Revisão SG

RESUMO

Princípios

**Confidencialidade**

•Confiabilidade de dados: capacidade de garantir que o nível de

sigilo seja aplicado em cada junção de dados em processamento.

•Prevenção contra a divulgação não autorizada dos dados.

•Fornecida por meio de técnicas de criptografia de dados e da

forma como eles são armazenados e transmitidos.

**Integridade**

•Integridade e a garantia de rigor e confiabilidade das informações

e sistemas e de que não ocorrerão modificações não autorizadas

nos dados, ou seja, a possibilidade de verificar a consistência da

informação contida nos dados.

**Disponibilidade**

•Disponibilidade está relacionada com a capacidade que os sistemas e

redes devem ter para executar e disponibilizar os dados de forma

previsível e adequada às necessidades da empresa.

•Os dados devem ser recuperados de forma rápida e segura caso haja

alguma queda de disponibilidade dos serviços em uma empresa.

•Os backups devem estar disponíveis para uma rápida recuperação de

sistemas e dados críticos na empresa

Informações:  
publica

Privada

restrita

Técnicas de proteção

•Criptografia

•Firewall e antivírus

•Autenticação e autorização

•Controle de acesso

Ameaças comuns

• Alguns tipos de ameaças comuns:

•Malware

•Ataques de força bruta

•Vulnerabilidade de software

•Ataques de negociação de serviços

•Fraudes.

**Ameaça**: Qualquer evento ou circunstância que possa potencialmente comprometer a

segurança da informação. Isso pode incluir ameaças internas (como funcionários malintencionados) e ameaças externas (como hackers, malware ou desastres naturais).

2.**Vulnerabilidade**: Uma fraqueza ou falha em um sistema que pode ser explorada por uma

ameaça para causar danos. Isso pode envolver falhas de segurança em software, configurações

incorretas de sistemas, falta de atualizações, entre outros.

3.**Impacto**: As consequências resultantes da exploração de uma vulnerabilidade por uma

ameaça. Isso pode incluir perda de dados, danos à reputação, interrupção de serviços, perdas

financeiras e até mesmo impactos legais ou regulatórios.

Gerenciamento de riscos

•Identificação de Riscos

•Análise de Riscos

•Avaliação dos Riscos

•Planejamento de Respostas aos riscos

•Implementação das ações

•Monitoramento e controle

•Comunicação

4 Tratamentos de riscos:

Mitigação: Ações preventivas para diminuiro ou evitar

Aceitacao: Aceitar que se o risco ocorrer para que caso ele ocorra não de tanto impacto

Transferencia: Transferir o impacto para seguradora ou seja outra pessoa toma conta

Evitacao: Estratégias para evitar por completo situações de risco:

-Criptografia

-Confidencialidade

- Integridade

- Disponibilidade

- Autenticidade

Algoritimo para criptografia:

AES: Criptografia simétrica e DES que caiu em desuso

RSA: Criptografia assimétrica chave pub e privada

Assinatura digital:

-Possui certificado digital usado para grantir que o ducomento não seja alterado

- Garante Autenticidade

Certificados digitais

Autoridade certificadora:

Se submente a ICP-BRASIL

- É responsável por emitir,distribuir,renovar,revogar e gerenciar certificados digitais

-AC-RAIZ: Primeira na cadeia, compete a ela: emitir, expedir,distribuir, revogar e gerenciar certificados das ACs mais baixos.

-**OBS: Assinatura digital não é a mesma coisa que assinatura ELETRONICA, sendo que assinatura eletrônica não possui certificado DIGITAL**

QUESTÕES

1. quais são 4 estratégias de tratamento de risco na segurança da informação

As quatro estrátegias são Mitigação, Aceitação, Tranferência de responsabilidade e Evitação

1. as politicas e procedimentos em segurança da informação são fundamentais para garantir a proteção dos dados, sistemas e recursos de uma organização contra ameaças cibernéticas e riscos de segurança. De acordo com o material disponibilizado para estudo, quais são os elementos chave que podem ser abordados nas politicas e procedimentos de segurança da informação

Os elementos-chave podem ser considerados como tudo aquilo que se faz para evitar, mitigar danos e impactos na empresa algo de ameaças. Podemos citar então medidas como gerecimanete de riscos, aceitação de riscos, Criptografia de dados, Assinaturas digitais que ocorram com certificados digitais devidamente cadastrados nas ACs. Temos também análises de ameaças e vulnerabilidades, entendimento dos possíveis impactos na empresa. Todos esses são elementos que permeiam as políticas de segurança da informação

1. em relação ao conteúdo sobre análise de riscos, qual é a disserte sobre as diferenças entre analise qualitativa de risco e analise quantitativa de risco

A análise de riscos qualitativa é feita de forma subjetiva utilizando-se de experiências passadas onde chega-se a resultado mensurando do risco, podendo ser ele baixo,médio ou alto. Já a análise de riscos quantitativa baseia-se em dados precisos e utiliza de métodos matemáticos para fazer uma análise precisa dos riscos.

1. o que é criptografia? Quais são os dois tipos de criptografia usados para compartilhamento de dados de forma segura? Disserte sobre os dois

Critografia é uma forma de evitar vulnerabilidades nos dados, fazendo com que esses se transformem em dados criptografados que só serão acessados por pessoas que possuírem a chave especiífica para descriptografar.

Existem dois dtipos de criptografia, assimétrica e simétrica. A simétrica trata-se da utilização de uma chave privada responsável por criptografar e descriptografar. Já a criptografia assimétrica temos 2 chaves, uma pública e outra privada. A chave pública é responsável por criptografar os dados e ela possui uma correspondete única que é sua chave privada. Os dados só poderam ser descriptografados pela chave privada correspodente