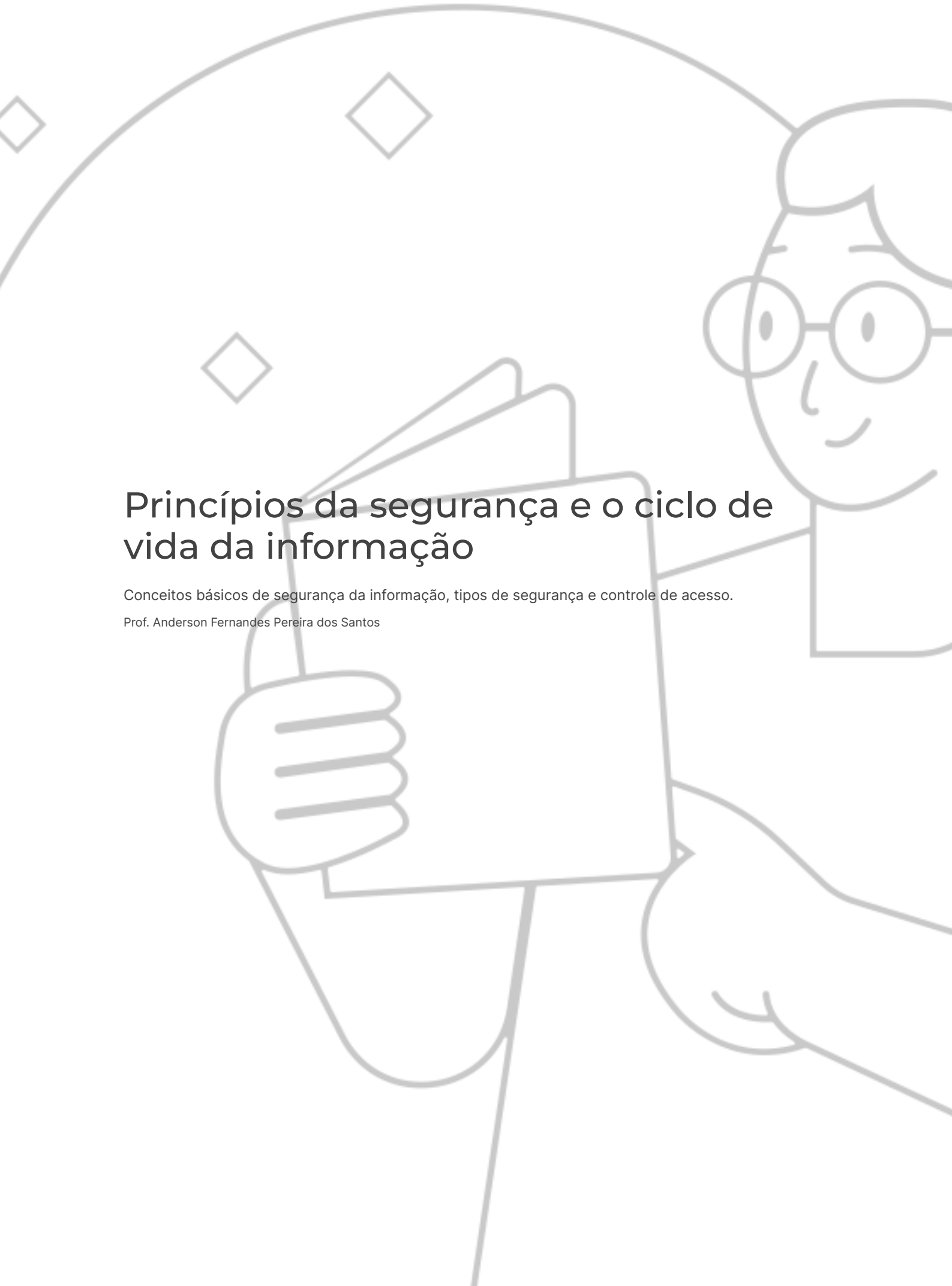


Princípios da segurança e o ciclo de vida da informação

Conceitos básicos de segurança da informação, tipos de segurança e controle de acesso.

Prof. Anderson Fernandes Pereira dos Santos

Propósito

Apresentar os conceitos de segurança da informação e os tipos de segurança, assim como a aplicação deles.

Objetivos

- Empregar os conceitos básicos da área de segurança e informação, seu valor, ciclo de vida e sua propriedade.
- Formular segurança física, lógica e controle de acesso.

Introdução

A segurança da informação é um tema de extrema importância para a sustentabilidade e longevidade de uma organização, especialmente no contexto do mundo atual, que foca na digitalização das informações e na transformação digital.

Apesar das organizações já terem uma consciência bem consolidada de importância de cuidar da segurança interna e externa por elas gerenciadas, há por vezes dúvidas com relação à abrangência do termo segurança da informação, dos seus conceitos básicos, do seu real valor para a organização, bem como do seu ciclo de vida.

O conhecimento dos conceitos básicos sobre segurança da informação é a base para que seja possível formular a segurança da informação de forma adequada, contemplando não apenas as questões lógicas, realizadas pelos softwares, mas também os aspectos físicos ligados à segurança da informação, bem como o controle de acesso.

Ao longo deste conteúdo vamos detalhar os conceitos básicos de segurança da informação, os diferentes tipos de segurança e da importância do controle de acesso. Serão apresentados, também, aplicação prática para que possamos visualizar o que de fato uma organização precisa fazer para garantir a segurança das informações por ela produzida, gerida ou tratada.

Introdução

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Vamos começar!

Conceitos básicos da área de segurança e informação

Veja o valor, ciclo e a propriedade de vida da área de segurança e informação.

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Dado e informação

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

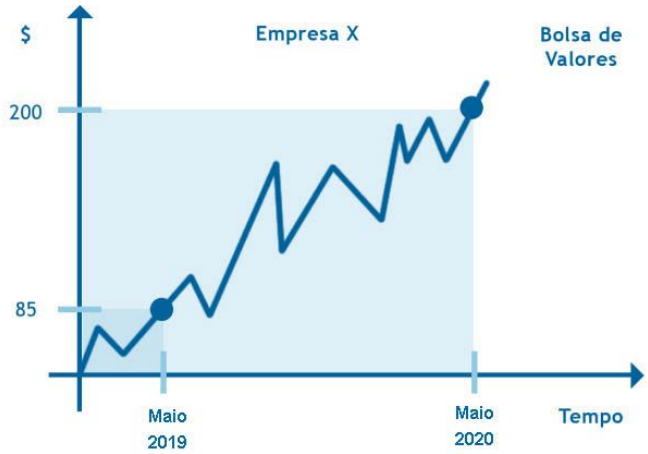
As primeiras figuras rupestres datam de mais de 70 mil anos antes de Cristo.

Dos manuscritos do Mar Morto até o último livro disponibilizado pela Amazon, a humanidade sempre precisou armazenar seus conhecimentos de alguma forma. Isso nos remete ao conceito de conhecimento - ou, mais especificamente, de **informação**.

O conceito fundamental que dá origem à informação, é conhecido como **dado**. Mas como defini-lo?

O dado pode ser considerado o valor de determinada medida sem uma contextualização e, portanto, sem valor para ser aplicado ou tratado. No momento em que um dado é contextualizado, ou seja, é atribuído a um contexto ou a uma situação, torna-se uma informação, consequentemente, obtendo valor.

Observe o gráfico de uma empresa na Bolsa de Valores: Na abscissa, ele apresenta o eixo temporal; na ordenada, o valor da ação na Bolsa.



Suponhamos que ela tenha registrado um crescimento durante a pandemia de covid-19. O valor das ações desta empresa praticamente dobrou na Bolsa de Valores. Vamos analisar:

Situação 1

Imagine que você conheça somente os pares de dados, ($85, Maio 2019) e ($200, Maio 2020), fora de contexto.

Situação 2

Imagine que os dois valores sejam registrados nos meses de maio de 2019 e 2020, e que você seja informado sobre isso em meados de dezembro de 2019.

Normalmente, uma situação do tipo não ocorre. Afinal, é muito difícil existir uma valorização tão grande em um curto espaço de tempo. Veja o que ocorre em cada situação:

- Na **situação 1**, os valores US$85 e US$200 são dados – e não contextualizados. Portanto, não é possível auferir ganhos financeiros ou elaborar uma percepção monetária a respeito deles. Mesmo que o maior expert em investimentos da Bolsa de Valores tivesse ciência de ambos, ele nada poderia fazer para lucrar com tais dados.
- Na **situação 2**, esses valores são dados contextualizados; por isso, conhecê-los configuraria uma informação passível de se auferir ganhos monetários.

Com o exemplo apresentado, como podemos definir uma **informação**?

Resposta

Ela pode ser definida como um dado contextualizado no qual existe uma percepção de valor. É necessário haver uma atenção quanto à sua preservação.

Ciclo de vida da informação

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Por se tratar de um dado contextualizado, a informação possui o seguinte ciclo de vida:

Criação

Transporte

Manuseio

Descarte

Após a **primeira etapa (criação)**, o dado pode ser transportado ou manuseado. A ordem do ciclo representa o transporte antes do manuseio por tal procedimento ser o mais comum nesses casos, porém é perfeitamente possível que ele seja manuseado anteriormente. Na etapa final, a informação é **descartada**.

Durante todas essas etapas, a informação deve ser protegida. Seu vazamento em quaisquer etapas pode provocar problemas em vários aspectos. Vamos analisar as seguintes hipóteses:

Que conclusão podemos tirar dos casos apresentados? A informação, que é o dado contextualizado, precisa de **prot**
vida. A partir dos exemplos citados, conseguimos entender a necessidade de **sempre** estabelecer uma proteção ade
do seu ciclo de vida.

No caso do transporte de mídias magnéticas contendo informações sigilosas de usuários de determinada empresa, p
é o emprego da criptografia, que pode ser definida como o embaralhamento das informações por meio de uma sequ
chave e um algoritmo. Esta chave é usada para embaralhar (criptografar) e desembaralhar (decriptografar) as inform

Quando a mesma chave é usada nas duas etapas, a criptografia é dita **simétrica**; quando são usadas chaves distintas
exemplos nas imagens a seguir:

Criptografia simétrica

Criptografia assimétrica

Como você manuseia seu pen drive? Hoje em dia, por estarmos na era da informação, é comum sempre levarmos um
mochila ou na carteira. Afinal, como você cuida das suas informações?

Certamente, seu pen drive contém alguns arquivos nos quais você ainda deve estar trabalhando. Ele pode servir para
tipos de trabalho, como:

- Se você é um **programador**, pode estar mexendo em alguma parte de um sistema que está desenvolvendo.
- Se você trabalha na **direção**, pode estar atualizando alguma planilha com os dados financeiros da sua empres

Uma prática simples - mas eficiente - nestes casos é simplesmente compactar os seus arquivos usando uma senha,

Mais inseguro

Arquivos no pen drive sem senha.

Menos inseguro

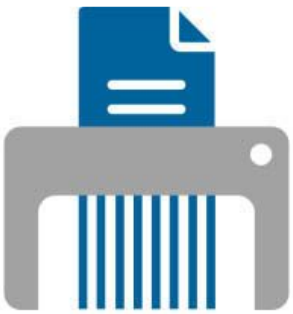
Arquivo compactado contendo
com senha.

Praticamente todas as ferramentas (até mesmo as gratuitas) possuem essa funcionalidade. Cada uma conta com um
senha ao processo de compactação. Um bom exemplo disso é a ferramenta 7-zip.

Essas ferramentas utilizam os melhores algoritmos de criptografia existentes no mercado. Além de economizar o esp
prática cria ainda uma camada de proteção para as informações contidas no dispositivo.

Devemos observar que a **proteção** e a **facilidade** caminham em direções contrárias. Por isso, o processo de compactar com senha gera um aumento de tempo no manuseio da informação, pois ele sempre torna necessária a tarefa de descompactar e compactar para tratar a informação.

Dessa forma, seu descarte deve ser realizado de forma padronizada, já que o propósito é evitar a recuperação de suas informações. Exemplo: pen drives, discos rígidos e outras mídias usadas precisam ser descartadas com o uso de trituradores adequados. Veja dois tipos de trituradores:



Triturador de papel

Triturador de disco rígido

A proteção e a facilidade
opostos.

Aspectos da segurança da informação

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

O três principais aspectos da informação requerem cuidados especiais:

Confidencialidade

Capacidade do acesso à informação apenas para quem possui autorização.

Integridade

Possibilidade de alteração da informa
autorizados.

Disponibilidade

Faculdade de a informação poder ser acessada, em qualquer tempo, por pessoas ou sistemas autorizados para tal.

Citados por diversos autores como pilares, estes três aspectos correspondem à prioridade do que deve ser protegid
Todos os exemplos citados correspondem à confidencialidade da informação em três momentos diferentes do seu ci

Portanto, a **segurança da informação** pode ser definida como as atividades, os procedimentos e as metodologias qu
informação, principalmente no que tange à confidencialidade, integridade e disponibilidade (CID).

Os aspectos seguintes, contudo, também são considerados importantes:

Autenticidade
Assegura que a informação foi gerada por pessoa ou sistema autorizado para isso.

Legalidade
Alinha informação e/ou dos processos com normas, portarias, leis e quaisquer outros documentos normativos, c
esfera de atribuição e abrangência.

Não repúdio
Relaciona-se ao fato de o emissor negar a autoria de uma informação divulgada. Também é conhecido como **irre**

Juntos, todos eles compõem os principais aspectos empregados pelos controles - ou pelas ferramentas que proporc
informação - para proteger a informação. Além dos 3 principais aspectos já citados, temos ainda:

1
Irretratabilidade
Capacidade do emissor de negar a autoria de uma informação divulgada.

2
Autenticidade
Capacidade de assegurar que a informação foi gerada por pessoa ou sistema autorizado para isso.

3
Legalidade
Capacidade de alinhar a informação ou os processos com normas, portarias, leis e quaisquer outros documen

Mão na Massa

Questão 1

(2019 - Instituto UniFil - Prefeitura de Cambé/PR - psicólogo) A segurança da informação está relacionada à proteçã
sentido de preservar os valores que possuem para um indivíduo ou uma organização. O conceito se aplica a todos os
informações e dados. O conceito de segurança informática ou segurança de computadores está intimamente relacio
apenas a segurança dos dados/informação, mas também a dos sistemas em si. Assinale a alternativa que não repres
segurança da informação.

A

Confidencialidade

B

Integridade

C

Permutabilidade

D

Disponibilidade

E

Irretratabilidade

A alternativa C está correta.

Os principais pilares da segurança da informação são a confidencialidade, integridade e disponibilidade. Há os com
autenticidade, a legalidade e o não repúdio.

Questão 2

(2019 - IDECAN - IF-AM - bibliotecário documentalista) A segurança da informação está baseada em três pilares: co
disponibilidade. Com base nessa informação, analise as afirmativas a seguir.

I. Garantir o acesso por pessoa ou dispositivo devidamente autorizado a todo hardware, software e dados sempre qu

II. As informações devem ser armazenadas da forma como foram criadas, de modo que não sejamcorrompidas ou da

III. As informações não poderão ser vistas ou utilizadas sem as devidas autorizações de acesso por pessoas ou dispo

Assinale a alternativa que apresente a ordem correta de associação com os três pilares da segurança da informação.

A

I - Disponibilidade; II - Integridade; III - Confidencialidade.

B

I - Confidencialidade; II - Integridade; III - Disponibilidade.

C

I - Integridade; II - Confidencialidade; III - Disponibilidade.

D

I - Confidencialidade; II - Disponibilidade; III - Integridade.

E

I - Disponibilidade; II - Confidencialidade; III - Integridade.

A alternativa A está correta.

A disponibilidade determina que seja garantido o acesso. O fato de as informações serem armazenadas da forma c
se automaticamente com a integridade. A informação que poder ser vista apenas por pessoas autorizadas é a conf

Questão 3

(2020 - IDIB - Prefeitura de Colinas do Tocantins/TO - engenheiro civil) Em se tratando de segurança da informação,
tecnologia da informação elenca três prioridades básicas. Essas três prioridades também são chamadas de pilares d
Assinale a alternativa que indica corretamente o nome da prioridade básica relacionada ao uso de recursos que visar
informações.

A

Inviolabilidade

B

Confidencialidade

C

Acessibilidade

D

Invulnerabilidade

E

Indisponibilidade

A alternativa B está correta.

Os principais pilares da segurança da informação são a confidencialidade, integridade e disponibilidade. Há os com
autenticidade, a legalidade e o não repúdio.

Questão 4

A internet foi criada no final da década de 1990 nos laboratórios do CERN pelo físico britânico Tim Berns-Lee. Desde
criações vieram moldando as gerações subsequentes. Atualmente, destacam-se as imagens na internet conhecidas
têm um caráter educativo, ensinando, de forma lúdica, algumas práticas que não devem ser seguidas. Uma delas é o

Na verdade, a ideia é ensinar ao usuário a manusear sua senha de forma correta, não a deixando, por exemplo, emba
tapete que fala, o objetivo é ensinar ao usuário como manejá-la corretamente. Marque o item que integra esse ensina

A

Confidencialidade

B

Disponibilidade

C

Integridade

D

Irretratabilidade

E

Criptografia

A alternativa A está correta.

A confidencialidade está relacionada à manutenção de uma informação passível de ser observada, lida ou acessad
direito. Em outras palavras, é semelhante a deixar uma conta de e-mail aberta para que qualquer pessoa possa lê-l
(chave embaixo do tapete, senha embaixo do teclado).

Questão 5

Alguns anos após sua aposentadoria, Bill resolve estudar para obter uma certificação de segurança. Ele e seu vizinho
gostaria de tirar a tão sonhada certificação, resolvem criar mnemônicos para decorar os assuntos.

Para decorar os pilares da segurança da informação, eles criam o seguinte mnemônico: “Cresci vendo televisão. Sem
ao narrar as reportagens”. Bill e Steve criaram vários mnemônicos. No dia seguinte, houve a prova de certificação. Su
sobre os pilares. A ideia do mnemônico deu certo, mas eles esqueceram o que representava cada letra.

Você resolve explicar para eles o significado de cada uma. Marque a alternativa que apresenta os termos corretos.

A

Confidencialidade, integridade e disponibilidade.

B

Confiabilidade, integridade e disponibilidade.

C

Confiabilidade, integridade e disponibilidade.

D

Confiabilidade, integridade e dedutibilidade.

E

Confidencialidade, disponibilidade e integridade.

A alternativa A está correta.

C é de confidencialidade: a capacidade do acesso à informação apenas por aqueles que possuem autorização; I, de
de alteração da informação por pessoas ou sistemas autorizados; e D, de disponibilidade: a faculdade de uma infor
em qualquer tempo, por pessoas ou sistemas autorizados para tal.

Teoria na prática

Chave de resposta

A resposta padrão a este questionamento cada vez mais comum é o uso de criptografia na base de dados sem que
ou privada) esteja em hard code , tampouco armazenada no BD ou no arquivo de computador.

Verificando o aprendizado

Questão 1

Ao realizarmos o download de uma ISO de um software, normalmente usamos as funções de hash. Marque a alternat
segurança da informação que corresponde ao uso dessas funções.

A

Confidencialidade

B

Integridade

C

Disponibilidade

D

Legalidade

E

Integralidade

A alternativa B está correta.

As funções de *hash* criam um conjunto de valores alfanuméricos que representa a informação. Alterando-se um bit todo o conjunto de valores é alterado. Dessa forma, assegura-se de que não haverá alteração da informação.

Questão 2

Constitui um dever de todo cidadão elaborar anualmente o imposto de renda. Com o advento da internet, a nossa de enviada diretamente para os servidores do governo. No início dessa metodologia, era comum haver notícias nos tele aguentaram e se desligarem sozinhos. Marque a alternativa que apresenta o pilar da segurança da informação que d situação.

A

Confidencialidade

B

Integridade

C

Disponibilidade

D

Conformidade

E

Confiabilidade

A alternativa C está correta.

Quando os servidores foram desligados, pararam de funcionar; com isso, tornaram-se indisponíveis.

Vamos começar!

Conceito de segurança física, lógica e controle de acesso

Veja o conceito de segurança física e lógica, além de controle de acesso.

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Segurança física

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

No módulo anterior, vimos o exemplo de roubo de dados no transporte. Mesmo que eles estivessem criptografados, mesma forma, pois ela foi uma consequência de vulnerabilidades na segurança física das mídias em questão. Assim, transgredidos:

Integridade

Depende da informação ser ou não totalmente impactada, pois a mídia poderia ser destruída.

Confidencialidade

Depende da informação armaze controle de proteção, como a cri

A família de normas ABNT ISO/IEC 27.000 divide a segurança física em dois aspectos: um é relacionado aos **equipam**

A segurança da informação age dessa forma. Ela é entendida como **camadas justapostas** que permitem à informação ficar cada vez mais protegida. É como se nossa informação recebesse camadas de proteção similar a uma cebola.

Quanto ao ambiente, em uma instalação empresarial, por exemplo, é possível observar as camadas de segurança físicas e, a partir daí, estabelecer um paralelo com a imagem da cebola.

Imaginemos a seguinte situação: Ao nos aproximarmos de uma instalação, alcançamos a cancela para automóveis, que, geralmente, conta com dois seguranças. Sua função é solicitar identificação ou verificar se o veículo possui algum selo de identificação. Normalmente, esse selo é único para aquela instituição. Em alguns casos, essa verificação pode ser feita de forma automatizada com alguma tecnologia de emissão de sinal de baixa frequência, como o RFID.

Após a ultrapassagem dessa primeira barreira (camada mais externa à nossa cebola de segurança), geralmente existe mais uma etapa: catraca e elevador. Ela está vinculada a algum controle biométrico novamente surge como um exemplo.

Exemplo de RFID

Esses controles físicos são justapostos, permitindo que a vulnerabilidade de um deles possa ser recoberta por outro forma similar nas salas de servidores, *data centers* e salas-cofres, criando camadas de segurança que dificultam o a

Outro aspecto que deve ser levado em consideração é a **proteção contra ameaças da natureza**, como enchentes, inc provocadas pela natureza e/ou pelo homem.

Tendo isso em vista, certos controles de monitoramento e prevenção devem ser instalados e controlados.

Exemplo

Câmeras de segurança, controles de temperatura, extintores de incêndio e sprinkles (algumas vezes traduzidos c automáticos).

O **cabeamento** e o a**cesso à rede externa (internet)**, bem como ao **fornecimento de energia**, são fatores fundamentais dependem de um fornecimento feito por terceiros, certos aspectos contratuais e de redundância precisam ser estab

Além disso, **políticas e instruções normativas** devem ser instituídas, treinadas e simuladas visando à prontidão. Ness redundância no fornecimento de rede (internet), bem como uma independência física desse fornecimento no que tar estipulada. Veja:

É necessário evitar o uso compartilhado de conexões entre fornecedores distintos. Desse modo, se, para um fornecedor, a conexão é feita por meio de fibra ótica, para o outro ela poderia ser realizada por intermédio de link rádio.

É necessário, sobre a parte de energia elétrica, o uso de bancos de bateria (e/ou no-breaks) e de geradores. Quanto aos geradores, deve-se levar em consideração o fornecimento de insumos necessários e periódicos, como o combustível.

É necessário adotar medidas como senha na BIOS e configuração de botões físicos e de ordem de execução na inicialização dos computadores, pois em relação aos equipamentos, a ideia de segurança tem a ver com o acesso físico aos componentes de hardware e aos dispositivos de entrada.

Os maiores computadores do mundo são organizados em uma lista conhecida como Top 500 (top500.org). Pelo cust
esses equipamentos requerem uma série de recursos de proteção.

Maior recurso computacional do Brasil, o supercomputador Santos Dumont consta nessa lista. Para prover os recurso
uma série de medidas foi tomada e, em seguida, publicada no Youtube.

Segurança lógica

Medidas baseadas em software

Em adição às medidas de segurança física, há as de **segurança lógica**, que correspondem às medidas baseadas em software. Dessa lista, podemos destacar as senhas, as listas de controle de acesso, a criptografia, e o firewall.

Repetindo o padrão já apresentado, esses mecanismos estão justapostos, isto é, intercalados entre si. Dessa forma, a demanda de uma camada pode criar uma adicional a outra que possua alguma vulnerabilidade particular.

Em adição às medidas de segurança física, há as de **segurança lógica**, que correspondem às medidas baseadas em software. Dessa lista, podemos destacar as senhas, as listas de controle de acesso, a criptografia, e o firewall.

Repetindo o padrão já apresentado, esses mecanismos estão justapostos, isto é, intercalados entre si. Dessa forma, a demanda de uma camada pode criar uma adicional a outra que possua alguma vulnerabilidade particular.

Como exemplo disso, existem no próprio equipamento controles de acessos biométricos, como a leitura de digital e o reconhecimento facial. Esses sistemas de controle biométricos são caracterizados pela captura da geometria humana, a qual, em grande parte, difere em cada pessoa.

Atualmente, os leitores de digitais têm dado espaço para o reconhecimento facial pela disseminação dos sensores e diversas APIs disponibilizadas para uso gratuito e comercial, como a API do **Amazon Rekognition**. Esses controles atu confidencialidade da informação.

A **criptografia** corresponde ao conjunto de técnicas que permite o embaralhamento de dados por intermédio do uso computacionais baseados em funções matemáticas. Essas funções propiciam, em linhas gerais, a presença de duas os simétricos e os assimétricos. Vejamos!

Criptografia simétrica

Segurança lógica - criptografia simétrica

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Utiliza funções matemáticas mais simples e uma única chave para criptografar e decriptografar. Esta classe de algori outros exemplos, Cifra de César, Blowfish, Twofish e Rijnadel. Graças a esse controle, é possível assegurar a confide o conjunto na tabela a seguir:

Algoritmo	Tamanho da
AES (Rijnadel)	128, 192 e 25
Twofish	128, 192 e 25
Serpent	128, 192 e 25
Blowfish	32 a 448-b
RC4	40-128 bi
3DES (baseado no DES)	168 bits
IDEA	128 bits

Rafael D'orsi

Criptografia assimétrica

Segurança lógica - criptografia assimétrica

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Caracteriza-se por algoritmos que normalmente envolvem técnicas matemáticas mais sofisticadas, como a fatoração logaritmo discreto. Esta família **emprega duas chaves**: uma é utilizada para cifrar; a outra, para decifrar. Tais chaves s

Pública

Fica disponibilizada em um servidor de confiança.

Privada

Está sob a posse do usuário.

Com a combinação dessas chaves, é possível assegurar não somente a **confidencialidade**, mas também o **não repúd** pode-se combinar o uso desse controle tanto com a chave privada do emissor (não repúdio) quanto com a pública d (confidencialidade). Diffie-Hellman, El Gamal e Curvas Elípticas são alguns dos algoritmos dessa família. Quanto aos destacam-se os **firewalls**, os sistemas detectores de intrusão e os VPNs.

Firewalls

Equipamentos que filtram o tráfego de rede relacionado à troca de dados entre clientes e servidores.

Esses controles permitem a criação de **zonas de segurança** dentro e fora da instituição. Tais zonas possibilitam a cria funcionalidades. Das zonas de segurança, a mais comumente encontrada é a DMZ. Zona desmilitarizada, ela limita a e de aplicação podem ficar. Observe:

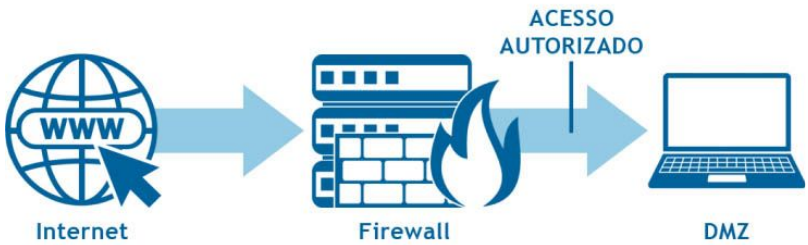


Diagrama simplificado de uma DMZ

As regras dos firewalls podem seguir duas políticas:

Negar por padrão

Todo o tráfego é negado. Apenas os servidores e os protocolos são autorizados.Trata-se da política normalmente encontrada e recomendada no mercado. Como todos os tráfegos são negados, apenas podem trafegar os tráfegos cujas regras (R1) são aceitas.

Aceitar por padrão

Todo o tráfego é autorizado, embora o determinados servidores seja negado por padrão. Regras específicas (R1 e R negados.

Mão na Massa

Questão 1

(2019 - IF-BA - assistente em administração) A respeito dos conceitos que envolvem a segurança da informação, ana

I.Os mecanismos de segurança podem ser lógicos ou físicos.
II. A perda de confidencialidade, integridade e disponibilidade é um exemplo dos eventos que comprometem a segur
III. Assinatura digital, encriptação e firewall são exemplos de mecanismos lógicos de segurança.

Assinale:

A

Se somente as afirmativas I e II estiverem corretas.

B

Se somente a afirmativa II estiver correta.

C

Se somente a afirmativa I estiver correta.

D

Se todas as afirmativas estiverem corretas.

E

Se nenhuma das afirmativas estiver correta.

A alternativa D está correta.

Mecanismos ou controles de segurança podem ser lógicos e físicos. A segurança da informação é baseada em três confidencialidade, integridade e disponibilidade. Desse modo, a perda de qualquer um dos três aspectos já impacta situação ocorre quando perdemos os três juntos: trata-se praticamente de uma catástrofe. Por fim, os mecanismos envolvem algoritmos.

Questão 2

(2019 - Comperve - UFRN - analista de tecnologia da informação) A segurança computacional possui uma terminolog na utilização dessa terminologia garante o correto entendimento entre os diferentes agentes envolvidos. Em relação afirmações sobre a segurança computacional.

I. A segurança física visa providenciar mecanismos para restringir o acesso às áreas críticas da organização a fim de autenticidade dos dados.
II. Uma ameaça pode ser definida como algum evento que pode ocorrer e acarretar algum perigo a algum ativo da re intencionais ou não intencionais.
III. São ameaças mais comuns às redes de computadores o acesso não autorizado, o reconhecimento (ex.: PortScan) DoS ou DDoS).
IV. O "tripé da segurança" é formado de pessoas, processos e políticas de segurança. De nada adianta uma política d processos não forem considerados.

Em relação à segurança computacional, estão corretas as afirmativas:

A

III e IV.

B

II e IV.

C

II e III.

D

I e II.

E

I e III.

A alternativa C está correta.

A segurança é baseada em camadas; na parte física, são definidos os controles de acesso a determinadas regiões cancelas, catracas e sistemas de acesso biométrico. Quando eles perdem sua finalidade, o atacante pode chegar f equipamento, podendo danificar a parte física dele. Dos vários problemas que podem ser realizados, devemos dest quebrar o equipamento (colocando em risco a integridade da informação) ou modificá-lo de forma prejudicial (colo autenticidade da informação). Contudo, não podemos garantir esses fatores. Neste ponto, um problema é gerado, mecanismos que podem prover, pelo menos, a autenticidade dos dados.

A ameaça é um evento que pode provocar a perda de um dos três pilares da segurança: confidencialidade, integrid as ameaças comuns às redes, os exemplos estão corretos, porém, de acordo com as últimas estatísticas, isso pode Tais ameaças são comuns, pois, até o momento, não existe uma solução completa para isso.

Questão 3

(2016 - CESPE /Cebraspe - TRT - 8ª Região - analista judiciário - tecnologia da informação) Correspondem a itens ca
proteção no âmbito da segurança física preventiva:

A

As chaves públicas criptográficas.

B

Os dispositivos de autenticação biométrica.

C

Os sistemas de autenticação por senhas *single sign on*.

D

Os certificados digitais.

E

Os sistemas de Firewall.

A alternativa B está correta.

A segurança física está relacionada ao acesso às dependências das instalações; a lógica, aos algoritmos que prote

Questão 4

(2013 - FCC - TRT - 9ª Região - técnico judiciário – segurança) Convém que sejam utilizados perímetros de seguranç
portões de entrada controlados por cartão ou balcões de recepção com recepcionistas) para proteger as áreas que
instalações de processamento da informação. Além disso, que sejam levadas em consideração e implementadas as
perímetros de segurança física, quando apropriado:

I. Os perímetros de segurança devem ser claramente definidos, assim como a localização e capacidade de resistênci
depender dos requisitos de segurança dos ativos existentes no interior do perímetro e dos resultados da análise/ava
II. Os perímetros de um edifício ou de um local que contenha instalações de processamento da informação precisam
seja, o perímetro não deve ter brechas nem pontos onde poderia ocorrer facilmente uma invasão).
III. Deve-se implantar uma área de recepção ou outro meio para controlar o acesso físico ao local ou ao edifício. Esse
somente ao pessoal autorizado.
IV. Devem ser construídas barreiras físicas para impedir o acesso físico não autorizado e a contaminação do meio am

Está correto o que se afirma em:

A

II, III e IV.

B

I, II e III.

C

II e III.

D

I, II, III e IV.

E

I e III.

A alternativa D está correta.

As instalações físicas devem possuir seguranças justapostas de forma que a fraqueza de uma camada possa ser re
lógica fica clara no funcionamento de guaritas, cancelas e sensores biométricos.

Questão 5

Ao projetar uma rede, é comum adotar um firewall para proteger uma rede interna. Com relação ao papel do firewall,
uma forma correta de classificar esse ativo de TIC.

A

Segurança lógica

B

Segurança física

C

Segurança patrimonial

D

Segurança empresarial

E

Nenhuma das alternativas

A alternativa A está correta.

O firewall é um importante ativo de rede; desse modo, encontrá-lo em um projeto de rede torna-se imprescindível.
analisando e bloqueando, por meio de algoritmos proprietários de cada marca, o acesso e o transporte de dados pa
manipulá-los, este ativo é classificado como segurança lógica.

Questão 6

A partir da pandemia ocorrida em 2020, os sistemas de acesso evoluíram para o uso de reconhecimento facial. Muito
slogans bem criativos, como este: “Um sistema de acesso com reconhecimento facial permite levar a sua empresa di
alta tecnologia por meio do uso desta importante ferramenta de segurança: _____”.

Marque a alternativa que apresenta o termo que completa o slogan anterior de forma mais satisfatória.

A

Lógica

B

Física

C

Mista

D

Empresarial

E

Patrimonial

A alternativa B está correta.

Um sistema de acesso, independentemente do tipo de chave (senha) criado, permite o bloqueio físico a determinad
com o passar do tempo, vem evoluindo bastante: cartões com códigos de barra, tarja magnética, digital, veias da m
facial.

Verificando o aprendizado

Questão 1

(2019 - FCC - TRF - 4ª Região - analista judiciário - sistemas de tecnologia da informação) Suponha que um analista
4ª Região se depare com uma situação em que deve implantar mecanismos de proteção interna voltados à segurança
informações no ambiente do tribunal. Para isso, ele levantou os seguintes requisitos:

I. Não instalar em áreas de acesso público equipamentos que permitam o acesso à rede interna do tribunal.
II. Os usuários não podem executar transações de TI incompatíveis com sua função.
III. Apenas usuários autorizados devem ter acesso ao uso dos sistemas e aplicativos.
IV. É necessário proteger o local de armazenamento das unidades de backup e restringir o acesso a computadores e
conter dados confidenciais.

O analista classificou correta e respectivamente os requisitos de I a IV como uma segurança:

A

física, física, lógica e física.

B

física, lógica, lógica e física.

C

lógica, física, lógica e física.

D

lógica, física, física e lógica.

E

física, lógica, lógica, lógica.

A alternativa B está correta.

A segurança física está relacionada ao acesso às instalações, enquanto a lógica trata dos algoritmos.

Questão 2

(2018 - Cesgranrio - Transpetro - analista de sistemas júnior - processos de negócio) Para proteger as redes de dad
perímetros de segurança formados por componentes que avaliam o tráfego de ingresso e egresso. O componente qu
acesso formadas por regras que determinam se um pacote pode ou não atravessar a barreira é a(o):

A

firewall.

B

proxy.

C

DMZ.

D

IPS.

E

roteador.

A alternativa A está correta.

O firewall usa as regras para criar barreiras e políticas relacionadas.

Considerações finais

Elencamos os conceitos básicos da área de segurança e informação, citando seu valor, sua propriedade e seu ciclo d
segurança física, lógica e controle de acesso.

Abordamos o ciclo de vida e os problemas relacionados em cada etapa. Em seguida, apresentamos os principais me
criptografia, além destes pilares de segurança: confidencialidade, integridade e disponibilidade.

Falamos sobre a segurança física, que se relaciona com o acesso físico às instalações; e a lógica, que está ligada aos
verificamos conceitos importantes, como o do firewall e das zonas delimitadas por ele.

Podcast

Para encerrar, ouça um resumo sobre os principais assuntos abordados.

Conteúdo interativo

Acesse a versão digital para ouvir o áudio.

Explore +

Confira o que separamos especialmente para você!

Pesquise no Youtube os seguintes vídeos:

IBM Cloud e Amazon Web Services. A nuvem ou cloud computing é um processo que vem mostrando muita força.

Supercomputador Santos Dumont. É o maior recurso computacional do país; conhecê-lo é uma ótima forma de analis

Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Norma ABNT ISO/IEC 27.0002/2013** – boas práticas para gestão
Código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2005.

BARRETO, J. dos S.; ZANIN, A.; MORAIS, I. S. de; VETTORAZZO, A. de S. **Fundamentos de segurança da informação**. S

BE COMPLIANCE. **Ladrão rouba HDs com dados de 29 mil funcionários do Facebook**. Publicado em: 19 dez. 2019.

BRASIL. **Decreto-lei nº 3.689, de 3 de outubro de 1941**. Código de Processo Penal. Brasília, 1941.

FREIRE, A. **Notebooks furtados da Petrobras estavam na Bacia de Santos, diz PF**. G1, 5 fev. 2008.

GUSMÃO, G. **Os 15 maiores vazamentos de dados da década**. Exame, 21 fev. 2014.

MEARIAN, L. **Survey**: 40% of hard drives bought on eBay hold personal, corporate data. Computerworld, 10 fev. 2009

RODRIGUES, F. N. **Segurança da informação** - princípios e controles de ameaças. São Paulo: Érica, 2019.