Estratégia Concursos

Aula 00 - Prof. André Castro

FUNPRESP-EXE (Analista de Previdência Complementar - Área 9: Sistemas e Governança de Tecnologia da Informação) Segurança da Informação - 2024 (Pós-Edital)

Autor:
André Castro

14 de Dezembro 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

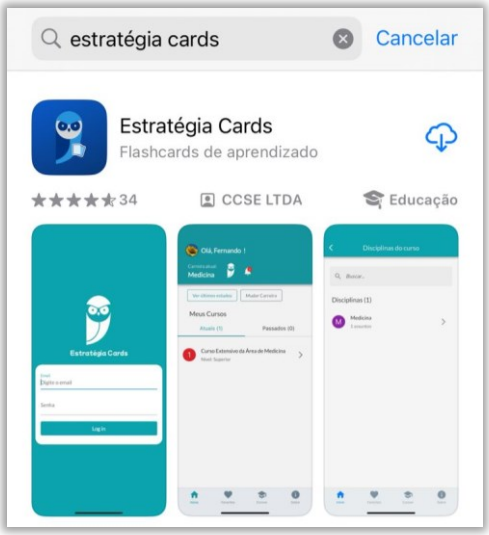
📚 Você tem dificuldade de estudar, memorizar e revisar os conteúdos que estuda em nossas aulas? Então nós temos a ferramenta perfeita para você!

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.

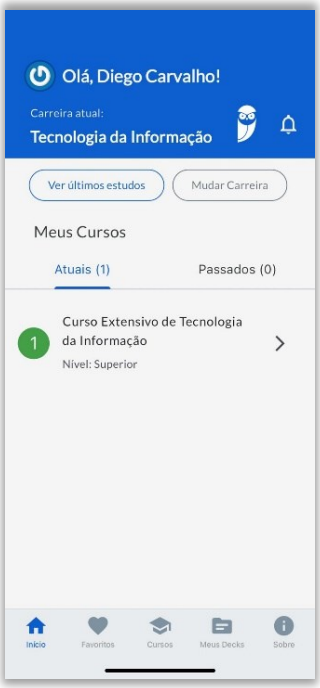
Se você tiver um Android, basta acessar a **Google Play**;

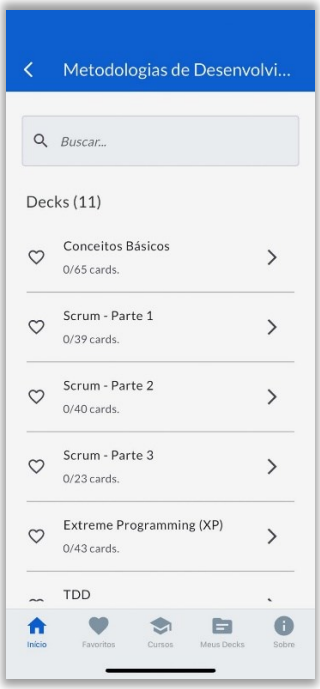
Se for tiver um iPhone, basta acessar a **App Store (iOS)**.

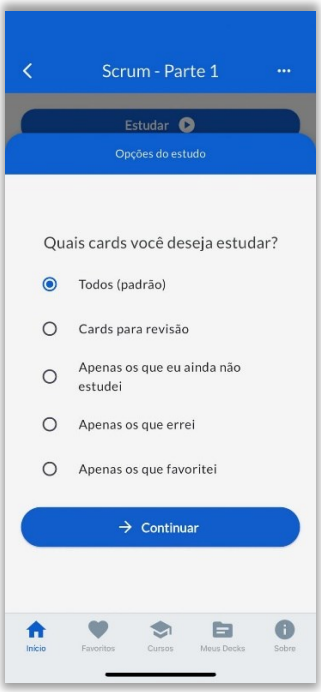
E para acessar?

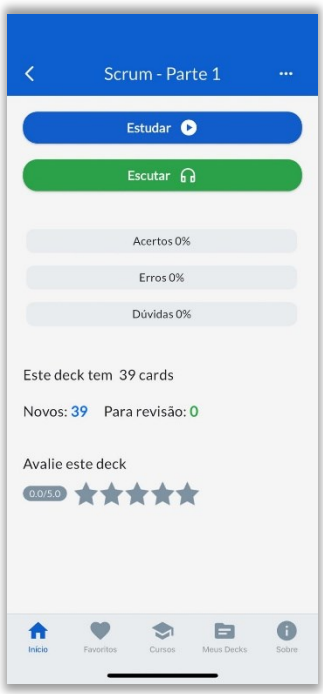
Para acessar, basta ter uma conta no Estratégia Concursos. Em seguida, utilize suas credenciais de login e senha para acessar o aplicativo. Por fim, acessa a carreira de Tecnologia da Informação.

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.

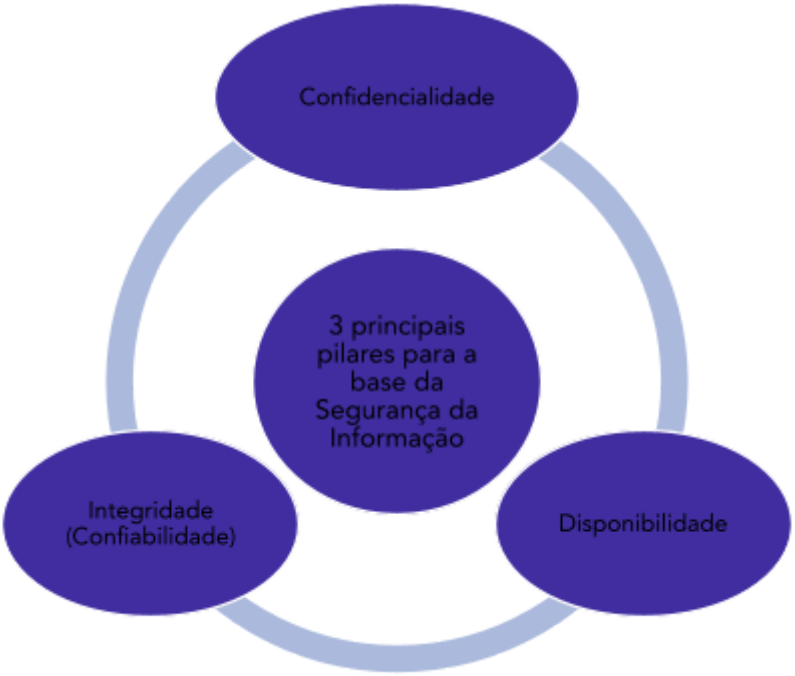
Agora, caso a pessoa altere a mensagem, teremos sim um problema de integridade dos dados.

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.

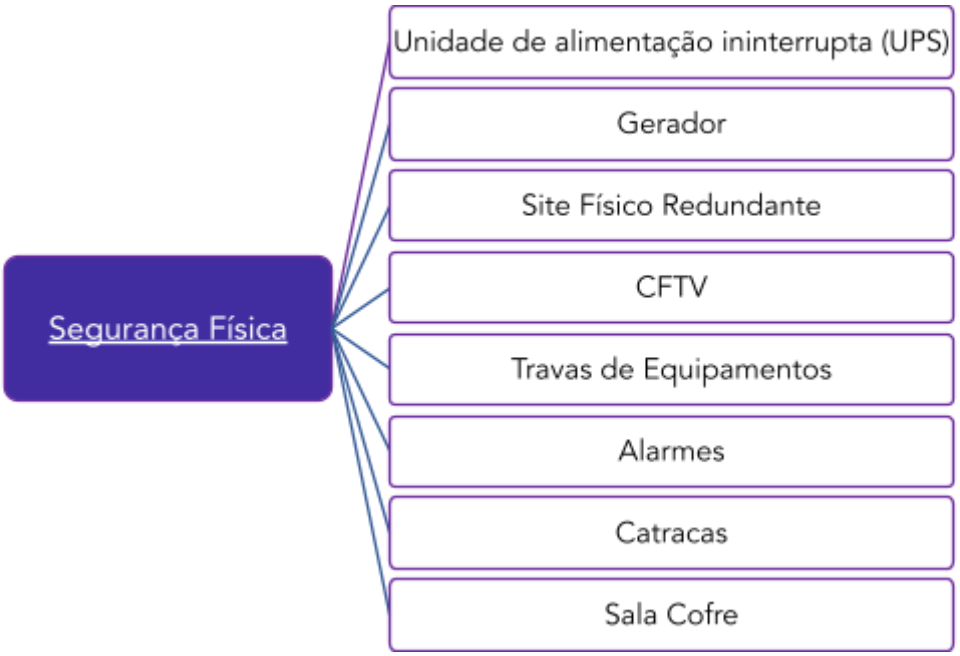
- CFTV – Temos aqui a utilização de câmeras para registro e visualização dos ambientes de uma organização. É um meio eminentemente reativo, uma vez que, na maioria das vezes, é utilizado para gravar o vídeo e ser utilizado posteriormente para análise e auditoria.

- 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.

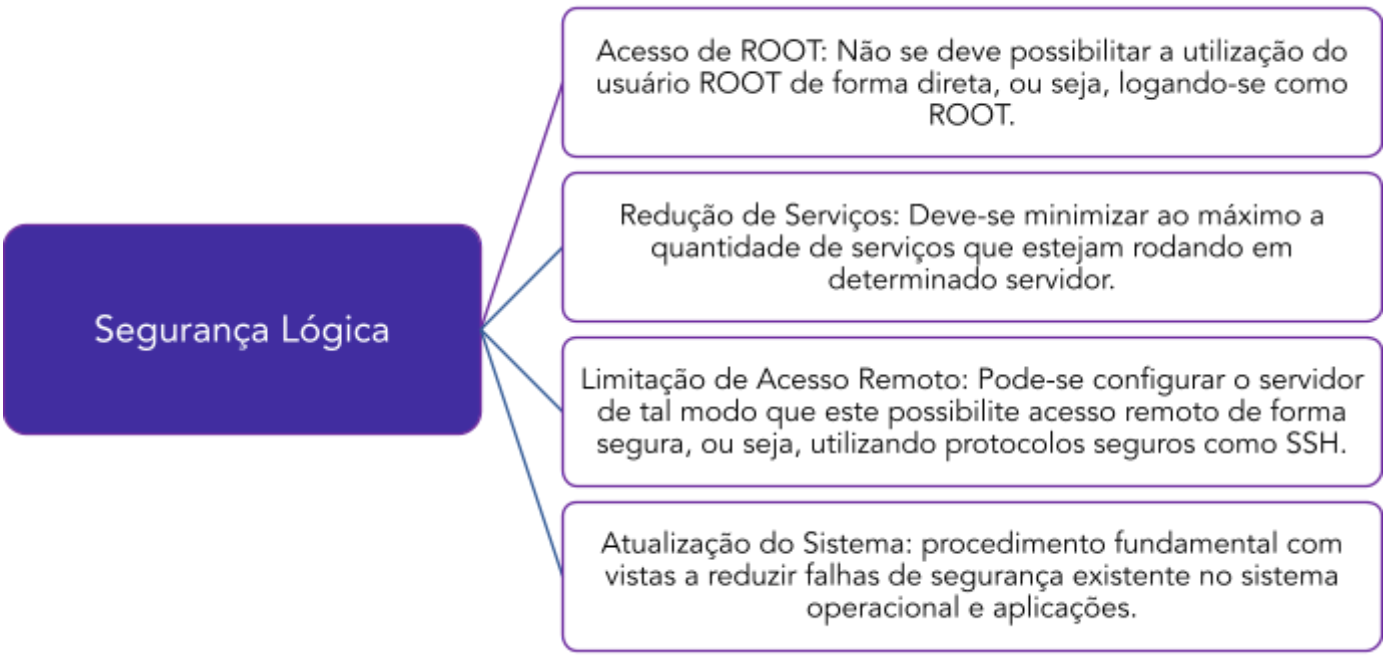
Diversos são os métodos ou regras a serem implementadas. Buscarei elencar algumas e complementaremos, eventualmente, nos exercícios:

- 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.



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

AUDITORIA E CONFORMIDADE

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

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

Em um conceito básico, temos que

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

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

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

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

Quando falamos que devemos registrar os acessos dos usuários, por exemplo, tem-se como pano de fundo o fato de que, em um eventual problema de vazamento de dados, novamente, como exemplo, pode-se avaliar as informações e identificar o responsável por tal ação. Isso está muito atrelado ao conceito do **AAA – Autenticação, Autorização e Auditoria.**

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

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

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

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

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

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

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

Comentários:

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

Questões Comentadas - Noções Básicas de Continuidade de Negócios - CESPE

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

Comentários:

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

Gabarito: errada.

Lista de Questões - Noções Básicas de Continuidade de Negócios - CESPE

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

GABARITO

GABARITO

1. Errada

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.