Lista de exercícios

João dos Santos Neto

1 - Qual é a importância da segurança da informação e por que é essencial para as organizações?

R - Ela é importante para proteger os dados que estão sendo utilizados em algum tipo de finalidade e é bastante essencial para deixar a organização mais segura e confiável.

2 - O que é Auditoria de Sistemas de Informação e quais são seus principais objetivos?

R - Seria uma análise completa do sistema que deverá ser implantado e implementado, ela visa manter todo o sistema operativo e ativo mantendo a integridade dos dados que estão sendo utilizados.

3 - Explique a relação entre Auditoria e Segurança de Sistemas de Informação. Como essas disciplinas se complementam?

R - Essa relação consiste na análise da forma como a segurança da aplicação está sendo feita, observando se os dados utilizados estão sendo protegidos corretamente, unidas elas garantem que o projeto está no caminho certo.

4 - Como a auditoria de sistemas de informação pode ajudar a detectar vulnerabilidades de segurança?

R - Pois faz uma análise completa e sistemática de todo o projeto desde a entrada dos dados até a forma e como eles estão sendo utilizados até a finalidade.

5 - Quais são as etapas do processo de auditoria de sistemas de informações? Explique brevemente cada uma delas.

R - Planejamento, execução, relatórios e acompanhamento.

Planejamento: estende desde a definição do escopo, definição de objetivos, equipe, plano e regulamentos até as normas relevantes que devem estar presentes.

Execução: consiste na realização de testes com a finalidade de procurar algum tipo de vulnerabilidade ou buscar uma desconformidade.

Relatórios: resumi-se em detalhar os pontos fortes e fracos com o objetivos de fazer recomendações de melhorias.

Acompanhamento: essa etapa baseia-se na verificação de mudanças feitas através das recomendações, observando se estas resolveram o problema.

6 - Qual é a importância do acompanhamento e revisão das ações corretivas após uma auditoria?

R - Essa etapa é importante pois através dela é feita uma revisão de todo o projeto novamente procurando falhas e vulnerabilidades, podendo fazer uma comparação se uma mudança feita alterou algum outro ponto, seja ele fraco ou forte.

7 - O que é o "princípio do mínimo privilégio"? Como ele ajuda a melhorar a segurança de sistemas?

R - Entende-se no nível de acesso de determinado integrante no projeto, restringido-o de informação que este possa obter. O benefício dessa implantação melhora os riscos de ataques de engenharia social.

8 - Por que a conscientização dos funcionários é fundamental para a segurança da informação? Quais são algumas estratégias eficazes para treinar e conscientizar os funcionários sobre práticas seguras?

R - Essa conscientização é importante pois ela determina que os funcionários saibam que tal ação tem uma influência no projeto, podendo gerar riscos à funcionalidade. Identificação de emails falsos(phishing) e proteger informações sensíveis.

9 - Qual é o papel da auditoria de sistemas de informações na avaliação da eficácia dos controles de segurança? Por que é importante verificar a conformidade com políticas e regulamentos?

R - Pois ela revisa se a aplicação está seguindo normas e regras que protegem os dados dos usuários do sistema. Essa verificação é importante pois existem regulamentos que protegem os usuários em casos de vazamentos e utilização dos seus dados.

10 - Como a auditoria de sistemas de informação pode contribuir para a prevenção de futuros incidentes de segurança?

R - Ela previne realizando relatórios especificando falhas e vulnerabilidades que possam ser descobertas.

11 - O que é uma política de segurança e quais são seus principais objetivos?

R - Seria um conjunto de regras e regulamentações que protegem os sistemas e dados de uma organização. Seus objetivos são bem claros, proteger os dados, prevenir contra ameaças, manter a conformidade com as regulamentações e conscientização de funcionários.

12 - Descreva alguns elementos comuns em uma política de segurança. O que é uma política de privacidade e quais são seus objetivos?

R - Políticas de senhas(evitar senhas que originam-se do próprio usuário, criar senhas fortes com letras maiúsculas e minúsculas, caracteres especiais e evitar que tenha alguma relação com o usuário), Controle de acesso(Regras que mantém o acesso restringido a determinado usuário do sistema) e Monitoramento de Rede(verificação de atividades de tráfego, observar se o tráfego está com transferência de dados sensíveis que não deveriam estar ali, verificar se a atividade está sendo feita com a finalidade que ela foi feita).

Política de privacidade é uma definição de como estabelecer a coleta, armazenamento, e proteger os dados, tendo os objetivos de transparecer, obter o consentimento dos usuários, garantir a proteção destes e estar conforme as normas.

13 - Liste alguns elementos típicos encontrados em uma política de privacidade.

R - Informações coletadas

Finalidade da coleta

Compartilhamento da coleta

Segurança dos Dados

Diretos do Usuário

14 - Explique o conceito de privacidade na era digital e por que é essencial proteger informações pessoais online.

R - Esse conceito ajuda a manter os dados que estão sendo entregues na aplicação de forma segura, transparente e confiável. É essencial pois a partir desses dados é possível montar um perfil e utilizar para induzir o usuário a tal finalidade.

15 - Quais são os principais desafios para a privacidade online?

R - Atualmente, existem várias dificuldades para proteger a privacidade, por exemplo:

o compartilhamento indevido entre empresas, sites fakes que visam roubar dados, ransomwares que tentam sequestrar dados.

16 - O que é identificação de ameaças e por que é uma parte essencial da segurança da informação?

R - É identificar que um determinado acesso ao sistema tem intenções maliciosas que comprometem a funcionalidade do sistema. É uma parte bastante importante porque a partir dela pode- se defender o sistema e proteger os dados armazenados.

17 - Explique a importância de identificar e mitigar ameaças à segurança cibernética em um ambiente digital.

R - É importante para prevenir que essas ameaças controlem o sistema, deixando inutilizável ou até para atos terroristas.