do tratamento ajuda a proteger contra a perda de informações críticas.

2 - Falha de hardware na máquina de radioterapia:

Solução: Monitoramento do hardware. O monitoramento contínuo do hardware permite detectar possíveis falhas, podendo assim solucioná-las com antecedência.

3 - Falha de comunicação entre o Banco de Dados e a Máquina de Radioterapia.

Solução: Verificação da Integridade dos Dados. A verificação de integridade dos dados ajuda a garantir que os dados inseridos no banco de dados de tratamento sejam transferidos sem erros para a máquina de radioterapia. Isso reduz o risco de falhas de comunicação que poderiam levar a tratamentos incorretos.

D) - Existem dois requisitos de segurança essenciais para o sistema de proteção de um trem:

• O trem não deve entrar em um segmento de via sinalizado com uma luz vermelha.

• O trem não pode exceder o limite de velocidade estabelecido para um segmento de via.

Supondo que o status de sinal e o limite de velocidade para o segmento de via sejam transmitidos para o software a bordo no trem antes de ele entrar no segmento de via, proponha **cinco** possíveis requisitos funcionais de sistema para o software a bordo que possam ser gerados a partir dos requisitos de segurança de sistema.

- Monitoramento de Sinalização:
    - O software a bordo deve monitorar o status das luzes de sinalização ao longo da via. Se uma luz vermelha for detectada em um segmento de via para o qual o trem está se aproximando, o software deve ativar automaticamente os freios de emergência e interromper a movimentação do trem.
- Limite de Velocidade:
    - O software a bordo deve receber informações sobre os limites de velocidade da via. O software deve ajustar automaticamente a velocidade do trem para garantir que ela não exceda o limite de velocidade permitido.
- Comunicação com o Sistema de Controle Central:
    - O software a bordo deve ser capaz de se comunicar com o sistema de controle

central da ferrovia, a comunicação deve ser estabelecida para relatar eventos de segurança e receber instruções ou atualizações de segurança do sistema central.

- Verificação de Integridade dos Sensores:
    - O software deve realizar verificações periódicas da integridade e do funcionamento correto dos sensores responsáveis por detectar luzes de sinalização e limites de velocidade. Em caso de falha ou mau funcionamento de um sensor, o sistema deve ser capaz de gerar um alerta e tomar medidas adequadas para manter a segurança.
- Sistema de Parada de Emergência Manual:
    - O software deve incluir um sistema de parada de emergência manual que permita ao maquinista interromper o trem imediatamente em caso de situações de emergência. Esse sistema deve ser projetado para anular quaisquer comandos automáticos do software em situações críticas.

E) - Explique por que, durante o desenvolvimento de um sistema, existe a necessidade da avaliação preliminar de riscos de proteção e da avaliação de riscos de proteção de ciclo de vida.

A avaliação preliminar de riscos de proteção estabelece uma base sólida para o desenvolvimento seguro do sistema, ajudando a identificar e mitigar riscos potenciais desde o início do processo de design. Isso não apenas protege os ativos e as pessoas envolvidas, mas também economiza recursos e evita problemas de segurança dispendiosos no futuro.

Enquanto a avaliação de riscos de ciclo de vida garante que a segurança seja mantida ao longo da vida útil do sistema, adaptando-se a mudanças e mantendo a conformidade com regulamentações em constante evolução.