Estratégia Concursos

Aula 00

DPE-RO (Analista de Defensoria - Programação) Segurança da Informação

Autor:
André Castro, Equipe Informática e TI

13 de Janeiro de 2023

Índice

Sumário

PRINCÍPIOS DE SEGURANÇA

Considerando a era da Informação em que nos encontramos atualmente, aspectos de **Segurança da Informação** são **fundamentais em qualquer ambiente.**

Diversas são as empresas e organizações que mantêm toda a sua vantagem competitiva, base de negócios, investimentos, entre outros pontos extremamente importantes ancorados em suas informações ou dados. A informação e seus ativos são, de fato, os elementos mais importantes de uma organização.

Desse modo, tais instituições necessariamente devem se resguardar de diversas formas de possíveis problemas relacionados a esse tópico.

Nesse sentido, aplicam-se muitos conceitos e padrões de segurança que visam amenizar os problemas atrelados de alguma forma a esse assunto.

Para iniciarmos, de fato, o referido assunto, vamos definir os três principais pilares que compõem a base da Segurança da Informação, quais sejam:

> **1. Confidencialidade** – Aqui temos o princípio que visa **zelar pela privacidade** e sigilo dos dados de tal modo que estes devem ser acessados ou visualizados somente por aqueles de direito, ou seja, a informação só deve estar disponível para aqueles com a devida autorização.

Desse modo, a título de analogia, caso alguém envie uma carta dentro de um envelope e alguma pessoa indevidamente tenha acesso ao envelope, até então não temos problemas.

Referenciamos tal fato como interceptação dos dados. Entretanto, caso a pessoa mal-intencionada coloque o envelope contra a luz e verifique o conteúdo da carta, aí sim termos a violação do princípio da confidencialidade.

Ano: 2021 Banca: CESPE Órgão: UFES Prova: Analista em TI

Segundo Machado (2014), o princípio fundamental de segurança da informação que é definido como a capacidade de garantir que o nível necessário de sigilo seja aplicado aos dados, tratando-se da prevenção contra a divulgação não autorizada desses dados

A) integridade.

B) disponibilidade.

C) criptografia.

D) privacidade.

E) confidencialidade.

Comentários:

Primeira questão da nossa sequência de conteúdo a ser abordado. Pessoal, percebam que o foco no enunciado é justamente o sigilo e prevenção contra a divulgação não autorizada. Vimos que duas palavras chaves do princípio da Confidencialidade são SIGILO e PRIVACIDADE.

Muito cuidado, pois, a privacidade é uma característica do princípio da CONFIDENCIALIDADE.

Gabarito: E

2. Integridade (Confiabilidade) – No segundo princípio, temos como objetivo garantir que os **dados trafegados sejam os mesmos** do início ao fim de um determinado trecho, ou seja, que a mesma mensagem gerada na origem chegue ao destino de forma intacta.

Ora, considerando o exemplo anterior, após a leitura indevida dos dados, a pessoa mal-intencionada poderia entregar o envelope com a carta para o destinatário. Logo, a mensagem é a mesma que foi gerada pela origem, certo? Exato! Dessa forma, não tivemos a violação do princípio da integridade.

Agora, caso a pessoa altere a mensagem, teremos sim um problema de integridade dos dados.

Importante destacar que também há a perspectiva dos dados em repouso, isto é, armazenado em algum local. Nessa condição, também deverá ser observado o princípio da integridade. Na prática, **caso este arquivo armazenado sofra algum tipo de modificação não autorizada,** também teremos uma violação do princípio.

Um exemplo que gosto de citar para materializar um pouco algum interesse difuso nesse aspecto seria alguém conseguir acessar os dados e arquivos de um contador. Nos referidos documentos, consta uma planilha de controle com a relação de empresas e referidas contas bancárias gerenciadas pelo profissional. Na ocasião, o usuário que está com má intenção realizará a alteração das contas no documento para que ele possa se beneficiar de alguma forma nesse processo.

FGV – Analista Técnico – Tecnologia da Informação (TCE-TO)/2022

O auditor José recebeu o arquivo AnexoJ em formato digital. Antes de proceder com a abertura do AnexoJ, José determinou a fidedignidade do referido arquivo, avaliando a conformidade dos dados do AnexoJ por ele recebido com os dados do AnexoJ transmitido pelo emissor.

Essa avaliação feita por José em AnexoJ está diretamente relacionada com o seguinte princípio da segurança de informações:

a) integridade;

b) confidencialidade;

c) autenticidade;

d) disponibilidade;

e) qualidade.

Comentários:

Pessoal, vejam que a palavra fidedignidade vem justamente para reforçar o conceito de integridade e conformidade dos dados. Isso quer dizer que o documento não sofreu adulteração ou problemas na transmissão, logo, pode-se confiar no documento em tela.

Gabarito: A

3. Disponibilidade – Nesse princípio, temos como principal objetivo o fato de determinado **recurso poder ser utilizado** quando este for requisitado em um determinado momento, considerando a devida autorização do usuário requisitante e a própria integridade do dado ou serviço a ser requisitado. Desse modo, quando tentamos acessar o site da Receita Federal, por exemplo, no primeiro dia de declaração de Imposto de Renda, teremos a experiência por diversos usuários da violação do princípio da disponibilidade caso estes não consigam acessar o site ou enviar suas requisições por falha no sistema ou volume de acesso que consomem todos os recursos disponíveis, impedindo a utilização por novos usuários.

FGV - 2023 - CGE-SC - Auditor do Estado - Ciências da Computação - Tarde (Conhecimentos Específicos)

Para o caso hipotético descrito a seguir, somente informações corretas são consideradas disponíveis.

Um determinado funcionário atende um pedido por telefone de alguém que se identifica como o cliente A. Essa pessoa explica que seus dados cadastrais estão errados e pede que seja feito um novo cadastro com as informações que ela está passando. O funcionário atende ao pedido e atualiza o sistema da empresa removendo o cadastro antigo e criando um novo.

Dias depois, ao tentar emitir uma fatura, a empresa nota que os dados do cliente A não estão completos e resolve abrir uma investigação. Durante a investigação descobre-se que os dados passados pela pessoa ao telefone eram falsos e que é portanto necessário refazer o cadastro.

Neste caso, avalie se, durante o processo de atendimento mencionado, ocorreu um incidente com quebra da

I. Confidencialidade dos dados do cliente A. II. Disponibilidade dos dados do cliente A. III. Integridade dos dados do cliente A.

Está correto o que se afirma em

A I, apenas.

B II, apenas.

C III, apenas.

D I e II, apenas.

E II e III, apenas.

Comentários:

Questão bem interessante da FGV que traz a perspectiva mais correta, a meu ver, do entendimento do princípio da disponibilidade em conjunto com a integridade.

Creio que não temos muitas dúvidas a respeito da quebra do princípio da integridade, correto? É uma tendência natural associar somente a ela, visto que as informações não estavam adequadas ou íntegras, gerando assim a necessidade de um recadastro.

O ponto de atenção fica por conta da disponibilidade dos dados, uma vez que, os dados disponíveis não eram úteis à necessidade da empresa. Assim, a disponibilidade também fora afetada, uma vez que não se tinha a informação necessária no momento.+

Gabarito: E

Ademais, outros conceitos também surgem com grande relevância, senão vejamos:

1. Autenticidade – O princípio da autenticidade busca garantir que determinada pessoa ou sistema é, de fato, quem ela diz ser. Ou seja, quando utilizamos o simples recurso de inserir as informações de login e senha em um computador, estamos dizendo ao computador que **realmente somos o usuário** pois ele assume que somente o usuário legítimo em questão possui a informação de login e senha.

Importante informar que nesse processo, para a devida realização da autenticação, é necessário cumprir a etapa preliminar de identificação, onde será possível coletar as informações necessárias sobre o usuário para posteriormente, validá-lo.

Nesta etapa de identificação, temos muitos exemplos de cunho muito prático do nosso dia a dia, seja pela utilização de uma **impressão digital ou reconhecimento facial, logins e senhas tradicionais, utilização de cartões físicos ou digitais de acesso, entre muitos outros.**

Ano: 2020 Banca: CESPE Órgão: SEFAZ/AL Prova: Auditor de Finanças e Controle

Identificação e autenticação são requisitos de segurança da informação que consistem em identificar usuários do sistema e verificar as suas identidades, como pré-requisito para permitir o acesso desses usuários ao sistema.

Comentários:

Tranquilo, certo pessoal? Mencionamos a importância do processo de identificação preliminarmente, para posterior realização do processo de autenticação. Um peque destaque que deixo nessa questão, que abordaremos mais à frente da nossa aula é a questão das permissões e autorizações de acesso. Vejam que a questão não tratou a identificação e autenticação como garantidores dessa permissão, mas como pré-requisitos apenas.

Veremos mais à frente que o processo de autenticação é complementado pela etapa de autorização, que será responsável por gerenciar as credenciais e permissões de acesso.

Gabarito: C

2. Não-Repúdio (Irretratabilidade) – Neste princípio, busca-se garantir que o **usuário não tenha condições de negar ou contrariar o fato de que foi ele quem gerou determinado conteúdo ou informação**, ou ainda que determinado receptor tenha, de fato, recebido certa mensagem. Tal princípio se aplica, por exemplo, na geração de uma autorização para compra de determinado produto e depois, o gestor responsável queira negar a autorização. Entretanto, utiliza-se mecanismos para que não haja possibilidade de haver a referida negação.

Stallings traz ainda a seguinte definição:

"A **irretratabilidade impede que o emissor ou o receptor negue uma mensagem transmitida.** Assim, quando uma mensagem é enviada, o receptor pode provar que o emissor alegado de fato enviou a mensagem. De modo semelhante, quando uma mensagem é recebida, o emissor pode provar que o receptor alegado de fato recebeu a mensagem."

Ano: 2022 Banca: FGV Órgão: TJDFT Prova: Suporte em TI

Lucas é um trader profissional que trabalha em uma corretora de valores. Ele efetua muitas operações durante o período em que a bolsa negocia seus ativos. Após fazer uma revisão em suas operações do dia, não validou, como sendo efetuadas por ele, algumas das operações que obtiveram prejuízo. Lucas, então, entrou em contato com a corretora e esta demonstrou, a partir de registros de auditoria e garantia de identidade, que as operações em questão realmente foram executadas por ele.

Para que a corretora prove que foi Lucas quem realmente executou as operações, ela deve fazer uso do conceito de segurança chamado:

A) confidencialidade;

B) autenticidade;

C) integridade;

D) disponibilidade;

E) irretratabilidade.

Comentários:

Exatamente como vimos na nossa explanação. Tenham muito cuidado na leitura da questão, pois, conforme este caso, o aluno poderia marcar a opção autenticidade por observar as menções no enunciado de reconhecer o usuário. Mas percebam que o foco é justamente na incapacidade de Lucas negar que tenha realizado tal operação.

Gabarito: E

3. Legalidade – O aspecto de legislação e normatização é fundamental nos processos relacionados à Segurança da Informação. Desse modo, **respeitar a legislação vigente é um aspecto fundamental e serve, inclusive, como base para o aprimoramento e robustez dos ambientes.**

(Ano: 2021 Banca: FGV Órgão: IMBEL Prova: FGV - 2021 - IMBEL - Supervisor - Tecnologia da Informação) Segundo padrões internacionais, a Segurança da Informação distingue quatro atributos básicos que orientam a implementação de políticas e procedimentos de proteção. Assinale o atributo que não é parte desse grupo.

A) Autenticidade.

B) Completude.

C) Confidencialidade.

D) Disponibilidade.

E) Integridade.

Comentários:

Sem muito segredo até aqui, certo? Acabamos de destacar as características dos principais princípios: Autenticidade; Confidencialidades; Disponibilidade; Integridade.

Gabarito: B

Tranquilo até aqui pessoal? Esses conceitos são extremamente importantes. Quero aproveitar para registrar alguns conceitos complementares previstos na norma de referência X.800 que trata da Segurança de arquiteturas, principalmente no que tange a soluções de rede distribuídas. Vamos conhecê-los:

- **Autenticação de entidade Parceiras**
  - Usada em associação com uma conexão lógica com a capacidade de prover confiabilidade a respeito da identidade das entidades conectadas.

- **Autenticação da origem dos Dados**
  - Considerando uma transferência sem conexão entre as partes, visa assegurar que a origem dos dados recebidos é quem ela afirma ser.

- **Confidencialidade de campo seletivo**
  - Busca-se manter a confidencialidade de campos específicos dentro do volume de dados de um usuário em uma conexão.

- **Confidencialidade do fluxo de tráfego**
  - Busca-se gerar a confidencialidade sob a perspectiva do fluxo, ou seja, a simples análise do fluxo de dados não deve ser capaz de gerar informações indevidas.

- **Integridade de conexão com recuperação**
  - Como o próprio nome diz, é capaz de detectar qualquer modificação, inserção, deleção ou repetição de quaisquer dados dentro de uma sequência de dado. Além disso, é capaz de recuperar a intervenção realizada.

- **Integridade de conexão sem recuperação**
  - Como vimos, neste caso, não há capacidade de recuperação, mas tão somente de detecção.

- **Integridade de conexão de campo seletivo**
  - Assim como a confidencialidade seletiva, aqui, busca-se garantir a integridade de áreas e dados específicos. Assim, busca-se avaliar se houve modificação, inserção, eliminação ou repetição dessa parcela.

- **Integridade sem conexão**
  - Considera a capacidade de prover a integridade de dados em um ambiente sem conexão. Possui o foco na detecção de modificações e uma capacidade limitada de detectar repetições.

- **Integridade de campo seletivo sem conexão**

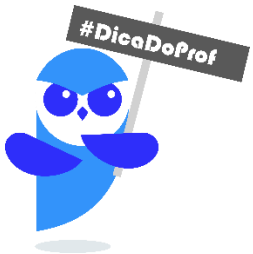
- Mesma condição do tipo acima, porém, de áreas de dados específicos ou seletivos.

- **Irretratabilidade de origem**
  - É o padrão que vimos, uma vez que é possível provar que a mensagem foi enviada por determinada parte.

- **Irretratabilidade de destino**
  - A perspectiva aqui é diferente. Consegue-se provar que o destinatário recebeu determinada mensagem.

Segurança de Redes

O Cert.br, principal órgão do Brasil responsável pelo fomento **à Segurança da Informação**, nos traz alguns conceitos que são constantemente explorados pelas bancas examinadoras. Nesse sentido, vamos conhecê-los:



- **Furto de dados:** informações pessoais e outros dados podem ser obtidos tanto pela interceptação de tráfego como pela exploração de possíveis vulnerabilidades existentes em seu computador;

- **Uso indevido de recursos:** um atacante pode ganhar acesso a um computador conectado à rede e utilizá-lo para a prática de atividades maliciosas, como obter arquivos, disseminar spam, propagar códigos maliciosos, desferir ataques e esconder a real identidade do atacante;

- **Varredura:** um atacante pode fazer varreduras na rede, a fim de descobrir outros computadores e, então, tentar executar ações maliciosas, como ganhar acesso e explorar vulnerabilidades;

- **Interceptação de tráfego:** um atacante, que venha a ter acesso à rede, pode tentar interceptar o tráfego e, então, coletar dados que estejam sendo transmitidos sem o uso de criptografia;

- **Exploração de vulnerabilidades:** por meio da exploração de vulnerabilidades, um computador pode ser infectado ou invadido e, sem que o dono saiba, participar de ataques, ter dados indevidamente coletados e ser usado para a propagação de códigos maliciosos. Além disto, equipamentos de rede (como modems e roteadores) vulneráveis também podem ser invadidos, terem as configurações alteradas e fazerem com que as conexões dos usuários sejam redirecionadas para sites fraudulentos;

- **Ataque de negação de serviço:** um atacante pode usar a rede para enviar grande volume de mensagens para um computador, até torná-lo inoperante ou incapaz de se comunicar;

- **Ataque de força bruta:** computadores conectados à rede e que usem senhas como métodos de autenticação estão expostos a ataques de força bruta. Muitos computadores, infelizmente, utilizam, por padrão, senhas de tamanho reduzido e/ou de conhecimento geral dos atacantes;

- **Ataque de personificação**: um atacante pode introduzir ou substituir um dispositivo de rede para induzir outros a se conectarem a este, ao invés do dispositivo legítimo, permitindo a captura de senhas de acesso e informações que por ele passem a trafegar.


Segurança da Informação
Furto de dados: dados podem ser obtidos pela interceptação de tráfego
Ataque de personificação: atacante pode introduzir ou substituir um dispositivo de rede para induzir outros a se conectarem a este
Ataque de força bruta: computadores conectados à rede e que usem senhas como métodos de autenticação estão expostos a ataques de força bruta
Ataque de negação de serviço: atacante pode usar a rede para enviar grande volume de mensagens para um computador, até torná-lo inoperante ou incapaz de se comunicar
Exploração de vulnerabilidades: computador pode ser infectado ou invadido
Interceptação de tráfego: atacante pode tentar interceptar o tráfego e coletar dados que estejam sendo transmitidos sem o uso de criptografia
Varredura: atacante pode fazer varreduras na rede, a fim de descobrir outros computadores
Uso indevido de recursos: atacante pode ganhar acesso a um computador conectado à rede e utilizá-lo

SEGURANÇA FÍSICA, LÓGICA E CONTROLE DE ACESSO

Quando falamos de Segurança da Informação, há uma diferenciação clássica no que tange as características dos elementos e ferramentas utilizadas para esta finalidade.

Seguimos aqui o mesmo princípio visto na nossa aula de topologia de redes em que diferenciamos os conceitos de implementação física e lógica.

Lembrando que a **física diz respeito aos aspectos tangíveis** e que, de fato, podem ser tocados, enquanto a **lógica está relacionada aos dados em seu formato analógico ou digital**, tanto no aspecto de transmissão, processamento e armazenamento.

Segurança Física

Podemos citar diversos elementos que são considerados como recursos para a segurança física. Vamos conhecer alguns:

1. ***Unidade de Alimentação Ininterrupta (UPS)*** **–** São sistemas munidos de baterias que são capazes de **armazenar energia e fornecer corrente elétrica aos demais equipamentos por um período limitado.** Assim, em caso de ausência de energia, esses equipamentos possibilitam o funcionamento dos equipamentos por um período suficiente em que os administradores da rede podem atuar com vistas a mitigar perdas.

2. ***Gerador –*** Seguindo a mesma linha do IPS, o gerador também tem como propósito **manter o sistema em operação frente à eventual falta de energia**. Entretanto, estamos falando de um período muito mais de sustentação podendo ser prolongado facilmente, uma vez que se utiliza combustível como fonte de energia.

3. ***Site físico redundante –*** *Busca*-se criar outro ambiente **que seja capaz de assumir a operação em caso de catástrofe que prejudique o ambiente principal**. Para tanto, é muito importante que os dados sejam armazenados e replicados, seja online, ou em fitas e equipamentos disponibilizados em outro local.

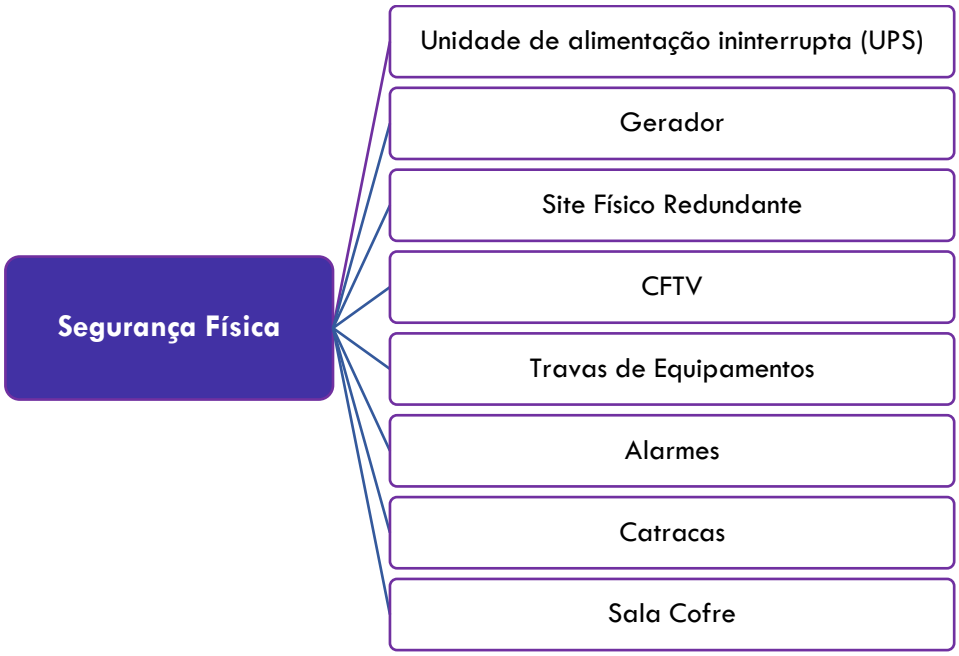
4. ***CFTV –*** Temos aqui a utilização de câmeras para registro e visualização dos ambientes de uma organização. É um meio eminentemente reativo, uma vez que, na maioria das vezes, **é utilizado para gravar o vídeo e ser utilizado posteriormente para análise e auditoria.**

5. ***Travas de Equipamentos –*** *As* referidas travas podem ser utilizadas tanto para impedir a utilização de determinados recursos, como bloqueio de portas USB ou unidades de DVD, de forma física, como também no intuito de não possibilitar o furto de notebooks, por exemplo, através das conhecidas chaves **kensington,** que, literalmente, “prendem” o equipamento em uma localidade.

6. ***Alarmes –*** Temos aqui um sistema de aviso que pode ser considerando no seu aspecto físico, como **alarmes de incêndio**, como no **aspecto lógico**, como **alarmes lógicos de rede**.

7. ***Catracas –*** A partir da utilização de senhas, crachás, smartcards, entre outros, **pode-se restringir o acesso somente a pessoas autorizadas** em determinados locais.

8. ***Sala Cofre –*** As Salas Cofre são criadas para serem um ambiente seguro para datacenters, implementando **diversos tipos de controles de segurança**, de acesso, mecanismos de reação a catástrofes, entre outros.



Segurança Lógica

A segurança lógica possui diversas vertentes que podem ser consideradas. Podemos considerar a segurança a nível de um servidor de rede e serviços, por exemplo, em que devemos considerar a proteção dos recursos computacionais em todas as suas camadas, desde a **linguagem de máquina** e **Kernel do SO**, passando pelo próprio sistema operacional, arquivos, aplicações, dados, entre outros.

Podemos considerar a segurança lógica a nível da rede em que devemos inserir elementos que visam controlar o tráfego e impedir o acesso indevido aos dados trafegados ou ainda impedir que determinados tipos de fluxos passem pela rede. Neste cenário, pode-se utilizar **firewalls, IDS, IPS, Proxies, entre outros elementos.**

Podemos contemplar ainda as autorizações de usuários específicos e sistemas que podem acessar e utilizar determinados recursos na rede, sendo esse mecanismo **conhecido como autorização.**

Mencionamos ainda os registros e logs dos diversos equipamentos, sistemas e aplicações em um parque tecnológico. Tais registros são fundamentais para processos de auditoria, sendo, portanto, um recurso de segurança lógica.

Ano: 2021 Banca: CESPE / CEBRASPE Órgão: PG-DF

As boas práticas da gestão dos controles de acesso lógico de uma organização incluem atribuir direitos de acesso aos usuários, conforme necessidades reais de seu trabalho ou cargo, disponibilizar contas de usuários apenas a pessoas autorizadas, armazenar senhas criptografadas e usar técnicas visíveis de identificação.

Comentário:

Muito cuidado pessoal. A questão traz uma boa narrativa que convence. Mas nem todos os itens elencados são boas práticas. O item que fica fora dessa lista é a técnica de armazenamento de senhas criptografadas. Na prática, uma forma de deixar os servidores e os dados armazenados neste equipamento mais seguros é por meio do armazenamento dos HASHES dessas senhas. O HASH, nada mais é do que uma função unidirecional que gera um resumo do conteúdo de entrada com tamanho físico.

Nosso objetivo não é aprender sobre HASH nessa aula, mas saber que ele é uma boa prática associada ao armazenamento de senhas.

Os demais itens, lembrando, estão aderentes como boas práticas a serem adotadas.

Gabarito: E

Outro conceito interessante que surge a esse respeito é o de **HARDENING.** A ideia do HARDENING é, de fato, **"endurecer"** um servidor de tal modo a deixá-lo mais robusto e seguro.

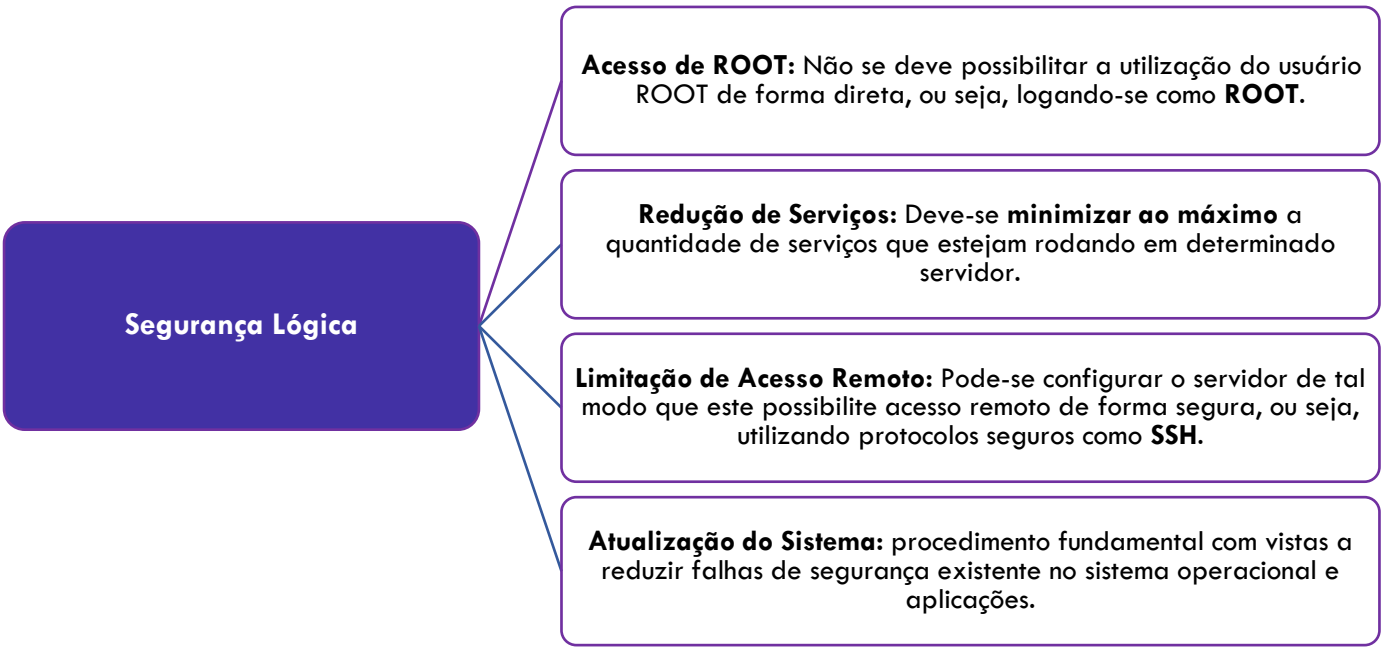
Diversos são os métodos ou regras a serem implementadas. Buscarei elencar algumas e complementaremos, eventualmente, nos exercícios:

1. **Acesso de ROOT** – Não se deve possibilitar a utilização do usuário ROOT de forma direta, ou seja, logando-se como **ROOT**. Para tanto, deve-se utilizar apenas o método de escalação de privilégios, ou seja, deve-se logar como determinado usuário para posterior mudança de privilégio e consequente execução de comandos ou aplicações. Isto possibilita a geração de lastros e trilhas de auditorias, além de ser mais uma camada de segurança.

2. **Redução de Serviços** – Deve-se **minimizar ao máximo** a quantidade de serviços que estejam rodando em determinado servidor. Isto tem o intuito de reduzir a possibilidade de vulnerabilidades existentes nas aplicações e serviços, bem como aumentar o desempenho do servidor. Portanto, deve-se manter apenas os serviços e aplicações necessárias, nada mais.

3. **Limitação de Acesso Remoto** – Pode-se configurar o servidor de tal modo que este possibilite acesso remoto de forma segura, ou seja, utilizando protocolos seguros como **SSH**. Além disso, pode-se restringir a máquinas ou redes específicas que poderão acessar o referido servidor.

4. **Atualização do Sistema** – É um procedimento fundamental com vistas a reduzir falhas de segurança existente no sistema operacional e aplicações. Assim, deve-se manter e instalar as **últimas versões e mais atualizadas.**



FGV - 2021 - Banestes - Analista em Tecnologia da Informação - Segurança da Informação

O conceito de hardening caracteriza-se principalmente por medidas e ações que visam:

A permitir a recuperação de sistemas computacionais na sequência de um desastre natural;

B criar ambientes similares ao de servidores físicos, de modo que sistemas computacionais operem independentes do hardware;

C mapear ameaças, mitigar riscos e tornar sistemas computacionais preparados para enfrentar tentativas de ataque;

D distribuir a carga de trabalho uniformemente entre dois ou mais computadores para aumentar a confiabilidade através da redundância;

E construir sistemas computacionais sem preocupação com a infraestrutura em que esses sistemas estão rodando.

Comentário:

Temos uma abordagem conceitual. Então, de fato, ao mapear as ameaças e realizar ações de mitigação de riscos, pode-se reduzir a superfície de ataque e torná-los mais difíceis ou ineficientes.

A) Esse item se refere a processo de disaster recovery.

B) Estamos falando dos conceitos de virtualização.

D) Estamos falando de balanceamento de carga.

E) Também associado aos conceitos de virtualização.

Gabarito: C

(Ano: 2021 Banca: CESPE Órgão: PG-DF Prova: Técnico Jurídico – TI)

Suponha que um Analista do Tribunal Regional Federal da 4ª Região – TRF4 se depare com uma situação em que deve implantar mecanismos de proteção interna voltados à segurança física e lógica das 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 de uso dos sistemas e aplicativos.

IV. Proteger o local de armazenamento das unidades de backup e restringir o acesso a computadores e impressoras que possam conter dados confidenciais.

O Analista classificou correta e respectivamente os requisitos de I a IV como 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, física e lógica.

Comentários:

Pessoal, lembrem-se da dica no sentido de entenderem se o item é tangível, ou seja, algo que se toca, ou não. Caso seja o primeiro, estamos falando de segurança física. Caso seja o segundo, estamos falando de segurança lógica.

I – Trata-se se segurança física, pois a itenção é não permitir o acesso direto ao equipamento, no caso, o Access Point.

II – Estamos falando de transações, ou seja, operações nos sistemas. Neste aspecto, estamos no mundo lógico.

III – Novamente, estamos falando de acesso lógicos, em sistemas e aplicativos. E não acesso a equipamentos. Logo, também é lógico.

IV – Vejam que o interesse é em proteção de local, além de acesso aos computadores e impressoras, que também são itens materiais. Logo, segurança física.

Gabarito: B

(Ano: 2021 Banca: CESPE Órgão: PG-DF Prova: Técnico Jurídico – TI)

O conceito de hardening caracteriza-se principalmente por medidas e ações que visam:

A) permitir a recuperação de sistemas computacionais na sequência de um desastre natural;

B) criar ambientes similares ao de servidores físicos, de modo que sistemas computacionais operem independentes do hardware;

C) mapear ameaças, mitigar riscos e tornar sistemas computacionais preparados para enfrentar tentativas de ataque;

D) distribuir a carga de trabalho uniformemente entre dois ou mais computadores para aumentar a confiabilidade através da redundância;

E) construir sistemas computacionais sem preocupação com a infraestrutura em que esses sistemas estão rodando.

Comentários:

Vejam que a questão traz alguns pontos que devem ser observados previamente à realização das ações de HARDENING propriamente dito. Então, quando se fala em Mapear ameaças para mitigar riscos, naturalmente devemos realizar ações que tornarão os sistemas computacionais mais seguros e isso quer dizer que eles precisam ter maior robustez frente às suas configurações e serviços habilitados.

Gabarito: C

Controle de Acesso

Temos aqui um método aplicado tanto no contexto físico e lógico, com vistas a estabelecer barreiras que podem restringir determinados acessos a locais, equipamentos, serviços e dados **a pessoas. O controle de acesso está diretamente ligado ao princípio da autenticidade e autorização.**

Considerando o controle de acesso físico, temos então a primeira barreira a ser implementada. Nessa etapa pode-se diferenciar funcionários que são da organização ou não, usuários da organização que possuem autorização para acessar determinadas localidades, entre outros.

Assim, como exemplo, **para um usuário acessar fisicamente o ambiente** de datacenter de uma empresa, ele necessitará passar por diversos fatores de controle de acesso, como a cancela de entrada para o veículo, portaria e catraca na entrada do edifício, autenticação e autorização por algum mecanismo, como o de biometria para a sala, possuir alguma chave específica para acessar determinado rack com os servidores, e por aí vai.

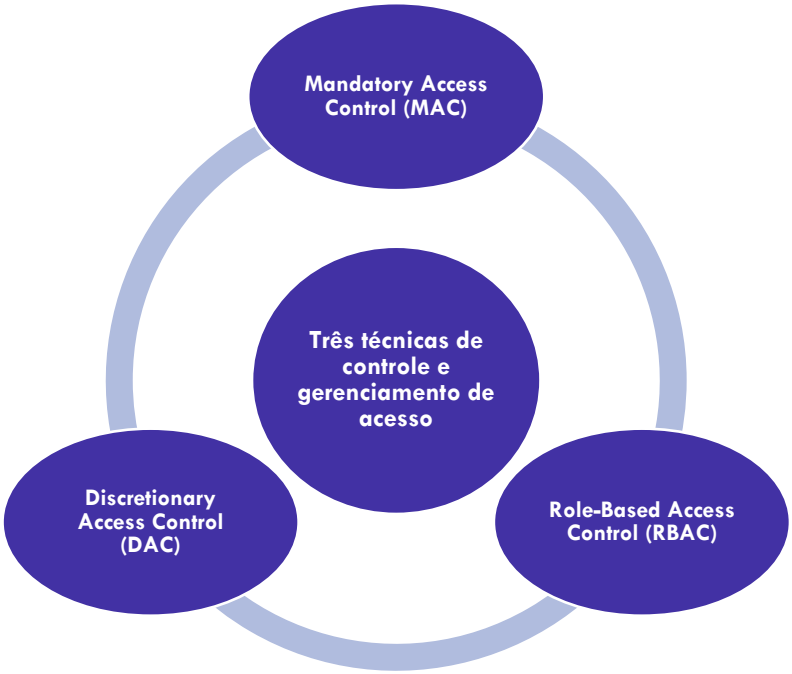
Além disso, pode-se implementar recursos para controle de acesso lógico. Entre eles podemos citar a restrição de acesso por IP a determinado serviço, necessidade de login e senha, tanto para o usuário quanto para o root, entre outros.

Existem **três técnicas de controle e gerenciamento de acesso** que são amplamente utilizadas nos ambientes de tecnologia da informação.

- **Mandatory Access Control (MAC)** – O administrador do sistema é responsável por atribuir as devidas permissões para os usuários. Este modelo utiliza o conceito de “label” para identificar o nível de sensibilidade a um determinado objeto. O label do usuário é verificado pelo gerenciador de acesso e através desta avaliação, é verificado o nível de acesso do usuário e quais recursos ele é capaz de usar.

- **Discretionary Access Control (DAC)** – Este é um modelo mais flexível quando comparado com o MAC e considerando o usuário que necessita compartilhar o recurso com outros usuários. Nesta técnica, o usuário tem o controle de garantir privilégios de acesso a recursos aos que estão sob seu domínio. Como exemplo desta técnica, podemos citar o próprio sistema de permissão do linux ou windows, por exemplo, em que o próprio usuário pode determinar as permissões do arquivo em que ele tem a posse.

- **Role-Based Access Control (RBAC)** – Também conhecido como controle baseado em papéis. Nesta técnica, o administrador garantir privilégios de acordo com a função exercida pelo usuário. Esta estratégia simplifica o gerenciamento das permissões dadas aos usuários.



Ano: 2019 Banca: CESPE / CEBRASPE Órgão: TCE-RO

O modelo de controle de acesso que permite níveis de interação e acesso aos recursos dos sistemas de acordo com as funções que os usuários desempenham na organização é o

A discricionário.

B embasado em papéis.

C em matriz.

D embasado em regras.

E mandatório.

Comentários:

Vejam a palavra chave, pessoal. De acordo com as suas funções ou papeis. Logo, temos o modelo RBAC, que é, embasado em papéis.

Gabarito: B

(Ano: 2021 Banca: CESPE Órgão: PG-DF Prova: Técnico Jurídico – TI)

Para o controle de acesso a sistemas de informação, podem ser adotadas diferentes formas de controle de acesso lógico, com vistas à segurança de um recurso. Quanto a essas formas de controle, assinale a opção correta.

A Do ponto de vista do usuário, um controle discricionário é, em geral, menos flexível que um mandatório.

B Em geral, é mais difícil auditar sistemas que operam com controle de acesso discricionário do que sistemas com controle de acesso mandatório.

C Como regra geral, no controle de acesso mandatório, os donos e usuários de recursos podem conceder acesso além dos limites declarados pela política da empresa.

D No controle discricionário, podem ser transferidos para terceiros os direitos de acesso, mas não a propriedade de um recurso.

E Em um sistema mandatório, o acesso é concedido com base na avaliação das funções dos sujeitos em relação às reivindicações relacionadas ao seu papel no sistema de informação.

Comentários:

Cobrança direta do conteúdo que acabamos de ver. Vamos aos itens:

a) Vimos que o controle mandatório é o mais rídigo, logo, menos flexível, e não o discricionário como a presenta o item.

b) Exatamente pessoal. Como o mandatório tem a visão centralizada, a partir do admin da rede, há menos variação nas pastas e objetos. Logo, de fato, é mais fácil de se auditar.

c) Questão invertida. Tem-se a descrição do controle discricionário.

d) O erro estaá em afirmar que não se pode transferir a propriedade. Ela é possível também de ser transferida.

e) Aqui, temos o descritivo do modelo RBAC, dado o trecho focado nas funções ou papeis dos sujeitos.

Gabarito: B

AUTENTICAÇÃO E SEUS MECANISMOS

Os mecanismos de autenticação são **procedimentos, rotinas, ferramentas ou soluções que implementam, de fato, o princípio de autenticação com o devido controle de acesso.** Estes podem ser subdivididos em três grandes grupos, quais sejam:

1. ***Algo que você sabe***

Nesta categoria, busca-se determinar a autenticidade dos usuários baseado em alguma informação que seja **de conhecimento único daquele usuário**. Podemos utilizar, como exemplo clássico, a nossa senha de acesso à rede corporativa do local onde trabalhamos. Ora, assume-se que a informação de senha seja de conhecimento apenas do dono da conta.

2. *Algo que você tem*

Quando se vincula a autenticação à alguma coisa **que esteja sob a posse exclusiva do usuário,** temos a aplicação desta categoria. Temos diversos exemplo, entre eles, a utilização de um token, crachá, smart card.

3. *Algo que você é*

Temos aqui, em regra, o mecanismo mais robusto na garantia do princípio da autenticidade. Aqui, **uma característica específica e exclusiva dos usuários é utilizada como parâmetro.** Os exemplos clássicos que se aplicam aqui é a utilização da biometria.

Um detalhe importante a se mencionar é que a **biometria não se restringe à impressão digital.** Pode-se utilizar a informação da Íris, padrão de voz, imagem da face, entre outros.

Avançando a nossa discussão, temos ainda que o serviço de autenticação traz agregado consigo outras funções e recursos muito importantes, **como a autorização e a auditabilidade.** O primeiro corresponde ao fato de que determinado usuário ou serviço dependerá da devida validação de suas credenciais para verificar se este pode ou não acessar determinado recurso. Ou seja, agora, não basta simplesmente ser um usuário válido no sentido de autenticação, mas deve-se ter autorização para tal recurso.

Como exemplo, podemos citar o fato de se ter permissão para ler informações de um diretório, porém, não há permissão para modificar ou criar informações em um diretório.

Conforme mencionamos, temos ainda o aspecto da auditabilidade que permite o registro das ações dos usuários de tal forma que permita o rastreamento para identificação de falhas ou atos indevidos com seus respectivos responsáveis.

> O conjunto dessas três características conceitua o termo **AAA (authentication, authorization e accounting).**

É pacífica a ideia de que a segurança não é 100% confiável. Entretanto, utilizam-se meios diversos para tentar se aproximar desse percentual, ou seja, de dificultar o processo de quebra. No aspecto da autenticação não é diferente.

Nesse sentido surge o **conceito de autenticação forte ou de dois fatores (duas etapas) ou ainda, duplo faltor de autenticação (2FA).** Como o próprio nome sugere, nada mais é do que

dividir a fase de autenticação em duas etapas. Destaca-se que esse processo deve, necessariamente, **envolver a combinação de ALGO QUE VOCÊ SABE, ALGO QUE VOCÊ TEM ou ALGO QUE VOCÊ É.**

Muito cuidado com essa combinação.

Um exemplo que temos é: na primeira etapa, em regra, tem-se a inserção das informações de usuário e senha. Em seguida, utilizando-se de algum outro meio (sms, email, aplicativo de celular), o usuário receberá uma outra senha aleatória ou código que deverá ser inserido na aplicação inicial para acessar o recurso, sendo esta a segunda etapa.

Percebam que esse código funciona como se fosse uma chave de sessão, ou seja, servirá para aquele acesso durante um período específico. Se você tentar, em um segundo momento, acessar de novo a sua conta, um novo código será gerado. **Esse exemplo contemplou os fatores de ALGO QUE VOCÊ SABE com ALGO QUE VOCÊ TEM.**

Algumas aplicações que utilizam esse recurso: BB CODE do banco do Brasil; Steam Guard para Games; Gmail quando se habilita a funcionalidade. Basicamente as principais aplicações WEB suportam esse recurso.

Reparem que nesse caso, assumindo que sua senha seja violada, o invasor não conseguirá acessar sua conta uma vez que dependerá do código aleatório que será enviado na segunda etapa de autenticação.

Por fim, merece destacar também a **existência do MULTIFATOR de autenticação, ou MFA, que segue o mesmo princípio, e pode ter 2 ou mais fatores.**

CESPE / CEBRASPE - 2022 - TCE-SC - Auditor Fiscal de Controle Externo - Ciência da Computação

No controle de acesso, somente os usuários que tenham sido especificamente autorizados podem usar e receber acesso às redes e aos seus serviços.

Comentários:

Exatamente pessoal. Importante sempre lembrar essa diferença básica da autenticação e autorização.

Gabarito: C

Ano: 2021 Banca: CESPE / CEBRASPE Órgão: SEFAZ-CE

Códigos de verificação de um sistema de autenticação de dois fatores podem ser enviados por email ou gerados por um aplicativo autenticador instalado no dispositivo móvel do usuário.

Comentários:

Exatamente pessoal. Típica questão conceito. Veremos mais a frente algumas questões mais práticas sobre o funcionamento desses apicativos? Mas tenho certeza que muitos de vocês já usaram, como o Google Authenticator, por exemplo, ou algum serviço semelhante, onde são geradas senhas para cada usuário. Agora importante destacar que aqui nós temos o modelo de algo que você sabe, com algo que você possui.

Gabarito: C

Ano: 2021 Banca: CESPE / CEBRASPE Órgão: PG-DF

Para acessar a intranet corporativa, um colaborador informa seu CPF, senha pessoal e um código enviado para o seu celular cadastrado.

O mecanismo de reforço implementado nessa intranet para confirmar a identidade do usuário contra acessos indevidos é a autenticação:

A biométrica;

B Kerberos;

C Oauth2;

D 2FA;

E Openid.

Comentários:

Conforme nós vimos pessoal, há a necessidade de conhecimento de algo que VOCÊ SABE (CPF + senha), com ALGO QUE VOCÊ POSSUI (celular). Logo, temos aí o 2FA.

Gabarito: D

Um outro tópico que surge ainda no mundo da autenticação é o **conceito de Single Sign On (SSO).** A ideia básica e simplista aqui é possibilitar a determinado usuário consumir recursos de diversos sistemas e serviços a partir de uma única camada de autenticação.

Ou seja, no seu serviço por exemplo, uma vez que você chegou e acessou a sua máquina com login e senha, a partir de então, você será capaz acessar os recursos de ponto eletrônico, email, serviço de diretórios, outros sistemas internos, sem ser necessário digitar novamente o login e a senha. Importante destacar que é um serviço que permite a integração de sistemas independentes.

O principal protocolo que roda por trás desse recurso é o LDAP, no âmbito corporativo. Uma implementação mais simples é por intermédio dos cookies dos browsers dos dispositivos. O conceito de Single Sign OFF também se aplica no sentido inverso.

Ano: 2020 Banca: CESPE / CEBRASPE Órgão: SEFAZ-AL

Identificação e autenticação são requisitos de segurança da informação que consistem em identificar usuários do sistema e verificar as suas identidades, como pré-requisito para permitir o acesso desses usuários ao sistema.

Comentários:

A dinâmica é sempre essa pessoal. A autentação é o ato final de reconhecimento do usuário ou sistema. Fato é que, para autenticar, devemos identificar. E esse processo pode acontecer de diferentes formas. Ainda, após o processo de identificação e autenticação, temos a autorização, recebendo esses dois como pré-requisitos.

Gabarito: C

SAML - Security Assertion Markup Language

Avançando um pouco mais na nossa conversa a respeito de processos de identificação e acesso, é importante falarmos sobre o **SAML.** Esse assunto tem sido cobrado cada vez mais em provas, trazendo um contexto de aplicação para ambientes corporativo com alta e média e complexidade.

Importante destacar que o SAML não é uma tecnologia em si, mas sim, **um padrão aberto que permite com que provedores de serviços e recursos de identidade passe credenciais de autorização para provedores de serviços**. Vejam que na sua própria definição, há instância e regimes de competências a serem observados. Então se aplica aqui o contexto de simplicidade de implementação quando falamos de logins centralizados e unificados.

A título de referência sobre esse serviço e o Single-Sign-On, temos a própria camada de login único criado pelo Governo Federal, conhecido como **Acesso.gov**, da plataforma Gov.br. Basicamente, a partir deste serviço, busca-se eliminar a múltiplas instâncias de identidade de diferentes órgãos e serviços, passando a responsabilidade pelo processo de gestão de identidade de forma

centralizada, e, a partir daí, uma vez que o usuário é reconhecido, **cabe a cada serviço ou dono do produto (no caso os ministérios), definirem se o mesmo possui ou não acesso para tal.**

Importante destacar ainda que tal gestão de identidade pode alcançar diferentes níveis de abordagem. Podemos ter, a partir dessa estrutura centralizada, usuários com processos de validação e credenciamento que foram mais criteriosos ou não, e isso determinar o nível de acesso a soluções. Novamente, vou trazer um contexto muito prático do nosso dia a dia, no mesmo regime de serviços do Governo Federal.

Atualmente, os serviços do Acesso.Gov, que atua com instância de login único, se utiliza de processos variados de reconhecimento de credenciais dos usuários para compor sua base. Nesse aspecto, há **três formas básicas** (espécie de categoria). **São elas a bronze, prata e ouro.** Tal definição reside basicamente do nível de confiabilidade que foi gerado no cadastramento e reconhecimento do usuário.

O **nível bronze** contempla usuários que **cadastraram seu e-mail, responderam algumas perguntas básicas** derivadas de uma inteligência de cruzamento de bases do Governo Federal, **tendo gerado login e senha.** Exemplo, no ato do cadastro, são perguntas de registro do último emprego, data de nascimento, nome da mãe, e outras informações que o Governo Federal possui para reconhecer um cidadão. Caso **todas essas perguntas sejam respondidas durante o processo de validação, tem-se um cadastro nível bronze.**

Percebam que há um modelo federado no fornecimento de informações e bases para a gestão de identidades. Seguindo esse raciocínio, tem-se ainda o **nível prata**, que basicamente **utiliza o conceito de reconhecimento do usuário por meio da comprovação de documentos, sejam físicos ou digitais.** Assim, caso haja esse reconhecimento em alguma medida, o usuário terá sua credencial nível prata.

Por fim, o **nível Ouro**, que envolve **reconhecimento biométrico**. Basicamente, o principal provedor dessa informação atualmente é o Tribunal Superior Eleitoral, que disponibiliza sua base biométrica para todo o Governo Federal.

Dessa forma, a partir dessa base centralizada de gestão de acesso e credenciais, os demais serviços do Governo Federal podem realizar seus critérios para definição do nível desejado para determinado tipo de serviço. A **sensibilidade** fica por conta do órgão, ao considerar o tipo de transação que pode ser feita. A título de exemplo, caso seja um serviço de consulta a informações de cunho social ou ainda o *status* de alguma requisição, pode-se aceitar o nível bronze.

Agora, caso seja um serviço por exemplo, de declaração de Imposto de Renda, com alta sensibilidade e criticidade, exige-se o nível Ouro, e por aí vai. Ficou claro pessoal a lógica da gestão de identidades?

Nesse contexto, as definições e padrões são fundamentais nesse processo. E aí onde o **SAML** exerce um papel fundamental. Suas **transações** geralmente usam **XML**. Assim, por meio do SMAL, é possível prover serviços como SaaS, com um ambiente gerenciável e seguro, integrando e ativando recursos diversos de SSO, com logins únicos e sessões compartilhadas, a partir de sua reutilização.

O SAML trabalha **transmitindo informações sobre usuários, logins e atributos** entre o provedor de identidade e os provedores de serviços. Cada usuário efetua **login uma única vez** com o provedor de identificação e, em seguida, o provedor de identificação pode passar os atributos de SAML para o provedor de serviços, que solicita a autorização e a autenticação. Como ambos os sistemas falam a mesma linguagem – SAML -, o usuário só precisa efetuar login uma vez.

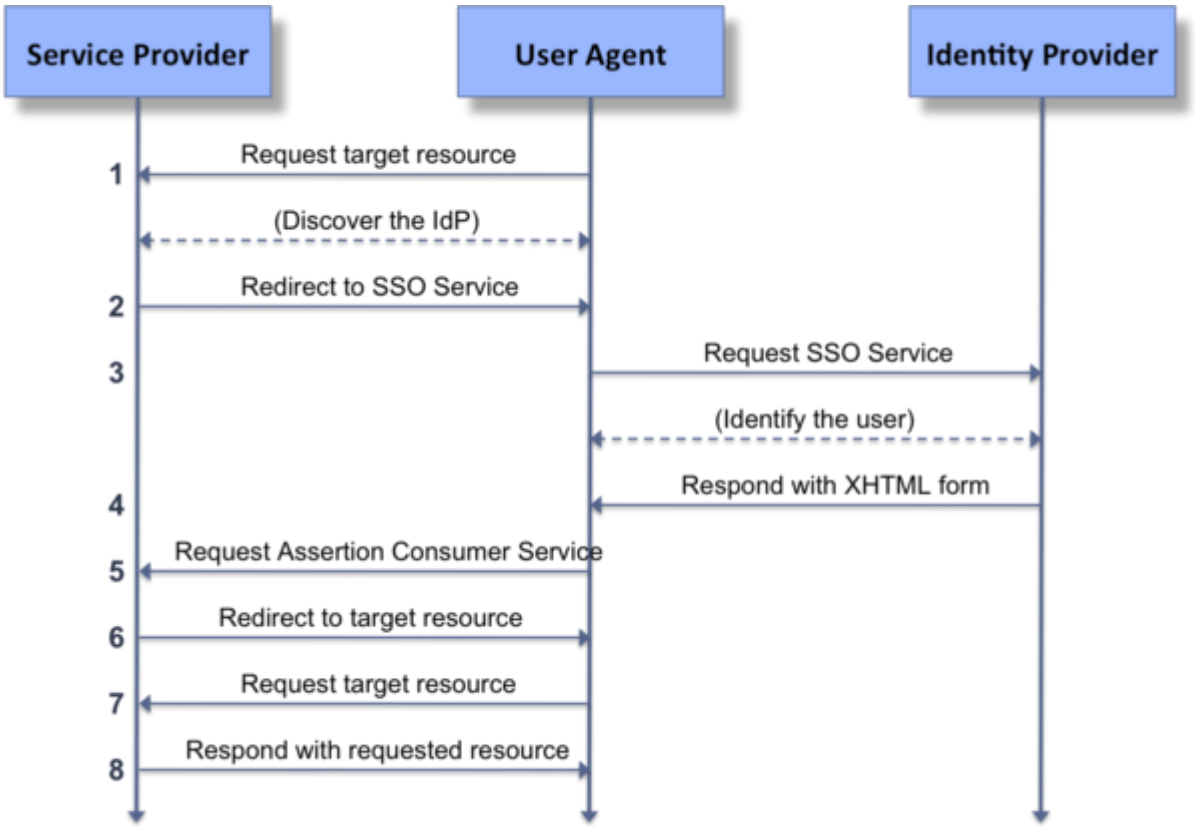
O **SAML** está na versão 2.0, e, em suas especificações, define basicamente 3 papéis:

1. **O principal (tipicamente um humano);**
2. **O Provedor de Identidades (Identity Provider - IDP)**
3. **O Provedor de Serviços (Service Provider - SP)**

Em uma rotina básica de fluxo, tem-se que o Principal, portanto, **acessa ou solicita os recursos ao Provedor de Serviços.** Este então, precisa reconhecer o usuário a partir de sua autorização. Tal processo é feito com uma chamada do Provedor de Serviços ao Provedor de Identidades. Este último, solicita então ao Principal, que insira suas informações de Login e Senha, no mínimo, para ser reconhecido, e liberar acesso aos recursos.

Importante destacar que **o SAML não especifica ou define um método específico de autenticação no âmbito do Provedor de Identidade**. Pode usar o modelo de Login e Senha mencionado anteriormente, ou qualquer outro modo de autenticação, inclusive, incorporando as técnicas de múltiplo fator de autenticação (MFA). Então, para cada serviço que se deseje utilizar, todo o processo do MFA deve ser realizado, ou, no mínimo, a confirmação da segunda camada de segurança. Ainda, a título de exemplo, pode-se utilizar serviços como RADIUS, LDAP ou ainda Active Directory da Microsoft. Nesse aspecto, já começamos a introduzir também a capacidade de autenticação por meio de serviços de terceiros, como Google, Facebook, Twitter, o qual detalharemos a seguir no padrão OAuth.

A imagem a seguir representa em fluxo, de forma simplificada, esse processo:



FGV - 2022 - Senado Federal - Analista Legislativo - Análise de Sistemas

O padrão SAML V2 define 3 tipos de declarações que podem ser transmitidas em uma afirmação.

As declarações de autenticação

A definem algo que o sujeito é autorizado a fazer.

B descrevem, no mínimo, o método usado para autenticar e quando a autenticação ocorreu.

C precisam ser codificadas utilizando o algoritmo XTEA antes do envio.

D são criadas pelo cliente que solicitou a autenticação.

E precisam ser transmitidas no formato JSON.

Comentários:

Vamos às questões:

A) **Incorreta**. As declarações de autenticação não definem algo que o sujeito é autorizado a fazer, mas sim, informações sobre a autenticação do sujeito.

B) **Correta**. As declarações de autenticação descrevem, no mínimo, o método usado para autenticar o sujeito e quando a autenticação ocorreu. Elas fornecem informações sobre como e quando o sujeito foi autenticado.

C) **Incorreta**. O padrão SAML V2 não exige que as declarações sejam codificadas utilizando o algoritmo XTEA. As declarações são normalmente codificadas em XML.

D) **Incorreta**. As declarações de autenticação são criadas pelo provedor de identidade (IdP), não pelo cliente que solicitou a autenticação.

E) **Incorreta**. O padrão SAML V2 usa o formato XML, e não JSON, para transmitir informações de autenticação e autorização.

Gabarito: C

OAuth

Antes de darmos seguimento ao tópico de OAuth especificamente, é importante entendermos que há diversas formas de autenticação nos métodos de chamada do HTTP, sendo o OAuth, um desses mecanismos.

A estrutura geral de autenticação HTTP é usado por vários esquemas de autenticação. Basicamente, a depender da necessidade de segurança, nível e complexidade, bem como do suporte das tecnologias e recursos entre as partes.

O esquema mais comum de autenticação é o "Basic". Vamos conhecê-los, bem como os demais:

- **Autenticação Básica (Basic Authentication):** É um dos esquemas de autenticação mais simples e amplamente utilizado. A autenticação básica exige que o usuário forneça um nome de usuário e uma senha, que são então codificados em Base64 e enviados no cabeçalho "Authorization" da requisição HTTP. No entanto, a autenticação básica não é segura, pois a codificação em Base64 pode ser facilmente revertida, expondo as credenciais em texto claro. Por isso, é recomendável usar a autenticação básica em conjunto com uma conexão segura, como HTTPS.

- **Autenticação Digest:** É uma melhoria em relação à autenticação básica, oferecendo maior segurança. A autenticação digest utiliza um método criptográfico de hash (como MD5) para gerar um "resumo" (digest) das credenciais do usuário, que é enviado no cabeçalho "Authorization" da requisição HTTP. Isso evita o envio de credenciais em texto claro, tornando mais difícil para um atacante interceptá-las. No entanto, a autenticação digest ainda é vulnerável a ataques de repetição e não é considerada tão segura quanto outras opções.

- **Autenticação por Token (Token-based Authentication):** Este esquema de autenticação utiliza tokens, como JSON Web Tokens (JWT), para autenticar usuários. Em vez de enviar credenciais em todas as requisições, o usuário fornece suas credenciais uma vez para obter um token de acesso. Esse token é então enviado no cabeçalho "Authorization" da requisição HTTP em chamadas subsequentes. A autenticação por token é mais segura do que a autenticação básica e digest, pois os

tokens podem ser assinados e criptografados, garantindo a integridade e confidencialidade das informações.

- **Autenticação OAuth ou Bearer:** Veremos a seguir, mas já adianto. OAuth é um protocolo de autorização amplamente utilizado que também pode ser usado para autenticação. Ele permite que aplicativos de terceiros acessem recursos protegidos em nome do usuário sem a necessidade de compartilhar suas credenciais diretamente. O OAuth usa tokens de acesso temporários, também conhecidos como bearer tokens, que são obtidos através de um fluxo de autorização específico. OAuth 2.0 é a versão mais recente e é amplamente adotada devido à sua flexibilidade e segurança.

Cada esquema de autenticação HTTP tem suas vantagens e desvantagens, e a escolha do esquema mais adequado depende dos requisitos de segurança e das funcionalidades da aplicação.

FGV - 2022 - MPE-SC - Analista em Tecnologia da Informação

O analista em TI Tomé implantou a aplicação MPWebApp no servidor web HServer. Para controlar o acesso à MPWebApp, Tomé habilitou em HServer um esquema de autenticação do HTTP (Hypertext Transfer Protocol). O esquema habilitado por Tomé exige que o cliente envie o usuário e a senha de acesso codificados em Base64 diretamente no cabeçalho Authorization da mensagem de requisição.

Logo, Tomé habilitou em HServer o esquema de autenticação HTTP:

A Digest;

B Bearer Token;

C Hawk;

D OAuth 1.0;

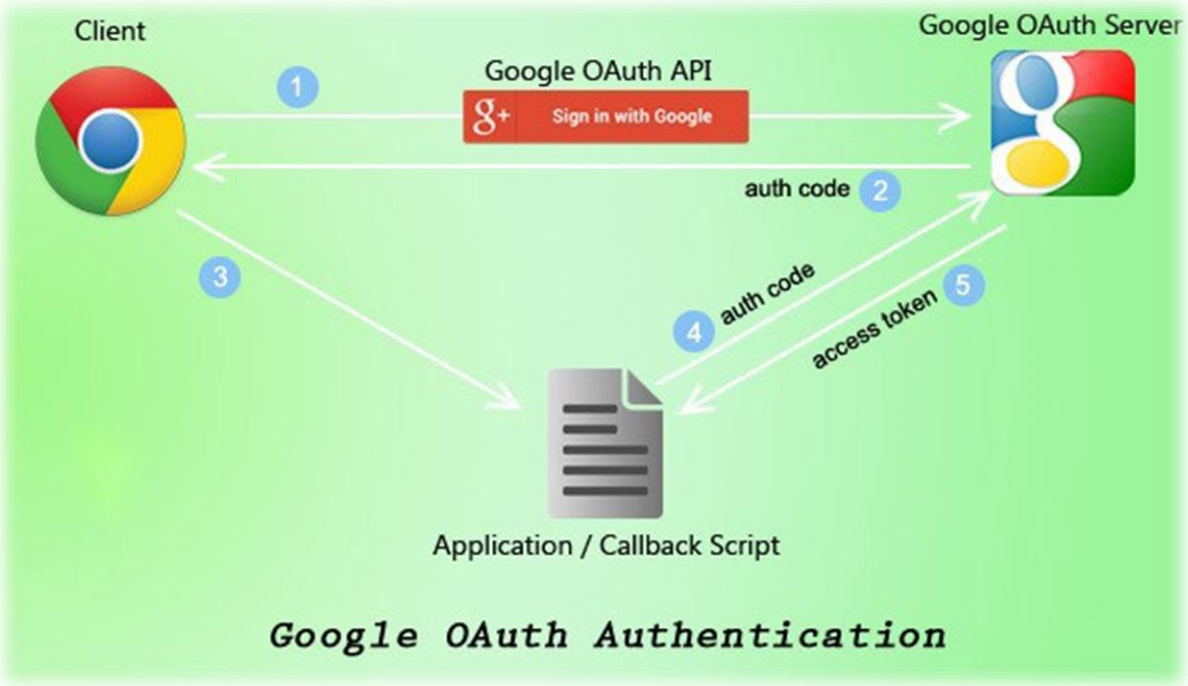
E Basic.

Comentários:

Conforme acabamos de ver na nossa teoria, certo pessoal? O Basic é o tradicional, e aquele que se ancora na codificação Base64.

Gabarito: E

Seguindo a nossa estrutura de gestão de identidade e credenciais, temos agora o Oauth. Tal padrão foi concebido no nicho privado, em conjunto pela Google e pelo Twitter, permitindo assim **logins simplificados e integrados a múltiplos serviços na Internet**. O processo por trás é muito semelhante ao SAML que mencionamos.



A figura acima ilustra um processo base de quando efetuamos logins por meio do **OAuth** da Google. Creio que muito estão familiarizados com a imagem vermelha do centro, certo? Basicamente, estamos autorizando a aplicação ou serviço que estamos consumindo a realizar troca de informações com os servidores e provedores de credenciais da Google para reconhecimento da nossa identidade. A partir da chamada do serviço, no passo 2, **a aplicação recebe o código de autenticação gerado pelo servidor** Oauth do Google e por meio de processos em background e serviços próprios, realiza o processo de checagem para liberação de acesso com o recebimento de um token.

Nosso intuito não é entrar no detalhe de implementação do OAuth, por ser um aspecto de cobrança mais associado a itens de desenvolvimento ao considerar bibliotecas JWT e outros. Aqui, estamos focando nos conceitos das soluções e ferramentas, além de processos que garantem a gestão de identidade e credenciais.

O OAuth atualmente está em sua versão 2.0 e possui compatibilidade completa com sua versão 1.0. Nesse processo, são definidos 4 papéis básicos. São eles:

1. Resource Owner - Basicamente é a pessoa que concede acesso aos seus dados. Quando clicamos na opção de login integrado com o Google, por exemplo, teremos que incluir nosso login e senha do google, a partir da chamada de serviço. Caso você tenha uma sessão já aberta do serviço, essa etapa não será necessária. O ponto é, após a inclusão das informações de login e senha, tem-se um processo de autorização, em que você autoriza a aplicação ou serviço, a obter suas informações do servidor OAuth. **Na prática, temos aqui o DONO DO RECURSO.**

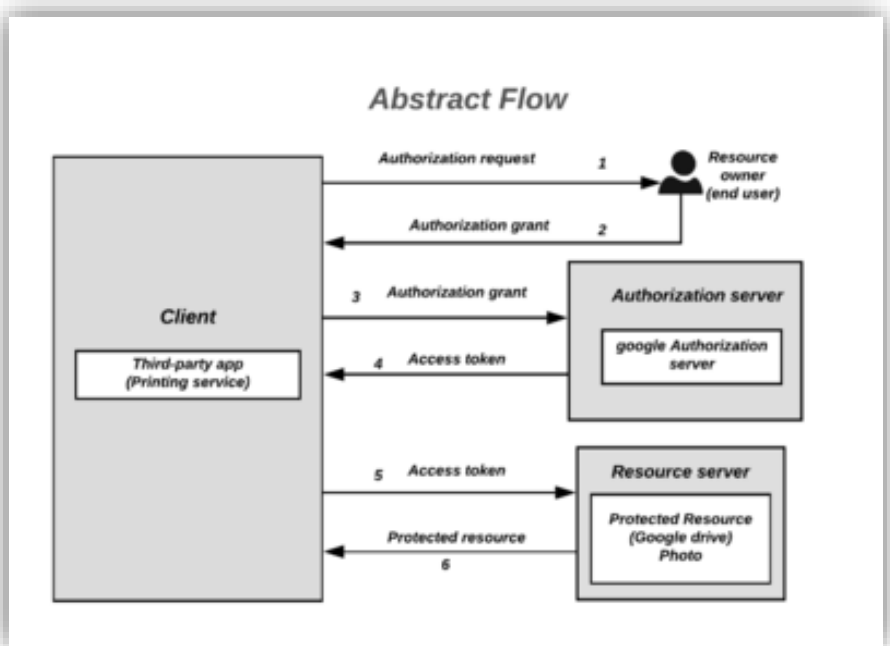
2. Resource Server - Em resumo, é a camada de serviço/integração disponibilizada pelo provedor de identidades. Este serviço, com as devidas camadas de segurança, está exposto para a Internet, caso seja uma API Pública, a exemplo da Google, Twitter, Facebook, ou pode estar em um contexto

mais restrito, como foi o caso do serviço do Acesso.Gov que mencionamos, que pode ser utilizado apenas por órgãos de Governo. O que importa é que, nesse processo, é necessário que o serviço que realiza chamada a essa API tenha um token emitido pelo servidor de autorização, que mencionaremos a seguir.

3. Authorization Server - Responsável por autenticação e emissão dos tokens de acesso (Access Token) para os *Clients* (aplicação requisitante). **Estes recursos possuem informações dos Resource Owner (Usuários) e** expõe no formato de *Claims* através do *Bearer Token.* Autentica e interage com o usuário após identificar e autorizar o client. Não vamos entrar em detalhes técnicos de implementação, mas registro apenas que o *Bearer Token* é referenciado em chamadas nos cabeçalhos HTTP e pode ser implementado de diferentes formas. No caso, tais chamadas são sempre realizados por meio de HTTPS, uma vez que o token é passado de forma aberta no cabeçalho HTTP. Esse ponto é fundamental para garantir a segurança do Oauth2.0.

4. Client - É a aplicação que interage com o **Resource Owner**. No caso de uma App Web, seria a aplicação do Browser. Na prática, é a camada que oferece os serviços requisitados pelos usuários.

A imagem a seguir representa bem a execução desses papeis e respectivos fluxos, vejamos:



FGV - 2022 - TRT - 13ª Região (PB) - Analista Judiciário - Tecnologia da Informação

O protocolo de autorização OAuth 2.0 permite que aplicativos obtenham acesso limitado aos serviços HTTP.

As quatro funções (roles) descritas na RFC 6749 para esse protocolo são

A protected resource, resource user, client e token server.

B access token, HTTP server, client credential e authorization broker.

C resource owner, resource server, client e authorization server.

D authorization resource, authorization code, client e token server.

E resource owner, password credential, access token e refresh token.

Comentários:

Trazendo exatamente todos os papeis que acabamos de ver na estrutura básica do OAUTH.

Gabarito: C

A partir do momento, portanto, que um usuário acessa um *site* e solicita o acesso ou tenta realizar o login, inicia-se o processo

ETAPA 1 - A aplicação (*cliente)* solicita autorização para o usuário, para que a aplicação possa interagir e solicitar informações de suas credenciais junto ao provedor de identidade.

ETAPA 2 - O Dono do Recurso (*resource owner)* realiza a autorização.

ETAPA 3 - De posse da autorização, esta é encaminhada pelo *cliente* ao Servidor de Autorização, responsável por viabilizar a passagem das credenciais de acesso aos serviços do provedor.

ETAPA 4 - O provedor de credenciais passa o TOKEN, por meio de uma comunicação segura. De posse desse token, a aplicação poderá acessar os recursos do usuário requisitante. Aqui é onde temos a referência ao nosso *BEARER TOKEN,* que também será utilizado na etapa 5. São as credenciais em si usadas para acessar os recursos protegidos.

ETAPA 5 - Passa-se o token aos provedores de serviços que detêm os recursos protegidos dos usuários. Na imagem em questão, temos exemplo de serviços da google como o Google Drive ou Google Photo, que passa a ser acessado pelo *Client* com a devida autorização do usuário Dono do Recurso, realizado no passo 2.

ETAPA 6 - As informações e recursos protegidos são compartilhados com o *Cliente.* É nessa etapa que é possível, por exemplo, já ter a sua foto integrada com o serviço web requisitado, outras informações, como e-mail, dados de telefone, recursos específicos no Drive, lista de amigos e contatos, entre muitos outros.

Cebraspe – Analista Judiciário – Tecnologia da Informação (TRT-AP/PA)/2022

No protocolo OAuth2, a concessão de autorização que é obtida por meio de um servidor intermediário entre o cliente e o proprietário do recurso é do tipo

a) access token.

b) authorization code.

c) resource owner password credentials.

d) client credentials.

e) implicit.

Comentários:

Questão bem sutil pessoal. Muito cuidado. Vejam que ele foca na geração da autorização por parte, que é a etapa inicial do processo. Ele ainda não está falando da etapa de geração do token para acesso ao recurso. Nessa etapa 1 e 2, de geração da autorização, na prática, tem-se um código de autorização, chamado de authorization code.

Gabarito: B

OPENID Connect

Aqui temos um conceito associado à criação da camada que atua sobre as soluções de gestão de identidade (OAUTH).

Ela permite aos clientes/aplicações a verificação da identidade do usuário final integrado aos recursos do Servidor de Autorização.

Utiliza a interoperabilidade por meio de API/RESTFULL e tem como característica o fato de ser Multiplataforma.

KeyCloak

Na mesma linha, temos aqui uma ferramenta muito importante e de código aberto (opensource) de Gerenciamento de Acesso e Identidade.

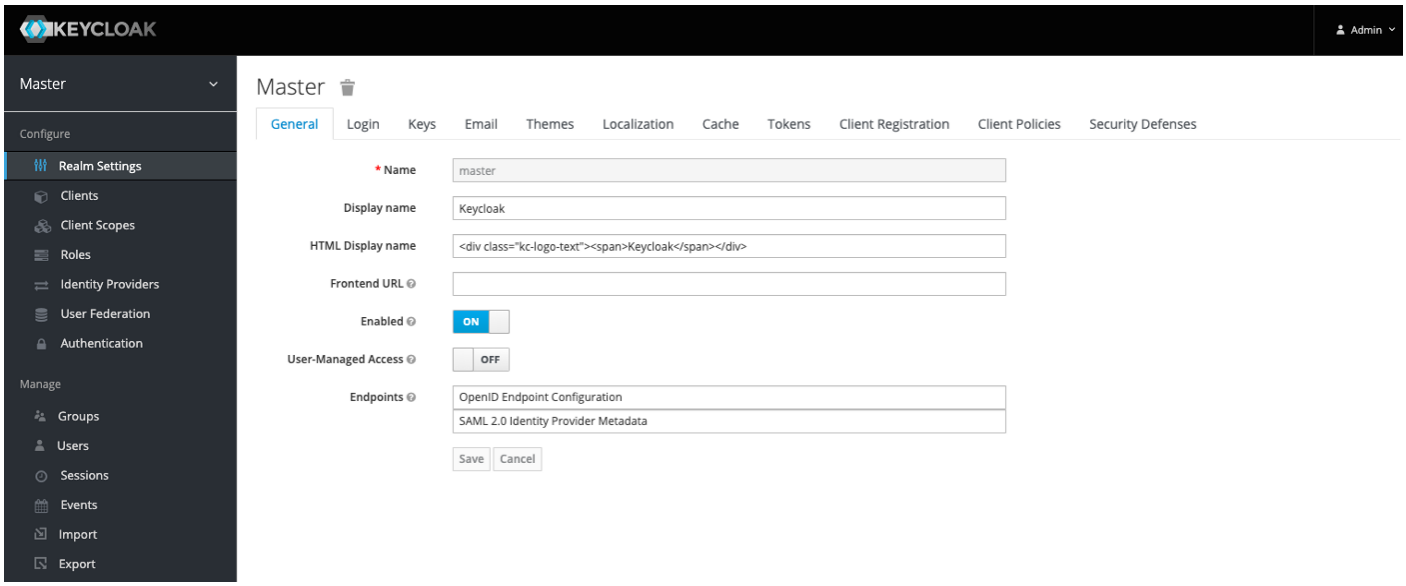
Sendo muito fácil de configurar e implantar a gestão de identidade, o KeyCloak vem sendo usado cada vez mais pelas instituições.

A ferramenta, assim como o OPENID Connect é baseada em API-Restfull, tendo as seguintes características:

- Fornece telas de login personalizáveis
- Recursos de Recuperação de Senhas
- Termos de uso
- Ausência de necessidade de codificação
- Recurso de MFA
- Isolamento da aplicação com a camada de autenticação
- Visualização dos tokens do KeyCloak
- Recursos de SSO

- Utiliza OAUTH2.0 + OpenID
- Possui banco de dados próprio
- Pode integrar com AD ou LDAP

A seguir, temos uma tela exemplo da ferramenta e seu painel de gerenciamento e configuração:



FGV - 2022 - TRT - 13ª Região (PB) - Técnico Judiciário - Tecnologia da Informação

Marcia decidiu padronizar o mecanismo de autenticação de suas APIs RESTful e armazenar com segurança as credenciais de usuários e suas respectivas permissões. Para isso, ela deseja utilizar uma ferramenta de código aberto.

A ferramenta que tem por principal finalidade o gerenciamento de identidade e acesso que Marcia deve escolher é

A JBoss.

B Keycloak.

C Kibana.

D RabbitMQ.

E Wildfly.

Comentários:

Temos aí pessoal uma questão que traz a forma de abordagem da solução KeyCloak. Apenas apra validarmos as outras tecnologias/ferramentas:

JBoss - Um servidor de aplicação Java EE de código aberto, desenvolvido pela Red Hat. Oferece uma plataforma para construir, implementar e executar aplicações empresariais. Suporte a diversas tecnologias, como EJB, CDI, JPA e JSF.

Kibana: Uma ferramenta de visualização de dados e interface de usuário do Elastic Stack. Permite explorar, analisar e visualizar dados armazenados no Elasticsearch. Utilizada para monitoramento, análise de logs e business intelligence.

RabbitMQ: Um message broker de código aberto que implementa o protocolo Advanced Message Queuing Protocol (AMQP). Facilita a comunicação entre aplicações através de mensagens assíncronas. Oferece alta disponibilidade e escalabilidade.

Wildfly: Anteriormente conhecido como JBoss AS, é um servidor de aplicação Java EE de código aberto. Desenvolvido pela Red Hat, permite a criação e implantação de aplicações empresariais. Suporta diversas tecnologias, como EJB, CDI, JPA e JSF.

Gabarito: B

Biometria

Algumas questões tratam os aspectos de **BIOMETRIA** de uma maneira mais detalhada. Por esse motivo, reservaremos essa seção para isso

Para balizarmos o nosso princípio, ao analisarmos a etimologia da palavra temos: **BIO (VIDA) + METRIA (MEDIDA).** Podemos traduzir isso também como a forma de identificar de maneira única um indivíduo por meio de suas características físicas ou comportamentais.

Trazendo um pouco mais de história em nosso estudo, importante citar a importância de FRANCIS DALTON, considerado um dos fundadores do processo de biometria. Seu estudo era baseado na identificação de características e traços genéticos. **Em 1982, GALTON inventou o primeiro sistema moderno de IMPRESSÕES DIGITAIS**, e que fora amplamente utilizado nos departamentos de polícia.

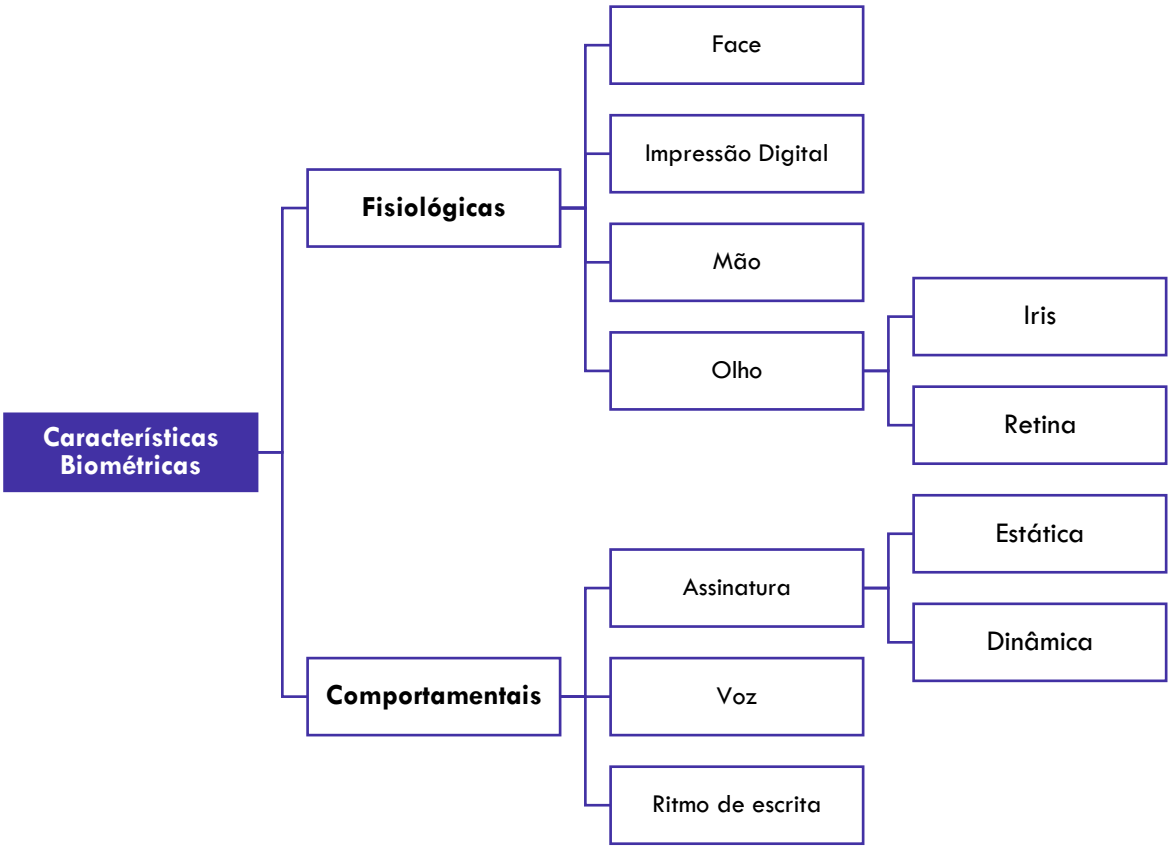
Como vimos anteriormente, o processo de biometria está atrelado à fase de autenticação e autorização, principalmente, para fins de controle de acesso.

Desse modo, quando falamos de **ALGO QUE VOCÊ É,** podemos utilizar alguns recursos para tal finalidade, como por exemplo:

1. **Impressão Digital;**
2. **Palma da mão;**
3. **Imagem da Face;**
4. **Retina ou íris dos olhos (*a retina analisa o fundo do olho, enquanto a retina analisa os anéis coloridos do olho, sendo este mais rápido que aquele);***
5. **Reconhecimento de voz;**

Desse modo, os filmes futuristas, bem como aqueles que retratam assaltos a cofres muito seguros necessariamente passam pelo processo de biometria.

A imagem abaixo nos traz uma visão agregada das principais técnicas de biometria:



Fonte: http://www.sinfic.pt

Nesse sentido, a biométrica zela pelos princípios de unicidade abaixo:

1. **Universalidade** – Significa que todas as pessoas devem possuir a característica;
2. **Singularidade** – Indica que esta característica não pode ser igual em pessoas diferentes;
3. **Permanência** – Significa que a característica não deve variar com o tempo;
4. **Mensurabilidade** – Indica que a característica pode ser medida quantitativamente;

Analisando a estrutura de um sistema biométrico, podemos elencar ainda as etapas desses sistemas:

1. **Captura** – Aquisição da amostra biométrica;
2. **Extração** – Remoção da amostra com informações únicas para posterior análise;
3. **Comparação** – Comparação com as informações armazenadas em uma base de dados. Caso a comparação seja positiva, tem-se um *"match",* dando o resultado como positivo.

Ano: 2021 Banca: CESPE / CEBRASPE Órgão: SEFAZ-AL

O uso de senhas ou a adoção de identificação física, como biometrias, são formas de autenticação para fins de identificação única e exclusiva de usuários.

Comentários:

Pessoal, a questão retrata, de fato, as finalidades de senhas associadas a biometrias. A exclusividade, como vimos é um princípio da biometria. No trecho, vimos o termo SINGULARIDADE.

Gabarito: C

Ano: 2021 Banca: CESPE / CEBRASPE Órgão: PG-DF

Uma das condições para a autenticação é que o sinal biométrico apresente correspondência exata entre o sinal biométrico recebido pelo sistema e o gabarito armazenado.

Comentários:

Pessoal, vimos que existem os modelos comportamentais, certo? Esses modelos, também são sinais biométricos e trabalham com referências variáveis, mas dentro de um padrão aceitável, com taxa de similaridade e equivalência alto. Agora, dizer que o gabarito tem que ser exato, não é uma verdade para sua generalização.

Gabarito: E

(CESPE – TJ-SE/Analista Judiciário – Segurança da Informação/2014)

Os métodos de autenticação comumente empregados fundamentam-se na clássica divisão entre o que você sabe (senha ou número PIN); o que você tem (token ou um smart card); e o que você é (íris, retina e digitais).

Comentários:

Conforme vimos, de fato, estes são os três principais métodos.

Gabarito: C

SEGURANÇA EM ENDPOINTS

Primeira coisa para validarmos e lembrarmos para esse capítulo é o conceito de ENDPOINT. Basicamente, quando falamos de **ENDPOINTS,** referenciamos os equipamentos finais que ficam

nas mãos dos usuários finais (computadores, laptops, smartphones, entre outros). A segurança desses equipamentos busca evitar ataques cibernéticos, detectar atividades maliciosas e fornecer recursos de correção instantânea, entre outros.

Importante destacar que estamos na era da Internet das Coisas, diretamente associada ao conceito de **BYOD (bring your own device)**, além de toda dinâmica associada ao trabalho remoto potencializado pela pandemia. Com esses conceitos modernos e dinâmica de utilização dos equipamentos, fica evidente a necessidade de aprimoramento dos aspectos voltados para segurança destes dispositivos.

Um outro ponto que merece destaque a respeito da dinâmica de uso dos dados e serviços corporativos está **associado ao princípio de desoneração de recursos locais nas máquinas e dispositivos**, com a potencialização do uso de recursos em nuvem, até mesmo explorando conceitos de Desktops Virtuais Corporativos.

A título de referência, podemos extrair de um dos grandes fornecedores de soluções de segurança a nível mundial, a Mcafee, que extrapola ainda mais o conceito de **Endpoints:**

Na prática, **se o dispositivo está conectado à rede em alguma medida, com a capacidade de processar informação e trafegar dados,** poderá ser classificado como um ENDPOINT.
Basicamente, ao longo das diversas disciplinas do Curso de Segurança, diversas ações que contribuem para esse processo são tratadas e detalhadas. Entretanto, reforçaremos alguns conceitos. Destaco também que muitos destes são tratados em diretrizes e ações como a **ISO**

27002 e **Medidas de Controle de Segurança diversos**, definidos em **Frameworks de referência como o CIS CONTROLS ou NIST.**

Primeiro ponto a ser observado é o **conceito de camada e plataforma**. É importante que tais defesas contemplem as camadas horizontais (camadas da arquitetura TCP/IP), camadas horizontais (envolvem as etapas de pré-execução, execução e pós-execução de malwares ou ações maliciosas em geral), além de serem multiplataformas como diferentes linguagens de programação de sistemas e softwares, sistemas operacionais, entre outros. Lembrando que no bojo das plataformas, devemos considerar também soluções mobile, que envolvem, por exemplo, iOS e Android.

Dentre alguns recursos e contextos de aplicação das soluções voltadas para segurança em EndPoints, podemos citar **Antivírus, Antimalwares, firewalls, HIDS e HIPS, Atualizações diversas de drivers, softwares e S.O., entre outros**. Vamos reforçar alguns recursos e conceitos para cada um desses aspectos.

1. Uso de Assinaturas e Inteligência Artificial

Sem dúvida, o uso de assinaturas de códigos e programas sempre foram a **linha de base de identificação de quaisquer malwares em equipamentos.** Entretanto, diversas técnicas de ofuscação de código podem ser implementadas, de tal modo que reduzem, sobremaneira, a eficiência dessa técnica de identificação.

Destaca-se que há compartilhamentos de múltiplas bases de assinaturas e identificação desses softwares que não se restringem necessariamente a fabricantes ou provedores de tecnologia especificamente. Esse arranjo ajuda a fortalecer a capacidade de identificação por meio da disseminação de informações. Entretanto, mesmo essas medidas não são suficientes no processo.

Assim, surgem as técnicas de análise de comportamento por meio de inteligência artificial e aprendizado de máquina que traçam linhas de base com base em heurísticas, redes neurais e muitas outras técnicas, para tentar prever determinados *malwares* e outras ações.

Importante destacar que ataques como ***ZERO-DAY***, onde não são conhecidos em nenhuma assinatura, somente poderão ser detectados preventivamente por meio dessas técnicas ou ações manuais. Lembrando que ataques ZERO-DAY **basicamente são aqueles que ainda não foram descobertos pelas comunidades e provedores de soluções de segurança**, ou ainda, pelo donos das soluções e produtos, para que possam implementar as medidas de segurança ou correções necessárias para eliminar a vulnerabilidade.

Nesse ponto, além dos recursos já mencionados na introdução, merece comentar também recursos voltados para atuação no ambiente de pré-inicialização do Sistema Operacional, para monitoramento da integridade do firmware por meio do UEFI (Interface de Firmware Extensível Unificada.

2. Monitoramento de Processos, Serviços e Memória

Um outro recurso interessante que se conecta com o recurso de inteligência é justamente o monitor de eventos e comportamentos, que atua nos processos, serviços e memórias dos equipamentos.

Ataques mais modernos se utilizam da memória para poderem acelerar seu poder de fogo e reduzir a capacidade de detecção, uma vez que não passa por arquivos em disco, não havendo, nesse caso persistência.

Assim, **entender o comportamento da memória é importante no contexto atual para se prevenir e tentar combater esse tipo de ataque.**

3. Monitoramento de Atualizações e Patches de Segurança

Apesar de trivial, mas nem sempre é feito de forma efetiva e de forma automática. Garantir com que os sistemas operacionais, softwares instalados, drivers dos dispositivos, entre outros, possuam as últimas atualizações instaladas é de suma importância.

Os ***Patches*** de atualização geralmente agregam recursos de Segurança e eliminação de vulnerabilidades identificadas.

4.Área segura e virtualizada para execução de arquivos (*sandbox)*

Um outro recurso importante que também é incorporado nas múltiplas ferramentas elencadas acima é o ***SANDBOX***. Tal recurso se trata, basicamente, de uma área virtualizada criada com a capacidade de isolar o processamento de determinado arquivo.

Na prática, cria-se um contexto virtual capaz de emular todos os recursos de uma máquina, para avaliar o comportamento do software. Muitas das vezes, há trechos no código que não são reconhecidos e gera-se dúvidas sobre sua forma de atuação e potenciais resultados derivados. Basicamente tem-se a questão da ofuscação do código ou trecho dele que procederá exatamente com as funcionalidades maliciosas.

Nesse contexto, portanto, dentro de uma *sandbox*, **pode-se executar o código e avaliar o comportamento** e, caso seja, de fato, um software malicioso, o dano será gerado apenas em estruturas virtuais, que podem ser facilmente excluídas posteriormente e não havendo qualquer propagação para as estruturas do Sistema Operacional base.

Tal técnica é a mesma utilizada, por exemplo, quando se deseja navegar em redes não confiáveis, ou ainda, a *deep web.* Nesse caso, não se trata de uma instância simplificada criada pelas ferramentas de antivírus ou antimalware, por exemplo, mas sim, uma ferramenta de virtualização, de fato, de máquinas, como Virtual Box ou Virtual Machine. Assim, a partir das instâncias virtualizadas criadas, pode-se navegar em redes inseguras sem colocar em risco, da mesma forma, o próprio Sistema Operacional.

5.Navegação Segura e e-mails seguros

Já adiantamos o assunto na seção anterior, e é importante reforçar a dinâmica de navegação na WEB por parte desses *endpoints.* Desta feita, **utiliza-se técnicas como proxies e outros recursos a nível da camada de aplicação que são capazes de promover uma navegação segura e controlada,** inclusive, trabalhando com práticas de *blacklists* e *whitelists.*

Ações proativas em torno da navegação são fundamentais nesse processo.

No mesmo contexto, pode-se implementar técnicas e soluções associadas aos clientes de e-mail que eventualmente sejam instalados e utilizados nos *Endpoints*, ou ainda, clientes web que

também sejam acessados. Nesse ponto, **destaca-se a possibilidade de utilização da tecnologia MFA (Multi Factor Authentication).**

6.Gerenciamento Centralizado

Um outro recurso que pode ser utilizado associado à segurança de endpoints é um gerenciamento centralizado. Com isso, é possível incluir tanto equipamentos corporativos como equipamentos particulares que possuem acesso aos recursos corporativos. Desse modo, **a partir do gerenciamento Centralizado, é possível estabelecer *policies* diversas, com categorias e tipos de uso dos equipamentos**, garantindo *baselines* de configuração, com a possibilidade de varreduras e ações remotas de forma automática nesses equipamentos.

Trata-se de um recurso que impõe uma dinâmica, por vezes, invasivas, principalmente quando se fala de inclusão de dispositivos pessoais neste monitoramento. Mas é sempre um *trade off* quando se trata de privacidade e comodidade, para unificar procedimentos e soluções em torno da vida pessoal e necessidades particulares em conjunto com o contexto corporativo.

(FGV/CGU/2022) Roberto é funcionário de um órgão público e está trabalhando em home office devido ao cenário pandêmico. Para que não haja perda de produtividade, Roberto precisa acessar a rede interna do órgão onde trabalha. Para isso, Roberto irá utilizar um computador considerado um endpoint, por se tratar de um dispositivo final que se conecta fisicamente a uma rede interna do órgão. Para que o órgão público em que Roberto trabalha possa confiar em conexões externas com a rede interna, soluções de segurança de endpoints precisam ser implementadas e ter como características:

A redução de custos e facilidade de atualização;

B configuração simplificada e fácil instalação de API;

C monitoramento completo e antivírus atualizado;

D administração descentralizada e facilidade de integração com novas tecnologias;

E bloqueio de ações indesejadas e controle no lado do usuário.

Comentários:

Essa foi uma questão extremamente polêmica, pessoal. É um desafio para os candidatos lidarem com assuntos novos, pois não se tem muito parâmetro de como esse assunto será cobrado. E nesse contexto, foi exatamente o que aconteceu. A Banca utilizou uma referência extremamente frágil na perspectiva de um fabricante sem relevância, e trouxe como gabarito a alternativa A. Agora, há de se destacar que há diversas outras fontes de outros fabricantes, que também trazem as perspectivas das alternativas B e C.

Então focando nos comentários dos itens isolados, temos:

- Redução de custos pois concentra o regime de oferta de soluções, não implicando em custos avulsos e descentralizados para os endpoints.

- Facilidade de Atualização traz a perspectiva de você manter uma base centralizada com as versões e bases de conhecimento para combate a ataques diversos. Então torna-se um processo automático e simples.

Agora os outros itens:

- Configuração simplificada seria um item também viável, pois as soluções de Segurança em Endpoints precisam ser usáveis e simples, permitindo a implantação em qualquer dispositivo.

- Fácil instalação de API, diz respeito ao fato de que múltiplas soluções não são completas em si e abarcam todas as frentes de segurança, cabendo modelos de integração e troca de informações entre soluções distintas

- Monitoramento Completo abarca o contexto e capacidade da ferramenta/solução extrair a visão completa dos fluxos de trabalho e processos dos equipamentos por meio de agendas e troca de informações, resguardando assim os endpoints.

- Antivírus atualizado é o mínimo que se espera de uma solução que busca estabelecer parâmetros mínimos de segurança para seus equipamentos.

Gabarito: A (Gabarito do Professor: Anulação)

AUDITORIA E CONFORMIDADE

Outros assuntos que constantemente caem em prova em termos conceituais e suas aplicações, é a **auditoria** e **conformidade.**

Já mencionamos na aula de hoje alguns instrumentos e mecanismos utilizados para fins de auditoria.

Em um conceito básico, temos que

> A **auditoria** em tecnologia da informação diz respeito à **análise cuidadosa e sistemática dos recursos de TI**, pessoas, documentos, sistemas, entre outros, no intuito de se averiguar se estes estão de acordo com aquilo que fora planejado ou em relação às atividades e comportamentos definidos como padrão. Avalia-se quanto à sua eficácia e eficiência em torno dos objetivos e resultados esperados.

Geralmente, lembramos de auditoria em ações que buscam evidenciar aspectos para fins de apuração de algum tipo de desvio ou comportamento indesejado.

Uma outra definição para a **auditoria de Segurança da Informação,** trazida pelo TCU é:

> Avaliação se a **gestão da segurança da informação, o controle dos ativos e os riscos envolvidos são considerados de forma efetiva pela organização.** A auditoria de SI visa avaliar a gestão da organização com relação à segurança. Aborda aspectos de confidencialidade, integridade e disponibilidade embutidos nos conceitos de segurança lógica e física.

Quando falamos que devemos registrar os acessos dos usuários, por exemplo, tem-se como pano de fundo o fato de que, em um eventual problema de vazamento de dados, novamente, como

exemplo, pode-se avaliar as informações e identificar o responsável por tal ação. Isso está muito atrelado ao conceito do **AAA – Autenticação, Autorização e Auditoria.**

Assim, uma auditoria de TI deve ter um escopo bem definido que contemple a identificação e avaliação de controles que possa afetar a segurança da informação, tanto em um contexto macro, quanto micro (mais aprofundado e técnico) a depender a intenção e necessidade de análise.

Falando um pouco sobre **conformidade,** podemos definir como:

> Conceito relacionado à **adesão dos sistemas de informação às políticas** e às normas organizacionais de segurança da informação.

Conforme veremos mais à frente, há diversas normas e padrões, além de políticas diversas que apresentam as melhores práticas e aspectos para certificações nos mais distintos nichos e contextos da segurança da informação. Assim, quando uma empresa prima pelas boas práticas, ela deve estar aderente, ou seja, em conformidade com os referidos padrões.

Importante destacar que os critérios de conformidade **não se restringem a essas normas e padrões internacionais.** Trazendo a nossa análise para o contexto do próprio Governo, uma vez que estamos falando de concursos públicos, há órgãos diversos do Governo capazes de gerar normas, manuais, políticas, boas práticas e diretrizes a serem seguidas pelos órgãos da administração pública. Sem contar as leis e Decretos que devem ser seguidas.

Assim, espera-se que os órgãos estejam em conformidade com essas questões que mencionamos.

(CESPE - 2014 - TJ-SE - Analista Judiciário - Segurança da Informação) Atividades de usuários, exceções e outros eventos são registros ou logs de eventos produzidos e mantidos pela instituição, mas, por constituírem eventos qualitativos, não são objetos apropriados para futuras investigações ou auditorias.

Comentários:

Questão tranquila, certo pessoal? Já vimos a importância dos referidos registros e logs para as auditorias e investigações.

CONTINUIDADE DE NEGÓCIOS

Nada melhor do que avaliarmos os conceitos estabelecidos nas normas. Nesse caso, vamos ver o que a **ISO 27002** nos traz a respeito do **objetivo da Gestão da Continuidade de Negócios:**

> "não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos, e assegurar a sua **retomada em tempo hábil**, se for o caso"

Ou seja, é uma questão de sobrevivência de uma empresa. Quando há falhas ou desastres significativos, estamos falando inclusive de catástrofes, como enxurradas, terremotos, entre outros. Falaremos um pouco mais sobre isso depois.

Nesse contexto, a criticidade do negócio varia caso a caso. Uma coisa é falarmos de uma estrutura para continuidade de negócios de empresas como a GOOGLE, AMAZON, entre outros.... Nesses casos, **minutos são críticos para gerar qualquer tipo de indisponibilidade dos serviços.**

Agora para as demais empresas, **esses parâmetros devem ser avaliados caso a caso, justamente para se chegar ao ponto de equilíbrio** em que a prevenção ou gestão/controle se torne tão onerosos a ponto de não se sustentarem.

Não temos como deixar de mencionar um caso clássico de exemplo desse aspecto que é o infeliz atentado de 11 de setembro.

Sem entrar no mérito da causa e, obviamente, ciente de que as vidas eram os bens mais precioso nesse contexto, vamos focar na nossa análise de Continuidade de Negócio.

Nesse momento da foto, várias empresas e negócios já estavam sofrendo com dados e informações perdidas, estruturas de Datacenter danificados. Nesse contexto, **uma alternativa era colocar uma redundância ou Backup (solução alternativa para funcionar no caso de parada da principal) no prédio ao lado.** Mas todos nós já sabemos o fim que se deu. A gestão da continuidade do

negócio não considerou algo que parecia ser impossível, um atentado quase que simultâneo nas duas torres.

É nessa mesma toada que muitas empresas não enviam seus conselhos e executivos nos mesmos aviões e em mesmos horários, pois em caso de acidente de um, ainda se tem o restante da equipe para continuar girando os negócios.

ESCLARECENDO!

A título de curiosidade, para você se divertir após passar a sua prova, veja o seriado "DESIGNATED SURVIVOR", que nos retrata um pouco sobre essas alternativas em casos extremos de catástrofes.

Fato é que o atentado foi um momento em que grandes empresas e bancos passaram a reavaliar seus processos de gestão de continuidade de negócios. **Muitas empresas até tinham seus planos e soluções alternativas, mas sofreram para voltarem ao seu funcionamento.**

Aqui cabe mais um caso clássico que é o uso de nobreaks e geradores em soluções de redundância e backup. Mas de nada adianta se não houver uma manutenção desses equipamentos para manter as células de bateria carregadas ou o combustível disponível. Nesse aspecto que auditorias constantes nos planos e soluções ajudam a manter um ambiente estável e "pronto" para eventuais catástrofes.

Nesse contexto surge o **PCN – Plano de Continuidade de Negócios**. Este é o documento responsável por consolidar as ações para continuidade do negócio. **Todos os riscos envolvidos**, no que tange às suas probabilidades e impactos devem ser analisados. O PCN possui como foco tanto o capital intelectual (informações), bem como suas instalações.

Se o PCN não estiver atualizado e for constantemente revisado e internalizado pelas equipes, com certeza haverá uma grande dificuldade no reestabelecimento dos serviços e do negócio nos casos de necessidade. Por isso, pensar nas pessoas e testar esses planos, por intermédio de questionários e teoria, e até simulações práticas, é de suma importância.

O PCN deve então contemplar as estratégias e planos de ação com vistas a manter os serviços essenciais ativos. Obviamente, **tem-se uma etapa prévia que é a identificação desses serviços essenciais.**

Neste plano terá todos os detalhamentos dos procedimentos a serem seguidos, bem como as devidas matrizes de responsabilidades e ações por componente e recurso envolvido.

Alguns exemplos de cenários e eventos que podem ser considerados em um PCN:

1. Falhas humanas;

2. Falhas das soluções e componentes de TI;

3. Fenômenos da natureza que geram acidentes e catástrofes (furação, tempestades, maremotos);

4. Interrupções de abastecimento;

5. Distúrbios civis (greves, vandalismos);

6. Malwares e Vírus;

7. Sabotagem;

8. Terrorismo, etc.

Assim, fechamos essa parte de noções básicas de Continuidade de Negócios.

PRINCÍPIOS DE NORMAS E PADRÕES

Nosso intuito nesse capítulo é darmos uma visão geral a respeito das principais normas e padrões voltados para o cenário de Segurança da Informação.

Desse modo, vamos conhecê-las. Começaremos pela família **ISO 27000** que trata da Gestão da Segurança da Informação.

- **ISO 27001**

Esta norma define os requisitos de um Sistema de Gestão da Segurança da Informação – SGSI. O referido sistema deve estar inserido no contexto de um sistema global da organização, contemplando aspectos voltados para o risco de negócio.

Frente a isso, a referida norma busca **ESTABELECER, IMPLEMENTAR, OPERAR, MONITORAR, REVISAR, MANTER e MELHORAR** a Segurança da Informação através do SGSI.

Esta norma é a mais básica e serve como pilar para as demais, principalmente no aspecto de certificação empresarial em gestão de segurança da informação.

- **ISO 27002**

A norma ISO/IEC 27002, de forma bem objetiva, **apresenta um código de boas práticas com controles de Segurança da Informação.** Estes subsidiam a implantação de um Sistemas de Gestão da Segurança da Informação.

- **ISO 27003**

Nesta norma, temos uma abordagem mais alto nível que define diretrizes para a implementação de um SGSI. Lembremos que a ISO 27001 trata apenas dos requisitos.

- **ISO 27004**

Aqui, teremos **uma definição de métricas para medição da gestão da segurança da informação.**

- **ISO 27005**

Outra norma extremamente importante que aborda a gestão de riscos da segurança da informação.

- **NBR 15999**

A referida norma trata da gestão de continuidade de negócios. Lembremos que quando falamos de continuidade de negócios, **estamos buscando garantir um maior grau de disponibilidade de tal modo que frente a eventos diversos**, entre eles os mais catastróficos, a organização não pode ter seu negócio prejudicado, gerando a continuidade necessária.

- **NBR 22301**

Esta norma trata dos requisitos para criação de um sistema de gestão de continuidade de negócios.

- **NBR 31000**

Tal norma tratar da gestão de riscos em um caráter organizacional.

Gerência de Riscos

Costumeiramente ouvimos falar dessa palavrinha tão comum no meio de segurança da informação, que é RISCO! Sem dúvida, considera-la é fundamental na implantação de qualquer ambiente que trate a informação de alguma forma.

Entretanto, o que vem a ser, de fato, risco? Antes de definirmos propriamente o risco, vamos trabalhar alguns conceitos prévios.

Primeiramente, vamos falar **da VULNERABILIDADE**. A vulnerabilidade, segundo a norma ISO 27002, **"é a fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças".** Portanto, temos uma situação ou condição que poderá ser um meio, um vetor, uma entrada para um eventual problema de segurança. Como exemplo, podemos citar o fato de não termos uma rede estabilizada e aterrada.

Surge então um segundo conceito, que é o **de AMEAÇA.** Este conceito nada mais é do que um fator, elemento, causa que poderá explorar uma determinada vulnerabilidade. Segundo a ISO 27002, temos que a ameaça **"é a causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização. "**

Percebam, portanto, que não devemos vincular o conceito de AMEAÇA a alguém mal-intencionado com o objetivo de vazar informações ou gerar algum dano. A simples existência de períodos

chuvosos com raios pode ser uma ameaça para a vulnerabilidade que utilizamos como exemplo anteriormente, pois, neste caso, poderá gerar descarga nos equipamentos e queimá-los, gerando indisponibilidade dos serviços.

Avançando um pouco mais, temos o conceito de **IMPACTO,** que considera o resultado gerado decorrente da verificação de um determinado evento de segurança sobre um ou mais recursos. Na maioria das vezes, este resultado está atrelado a algum dano ou prejuízo gerado quando uma ameaça explora determinada vulnerabilidade.

Culminamos então **no conceito de RISCO** que é a probabilidade potencial associada à exploração de uma ou mais vulnerabilidades por parte de uma ou mais ameaças, capazes de gerar determinado IMPACTO para a organização. Percebam que o RISCO está atrelados a todos os demais conceitos que vimos anteriormente.

Resumindo, portanto, temos:

- **RISCO**: probabilidade de uma fonte de ameaça explorar uma vulnerabilidade, resultando em um impacto para a organização;
- **AMEAÇA:** Causa potencial de um incidente indesejado.
- **VULNERABILIDADE:** Fragilidade de um ativo que pode ser explorada por uma ou mais ameaças
- **IMPACTO:** Resultado gerado por uma ameaça ao explorar uma vulnerabilidade.

É importante aproveitarmos o contexto para definir, segundo a ISO 27001, o **conceito de incidente:**

> "Incidente de segurança da informação é indicado por um simples ou por uma série de **eventos de segurança da informação indesejados ou inesperados**, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação".

Muita atenção para o fato de ser indesejado e inesperado, pois são esses elementos que o diferenciam do evento, como veremos em algumas questões.

Existem algumas formas básicas de como a organização deve reagir aos riscos. Pode-se tomar basicamente quatro tipos de ação, quais sejam:

- **Evitar –** Busca-se ações com vistas a prevenir a ocorrência de determinado risco. Como exemplo, pode-se bloquear o acesso de determinado usuário à internet. Isso poderia evitar que este acesse serviços remotamente e vaze dados pela Internet.

- **Transferir –** Busca-se transferir o risco para uma terceira parte. Nesse caso, a terceira parte assume a responsabilidade das ações frente ao risco, bem como custos e outros fatores. Analogia simples ao seguro de carro que fazemos, passando o risco de acidente e roubo para a seguradora.

- **Mitigar –** Objetiva-se atuar em prol da minimização dos riscos. Como exemplo, pode-se restringir o acesso de determinados usuários a sites controlados.

- **Aceitar ou Reter –** Determinados riscos não valem a penas ser evitados, mitigados ou transferidos por agregar custos ou esforços extremamente elevados que, em termos quantitativos, são maiores que os dados ou informação em análise. Desse modo, aceita-se o risco em caso de ocorrência.

FCC – TCE-GO/Analista de Controle Externo/2014

Pedro trabalha na área que cuida da Segurança da Informação de uma empresa. Frente ao risco de indisponibilidade de uma aplicação, criou um servidor de backup para tentar garantir que as informações sejam replicadas, automaticamente, do servidor principal para o servidor backup de forma redundante. A estratégia utilizada por Pedro para tratar o risco é considerada como

A) aceitação do risco.

B) transferência do risco.

C) eliminação do risco.

D) especificação do risco.

E) mitigação do risco.

Comentário:

Quando se criar um ambiente replicado, temos uma redução do risco de perda de dados em caso de falhas ou catástrofes. Entretanto pessoal, isso não evita ou elimina o risco, pois, ainda assim, pode-se ter uma catástrofe que impacte os dois ambientes.

Gabarito: E

DIRETRIZES PARA O DESENVOLVIMENTO DE SOFTWARE SEGURO

Quando falamos de Segurança da Informação, devemos nos preocupar com todas as camadas, objetos, recursos, locais, entre outros, que de alguma forma tratará os dados em uma comunicação, ou seja, que manipulará a informação em algum momento.

Desse modo, **aplicações** e **softwares** estão **diretamente envolvidos nesse processo**. Portanto, é fundamental estabelecer diretrizes, regras, rotinas e boas práticas que de alguma forma visam tornar o processo de desenvolvimento das aplicações mais seguro e consequentemente obter um software mais seguro

Esses softwares devem ser capazes de aplicar regras de controle de acesso, gerar registros e logs que possibilitem verificar as trilhas de auditoria e, obviamente, serem robustos com vistas a manter a disponibilidade dos recursos.

É importante destacar que os aspectos de segurança da informação, em um modelo ideal, devem ser incorporados aos requisitos de desenvolvimento, além de participar em todas as fases de desenvolvimento do software, desde a modelagem, passando pela etapa de desenvolvimento, testes, instalação e homologação.

Veremos então neste tópico diversos aspectos que devem ser considerados para tal finalidade.

- **Senhas Fortes**

A utilização de senhas fortes é **amplamente difundida no mundo da Segurança da Informação.** Entretanto, é extremamente negligenciado pelos usuários. Quantos de vocês realmente têm essa preocupação? Buscam utilizar senhas diferentes para cada aplicação? Utilizam números, letras maiúsculas e minúsculas, caracteres especiais, entre outros

Creio que a maioria reconheceu que não.. e acabam por estar na lista daqueles que negligenciam esse ponto.

Desse modo, **as aplicações atuais buscam "obrigar" o usuário a cadastrar senhas que tenham parâmetros mínimos de segurança, conforme elencamos, além de considerar os tamanhos das senhas. Recomenda-se um tamanho mínimo de 8 caracteres, apesar de diversas aplicações aceitarem como quantidade razoável 6 caracteres.**

Atualmente, existem diversas soluções de mercado que permite a utilização de cofres de senhas. Tais cofres podem ser instalados em uma máquina ou servidor e gerenciar as diversas senhas do usuário, além de prover um armazenamento seguro e criptografado na máquina. Além disso, são capazes também de gerar senhas extremamente fortes para os usuários.

- **Atualização de aplicações**

Temos aqui mais um ponto amplamente difundido, entretanto, mais uma vez, negligenciado pelos usuários. É importante lembrar que as atualizações disponibilizadas pelos fabricantes **não se restringem ao acréscimo de novas funcionalidades e recursos, mas também contemplam correções de bugs, falhas de segurança, entre outros**.

Assim, não basta que o software seja seguro por si próprio se softwares complementares e integrados ou sistemas operacionais não se encontram atualizados, com diversas brechas de segurança.

- **Fuzzing**

Esta é uma técnica utilizada para testar erros em aplicações. É **amplamente utilizado no processo de desenvolvimento de softwares seguros devido sua capacidade de detectar defeitos que usuários não descobrem com facilidade**. Assim, caso este seja descoberto em ambiente de produção, pode gerar grandes danos aos usuários de determinada aplicação.

A referida técnica consiste, basicamente, **em enviar entradas randômicas para a aplicação**. Por este motivo, também é conhecida como injeção de falhas, teste de validação robusta, teste de sintaxe ou teste de negação.

Como exemplo, podemos citar um formulário que foi criado com a expectativa de receber determinado conjunto de caracteres e dados, como informações de telefone, CEP, entre outros.

Assim, o Fuzzing injetará informações incomuns como tamanhos diferenciados, caracteres não utilizados e, paralelamente, monitorará o comportamento da aplicação, pois esta poderá travar ou vazar dados de forma indevida.

- **Boas práticas de Código Seguro**

Diversas aplicações necessitam ser desenvolvidas dentro de prazos específicos e muitas vezes, arrojados. Assim, cumprir prazo e entregar o produto é a principal prioridade e, por muitas vezes, amplifica o surgimento de novas falhas, vulnerabilidades, entre outros. Neste sentido, temos diversas boas práticas que podem ser seguidas no desenvolvimento dessas aplicações, quais sejam:

  - ***Documentação*** – A documentação pode ser extremamente importante no diagnóstico e resolução de forma mais fácil e rápida de problemas.

  - ***Validação de Entrada*** – Este processo consiste em inserir dados em pontos de entrada da aplicação e verificar se o comportamento está de acordo com o esperado pelo desenvolvedor, documentando todo o processo. Um típico exemplo é a utilização de máscaras que obrigam o usuário de inserir dados no formato esperado, como o CPF.

  - ***Manipulação de Erros*** – O tratamento de erros é um ponto muito importante no desenvolvimento de aplicações seguras. Essas aplicações sempre estarão sujeitas a

erros e, por medida de segurança, é importante que haja um padrão de mensagem de erro para o usuário que não vaze informações a respeito da aplicação, evitando assim que um atacante obtenha essas informações para aprimorar seus ataques. Sob a perspectiva do desenvolvedor em utilizar tais mensagens para correção, recomenda-se que este utilize logs das aplicações e controle de forma segura em um ambiente seguro.

- **Baseline de Configuração de Aplicação**

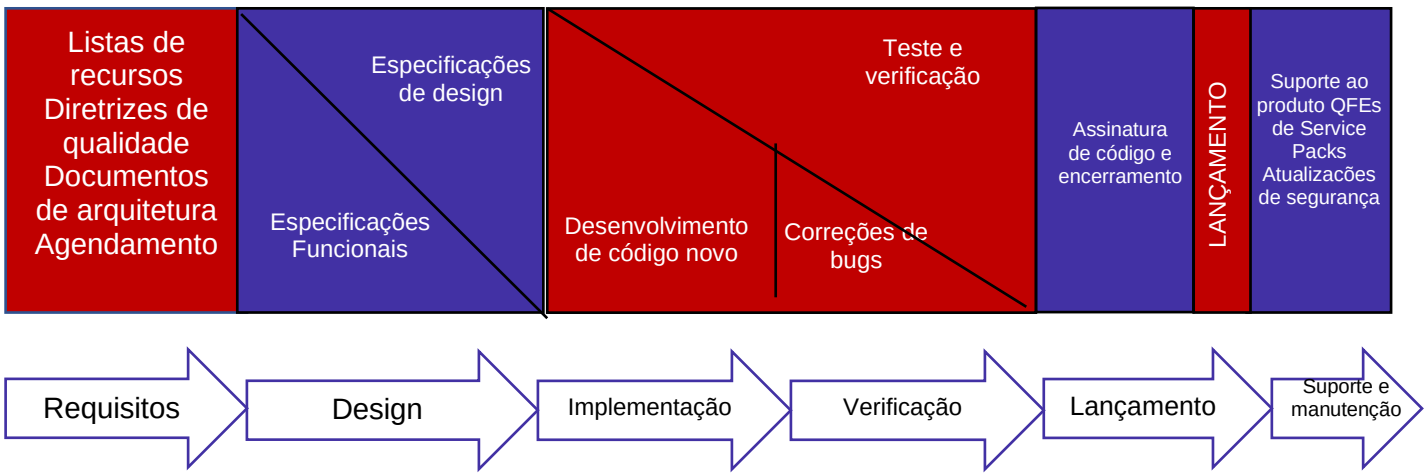
As aplicações podem utilizar diversos componentes pelos quais possuem dependências para seu funcionamento. É importante **identificar esses componentes e entender como as aplicações fazem uso dessas.** A partir de então, pode-se trabalhar em cima dessas aplicações com configurações seguras que darão a devida base e sustentação da aplicação principal.

SDL (Security Development Lifecycle)

Falando um pouco mais sobre segurança no processo de desenvolvimento, vamos abordar agora o **SDL (Security Development Lifecycle ou Ciclo de Vida do Desenvolvimento Seguro).**

É uma metodologia criada pela Microsoft para o desenvolvimento de softwares que precisam suportar ataques de usuários mal-intencionados.

O processo engloba a **adição de uma série de atividades e produtos concentrados na segurança em cada fase do processo de desenvolvimento de software da Microsoft.** Essas atividades e esses produtos incluem o desenvolvimento de modelos de ameaças durante o design do software, o uso de ferramentas de verificação de código de análise estática durante a implementação e a realização de revisões de código e testes de segurança durante um "esforço de segurança" direcionado.



O SDL tem relação direta com as fases do ciclo de vida para desenvolvimento de software. Esse processo segue o modelo espiral para aqueles que já estudaram metodologias de desenvolvimento de software.

Nesse modelo, a **MICROSOFT** criou os princípios de segurança no desenvolvimento conhecido como SD3 + C:

a) Secure by Design (Seguro por Desenho)

A arquitetura, o design e a implementação do software devem ser executados de forma a protegê-lo e proteger as informações que ele processa, além de resistir a ataques.

b) Secure by Default (Seguro por Padrão)

Na prática, o software não atingirá uma segurança perfeita; portanto, os designers devem considerar a possibilidade de haver falhas de segurança. Para minimizar os danos que ocorrem quando invasores miram nessas falhas restantes, o estado padrão do software deve aumentar a segurança.

Por exemplo, o software deve ser executado com o privilégio mínimo necessário, e os serviços e os recursos que não sejam amplamente necessários devem ser desabilitados por padrão ou ficar acessíveis apenas para uma pequena parte dos usuários.

c) Secure by Deployment (Seguro na Implantação)

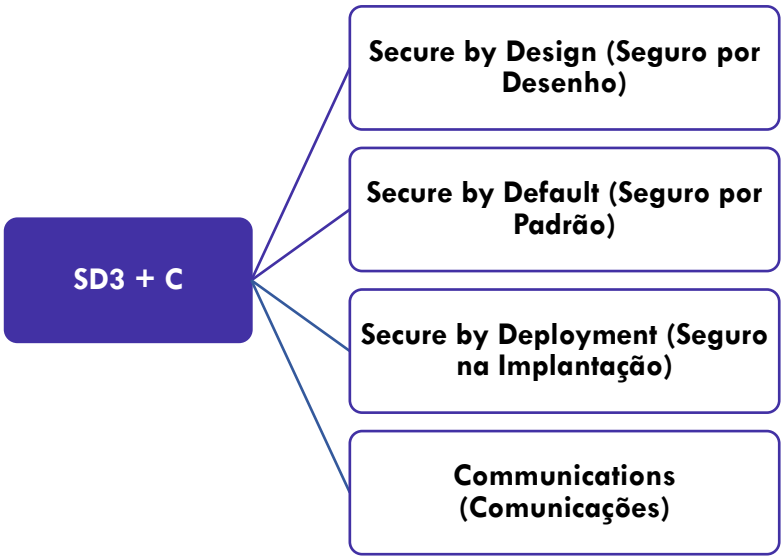
O software deve conter ferramentas e orientação que ajudem os usuários finais e/ou administradores a usá-lo com segurança. Além disso, a implantação das atualizações deve ser fácil.

d) Communications (Comunicações)

*Os desenvolvedores de software devem estar **preparados para a descoberta de vulnerabilidades do produto** e devem comunicar-se de maneira aberta e responsável com os usuários finais e/ou com os administradores para ajudá-los a tomar medidas de proteção (**como instalar patches ou implantar soluções alternativas**).*

Destes, considera-se que os dois primeiros são os que possuem a maior capacidade de agregar segurança no software.

Vamos explorar um pouco mais os aspectos de segurança considerados em cada uma das fases.



1. FASE DE REQUISITOS

Durante a fase de requisitos, a equipe de produto entra em contato com a equipe de segurança central para solicitar a designação **de um supervisor de segurança** (chamado de o "cara da segurança" na implementação do SDL na Microsoft) que serve como um ponto de contato, pesquisa e orientação durante o planejamento.

O supervisor de segurança também serve como ponto de contato entre a equipe de segurança e a gerência da equipe de produto, e aconselha a gerência da equipe quanto ao controle do elemento de segurança de seus projetos, de forma a evitar surpresas relacionadas à segurança posteriormente durante o processo.

A fase de requisitos é a oportunidade para a equipe de produto considerar **como a segurança será integrada no processo de desenvolvimento,** identificar os objetivos-chave de segurança e maximizar a segurança de software, minimizando a quebra de planos e cronogramas.

Como parte desse processo, a equipe precisa considerar como os recursos de segurança e as medidas de controle de seu software serão integrados com outros softwares que provavelmente serão usados com ele.

A perspectiva geral da equipe de produto sobre os objetivos, os desafios e os planos de segurança devem se refletir nos documentos de planejamento produzidos durante a fase de requisitos. Embora os planos estejam sujeitos a alterações conforme o andamento do projeto, a **articulação precoce desses planos ajuda a garantir que nenhum requisito seja desconsiderado ou estabelecido na última hora**.

2. FASE DE DESIGN

Nesta fase, tem-se a identificação da estrutura e os requisitos gerais do software. Na perspectiva de segurança, os elementos-chave dessa fase são:

- **Definir as diretivas de design e arquitetura de segurança;**
- **Documentar os elementos da superfície de ataque do software;**
- **Realizar a modelagem de ameaças;**
- **Definir critérios de fornecimento complementar.**

3. FASE DE IMPLEMENTAÇÃO

Durante a fase de implementação, a equipe de produto gera o código, testa e integra o software.

Os resultados da modelagem de ameaças fornecem uma orientação particularmente importante durante a fase de implementação. Os desenvolvedores dedicam atenção especial em corrigir o código de modo a atenuarem as ameaças de alta prioridade e os testadores concentram seus testes na garantia de que essas ameaças estejam de fato bloqueadas ou atenuadas.

Os elementos do SDL considerados nessa fase são:

- **Aplicar padrões de codificação e teste.**
- **Aplicar ferramentas de testes de segurança, incluindo ferramentas de difusão.**
- **Aplicar ferramentas de verificação de código de análise estática.**
- **Realizar revisões de código.**

A atenção especial fica em relação ao fato de que não se considera a aplicação de ferramentas de verificação de código de análise dinâmica nessa fase.

4. FASE DE VERIFICAÇÃO

A fase de verificação é o ponto em que o software está funcionalmente concluído e entra em testes beta por usuários. Durante essa fase, **enquanto o software passa por testes beta, a equipe de produto realiza um "esforço de segurança"** que inclui revisões do código de segurança além das concluídas na fase de implementação, bem como testes de segurança direcionados.

5. FASE DE SUPORTE E MANUTENÇÃO

Apesar da aplicação do SDL durante o desenvolvimento, as práticas de desenvolvimento mais avançadas ainda não dão suporte ao fornecimento de software completamente livre de vulnerabilidades, e há bons motivos para acreditarmos que isso nunca acontecerá.

Mesmo que o processo de desenvolvimento pudesse eliminar todas as vulnerabilidades do software fornecido, novos ataques seriam descobertos e o software que era "seguro" estaria vulnerável. Assim, as equipes de produto devem se preparar para responder a vulnerabilidades recém-descobertas no software fornecido aos clientes.

Parte do processo de resposta envolve a preparação para avaliar relatórios de vulnerabilidades e lançar orientações e atualizações de segurança quando apropriado. O outro componente do processo de resposta é a condução de um post-mortem das vulnerabilidades relatadas e a adoção de medidas, conforme necessário.

As medidas em resposta a uma vulnerabilidade **variam de emitir uma atualização para um erro isolado até atualizar as ferramentas de verificação de código** e iniciar revisões do código dos principais subsistemas.

O objetivo durante a fase de resposta é aprender a partir dos erros e utilizar as informações fornecidas em relatórios de vulnerabilidade para ajudar a detectar e eliminar mais vulnerabilidades antes que sejam descobertas no campo e utilizadas para colocar os clientes em risco.

O processo de resposta também ajuda a equipe de produto e a equipe de segurança a adaptar processos de forma que erros semelhantes não sejam introduzidos no futuro.

CLASP (Comprehensive, Lightweight Application Security Process)

O CLASP (Comprehensive, Lightweight Application Security Process) **é uma metodologia de desenvolvimento seguro de software** orientada a atividades e papéis, que descreve melhores práticas para projetos novos ou em andamento.

São propostas 24 atividades divididas em componentes de processos discretos ligados a um ou mais papéis de um projeto. Desta forma, **o CLASP provê um guia para participantes de um projeto:** gerentes, auditores de segurança, desenvolvedores, arquitetos e testadores, entre outros.

A estrutura do processo é dividida em **cinco perspectivas**, denominadas Visões CLASP. Cada Visão, por sua vez, é dividida em atividades, que contém os componentes do processo. São as Visões:

- **Visão Conceitual;**
- **Visão de Papéis;**
- **Visão de Avaliação de Atividade**
- **Visão de Implementação de Atividade**
- **Visão de Vulnerabilidades.**

As visões também são referenciadas como Conjuntos de Taxonomias de vulnerabilidades a serem consideradas no desenvolvimento do software.

A Visão Conceitual apresenta uma visão geral de como funciona o processo CLASP e como seus componentes interagem. São introduzidas as melhores práticas, a interação entre o CLASP e as políticas de segurança, alguns conceitos de segurança e os componentes do processo.

A Visão de Papéis introduz as responsabilidades básicas de cada membro do projeto (gerente, arquiteto, especificador de requisitos, projetista, implementador, analista de testes e auditor de segurança) relacionando-os com as atividades propostas, além de especificar quais são os requerimentos básicos para que cada função seja desempenhada.

A Visão de Avaliação de Atividades descreve o propósito de cada atividade, bem como os responsáveis, contribuidores, a aplicabilidade, o impacto relativo, os riscos em caso de omissão da atividade, a frequência da atividade e sugere uma aproximação do valor para homens/hora.

A Visão de Implementação descreve o conteúdo das 24 atividades de segurança definidas pelo CLASP e identifica os responsáveis pela implementação, bem como as atividades relacionadas.

A Visão de Vulnerabilidades possui um catálogo que descreve 104 tipos de vulnerabilidades no desenvolvimento de software, divididas em 5 categorias:

- Erros de Tipo e Limites de Tamanho;
- Problemas do Ambiente;
- Erros de Sincronização e Temporização;
- Erros de Protocolo;
- Erros Lógicos em Geral.

SAST (Static Application Security Testing)

Avançando na nossa discussão a respeito da criação de softwares seguros, vamos conversar um pouco a respeito de ferramentas de testes que podem ser utilizadas para tais finalidades.

O primeiro agrupamento desse tipo de solução é conhecido como **SAST,** ou em sua tradução literal, “aplicação estática para teste de segurança”.

Quando nos remetemos ao conceito de estático, imediatamente vinculamos ao código gerado para as aplicações e softwares em geral. Essas ferramentas de análise também são conhecidas como **“Ferramentas de análise de Código Fonte”.**

Então até aqui não temos muito segredo. O seu propósito é avaliar o código fonte e as diversas versões compiladas para buscar identificar brechas de segurança.

A utilização dessas ferramentas na fase de implementação e codificação reduz drasticamente o risco de se propagar um código de produto que possua falhas de implementação. Então, pensando no ciclo de vida de desenvolvimento, utilizá-las de maneira contínua ao longo das fases tende a evitar possíveis retrabalhos futuros, resolvendo o problema diretamente com os desenvolvedores envolvidos.

Podemos considerar como **VANTAGENS** desse tipo de ferramenta:

a) Pode ser executado **sucessivamente em versões de software ou agrupamento destes,** de maneira repetitiva e baixo custo;
b) **Pode ser utilizado para verificar aspectos de segurança na parcela de código considerada sensível e, por vezes, altamente confidencial**, como capacidades de buffer (prevendo estouro de buffers da aplicação), bem como outras regras de bando de dados, por exemplo;
c) Resultados são ótimos para os desenvolvedores considerando ainda a fase de desenvolvimento. **É capaz de apontar exatamente o ponto de falha ou vulnerabilidade** (linha de código ou seção do código), cabendo ao desenvolvedor corrigir de maneira precisa e objetiva.

Como **DESVANTAGENS**, podemos considerar:

a) Possui capacidade limitada de identificação de falhas, uma vez que os principais ataques são feitos sobre falhas no contexto de funcionamento da solução (aspectos dinâmicos). Desse modo, acabam por atuar sobre uma pequena parcela de todo o rol de vulnerabilidades possíveis;
b) Gera bastante falso-positivo. (Alerta de falha, porém, na prática, não é uma falha);
c) Não abrange falhas de segurança referentes a configurações do software, uma vez que extrapolam simplesmente o código-fonte;
d) Dificuldade em lidar com versões não compiláveis ou ainda, com as diversas bibliotecas utilizadas para desenvolvimento do software;

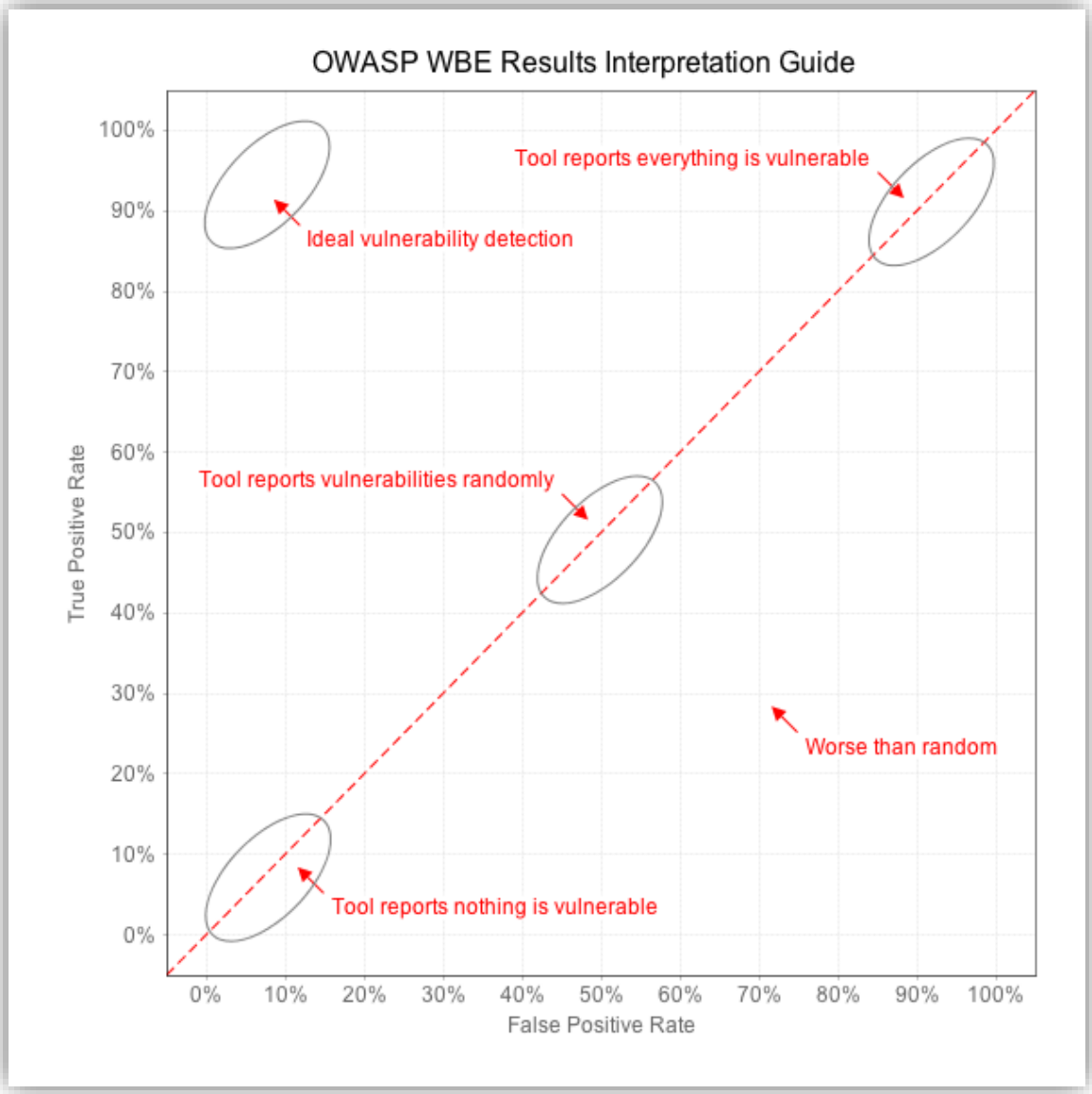
Todos esses aspectos são definidos diretamente pela OWASP (Open Application Security Project). Trata-se de uma **comunidade aberta** dedicada a permitir que as organizações concebam, desenvolvam, adquiram, operem e mantenham aplicativos confiáveis, fornecendo conhecimento para aprendizado e compartilhamento contínuo.

Um ponto de observação a ser considerado diz respeito aos critérios a serem considerados na escolha de uma ferramenta do tipo **SAST:**

1) Deve ser aderente à linguagem de desenvolvimento utilizada;

2) Quais os principais tipos de vulnerabilidades que a ferramenta é capaz de detectar;
3) Qual o nível de acurácia e precisão dos resultados? Quais as taxas de falsos positivos/falsos negativos registrados?
4) Possui consolidado adequado às diversas bibliotecas e frameworks utilizados?
5) Depende de versões completas e compiladas para processamento?
6) Suporta análise do código binário e código fonte?
7) Quão complexo é seu processo de configuração e ajuste para análise?
8) Possui suporte a implementação de regras de automatização e análise contínua?
9) Custos de licença envolvidos;

A imagem abaixo nos dá uma perspectiva de comparação quando se considera a performance em termos de resultados das diversas ferramentas:



DAST (Dynamic Application Security Testing)

Dando continuidade à nossa discussão, quando falamos de ferramentas dinâmicas, basicamente consideramos o software em operação, ou seja, em funcionamento com as diversas operações e interações que são geradas.

Esse tipo de teste é amplamente utilizado para fins de **verificação de compliance de segurança e padrões internacionais da indústria,** bem como para geração de releases e evoluções do software após seu lançamento.

Pode ser chamado também de **TESTE DE COMPORTAMENTO.** Ou seja, a falha pode não estar relacionada diretamente ao código fonte, mas são comportamentos gerados durante sua utilização. Assim, a partir de um comportamento que gere risco, deve-se fazer o processo reverso para buscar mapear uma forma de evitar o devido comportamento.

Um outro viés que se constrói com esse tipo de ferramenta é o teste de penetração. Assim, utiliza-se de diversas ferramentas com características e capacidades diferentes de maneira complementar para avaliar as vulnerabilidades comportamentais do software.

Podemos elencar como **VANTAGENS:**

a) Geralmente é rápido em termos de análise e possui custo reduzido;
b) Geralmente exige um conhecimento técnico menor quando comparado com as ferramentas SAST;
c) Testa os códigos que já estão expostos e em produção;

Como **DESVANTAGENS:**

a) Atuação tardia no processo do Ciclo de Vida de Desenvolvimento;
b) Testa apenas o impacto na abordagem frontal e direta da aplicação;

Na prática, o que se busca é a utilização conjugada das aplicações de teste que possuem os dois recursos.

IAST (Interactive Application Security Testing)

Temos aqui um conceito relativamente novo que vem aparecendo em prova. O nome nos ajuda a caracterizá-lo de forma mais concreta. Ainda que o DAST tenha características de operação da aplicação, como falamos, o IAST, vem com uma vertente mais completa, estando inserido diretamente no contexto do servidor de aplicação, sendo capaz de incorporar, inclusive, aspectos de linha de código fonte.

Essa perspectiva “interna” do IAST é uma grande característica. Então, na prática, ele acaba combinando o DAST e SAST em seu processo. Desse modo, a ferramenta consegue emitir resultados em tempo real para atuação imediata da equipe de sustentação e correção do produto.

Percebam que seu horizonte de atuação está associado à reação do IAST, logo, este não funciona como ferramenta preventiva de ataques.

Um outro aspecto que merece destaque é sua força de aplicação em ambientes automatizados que implementam esteiras de desenvolvimento como Integração Contínua.

FGV – Analista Técnico – Tecnologia da Informação (TCE-TO)/2022

O analista Gideão instalou a ferramenta SecEval no cenário de integração contínua do TCE/TO. A SecEval analisa uma aplicação em execução buscando encontrar vulnerabilidades de segurança por meio de telemetrias coletadas em tempo real de sensores inseridos no interior da aplicação. Porém, SecEval não dispõe de recursos para bloquear ataques contra aplicações em execução.

Portanto, SecEval é uma ferramenta de teste de segurança do tipo:

a) Interactive Application Security Testing;

b) Static Application Security Testing;

c) Dynamic Application Security Testing;

d) Software Composition Analysis;

e) Runtime Application Self-Protection.

Comentário:

Vejam que a questão traz muitas características do DAST e IAST. O ponto chave da questão está na perspectiva "Interna", conforme comentamos. Vejam que o termo do enunciado "sensores inseridos no interior da aplicação" materializa a ferramenta do tipo IAST.

Ainda, há uma relação direta com um agente externo, ou seja, não está dentro do domínio de desenvolvimento e produção de aplicação na ótica da organização.

Além disso, o destaque à perspectiva reativa é um ponto importante também.

Gabarito: A

OWASP Secure Coding Practices

Antes de iniciarmos esse bloco, é importante conceituar o que vem a ser o OWASP (Open Web Application Security Project). O OWASP é uma fundação sem fins lucrativos que trabalha para melhorar a segurança de softwares. É uma referência global em vários eixos de atuação, e tem sido referenciado diretamente e explicitamente em provas, e também em questões. Suas atuações são diversas frente ao escopo de atuação. Sem dúvida, seu grande destaque é o monitoramento e geração de relatórios dos conhecidos TOP 10 ataques e vulnerabilidades exploradas, ano após ano.

Entretanto, este não será o assunto desde bloco, mas sim, as suas referências práticas para desenvolvimento de códigos seguros.

A OWASP, reforçando, é uma comunidade aberta dedicada a permitir que as organizações concebam, desenvolvam, adquiram, operem e mantenham aplicativos confiáveis. Todos os projetos, ferramentas, documentos, fóruns e capítulos são gratuitos e abertos a qualquer pessoa interessada em melhorar a segurança de aplicativos. A Fundação OWASP foi lançada em 1º de dezembro de 2001, tornando-se uma instituição de caridade sem fins lucrativos dos Estados Unidos em 21 de abril de 2004.

Voltando o nosso foco às práticas seguras de desenvolvimento, destacamos primeiramente a sua característica agnóstica, ou seja, não há vínculo ou restrição com tecnologias específicas. Trata-se de um checklist que pode ser integrado em qualquer ciclo de desenvolvimento. Na sua concepção, o objetivo foi gerar um documento simples e enxuto, capaz de ser facilmente compreendido e absorvido pelas instituições.

Abaixo, você encontra o link com todas as práticas que são recomendadas nesse escopo.

https://www.owasp.org/index.php/Testing_Guide_Introduction#Principles_of_Testing

QUESTÕES COMENTADAS

Princípios de Segurança

1.CESPE – Banco da Amazônia/Técnico Científico – Segurança da Informação/2013

A segurança da informação pode ser entendida como uma atividade voltada à preservação de princípios básicos, como confidencialidade, integridade e disponibilidade da informação

Comentários:

Como vimos, estes são os principais pilares da Segurança da Informação.

Gabarito: C

---

2. (CESPE – TCE-PR/Analista de Controle – Área TI/2016) A integridade de dados que detecta modificação, inserção, exclusão ou repetição de quaisquer dados em sequência, com tentativa de recuperação, é a integridade

a) conexão com recuperação.

b) autenticação da origem de dados.

c) entidade par a par.

d) conexão com campo selecionado.

e) fluxo de tráfego.

Comentários:

Pessoal, os únicos itens que tratam da integridade são as letras “A” e “D”. As letras “B” e “C” tratam do princípio da autenticidade, enquanto a letra “E” de confidencialidade.

Assim, para a letra “A”, temos o grande diferencial que é a capacidade de detecção e recuperação de todos os dados. Para a letra “D”, temos que será aplicado o princípio de monitoramento em uma parcela específica, ou seja, uma área selecionada dos dados. Percebam que nesse caso não há recuperação, mas tão somente detecção.

Gabarito: A

3.(CESPE – TJDFT/Analista Judiciário – Análise de Sistemas/2015) Possíveis dificuldades apresentadas por colaboradores para acessar as informações do sistema da organização por mais de dois dias indicam de violação da autenticidade das informações.

Comentários:

O princípio descrito está relacionado à disponibilidade e não à autenticidade.

Gabarito: E

4.(CESPE – TJDFT/Analista Judiciário – Análise de Sistemas/2015) Se, para cometer o incidente, um colaborador usou software sem licenciamento regular e sem autorização formal da política de segurança da organização, então houve violação da integridade das informações da organização.

Comentários:

O princípio da integridade visa garantir que os dados originados de um determinado ponto chegaram ao destino sem serem violados e adulterados. Uma típica utilização para essa finalidade é por intermédio de funções HASH.

Gabarito: E

5.(CESPE – TJDFT/Analista Judiciário – Análise de Sistemas/2015) Se um colaborador conseguiu visualizar informações das quais ele não possuía privilégios, então houve violação da confidencialidade das informações.

Comentários:

Temos aqui um exemplo de acesso a dados que não deveriam ser acessados pelo usuário em tela. Ou seja, se o dado foi acessado de forma indevida por algum ente sem autorização, nitidamente temos a violação do princípio da confidencialidade.

Gabarito: C

6.(CESPE – ANTAQ/Analista Administrativo – Infraestrutura de TI/2013) Confidencialidade diz respeito à propriedade da informação que não se encontra disponível a pessoas, entidades ou processos não autorizados.

Comentários:

Pessoal, muita atenção aqui. Se devemos garantir que a informação não esteja disponível para aqueles que não possuem autorização, queremos garantir que a informação não seja acessada de forma indevida, logo, estamos falando da propriedade da confidencialidade.

Gabarito: C

7.(CESPE – TCE-RO/Analista de Informática/2013) Considere que um arquivo que esteja sendo transferido entre dois usuários tenha sido interceptado e seu conteúdo tenha sido visualizado e encaminhado a outros usuários. Nessa situação, caracterizou-se a ocorrência do comprometimento da integridade do arquivo

Comentários:

Mais uma questão bacana do CESPE. Temos descrito aqui a violação do princípio da confidencialidade quando a assertiva afirma que "o seu conteúdo tenha sido visualizado". Entretanto, a informação se manteve íntegra pois não houve alteração de seu conteúdo, não havendo, portanto, a violação do princípio da integridade.

Gabarito: E

8.(CESPE – TCE-RO/Analista de Informática/2013) Se um sítio da web sofrer comprometimento devido a problemas de hardware no servidor, impossibilitando a visualização do conteúdo pelos usuários, esse fato poderá ser considerado como comprometimento da disponibilidade do serviço.

Comentários:

Se usuários legítimos não estão conseguindo usufruir dos serviços oferecidos, temos, de fato, a violação do princípio da disponibilidade.

Gabarito: C

9.(CESPE – CNJ/Técnico Judiciário – Programação de Sistemas/2013)A proteção aos recursos computacionais inclui desde aplicativos e arquivos de dados até utilitários e o próprio sistema operacional.

Comentários:

Sem dúvida, todos esses elementos devem ser protegidos no que tange à proteção de recursos computacionais, pois, todos podem ser vetores de ataques ou de vazamento de dados.

Gabarito: C

10.(CESPE – CNJ/Técnico Judiciário – Programação de Sistemas/2013) O princípio da autenticidade é garantido quando o acesso à informação é concedido apenas a pessoas explicitamente autorizadas.

Comentários:

Não, né pessoal? Se restringimos o acesso somente às pessoas autorizadas, temos o princípio da confidencialidade.

Gabarito: E

11.(CESPE – TRE-RJ/Analista Judiciário – Análise de Sistemas/2012)Na atualidade, os ativos físicos de uma organização são mais importantes para ela do que os ativos de informação.

Comentários:

A informação é a base para qualquer organização, sendo ela e seus ativos de informação, sem dúvida, os elementos mais importantes.

Gabarito: E

12.(CESPE – TRE-RJ/Analista Judiciário – Análise de Sistemas/2012)O termo de confidencialidade, de acordo com norma NBR ISO/IEC, representa a propriedade de salvaguarda da exatidão e completude de ativos.

Comentários:

Temos aqui a descrição de Integridade, certo?

Gabarito: E

13.(CESPE – TRE-RJ/Analista Judiciário – Análise de Sistemas/2012)Na área de segurança da informação, vulnerabilidade representa causa potencial de um incidente indesejado.

Comentários:

Pessoal, a descrição apresentada refere-se ao conceito de ameaça e não vulnerabilidade.

Gabarito: E

14.(CESPE – TRE-RJ/Analista Judiciário – Análise de Sistemas/2012) A contratação de grande quantidade de novos empregados para a empresa é um incidente grave para a segurança da informação, que deve ser comunicado ao setor competente e tratado rapidamente.

Comentários:

Se é uma contratação, consequentemente houve uma aprovação e controle por parte da organização, não podendo ser categorizado como algo indesejado e inesperado. Logo, não podemos dizer que é um incidente.

Gabarito: E

15.(CESPE – TRE-RJ/Analista Judiciário – Análise de Sistemas/2012) Considere que um usuário armazenou um arquivo nesse servidor e, após dois dias, verificou que o arquivo está modificado, de forma indevida, uma vez que somente ele tinha privilégios de gravação na área em que armazenou esse arquivo. Nessa situação, houve problema de segurança da informação relacionado à disponibilidade do arquivo.

Comentários:

Houve violação do princípio da integridade e não da disponibilidade, considerando que o arquivo, ainda que alterado, esteja disponível.

Gabarito: E

16.(CESPE – TRE-RJ/Analista Judiciário – Análise de Sistemas/2012) Se as mídias das cópias de segurança são enviadas para outro local, fisicamente distante do servidor de arquivos, pelo menos uma vez a cada cinco dias úteis e tendo em vista que o transporte desses dados é feito por uma empresa terceirizada, uma forma de aumentar a segurança dessa informação é efetuar procedimento para criptografar os dados armazenados nas mídias.

Comentários:

Ora, com a criptografia, temos que os dados poderão até ser acessados, porém, não poderão ser lidos ou interpretados de forma não autorizada. Assim, temos a garantia do princípio da confidencialidade, que é uma forma de aumentar a segurança da informação.

Gabarito: C

17.(CESPE – TJ-ES/Analista Judiciário – Análise de Sistemas/2012) Para o controle lógico do ambiente computacional, deve-se considerar que medidas de segurança devem ser atribuídas aos sistemas corporativos e aos bancos de dados, formas de proteção ao código-

fonte, preservação de arquivos de log de acesso ao sistema, incluindo-se o sistema de autenticação de usuários.

Comentários:

Dos elementos apresentados, o que não apresentamos como recurso de segurança lógica na nossa teoria é a proteção de código fonte. Existem algumas ferramentas, como ofuscadores de código ou a própria criptografia que visam tornar o código fonte mais seguro, impossibilitando o acesso ou visualização por parte de usuários mal intencionados.

Gabarito: C

18.(CESPE – TJ-AC/Técnico Judiciário – Informática/2012) Para garantir a segurança da informação, é recomendável não apenas a instalação de procedimentos relacionados a sistemas e manipulação de dados eletrônicos, mas também daqueles pertinentes ao controle de acesso físico.

Comentários:

Nada mais é do que implementar de fato os aspectos de segurança física e lógica, certo pessoal?

Gabarito: C

19.(CESPE – TJ-SE/Analista Judiciário – Segurança da Informação/2014) Considere que uma empresa tenha introduzido sistema de autenticação biométrica como controle de acesso de seus funcionários às suas instalações físicas. Nessa situação, o uso desse tipo de controle é um procedimento de segurança da informação.

Comentários:

Lembremos que autenticação biométrica está baseado no mecanismo de "algo que você é". Como sabemos, esse é um procedimento de segurança da informação.

Gabarito: C

20.(CESPE – TJ-SE/Analista Judiciário – Segurança da Informação/2014) Separação de tarefas, privilégio mínimo e necessidade de saber são conceitos que identificam os três principais tipos de controle de acesso.

Comentários:

Vimos que os três principais tipos de autenticação e também de controle de acesso estão amparados em: algo que você sabe (necessidade de saber), algo que você tem (necessidade de ter) e algo que você é (necessidade de ser).

Gabarito: E

21.(CESPE – TJ-SE/Analista Judiciário – Segurança da Informação/2014) O controle de acesso RBAC (role-based access control) indica, com base em uma engenharia de papéis, o método de acesso, de modo que o nível de acesso de um colaborador, por exemplo, possa ser determinado a partir do tipo de atividade que este exerce.

Comentários:

Este é um modelo amplamente usado em organizações uma vez que reflete a estrutura da organização em termos dos papéis dos usuários em relação à instituição e permissões atreladas a estes.

Gabarito: C

22.(CESPE – TJ-SE/Analista Judiciário – Segurança da Informação/2014) Os métodos de autenticação comumente empregados fundamentam-se na clássica divisão entre o que você sabe (senha ou número PIN); o que você tem (token ou um smart card); e o que você é (íris, retina e digitais).

Comentários:

Conforme vimos, de fato, estes são os três principais métodos.

Gabarito: C

23.(CESPE – SUFRAMA/Analista de Sistemas – Desenvolvimento/2014) O controle de acesso refere-se à verificação da autenticidade de uma pessoa ou de dados. As técnicas utilizadas, geralmente, formam a base para todas as formas de controle de acesso a sistemas ou dados da organização.

Comentários:

Duas observações nessa questão. Primeiro, que o controle de acesso se aplica a pessoas de uma organização. E segundo, que se deve considerar também, além da autenticidade, a autorização.

Gabarito: C

24.(CESPE – TCE-RN/Assessor Técnico De Informática – Controle Externo/2015) A prática de contratação de seguro para equipamentos de alto custo de TIC, tais como servidores de alto desempenho e sistemas de armazenamento em escala, caracteriza transferência de risco.

Comentários:

Exatamente conforme vimos na teoria na analogia com o seguro do carro.

Gabarito: C

25.(CESPE - TCE-ES/Informática/2013) Tendo em vista que a segurança da informação tem importância estratégica, contribuindo para garantir a realização dos objetivos da organização e a continuidade dos negócios, assinale a opção correta.

a) Os principais atributos da segurança da informação são a autenticidade, a irretratabilidade e o não repúdio.

b) No contexto atual do governo e das empresas brasileiras, a segurança da informação tem sido tratada de forma eficiente, não permitindo que dados dos cidadãos ou informações estratégicas sejam vazados.

c) A privacidade constitui uma preocupação do comércio eletrônico e da sociedade da informação, não estando inserida como atributo de segurança da informação, uma vez que é prevista no Código Penal brasileiro.

d) A área de segurança da informação deve preocupar-se em proteger todos os ativos de informação de uma organização, governo, indivíduo ou empresa, empregando, em todas as situações, o mesmo nível de proteção.

e) Entre as características básicas da segurança da informação estão a confidencialidade, a disponibilidade e a integridade.

Comentários:

Vamos aos itens:

a) Temos que os principais princípios ou atributos da Segurança da Informação são a disponibilidade, integridade e confidencialidade. Muitos já complementam com a autenticidade, formando a nossa DICA. **INCORRETO**

b) À época, diversas foram a ocorrência de vulnerabilidade e invasões a sites do Governo e de empresas brasileiras. **INCORRETO**

c) A privacidade é um conceito diretamente ligada ao aspecto da confidencialidade e que muitas vezes são tratados como sinônimos para fins de comunicação dos dados. **INCORRETO**

d) Não né pessoal? Temos aí uma violação à classificação da informação ou da diferenciação de níveis de acesso considerando o grau de sigilo ou proteção dos dados ou ativos em um determinado ambiente. **INCORRETO**

e) Ainda que tivéssemos dúvida em algum dos itens acima, essa questão nos traz a tranquilidade na resposta, certo? Temos os três princípios relacionados à Segurança da Informação. **CORRETO**

Gabarito: E

26.(CESPE - TCE-ES/Informática/2013) Assinale a opção correta acerca dos mecanismos de segurança disponíveis para a implementação da segurança da informação.

a) A seleção de mecanismos e controles a serem implementados para promover a segurança da informação deve seguir critérios com base na avaliação do que se deseja proteger, dos riscos associados e do nível de segurança que se pretende atingir.

b) Todos os mecanismos de segurança disponíveis devem ser utilizados, tendo em vista que a segurança da informação exige sempre o grau máximo de proteção dos ativos de informação.

c) Controles físicos, barreiras que limitem o contato ou acesso direto a informação ou à infraestrutura para garantir a existência da informação, não são geridos pela área de segurança da informação.

d) Mecanismos de cifração ou encriptação que permitem a transformação reversível da informação, de forma a torná-la ininteligível a terceiros, em geral, são suficientes para apoiar uma boa estratégia de segurança da informação.

e) Os mais importantes mecanismos de segurança da informação incluem, necessariamente, o emprego de firewalls, detectores de intrusões, antivírus, filtros anti-spam e controle de acesso.

Comentários:

Vamos aos itens:

a) Ao se considerar os ativos e a informação a serem protegidos, deve-se considerar o quanto tal recurso é importante para a informação. Muitas das vezes, o investimento para se proteger tal recurso é tão elevado que não se justifica frente ao valor do ativo. Assim, deve-se fazer a devida ponderação dos critérios elencados no item. ***CORRETO***

b) Bem forçado, certo pessoal? Implementar todos? Não é bem assim... Deve-se implementar aquilo que é necessário para cada ambiente. ***INCORRETO***

c) Conforme vimos, os controles físicos são sim parte dos quesitos a serem considerados pela área de Segurança da Informação. ***INCORRETO***

d) Mais uma palavra forte e chave para o nosso item. São SUFICIENTES? É um pouco demais certo? Como exemplo, a simples existência e utilização da criptografia não impede que os dados sejam destruídos, sendo assim uma vulnerabilidade a ser explorada por uma ameaça. ***INCORRETO***

e) E para fechar, temos outra palavra problemática... NECESSARIAMENTE? Não é bem assim! Tudo depende do negócio e da relevância de cada recurso frente aos mecanismos de proteção. ***INCORRETO***

Gabarito: A

27.(CESPE - TCE-RO/Ciências da Computação/2013) As ações referentes à segurança da informação devem focar estritamente a manutenção da confidencialidade e a integridade e disponibilidade da informação.

Comentários:

Lembremos sempre de ficarmos atentos a essas afirmações restritivas. No caso em questão, temos o termo "ESTRITAMENTE". Não né pessoal? O simples princípio da autenticidade ficou de fora da lista.

Gabarito: E

28.(CESPE - SUFRAMA/Analista de Sistemas/2014) A utilização de algoritmos de criptografia garante a disponibilidade e a autenticidade de informações em ambientes de tecnologia da informação.

Comentários:

Podemos usar o mesmo exemplo que demos logo acima. O fato de você criptografar um disco com dados não impede que ele seja destruído e os dados sejam perdidos. Assim, apesar de usar a criptografia, os dados não estarão mais disponíveis.

Gabarito: E

29.(CESPE - SUFRAMA/Analista de Sistemas/2014) A lentidão e a paralisação do funcionamento de um sítio de comércio eletrônico que provê transações para venda de produtos é considerado incidente que viola a confidencialidade das informações do sítio.

Comentários:

Se teremos problemas com acessos gerando dificuldades no acesso e utilização dos recursos da página, temos um problema de disponibilidade e não confidencialidade.

O problema de confidencialidade existiria se alguém invadisse a página e conseguisse acesso às informações de usuário e senha de outros usuários, por exemplo.

Gabarito: E

30.(CESPE - TRT8/Analista Judiciário - Tecnologia da Informação/2013) Considere que, em uma organização, uma planilha armazenada em um computador (o servidor de arquivos) tenha sido acessada indevidamente por usuários que visualizaram as informações contidas na planilha, mas não as modificaram. O princípio da segurança da informação comprometido com esse incidente foi

a) a disponibilidade

b) a autenticidade

c) o não repúdio

d) a confidencialidade

e) a integridade

Comentários:

Quando falamos de acesso indevido a informações ou dados, estamos falando de violação do princípio da confidencialidade. Atenção para o fato de que a questão deixou claro que o invasor não fez qualquer alteração no conteúdo da planilha, ou seja, não houve prejuízo à integridade desta planilha.

Gabarito: D

31.(CESPE – TRT17/Técnico Judiciário – TI/2013) A segurança da informação tem por objetivo proteger as organizações dos vários tipos de ameaças, não se destinando a garantir a continuidade do negócio.

Comentários:

A continuidade de negócio é sem dúvida um dos principais motivos de se implementar os recursos e mecanismos de segurança. A parada do negócio de uma instituição pode gerar diversos tipos de prejuízos muitas vezes irreversíveis.

Gabarito: E

32.(CESPE – ANCINE/Analista Administrativo/2013) No que tange à autenticação, a confiabilidade trata especificamente da proteção contra negação, por parte das entidades envolvidas em uma comunicação, de ter participado de toda ou parte desta comunicação.

Comentários:

Temos aí a descrição do princípio da irretratabilidade ou não repúdio pessoal.

Gabarito: E

33.(CESPE – ANTAQ/Analista de Infraestrutura/2014) A utilização adequada dos mecanismos de criptografia permite que se descubra qualquer alteração em um documento por partes não autorizadas, o que garante a confidencialidade do documento.

Comentários:

Duas observações nessa questão. Primeiro, se estamos falando de alteração de documento, estamos falando da integridade e não confidencialidade. Em relação ao tópico de criptografia, na prática se utiliza funções HASH que possuem um caráter um pouco diferente. Veremos isso com mais calma em um outro momento.

Gabarito: E

34.(CESPE – DEPEN/Área 07/2015) O principal objetivo da segurança da informação é preservar a confidencialidade, a autenticidade, a integridade e a disponibilidade da informação.

Comentários:

Temos aí a simples apresentação dos princípios que formam o nosso principal mnemônico: DICA.

Gabarito: C

35.(CESPE – TCU/Auditor Federal de Controle Externo – TI/2015) Confidencialidade é a garantia de que somente pessoas autorizadas tenham acesso à informação, ao passo que integridade é a garantia de que os usuários autorizados tenham acesso, sempre que necessário, à informação e aos ativos correspondentes.

Comentários:

Questão bem tranquila por ser do TCU. O erro da questão se encontra no segundo trecho ao se descrever o princípio da disponibilidade e não integridade. Gostaria apenas de destacar o trecho de "usuários autorizados tenham acesso". Qual é a ideia aqui pessoal?

Se eu tenho um sistema interno que somente os usuários de gestão devem acessar, caso esse sistema fique fora do ar e ninguém tente acessar nesse período ou caso um técnico financeiro não autorizado tente acessar e verifique o sistema fora do ar, não poderemos dizer que houve indisponibilidade, pois não houve pessoas autorizadas tentando acessar o sistema no período de indisponibilidade. Certo?

Gabarito: E

36.(CESPE - 2018 - EBSERH - Analista de Tecnologia da Informação) Uma auditoria no plano de continuidade de negócios de uma organização precisa verificar se o plano é exequível e se o pessoal está treinado para executá-lo.

Comentários:

Como mencionamos, a auditoria pode atuar em qualquer etapa, fase ou tipo de processo, recurso (inclusive humano) ou documento.

Desta feita, é recomendado que se avalie a exequibilidade dos planos gerados na empresa, bem como se as equipes estão aptas a executarem os mesmos.

Gabarito: C

37.(CESPE - 2018 - ABIN - Oficial de Inteligência - Área 4) A análise de linha do tempo de eventos de interesse forense requer a existência sistematizada de registros de logs dos sistemas periciados para ser realizada, sendo sua aplicação limitada à análise forense de sistemas corporativos que dispõem desses recursos.

Comentários:

O problema da questão está na palavra "Limitada". O escopo é mais amplo da auditoria, ainda que seja para fins de análise forense.

Gabarito: E

38.(CESPE - 2015 - Telebras - Engenheiro - Engenharia de Redes) Os logs de auditoria constituem importante fonte de informação para as análises realizadas por sistemas de detecção de intrusão baseados em hosts.

Comentários:

Sem dúvida, logs são fundamentais nesse processo de geração de evidências e informações para análises em um contexto geral. No caso da questão, é apresentado o sistema de detecção de instrução, que falaremos mais detalhadamente em aula posterior de equipamentos de segurança da informação, caso seja escopo da prova.

Gabarito: C

39.(CESPE - 2015 - MEC - Gerente de Suporte) A gerência da auditoria de segurança engloba, entre outros aspectos, a administração da política de segurança e os procedimentos de recuperação após desastres; além disso, é de responsabilidade dessa gerência a constante atualização com respeito a problemas e riscos de segurança.

Comentários:

A primeira parte da questão está correta. O problema surge na responsabilidade. A auditoria faz os apontamentos e aponta as ações que devem ser tomadas. Nesse caso, a própria ação seria de manter uma rotina de atualização a respeito dos problemas e riscos de segurança.

Agora a responsabilidade de operacionalização é da equipe de gestão de segurança da informação.

Gabarito: E

40.(CESPE - 2014 - TJ-SE - Analista Judiciário - Segurança da Informação) Conformidade é um conceito relacionado à adesão dos sistemas de informação às políticas e às normas organizacionais de segurança da informação.

Comentários:

Em "Conformidade" com nossa teoria, certo pessoal? Uma boa questão para utilizarmos como padrão de resposta e resumo de conceito.

Gabarito: C

41.(CESPE - 2014 - TJ-SE - Analista Judiciário - Segurança da Informação)A execução correta dos procedimentos de segurança da informação, em conformidade com normas e com a política de segurança da empresa, deve ser garantida pelos vários gestores, cada um em sua área.

Comentários:

Tal aspectos tem como origem o que preconiza a própria política de segurança da informação, uma vez que é necessário o envolvimento de todos, inclusive no que tange à conformidade com normas e políticas, tanto externas quanto internas.

Gabarito: C

42.(CESPE - 2014 - TJ-SE - Analista Judiciário - Segurança da Informação) Atividades de usuários, exceções e outros eventos são registros ou logs de eventos produzidos e mantidos pela instituição, mas, por constituírem eventos qualitativos, não são objetos apropriados para futuras investigações ou auditorias.

Comentários:

Questão tranquila, certo pessoal? Já vimos a importância dos referidos registros e logs para as auditorias e investigações.

Gabarito: E

Diretrizes para Software Seguro

43.(CESPE – CNJ/Técnico Judiciário – Programação de Sistemas/2013) Para aumentar a segurança de um programa, deve-se evitar o uso de senhas consideradas frágeis, como o próprio nome e identificador de usuário, sendo recomendada a criação de senhas consideradas fortes, ou seja, aquelas que incluem, em sua composição, letras (maiúsculas e minúsculas), números e símbolos embaralhados, totalizando, preferencialmente, mais de seis caracteres.

Comentários:

Conforme vimos, a segurança e controle dos formatos de senhas permitidas pelos usuários faz parte de um processo seguro de uma aplicação. Mencionamos ainda que na prática, utiliza-se oito caracteres como uma quantidade segura, entretanto, algumas aplicações e examinadores consideram seis como uma quantidade suficiente.

Gabarito: C

44.(CESPE – TCE-PA/Auditor de Controle Externo – Informática/2016) Na metodologia de desenvolvimento seguro de software SDL (Security Development Lifecycle), a modelagem de ameaças é realizada na fase de requisitos.

Comentários:

A modelagem de ameaças se dá na fase de DESIGN. Lembremos os principais aspectos considerados nessa fase:

- Definir as diretivas de design e arquitetura de segurança;
- Documentar os elementos da superfície de ataque do software;
- Realizar a modelagem de ameaças;
- Definir critérios de fornecimento complementar.

Gabarito: E

45.(CESPE – CNJ/Analista Judiciário – Análise de Sistemas/2013) O SDL é um processo de desenvolvimento de software seguro, que envolve a adição de produtos e atividades, como o desenvolvimento de modelos de ameaças.

Comentários:

Essa é a definição básica do processo contemplado pelo SDL.

Gabarito: C

46.(CESPE – Polícia Federal/Perito Criminal Federal – Cargo 3/2013) O CLASP (Comprehensive, Lightweight Application Security Process) fornece uma taxonomia de vulnerabilidades que podem ocorrer no código-fonte e que podem ser verificadas com o uso de ferramentas automatizadas para análise estática de código.

Comentários:

É uma das definições apresentadas para o CLASP, complementada por suas VISÕES do software, conforme vimos em nossa teoria.

Gabarito: C

QUESTÕES COMENTADAS COMPLEMENTARES

1. **FGV - 2022 - SEFAZ-AM - Analista de Tecnologia da Informação da Fazenda Estadual - Manhã**

A administração de dados deve observar princípios básicos que são largamente adotados pela comunidade segurança da informação. Além da Confidencialidade, Integridade, Disponibilidade e Autenticidade, o princípio da Irretratabilidade completa a lista.

Assinale o significado do princípio da Irretratabilidade.

A Garantia de que os usuários que originam as informações são conhecidos e autorizados, de modo que não possam se passar por terceiros.

B Impossibilidade de negação de que uma pessoa tenha sido autora de uma determinada informação.

C Obrigatoriedade dos agentes pelo zelo com todas as informações coletadas.

D Preservação fidedigna das informações.

E Restrição de acesso às informações apenas aos autorizados.

Comentário:

Vamos aos itens:

a) Estamos falando aqui da prática de controle de acesso com autenticação e autorização. INCORRETO

b) Exatamente pessoal. Lembrando que a irretratabilidade também se aplica ao destinatário, no sentido dele não ser capaz de negar o recebimento da informação. **CORRETO**

c) Estamos falando aqui de processo de cultura organizacional. INCORRETO

d) Temos o princípio da integridade. INCORRETO

e) Novamente, controle de acesso, associado à confidencialidade. INCORRETO

Gabarito: B

---

2. (FCC – TRE-RR/Analista Judiciário/2015)

O processo de proteção da informação das ameaças caracteriza-se como Segurança da Informação. O resultado de uma gestão de segurança da informação adequada deve oferecer suporte a cinco aspectos principais:

I. Somente as pessoas autorizadas terão acesso às informações.

II. As informações serão confiáveis e exatas. Pessoas não autorizadas não podem alterar os dados.

III. Garante o acesso às informações, sempre que for necessário, por pessoas autorizadas.

IV. Garante que em um processo de comunicação os remetentes não se passem por terceiros e nem que a mensagem sofra alterações durante o envio.

V. Garante que as informações foram produzidas respeitando a legislação vigente.

Os aspectos elencados de I a V correspondem, correta e respectivamente, a:

a) autenticidade -integridade -disponibilidade - legalidade -confidencialidade.

b) autenticidade -confidencialidade -integridade - disponibilidade -legalidade.

c) integridade -disponibilidade -confidencialidade - autenticidade -legalidade.

d) disponibilidade -confidencialidade -integridade - legalidade -autenticidade.

e) confidencialidade -integridade -disponibilidade - autenticidade -legalidade.

Comentário:

Vimos todas essas características no início do nosso conteúdo de princípios de segurança. Vale mencionar que no item IV, temos a descrição tanto da autenticidade quanto da integridade.

Gabarito: E

---

3. FGV - 2021 - Banestes - Analista em Tecnologia da Informação - Segurança da Informação

Um pequeno dispositivo que contém um código de proteção precisa necessariamente ficar conectado à porta USB do computador para que determinado software possa ser utilizado.

Esse dispositivo utilizado para prevenir o uso não autorizado de determinado software é conhecido como:

A Vault;

B Keycloak;

C KeePass;

D Keylogger;

E Hardlock.

Comentário:

Um dongle (HARDLOCK) de proteção de software é um dispositivo de proteção eletrônica contra cópia e proteção de conteúdo. Quando conectados a um computador ou outros eletrônicos, eles desbloqueiam a funcionalidade do software ou decodificam o conteúdo. Ele funciona como uma "chave" que autentica o usuário e protege o software contra cópias e uso não autorizado.

Vamos aos demais itens:

A) INCORRETO. "Vault" geralmente se refere a um local seguro para armazenar informações sensíveis, como senhas e chaves criptográficas.

B) INCORRETO. "Keycloak" é um software de gerenciamento de identidade e acesso de código aberto, que fornece serviços de autenticação e autorização.

C) INCORRETO. "KeePass" é um gerenciador de senhas de código aberto que armazena credenciais de usuário criptografadas. Embora possa ajudar a proteger informações de acesso, não se refere a um dispositivo físico que precisa ser conectado à porta USB para utilizar um software específico.

D) INCORRETO. "Keylogger" é um tipo de software ou hardware malicioso que registra as teclas pressionadas pelos usuários, com o objetivo de roubar informações confidenciais, como senhas e números de cartão de crédito.

Gabarito: E

---

4. (FCC – TRE-RR/Analista Judiciário/2015)

O processo de proteção da informação das ameaças caracteriza-se como Segurança da Informação. O resultado de uma gestão de segurança da informação adequada deve oferecer suporte a cinco aspectos principais:

I. Somente as pessoas autorizadas terão acesso às informações.

II. As informações serão confiáveis e exatas. Pessoas não autorizadas não podem alterar os dados.

III. Garante o acesso às informações, sempre que for necessário, por pessoas autorizadas.

IV. Garante que em um processo de comunicação os remetentes não se passem por terceiros e nem que a mensagem sofra alterações durante o envio.

V. Garante que as informações foram produzidas respeitando a legislação vigente.

Os aspectos elencados de I a V correspondem, correta e respectivamente, a:

a) autenticidade -integridade -disponibilidade - legalidade -confidencialidade.

b) autenticidade -confidencialidade -integridade - disponibilidade -legalidade.

c) integridade -disponibilidade -confidencialidade - autenticidade -legalidade.

d) disponibilidade -confidencialidade -integridade - legalidade -autenticidade.

e) confidencialidade -integridade -disponibilidade - autenticidade -legalidade.

Comentário:

Vimos todas essas características no início do nosso conteúdo de princípios de segurança. Vale mencionar que no item IV, temos a descrição tanto da autenticidade quanto da integridade.

Gabarito: E

---

5. FGV - 2020 - IBGE - Agente Censitário Operacional - Reaplicação

Considere as seguintes regras para a composição de senhas de 4 caracteres:

I. Dois dígitos numéricos + duas letras maiúsculas;

II. Quatro letras minúsculas;

III. Quatro dígitos numéricos;

IV. Três letras minúsculas + um dígito numérico;

V. Uma letra minúscula + três dígitos numéricos.

A regra que permite a criação de senhas mais fortes é:

A I;

B II;

C III;

D IV;

E V.

Comentário:

Temos aqui muito mais uma questão de probabilidade e estatística, do que de segurança em si.

Pessoal, quanto mais possibilidade temos de gerar caracteres diferentes e na combinação deles, senhas diferentes, teremos maior robustez.

Sendo assim, quando indicamos que um campo suporta apenas números, temos 10 opções (0 a 10). Quando falamos de letras, temos 26 possibilidades de minúsculas e outras 26 de maiúsculas, a depender do alfabeto suportado. Sendo assim, quando colocamos quatro opções de letras minúsculas, teremos 26x26x26x26 como total de combinações possíveis.

Gabarito: B

---

6. FGV - 2018 - AL-RO - Analista Legislativo - Infraestrutura de Redes e

No contexto da Segurança da Informação, o primeiro controle de acesso a ser estabelecido, isto é, a primeira barreira de segurança deve ser o controle de acesso

A lógico.

B físico.

C por nome de usuário (login) e senha.

D por DMZ.

E por criptografia.

Comentário:

Pessoal, sem dúvida, a boa prática traz a primeira camada física de proteção como referência. Estamos falando aqui de controles em portarias, hall de entrada, garagens, seja com estruturas que envolvem pessoas ou não. Todas as demais são recursos a serem implantados em novas camadas de segurança.

Gabarito: B

---

7. FGV - 2018 - MPE-AL - Técnico do Ministério Público - Tecnologia da Informação

Em muitas transações financeiras realizadas pela Internet é necessário que o usuário, além de fornecer o seu e-mail e senha, digite um código gerado ou recebido em seu celular. Essa tecnologia é conhecida como

A biometria.

B cartão inteligente.

C certificado digital.

D criptografia.

E token de segurança.

Comentário:

Estamos falando dos recursos associados aos múltiplos fatores de segurança da informação. Assim, quando se tem uma mensagem enviada ao celular, estamos tratando de uma camada de segurança de algo que você tem, sendo também referenciado como token de segurança para validação do usuário.

Gabarito: E

---

8. FGV - 2017 - SEPOG - RO - Analista em Tecnologia da Informação e Comunicação

O reconhecimento biométrico consiste em reconhecer um indivíduo com base nas suas características físicas ou comportamentais.

A técnica adotada pelo sistema de identificação biométrico que implica em detectar e comparar a posição das minúcias (minutiae), também conhecida como características de Galton, é utilizada no reconhecimento da

A impressão digital.

B íris.

C retina.

D face.

E voz.

Comentário:

Vamos aos itens:

A) **CORRETO**. A técnica que detecta e compara a posição das minúcias (minutiae) ou características de Galton é utilizada no reconhecimento de impressões digitais. As minúcias são pontos específicos das impressões digitais, como bifurcações e terminações de cristas, que são únicos para cada indivíduo e podem ser utilizados para identificá-los de forma confiável.

B) INCORRETO. O reconhecimento da íris se baseia na análise das características únicas da íris de um indivíduo, como padrões de cores, estruturas e texturas. Essa técnica não utiliza minúcias para realizar a identificação.

C) INCORRETO. O reconhecimento de retina envolve a análise dos padrões de vasos sanguíneos da retina, que são únicos para cada indivíduo. A técnica de minúcias não é aplicada nesse método de reconhecimento biométrico.

D) INCORRETO. O reconhecimento facial analisa características faciais específicas, como distâncias entre os olhos, formato do nariz e contorno dos lábios. A técnica de minúcias não é empregada nesse tipo de reconhecimento biométrico.

E) INCORRETO. O reconhecimento de voz utiliza características comportamentais, como a frequência, tom e ritmo da fala, para identificar um indivíduo. A técnica de minúcias não é relevante para o reconhecimento de voz.

Gabarito: B

---

9. **(FCC – TRE-CE/Analista Judiciário – Análise de Sistemas/2015) Em relação à segurança da informação, considere:**

I. Capacidade do sistema de permitir que alguns usuários acessem determinadas informações, enquanto impede que outros, não autorizados, sequer as consultem.

II. Informação exposta, sob risco de manuseio (alterações não aprovadas e fora do controle do proprietário da informação) por pessoa não autorizada.

III. O sistema deve ter condições de verificar a identidade dos usuários, e este ter condições de analisar a identidade do sistema.

Os itens I, II e III, associam-se, direta e respectivamente, aos princípios de

a) confidencialidade, integridade e autenticidade.

b) autenticidade, confidencialidade e irretratabilidade.

c) confidencialidade, confidencialidade e irretratabilidade.

d) autenticidade, confidencialidade e autenticidade.

e) integridade, confidencialidade e integridade.

Comentário:

Reforçando os conceitos que vimos previamente. Observemos que, no item II, o examinador destaca o aspecto de alteração não autorizada, ou seja, impactando o princípio de integridade.

Gabarito: A

---

10. (FCC – TRE-CE/Técnico Judiciário – Programação de Sistemas/2012) A propriedade que garante que nem o emissor nem o destinatário das informações possam negar a sua transmissão, recepção ou posse é conhecida como

a) autenticidade.

b) integridade.

c) irretratabilidade.

d) confidenciabilidade.

e) acessibilidade.

Comentário:

Pessoal, temos aqui uma abordagem um pouco mais ampla do conceito de não-repúdio ou irretratabilidade.

Gabarito: C

---

11. (FCC – TJ-AP/Analista Judiciário – Banco de Dados/2014) O controle de acesso à informação é composto por diversos processos, dentre os quais, aquele que identifica quem efetua o acesso a uma dada informação. Esse processo é denominado

A) autenticação.

B) auditoria.

C) autorização.

D) identificação.

E) permissão.

Comentário:

Lembrando que o controle de acesso envolve tanto a autenticação quanto a autorização. Entretanto, o processo de identificação está relacionado à autenticação.

Gabarito: A

---

12. (FCC – TRF 4ª Região / Analista Judiciário – Informática/2014) José deve estabelecer uma política de segurança e implantar os mecanismos de segurança para o TRF da 4a Região. Dentre os mecanismos para a segurança física, José deve escolher o uso de

A) senha de acesso ao computador do TRF.

B) Token criptográfico para autenticar os dados acessados no computador do TRF.

C) senha de acesso às páginas web do TRF.

D) cartão de acesso para as pessoas que entram no TRF.

E) criptografia na troca de informações entre os computadores do TRF.

Comentário:

Pessoal, o problema nessa questão está nos itens "B" e "D", pois, ambos são itens utilizados para segurança física. Entretanto, no item "B", temos a descrição incorreta pois não se objetiva autenticar os dados e sim a pessoa.

Gabarito: D

---

13. (FCC – SABESP/Analista de Gestão – Sistemas/2014) Todos os procedimentos de segurança listados abaixo referem-se a controles de acesso lógico, EXCETO:

A) utilizar mecanismos de time-out automático, isto é, desativar a sessão após um determinado tempo sem qualquer atividade no terminal ou computador. Para restaurá-la, o usuário é obrigado a fornecer novamente seu ID e senha.

B) definir o controle de acesso nas entradas e saídas através de travas, alarmes, grades, vigilante humano, vigilância eletrônica, portas com senha, cartão de acesso e registros de entrada e saída de pessoas e objetos.

C) utilizar logs como medidas de detecção e monitoramento, registrando atividades, falhas de acesso (tentativas frustradas de logon ou de acesso a recursos protegidos) ou uso do sistema operacional, utilitários e aplicativos, e detalhando o que foi acessado, por quem e quando.

D) definir as permissões e os privilégios de acesso para cada recurso ou arquivo no sistema. Quando um usuário tenta acessar um recurso, o sistema operacional verifica se as definições de acesso desse usuário e do recurso desejado conferem. O usuário só conseguirá o acesso se essa verificação for positiva.

E) limitar o número de tentativas de logon sem sucesso e limitar o horário de uso dos recursos computacionais de acordo com a real necessidade de acesso aos sistemas. Pode-se, por exemplo, desabilitar o uso dos recursos nos fins de semana ou à noite.

Comentário:

O item "B" nos traz uma lista de itens que fazem parte da segurança física de qualquer ambiente. Questão bem extensa, porém, bem tranquila.

Gabarito: B

---

14. (FCC – TCE-GO/Analista de Controle Externo/2014) Pedro trabalha na área que cuida da Segurança da Informação de uma empresa. Frente ao risco de indisponibilidade de uma aplicação, criou um servidor de backup para tentar garantir que as informações sejam replicadas, automaticamente, do servidor principal para o servidor backup de forma redundante. A estratégia utilizada por Pedro para tratar o risco é considerada como

A) aceitação do risco.

B) transferência do risco.

C) eliminação do risco.

D) especificação do risco.

E) mitigação do risco.

Comentário:

Quando se criar um ambiente replicado, temos uma redução do risco de perda de dados em caso de falhas ou catástrofes. Entretanto pessoal, isso não evita ou elimina o risco, pois, ainda assim, pode-se ter uma catástrofe que impacte os dois ambientes.

Gabarito: E

---

15. (FCC – TRT – 6ª Região (PE)/Analista Judiciário - TI/2018) A gerência de riscos na segurança da informação inclui o uso de diversos tipos e recursos de segurança. Um recurso de segurança categorizado como mecanismo de controle de acesso lógico é

a) a função hash.

b) o sistema biométrico.

c) a catraca eletrônica.

d) o sistema de detecção de intrusão.

e) o sniffer.

Comentários:

Questão bem tranquila, certo pessoal? Vimos que um dos mecanismos de controle de acesso é o sistema biométrico. Nele podemos controlar o acesso a partir de **ALGO QUE VOCÊ É.**

a) Algoritmo utilizado para fins de integridade. **ERRADO**
c) Controle de acesso físico. **ERRADO**
d) Ferramenta para gerenciamento de segurança de redes de computadores. **ERRADO**
e) Ferramenta utilizada para capturar e analisar dados lógicos (pacotes) que trafegam na rede. **ERRADO**

Gabarito: B

---

16. **(FCC – TRF – 4ª Região/Técnico Judiciário/2014) Os sistemas de identificação biométricos funcionam através da comparação de características físicas apresentadas por um usuário com as correspondentes armazenadas em um determinado banco de dados, identificando-o ou não como um dos usuários cadastrados, dificultando sobremaneira as fraudes praticadas contra as várias formas de verificação de identidades. O sistema de identificação biométrica que utiliza a parte do fundo do olho como identificador é conhecido como identificação**

a) datiloscópica ou fingerprint.

b) da íris

c) da retina.

d) cognitiva.

e) teclar.

Comentários:

Como vimos em nossa teoria:

1. Retina – Analisa os vasos sanguíneos do fundo do olho;
2. Íris – Analise os anéis coloridos do olho;

Gabarito: C

---

17. **(FCC - 2013 - SEFAZ-SP - Agente Fiscal de Rendas - Gestão Tributária - Prova 3)**

A auditoria da segurança da informação avalia a política de segurança e os controles relacionados adotados em cada organização. Nesse contexto, muitas vezes, as organizações não se preocupam, ou até negligenciam, um aspecto básico da segurança que é a localização dos equipamentos que podem facilitar a intrusão. Na auditoria de segurança da informação, esse aspecto é avaliado no Controle de :

a) acesso lógico.
b) acesso físico.
c) programas.
d) conteúdo.
e) entrada e saída de dados.

Comentários:

Percebam que a questão aborda a questão da "Localização dos equipamentos". Ora, estamos falando, portanto, das questões atreladas ao controle físico.

Gabarito: B

LISTA DE QUESTÕES CESPE

Princípios de Segurança

1. **(CESPE – Banco da Amazônia/Técnico Científico – Segurança da Informação/2013) A segurança da informação pode ser entendida como uma atividade voltada à preservação de princípios básicos, como confidencialidade, integridade e disponibilidade da informação**

---

2. **(CESPE – TCE-PR/Analista de Controle – Área TI/2016) A integridade de dados que detecta modificação, inserção, exclusão ou repetição de quaisquer dados em sequência, com tentativa de recuperação, é a integridade**

A) conexão com recuperação.

B) autenticação da origem de dados.

C) entidade par a par.

D) conexão com campo selecionado.

E) fluxo de tráfego.

---

3. **(CESPE – TJDFT/Analista Judiciário – Análise de Sistemas/2015) Possíveis dificuldades apresentadas por colaboradores para acessar as informações do sistema da organização por mais de dois dias indicam de violação da autenticidade das informações.**

---

4. **(CESPE – TJDFT/Analista Judiciário – Análise de Sistemas/2015) Se, para cometer o incidente, o colaborador usou software sem licenciamento regular e sem autorização**

formal da política de segurança da organização, então houve violação da integridade das informações da organização.

---

5. (CESPE – TJDFT/Analista Judiciário – Análise de Sistemas/2015) Se um colaborador conseguiu visualizar informações das quais ele não possuía privilégios, então houve violação da confidencialidade das informações.

---

6. (CESPE – ANTAQ/Analista Administrativo – Infraestrutura de TI/2014) Confidencialidade diz respeito à propriedade da informação que não se encontra disponível a pessoas, entidades ou processos não autorizados.

---

7. (CESPE – TCE-RO/Analista de Informática/2013) Considere que um arquivo que esteja sendo transferido entre dois usuários tenha sido interceptado e seu conteúdo tenha sido visualizado e encaminhado a outros usuários. Nessa situação, caracterizou-se a ocorrência do comprometimento da integridade do arquivo

---

8. (CESPE – TCE-RO/Analista de Informática/2013) Se um sítio da web sofrer comprometimento devido a problemas de hardware no servidor, impossibilitando a visualização do conteúdo pelos usuários, esse fato poderá ser considerado como comprometimento da disponibilidade do serviço.

---

9. (CESPE – CNJ/Técnico Judiciário – Programação de Sistemas/2013) A proteção aos recursos computacionais inclui desde aplicativos e arquivos de dados até utilitários e o próprio sistema operacional.

---

10. (CESPE – CNJ/Técnico Judiciário – Programação de Sistemas/2013) O princípio da autenticidade é garantido quando o acesso à informação é concedido apenas a pessoas explicitamente autorizadas.

---

11. (CESPE – TRE-RJ/Analista Judiciário – Análise de Sistemas/2012) Na atualidade, os ativos físicos de uma organização são mais importantes para ela do que os ativos de informação.

12. (CESPE – TRE-RJ/Analista Judiciário – Análise de Sistemas/2012) O termo de confidencialidade, de acordo com norma NBR ISO/IEC, representa a propriedade de salvaguarda da exatidão e completude de ativos.

13. (CESPE – TRE-RJ/Analista Judiciário – Análise de Sistemas/2012) Na área de segurança da informação, vulnerabilidade representa causa potencial de um incidente indesejado.

14. (CESPE – TRE-RJ/Analista Judiciário – Análise de Sistemas/2012) A contratação de grande quantidade de novos empregados para a empresa é um incidente grave para a segurança da informação, que deve ser comunicado ao setor competente e tratado rapidamente.

15. (CESPE – TRE-RJ/Analista Judiciário – Análise de Sistemas/2012) Considere que um usuário armazenou um arquivo nesse servidor e, após dois dias, verificou que o arquivo está modificado, de forma indevida, uma vez que somente ele tinha privilégios de gravação na área em que armazenou esse arquivo. Nessa situação, houve problema de segurança da informação relacionado à disponibilidade do arquivo.

16. (CESPE – TRE-RJ/Analista Judiciário – Análise de Sistemas/2012) Se as mídias das cópias de segurança são enviadas para outro local, fisicamente distante do servidor de arquivos, pelo menos uma vez a cada cinco dias úteis e tendo em vista que o transporte desses dados é feito por uma empresa terceirizada, uma forma de aumentar a segurança dessa informação é efetuar procedimento para criptografar os dados armazenados nas mídias.

17. (CESPE – TJ-ES/Analista Judiciário – Análise de Sistemas/2012) Para o controle lógico do ambiente computacional, deve-se considerar que medidas de segurança devem ser atribuídas aos sistemas corporativos e aos bancos de dados, formas de proteção ao código-fonte, preservação de arquivos de log de acesso ao sistema, incluindo-se o sistema de autenticação de usuários.

18. (CESPE – TJ-AC/Técnico Judiciário – Informática/2012) Para garantir a segurança da informação, é recomendável não apenas a instalação de procedimentos relacionados a sistemas e manipulação de dados eletrônicos, mas também daqueles pertinentes ao controle de acesso físico.

---

19. (CESPE – TJ-SE/Analista Judiciário – Segurança da Informação/2014) Considere que uma empresa tenha introduzido sistema de autenticação biométrica como controle de acesso de seus funcionários às suas instalações físicas. Nessa situação, o uso desse tipo de controle é um procedimento de segurança da informação.

---

20. (CESPE – TJ-SE/Analista Judiciário – Segurança da Informação/2014) Separação de tarefas, privilégio mínimo e necessidade de saber são conceitos que identificam os três principais tipos de controle de acesso.

---

21. (CESPE – TJ-SE/Analista Judiciário – Segurança da Informação/2014) O controle de acesso RBAC (role-based access control) indica, com base em uma engenharia de papéis, o método de acesso, de modo que o nível de acesso de um colaborador, por exemplo, possa ser determinado a partir do tipo de atividade que este exerce.

---

22. (CESPE – TJ-SE/Analista Judiciário – Segurança da Informação/2014) Os métodos de autenticação comumente empregados fundamentam-se na clássica divisão entre o que você sabe (senha ou número PIN); o que você tem (token ou um smart card); e o que você é (íris, retina e digitais).

---

23. (CESPE – SUFRAMA/Analista de Sistemas – Desenvolvimento/2014) O controle de acesso refere-se à verificação da autenticidade de uma pessoa ou de dados. As técnicas utilizadas, geralmente, formam a base para todas as formas de controle de acesso a sistemas ou dados da organização.

---

24. (CESPE – TCE-RN/Assessor Técnico De Informática – Controle Externo/2015) A prática de contratação de seguro para equipamentos de alto custo de TIC, tais como servidores de alto desempenho e sistemas de armazenamento em escala, caracteriza transferência de risco.

25. (CESPE - TCE-ES/Informática/2013) Tendo em vista que a segurança da informação tem importância estratégica, contribuindo para garantir a realização dos objetivos da organização e a continuidade dos negócios, assinale a opção correta.

a) Os principais atributos da segurança da informação são a autenticidade, a irretratabilidade e o não repúdio.

b) No contexto atual do governo e das empresas brasileiras, a segurança da informação tem sido tratada de forma eficiente, não permitindo que dados dos cidadãos ou informações estratégicas sejam vazados.

c) A privacidade constitui uma preocupação do comércio eletrônico e da sociedade da informação, não estando inserida como atributo de segurança da informação, uma vez que é prevista no Código Penal brasileiro.

d) A área de segurança da informação deve preocupar-se em proteger todos os ativos de informação de uma organização, governo, indivíduo ou empresa, empregando, em todas as situações, o mesmo nível de proteção.

e) Entre as características básicas da segurança da informação estão a confidencialidade, a disponibilidade e a integridade.

26. (CESPE - TCE-ES/Informática/2013) Assinale a opção correta acerca dos mecanismos de segurança disponíveis para a implementação da segurança da informação.

a) A seleção de mecanismos e controles a serem implementados para promover a segurança da informação deve seguir critérios com base na avaliação do que se deseja proteger, dos riscos associados e do nível de segurança que se pretende atingir.

b) Todos os mecanismos de segurança disponíveis devem ser utilizados, tendo em vista que a segurança da informação exige sempre o grau máximo de proteção dos ativos de informação.

c) Controles físicos, barreiras que limitem o contato ou acesso direto a informação ou à infraestrutura para garantir a existência da informação, não são geridos pela área de segurança da informação.

d) Mecanismos de cifração ou encriptação que permitem a transformação reversível da informação, de forma a torná-la ininteligível a terceiros, em geral, são suficientes para apoiar uma boa estratégia de segurança da informação.

e) Os mais importantes mecanismos de segurança da informação incluem, necessariamente, o emprego de firewalls, detectores de intrusões, antivírus, filtros anti-spam e controle de acesso.

27. (CESPE - TCE-RO/Ciências da Computação/2013) As ações referentes à segurança da informação devem focar estritamente a manutenção da confidencialidade e a integridade e disponibilidade da informação.

---

28. (CESPE - SUFRAMA/Analista de Sistemas/2014) A utilização de algoritmos de criptografia garante a disponibilidade e a autenticidade de informações em ambientes de tecnologia da informação.

---

29. (CESPE - SUFRAMA/Analista de Sistemas/2014) A lentidão e a paralisação do funcionamento de um sítio de comércio eletrônico que provê transações para venda de produtos é considerado incidente que viola a confidencialidade das informações do sítio.

---

30. (CESPE - TRT8/Analista Judiciário - Tecnologia da Informação/2013) Considere que, em uma organização, uma planilha armazenada em um computador (o servidor de arquivos) tenha sido acessada indevidamente por usuários que visualizaram as informações contidas na planilha, mas não as modificaram. O princípio da segurança da informação comprometido com esse incidente foi

a) a disponibilidade

b) a autenticidade

c) o não repúdio

d) a confidencialidade

e) a integridade

---

31. (CESPE – TRT17/Técnico Judiciário – TI/2013) A segurança da informação tem por objetivo proteger as organizações dos vários tipos de ameaças, não se destinando a garantir a continuidade do negócio.

---

32. (CESPE – ANCINE/Analista Administrativo/2013) No que tange à autenticação, a confiabilidade trata especificamente da proteção contra negação, por parte das entidades envolvidas em uma comunicação, de ter participado de toda ou parte desta comunicação.

33. **(CESPE – ANTAQ/Analista de Infraestrutura/2014) A utilização adequada dos mecanismos de criptografia permite que se descubra qualquer alteração em um documento por partes não autorizadas, o que garante a confidencialidade do documento.**

34. **(CESPE – DEPEN/Área 07/2015) O principal objetivo da segurança da informação é preservar a confidencialidade, a autenticidade, a integridade e a disponibilidade da informação.**

35. **(CESPE – TCU/Auditor Federal de Controle Externo – TI/2015)Confidencialidade é a garantia de que somente pessoas autorizadas tenham acesso à informação, ao passo que integridade é a garantia de que os usuários autorizados tenham acesso, sempre que necessário, à informação e aos ativos correspondentes.**

36. **(CESPE - 2018 - EBSERH - Analista de Tecnologia da Informação)**

Uma auditoria no plano de continuidade de negócios de uma organização precisa verificar se o plano é exequível e se o pessoal está treinado para executá-lo.

37. **(CESPE - 2018 - ABIN - Oficial de Inteligência - Área 4)**

A análise de linha do tempo de eventos de interesse forense requer a existência sistematizada de registros de logs dos sistemas periciados para ser realizada, sendo sua aplicação limitada à análise forense de sistemas corporativos que dispõem desses recursos.

38. **(CESPE - 2015 - Telebras - Engenheiro - Engenharia de Redes)**

Os logs de auditoria constituem importante fonte de informação para as análises realizadas por sistemas de detecção de intrusão baseados em hosts.

39. **(CESPE - 2015 - MEC - Gerente de Suporte)**

A gerência da auditoria de segurança engloba, entre outros aspectos, a administração da política de segurança e os procedimentos de recuperação após desastres; além disso, é de responsabilidade dessa gerência a constante atualização com respeito a problemas e riscos de segurança.

---

40. (CESPE - 2014 - TJ-SE - Analista Judiciário - Segurança da Informação)

Conformidade é um conceito relacionado à adesão dos sistemas de informação às políticas e às normas organizacionais de segurança da informação.

---

41. (CESPE - 2014 - TJ-SE - Analista Judiciário - Segurança da Informação)

A execução correta dos procedimentos de segurança da informação, em conformidade com normas e com a política de segurança da empresa, deve ser garantida pelos vários gestores, cada um em sua área.

---

42. (CESPE - 2014 - TJ-SE - Analista Judiciário - Segurança da Informação) Atividades de usuários, exceções e outros eventos são registros ou logs de eventos produzidos e mantidos pela instituição, mas, por constituírem eventos qualitativos, não são objetos apropriados para futuras investigações ou auditorias.

Diretrizes para Software Seguro

43. (CESPE – CNJ/Técnico Judiciário – Programação de Sistemas/2013) Para aumentar a segurança de um programa, deve-se evitar o uso de senhas consideradas frágeis, como o próprio nome e identificador de usuário, sendo recomendada a criação de senhas consideradas fortes, ou seja, aquelas que incluem, em sua composição, letras (maiúsculas e minúsculas), números e símbolos embaralhados, totalizando, preferencialmente, mais de seis caracteres.

---

44. (CESPE – TCE-PA/Auditor de Controle Externo – Informática/2016) Na metodologia de desenvolvimento seguro de software SDL (Security Development Lifecycle), a modelagem de ameaças é realizada na fase de requisitos.

---

45. (CESPE – CNJ/Analista Judiciário – Análise de Sistemas/2013) O SDL é um processo de desenvolvimento de software seguro, que envolve a adição de produtos e atividades, como o desenvolvimento de modelos de ameaças.

---

46. (CESPE – Polícia Federal/Perito Criminal Federal – Cargo 3/2013) O CLASP (Comprehensive, Lightweight Application Security Process) fornece uma taxonomia de vulnerabilidades que podem ocorrer no código-fonte e que podem ser verificadas com o uso de ferramentas automatizadas para análise estática de código.

HORA DE PRATICAR!

LISTA DE QUESTÕES COMPLEMENTARES

Princípios de Segurança

1. **FGV - 2022 - SEFAZ-AM - Analista de Tecnologia da Informação da Fazenda Estadual - Manhã**

A administração de dados deve observar princípios básicos que são largamente adotados pela comunidade segurança da informação. Além da Confidencialidade, Integridade, Disponibilidade e Autenticidade, o princípio da Irretratabilidade completa a lista.

Assinale o significado do princípio da Irretratabilidade.

A Garantia de que os usuários que originam as informações são conhecidos e autorizados, de modo que não possam se passar por terceiros.

B Impossibilidade de negação de que uma pessoa tenha sido autora de uma determinada informação.

C Obrigatoriedade dos agentes pelo zelo com todas as informações coletadas.

D Preservação fidedigna das informações.

E Restrição de acesso às informações apenas aos autorizados.

Comentário:

Vamos aos itens:

a) Estamos falando aqui da prática de controle de acesso com autenticação e autorização. INCORRETO

b) Exatamente pessoal. Lembrando que a irretratabilidade também se aplica ao destinatário, no sentido dele não ser capaz de negar o recebimento da informação. **CORRETO**

c) Estamos falando aqui de processo de cultura organizacional. INCORRETO

d) Temos o princípio da integridade. INCORRETO

e) Novamente, controle de acesso, associado à confidencialidade. INCORRETO

Gabarito: B

---

2. **(FCC – TRE-RR/Analista Judiciário/2015)**

O processo de proteção da informação das ameaças caracteriza-se como Segurança da Informação. O resultado de uma gestão de segurança da informação adequada deve oferecer suporte a cinco aspectos principais:

I. Somente as pessoas autorizadas terão acesso às informações.

II. As informações serão confiáveis e exatas. Pessoas não autorizadas não podem alterar os dados.

III. Garante o acesso às informações, sempre que for necessário, por pessoas autorizadas.

IV. Garante que em um processo de comunicação os remetentes não se passem por terceiros e nem que a mensagem sofra alterações durante o envio.

V. Garante que as informações foram produzidas respeitando a legislação vigente.

Os aspectos elencados de I a V correspondem, correta e respectivamente, a:

a) autenticidade -integridade -disponibilidade - legalidade -confidencialidade.

b) autenticidade -confidencialidade -integridade - disponibilidade -legalidade.

c) integridade -disponibilidade -confidencialidade - autenticidade -legalidade.

d) disponibilidade -confidencialidade -integridade - legalidade -autenticidade.

e) confidencialidade -integridade -disponibilidade - autenticidade -legalidade.

Comentário:

Vimos todas essas características no início do nosso conteúdo de princípios de segurança. Vale mencionar que no item IV, temos a descrição tanto da autenticidade quanto da integridade.

Gabarito: E

---

3. **FGV - 2021 - Banestes - Analista em Tecnologia da Informação - Segurança da Informação**

Um pequeno dispositivo que contém um código de proteção precisa necessariamente ficar conectado à porta USB do computador para que determinado software possa ser utilizado.

Esse dispositivo utilizado para prevenir o uso não autorizado de determinado software é conhecido como:

A Vault;

B Keycloak;

C KeePass;

D Keylogger;

E Hardlock.

Comentário:

Um dongle (HARDLOCK) de proteção de software é um dispositivo de proteção eletrônica contra cópia e proteção de conteúdo. Quando conectados a um computador ou outros eletrônicos, eles desbloqueiam a funcionalidade do software ou decodificam o conteúdo. Ele funciona como uma "chave" que autentica o usuário e protege o software contra cópias e uso não autorizado.

Vamos aos demais itens:

A) INCORRETO. "Vault" geralmente se refere a um local seguro para armazenar informações sensíveis, como senhas e chaves criptográficas.

B) INCORRETO. "Keycloak" é um software de gerenciamento de identidade e acesso de código aberto, que fornece serviços de autenticação e autorização.

C) INCORRETO. "KeePass" é um gerenciador de senhas de código aberto que armazena credenciais de usuário criptografadas. Embora possa ajudar a proteger informações de acesso, não se refere a um dispositivo físico que precisa ser conectado à porta USB para utilizar um software específico.

D) INCORRETO. "Keylogger" é um tipo de software ou hardware malicioso que registra as teclas pressionadas pelos usuários, com o objetivo de roubar informações confidenciais, como senhas e números de cartão de crédito.

Gabarito: E

---

4. (FCC – TRE-RR/Analista Judiciário/2015)

O processo de proteção da informação das ameaças caracteriza-se como Segurança da Informação. O resultado de uma gestão de segurança da informação adequada deve oferecer suporte a cinco aspectos principais:

I. Somente as pessoas autorizadas terão acesso às informações.

II. As informações serão confiáveis e exatas. Pessoas não autorizadas não podem alterar os dados.

III. Garante o acesso às informações, sempre que for necessário, por pessoas autorizadas.

IV. Garante que em um processo de comunicação os remetentes não se passem por terceiros e nem que a mensagem sofra alterações durante o envio.

V. Garante que as informações foram produzidas respeitando a legislação vigente.

Os aspectos elencados de I a V correspondem, correta e respectivamente, a:

a) autenticidade -integridade -disponibilidade - legalidade -confidencialidade.

b) autenticidade -confidencialidade -integridade - disponibilidade -legalidade.

c) integridade -disponibilidade -confidencialidade - autenticidade -legalidade.

d) disponibilidade -confidencialidade -integridade - legalidade -autenticidade.

e) confidencialidade -integridade -disponibilidade - autenticidade -legalidade.

Comentário:

Vimos todas essas características no início do nosso conteúdo de princípios de segurança. Vale mencionar que no item IV, temos a descrição tanto da autenticidade quanto da integridade.

Gabarito: E

---

5. **FGV - 2020 - IBGE - Agente Censitário Operacional - Reaplicação**

Considere as seguintes regras para a composição de senhas de 4 caracteres:

I. Dois dígitos numéricos + duas letras maiúsculas;

II. Quatro letras minúsculas;

III. Quatro dígitos numéricos;

IV. Três letras minúsculas + um dígito numérico;

V. Uma letra minúscula + três dígitos numéricos.

A regra que permite a criação de senhas mais fortes é:

A I;

B II;

C III;

D IV;

E V.

Comentário:

Temos aqui muito mais uma questão de probabilidade e estatística, do que de segurança em si.

Pessoal, quanto mais possibilidade temos de gerar caracteres diferentes e na combinação deles, senhas diferentes, teremos maior robustez.

Sendo assim, quando indicamos que um campo suporta apenas números, temos 10 opções (0 a 10). Quando falamos de letras, temos 26 possibilidades de minúsculas e outras 26 de maiúsculas, a depender do alfabeto suportado. Sendo assim, quando colocamos quatro opções de letras minúsculas, teremos 26x26x26x26 como total de combinações possíveis.

Gabarito: B

---

6. FGV - 2018 - AL-RO - Analista Legislativo - Infraestrutura de Redes e

No contexto da Segurança da Informação, o primeiro controle de acesso a ser estabelecido, isto é, a primeira barreira de segurança deve ser o controle de acesso

A lógico.

B físico.

C por nome de usuário (login) e senha.

D por DMZ.

E por criptografia.

Comentário:

Pessoal, sem dúvida, a boa prática traz a primeira camada física de proteção como referência. Estamos falando aqui de controles em portarias, hall de entrada, garagens, seja com estruturas que envolvem pessoas ou não. Todas as demais são recursos a serem implantados em novas camadas de segurança.

Gabarito: B

---

7. FGV - 2018 - MPE-AL - Técnico do Ministério Público - Tecnologia da Informação

Em muitas transações financeiras realizadas pela Internet é necessário que o usuário, além de fornecer o seu e-mail e senha, digite um código gerado ou recebido em seu celular. Essa tecnologia é conhecida como

A biometria.

B cartão inteligente.

C certificado digital.

D criptografia.

E token de segurança.

Comentário:

Estamos falando dos recursos associados aos múltiplos fatores de segurança da informação. Assim, quando se tem uma mensagem enviada ao celular, estamos tratando de uma camada de segurança de algo que você tem, sendo também referenciado como token de segurança para validação do usuário.

Gabarito: E

---

8. FGV - 2017 - SEPOG - RO - Analista em Tecnologia da Informação e Comunicação

O reconhecimento biométrico consiste em reconhecer um indivíduo com base nas suas características físicas ou comportamentais.

A técnica adotada pelo sistema de identificação biométrico que implica em detectar e comparar a posição das minúcias (minutiae), também conhecida como características de Galton, é utilizada no reconhecimento da

A impressão digital.

B íris.

C retina.

D face.

E voz.

Comentário:

Vamos aos itens:

A) **CORRETO**. A técnica que detecta e compara a posição das minúcias (minutiae) ou características de Galton é utilizada no reconhecimento de impressões digitais. As minúcias são pontos específicos das impressões digitais, como bifurcações e terminações de cristas, que são únicos para cada indivíduo e podem ser utilizados para identificá-los de forma confiável.

B) INCORRETO. O reconhecimento da íris se baseia na análise das características únicas da íris de um indivíduo, como padrões de cores, estruturas e texturas. Essa técnica não utiliza minúcias para realizar a identificação.

C) INCORRETO. O reconhecimento de retina envolve a análise dos padrões de vasos sanguíneos da retina, que são únicos para cada indivíduo. A técnica de minúcias não é aplicada nesse método de reconhecimento biométrico.

D) INCORRETO. O reconhecimento facial analisa características faciais específicas, como distâncias entre os olhos, formato do nariz e contorno dos lábios. A técnica de minúcias não é empregada nesse tipo de reconhecimento biométrico.

E) INCORRETO. O reconhecimento de voz utiliza características comportamentais, como a frequência, tom e ritmo da fala, para identificar um indivíduo. A técnica de minúcias não é relevante para o reconhecimento de voz.

Gabarito: B

---

9. (FCC – TRE-CE/Analista Judiciário – Análise de Sistemas/2012) Em relação à segurança da informação, considere:

I. Capacidade do sistema de permitir que alguns usuários acessem determinadas informações, enquanto impede que outros, não autorizados, sequer as consultem.

II. Informação exposta, sob risco de manuseio (alterações não aprovadas e fora do controle do proprietário da informação) por pessoa não autorizada.

III. O sistema deve ter condições de verificar a identidade dos usuários, e este ter condições de analisar a identidade do sistema.

Os itens I, II e III, associam-se, direta e respectivamente, aos princípios de

a) confidencialidade, integridade e autenticidade.

b) autenticidade, confidencialidade e irretratabilidade.

c) confidencialidade, confidencialidade e irretratabilidade.

d) autenticidade, confidencialidade e autenticidade.

e) integridade, confidencialidade e integridade.

---

10. (FCC – TRE-CE/Técnico Judiciário – Programação de Sistemas/2012) A propriedade que garante que nem o emissor nem o destinatário das informações possam negar a sua transmissão, recepção ou posse é conhecida como

a) autenticidade.

b) integridade.

c) irretratabilidade.

d) confidenciabilidade.

e) acessibilidade.

---

11. (FCC – TJ-AP/Analista Judiciário – Banco de Dados/2014) O controle de acesso à informação é composto por diversos processos, dentre os quais, aquele que identifica quem efetua o acesso a uma dada informação. Esse processo é denominado

a) autenticação.

b) auditoria.

c) autorização.

d) identificação.

e) permissão.

12. (FCC – TRF 4ª Região / Analista Judiciário – Informática/2014) José deve estabelecer uma política de segurança e implantar os mecanismos de segurança para o TRF da 4a Região. Dentre os mecanismos para a segurança física, José deve escolher o uso de

a) senha de acesso ao computador do trf.

b) token criptográfico para autenticar os dados acessados no computador do trf.

c) senha de acesso às páginas web do trf.

d) cartão de acesso para as pessoas que entram no trf.

e) criptografia na troca de informações entre os computadores do trf.

---

13. (FCC – SABESP/Analista de Gestão – Sistemas/2014) Todos os procedimentos de segurança listados abaixo referem-se a controles de acesso lógico, EXCETO:

a) utilizar mecanismos de time-out automático, isto é, desativar a sessão após um determinado tempo sem qualquer atividade no terminal ou computador. para restaurá-la, o usuário é obrigado a fornecer novamente seu id e senha.

b) definir o controle de acesso nas entradas e saídas através de travas, alarmes, grades, vigilante humano, vigilância eletrônica, portas com senha, cartão de acesso e registros de entrada e saída de pessoas e objetos.

c) utilizar logs como medidas de detecção e monitoramento, registrando atividades, falhas de acesso (tentativas frustradas de logon ou de acesso a recursos protegidos) ou uso do sistema operacional, utilitários e aplicativos, e detalhando o que foi acessado, por quem e quando.

d) definir as permissões e os privilégios de acesso para cada recurso ou arquivo no sistema. quando um usuário tenta acessar um recurso, o sistema operacional verifica se as definições de acesso desse usuário e do recurso desejado conferem. o usuário só conseguirá o acesso se essa verificação for positiva.

e) limitar o número de tentativas de logon sem sucesso e limitar o horário de uso dos recursos computacionais de acordo com a real necessidade de acesso aos sistemas. pode-se, por exemplo, desabilitar o uso dos recursos nos fins de semana ou à noite.

---

14. (FCC – TCE-GO/Analista de Controle Externo/2014) Pedro trabalha na área que cuida da Segurança da Informação de uma empresa. Frente ao risco de indisponibilidade de uma aplicação, criou um servidor de backup para tentar garantir que as informações sejam replicadas, automaticamente, do servidor principal para o servidor backup de forma redundante. A estratégia utilizada por Pedro para tratar o risco é considerada como

a) aceitação do risco.

b) transferência do risco.

c) eliminação do risco.

d) especificação do risco.

e) mitigação do risco.

---

15. (FCC – TRT – 6ª Região (PE)/Analista Judiciário - TI/2018) A gerência de riscos na segurança da informação inclui o uso de diversos tipos e recursos de segurança. Um recurso de segurança categorizado como mecanismo de controle de acesso lógico é

a) a função hash.

b) o sistema biométrico.

c) a catraca eletrônica.

d) o sistema de detecção de intrusão.

e) o sniffer.

---

16. (FCC – TRF – 4ª Região/Técnico Judiciário/2014) Os sistemas de identificação biométricos funcionam através da comparação de características físicas apresentadas por um usuário com as correspondentes armazenadas em um determinado banco de dados, identificando-o ou não como um dos usuários cadastrados, dificultando sobremaneira as fraudes praticadas contra as várias formas de verificação de identidades. O sistema de identificação biométrica que utiliza a parte do fundo do olho como identificador é conhecido como identificação

a) datiloscópica ou fingerprint.

b) da íris

c) da retina.

d) cognitiva.

e) teclar.

---

17. (FCC - 2013 - SEFAZ-SP - Agente Fiscal de Rendas - Gestão Tributária - Prova 3) A auditoria da segurança da informação avalia a política de segurança e os controles relacionados adotados em cada organização. Nesse contexto, muitas vezes, as organizações não se preocupam, ou até negligenciam, um aspecto básico da segurança que é a localização dos equipamentos que podem facilitar a intrusão. Na auditoria de segurança da informação, esse aspecto é avaliado no Controle de:

a) acesso lógico.
b) acesso físico.
c) programas.
d) conteúdo.
e) entrada e saída de dados.

GABARITO

Gabarito – Questões CESPE

1	C
2	A
3	E
4	E
5	C
6	C
7	E
8	C
9	C
10	E
11	E
12	E
13	E
14	E
15	E
16	C

17	C
18	C
19	C
20	E
21	C
22	C
23	C
24	C
25	E
26	A
27	E
28	E
29	E
30	D
31	E
32	E
33	E
34	C
35	E
36	C
37	E
38	C
39	E
40	C
41	C
42	E
43	C
44	E
45	C
46	C

Gabarito – Questões Complementares

1	B
2	E
3	E
4	E
5	B
6	B
7	E
8	B

9	A
10	C
11	A
12	D
13	B
14	E
15	B
16	C
17	B
18	
19	
20	

RESUMO

- **PRINCÍPIOS DE SEGURANÇA**

  - Três principais **pilares que compõem a base da Segurança da Informação**, quais sejam:

    - **Confidencialidade** – Aqui temos o princípio que visa **zelar pela privacidade** e sigilo dos dados de tal modo que estes devem ser acessados ou visualizados somente por aqueles de direito, ou seja, a informação só deve estar disponível para aqueles com a devida autorização.
    - **Integridade (Confiabilidade)** – No segundo princípio, temos como objetivo garantir que os **dados trafegados sejam os mesmos** do início ao fim de um determinado trecho, ou seja, que a mesma mensagem gerada na origem chegue ao destino de forma intacta.
    - **Disponibilidade** – Nesse princípio, temos como principal objetivo o fato de determinado **recurso poder ser utilizado** quando este for requisitado em um determinado momento, considerando a devida autorização do usuário requisitante.

  - **Segurança de Redes:** O Cert.br, principal órgão do Brasil responsável pelo fomento **à Segurança da Informação**, nos traz alguns conceitos que são constantemente explorados pelas bancas examinadoras. Nesse sentido, vamos conhecê-los:

    - **Furto de dados:** informações pessoais e outros dados podem ser obtidos tanto pela interceptação de tráfego como pela exploração de possíveis vulnerabilidades existentes em seu computador;

    - **Uso indevido de recursos:** um atacante pode ganhar acesso a um computador conectado à rede e utilizá-lo para a prática de atividades maliciosas, como obter

arquivos, disseminar spam, propagar códigos maliciosos, desferir ataques e esconder a real identidade do atacante;

- **Varredura:** um atacante pode fazer varreduras na rede, a fim de descobrir outros computadores e, então, tentar executar ações maliciosas, como ganhar acesso e explorar vulnerabilidades;

- **Interceptação de tráfego:** um atacante, que venha a ter acesso à rede, pode tentar interceptar o tráfego e, então, coletar dados que estejam sendo transmitidos sem o uso de criptografia;

- **Exploração de vulnerabilidades:** por meio da exploração de vulnerabilidades, um computador pode ser infectado ou invadido e, sem que o dono saiba, participar de ataques, ter dados indevidamente coletados e ser usado para a propagação de códigos maliciosos. Além disto, equipamentos de rede (como modems e roteadores) vulneráveis também podem ser invadidos, terem as configurações alteradas e fazerem com que as conexões dos usuários sejam redirecionadas para sites fraudulentos;

- **Ataque de negação de serviço:** um atacante pode usar a rede para enviar grande volume de mensagens para um computador, até torná-lo inoperante ou incapaz de se comunicar;

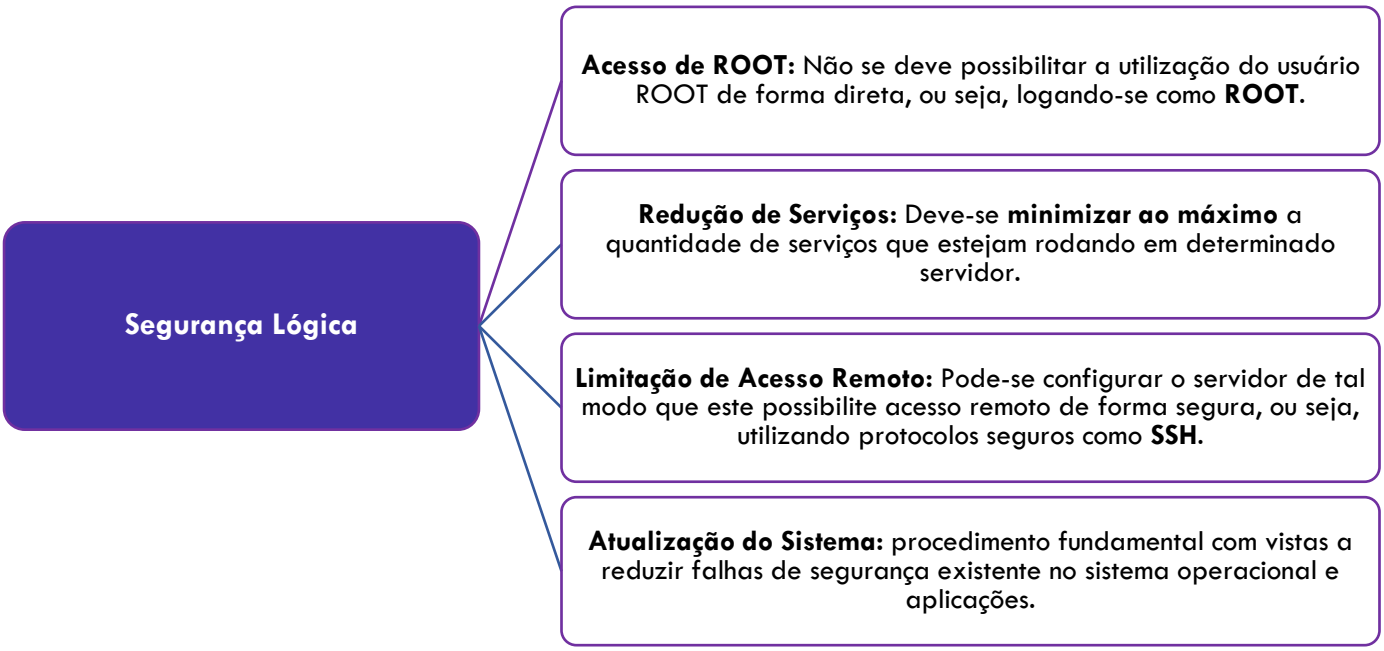
- **Ataque de força bruta:** computadores conectados à rede e que usem senhas como métodos de autenticação estão expostos a ataques de força bruta. Muitos computadores, infelizmente, utilizam, por padrão, senhas de tamanho reduzido e/ou de conhecimento geral dos atacantes;

- **Ataque de personificação**: um atacante pode introduzir ou substituir um dispositivo de rede para induzir outros a se conectarem a este, ao invés do dispositivo legítimo, permitindo a captura de senhas de acesso e informações que por ele passem a trafegar;

- **SEGURANÇA FÍSICA, LÓGICA E CONTROLE DE ACESSO:** A **física diz respeito aos aspectos tangíveis** e que, de fato, podem ser tocados, enquanto a **lógica está relacionada aos dados em seu formato analógico ou digital**, tanto no aspecto de transmissão, processamento e armazenamento.

  - **Segurança Física:** exemplos de elementos que são considerados como recursos para a segurança física: ***unidade de alimentação ininterrupta (UPS), gerador, site físico redundante, CFTV, travas de equipamentos, alarmes, catracas, sala cofre.***

  - **Segurança Lógica:**



- **Controle de Acesso:** método aplicado tanto no contexto físico e lógico, com vistas a estabelecer **barreiras que podem restringir determinados acessos a locais**, equipamentos, serviços e dados a pessoas. O controle de acesso está diretamente ligado ao princípio da autenticidade e autorização. Três técnicas de controle e gerenciamento de acesso: *Mandatory Access Control (MAC), Role-Based Access Control (RBAC), Discretionary Access Control (DAC).*

- **AUTENTICAÇÃO E SEUS MECANISMOS:** os mecanismos de autenticação são procedimentos, rotinas, ferramentas ou soluções que implementam, de fato, o princípio de autenticação com o devido controle de acesso.

  - **SAML - Security Assertion Markup Language:** não é uma tecnologia em si, mas sim, um padrão aberto que **permite com que provedores de serviços e recursos de identidade passe credenciais de autorização** para provedores de serviços.
  - **OAuth:** o padrão foi concebido no nicho privado, em conjunto pela Google e pelo Twitter, permitindo assim **logins simplificados e integrados a múltiplos serviços na Internet**.
  - **Biometria:** forma de identificar de maneira única um indivíduo por meio de suas características físicas ou comportamentais.

- **SEGURANÇA EM ENDPOINTS**

  - Na prática, **se o dispositivo está conectado à rede em alguma medida, com a capacidade de processar informação e trafegar dados,** poderá ser classificado como um ENDPOINT.

- Dentre alguns recursos e contextos de aplicação das soluções voltadas para segurança em EndPoints, podemos citar **Antivírus, Antimalwares, firewalls, HIDS e HIPS, Atualizações diversas de drivers, softwares e S.O., entre outros**.

AUDITORIA E CONFORMIDADE

- **Auditoria:** a auditoria em tecnologia da informação diz respeito à análise cuidadosa e sistemática dos recursos de TI, pessoas, documentos, sistemas, entre outros, no intuito de se averiguar se estes estão de acordo com aquilo que fora planejado ou em relação às atividades e comportamentos definidos como padrão. Avalia-se quanto à sua eficácia e eficiência em torno dos objetivos e resultados esperados.

- **Conformidade:** conceito relacionado à adesão dos sistemas de informação às políticas e às normas organizacionais de segurança da informação.

CONTINUIDADE DE NEGÓCIOS

- ISO 27002 sobre o **objetivo da Gestão da Continuidade de Negócios:** "não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos, e assegurar a sua retomada em tempo hábil, se for o caso"
- O **PCN – Plano de Continuidade de Negócios** é o documento responsável por consolidar as ações para continuidade do negócio. **Todos os riscos envolvidos**, no que tange às suas probabilidades e impactos devem ser analisados. O PCN possui como foco tanto o capital intelectual (informações), bem como suas instalações.

PRINCÍPIOS DE NORMAS E PADRÕES

- **Gerência de Riscos:** Existem algumas formas básicas de como a organização deve reagir aos riscos. Pode-se tomar basicamente quatro tipos de ação, quais sejam:
  - **Evitar –** Busca-se ações com vistas a prevenir a ocorrência de determinado risco. Como exemplo, pode-se bloquear o acesso de determinado usuário à internet. Isso poderia evitar que este acesse serviços remotamente e vaze dados pela Internet.

  - **Transferir –** Busca-se transferir o risco para uma terceira parte. Nesse caso, a terceira parte assume a responsabilidade das ações frente ao risco, bem como custos e outros fatores. Analogia simples ao seguro de carro que fazemos, passando o risco de acidente e roubo para a seguradora.

  - **Mitigar –** Objetiva-se atuar em prol da minimização dos riscos. Como exemplo, pode-se restringir o acesso de determinados usuários a sites controlados.

- **Aceitar ou Reter –** Determinados riscos não valem a penas ser evitados, mitigados ou transferidos por agregar custos ou esforços extremamente elevados que, em termos quantitativos, são maiores que os dados ou informação em análise. Desse modo, aceita-se o risco em caso de ocorrência.

- **DIRETRIZES PARA O DESENVOLVIMENTO DE SOFTWARE SEGURO**

  - **SDL (Security Development Lifecycle):** metodologia criada pela Microsoft para o desenvolvimento de softwares que precisam suportar ataques de usuários mal-intencionados.
  - **CLASP (Comprehensive, Lightweight Application Security Process):** metodologia de desenvolvimento seguro de software orientada a atividades e papéis, que descreve melhores práticas para projetos novos ou em andamento.
  - **SAST (Static Application Security Testing):** em sua tradução literal, "aplicação estática para teste de segurança". O propósito é avaliar o código fonte e as diversas versões compiladas para buscar identificar brechas de segurança.
  - **DAST (Dynamic Application Security Testing):** utilizado para fins de verificação de compliance de segurança e padrões internacionais da indústria, bem como para geração de releases e evoluções do software após seu lançamento.

CONSIDERAÇÕES FINAIS

Bom pessoal, encerramos a nossa primeira aula (AULA 00 - demonstrativa)!

Espero que tenham gostado!

As demais aulas estarão disponíveis em breve conforme cronograma proposto e espero poder caminhar junto com vocês em busca da aprovação.

Aguardo vocês nas próximas aulas!

Vamos juntos?

Um grande abraço.
Prof. André Castro.

 **Instagram: @ProfAndreCastro**  **Telegram: t.me/ProfessorAndreCastro**

ESSA LEI TODO MUNDO CONHECE:
PIRATARIA É CRIME.

Mas é sempre bom revisar o porquê e como você pode ser prejudicado com essa prática.

1. 

Professor investe seu tempo para elaborar os cursos e o site os coloca à venda.

2. 

Pirata divulga ilicitamente (grupos de rateio), utilizando-se do anonimato, nomes falsos ou laranjas (geralmente o pirata se anuncia como formador de "grupos solidários" de rateio que não visam lucro).

3. 

Pirata cria alunos fake praticando falsidade ideológica, comprando cursos do site em nome de pessoas aleatórias (usando nome, CPF, endereço e telefone de terceiros sem autorização).

4. 

Pirata compra, muitas vezes, clonando cartões de crédito (por vezes o sistema anti-fraude não consegue identificar o golpe a tempo).

5. 

Pirata fere os Termos de Uso, adultera as aulas e retira a identificação dos arquivos PDF (justamente porque a atividade é ilegal e ele não quer que seus fakes sejam identificados).

6. 

Pirata revende as aulas protegidas por direitos autorais, praticando concorrência desleal e em flagrante desrespeito à Lei de Direitos Autorais (Lei 9.610/98).

7. 

Concurseiro(a) desinformado participa de rateio, achando que nada disso está acontecendo e esperando se tornar servidor público para exigir o cumprimento das leis.

8. 

O professor que elaborou o curso não ganha nada, o site não recebe nada, e a pessoa que praticou todos os ilícitos anteriores (pirata) fica com o lucro.

Deixando de lado esse mar de sujeira, aproveitamos para agradecer a todos que adquirem os cursos honestamente e permitem que o site continue existindo.