PADRÃO DE RESPOSTA – DISCURSIVA

CONCURSO PÚBLICO – CÂMARA MUNICIPAL DE BELO HORIZONTE/MG

CARGO: ANALISTA DE TECNOLOGIA DA INFORMAÇÃO – ÁREA DE INFRAESTRUTURA DE SISTEMA

Questão 01

A resposta esperada pelo candidato, obrigatoriamente, terá que evidenciar os seguintes tópicos:

1. Riscos potenciais e vulnerabilidades nos sistemas de TI da Prefeitura, tanto para a segurança física quanto lógica.

Riscos Potenciais de Segurança Física:

a) Falha no fornecimento de energia elétrica devido a eventos climáticos extremos.
b) Incêndio nas instalações onde os servidores e sistemas de TI estão localizados, causando danos aos equipamentos e interrupção dos serviços.
c) Danos físicos aos servidores devido a incêndios ou desastres naturais.
d) Avaria de equipamentos devido a condições ambientais inadequadas, como superaquecimento de servidores devido à falta de refrigeração adequada.
e) Roubo ou vandalismo das instalações físicas onde os sistemas de TI estão localizados, resultando na perda de equipamentos ou dados.

Riscos Potenciais de Segurança Lógica:

1. Ataques de *ransomware* visando criptografar dados críticos.
2. Vazamento de informações confidenciais devido a vulnerabilidades de segurança nos sistemas.
3. Um funcionário descontente ou desonesto pode acessar informações confidenciais ou realizar ações maliciosas nos sistemas da empresa.
4. Ataques de negação de serviço (DDoS) direcionados aos servidores da prefeitura, sobrecarregando-os e impedindo o acesso aos serviços *on-line*.
5. Vulnerabilidades de *software* não corrigidas que podem ser exploradas por invasores para obter acesso não autorizado aos sistemas ou realizar atividades maliciosas.
6. Ataque de engenharia social direcionado aos funcionários da prefeitura, levando à divulgação não autorizada de informações confidenciais ou acesso indevido aos sistemas de TI.

2. Medidas preventivas para minimizar a ocorrência de falhas nos sistemas de TI.

1. Implementação de sistemas de alimentação ininterrupta (UPS) para garantir energia contínua aos servidores, mesmo durante interrupções elétricas.
2. Adoção de soluções de detecção e prevenção de incêndios em salas de servidores para mitigar riscos de danos físicos.
3. Instalação de *firewalls* de última geração e *software* antivírus atualizado para proteger os sistemas contra-ataques cibernéticos.
4. Atualização regular de sistemas e aplicativos com *patches* de segurança para corrigir vulnerabilidades conhecidas.
5. Realização de *backups* regulares dos dados críticos e armazenamento seguro em locais externos para mitigar os impactos de um ataque de *ransomware* ou outro tipo de ataque cibernético.

3. Procedimentos de resposta a incidentes para lidar com falhas quando ocorrerem.

1. Designação de uma equipe de resposta a incidentes de TI para investigar e resolver rapidamente problemas de segurança, como ataques de *malware* ou violações de dados.
2. Implementação de um processo formal de notificação de incidentes para relatar rapidamente quaisquer problemas de segurança à equipe de TI.
3. Realização de investigações forenses para identificar a origem e o impacto de incidentes de segurança, como ataques de *malware*.
4. Isolamento imediato de sistemas comprometidos para evitar a propagação de ataques ou danos adicionais.
5. Notificação de autoridades competentes e tomada de medidas legais contra invasores ou infratores de segurança.

3. Estratégias de recuperação podem ser utilizadas para restaurar os sistemas de TI o mais rápido possível após uma interrupção.

1. Utilização de *backups* para restaurar os sistemas e dados afetados após um incidente, minimizando o tempo de inatividade e permitindo a retomada rápida das operações.
2. Implementação de sistemas de espelhamento ou redundância para garantir a disponibilidade contínua dos serviços mesmo durante uma interrupção.
3. Utilização de ambientes de recuperação de desastres para manter os serviços críticos em funcionamento enquanto os sistemas principais estão sendo restaurados.
4. Implementação de planos de continuidade de negócios para garantir a disponibilidade de processos essenciais durante uma interrupção prolongada.

4. Estratégias para garantir a eficácia do plano de contingência.

1. Realização de testes regulares do plano de contingência, incluindo simulações de incidentes e exercícios de resposta a emergências.
2. Revisão periódica do plano de contingência para incorporar novas ameaças, tecnologias e lições aprendidas com incidentes anteriores.
3. Treinamento contínuo da equipe de TI e conscientização dos funcionários sobre os procedimentos de contingência e melhores práticas de segurança.
4. Envolvimento de partes interessadas internas e externas na revisão e validação do plano de contingência para garantir sua eficácia e relevância contínuas.

Fontes:

- **Plano De Contingência De TI: O Que É E Como Elaborar.** Disponível em: https://prolinx.com.br/plano-de-contingencia-ti/
- **Plano de Contingência e Continuidade dos Serviços de Tecnologia da Informação.** Disponível em: https://itp.ifsp.edu.br/files/CTI/Plano_de_Contingencia_IFSP_Campus_Itapetininga.pdf
- **Plano de Contingência de Segurança O que é, 7 Passos Elaborar.** Disponível em: https://gestaodesegurancaprivada.com.br/plano-de-contingencia-de-seguranca-o-que-e-7-passos-elaborar/

Questão 02

A **certificação digital** serve para autenticar a identidade de entidades online, como pessoas, empresas ou dispositivos. Ela fornece um meio seguro de identificação e comunicação na *Internet*, garantindo integridade, autenticidade e confidencialidade das informações trocadas. A certificação digital é baseada em tecnologias de criptografia assimétrica, em que um par de chaves criptográficas é utilizado para garantir a autenticidade, integridade e confidencialidade das informações. No contexto empresarial, a certificação digital é frequentemente utilizada para autenticar a identidade de empresas, organizações e indivíduos em transações eletrônicas. Para obter um certificado digital, uma entidade (indivíduo ou organização) precisa se submeter a um processo de validação realizado por uma Autoridade Certificadora (AC) confiável. Durante esse processo, a AC verifica a identidade da entidade e emite um certificado digital que contém informações como nome, chave pública, data de validade e o nome da AC que o emitiu.

Uma **assinatura digital** é um mecanismo criptográfico que garante a autenticidade e integridade de um documento ou mensagem eletrônica. Funciona através da utilização de chaves criptográficas, onde o remetente utiliza sua chave privada para gerar uma assinatura única para o documento ou mensagem. O destinatário pode então verificar a assinatura utilizando a chave pública correspondente, garantindo que o conteúdo não foi alterado e que o remetente é quem diz ser.

A assinatura digital é uma aplicação específica da certificação digital, onde a chave privada de uma entidade é utilizada para criar uma assinatura única em documentos eletrônicos ou mensagens. Essa assinatura digital é anexada ao documento e pode ser verificada utilizando a chave pública correspondente, garantindo assim a autenticidade e integridade do documento.

O processo de assinatura digital funciona da seguinte forma: o remetente utiliza sua chave privada para gerar uma assinatura digital única para o documento. O destinatário pode então utilizar a chave pública correspondente para verificar a assinatura e confirmar que o documento não foi adulterado e que o remetente é quem diz ser. A assinatura digital é amplamente utilizada em transações eletrônicas, contratos digitais, comunicações seguras e em qualquer situação onde a autenticidade e integridade dos documentos são críticas. Ela proporciona uma maneira eficiente e segura de garantir a confiança nas transações online e na troca de informações sensíveis.

As chaves simétricas e assimétricas são utilizadas em criptografia para proteger a confidencialidade dos dados. As principais características são:

Chaves simétricas: utilizam uma única chave para criptografar e descriptografar os dados. São mais rápidas e eficientes em termos de processamento, mas exigem um método seguro de compartilhamento da chave entre as partes envolvidas.

Chaves assimétricas: utilizam um par de chaves: uma pública e outra privada. A chave pública é utilizada para criptografar os dados, enquanto a chave privada é utilizada para descriptografá-los. São mais seguras em termos de compartilhamento de chaves, pois a chave privada nunca é compartilhada ou divulgada.

Na comunicação segura entre os funcionários da Empresa X, as chaves simétricas e assimétricas são utilizadas de diferentes maneiras. As chaves simétricas podem ser usadas para criptografar o conteúdo das mensagens, garantindo sua confidencialidade.

Por exemplo, quando um funcionário envia uma mensagem, ele pode criptografá-la com uma chave simétrica compartilhada entre remetente e destinatário. Em contrapartida, as chaves assimétricas são frequentemente utilizadas para estabelecer uma comunicação segura inicial, permitindo a troca segura de chaves simétricas. Por exemplo, ao iniciar uma conversa, os funcionários podem trocar chaves públicas para criptografar a chave simétrica usada na comunicação posterior.

Fontes:

- COMER, Douglas E. **Redes de computadores e internet.: Grupo A, 2016.** E-book. ISBN 9788582603734. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788582603734/. Acesso em: 13 fev. 2024.
- FONTES, Edison Luiz G. **Segurança da informação** – 1ª edição.: Editora Saraiva, 2012. E-book. ISBN 9788502122185. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502122185/. Acesso em: 13 fev. 2024.
- MORAES, Alexandre Fernandes de. **Segurança em Redes – Fundamentos.** Editora Saraiva, 2010. E-book. ISBN 9788536522081. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788536522081/. Acesso em: 13 fev. 2024.
- TERADA, R. **Segurança de dados: criptografia em redes de computador.** ed. São Paulo: Editora Edgard Blucher, 2008. p. 44.