Aula 00 (Prof. André Castro)

ANM (Cargo 25: Especialista em Recursos Minerais - Tecnologia da Informação - Governança e Inovação) Segurança da Informação - 2024 (Pós-Edital)

Autor:
André Castro

29 de Novembro de 2024

Índice

APRESENTAÇÃO

Olá, pessoal! Como estão? Espero que bem e animados para essa jornada.

Aqui é o André Castro, professor de Redes de Computadores e Segurança da Informação do Estratégia Concursos. Sou formado em Engenharia de Redes de Comunicação pela Universidade de Brasília – UnB e pós-graduado na área de Segurança e Administração de Redes também pela UnB.

Atualmente, após um ciclo de 14 anos no serviço público como servidor público, fiz uma transição de carreira para o setor privado. Hoje, estou exercendo a função de Estrategista de Governo e Especialista em Transformação Digital na Microsoft Brasil, em Brasília.

Na trajetória de Governo, exerci o último cargo de Analista em Tecnologia do Ministério da Economia ou atual Ministério da Gestão e Inovação, tendo exercido cargos de relevância à frente de unidades de tecnologia do Governo Federal. No último ciclo de Governo, estive como Assessor Especial de Tecnologia na AGU e antes disso, atuei como Subsecretário/CIO de Tecnologia da Informação do Ministério da Educação.

Fui aprovado ainda nos concursos de Analista Administrativo da Câmara dos Deputados, realizado em 2011 e aprovado no concurso de Analista para o Banco Central do Brasil em 2013. Exerci ainda atividades de instrução e apoio em alguns cursos na área de Redes e Segurança pela Escola Superior de Redes – ESR, da Rede Nacional de Pesquisa – RNP, além de outros projetos relacionados a concursos públicos, incluindo aulas presenciais.

Para você que se prepara para concursos públicos na área de tecnologia... Pois bem... preparei um material muito bacana e bem completo sobre os assuntos voltados para a nossa temática, que possuem algumas variações a depender do cargo e do concurso, e por isso buscamos trazer uma abordagem bem completa e eficiente para não deixar lacunas e não exceder conteúdos desnecessariamente.

A ideia é que você possa conhecer os tópicos mais importantes e ter uma abordagem diferenciada e com didática adequada para sua preparação. O meu foco é sempre buscar ser o mais preciso possível nos assuntos, otimizando e muito o seu tempo de preparação. Você perceberá isso ao longo do curso.

Abraço,

Prof. André Castro

@profandrecastro

Instagram YouTube

andrecastroprofessor@gmail.com
/professorandrecastro

Também gostaria de convidá-lo a conhecer alguns projetos da equipe de TI:

//estratégia tech ESTRATEGIA CONCURSOS	**Nosso podcast alternativo:** *https://anchor.fm/estrategia-tech*
Telegram a new era of messaging	**Nosso grupo do Telegram:** ***https://t.me/estrategia_ti***
Instagram	**Perfil no Instagram:** *http://instagram.com/estrategiaconcursosti*

Informações Gerais

É nítida a evolução conjunta das partes envolvidas em concursos públicos, uma vez que temos provas cada vez mais difíceis, com um nível maior de inteligência e preparação das questões, bem como o surgimento constante de novos conceitos e abordagens.

Além disso, o nível dos candidatos que têm concorrido às vagas de cargos públicos tem aumentado e tende a continuar aumentando, como se pode verificar pela simples análise das melhores notas obtidas em diversos concursos.

A preparação para concursos considerados de médio e alto nível demanda tempo e dedicação prévia.

Quando você tiver se preparando para o seu concurso, seja com edital ou não, tenho a intenção de possibilitar ao candidato a preparação, especificamente para o propósito a que propomos, bem como para os mais diversos editais na área de TI. A minha expectativa é que os nossos alunos estejam passos à frente dos demais candidatos nessa fase de preparação.

Informações Sobre o Curso

Abordaremos nesse curso todos os tópicos apresentados em nosso cronograma. Faremos juntos muitos exercícios para fixação do conteúdo ao final de cada aula, sempre de forma objetiva, prática e complementar.

Entretanto, gostaria de lembrar da dificuldade de esgotar as possibilidades de cada assunto até o seu nível máximo de detalhe em cada aula por se tratar de assuntos demasiadamente extensos.

O ponto chave de cada assunto é entender o perfil da banca e o perfil do órgão para o qual a banca está prestando o serviço. Diante disso, buscarei estar alinhado a esses pontos para direcioná-los da melhor forma possível, realizando diversos exercícios, principalmente dos últimos concursos ou concursos equivalentes. Contem comigo para isso!

Ressalto ainda o meu compromisso de buscar cumprir o cronograma da melhor maneira possível. No entanto, ao longo do curso, posso identificar alguns ajustes na ordem da apresentação dos conteúdos ou ainda a necessidade de adaptação a alguma alteração do Edital em caso de divulgação, portanto, digo a vocês que o cronograma não é de todo rígido.

Desde já eu agradeço a confiança de cada um de vocês e tenham certeza que esse curso irá auxiliá-los bastante nessa jornada. Não deixem de me procurar no fórum para esclarecimentos de dúvidas, por favor!

Não deixem acumular lacunas em seu aprendizado pois a "*lei de Murphy*" se aplica aqui...!!! Vai ser exatamente essa lacuna que será cobrada na prova e você vai se arrepender depois de não ter perguntado. *Digo por experiência própria!*

Críticas, reclamações, sugestões, comentários ou identificação de erros de digitação podem ser enviados para o nosso fórum. Tentarei responder com a maior brevidade possível.

Informações Sobre as Aulas

Apresento a vocês algumas metodologias adotadas em nossas aulas que aprendi ao estudar para concursos e que me ajudaram bastante, bem como no compartilhamento de experiências com outros professores:

1 - Parágrafos curtos e objetivos: Sempre que possível, os parágrafos serão reduzidos para facilitar a leitura e não a tornar cansativa, buscando sempre maior fluidez. O cronograma também segue esse princípio, deixando as aulas objetivas e eficazes em termos de organização e extensão do conteúdo. *De repente vocês terão tempo até para estudar as demais outras matérias...!!!*

2 - Entender o Básico (Princípios e Fundamentos): *Isso não é óbvio André?* Não, não é! Muitas das vezes nos preocupamos em aprender ou "decorar" os detalhes de determinada disciplina ou matéria, buscar tabelas e figuras para memorizar e esquecemos os princípios, o básico, aquilo que com certeza te ajudará a entender os detalhes. Portanto, estejam atentos a isso, por favor, ok?

3 - Linguagem Comum: Tentarei fazer com que a sua leitura se aproxime de um diálogo ou uma aula expositiva e presencial. O objetivo é não deixar a leitura cansativa para aqueles que talvez tenham dificuldades com leituras extensas, como eu. Combinado?

4 - Exercícios: Ler por si só já é bem cansativo. Imagina leituras bibliográficas, como o livro do Tanembaum, Forouzan ou Kurose com mais de 600 páginas? Convenhamos, né? Na maioria das vezes não vale a pena, a não ser para dúvidas pontuais e consolidação de determinado conteúdo. Além disso, deixe esse trabalho comigo, a não ser que você tenha tempo sobrando. Invista seu tempo em uma boa leitura do material e principalmente na resolução de exercícios!!!

A essência dos exercícios muitas vezes se repete, portanto, se você já tiver feito muitos, mas muitos exercícios, é provável que você se depare com questões iguais ou semelhantes nas provas seguintes.

Utilizarei exercícios também para esclarecer ou mencionar algum ponto que tenha passado na parte teórica. Vamos nos esforçar para que você precise de apenas mais uma prova para sua aprovação, certo?

Focaremos nos exercícios da Banca Examinadora do Concurso. Porém, sempre que houver necessidade, seja para complementarmos o conteúdo ou por falta de exercícios da banca sobre determinada matéria, utilizaremos exercícios de outras bancas também.

5 - Artifícios Complementares: O conteúdo de redes possui a vantagem de ter muita figura ilustrativa, o que nos ajuda a entender o conteúdo. Então sempre buscarei trazer figuras, imagens, tabelas e diagramas para tornar a leitura mais saudável e clara. Geralmente, é mais fácil memorizar uma figura ilustrativa do que puramente o conteúdo escrito.

6 - Linhas Destacadas em vermelho: Utilizarei esse recurso de destaque em negrito e vermelho das palavras e frases que são mais importantes dentro de alguns parágrafos para uma posterior leitura vertical (Segunda leitura do material com o objetivo de revisão dos pontos destacados).

7 - Revisão em Exercícios: Pessoal, a tendência é que nos assuntos iniciais, façamos a leitura e façamos os exercícios com um bom índice de acerto, pois você ainda estará com a memória fresca. Porém, tal índice nem sempre se mantém após semanas da leitura daquele conteúdo.

Portanto, é muito importante que estejam sempre voltando e fazendo alguns exercícios avulsos para fixar o conhecimento, além do que, será a oportunidade para descobrir onde você está tendo mais dificuldade de memorização e aprendizado.

ATENÇÃO

As videoaulas estão sendo constantemente gravadas e, dessa forma, não há garantia de que teremos todo o conteúdo disponível em vídeo. Então seu curso pode ou não ter as gravações a depender do edital.

Mas tenham certeza de que tudo e mais um pouco estará em seus PDF's.

Ufa, chega de apresentações e informações, certo? Vamos ao que interessa! Procurem estar descansados e tranquilos com vistas a obter uma leitura suave do conteúdo para otimizarmos os resultados das nossas aulas.

ESTRATÉGIA FLASHCARDS

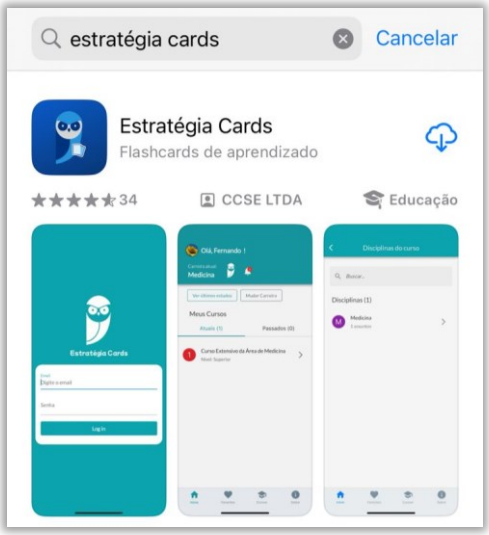
📚 Você tem dificuldade de estudar, memorizar e revisar os conteúdos que estuda em nossas aulas? Então nós temos a ferramenta perfeita para você!

Apresentamos o **Estratégia Cards**: app de flashcards que vai revolucionar sua forma de **estudar** e **revisar** conteúdos de provas de concurso público. Com nossa tecnologia inovadora e interface amigável, você dominará os tópicos mais complexos de maneira eficiente e divertida.

✨ Recursos do Estratégia Cards:

Curadoria de Flashcards	Flashcards criados e revisados por professores especializados em cada área, com qualidade e voltados para concursos públicos.
Flashcards Personalizados	Crie seus próprios flashcards, cobrindo os principais tópicos e matérias dos concursos públicos.
Repetição Espaçada	Técnica de aprendizagem que envolve revisar informações em intervalos crescentes para melhorar a retenção de longo prazo e combater o esquecimento.
Estatísticas Personalizadas	Visualize graficamente o percentual de acertos, erros ou dúvidas dos decks estudados.
Modo Offline	Estude em qualquer lugar, mesmo sem conexão à internet, fazendo o download dos decks.
Estudo por Áudio	*Está dirigindo ou fazendo esteira e quer continuar estudando?* Basta utilizar a opção "Escutar".
Decks Favoritos	Você pode escolher decks específicos como favoritos e visualizá-los em uma aba separada do app.
Opções de Estudo	Você poderá estudar todos os cards de um deck; ou apenas os que você errou; ou apenas os que você não estudou ainda; entre outras opções.

E como eu consigo baixar?



É muito fácil! Basta pesquisar por "Estratégia Cards" na loja oficial do seu smartphone.

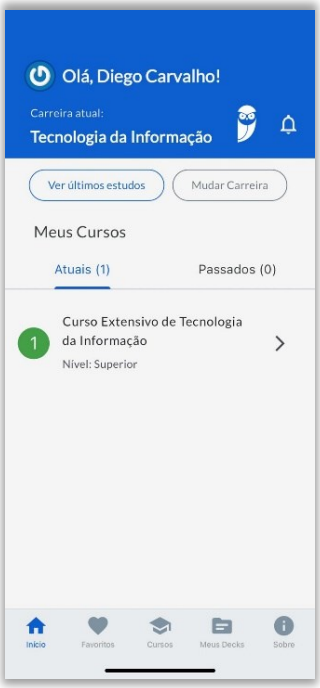
Se você tiver um Android, basta acessar a **Google Play**;

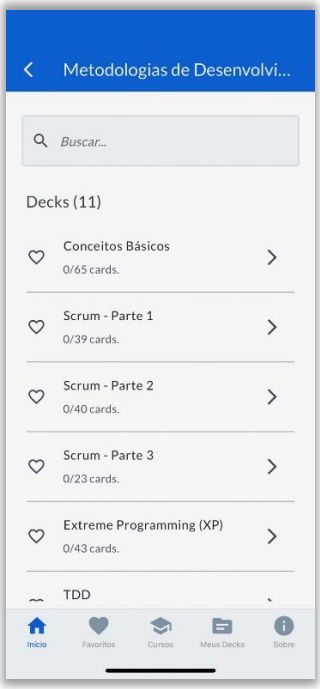
Se for tiver um iPhone, basta acessar a **App Store (iOS)**.

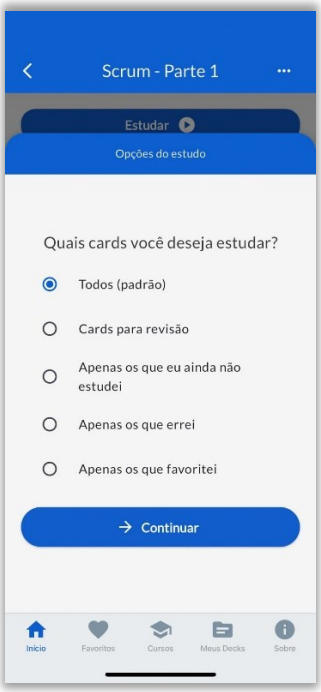
E para acessar?

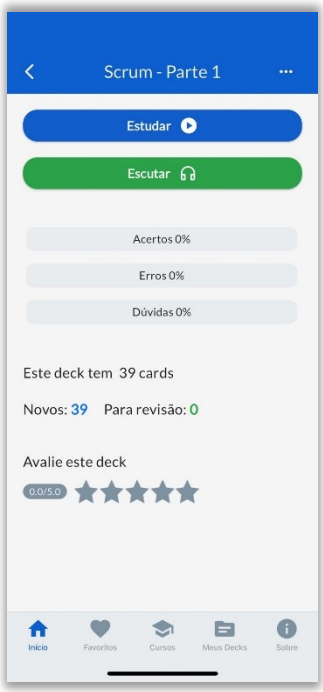
Para acessar, basta ter uma conta no Estratégia Concursos. Em seguida, utilize suas credenciais de login e senha para acessar o aplicativo. Por fim, acessa a carreira de Tecnologia da Informação.

Como utilizar o app:









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:

- Confidencialidade – Aqui temos o princípio que visa zelar pela privacidade e sigilo dos dados de tal modo que estes devem ser acessados e 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 teremos 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

- 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 violação do princípio da integridade.

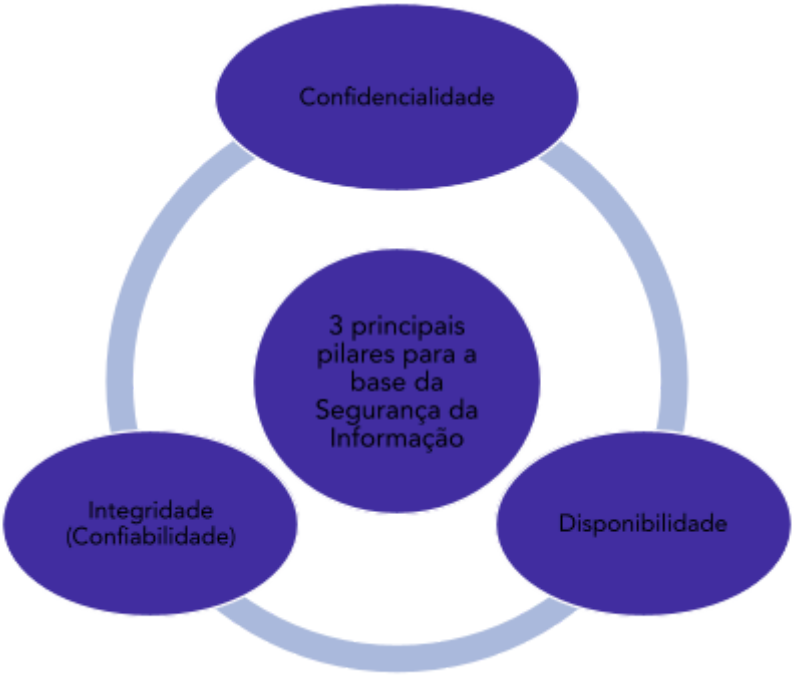
Agora, caso a pessoa altere a mensagem, teremos sim um problema de integridade dos dados.

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.

- Disponibilidade – Neste 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. 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.



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

- 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 mais 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.

CESPE-2020 - SEFAZ/AL - 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

- 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

- Irretroatividade – Um outro princípio importante diretamente associado ao processo de autenticidade, integridade e não repúdio é a Irretroatividade, ou seja, não é possível reverter o ato ou questionar a data/momento da sua realização. Na prática, ela estabelece que não é possível reverter um evento ou ação uma vez que ele tenha sido executado e registrado. Este princípio é importante para garantir a integridade dos dados e a confiabilidade dos sistemas de informação.

Podemos citar como exemplos:

- Uma vez que uma transação é registrada em um blockchain, não é possível alterá-la ou excluí-la.
- Uma vez que um certificado digital é emitido, não é possível revogá-lo retroativamente.
- Uma vez que um documento é assinado com certificado digital e assinatura digital, não é possível revertê-lo em termos do ato e do tempo.

- 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.

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 disso, 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

Questões Comentadas - Princípios de Segurança - CESPE

1. CEBRASPE (CESPE) - Tec (CNMP)/CNMP/Apoio Técnico Administrativo/Segurança Institucional/2023

São princípios da segurança da informação, entre outros, a confidencialidade, a integridade e a disponibilidade.

Comentários:

Questão bem básica, e que traz, de fato, alguns dos principais princípios. Da base principal, ficou de fora apenas a autenticidade.

Gabarito: C

2. CEBRASPE (CESPE) - Ana (SERPRO)/SERPRO/Tecnologia/2023

A integridade é uma propriedade que visa aplicar conhecimentos e habilidades para garantir a assinatura digital.

Comentários:

Temos uma inversão de conceitos. Na prática, a assinatura digital é que garante a autenticidade e integridade.

Gabarito: E

3. CEBRASPE (CESPE) - Per Crim (POLC AL)/POLC AL/Análise de Sistemas, Ciências da Computação, Informática. Processamento de Dados ou Sistemas da Informação/2023

A confidencialidade trata da proteção de dados contra ataques passivos e envolve mecanismos de controle de acesso e criptografia.

Comentários:

Importante a gente lembrar que os ataques passivos são aqueles que não alteram ou interferem no fluxo de dados. Ou seja, escutas ou interceptações apenas para coleta e leitura das informações, sem sua alteração, caracteriza esse tipo de ataque.

Já a confidencialidade é aquele princípio que justamente visa garantir o sigilo dos dados. Então, a questão está adequada em seus conceitos, e também na referência a práticas de segurança como os controles de acesso e criptografia, que visam restringir o acesso às informações e/ou, ainda que alguém tenha acesso, não consiga interpretá-las.

Alguns exemplos de ataques passivos:

Exemplos:

- Eavesdropping: Interceptação de dados em redes sem fio ou com fio.
- Análise de tráfego: Monitoramento de pacotes de rede para identificar informações confidenciais.
- Ataques de sniffing: Captura de dados em redes utilizando ferramentas específicas.

Gabarito: C

4. CEBRASPE (CESPE) - Tec (CNMP)/CNMP/Apoio Técnico Administrativo/Segurança Institucional/2023

Para determinar o grau de sigilo da informação, é necessário que sejam observados o interesse público da informação e a utilização do critério menos restritivo possível.

Comentários:

Muita atenção e cuidado nessa questão. Na prática, temos aqui uma referência a prática de classificação da informação, ou seja, quando se define níveis de acesso e, quem pode ou não acessar as informações.

Mas vejam que a questão traz a perspectiva de acesso amplo, ou seja, direito público de acesso. Logo, se há interesse público, há o princípio da transparência. Isso é preconizado na LEI DE ACESSO À INFORMAÇÃO, no artigo 24:

§ 5º Para a classificação da informação em determinado grau de sigilo, deverá ser observado o interesse público da informação e utilizado o critério menos restritivo possível,

Então vejam que, evitar estabelecer critérios restritivos para os casos de informações abertas e públicas é sim uma prática recomendada. Muito cuidado pois em alguma medida entra em conflito com tudo que trabalhamos sobre sigilo e restrição. Mas nesses casos, as informações, de fato, são restritas, e por isso, deve-se aumentar o grau de restrição.

São duas perspectivas distintas.

Gabarito: C

5. CEBRASPE (CESPE) - Ana TI (DATAPREV)/DATAPREV/Segurança Cibernética/2023

Em uma conexão criptografada, o princípio da disponibilidade é, de fato, atingido.

Comentários:

A criptografia está majoritariamente associada ao princípio da confidencialidade. Lembrando que ela também poderá estar associada ao princípio da autenticidade ao considerar a ordem das chaves a ser utilizada.

Gabarito: E

6. CEBRASPE (CESPE) - Ana (SERPRO)/SERPRO/Tecnologia/2023

A confidencialidade é uma propriedade segundo a qual as informações não podem ser disponibilizadas a indivíduos, entidades ou processos que não estejam previamente autorizados.

Comentários:

Sem muito o que acrescentar pessoal. A autorização de acesso é o recurso chave para garantir a restrição de acesso às informações confidenciais.

Gabarito: C

7. CEBRASPE (CESPE) - Ana Reg (AGER MT)/AGER MT/Ciências da Computação e Sistemas de Informação/2023

Funções de hash são muito utilizadas para verificação da propriedade básica da segurança da informação denominada

a) disponibilidade.

b) confidencialidade.

c) não-repúdio.

d) integridade.

e) perímetro.

Comentários:

O HASH sem dúvida está associado ao princípio da integridade. Lembrando que, por exemplo, na assinatura digital, temos a combinação da criptografia assimétrica com o HASH, onde a primeira técnica garante a autenticidade e a segunda, o HASH, garante a integridade. Por isso temos que a assinatura digital garante a autenticidade e a integridade.

Gabarito: D

8. CESPE / CEBRASPE - 2022 - APEX Brasil - Perfil 5: Tecnologia da Informação e Comunicação (TIC) - Especialidade: Infraestrutura e Operações de TIC

A característica de servidores de alta disponibilidade que permite a alternância imediata para uma rede em espera quando a rede principal falha denomina-se

A) balanceamento de carga.

B) failover.

C) nuvem privada escalável.

D) cluster.

Comentários:

A disponibilidade da informação é um dos princípios da segurança que vimos. E para isso, os sistemas e serviços, bem como o acesso à informação não pode deixar de acontecer.

Como prática de continuidade de negócios, sem dúvida, a técnica de FAILOVER é uma das principais. Ela diz respeito justamente à capacidade de um novo serviço, recurso, sistema, ou um DATACENTER completo começar a funcionar de forma subsidiária a partir do momento que a estrutura principal parou de funcionar.

Gabarito: B

9. 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

10. CESPE-2020 - SEFAZ/AL - 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 nesta 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

11. 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

---

12. (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

---

13. (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 violação da autenticidade das informações.

Comentários:

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

Gabarito: E

---

14. (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

---

15. (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

---

16. (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

---

17. (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

---

18. (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

---

19. (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

---

20. (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

---

21. (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

---

22. (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

---

23. (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

---

24. (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

---

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-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

---

27. (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

---

28. (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 tivermos 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

---

29. (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

---

30. (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

---

31. (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

---

32. (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

---

33. (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

---

34. (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

QUESTÕES COMENTADAS - PRINCÍPIOS DE SEGURANÇA - FCC

1. (FCC - AM (MPE PB)/MPE PB/Analista de Sistemas/Administrador de Banco de Dados/2023)

No âmbito da segurança da informação em bancos de dados, as dimensões privacidade de comunicação, armazenamento seguro de dados sensíveis, autenticação de usuários e controle de acesso granular são pertinentes ao aspecto

a) confidencialidade.

b) rastreabilidade.

c) integridade.

d) permissibilidade.

e) disponibilidade.

Comentários:

Vejam que todos os itens estão preocupados em garantir a restrição e eventual sigilo dos dados. Logo, o princípio associado é o da confidencialidade. Cuidado para não vincular autenticação a autenticidade de forma imediata. Nesse caso, a autenticação está associada ao requisito necessário para um acesso controlado.

Gabarito: A

---

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. (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

---

4. (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

---

5. (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

---

6. (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

QUESTÕES COMENTADAS - PRINCÍPIOS DE SEGURANÇA - FGV

1. (FGV - Ana (DPE RS)/DPE RS/Apoio Especializado (TI)/Infraestrutura e Redes/2023)

A empresa Progseg foi contratada via processo licitatório para a modernização das aplicações utilizadas no Tribunal de Justiça do Rio Grande do Norte. Aurélio, chefe do Departamento de Tecnologia, conduzirá junto à empresa o retrofit, que terá como foco a melhoria na segurança dos sistemas.

Os requisitos mandatórios dessa modernização são:

- Assegurar que informações privadas e confidenciais não estejam disponíveis nem sejam reveladas para indivíduos não autorizados; e

- Verificar que os usuários são quem dizem ser.

O requisito desejável dessa modernização é:

- Ser capaz de associar uma violação de segurança a uma parte responsável.

Com base nos requisitos citados, a Progseg deverá implementar, respectivamente:

a) confidencialidade, autenticidade, responsabilização;

b) disponibilidade, autenticidade, privacidade;

c) não repúdio, integridade de sistemas, confidencialidade;

d) integridade, disponibilidade, responsabilização;

e) autenticidade, integridade de dados, integridade de sistemas.

Comentários:

Questão bem prática e tranquila a respeito dos conceitos, certo?

O primeiro, tem foco no sigilo, logo, confidencialidade. Aqui, já teríamos resolvido a questão. O ponto de atenção fica pelo item de accountability ou responsabilização. Que é justamente você conseguir associar alguém a determinado ato para fins de registro.

Gabarito: A

2. (FGV - Aud Est (CGE SC)/CGE SC/Ciências da Computação/2023)

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:

Essa questão traz uma visão moderna, e que eu gosto muito, a respeito da associação entre a integridade e disponibilidade. Vejam que houve alteração indevida dos dados gravados, o que, por si só, afetou a integridade. O ponto adicional é que, em momento posterior, houve necessidade de consumo da informação, e esta estava com problema de integridade, o que acabou gerando indisponibilidade do dado.

Ainda, em nenhum momento, conforme enunciado, as informações originais que foram sobrescritas foram vazadas ou informadas sem autorização, o que não gerou problema com a confidencialidade.

Gabarito: E

3. (FGV - Ana (DPE RS)/DPE RS/Apoio Especializado (TI)/Infraestrutura e Redes/2023)

Tânia trabalha em uma prestadora de serviços de Internet. Equivocadamente, ela enviou ao servidor um comando UPDATE, o qual alterou indevidamente a base de dados, não permitindo mais seu acesso. De forma a ocultar seu erro, Tânia descobriu um post-it sob o teclado com a

senha de um dos técnicos que trabalhava com ela. Então, utilizando a senha, entrou no sistema e efetuou novas modificações, de forma que a culpa recaísse sobre o técnico.

No incidente relatado, houve a quebra do(a):

a) confidencialidade e autenticidade;

b) integridade e autenticidade;

c) irretratabilidade e disponibilidade;

d) não repúdio e confidencialidade;

e) confidencialidade e integridade.

Comentários:

Com o comando UPDATE, houve a alteração do dado indevidamente, o que gerou problema de integridade.

O segundo ponto, houve quebra da autenticidade, pois houve vazamento de senha e agora não é possível garantir a autoria da ação, pois estará associado ao usuário que nem sequer estava no local.

Gabarito: B

4. 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

---

5. (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

6. 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

Lista de Questões - Princípios de Segurança - CESPE

1. CEBRASPE (CESPE) - Tec (CNMP)/CNMP/Apoio Técnico Administrativo/Segurança Institucional/2023

São princípios da segurança da informação, entre outros, a confidencialidade, a integridade e a disponibilidade.

2. CEBRASPE (CESPE) - Ana (SERPRO)/SERPRO/Tecnologia/2023

A integridade é uma propriedade que visa aplicar conhecimentos e habilidades para garantir a assinatura digital.

3. CEBRASPE (CESPE) - Per Crim (POLC AL)/POLC AL/Análise de Sistemas, Ciências da Computação, Informática. Processamento de Dados ou Sistemas da Informação/2023

A confidencialidade trata da proteção de dados contra ataques passivos e envolve mecanismos de controle de acesso e criptografia.

4. CEBRASPE (CESPE) - Tec (CNMP)/CNMP/Apoio Técnico Administrativo/Segurança Institucional/2023

Para determinar o grau de sigilo da informação, é necessário que sejam observados o interesse público da informação e a utilização do critério menos restritivo possível.

5. CEBRASPE (CESPE) - Ana TI (DATAPREV)/DATAPREV/Segurança Cibernética/2023

Em uma conexão criptografada, o princípio da disponibilidade é, de fato, atingido.

6. CEBRASPE (CESPE) - Ana (SERPRO)/SERPRO/Tecnologia/2023

A confidencialidade é uma propriedade segundo a qual as informações não podem ser disponibilizadas a indivíduos, entidades ou processos que não estejam previamente autorizados.

7. CEBRASPE (CESPE) - Ana Reg (AGER MT)/AGER MT/Ciências da Computação e Sistemas de Informação/2023

Funções de hash são muito utilizadas para verificação da propriedade básica da segurança da informação denominada

a) disponibilidade.

b) confidencialidade.

c) não-repúdio.

d) integridade.

e) perímetro.

8. CESPE / CEBRASPE - 2022 - APEX Brasil - Perfil 5: Tecnologia da Informação e Comunicação (TIC) - Especialidade: Infraestrutura e Operações de TIC

A característica de servidores de alta disponibilidade que permite a alternância imediata para uma rede em espera quando a rede principal falha denomina-se

A) balanceamento de carga.

B) failover.

C) nuvem privada escalável.

D) cluster.

9. 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.

10. CESPE-2020 - SEFAZ/AL - 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.

11. 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.

12. (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.

13. (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 violação da autenticidade das informações.

14. (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.

15. (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.

16. (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.

17. (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

18. (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.

19. (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.

20. (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.

21. (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.

22. (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.

23. (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.

24. (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.

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-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.

27. (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.

28. (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.

29. (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

30. (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.

31. (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.

32. (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.

33. (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.

34. (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.

GABARITO

GABARITO

1. C
2. E
3. C
4. C
5. E
6. C
7. D
8. B
9. E
10. C
11. C
12. A
13. E
14. E
15. C
16. C
17. E
18. C
19. C
20. E
21. E
22. E
23. E
24. C
25. E
26. E
27. E
28. E
29. D
30. E
31. E
32. C
33. E
34. C

Lista de Questões - Princípios de Segurança - FCC

1. (FCC - AM (MPE PB)/MPE PB/Analista de Sistemas/Administrador de Banco de Dados/2023)

No âmbito da segurança da informação em bancos de dados, as dimensões privacidade de comunicação, armazenamento seguro de dados sensíveis, autenticação de usuários e controle de acesso granular são pertinentes ao aspecto

a) confidencialidade.

b) rastreabilidade.

c) integridade.

d) permissibilidade.

e) disponibilidade.

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.

3. (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.

4. (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.

5. (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.

6. (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.

GABARITO

GABARITO

1. A
2. E
3. E
4. A
5. C
6. A

Lista de Questões - Princípios de Segurança - FGV

1. (FGV - Ana (DPE RS)/DPE RS/Apoio Especializado (TI)/Infraestrutura e Redes/2023)

A empresa Progseg foi contratada via processo licitatório para a modernização das aplicações utilizadas no Tribunal de Justiça do Rio Grande do Norte. Aurélio, chefe do Departamento de Tecnologia, conduzirá junto à empresa o retrofit, que terá como foco a melhoria na segurança dos sistemas.

Os requisitos mandatórios dessa modernização são:

- Assegurar que informações privadas e confidenciais não estejam disponíveis nem sejam reveladas para indivíduos não autorizados; e

- Verificar que os usuários são quem dizem ser.

O requisito desejável dessa modernização é:

- Ser capaz de associar uma violação de segurança a uma parte responsável.

Com base nos requisitos citados, a Progseg deverá implementar, respectivamente:

a) confidencialidade, autenticidade, responsabilização;

b) disponibilidade, autenticidade, privacidade;

c) não repúdio, integridade de sistemas, confidencialidade;

d) integridade, disponibilidade, responsabilização;

e) autenticidade, integridade de dados, integridade de sistemas.

2. (FGV - Aud Est (CGE SC)/CGE SC/Ciências da Computação/2023)

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.

3. (FGV - Ana (DPE RS)/DPE RS/Apoio Especializado (TI)/Infraestrutura e Redes/2023)

Tânia trabalha em uma prestadora de serviços de Internet. Equivocadamente, ela enviou ao servidor um comando UPDATE, o qual alterou indevidamente a base de dados, não permitindo mais seu acesso. De forma a ocultar seu erro, Tânia descobriu um post-it sob o teclado com a senha de um dos técnicos que trabalhava com ela. Então, utilizando a senha, entrou no sistema e efetuou novas modificações, de forma que a culpa recaísse sobre o técnico.

No incidente relatado, houve a quebra do(a):

a) confidencialidade e autenticidade;

b) integridade e autenticidade;

c) irretratabilidade e disponibilidade;

d) não repúdio e confidencialidade;

e) confidencialidade e integridade.

4. 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.

5. (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.

6. 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.

GABARITO

GABARITO

1. A
2. E
3. B
4. B
5. E
6. B

Segurança Física, Lógica e Controle de Acesso

Quando falamos de Segurança da Informação, há uma diferenciação clássica no que tange às 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:

- 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.

- 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.

- 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.

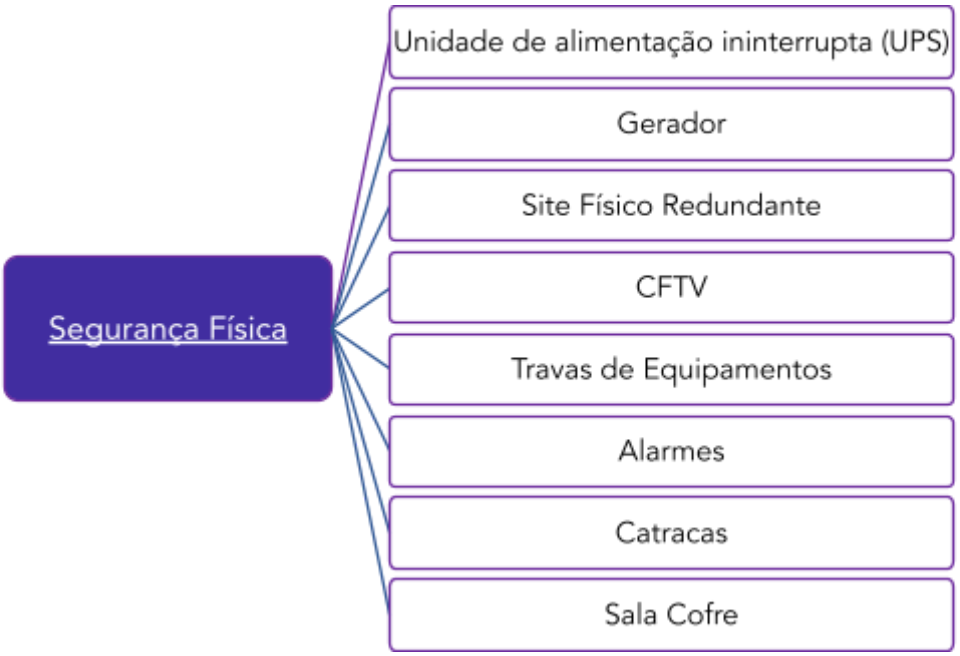
- CFTV – Temos aqui a utilização de câmeras para registro e visualização dos ambientes de uma organização. É um meio eminentemente reativo, uma vez que, na maioria das vezes, é utilizado para gravar o vídeo e ser utilizado posteriormente para análise e auditoria.

- 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.

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

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

- 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.



FGV - 2023 - Banco do Brasil - Técnico Atendimento

A catraca de controle de acesso é um dispositivo de segurança utilizado para dificultar o acesso não-autorizado a determinadas áreas de uma empresa, bem como possibilita monitorar o próprio fluxo de pessoal nessas áreas restritas.

O controle do acesso propriamente dito pode ser feito a partir da checagem de algum dado do usuário, como, por exemplo, a aproximação do seu crachá de identificação.

O mecanismo de detecção por aproximação em crachás está baseado em

A radiofrequência.

B infravermelho.

C ultravioleta.

D raio-X.

E ultrassom.

Comentários:

O mecanismo de detecção por aproximação em crachás, como o descrito, está baseado em radiofrequência. Essa tecnologia é comumente conhecida como RFID (Radio-Frequency Identification). Os crachás de identificação são equipados com uma pequena antena e um chip que emite sinais de radiofrequência quando aproximados de um leitor compatível. O leitor, que está integrado à catraca ou ao sistema de controle de acesso, captura esses sinais e autentica o usuário, permitindo ou negando o acesso com base nas informações contidas no crachá

Gabarito: A

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.

Comentários:

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 das 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 às 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.

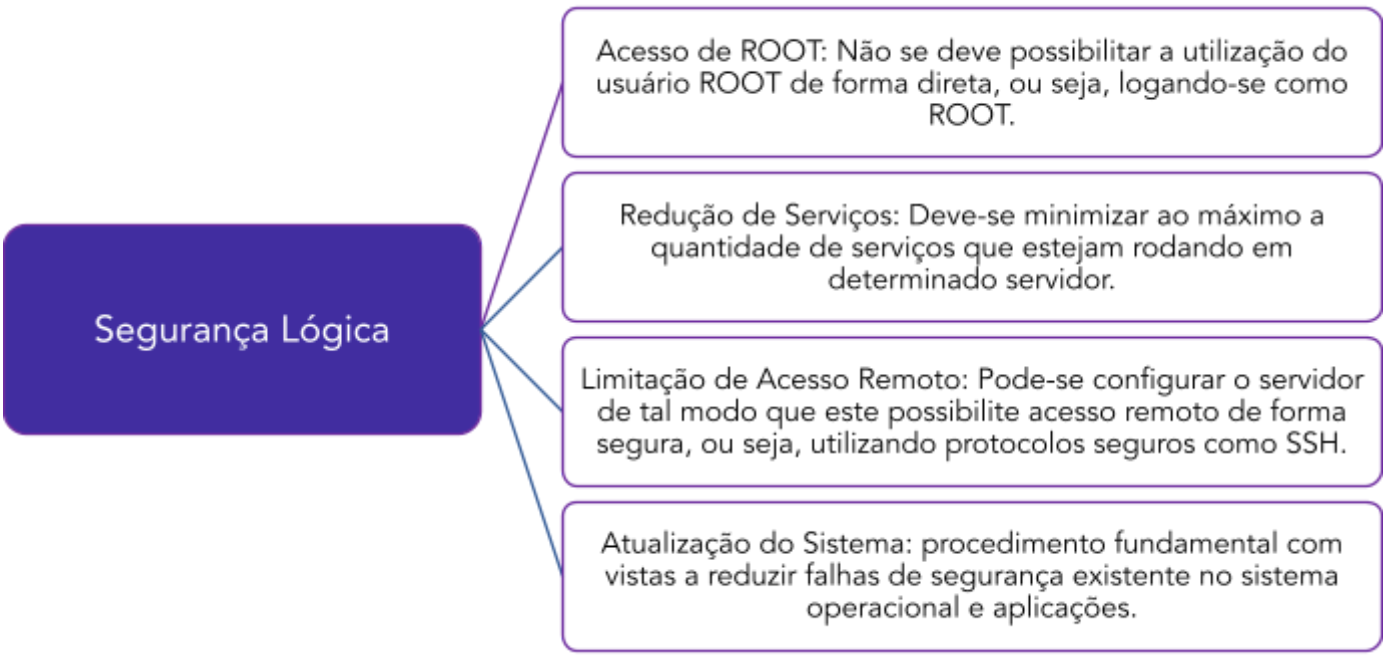
Diversos são os métodos ou regras a serem implementadas. Buscarei elencar algumas e complementaremos, eventualmente, nos exercícios:

- 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.

- 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.

- 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.

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



HORA DE PRATICAR!

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.

1. 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 quatro técnicas de controle e gerenciamento de acesso que são amplamente utilizadas nos ambientes de tecnologia da informação.

1. 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.

2. 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.

3. Role-Based Access Control (RBAC) – Também conhecido como controle baseado em papéis. Nesta técnica, o administrador garante privilégios de acordo com a função exercida pelo usuário. Esta estratégia simplifica o gerenciamento das permissões dadas aos usuários. Algumas questões têm trazido uma perspectiva mais aprofundada desse modelo. Portanto, vejamos os níveis de configuração que são possíveis com diferentes níveis de gerenciamento e atribuições:

    - RBAC 0: Esse modelo não possui hierarquia de papéis, o que significa que cada usuário teria que ter permissões específicas configuradas individualmente. Isso seria inviável em um ambiente com muitos usuários e diferentes níveis de acesso.
    - RBAC 1: Esse modelo introduz a hierarquia de papéis, permitindo que os administradores definam conjuntos de permissões que podem ser atribuídos a diferentes grupos de usuários. No entanto, o RBAC 1 não permite a delegação de permissões, o que pode ser uma limitação em ambientes complexos
    - RBAC 2: Esse modelo é o mais adequado para ambientes corporativos em geral. Ele permite a definição de hierarquias de papéis, a delegação de permissões e a restrição de acesso a recursos específicos. Isso oferece maior flexibilidade e granularidade no controle de acesso.
    - RBAC 3: Esse modelo é uma extensão do RBAC 2 que inclui suporte para controle de acesso baseado em tempo e em contexto. Estamos diante de um recurso de maior complexidade e que envolve um contexto corporativo mais maduro e gerenciável.
    - RBAC 4: Esse modelo é uma proposta recente que ainda não está totalmente implementada. Ele oferece recursos adicionais de segurança e flexibilidade, mas pode ser mais complexo de gerenciar.

4. Attribute-Based Access Control (ABAC) – É uma técnica de controle de acesso que concede ou nega acesso a recursos com base em atributos do sujeito, objeto e contexto. A principal diferença entre ABAC e RBAC é que ABAC é mais flexível e granular do que RBAC. ABAC permite que os administradores de segurança atribuam direitos de acesso com base em uma ampla gama de atributos, incluindo: Identidade do sujeito; Função do sujeito; Localização do sujeito; Tempo ; Tipo de recurso ; Critérios de segurança

    Por exemplo, imagine um sistema de gerenciamento de documentos com ABAC. Uma política ABAC poderia ser: "Permitir que usuários do departamento de vendas acessem documentos de vendas apenas durante horário comercial e a partir do escritório". Nesse caso, os atributos seriam a identidade do usuário, o departamento, o horário e a localização, e a decisão de acesso dependerá de como esses atributos se relacionam com a política.

FGV - Ana (DPE RS)/DPE RS/Apoio Especializado (TI)/Infraestrutura e Redes/2023

Aurélio está implementando o controle de acesso à rede wi-fi da Defensoria Pública do Estado do Rio Grande do Sul (DPE/RS). Ele se baseou no modelo de referência do RBAC (Role Based Access Control) para a definição dos perfis. O perfil mais restrito possui as permissões básicas para cada servidor e, a partir dele, o acesso vai se incrementando. Os servidores do Departamento de Segurança devem ter as permissões mais básicas, além de acrescentar restrições, que restringem os modos de configuração possíveis.

Com base nesse modelo de referência, Aurélio deverá atribuir para o Departamento de Segurança o modelo RBAC:

a) 0;

b) 1;

c) 2;

d) 3;

e) 4.

Comentários:

Conforme vimos em nossa teoria, estamos mais próximos da configuração tipo 2, que é, de fato, o modelo mais usual e que traz um equilíbrio entre controle, segurança e esforço para consolidar e implantar.

Gabarito: C

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 rígido, logo, menos flexível, e não o discricionário como apresenta 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 está 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

Lista de Questões - SEGURANÇA FÍSICA, LÓGICA E CONTROLE DE ACESSO - CESPE Órgão: PG-DF

1. CEBRASPE (CESPE) - Ana (SERPRO)/SERPRO/Tecnologia/2023

Acerca de conceitos relacionados a controle de acesso, julgue o item a seguir.

Para reduzir vulnerabilidades, os controles de acesso devem liberar a propriedade do registro para que usuário possa criar, ler, atualizar ou excluir qualquer registro.

2. CEBRASPE (CESPE) - Ana (SERPRO)/SERPRO/Tecnologia/2023

Acerca de conceitos relacionados a controle de acesso, julgue o item a seguir.

O uso de processos e ferramentas para criar, atribuir, gerenciar e revogar credenciais de acesso para usuários é considerado uma boa prática de segurança da informação.

3. CEBRASPE (CESPE) - Ana Sist (EMPREL)/EMPREL/2023

O emprego de controles apropriados para o acesso físico de pessoas a ambientes seguros de processamento de informações tem como principal finalidade

a) organizar a emissão de identidades funcionais permanentes e credenciais temporárias para o público externo.

b) criar um banco de dados de clientes, com foco em relacionamento corporativo.

c) assegurar que somente pessoas autorizadas tenham acesso permitido.

d) viabilizar e acelerar o acesso de fornecedores e prestadores de serviços em emergências.

e) estabelecer um histórico de todos os acessos, para fins logísticos e estatísticos.

4. CEBRASPE (CESPE) - Ana TI (DATAPREV)/DATAPREV/Segurança Cibernética/2023

Em função de sua codificação mais robusta, os firmwares de IoT são mais sofisticados que os sistemas operacionais executados em computadores e smartphones, o que os torna imunes a falhas consequentes das vulnerabilidades conhecidas.

5. 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.

6. (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.

7. (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.

8. (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.

9. 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.

10. (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.

11. (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.

GABARITO

GABARITO

1. E
2. E
3. C
4. E
5. E
6. C
7. B
8. C
9. B
10. B
11. C

QUESTÕES COMENTADAS - SEGURANÇA FÍSICA, LÓGICA E CONTROLE DE ACESSO - FCC

1. (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

---

2. (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

---

3. (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

---

4. (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

QUESTÕES COMENTADAS - SEGURANÇA FÍSICA, LÓGICA E CONTROLE DE ACESSO - FGV

1. (FGV - Ana (DPE RS)/DPE RS/Apoio Especializado (TI)/Infraestrutura e Redes/2023)

Aurélio está implementando o controle de acesso à rede wi-fi da Defensoria Pública do Estado do Rio Grande do Sul (DPE/RS). Ele se baseou no modelo de referência do RBAC (Role Based Access Control) para a definição dos perfis. O perfil mais restrito possui as permissões básicas para cada servidor e, a partir dele, o acesso vai se incrementando. Os servidores do Departamento de Segurança devem ter as permissões mais básicas, além de acrescentar restrições, que restringem os modos de configuração possíveis.

Com base nesse modelo de referência, Aurélio deverá atribuir para o Departamento de Segurança o modelo RBAC:

a) 0;

b) 1;

c) 2;

d) 3;

e) 4.

Comentários:

Estamos mais próximos da configuração tipo 2, que é, de fato, o modelo mais usual e que traz um equilíbrio entre controle, segurança e esforço para consolidar e implantar.

RBAC 2: Esse modelo é o mais adequado para ambientes corporativos em geral. Ele permite a definição de hierarquias de papéis, a delegação de permissões e a restrição de acesso a recursos específicos. Isso oferece maior flexibilidade e granularidade no controle de acesso.

Gabarito: C

2. FGV - 2023 - Banco do Brasil - Técnico Atendimento

A catraca de controle de acesso é um dispositivo de segurança utilizado para dificultar o acesso não-autorizado a determinadas áreas de uma empresa, bem como possibilita monitorar o próprio fluxo de pessoal nessas áreas restritas.

O controle do acesso propriamente dito pode ser feito a partir da checagem de algum dado do usuário, como, por exemplo, a aproximação do seu crachá de identificação.

O mecanismo de detecção por aproximação em crachás está baseado em

A radiofrequência.

B infravermelho.

C ultravioleta.

D raio-X.

E ultrassom.

Comentários:

O mecanismo de detecção por aproximação em crachás, como o descrito, está baseado em radiofrequência. Essa tecnologia é comumente conhecida como RFID (Radio-Frequency Identification). Os crachás de identificação são equipados com uma pequena antena e um chip que emite sinais de radiofrequência quando aproximados de um leitor compatível. O leitor, que está integrado à catraca ou ao sistema de controle de acesso, captura esses sinais e autentica o usuário, permitindo ou negando o acesso com base nas informações contidas no crachá

Gabarito: A

3. 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

QUESTÕES COMENTADAS - SEGURANÇA FÍSICA, LÓGICA E CONTROLE DE ACESSO - CESPE

1. CEBRASPE (CESPE) - Ana (SERPRO)/SERPRO/Tecnologia/2023

Acerca de conceitos relacionados a controle de acesso, julgue o item a seguir.

Para reduzir vulnerabilidades, os controles de acesso devem liberar a propriedade do registro para que usuário possa criar, ler, atualizar ou excluir qualquer registro.

Comentários:

Os controles de acesso devem restringir as permissões dos usuários, permitindo apenas as operações necessárias para suas funções. Liberar a propriedade do registro para criar, ler, atualizar ou excluir qualquer registro aumenta as vulnerabilidades.

Gabarito: E

2. CEBRASPE (CESPE) - Ana (SERPRO)/SERPRO/Tecnologia/2023

Acerca de conceitos relacionados a controle de acesso, julgue o item a seguir.

O uso de processos e ferramentas para criar, atribuir, gerenciar e revogar credenciais de acesso para usuários é considerado uma boa prática de segurança da informação.

Comentários:

O uso de processos e ferramentas para gerenciar credenciais de acesso é uma boa prática de segurança da informação, pois garante que apenas usuários autorizados tenham acesso aos recursos e que as credenciais sejam gerenciadas de forma segura.

Gabarito: E

3. CEBRASPE (CESPE) - Ana Sist (EMPREL)/EMPREL/2023

O emprego de controles apropriados para o acesso físico de pessoas a ambientes seguros de processamento de informações tem como principal finalidade

a) organizar a emissão de identidades funcionais permanentes e credenciais temporárias para o público externo.

b) criar um banco de dados de clientes, com foco em relacionamento corporativo.

c) assegurar que somente pessoas autorizadas tenham acesso permitido.

d) viabilizar e acelerar o acesso de fornecedores e prestadores de serviços em emergências.

e) estabelecer um histórico de todos os acessos, para fins logísticos e estatísticos.

Comentários:

Conforme vimos, o foco não se trata de aspectos de identificação, mas sim, indicar quem pode fazer algo nesse contexto. Essa é a essência da autorização e controle de acesso.

Gabarito: C

4. CEBRASPE (CESPE) - Ana TI (DATAPREV)/DATAPREV/Segurança Cibernética/2023

Em função de sua codificação mais robusta, os firmwares de IoT são mais sofisticados que os sistemas operacionais executados em computadores e smartphones, o que os torna imunes a falhas consequentes das vulnerabilidades conhecidas.

Comentários:

Os sistemas operacionais tradicionais são muito mais robustos do que os firmware que operam nesses hardwares de IoT. Lembrando que IoT é Internet das Coisas, ou seja, aquele conceito onde praticamente tudo se torna digital, e portanto, controlável e acessado pelas redes de computadores.

Esse novo contexto e realidade gera desafios imensos de segurança, justamente porque todo dispositivo conectado na rede ou internet passa a ser alvo de atacantes, e pode, inclusive, virar vetor para realização de outros ataques.

Gabarito: E

5. 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.

Comentários:

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 das 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 as boas práticas a serem adotadas.

Gabarito: E

6. (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

7. (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

8. (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

9. 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

10. (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 está 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

11. (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

Lista de Questões - SEGURANÇA FÍSICA, LÓGICA E CONTROLE DE ACESSO - FCC

1. (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.

2. (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.

3. (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.

4. (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

1. D
2. B
3. B
4. B

Lista de Questões - SEGURANÇA FÍSICA, LÓGICA E CONTROLE DE ACESSO - FGV

1. (FGV - Ana (DPE RS)/DPE RS/Apoio Especializado (TI)/Infraestrutura e Redes/2023)

Aurélio está implementando o controle de acesso à rede wi-fi da Defensoria Pública do Estado do Rio Grande do Sul (DPE/RS). Ele se baseou no modelo de referência do RBAC (Role Based Access Control) para a definição dos perfis. O perfil mais restrito possui as permissões básicas para cada servidor e, a partir dele, o acesso vai se incrementando. Os servidores do Departamento de Segurança devem ter as permissões mais básicas, além de acrescentar restrições, que restringem os modos de configuração possíveis.

Com base nesse modelo de referência, Aurélio deverá atribuir para o Departamento de Segurança o modelo RBAC:

a) 0;

b) 1;

c) 2;

d) 3;

e) 4.

2. FGV - 2023 - Banco do Brasil - Técnico Atendimento

A catraca de controle de acesso é um dispositivo de segurança utilizado para dificultar o acesso não-autorizado a determinadas áreas de uma empresa, bem como possibilita monitorar o próprio fluxo de pessoal nessas áreas restritas.

O controle do acesso propriamente dito pode ser feito a partir da checagem de algum dado do usuário, como, por exemplo, a aproximação do seu crachá de identificação.

O mecanismo de detecção por aproximação em crachás está baseado em

A) radiofrequência.

B)infravermelho.

C) ultravioleta.

D) raio-X.

E ultrassom.

3. 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.

GABARITO

GABARITO

1. C
2. A
3. 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:

- 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.

- Algo que você tem

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

- 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 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 fator 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 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 foi 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.

Ainda no contexto do MFA, temos a Autenticação Multifator Adaptativa (MFA Adaptativa), que é uma forma avançada de autenticação multi fator que ajusta dinamicamente os requisitos de autenticação com base no contexto e no comportamento do usuário. Em vez de aplicar os mesmos fatores de autenticação para todos os usuários em todas as situações, a MFA adaptativa analisa diversos parâmetros para determinar o nível apropriado de segurança necessário para cada tentativa de login.

A MFA adaptativa utiliza informações contextuais e padrões de comportamento do usuário para avaliar o risco associado a uma tentativa de login. Alguns dos fatores considerados incluem:

1. Localização: Onde o usuário está tentando se conectar.

2. Dispositivo: O dispositivo usado para fazer login.
3. Horário: O horário em que a tentativa de login está sendo feita.
4. Rede: Se a conexão está sendo feita a partir de uma rede privada ou pública.
5. Tentativas de Login: O número de tentativas de login falhadas.

Com base nesses parâmetros, a MFA adaptativa pode exigir diferentes níveis de autenticação. Por exemplo, se um usuário tenta fazer login de um local desconhecido ou em um horário incomum, o sistema pode solicitar uma verificação adicional, como um código enviado por SMS ou uma autenticação biométrica.

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. É 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 à frente algumas questões mais práticas sobre o funcionamento desses aplicativos? 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 é 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 autenticação 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 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 corporativos com alta e média 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 utilizam de processos variados de reconhecimento de credenciais dos usuários para compor sua base. Nesse aspecto, há três formas básicas (espécie de categoria). Elas são 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:

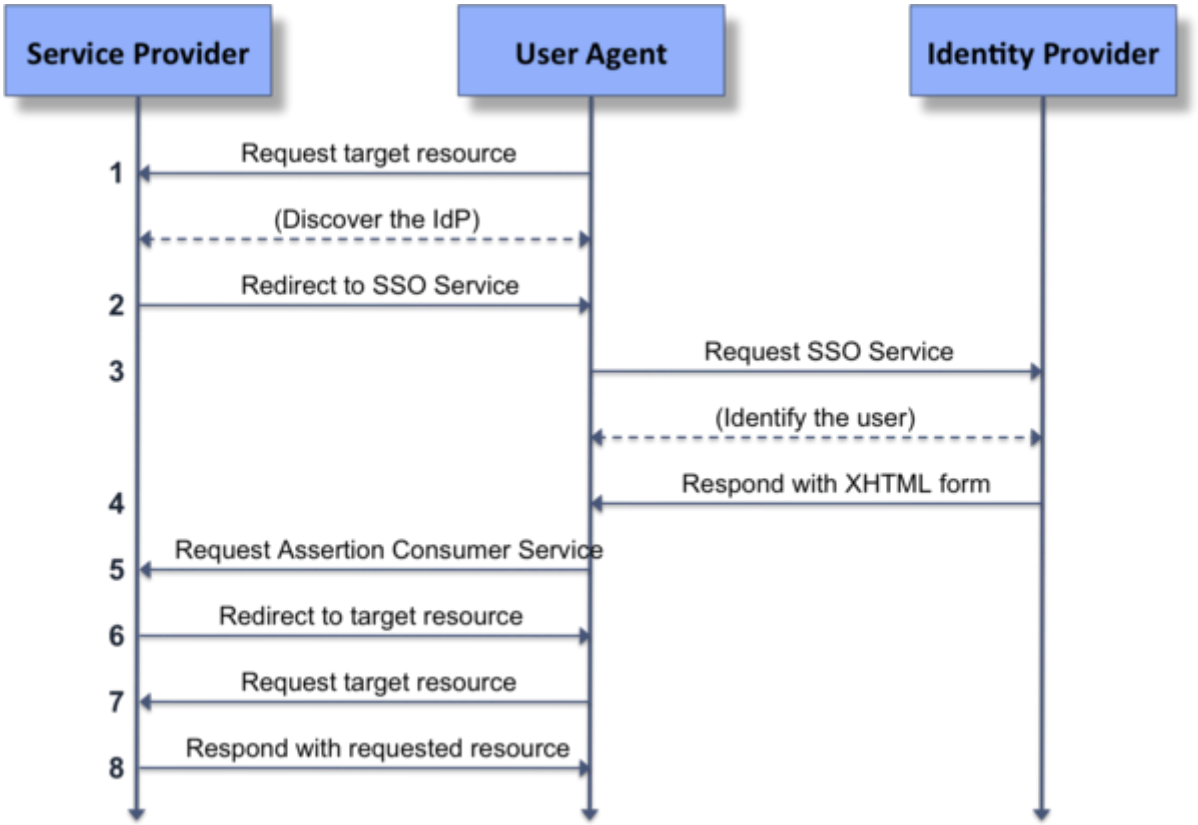
1. O principal (tipicamente um humano);
2. O Provedor de Identidades (Identity Provider - IDP)
3. O Provedor de Serviços (Service Provider - SP)

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

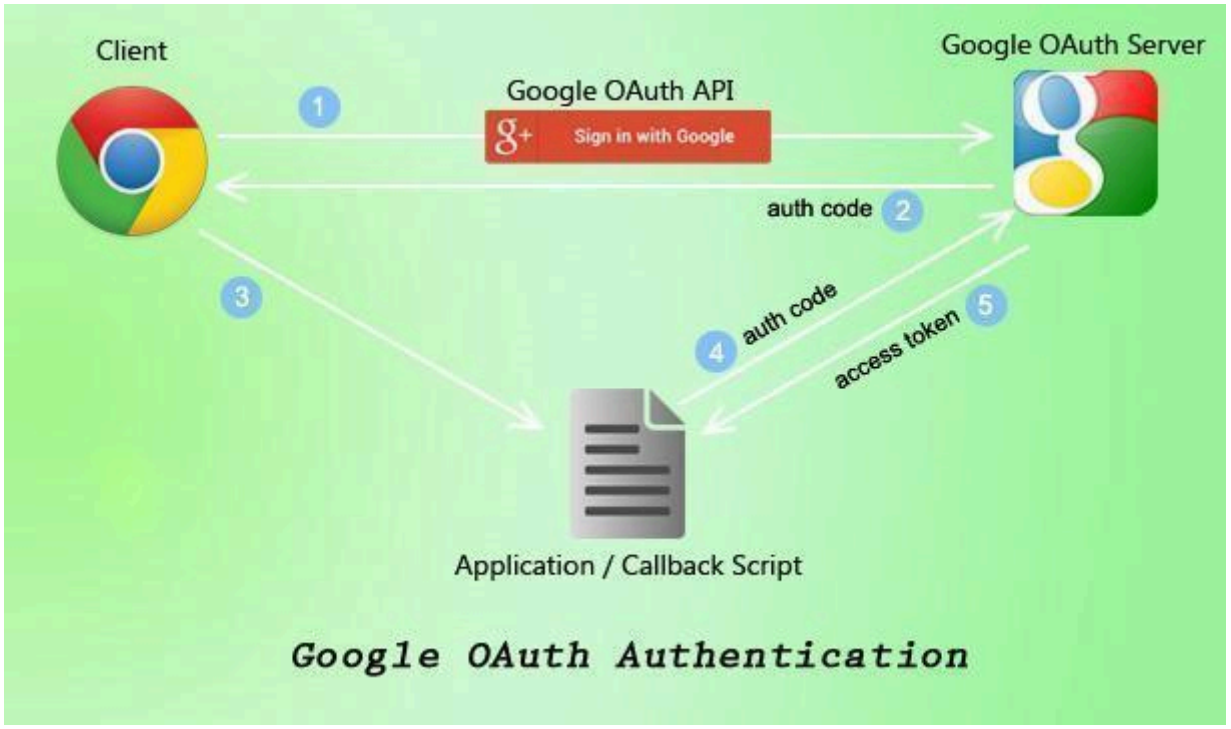
múltiplo fator de autenticação (MFA). Então, para cada serviço que se deseje utilizar, todo o processo do MFA deve ser realizado, ou, no mínimo, a confirmação da segunda camada de segurança. Ainda, a título de exemplo, pode-se utilizar serviços como RADIUS, LDAP ou ainda Active Directory da Microsoft. 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:



OAuth

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 muitos 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

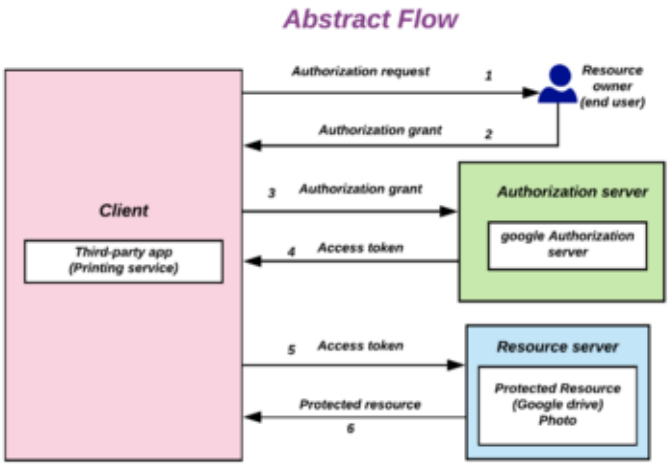
e senha, tem-se um processo de autorização, em que você autoriza a aplicação ou serviço, a obter suas informações do servidor OAuth. Na prática, temos aqui o DONO DO RECURSO.

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 realizadas 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 papéis e respectivos fluxos, vejamos:



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 exemplos 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.

Ano: 2024 Banca: CESPE / CEBRASPE Órgão: TCDF

Os tokens de acesso devem ser lidos e interpretados pelo cliente OAuth, que é o público-alvo do token.

Comentários:

Há uma série de propriedades de tokens de acesso que são fundamentais para o modelo de segurança do OAuth. Os tokens de acesso não devem ser lidos ou interpretados pelo cliente OAuth. O cliente OAuth não é o público-alvo do token.

Gabarito: E

Algumas bancas começam a trazer uma visão mais técnica para o conteúdo do OAUTH, exigindo do candidato um conhecimentos mais aprofundados de parâmetros, bibliotecas e itens de configuração, de uma forma geral. Esse mesmo assunto também é abordado pela nossa equipe de professores de desenvolvimento.

Entretanto, vou trazer alguns pontos relevantes aqui nesse contexto para garantir a visibilidade de vocês desses temas.

1. Tipos de Clientes:

No OAuth 2.0, existem dois tipos de clientes: confidenciais e públicos. Vamos entender as diferenças:

a) Clientes Confidenciais:

Estes tipos de clientes são registrados com um segredo do cliente. Com isso, podem manter a confidencialidade de suas credenciais.

Como exemplos, podemos citar as integrações entre serviços da organização ou aplicativos que consomem APIs internas. Esses clientes podem armazenar e proteger suas credenciais de acesso.

b) Clientes Públicos:

Em uma outra perspectiva, estes não conseguem manter a confidencialidade de suas credenciais. Por isso, são usados em cenários como aplicativos móveis ou baseados em navegador, justamente por não possuírem um segredo do cliente.

Assim, como requisito, temos que as credenciais do cliente não precisam ser mantidas em sigilo.

2. TIPOS DE TOKENS

a) Bearer Tokens:

São usados para acessar recursos protegidos em nome de um usuário. Neste contexto, o portador apresenta um token válido para obter acesso. Tem como vulnerabilidade ou ponto de atenção o fato de não haver verificação da legitimidade do remetente. Logo, pode ser vulnerável se cair em mãos não autorizadas.

b) Sender-Constrained Tokens (Mutual TLS):

Garantem que o remetente seja legítimo. Para tanto, são vinculados à conexão TLS mútua entre cliente e servidor de autorização. O servidor de recursos verifica o certificado do cliente, o que, na prática, traz uma burocracia para o processo justamente pela necessidade da Infraestrutura de chaves públicas e certificados do cliente.

O token inclui o hash do certificado (por exemplo, no JWT). O remetente deve provar que possui a chave privada do certificado vinculado.

c) ID Tokens:

Fornecem informações sobre o usuário autenticado. Como o próprio nome já diz, o ID, vem justamente de Identificação, sendo essas informações emitidas pelo provedor de identidade.

Contêm detalhes como ID do usuário e escopo. Justamente por tratar somente da camada de identificação e não de autenticação/autorização, propriamente ditos, acabam por não serem usados para acessar recursos protegidos.

d) Refresh Tokens:

Permitem obter novos *access tokens* sem novo login. São mais duradouros que os access tokens e geralmente são usados para renovar tokens expirados. Falaremos mais dele no tópico a seguir.

3. REFRESH TOKEN

Um Refresh Token é uma sequência (string) que o cliente OAuth pode usar para obter um novo access token sem a interação do usuário, tendo como premissa a autorização inicial que ele obteve na primeira requisição ao usuário.

Tanto clientes públicos quanto confidenciais podem usar refresh tokens. Se um refresh token emitido para um cliente público for roubado, o atacante pode se passar pelo cliente e usar o refresh token sem ser detectado.

Quando inicialmente se recebe o access token, ele pode incluir um refresh token e um tempo de expiração. Vejam que é um item opcional e configurável.

Com isso, é possível atualizar o conteúdo ou o recurso sem nova solicitação ou interação com o Dono do Recurso, sendo processado tudo em background dos sistemas envolvidos.

O valor "expires_in" indica quantos segundos o access token será válido.

É possível usar esse timestamp para atualizar os access tokens antes que eles expirem, evitando falhas em chamadas de API.

Para fins práticos, caso queira utilizar o refresh token, basta fazer uma solicitação POST para o endpoint de token com *grant_type=refresh_token*, incluindo o refresh token e as credenciais do cliente, se necessário:

POST /oauth/token HTTP/1.1

Host: authorization-server.com

grant_type=refresh_token

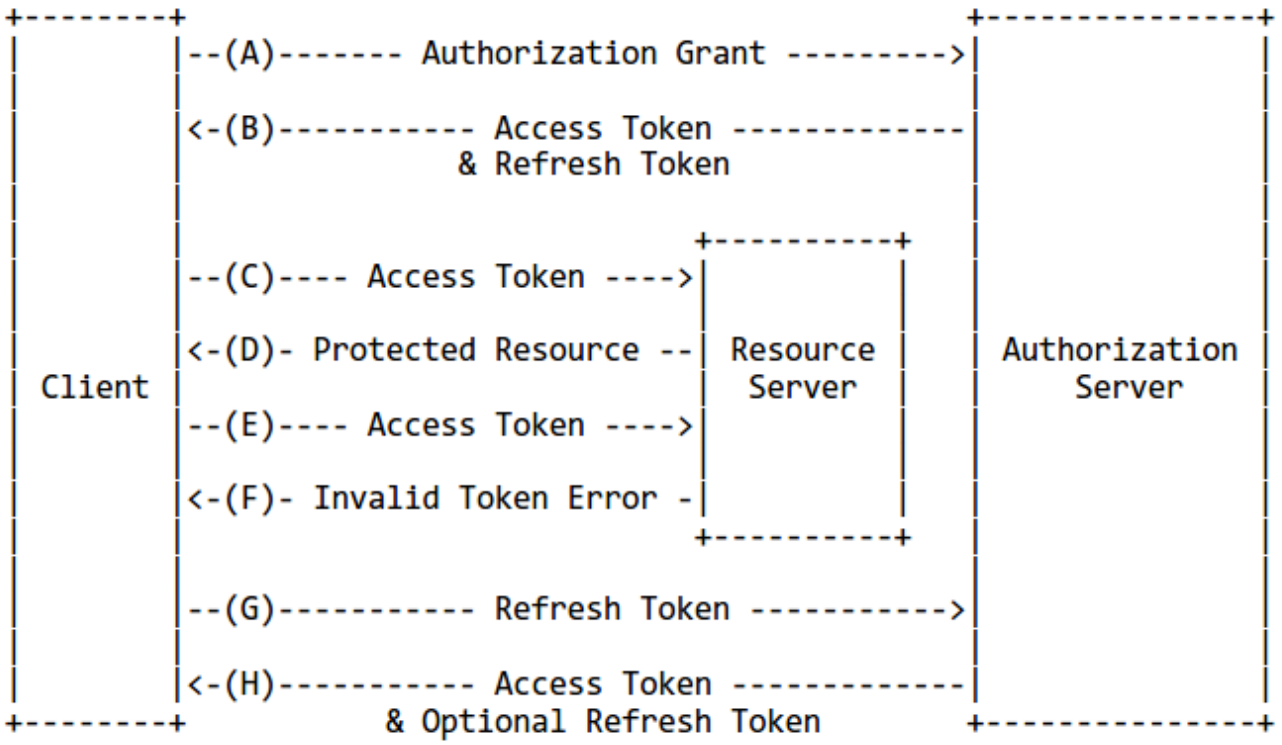
&refresh_token=xxxxxxxxxx

&client_id=xxxxxxxxxx

&client_secret=xxxxxxxxxx

A resposta incluirá um novo access token e, opcionalmente, um novo refresh token.

A imagem abaixo nos traz essa dinâmica em diagrama de fluxos de mensagens, extraído diretamente da documentação oficial do OAUTH. Reparem que, após o acesso ao recurso protegido, na etapa D, uma nova tentativa de uso do Token anterior é feita em E, porém, o token não é mais válido em F. Com isso, pode-se utilizar o Refresh Token em G para a geração de um novo TOKEN em H sem a interação com o usuário, bastante a interação com o Authorization Server.



Ano: 2024 Banca: CESPE / CEBRASPE Órgão: TCDF

Os tokens Sender-constrained exigem que, para usar o token de acesso, o cliente OAuth prove, de alguma forma, a posse de uma chave privada, de modo que o token de acesso por si só não seja utilizável.

Comentários:

Exatamente a camada adicional de segurança que comentamos em nossa teoria, que incorpora a infraestrutura de chaves públicas e certificados digitais, com a posse da chave privada..

Gabarito: C

Um ponto importante que tem aparecido em prova dentro deste tópico são as abordagens de boas práticas de configuração e perspectivas de segurança. Dessa forma, vamos trabalhar ainda alguns conceitos:

Boas Práticas de Segurança para JWT

1. Use Algoritmos Seguros:
    - Prefira algoritmos como HS256 ou RS256 para assinar seus tokens.
2. Mantenha as Chaves Secretas Seguras:
    - Armazene as chaves secretas em locais seguros e nunca as exponha no código-fonte.
3. Defina um Tempo de Expiração Curto:
    - Configure um tempo de expiração curto para os tokens (exp claim) para minimizar o impacto de um token comprometido.
4. Revogação de Tokens:
    - Implemente um mecanismo para revogar tokens, como uma lista de tokens revogados.
5. Validação de Tokens:
    - Sempre valide o token no servidor, verificando a assinatura e as claims.
6. Use HTTPS:
    - Transmita tokens apenas por conexões seguras (HTTPS) para evitar ataques de interceptação.
7. Minimize as Claims:
    - Inclua apenas as informações necessárias nas claims do token para reduzir o risco de exposição de dados sensíveis.
8. Verificação de Origem:
    - Verifique a origem do token (iss claim) para garantir que ele foi emitido por uma fonte confiável.

Boas Práticas de Configuração para JWT

1. Configuração de Claims:
    - Defina claims padrão como iss (issuer), sub (subject), aud (audience) e exp (expiration).
2. Uso de Bibliotecas Confiáveis:
    - Utilize bibliotecas bem mantidas e confiáveis para a geração e validação de JWTs.
3. Rotação de Chaves:
    - Implemente a rotação periódica de chaves para aumentar a segurança.
4. Escopo e Permissões:
    - Defina escopos e permissões claras dentro do token para controlar o acesso aos recursos.

5. Monitoramento e Logs:
    - Monitore e registre o uso de tokens para detectar e responder a atividades suspeitas.
6. Política de Renovação de Tokens:
    - Estabeleça uma política clara para a renovação de tokens, garantindo que os usuários obtenham novos tokens antes que os antigos expirem.

Manipulação de Tokens Sem Estado de Curta Duração

1. Tokens de Curta Duração:
    - Utilize tokens de curta duração para minimizar o impacto de um token comprometido. Tokens de curta duração são ideais para aplicações sem estado, onde o servidor não mantém informações sobre o estado do cliente entre as requisições.
2. Renovação de Tokens:
    - Implemente um mecanismo de renovação de tokens, onde um token de curta duração pode ser trocado por um novo token antes de expirar. Isso pode ser feito através de um endpoint de renovação seguro.
3. Tokens de Atualização (Refresh Tokens):
    - Utilize tokens de atualização para emitir novos tokens de curta duração. Os tokens de atualização devem ser armazenados de forma segura e transmitidos apenas por conexões seguras.
4. Verificação de Expiração:
    - Sempre verifique a expiração (exp claim) dos tokens de curta duração no servidor para garantir que apenas tokens válidos sejam aceitos.
5. Desempenho e Escalabilidade:
    - Tokens sem estado de curta duração são leves e não requerem armazenamento no servidor, o que melhora o desempenho e a escalabilidade da aplicação.

Biometria

Algumas questões tratam os aspectos de BIOMETRIA de uma maneira mais detalhada. Por esse motivo, reservamos 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, é 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.

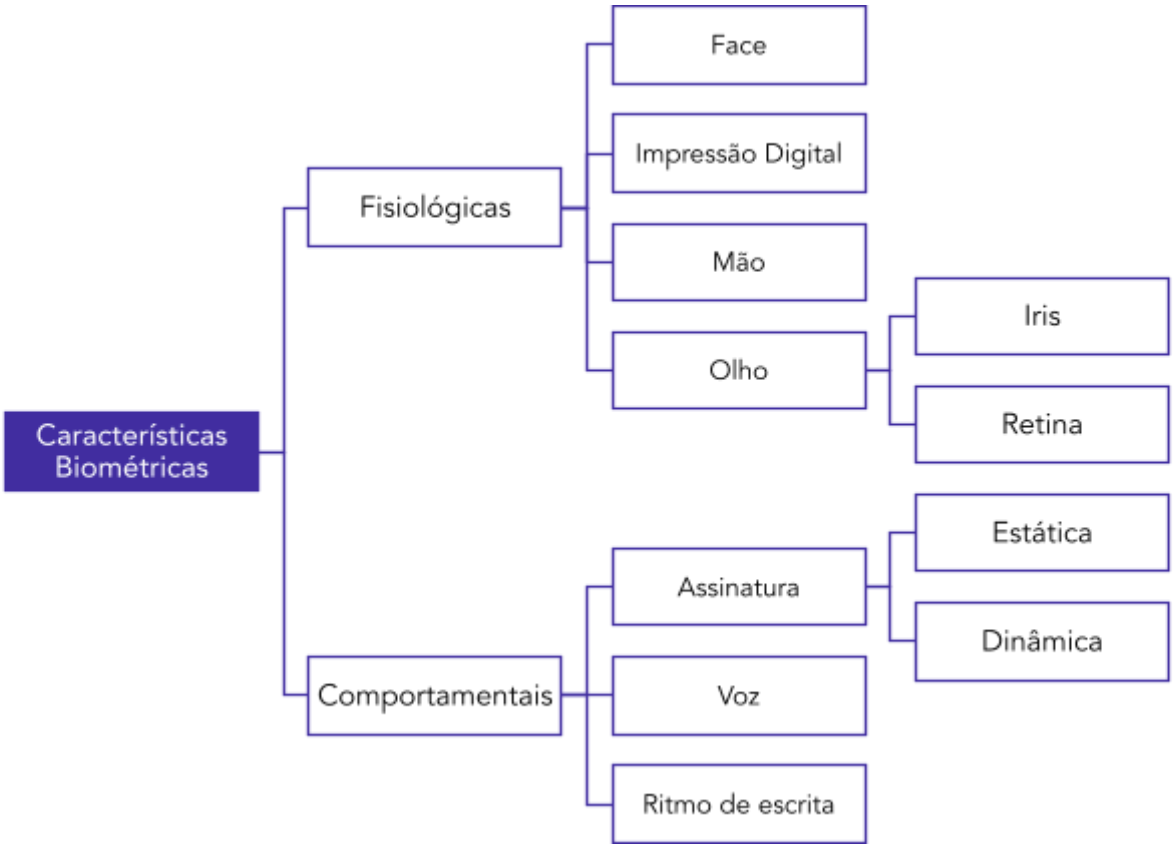
Como vimos anteriormente, o processo de biometria está atrelado à fase de autenticação e autorização, principalmente, para fins de controle de acesso.

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 apresenta 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).

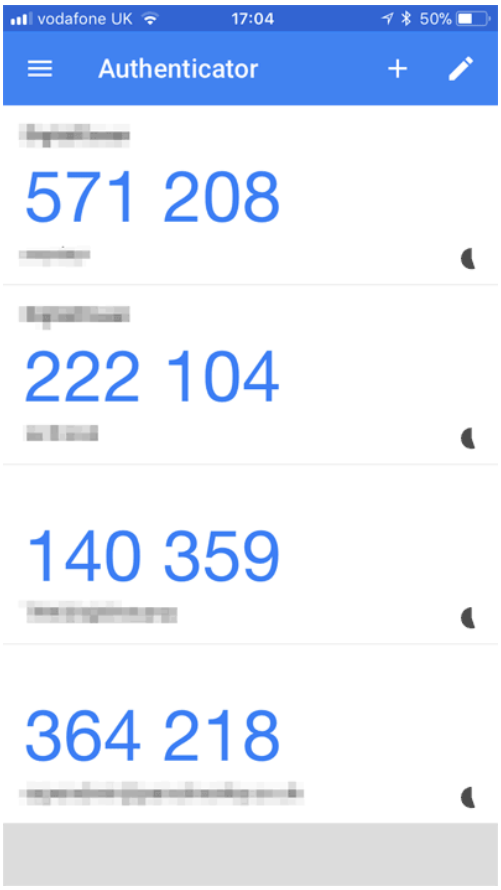
Comentários:

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

Gabarito: C

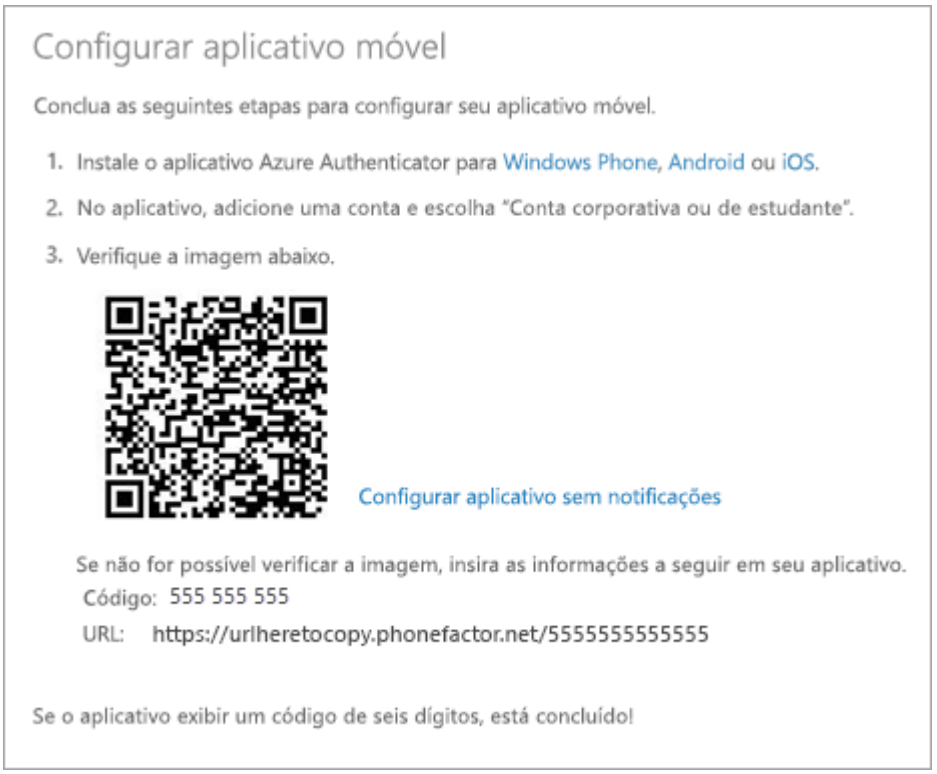
Um outro mecanismo interessante que surge é por meio de autenticadores em dispositivos móveis. Por vezes, também conhecidos como tokens de segurança ou chaves de sessão, podem ser efetivados por meio de aplicativos próprios que permitem a vinculação a determinados serviços e seus usuários.

Antes de explicarmos seu funcionamento, vamos citar alguns deles:


vodafone UK
17:04
50%
Authenticator
571 208
222 104
140 359
364 218


12:30
AWS
amazon
web services
AWS TOKEN IS:
7294528
AWS
john@gmail.com
Gmail
johnro...@gmail.com
Dropbox
jonathan.robertso...
Evernote
Digital Ocean
johnrob...@gmail.com
Facebook
jonatha...@gmail.com
Github
johndoe@gmail.com
Coinbase
Gmail
johnro...domine.com


Microsoft
Authenticator



Apresentei uma lista de três aplicativos distintos. O fluxo base de configuração é o mesmo. O site específico do serviço gerará um QRCODE para que seja lido pelo aplicativo. Neste momento, haverá a vinculação da conta e site, junto ao aplicativo. A partir deste instante, todo acesso dependerá de algum nível de aprovação no aplicativo como segundo fator de autenticação, ou ainda, será necessária a extração de uma informação dos códigos de cada aplicativo gerado no aplicativo. Esses códigos são dinâmicos e de tempos em tempos, geralmente 30 segundos, são alterados.

OPENID Connect - OIDC

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.

O OpenID Connect (OIDC) é um protocolo de autenticação que permite que usuários se autentiquem em um serviço usando suas credenciais de um provedor de identidade (IDP). O OIDC é um protocolo leve e flexível que pode ser integrado a uma ampla gama de serviços.

As principais características do OIDC são:

- Autenticação baseada em tokens: O OIDC usa tokens para autenticar usuários. Esses tokens são emitidos pelo IDP e são usados pelo serviço para verificar a identidade do usuário.
- Autorização baseada em declarações: O OIDC usa declarações para autorizar usuários a acessar recursos. Essas declarações são emitidas pelo IDP e são usadas pelo serviço para determinar quais recursos o usuário pode acessar.
- Descentralização: O OIDC é um protocolo descentralizado. Isso significa que não há um único ponto de falha ou controle.

Ainda, o OIDC oferece uma série de vantagens em relação a outras tecnologias de autenticação, incluindo:

- Simplicidade: O OIDC é um protocolo simples e fácil de implementar.
- Flexibilidade: O OIDC pode ser integrado a uma ampla gama de serviços.
- Segurança: O OIDC usa criptografia para proteger os dados do usuário.
- Interoperabilidade: O OIDC é um protocolo interoperável que pode ser usado com uma ampla gama de IDPs. Opera 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.

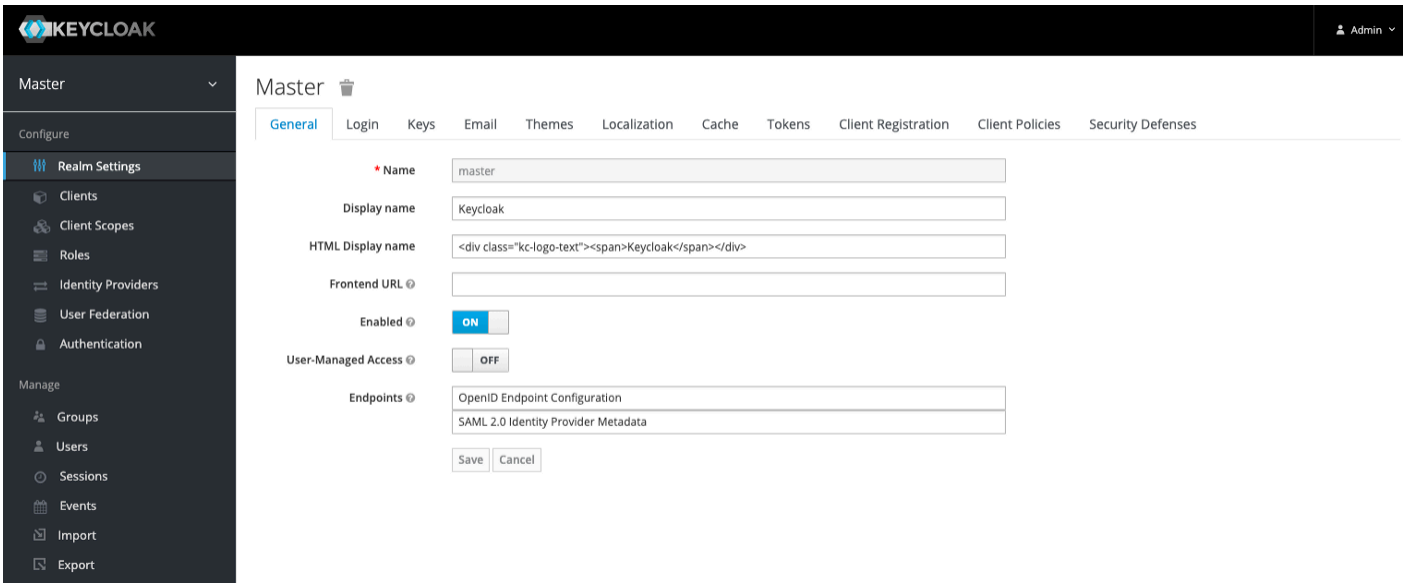
Sendo muito fácil de configurar e implantar a gestão de identidade, o KeyCloak vem sendo usado cada vez mais pelas instituições.

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 Márcia 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 para 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

Questões Comentadas - Autenticação e seus Mecanismos - CESPE

1. CEBRASPE (CESPE) - Ana Sist (EMPREL)/EMPREL/2023

Em situações de gerenciamento de acesso de usuários a sistemas críticos, o uso de ferramentas de segundo fator de autenticação e gerenciamento de acesso privilegiado é restrito aos administradores do sistema.

Comentários:

O uso de ferramentas de segundo fator de autenticação e gerenciamento de acesso privilegiado não se restringe apenas aos administradores do sistema, mas pode ser estendido a outros usuários que acessam sistemas críticos, dependendo da política de segurança da organização.

Gabarito: E

---

2. CEBRASPE (CESPE) - Ana Sist (EMPREL)/EMPREL/2023

No Single Sign-On, a funcionalidade em que as informações de login e senha permitem um melhor controle da equipe de TI é

a) a autenticação multifator.

b) o gerenciamento interno de credenciais.

c) a velocidade na recuperação de senhas.

d) o ponto único para reinserir senha.

e) a melhor aplicação da política de senha.

Comentários:

No Single Sign-On, o gerenciamento interno de credenciais é a funcionalidade que permite um melhor controle da equipe de TI, pois centraliza o gerenciamento das credenciais dos usuários, facilitando o controle de acesso e a revogação de permissões. Vejam que a questão não restringe qualquer aspecto de função ou privilégio.

Gabarito: B

---

3. 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. É importante sempre lembrar essa diferença básica da autenticação e autorização.

Gabarito: C

---

4. 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 à frente algumas questões mais práticas sobre o funcionamento desses aplicativos? 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 é importante destacar que aqui nós temos o modelo de algo que você sabe, com algo que você possui.

Gabarito: C

---

5. 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, 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

---

6. 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 autenticação 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 pré-requisitos.

Gabarito: C

---

7. 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

---

8. 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

9. 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

---

10. (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 baseada no mecanismo de "algo que você é". Como sabemos, esse é um procedimento de segurança da informação.

Gabarito: C

---

11. (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

---

12. (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

---

13. (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

Questões Comentadas - Autenticação e seus Mecanismos - FCC

1. (FCC - Ana (COPERGÁS)/COPERGÁS/Sistemas/2023)

Considere as seguintes medidas de segurança:

I. Centralizar o controle de acesso para todos os ativos corporativos por meio de um serviço de diretório ou provedor de SSO, onde houver suporte.

II. Usar Single-Factor Authentication (SFA) para todas as contas de acesso administrativo, em todos os ativos corporativos, sejam estes gerenciados no site local ou por meio de um provedor terceirizado, pois esta é a medida de acesso seguro mais usada atualmente nas organizações.

III. Definir e manter o controle de acesso baseado em funções, determinando e documentando os direitos de acesso necessários para cada função dentro da organização para cumprir com sucesso suas funções atribuídas.

IV. Estabelecer e seguir um processo, de preferência manual, para manter o acesso aos ativos corporativos, por meio da ativação de contas antigas imediatamente após o encerramento, revogação de direitos ou mudança de função de um usuário.

São medidas recomendadas e adequadas para a gestão do controle de acesso o que se afirma APENAS em

a) I e III.

b) II e IV.

c) I.

d) III e IV.

e) II.

Comentários:

Vamos aos itens:

I - Correto. Conforme vimos, o SSO é, sem dúvida, uma boa prática a ser implantada.

II - Incorreto. A recomendação é o MFA e não o SFA.

III - Correto. Estamos falando do RBAC. Lembrando que atualmente já temos o ABAC que é ainda mais recomendado.

IV- Incorreto. Processo manual? Forçando a barra. Ainda, deve-se desativar as contas antigas, e não ativar.

Gabarito: A

---

2. (FCC - TJ TRT18/TRT 18/Apoio Especializado/Tecnologia da Informação/2023)

Um serviço da web RESTful autentica solicitações antes de enviar uma resposta, usando métodos de autenticação. O método que combina senhas e tokens para acesso de login seguro, no qual primeiro o servidor solicita uma senha e, depois, um token adicional para concluir o processo de autorização, é o

a) API Key Security.

b) RSA Authentication.

c) Webhook.

d) Swagger SSO.

e) OAuth.

Comentários:

Vimos que o processo de troca de tokens (Bearer Token), é característico do OAUTH, correto? Apenas para validarmos os demais:

a) A autenticação por chave de API é um método que utiliza uma chave única (token) para autenticar um usuário ou aplicativo. No entanto, ela não combina senhas e tokens para acesso de login seguro. A chave de API é geralmente usada para identificar o aplicativo que faz a chamada da API, mas não é considerada segura para autenticação de usuários.

b) A autenticação RSA é um método de autenticação que utiliza criptografia de chave pública para autenticar usuários. Ela não combina senhas e tokens para acesso de login seguro. Em vez disso, usa um par de chaves pública e privada para autenticação.

c)Webhook é uma função de callback baseada em HTTP que viabiliza a comunicação entre duas interfaces de programação de aplicações (APIs). Ele não é um método de autenticação, mas sim um meio de enviar dados em tempo eal entre dois sistemas ou aplicativos distintos.

d) Swagger SSO (Single Sign-On) é um recurso do SwaggerHub On-Premise que suporta autenticação de usuários via Okta (SAML 2.0), Active Directory, OpenLDAP e GitHub. No entanto, ele não combina senhas e tokens para acesso de login seguro. Em vez disso, ele permite que os usuários façam login usando suas contas existentes nesses provedores de identidade.

Gabarito: E

---

3. (FCC - AM (MPE PB)/MPE PB/Analista de Sistemas/Administrador de Banco de Dados/2023)

Um Analista está utilizando o protocolo OAuth2 (RFC 6749) e, após realizar todos os passos para obtenção e geração de um access token em condições ideais, recebeu o seguinte retorno:

{

"access_token": "57f10f0e-3d2e-311f-a797-4011f66e1cbf",

" I ": "ca81cb16-43e4-3e96-aaea-4861e7791dc7",

"token_type": "access_token",

"expires_in": 3600

}

Considerando que a lacuna I se refere ao campo que poderá ser utilizado para atualizar um access token que tenha expirado, esta é corretamente denominada:

a) refresh_token

b) redirect_uri

c) extraInfo

d) expired_token

e) redirect_token

Comentários:

Vejam que a estrutura da questão assusta, pode imaginarmos que temos que saber codificar. Mas aqui o nosso conhecimento dos conceitos da base teórica são suficientes. Vimos que na Etapa 4 do fluxo do OAUTH, há o envio do TOKEN e do REFRESH TOKEN, este último sendo útil para geração de um novo TOKEN caso o primeiro expire.

Além disso, os demais parâmetros basicamente indicam o tipo de TOKEN e o prazo de validade. Em relação aos tipos de token temos:

Bearer: Este é o tipo de token mais comum. Qualquer parte que possua o token (um "portador") pode usar o token da mesma maneira que qualquer outra parte que o possua. Usar um token do tipo "Bearer" não requer que o portador prove a posse de material criptográfico (prova de posse).

MAC: Se você escolher o tipo MAC e sign_type (padrão hmac-sha-1 na maioria das implementações), o token de acesso é gerado e mantido como segredo no gerenciador de chaves como um atributo, e um segredo criptografado é enviado de volta como access_token.

Em relação aos outros itens:

b) redirect_uri: Este é o URI para o qual o cliente é redirecionado após a conclusão da autorização. Não é usado para atualizar um access_token.

c) extraInfo: Este não é um campo padrão no OAuth2. Pode ser usado para informações adicionais, mas não para atualizar um access_token.

d) expired_token: Este não é um campo padrão no OAuth2. O access_token expirado é inútil e não pode ser usado para obter um novo access_token.

e) redirect_token: Este não é um campo padrão no OAuth2. O redirect_uri do item B é usado no fluxo de autorização, mas não há redirect_token no OAuth2.

Gabarito: A

4. (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

Questões Comentadas - Autenticação e seus Mecanismos - FGV

1. 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 Márcia 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 para 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

2. 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

3. 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

4. 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

5. 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

Lista de Questões - Autenticação e seus Mecanismos - CESPE

1. CEBRASPE (CESPE) - Ana Sist (EMPREL)/EMPREL/2023

Em situações de gerenciamento de acesso de usuários a sistemas críticos, o uso de ferramentas de segundo fator de autenticação e gerenciamento de acesso privilegiado é restrito aos administradores do sistema.

2. CEBRASPE (CESPE) - Ana Sist (EMPREL)/EMPREL/2023

No Single Sign-On, a funcionalidade em que as informações de login e senha permitem um melhor controle da equipe de TI é

a) a autenticação multifator.

b) o gerenciamento interno de credenciais.

c) a velocidade na recuperação de senhas.

d) o ponto único para reinserir senha.

e) a melhor aplicação da política de senha.

3. 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.

4. 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.

5. 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.

6. 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.

7. 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.

8. 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.

9. 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).

10. (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.

11. (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.

12. (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).

13. (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.

GABARITO

GABARITO

1. E
2. B
3. C
4. C
5. D
6. C
7. C
8. E
9. C
10. C
11. E
12. C
13. C

Lista de Questões - Autenticação e seus Mecanismos - FCC

1. (FCC - Ana (COPERGÁS)/COPERGÁS/Sistemas/2023)

Considere as seguintes medidas de segurança:

I. Centralizar o controle de acesso para todos os ativos corporativos por meio de um serviço de diretório ou provedor de SSO, onde houver suporte.

II. Usar Single-Factor Authentication (SFA) para todas as contas de acesso administrativo, em todos os ativos corporativos, sejam estes gerenciados no site local ou por meio de um provedor terceirizado, pois esta é a medida de acesso seguro mais usada atualmente nas organizações.

III. Definir e manter o controle de acesso baseado em funções, determinando e documentando os direitos de acesso necessários para cada função dentro da organização para cumprir com sucesso suas funções atribuídas.

IV. Estabelecer e seguir um processo, de preferência manual, para manter o acesso aos ativos corporativos, por meio da ativação de contas antigas imediatamente após o encerramento, revogação de direitos ou mudança de função de um usuário.

São medidas recomendadas e adequadas para a gestão do controle de acesso o que se afirma APENAS em

a) I e III.

b) II e IV.

c) I.

d) III e IV.

e) II.

2. (FCC - TJ TRT18/TRT 18/Apoio Especializado/Tecnologia da Informação/2023)

Um serviço da web RESTful autentica solicitações antes de enviar uma resposta, usando métodos de autenticação. O método que combina senhas e tokens para acesso de login seguro, no qual primeiro o servidor solicita uma senha e, depois, um token adicional para concluir o processo de autorização, é o

a) API Key Security.

b) RSA Authentication.

c) Webhook.

d) Swagger SSO.

e) OAuth.

3. (FCC - AM (MPE PB)/MPE PB/Analista de Sistemas/Administrador de Banco de Dados/2023)

Um Analista está utilizando o protocolo OAuth2 (RFC 6749) e, após realizar todos os passos para obtenção e geração de um access token em condições ideais, recebeu o seguinte retorno:

{

"access_token": "57f10f0e-3d2e-311f-a797-4011f66e1cbf",

" I ": "ca81cb16-43e4-3e96-aaea-4861e7791dc7",

"token_type": "access_token",

"expires_in": 3600

}

Considerando que a lacuna I se refere ao campo que poderá ser utilizado para atualizar um access token que tenha expirado, esta é corretamente denominada:

a) refresh_token

b) redirect_uri

c) extraInfo

d) expired_token

e) redirect_token

4. (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.

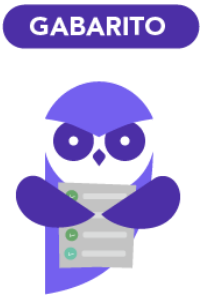
b) da íris

c) da retina.

d) cognitiva.

e) teclar.

GABARITO



1. A
2. E
3. A
4. C

Lista de Questões - Autenticação e seus Mecanismos - FGV

1. 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 Márcia deve escolher é

A) JBoss.

B) Keycloak.

C) Kibana.

D) RabbitMQ.

E) Wildfly.

2. 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.

3. 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.

4. 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.

5. 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.

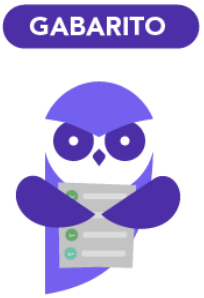
B) íris.

C) retina.

D) face.

E) voz.

GABARITO



1. B
2. E
3. B
4. E
5. B

RECURSO PARA GESTÃO DE ACESSO

IAM – Identity Access Management

PAM – Privileged Access Management

NTLM - Windows NT LAN Manager

Já vimos em momentos anteriores os desafios de se gerenciar os processos e etapas de autenticação e autorização, mantendo toda a rastreabilidade necessária nesse processo. Passamos pela referência prática do AAA.

Sendo assim, vamos tratar agora desses dois instrumentos que são de suma importância para a gestão de acesso nas organizações. Estamos falando do IAM e PAM.

De forma bem direta, vamos desde já diferenciá-los. O IAM possui foco na gestão de acessos de uma forma geral aos serviços e ambientes da organização. O PAM traz um olhar mais qualificado ao tratar as políticas de acesso para usuários privilegiados, ou seja, aqueles usuários que precisam interagir com áreas mais sensíveis da organização

Nesse contexto, ainda aparece o NTLM como solução mais antiga, porém, ainda com propósito de providenciar modelos de autenticação com base em modelo de desafio e resposta, algo semelhante ao que se pratica nas soluções de IPSeC, por exemplo.

Sendo assim, de forma bem objetiva, é importante termos a clareza dos três instrumentos:

- **IAM (Gerenciamento de Identidade e Acesso)** é um termo amplo que abrange uma variedade de tecnologias e processos para gerenciar identidades de usuário e acesso a sistemas e recursos. O IAM pode ser usado para autenticar usuários, autorizar seu acesso a recursos específicos e gerenciar suas permissões ao longo do tempo.
- **PAM (Gerenciamento de Acesso Privilegiado)** é um subconjunto do IAM que se concentra no gerenciamento do acesso de usuários privilegiados, como administradores e contas de serviço. O PAM pode ser usado para restringir o uso de contas privilegiadas, monitorar sua atividade e impedir acesso não autorizado.
- **NTLM (NT LAN Manager)** é um protocolo de autenticação mais antigo que é baseado em autenticação por desafio-resposta. O NTLM é considerado inseguro e não é recomendado para uso em novos sistemas. Se ancorava nas soluções Windows com o Kerberos para gestão de tokens de acesso.

Um ponto que se destaca nesses serviços, principalmente no modelo de PAM, é a gestão de segredos e/ou senhas. Essas soluções possuem a capacidade de se integrar diretamente aos serviços e recursos com vistas a gerar novas senhas dinamicamente para os usuários. Sendo assim, para cada novo acesso, é gerado uma nova senha e o usuário específico somente saberá no momento de solicitação do uso. Com isso, é possível

criar diversas políticas, incluindo aquelas que observam o horário de serviço do profissional, o local de acesso, entre muitas outras. Práticas como essa são conhecidas como acesso “just-in-time”.

Ainda, na ótica de capacidades, carece destacar que essas soluções podem incluir e excluir usuários, incorporar práticas de múltiplos fatores de autenticação, entre outros. Eles visam garantir que os usuários tenham o acesso certo com base em suas funções, responsabilidades e no princípio do menor privilégio. São soluções necessárias para uma arquitetura de segurança que se baseie na prática de Zero Trust.

Evoluindo o nível de controle exigido pelas soluções de PAM, é fundamental saber exatamente o que foi executado por um usuário com conta privilegiada. Nessa ótica, ainda são incorporadas funcionalidades de monitoramento das sessões, com controle de práticas e ações, com algum nível de alçada de aprovação ou notificação de grupos de administradores compartilhados para gestão do risco.

Aqui estão alguns exemplos específicos de ferramentas e recursos que podem ser usados em cada solução:

IAM:

- ***Gerenciamento de identidades:*** *ferramentas de gerenciamento de identidade como Active Directory, Okta e OneLogin.*
- ***Gerenciamento de acesso:*** *ferramentas de gerenciamento de acesso como Azure Active Directory, AWS Identity and Access Management (IAM) e Google Cloud Identity and Access Management (IAM).*
- ***Auditoria de acesso:*** *ferramentas de auditoria de acesso como Microsoft Advanced Auditing, AWS CloudTrail e Google Cloud Audit Logging.*

PAM:

- **Controle de acesso privilegiado:** ferramentas de controle de acesso privilegiado como CyberArk Privileged Access Management, BeyondTrust PowerBroker e Centrify Privileged Access Management.
- **Monitoramento de atividade privilegiada:** ferramentas de monitoramento de atividade privilegiada como CyberArk Privileged Session Manager, BeyondTrust PowerBroker Reporting e Centrify Privileged Access Audit.
- **Prevenção de acesso não autorizado:** ferramentas de prevenção de acesso não autorizado como CyberArk Privileged Identity Firewall, BeyondTrust Privileged Password Manager e Centrify Password Vault.

NTLM:

- **Autenticação por desafio-resposta:** o protocolo NTLM é integrado ao Windows e está disponível em todos os sistemas operacionais Windows.

NOÇÕES BÁSICAS DE 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 onerosa 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.

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, 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 restabelecimento dos serviços e do negócio nos casos de necessidade. Por isso, pensar nas pessoas e testar esses planos, por intermédio de questionários e teorias, 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.

NOÇÕES DE GESTÃO DE RISCOS

Costumeiramente ouvimos falar dessa palavrinha tão comum no meio de segurança da informação, que é RISCO! Sem dúvida, considerá-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.

Culminou 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 atrelado 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.

Comentários:

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

Questões Comentadas - Noções Básicas de Gestão de Riscos - FCC

1. (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.

Comentários:

Quando se cria 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

Lista de Questões - Noções Básicas de Gestão de Riscos - FCC

1. (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.

GABARITO

GABARITO

1. E

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.