UNIVERSIDADE FEDERAL DO PIAUÍ - UFPI
CAMPUS SENADOR HELVÍDIO NUNES DE BARROS - CSHNB
DISCIPLINA: AUDITORIA E SEGURANÇA DE SISTEMAS DE INFORMAÇÃO
PROFESSOR: JÚLIO VÍTOR MONTEIRO MARQUES

João dos Santos Neto

Atividade de Revisão

9 de novembro de 2023

1- Qual é o papel fundamental da segurança da informação em uma organização?

R - Esse papel destina-se a proteger os sistemas da organização de determinadas ameaças, como vírus, malware, entre outros tipos de ataques, prevenindo que os dados sejam roubados ou até vazados na rede.

2- Explique a relação entre auditoria de sistemas de informação e segurança, destacando como a auditoria contribui para a identificação de vulnerabilidades.

R - A auditoria visa identificar possíveis vulnerabilidades de sistemas ajudando a parte da segurança a proteger e corrigir essa vulnerabilidade.

3- Quais são os principais objetivos da auditoria de sistemas de informação?

R - A Auditoria tem como principais objetivos: conformidade, segurança e desempenho.

4- Descreva o processo de auditoria de sistemas de informação, incluindo suas etapas essenciais.

R - Inclui planejamento, coleta de evidências, avaliação de riscos e relatório de auditoria.

Planejamento: definição dos seus objetivos, identificação dos sistemas a serem auditados e estabelecer a equipe de auditoria.

Coleta de evidências: revisão de políticas, documentos e procedimentos.

Avaliação de riscos: identificação e avaliação dos riscos à segurança do sistema e priorizar a parte crítica.

Relatório de auditoria: entregar à equipe de segurança as vulnerabilidades encontradas e recomendar ações que possam corrigi-las.

5- Quais são algumas medidas de segurança comumente utilizadas em sistemas de informação?

R - Existem algumas medidas de segurança como a criptografia de dados,que fornece maior segurança a dados sensíveis, controles de acesso,restringe o acesso de usuários a determinadas partes do sistema, políticas de senha, geração de senhas mais fortes e complexas fortificando possíveis ataques de senha, firewall e treinamento em conscientização em segurança.

6- Como as normas e regulamentações contribuem para garantir a segurança da informação em uma organização?

R - Contribuem para segurança e proteção dos dados que estão sendo utilizados no sistemas.

7- Quais são os benefícios tanto da auditoria quanto da segurança da informação para uma empresa?

R - Esses benefícios são proteção de dados sensíveis, que ajudam a garantir ao usuário que seus dados não serão roubados, manutenção da confiança do cliente, conformidade com regulamentações, garante que a organização está fazendo o uso e manipulação correto dos dados, e redução de riscos.

8- Por que a segurança da informação é essencial para manter a vantagem competitiva, fluxo de caixa e rentabilidade de uma organização?

R - Pelo simples fato da organização seguir protocolos confiáveis, normas, regras e regulamentações que protegem e asseguram a manipulação ou fluxo dos dados na rede.

9- Quais são algumas ameaças de segurança que as organizações enfrentam atualmente?

R - Tais como ataques ddos, engenharia social, malware, phishing, ransomware, etc.

10- Explique a importância da confidencialidade na segurança da informação, fornecendo exemplos de medidas de confidencialidade.

R - É importante essa confidencialidade porque a segurança é uma parte bastante sensível do sistema, visto que nos tempos atuais dados valem ouro.
Um exemplo a seguir podemos citar a restrição do acesso de funcionários em partes do sistema onde essa parte possua dados sensíveis e não podem ser visualizados a qualquer um.

11- Como a integridade dos dados contribui para a segurança da informação e como ela pode ser mantida?

R - A integridade é um fator importante pois ela garante que os dados não sofram alteração constante em todo o ciclo de vida do sistema.

12- Quais são as características e medidas relacionadas à disponibilidade na segurança da informação?

R - Essas características são oportunidade, continuidade e robustez, onde:

Oportunidade - é a capacidade do sistema disponibilizar a informação a qualquer momento.
Continuidade - é a capacidade do sistema de continuar no ar mesmo após falhas.
Robustez - é a capacidade do sistema de suportar o trabalho da equipe.

Podemos citar algumas medidas como procedimentos de recuperação de dados, servidores de backup.

13- Descreva o conceito de avaliação de riscos e sua importância na gestão da segurança da informação.

R - É um processo que visa encontrar pontos seja ela de maior ou menor vulnerabilidade do sistema ou da organização em si.
Essa avaliação é importante pois ela encontra a vulnerabilidade e com isso é possível mitigar essas falhas.

14- Explique a abordagem de processo para a gestão da segurança da informação, destacando suas etapas.

R - Compreender os requisitos de segurança da organização, implementar e operar os controles de gerenciamento de riscos da segurança, monitorar e revisar o desempenho e eficácia do ISMS e a melhorar gradualmente com base nas medições objetivas.

15- Quais são os princípios fundamentais da segurança da informação e por que são essenciais em programas de segurança?

R - Confidencialidade, integridade e disponibilidade.
São essenciais pois fornecem um arcabouço para mitigar ameaças e proteger ativos digitais.

16 - O que representa o Triângulo CIA na segurança da informação e como ele se relaciona com os princípios de confidencialidade, integridade e disponibilidade?

R - É um modelo conceitual que representa os três pilares fundamentais da segurança da informação: Confidencialidade, Integridade e Disponibilidade.

Eles estão interligados: a quebra de um princípio pode afetar os outros. Por exemplo, a perda de confidencialidade pode comprometer a integridade dos dados. Garantir o equilíbrio entre esses princípios é essencial para proteger efetivamente os dados e sistemas, evitando falhas de segurança.

17- Descreva o hexagrama Parkeriano e seus seis elementos de segurança da informação.

R - O hexagrama Parkeriano destaca seis elementos essenciais da segurança da informação: confidencialidade, posse ou controle, integridade, autenticidade, disponibilidade e utilidade. Juntos, esses elementos formam uma abordagem abrangente para proteger os sistemas e dados, desde a prevenção até a resposta a incidentes, garantindo segurança contínua e resiliência.

18- Como as medidas de confidencialidade são aplicadas na proteção de informações estratégicas em uma organização?

R - Criptografia de dados para armazenamento e transmissão. Preenchimento de tráfego na rede. Estrito controle de acesso. Classificação de dados. Treinamento de pessoal.

19- Explique como a auditoria de conformidade contribui para garantir a conformidade com regulamentações externas, como leis de proteção de dados.

R - Ela contribui fazendo uma avaliação ou análise verificando se está tudo conforme as leis que protegem os dados.

20- Por que a ética profissional é crucial para os auditores de sistemas de informação durante o processo de auditoria?

R - Porque ela garante a imparcialidade, a confidencialidade e a credibilidade do processo, promovendo a confiança nos relatórios e mantendo a integridade da avaliação.

21- Qual é a importância de documentar procedimentos operacionais e atribuir responsabilidades nas operações de TI de uma organização?

R - Para padronizar práticas, transferir conhecimento, reduzir riscos, garantir conformidade, aumentar eficiência e facilitar melhorias contínuas.

22- Por que é crucial ter instruções de trabalho detalhadas, especialmente em relação ao desligamento e inicialização de computadores?

R - Para evitar erros, garantir a segurança dos dados, manter a funcionalidade dos sistemas, padronizar práticas e facilitar a recuperação em caso de falhas.

23- Explique como os procedimentos operacionais podem variar para computadores com diferentes sistemas operacionais, como Windows e Unix.

R - Podem variar devido às diferenças na interface, comandos, permissões, ferramentas e métodos de atualização e manutenção.
A estruturação e a forma de interagir com esses sistemas são diferentes, resultando em abordagens operacionais diferentes.

24- Qual é a finalidade principal de um procedimento operacional em relação à operação de equipamentos em uma organização?

R - É estabelecer diretrizes claras e detalhadas para garantir o uso seguro, eficiente e padronizado dos equipamentos, objetivando maximizar a eficiência, prevenir acidentes e prolongar a vida útil dos ativos da empresa.

25- Cite exemplos de informações abordadas em procedimentos operacionais, incluindo backups, manutenções e processamento de correspondências.

R -

Backups:
- Agendamento: Frequência e horários dos backups.
- Métodos de Backup: Descrição dos métodos utilizados (por exemplo, backup local, em nuvem, externo).

- Restauração: Passos detalhados para restaurar dados a partir dos backups em caso de falha.

2. Manutenções:
- Programação: Cronograma de manutenções e checklists detalhados para cada atividade.
- Procedimentos Preventivos: Instruções para limpeza, inspeção e troca de peças.
- Registro de Manutenção: Orientações sobre documentação das atividades e históricos de manutenção.

Processamento de Correspondências:
- Recebimento e Triagem: Procedimentos para registro, triagem e distribuição interna.
- Envio de Correspondências: Instruções para preparação, selagem e rotulagem de correspondências.
- Protocolos de Segurança: Medidas para lidar com correspondências sensíveis e suspeitas.

26- Por que os procedimentos operacionais são essenciais para evitar mal-entendidos na operação de equipamentos, independentemente de serem robôs, programas de controle ou programas de contabilidade?

R - Pois estabelecem práticas padronizadas, reduzem erros, garantem segurança, promovem eficiência, facilitam o treinamento de pessoal e asseguram a responsabilidade e transparência na operação.

27- Como as trilhas de auditoria e os arquivos de log contribuem para a segurança e resolução de problemas em sistemas e redes?

R - Detectando atividades maliciosas, rastreando alterações e garantindo conformidade. Na resolução de problemas, identificam falhas, analisam desempenho e oferecem um histórico detalhado das operações, auxiliando na resolução de questões em sistemas e redes.

28- Explique a importância de armazenar os arquivos de log em um local seguro e como eles podem ser cruciais em situações de incidentes.

R - Para preservar sua integridade, atender a requisitos legais, e, crucialmente, para investigar incidentes de segurança. Eles oferecem informações valiosas para entender a causa raiz dos incidentes, fornecendo evidências forenses e facilitando respostas eficazes a eventos indesejados.

29- Faça uma analogia entre os arquivos de log do sistema e a caixa preta de um avião em termos de registro de eventos críticos.

R - Tanto os arquivos de log do sistema quanto a caixa preta de um avião registram eventos críticos detalhados, são analisados após incidentes, fornecem evidências forenses e auxiliam na recuperação de dados.

30- Qual é a principal finalidade do gerenciamento de mudanças em relação à implementação de mudanças em uma organização?

R - O gerenciamento de mudanças visa garantir uma implementação eficiente e controlada de alterações em uma organização, reduzindo riscos, promovendo eficiência, assegurando conformidade e estimulando a aprendizagem contínua.

31- Explique a situação de "beco sem saída" mencionada no texto em relação à implementação ou não de uma mudança e os riscos envolvidos.

R - A implementação pode trazer disrupções e custos adicionais, enquanto a não implementação pode resultar em obsolescência ou perda de competitividade. O gerenciamento de mudanças é crucial para avaliar e mitigar riscos, auxiliando na tomada de decisões informadas.

32- Como o gerenciamento de mudanças aborda a necessidade de diferentes papéis, como o Encarregado de Segurança da Informação (ISO) e o gerente do sistema?

R - O ISO foca na avaliação dos impactos de segurança das mudanças propostas, enquanto o gerente do sistema avalia o impacto operacional.

33- Por que a implementação de mudanças pode envolver riscos e como esses riscos podem ser avaliados antes da implementação?

R - A implementação de mudanças pode acarretar riscos como interrupções, falhas de sistema, perda de dados e resistência à mudança. Antes da implementação, os riscos são avaliados através de análise de impacto, avaliação de riscos, testes, revisões e análise de custos-benefícios para minimizar falhas e interrupções significativas.

34- Qual é a importância de definir diferentes papéis no caso de mudanças, e como isso contribui para uma abordagem mais controlada?

R - uma abordagem mais controlada é estabelecida, permitindo uma distribuição eficaz de responsabilidades, melhor coordenação, avaliação de riscos mais abrangente e comunicação clara.

35- Explique a necessidade de considerar cuidadosamente e antecipadamente as mudanças em serviços de TI e sistemas de informação.

R - As organizações podem mitigar riscos, manter a continuidade operacional, garantir a segurança dos dados, melhorar a experiência do usuário, otimizar o uso de recursos e permanecer ágeis diante de um ambiente em constante evolução.

36- Como o Gerenciamento de Serviços de TI e a estrutura do ITIL estão relacionados ao gerenciamento de mudanças?

R - o ITIL fornece uma estrutura robusta e diretrizes claras para o Gerenciamento de Mudanças, auxiliando as organizações na implementação de mudanças de forma controlada, minimizando riscos e mantendo a eficácia dos serviços de TI.

37- Quais são os potenciais riscos de não instalar uma atualização de segurança, e quem é responsável por determinar esses riscos?

R - Vulnerabilidades de Segurança; Instabilidade do Sistema; Conformidade e Regulamentação; e Interrupção de Serviços.

Geralmente os responsáveis são Equipe de Segurança da Informação; Gerentes de TI e Sistemas; Equipe de Conformidade.

38- Destaque a importância de avaliar os riscos associados a mudanças, especialmente no contexto da estabilidade dos sistemas.

R - Prevenir interrupções operacionais, garantir desempenho confiável, proteger a segurança dos dados, controlar custos e preservar a reputação da organização.

39- Explique por que mudanças em serviços de TI devem ser conduzidas de forma cuidadosa e controlada.

R - Evitar interrupções operacionais, proteger a segurança dos dados, manter a estabilidade dos sistemas e cumprir requisitos regulatórios.

40- Como o gerenciamento de mudanças contribui para a prevenção de interrupções na infraestrutura de uma organização?

R - Previne interrupções na infraestrutura por meio da antecipação de riscos, planejamento estruturado, controle de processos, comunicação eficaz e avaliação pós-implementação.