PETROBRAS

Engenheiro(a) de Equipamentos Júnior - Eletrônica
Engenheiro(a) Júnior - Área: Automação

Redes de Computadores e Redes Industriais

Questões Resolvidas Passo a Passo

Produzido por Exatas Concursos
www.exatas.com.br
v3

Índice De Questões

QUESTÕES RESOLVIDAS NESTA APOSTILA: 70

QUESTÃO 1

ENGENHEIRO(A) DE EQUIPAMENTOS JÚNIOR - ELETRÔNICA - PETROBRAS 2018.1

Em automação industrial utilizam-se as redes SCADA que são a infraestrutura utilizada para controlar vários processos. A Tecnologia da Informação (TI) vem ajudando as indústrias a se protegerem e conservarem seus dados contra ataques externos.
Nesse contexto, dentre as ações de segurança em sistemas de controle consta(m) a(o)

(A) adoção de arquitetura redundante à prova de falhas e de fácil acesso tanto interno quanto externo ao ambiente industrial.
(B) análise e a compreensão dos riscos de segurança cibernética, através de uma análise de risco.
(C) habilitação dos pontos de comunicação em desuso e a garantia da possibilidade de causar impactos na segurança.
(D) documentação da infraestrutura de sistemas nos ambientes industriais e a garantia do acesso sem ordem às restrições adequadas.
(E) acesso físico aos equipamentos e aos dispositivos de pessoas não autorizadas.

RESOLUÇÃO

A segurança da informação refere-se à proteção existente sobre as informações pertencentes a uma empresa ou pessoa. Segundo *Tanenbaum (2003)*, os problemas de segurança das redes podem ser divididos nas seguintes áreas: confidencialidade, autenticidade, integridade, irretratabilidade, auditoria, disponibilidade e controle de acesso.

Os ativos da informação estão sujeitos a diversos eventos nocivos à sua segurança: ameaças, vulnerabilidades e incidentes. Estas categorias compõem e caracterizam os riscos. A integração de sistemas SCADA com redes corporativas insere novas vulnerabilidades no sistema e acaba compartilhando eventuais problemas de segurança que antes estavam restritos em cada rede. Por isso, a crescente preocupação com segurança da informação dentro de uma rede de automação.

(A) INCORRETA. A disponibilidade da rede pode ser preservada com adoção de arquiteturas redundantes, a prova de falhas, para os sistemas mais críticos e definição de capacidades de resposta frente aos riscos. O fácil acesso ao sistema de controle torna vulnerável a rede. Uma ação para ter maior segurança é restringir o acesso lógico e os direitos de acesso dos diferentes usuários dos sistemas.

(B) CORRETA. É importante analisar e compreender os riscos de Segurança Cibernética Industrial através de uma análise de riscos, identificando e avaliando os sistemas existentes, suas características técnicas e funcionalidades, entendendo ameaças, impactos e vulnerabilidades.

(C) INCORRETA. Os pontos de comunicação em desuso devem ser desabilitados para minimizar a possibilidade de um acesso indevido causar impacto à segurança do sistema.

(D) INCORRETA. Um Programa de Segurança para Sistemas de Automação e Controle incorpora normalmente documentar a infraestrutura de sistemas nos ambientes industriais. Já os acessos devem ser concedidos, mas sempre observando as restrições adequadas implantadas geralmente pelos sistemas de autenticação de credenciais.

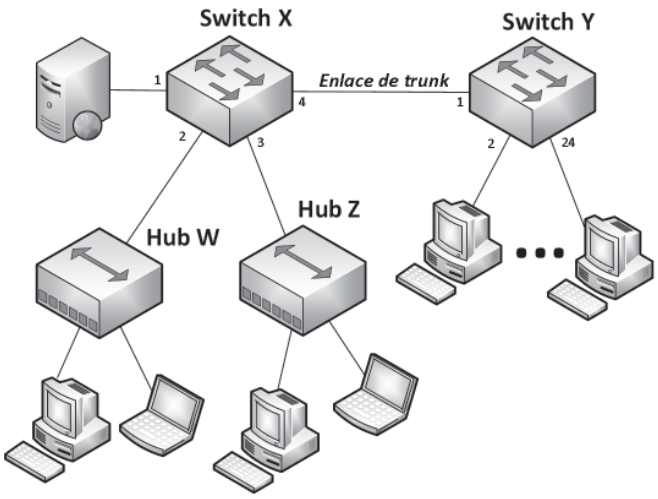
(E) INCORRETA. É importante restringir o acesso físico aos equipamentos e dispositivos para assegurar que não existe acesso não autorizado.

ALTERNATIVA (B)

QUESTÃO 2

ENGENHEIRO(A) DE EQUIPAMENTOS JÚNIOR - ELETRÔNICA - PETROBRAS 2018.1

Um administrador de rede projetou uma solução para a conectividade de uma empresa, utilizando 2 Switches (de nível 2) e 2 Hubs, conforme ilustra a Figura abaixo.



O Switch X, com 4 interfaces IEEE 802.3 1000BASE-T, tem sua interface 4 conectada à interface 1 do Switch Y por um enlace de trunk (seguindo o padrão IEEE 802.1Q). O Switch Y, com 24 interfaces IEEE 802.3 1000BASE-T, além da interface que o interliga ao Switch X (pelo enlace de trunk), está sendo utilizado para conectar 23 terminais de usuários (interfaces 2 a 24). Duas das três interfaces restantes do Switch X (interfaces 2 e 3) estão ligadas aos Hubs (Hub W e Hub Z – que operam como repetidores de nível 1), cada qual com 12 interfaces 100BASE-T. A interface restante (interface 1) do Switch X está ligada a um servidor HTTP.
A interface 1 do Switch X foi configurada para pertencer à VLAN 3; já as interfaces 2 e 3 desse mesmo Switch foram configuradas para pertencerem à VLAN 6. No Switch Y, 12 das 23 estações pertencem à VLAN 6, e as 11 restantes pertencem à VLAN 9.

Sem levar em conta o enlace de trunk, o número de domínios de colisão e de difusão pelos quais as estações se espalham nesse cenário são, respectivamente:

(A) 1 e 3
(B) 3 e 3
(C) 24 e 26
(D) 26 e 3
(E) 26 e 24

QUESTÃO 28

ENGENHEIRO(A) DE EQUIPAMENTOS JÚNIOR - ELETRÔNICA - PETROBRAS 2011

Uma rede com acesso à internet comporta uma sub-rede, configurada na notação CIDR pelo IP 149.187.160.0/21.

A máscara e o endereço de *broadcasting* para essa sub-rede são, respectivamente,

(A) 255.255.248.0 e 149.187.167.255
(B) 255.255.248.0 e 149.187.167.191
(C) 255.255.248.0 e 149.187.255.255
(D) 255.255.224.0 e 149.187.160.191
(E) 255.255.224.0 e 149.187.160.255

RESOLUÇÃO

Pela notação CIDR, sabemos que o número 21 após a barra no endereço de IP `149.187.160.0/21` indica o número de bits que compõe a máscara de sub-rede, ou seja, temos a seguinte máscara:

$$\underbrace{11111111.11111111.11111}_{\text{21 bits}}000.00000000 \longrightarrow 255.255.248.0$$

Agora que já conhecemos a máscara de sub-rede, precisamos analisar o IP dado para identificarmos qual é a parte deste IP que identifica a rede e qual identifica o *host*. Para isso, vamos converter o IP dado para a base binária:

$$149.187.160.0 \longrightarrow \underbrace{10010101.10111011.10100}_{\text{Sub-rede}}\underbrace{000.00000000}_{\text{hosts}}$$

Perceba que os decimais 149 e 187 do endereço IP não precisavam ser convertidos, pois já sabíamos que os 16 bits destes dois bytes já faziam parte da identificação da sub-rede.

Sabemos que o endereço de *broadcasting* é o maior endereço da sub-rede, ou seja, é quando todos os bits utilizados para endereçar os *hosts* são iguais a 1:

$$\underbrace{10010101.10111011.10100}_{\text{Sub-rede}}\underbrace{111.11111111}_{\text{broadcasting}} \longrightarrow 149.187.167.255$$

Resumindo, encontramos a máscara de sub-rede igual a:

$$255.255.248.0$$

e o endereço de *broadcasting* desta sub-rede igual a:

$$149.187.167.255$$

ALTERNATIVA (A)