Estratégia Concursos

Aula 00

Segurança da Informação p/ SEFAZ-RJ (Auditor - Área TI) - 2021 - Pré-Edital

Autor:
André Castro, Equipe Informática e TI

05 de Janeiro de 2021

Apresentação 2

Avaliação de Cursos Anteriores 4

Informações gerais 7

Informações sobre o curso 7

Sobre as aulas 9

AVISO SOBRE RECURSOS EM PROVAS DISCURSIVAS 11

PARE TUDO! E preste atenção!! 19

Princípios de Segurança 20

Segurança de Redes 23

Segurança Física, Lógica e Controle de Acesso 24

Segurança Física 25

Segurança Lógica 28

Controle de Acesso 29

Autenticação e seus mecanismos 31

Biometria 34

Auditoria e Conformidade 36

Continuidade de Negócios 38

Princípios de Normas e Padrões 41

Gerência de Riscos 43

Diretrizes para o Desenvolvimento de Software Seguro 45

SDL (Security Development Lifecycle) 48

CLASP (Comprehensive, Lightweight Application Security Process) 53

SAST (Static Application Security Testing) 54

DAST (Dynamic Application Security Testing) 57

EXERCÍCIOS COMENTADOS 59

Princípios de Segurança 59

Diretrizes para Software Seguro 77

EXERCÍCIOS COMENTADOS COMPLEMENTARES 79

Princípios de Segurança 79

LISTA DE EXERCÍCIOS 88

Princípios de Segurança 88

Diretrizes para Software Seguro 95

LISTA DE EXERCÍCIOS COMPLEMENTARES 96
Princípios de Segurança 96
GABARITO 101
Gabarito – Questões CESPE 101
Gabarito – Questões FCC 103

APRESENTAÇÃO

Olá pessoal, como estão? Espero que bem e ansiosos pelo nosso curso. Antes de tudo, gostaria de desejar-lhes boas-vindas ao nosso curso aqui no Estratégia!

Meu nome é André Castro! Sou formado em engenharia de Redes de Comunicação pela Universidade de Brasília – UnB, pós-graduado e mestrando na área de Segurança e Administração de Redes também pela UnB.

Comecei minha jornada em concursos públicos em 2009, ainda no oitavo semestre do curso de graduação, sendo **aprovado e classificado** no concurso para Analista de Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão. Agora já temos um novo nome, sendo Ministério do Planejamento, Desenvolvimento e Gestão.

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.

Exerço 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.

Possuo também algumas certificações na área de Tecnologia da Informação, como **CCNA, Itil Foundation e Cobit Foundation.**

Para ser aprovado nesses concursos, tive que experimentar a vida de *concurseiro ou concursando, como queiram*. Permaneço nela até hoje com outros objetivos, além da necessidade de sempre se manter atualizado e aprimorando esses anos de experiência.

Acrescido a isso, a experiência que tenho na área acadêmica me trouxe alguma bagagem para aprimorar ainda mais esse curso, **bem como nossa didática de ensino**.

Sei que as dificuldades para o *concursando* são muitas, mas posso afirmar que vale a pena cada esforço, **não só pela remuneração ($$$), mas pelos benefícios e vantagens oferecidos pelo setor público**, além da oportunidade de servir o cidadão brasileiro, em busca de uma máquina pública mais eficaz e eficiente.

Portanto, vamos persistir juntos nessa caminhada e espero poder contribuir bastante em sua jornada. E sempre lembrando que eu gosto bastante de churrasco, principalmente nas comemorações de aprovações!!!

Assim, mãos à obra!!!



AVALIAÇÃO DE CURSOS ANTERIORES

Já ministrei diversos cursos aqui no Estratégia Concursos. Desse modo, já pude receber o devido feedback de meus alunos ao longo desse período, o que tem me dado ainda mais ânimo para continuar trabalhando em nosso material com vistas a um aperfeiçoamento constante.

Abaixo apresento alguns quadros resumos de avaliações realizadas no próprio site do Estratégia Concursos de cursos ministrados, contemplando inclusive alguns cursos de alto grau de exigência de conteúdo.

Curso: Tecnologia da Informação (Parte II) p/ Analista de TI do MPOG

Total de avaliações: **117**

Não querem avaliar: **0**

Qualidade do curso:	Insuficiente 1 (0.87%)	**Regular** 4 (3.48%)	**Bom** 54 (46.96%)	**Excelente** 56 (48.70%)
Tempestividade e pertinência das respostas ao fórum de dúvidas:	Insuficiente 2 (1.74%)	**Regular** 3 (2.61%)	**Bom** 57 (49.57%)	**Excelente** 53 (46.09%)
Teria interesse em fazer outro curso com o professor?	**Não** 0 (0.00%)	**Sim** 0 (0.00%)		
Você aprovou esse curso?	**Não** 2 (1.79%)	**Sim** 110 (98.21%)		

Curso: Tecnologia da Informação (Parte III) p/ TCU - Auditor (Tecnologia da Informação)

Total de avaliações: **62**

Não querem avaliar: **0**

Qualidade do curso:	Insuficiente 2 (3.39%)	**Regular** 3 (5.08%)	**Bom** 21 (35.59%)	**Excelente** 33 (55.93%)
Tempestividade e pertinência das respostas ao fórum de dúvidas:	Insuficiente 2 (3.51%)	**Regular** 2 (3.51%)	**Bom** 21 (36.84%)	**Excelente** 32 (56.14%)
Teria interesse em fazer outro curso com o professor?	**Não** 0 (0.00%)	**Sim** 0 (0.00%)		
Você aprovou esse curso?	**Não** 3 (5.26%)	**Sim** 54 (94.74%)		

Curso: Tecnologia da Informação p/ TRT-MG (parte III) - Analista

Total de avaliações: **94**

Não querem avaliar: **0**

Qualidade do curso:	Insuficiente 0 (0.00%)	**Regular** 3 (3.26%)	**Bom** 52 (56.52%)	**Excelente** 37 (40.22%)
Tempestividade e pertinência das respostas ao fórum de dúvidas:	Insuficiente 0 (0.00%)	**Regular** 2 (2.17%)	**Bom** 51 (55.43%)	**Excelente** 39 (42.39%)
Teria interesse em fazer outro curso com o professor?	**Não** 0 (0.00%)	**Sim** 0 (0.00%)		

Você aprovou esse curso?	Não 2 (2.22%)	Sim 88 (97.78%)

Dessa forma, contem comigo para contribuir com vocês nessa jornada.
Creio que tenho muito a compartilhar com vocês!

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.

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 as 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.

AVISO SOBRE RECURSOS EM PROVAS DISCURSIVAS

(Caso se aplique ao seu concurso)

Quero tomar três minutinhos seus para apresentar-lhes esse trecho que entendo ser de suma importância para os candidatos de concursos públicos, sendo mais uma fase que muitos não dão a devida relevância.

A fase de recursos de provas e questões discursivas.

Sempre em minha vida de *concurseiro* apresento recursos nas minhas provas discursivas, tanto para almejar aprovação, como para aumentar a nota em busca de uma melhor classificação.

Com alguns resultados bastante positivos, entendi a importância dessa fase. Destaca-se que à época, eu sempre fazia meus recursos. Aumentei ainda mais meu desempenho em uma oportunidade de um conteúdo específico em que contratei um professor para fazer o recurso para mim de direito administrativo, o que me gerou também um resultado ainda melhor.

Diante disso, agora do lado de cá *(como professor*, rsrs), devido ao nosso grau de especialização nos conteúdos, disponibilidade de materiais que nem sempre estão ao alcance dos alunos e a experiência adquirida ao longo dos anos, comecei a prestar os serviços de elaboração de recursos para meus alunos e com um índice extremamente satisfatório.

A seguir, alguns resultados:

- Concurso de Analista de Controle Externo do Tribunal de Contas do Estado do Paraná/2016
  - *Assuntos*: Discursiva composta de 4 questões (Redes, Cobit e Eng. De Software)
  - *Total*: 20 pontos
  - *Banca*: CESPE

Nome	Nota P3 Prévia	Nota P3 Após Recurso	Ganho	Resultado
Vinícius Oliveira	10,63	11,29	(6,2%)	CLASSIFICADO (3º Lugar)
Taísa Takehara	8,83	10,28	(16,4%)	CLASSIFICADO (6º para 4º lugar)
Matheus Bastos	8,85	8,97	(1,35%)	
Gustavo Castanho	8,69	9	(3,5%)	
Thiago Lizardo	8,27	9,11	(10,2%)	

  - *Assunto*: Parecer Técnico P4 sobre Eng. De Software e Gestão de Projetos
  - *Total*: 20 pontos
  - Nota de Corte P4: 10 pontos
  - *Banca*: CESPE

Nome	Nota P4 Prévia	Nota P4 Após Recurso	Ganho	Resultado
Vinícius Oliveira	17,1	17,8	(4,1%)	CLASSIFICADO (3º Lugar)
Normel Andrei	9,45	10,36	(9,6%)	APROVAÇÃO



- *Assuntos*: Assinatura Digital – Segurança de Redes
- *Total*: 25 pontos

Nome	Nota Prévia	Nota Após Recurso	Ganho	Resultado
*Carlos Monteiro	15,87	19,87	4 (25,2%)	CLASSIFICADO

*nome fictício a pedido do aluno.

- Concurso de Analista em Tecnologia da Informação – MPOG/ATI /2015
  - *Assunto*: Governança – Cobit
  - *Total*: 40 pontos
  - Nota de Corte: 12 pontos

Nome	Nota Prévia	Nota Após Recurso	Ganho	Resultado
Rafaell Dias Leite Felix	11,5	16,05	4,55 (39,5%)	APROVAÇÃO
Rafael de Souza Berlanda	6,88	11,50	4,62 (67%)	APROVAÇÃO
Filippe da Mata Souza de Lima	10.13	12,63	2,5 (24,7%)	APROVAÇÃO

- Concurso de Analista Judiciário – TRT/MG /2015
  - *Assunto*: Engenharia de Software
  - *Total*: 200 pontos

Nome	Nota Prévia	Nota Após Recurso	Ganho	Resultado
Rômulo Silva Santos	165	175	10 (6%)	21º para 16º



- *Assuntos*: Redes/Segurança e Cobit
- *Total*: 40 pontos
- Nota de Corte: 20 pontos

Nome	Nota Prévia	Nota Após Recurso	Ganho	Resultado
Moiseis Fabian	21,78	25,38	3,6 (16,5%)	APROVAÇÃO
Gilliard Alan	27,06	29,46	2,4 (8,8%)	CLASSIFICADO
Diego Nunes	18,88	20,08	1,2 (6,3%)	APROVAÇÃO

Nesse sentido, gostaria de me colocar à disposição de vocês para o serviço em questão. É extremamente importante que o aluno gere a maior quantidade de informação possível em sua prova discursiva para que possamos ter mais oportunidades de exploração de argumentos no recurso. Já vi descontos de nota por escrever “pouco”, agora não vi por escrever “muito”!

Basta enviar um e-mail para andrecastroprofessor@gmail.com, com:

1. Enunciado da questão;
2. Conteúdo gerado pelo aluno na prova;
3. Espelho de sua correção da prova;
4. Espelho do gabarito apresentado pela banca;
5. Objetivos esperados pelo candidato
    a. Aprovação (a nota está eliminando o candidato);
    b. Entrar na lista de classificados (a pontuação até o momento não é suficiente para estar nas vagas);
    c. Ganhar posições para ficar mais próximo do cadastro reserva;
    d. entre outros.

Diante das questões acima, farei a avaliação o mais breve possível da possibilidade de ganho e retornarei com o orçamento proposto, com modelo de acordo com os objetivos apresentados.

Adianto que o serviço em questão é avulso, prestado exclusivamente por mim e não pelo ESTRATÉGIA CONCURSOS, **uma vez que está fora do escopo previsto para o nosso curso.**

Informo ainda que o modelo de serviço é baseado em uma parcela de execução mais uma parcela de resultado com compartilhamento dos benefícios alcançados.

Importante lembrar que tenho uma quantidade de recursos limite por concurso, sendo o critério de ordem de chegada e fechamento do acordo, os critérios de seleção, até porque o foco é prestar um serviço de qualidade altamente especializado para cada um dos meus alunos.

Lembrando que o esforço é concentrado e geralmente é feito em uma virada de noite tendo em vista o prazo mais padrão de 2 dias a contar da data de divulgação do resultado. Por isso a importância de adiantar a reserva e enviar as informações necessárias para avaliação.

E para fechar, gostaria de lembrar que a fase de recursos de provas discursivas possui a característica de ter um caráter subjetivo do avaliador, de tal modo que não há garantia do resultado, sendo um fator de risco do modelo de serviços em tela. **Obviamente, com a experiência agregada, é que mantenho a taxa de sucesso acima.**

Entretanto, a parcela de compartilhamento de benefícios surge como um fator de garantia de que o serviço será prestado da melhor maneira possível frente ao interesse mútuo. Literalmente o serviço será “como se fosse para mim mesmo”, o que na prática será.

Informo que não restrinjo a prestação do serviço aos assuntos ministrados nesse curso, ou seja, redes e segurança, fator este que será avaliado por mim frente a cada assunto requisitado, conforme conteúdo das questões discursivas.

- Depoimento

"Tenho muito a agradecer ao professor André. Fiz o concurso de ATI do MPOG em 2015 e minha redação precisava de 1,84 ponto para me colocar dentro das vagas. Recorri, então, a vários professores de cursinhos renomados para me ajudar com o recurso e o que ouvi da maioria deles é que seria perda de tempo e de dinheiro, que não valia a pena fazer recurso para a minha redação. Até que um dos professores que rejeitou fazer o meu recurso me passou o contato do professor André pra eu fazer uma consulta. Após retorno do meu contato, enviei minha redação e ele elaborou um recurso muito bem fundamentado, referenciado e agressivo (no bom sentido), sob medida para o Cespe. Mesmo após eu ter enviado o recurso ao Cespe, ele continuou me dando suporte e acompanhando o andamento do resultado junto comigo. Ao sair o resultado, veio a alegria... ganhei 2,5 pontos, entrei nas vagas e hoje sou servidor público federal. A intervenção do professor André foi fundamental para essa conquista que nem eu acreditava que fosse de fato se realizar. Desejo muito sucesso para ele e a todos os concurseiros. Um abraço! ".

Filippe da Mata Souza de Lima

PARE TUDO! E PRESTE ATENÇÃO!!

Hoje eu faço parte de uma equipe **SENSACIONAL** de professores! Depois de muita luta conseguimos reunir **um time** de profissionais extremamente QUALIFICADO e sobretudo **COMPROMISSADO** em fazer o melhor pelos alunos. Para tal criamos um conjunto de ações para nos aproximarmos dos alunos, entendermos suas necessidades e evoluirmos nosso material para um patamar ainda mais diferenciado. São 3 as novidades que gostaria de convidá-lo a conhecer:



Nosso podcast alternativo ... livre, descontraído e com dicas rápidas que todo CANETA PRETA raiz de ouvir. Já temos alguns episódios disponíveis e vários outros serão gravados nas próximas semanas ... acompanhe em:

http://anchor.fm/estrategia-tech



Nosso grupo do Telegram é um local onde ouvimos os alunos e trocamos ideias com eles. Está crescendo a cada dia. A regra do grupo é: só vale falar sobre concursos. Lá divulgamos nossas aulas ao vivo e falamos sobre os concursos abertos, expectativas de novos concursos, revisões de véspera ...

http://t.me/estrategia_ti



Criamos um perfil no Instagram ... e qual o objetivo? Fazer com que os alunos percam tempo nas redes sociais? Claro que não!! Estamos consolidando diversos posts dos professores! São dicas especiais, um patrimônio que deve ser explorado por todos os concurseiros de TI ...

http://instagram.com/estrategiaconcursosti

PRINCÍPIOS DE SEGURANÇA

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

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

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

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



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

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

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

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

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

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

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

3. **Disponibilidade** – Nesse princípio, temos como principal objetivo o fato de determinado recurso poder ser utilizado quando este for requisitado em um determinado momento, considerando a devida autorização do usuário requisitante. 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:

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

2. **Não-Repúdio (Irretratabilidade) –** Neste princípio, busca-se garantir que o usuário não tenha condições de negar ou contrariar o fato de que foi ele quem gerou determinado conteúdo ou informação. 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. ”

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



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

- **Autenticação de entidade Parceiras**
  - Usada em associação com uma conexão lógica com a capacidade de prover confiabilidade a respeito da identidade das entidades conectadas.
- **Autenticação da origem dos Dados**
  - Considerando uma transferência sem conexão entre as partes, visa assegurar que a origem dos dados recebidos é quem ela afirma ser.
- **Confidencialidade de campo seletivo**
  - Busca-se manter a confidencialidade de campos específicos dentro do volume de dados de um usuário em uma conexão.
- **Confidencialidade do fluxo de tráfego**
  - Busca-se gerar a confidencialidade sob a perspectiva do fluxo, ou seja, a simples análise do fluxo de dados não deve ser capaz de gerar informações indevidas.

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

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

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

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

- **Integridade de campo seletivo sem conexão**
  - Mesma condição do tipo acima, porém, de áreas de dados específicos ou seletivos.

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

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

SEGURANÇA DE REDES

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

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

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

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

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

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

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

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

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

Segurança Física, Lógica e Controle de Acesso

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

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

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

SEGURANÇA FÍSICA

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

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



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



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

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

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





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

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

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



SEGURANÇA LÓGICA

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

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

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

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

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 deixa-lo mais robusto e seguro.

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

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

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

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

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

CONTROLE DE ACESSO

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

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

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

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



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

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

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

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

AUTENTICAÇÃO E SEUS MECANISMOS

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

1. *Algo que você sabe*

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

2. *Algo que você tem*

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

3. *Algo que você é*

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

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

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

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

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

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



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

Nesse sentido surge o **conceito de autenticação forte ou de dois fatores (duas etapas).** Como o próprio nome sugere, nada mais é do que dividir a fase de autenticação em duas etapas. Destaca-se que esse processo deve, necessariamente, **envolver a combinação de ALGO QUE VOCÊ SABE, ALGO QUE VOCÊ TEM ou ALGO QUE VOCÊ É.**

Muito cuidado com essa combinação.

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

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

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

Reparem que nesse caso, assumindo que sua senha seja violada, o



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

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

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

Algumas configurações são baseadas em outros instrumentos de autenticação, como o KERBEROS, SMART CARD, SAML (XML)...

BIOMETRIA

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

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

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

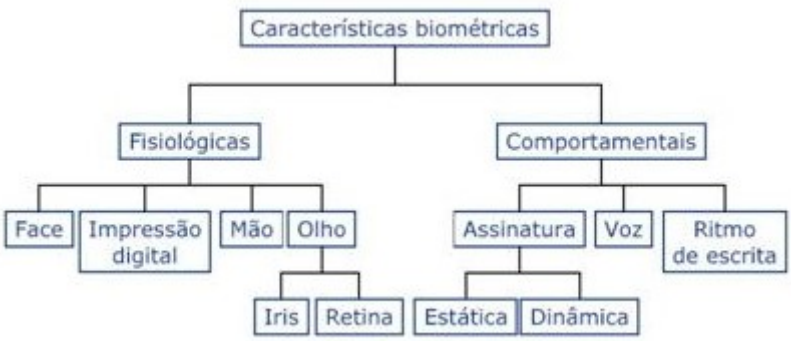
Como vimos anteriormente, o processo de biometria está atrelado à fase de autenticação e autorização, principalmente, para fins de controle de acesso.

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

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

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

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



Fonte: http://www.sinfic.pt

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

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

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

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

AUDITORIA E CONFORMIDADE

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

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

Em um conceito básico, temos que

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

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

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

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

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

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

Falando um pouco sobre conformidade, podemos definir como:

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

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

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

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

CONTINUIDADE DE NEGÓCIOS

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

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

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

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

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

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



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

Nesse momento da foto, várias empresas e negócios já estavam sofrendo com dados e informações perdidas, estruturas de Datacenter danificados. Nesse contexto, uma alternativa era colocar uma redundância ou Backup (solução alternativa para funcionar no caso de parada da principal) no prédio ao lado. Mas todos nós já sabemos o fim que se deu. A gestão da continuidade do negócio não considerou algo que parecia ser impossível, um atentado quase que simultâneo nas duas torres.

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



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

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

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

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

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

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

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

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

1. Falhas humanas;
2. Falhas das soluções e componentes de TI;
3. Fenômenos da natureza que geram acidentes e catástrofes (furação, tempestades, maremotos);
4. Interrupções de abastecimento;
5. Distúrbios civis (greves, vandalismos);
6. Malwares e Vírus;
7. Sabotagem;
8. Terrorismo, etc.

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

PRINCÍPIOS DE NORMAS E PADRÕES

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

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

- **ISO 27001**

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

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

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

- **ISO 27002**

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

- **ISO 27003**

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

- **ISO 27004**

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

- **ISO 27005**

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

- **NBR 15999**

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

- **NBR 22301**

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

- **NBR 31000**

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

GERÊNCIA DE RISCOS

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

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

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

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

Percebam, portanto, que não devemos vincular o conceito de AMEAÇA a alguém mal intencionado com o objetivo de vazar informações ou gerar algum dano. A simples existência de períodos chuvosos com raios pode ser uma ameaça para a vulnerabilidade que utilizamos como exemplo anteriormente, pois, neste caso, poderá gerar descarga nos equipamentos e queimá-los, gerando indisponibilidade dos serviços.

Avançando um pouco mais, temos o conceito de IMPACTO, que considera o resultado gerado decorrente da verificação de um determinado evento de segurança sobre um ou mais recursos. Na maioria das vezes, este resultado está atrelado a algum dano ou prejuízo gerado no momento em que uma ameaça explora determinada vulnerabilidade.

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

Resumindo, portanto, temos:

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

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

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

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



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

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

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

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

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

Diretrizes para o Desenvolvimento de Software Seguro

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

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

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

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

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

- **Senhas Fortes**

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

Creio que a maioria reconheceu que não e está na lista daqueles que negligenciam esse ponto.

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

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

- **Atualização de aplicações**

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

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

- **Fuzzing**

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

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

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

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

- **Boas práticas de Código Seguro**

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

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

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

- *Manipulação de Erros* – O tratamento de erros é um ponto muito importante no desenvolvimento de aplicações seguras. Essas aplicações sempre estarão sujeitas a erros e, por medida de segurança, é importante que haja um padrão de mensagem de erro para o usuário que não vaze informações a respeito da aplicação, evitando assim que um atacante obtenha essas informações para aprimorar seus ataques. Sob a perspectiva do desenvolvedor em utilizar tais mensagens para correção, recomenda-se que este utilize logs das aplicações e controle de forma segura em um ambiente seguro.

- **Baseline de Configuração de Aplicação**

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

Recomendo a leitura da norma complementar nº 16 do DSIC/GSIPR que trata das diretrizes para desenvolvimento de software seguro para a administração pública. É um documento bem curto que vale a pena o esforço. Segue o link:

http://dsic.planalto.gov.br/legislacao/nc_16_software_seguro.pdf

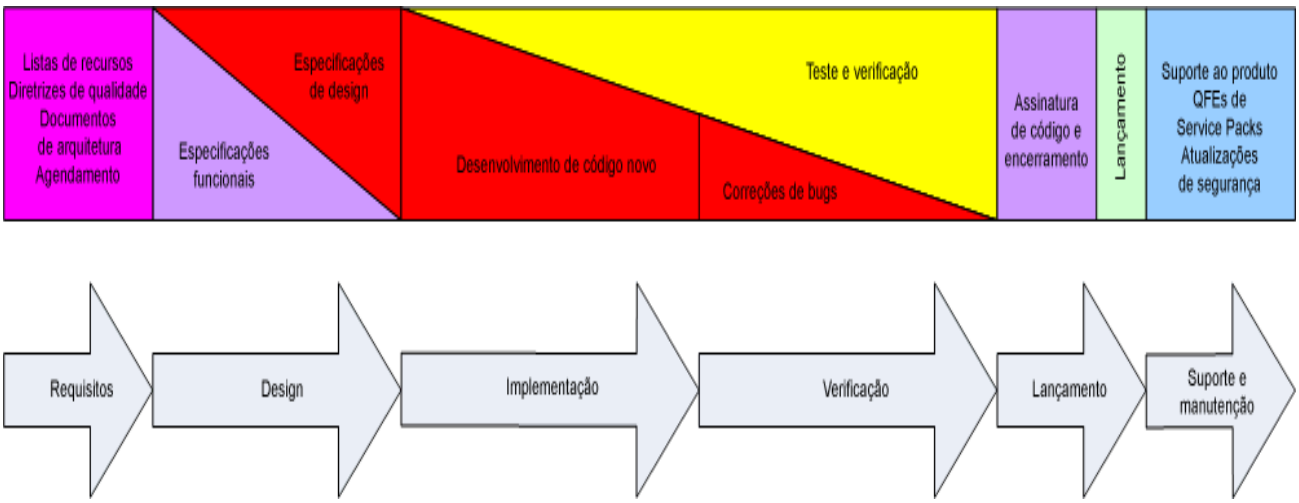
---

SDL (Security Development Lifecycle)

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

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

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



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

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

a) Secure by Design (Seguro por Desenho)

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

b) Secure by Default (Seguro por Padrão)

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

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

c) Secure by Deployment (Seguro na Implantação)

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

d) Communications (Comunicações)

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

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

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

1. FASE DE REQUISITOS

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

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

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

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

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

2. FASE DE DESIGN

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

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

3. FASE DE IMPLEMENTAÇÃO

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

Os resultados da modelagem de ameaças fornecem uma orientação particularmente importante durante a fase de implementação. Os desenvolvedores dedicam atenção especial em corrigir o código de modo a atenuarem as ameaças de alta prioridade e os

testadores concentram seus testes na garantia de que essas ameaças estejam de fato bloqueadas ou atenuadas.

Os elementos do SDL considerados nessa fase são:

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

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

4. FASE DE VERIFICAÇÃO

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

5. FASE DE SUPORTE E MANUTENÇÃO

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

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

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

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

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

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

CLASP (Comprehensive, Lightweight Application Security Process)

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

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

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

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

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

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

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

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

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

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

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

SAST (Static Application Security Testing)

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

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



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

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

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

Podemos considerar como VANTAGENS desse tipo de ferramenta:

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

Como DESVANTAGENS, podemos considerar:

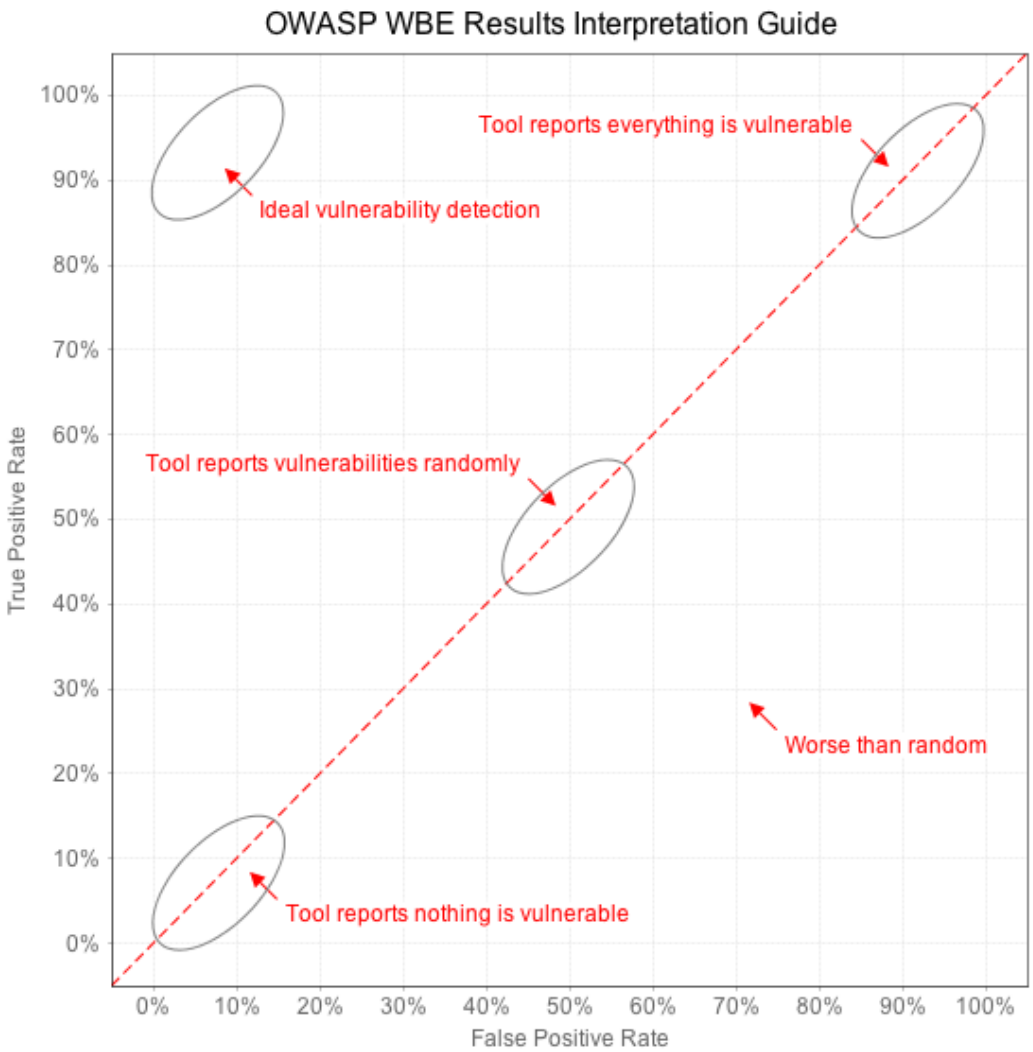
a) Possui capacidade limitada de identificação de falhas, uma vez que os principais ataques são feitos sobre falhas no contexto de funcionamento da solução (aspectos dinâmicos). Desse modo, acabam por atuar sobre uma pequena parcela de todo o rol de vulnerabilidades possíveis;
b) Gera bastante falso-positivo.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

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

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

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

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



DAST (Dynamic Application Security Testing)

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

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

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

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

Podemos elencar como VANTAGENS:

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

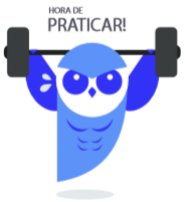
Como DESVANTAGENS:

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

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

Para os alunos que desejarem aprofundar bastante o assunto, recomendo a leitura do link:

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



EXERCÍCIOS COMENTADOS

PRINCÍPIOS DE SEGURANÇA

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

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

Comentários:

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

Gabarito: C

---

2. CESPE – TCE-PR/Analista de Controle – Área TI/2016

A integridade de dados que detecta modificação, inserção, exclusão ou repetição de quaisquer dados em sequência, com tentativa de recuperação, é a integridade

A conexão com recuperação.

B autenticação da origem de dados.

C entidade par a par.

D conexão com campo selecionado.

E fluxo de tráfego.

Comentários:

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

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

Gabarito: A

---

3. CESPE – TJDFT/Analista Judiciário – Análise de Sistemas/2015

Possíveis dificuldades apresentadas por colaboradores para acessar as informações do sistema da organização por mais de dois dias indicam de violação da autenticidade das informações.

Comentários:

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

Gabarito: E

---

4. CESPE – TJDFT/Analista Judiciário – Análise de Sistemas/2015

Se, para cometer o incidente, um colaborador usou software sem licenciamento regular e sem autorização formal da política de segurança da organização, então houve violação da integridade das informações da organização.

Comentários:

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

Gabarito: E

---

5. CESPE – TJDFT/Analista Judiciário – Análise de Sistemas/2015

Se um colaborador conseguiu visualizar informações das quais ele não possuía privilégios, então houve violação da confidencialidade das informações.

Comentários:

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

Gabarito: C

---

6. CESPE – ANTAQ/Analista Administrativo – Infraestrutura de TI/2014

Confidencialidade diz respeito à propriedade da informação que não se encontra disponível a pessoas, entidades ou processos não autorizados.

Comentários:

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

Gabarito: C

---

7. CESPE – TCE-RO/Analista de Informática/2013

Considere que um arquivo que esteja sendo transferido entre dois usuários tenha sido interceptado e seu conteúdo tenha sido visualizado e encaminhado a outros usuários. Nessa situação, caracterizou-se a ocorrência do comprometimento da integridade do arquivo

Comentários:

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

Gabarito: E

---

8. CESPE – TCE-RO/Analista de Informática/2013

Se um sítio da web sofrer comprometimento devido a problemas de hardware no servidor, impossibilitando a visualização do conteúdo pelos usuários, esse fato poderá ser considerado como comprometimento da disponibilidade do serviço.

Comentários:

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

Gabarito: C

---

9. CESPE – CNJ/Técnico Judiciário – Programação de Sistemas/2013

A proteção aos recursos computacionais inclui desde aplicativos e arquivos de dados até utilitários e o próprio sistema operacional.

Comentários:

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

Gabarito: C

---

10. CESPE – CNJ/Técnico Judiciário – Programação de Sistemas/2013

O princípio da autenticidade é garantido quando o acesso à informação é concedido apenas a pessoas explicitamente autorizadas.

Comentários:

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

Gabarito: E

11.CESPE – TRE-RJ/Analista Judiciário – Análise de Sistemas/2012

Na atualidade, os ativos físicos de uma organização são mais importantes para ela do que os ativos de informação.

Comentários:

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

Gabarito: E

12.CESPE – TRE-RJ/Analista Judiciário – Análise de Sistemas/2012

O termo de confidencialidade, de acordo com norma NBR ISO/IEC, representa a propriedade de salvaguarda da exatidão e completude de ativos.

Comentários:

Temos aqui a descrição de Integridade, certo?

Gabarito: E

13.CESPE – TRE-RJ/Analista Judiciário – Análise de Sistemas/2012

Na área de segurança da informação, vulnerabilidade representa causa potencial de um incidente indesejado.

Comentários:

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

Gabarito: E

14.CESPE – TRE-RJ/Analista Judiciário – Análise de Sistemas/2012

A contratação de grande quantidade de novos empregados para a empresa é um incidente grave para a segurança da informação, que deve ser comunicado ao setor competente e tratado rapidamente.

Comentários:

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

Gabarito: E

15.CESPE – TRE-RJ/Analista Judiciário – Análise de Sistemas/2012

Considere que um usuário armazenou um arquivo nesse servidor e, após dois dias, verificou que o arquivo está modificado, de forma indevida, uma vez que somente ele tinha privilégios de gravação na área em que armazenou esse arquivo. Nessa situação, houve problema de segurança da informação relacionado à disponibilidade do arquivo.

Comentários:

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

Gabarito: E

16.CESPE – TRE-RJ/Analista Judiciário – Análise de Sistemas/2012

Se as mídias das cópias de segurança são enviadas para outro local, fisicamente distante do servidor de arquivos, pelo menos uma vez a cada cinco dias úteis e tendo em vista que o transporte desses dados é feito por uma empresa terceirizada, uma forma de aumentar a segurança dessa informação é efetuar procedimento para criptografar os dados armazenados nas mídias.

Comentários:

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

Gabarito: C

17.CESPE – TJ-ES/Analista Judiciário – Análise de Sistemas/2012

Para o controle lógico do ambiente computacional, deve-se considerar que medidas de segurança devem ser atribuídas aos sistemas corporativos e aos bancos de dados, formas de proteção ao código-fonte, preservação de arquivos de log de acesso ao sistema, incluindo-se o sistema de autenticação de usuários.

Comentários:

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

Gabarito: C

18.CESPE – TJ-AC/Técnico Judiciário – Informática/2012

Para garantir a segurança da informação, é recomendável não apenas a instalação de procedimentos relacionados a sistemas e manipulação de dados eletrônicos, mas também daqueles pertinentes ao controle de acesso físico.

Comentários:

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

Gabarito: C

19.CESPE – TJ-SE/Analista Judiciário – Segurança da Informação/2014

Considere que uma empresa tenha introduzido sistema de autenticação biométrica como controle de acesso de seus funcionários às suas instalações físicas. Nessa situação, o uso desse tipo de controle é um procedimento de segurança da informação.

Comentários:

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

Gabarito: C

20.CESPE – TJ-SE/Analista Judiciário – Segurança da Informação/2014

Separação de tarefas, privilégio mínimo e necessidade de saber são conceitos que identificam os três principais tipos de controle de acesso.

Comentários:

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

Gabarito: E

21.CESPE – TJ-SE/Analista Judiciário – Segurança da Informação/2014

O controle de acesso RBAC (role-based access control) indica, com base em uma engenharia de papéis, o método de acesso, de modo que o nível de acesso de um colaborador, por exemplo, possa ser determinado a partir do tipo de atividade que este exerce.

Comentários:

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

Gabarito: C

22.CESPE – TJ-SE/Analista Judiciário – Segurança da Informação/2014

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

Comentários:

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

Gabarito: C

23.CESPE – SUFRAMA/Analista de Sistemas – Desenvolvimento/2014

O controle de acesso refere-se à verificação da autenticidade de uma pessoa ou de dados. As técnicas utilizadas, geralmente, formam a base para todas as formas de controle de acesso a sistemas ou dados da organização.

Comentários:

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

Gabarito: C

24.CESPE – TCE-RN/Assessor Técnico De Informática – Controle Externo/2015

A prática de contratação de seguro para equipamentos de alto custo de TIC, tais como servidores de alto desempenho e sistemas de armazenamento em escala, caracteriza transferência de risco.

Comentários:

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

Gabarito: C

25.CESPE - TCE-ES/Informática/2013

Tendo em vista que a segurança da informação tem importância estratégica, contribuindo para garantir a realização dos objetivos da organização e a continuidade dos negócios, assinale a opção correta.
a) Os principais atributos da segurança da informação são a autenticidade, a irretratabilidade e o não repúdio.
b) No contexto atual do governo e das empresas brasileiras, a segurança da informação tem sido tratada de forma eficiente, não permitindo que dados dos cidadãos ou informações estratégicas sejam vazados.
c) A privacidade constitui uma preocupação do comércio eletrônico e da sociedade da informação, não estando inserida como atributo de segurança da informação, uma vez que é prevista no Código Penal brasileiro.
d) A área de segurança da informação deve preocupar-se em proteger todos os ativos de informação de uma organização, governo, indivíduo ou empresa, empregando, em todas as situações, o mesmo nível de proteção.
e) Entre as características básicas da segurança da informação estão a confidencialidade, a disponibilidade e a integridade.

Comentários:

Vamos aos itens:

a) Temos que os principais princípios ou atributos da Segurança da Informação são a disponibilidade, integridade e confidencialidade. Muitos já complementam com a autenticidade, formando a nossa DICA. INCORRETO
b) À época, diversas foram a ocorrência de vulnerabilidade e invasões a sites do Governo e de empresas brasileiras. INCORRETO
c) A privacidade é um conceito diretamente ligada ao aspecto da confidencialidade e que muitas vezes são tratados como sinônimos para fins de comunicação dos dados. INCORRETO
d) Não né pessoal? Temos aí uma violação à classificação da informação ou da diferenciação de níveis de acesso considerando o grau de sigilo ou proteção dos dados ou ativos em um determinado ambiente. INCORRETO
e) Ainda que tivéssemos dúvida em algum dos itens acima, essa questão nos traz a tranquilidade na resposta, certo? Temos os três princípios relacionados à Segurança da Informação. CORRETO

Gabarito: E

26.CESPE - TCE-ES/Informática/2013

Assinale a opção correta acerca dos mecanismos de segurança disponíveis para a implementação da segurança da informação.
a) A seleção de mecanismos e controles a serem implementados para promover a segurança da informação deve seguir critérios com base na avaliação do que se deseja proteger, dos riscos associados e do nível de segurança que se pretende atingir.
b) Todos os mecanismos de segurança disponíveis devem ser utilizados, tendo em vista que a segurança da informação exige sempre o grau máximo de proteção dos ativos de informação.
c) Controles físicos, barreiras que limitem o contato ou acesso direto a informação ou à infraestrutura para garantir a existência da informação, não são geridos pela área de segurança da informação.
d) Mecanismos de cifração ou encriptação que permitem a transformação reversível da informação, de forma a torná-la ininteligível a terceiros, em geral, são suficientes para apoiar uma boa estratégia de segurança da informação.
e) Os mais importantes mecanismos de segurança da informação incluem, necessariamente, o emprego de firewalls, detectores de intrusões, antivírus, filtros anti-spam e controle de acesso.

Comentários:

Vamos aos itens:

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

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

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

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

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

Gabarito: A

27.CESPE - TCE-RO/Ciências da Computação/2013

As ações referentes à segurança da informação devem focar estritamente a manutenção da confidencialidade e a integridade e disponibilidade da informação.

Comentários:

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

Gabarito: E

28.CESPE - SUFRAMA/Analista de Sistemas/2014

A utilização de algoritmos de criptografia garante a disponibilidade e a autenticidade de informações em ambientes de tecnologia da informação.

Comentários:

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

Gabarito: E

29.CESPE - SUFRAMA/Analista de Sistemas/2014

A lentidão e a paralisação do funcionamento de um sítio de comércio eletrônico que provê transações para venda de produtos é considerado incidente que viola a confidencialidade das informações do sítio.

Comentários:

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

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

Gabarito: E

30.CESPE - TRT8/Analista Judiciário - Tecnologia da Informação/2013

Considere que, em uma organização, uma planilha armazenada em um computador (o servidor de arquivos) tenha sido acessada indevidamente por usuários que visualizaram as informações contidas na planilha, mas não as modificaram. O princípio da segurança da informação comprometido com esse incidente foi
a) a disponibilidade
b) a autenticidade
c) o não repúdio
d) a confidencialidade
e) a integridade

Comentários:

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

Gabarito: D

31.CESPE – TRT17/Técnico Judiciário – TI/2013

A segurança da informação tem por objetivo proteger as organizações dos vários tipos de ameaças, não se destinando a garantir a continuidade do negócio.

Comentários:

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

Gabarito: E

32.CESPE – ANCINE/Analista Administrativo/2013

No que tange à autenticação, a confiabilidade trata especificamente da proteção contra negação, por parte das entidades envolvidas em uma comunicação, de ter participado de toda ou parte desta comunicação.

Comentários:

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

Gabarito: E

33.CESPE – ANTAQ/Analista de Infraestrutura/2014

A utilização adequada dos mecanismos de criptografia permite que se descubra qualquer alteração em um documento por partes não autorizadas, o que garante a confidencialidade do documento.

Comentários:

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

Gabarito: E

34.CESPE – DEPEN/Área 07/2015

O principal objetivo da segurança da informação é preservar a confidencialidade, a autenticidade, a integridade e a disponibilidade da informação.

Comentários:

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

Gabarito: C

35.CESPE – TCU/Auditor Federal de Controle Externo – TI/2015

Confidencialidade é a garantia de que somente pessoas autorizadas tenham acesso à informação, ao passo que integridade é a garantia de que os usuários autorizados tenham acesso, sempre que necessário, à informação e aos ativos correspondentes.

Comentários:

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

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

Gabarito: E

36.CESPE - 2018 - EBSERH - Analista de Tecnologia da Informação

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

Comentários:

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

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

Gabarito: C

37.CESPE - 2018 - ABIN - Oficial de Inteligência - Área 4

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

Comentários:

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

Gabarito: E

38.CESPE - 2015 - Telebras - Engenheiro - Engenharia de Redes

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

Comentários:

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

Gabarito: C

39.CESPE - 2015 - MEC - Gerente de Suporte

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

Comentários:

A primeira parte da questão está correta. O problema surge na responsabilidade. A auditoria faz os apontamentos e aponta as ações que devem ser tomadas. Nesse caso, a

própria ação seria de manter uma rotina de atualização a respeito dos problemas e riscos de segurança.

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

Gabarito: E

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

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

Comentários:

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

Gabarito: C

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

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

Comentários:

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

Gabarito: C

42.CESPE - 2014 - TJ-SE - Analista Judiciário - Segurança da Informação

Atividades de usuários, exceções e outros eventos são registros ou logs de eventos produzidos e mantidos pela instituição, mas, por constituírem eventos qualitativos, não são objetos apropriados para futuras investigações ou auditorias.

Comentários:

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

Gabarito: E

DIRETRIZES PARA SOFTWARE SEGURO

43.CESPE – CNJ/Técnico Judiciário – Programação de Sistemas/2013

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

Comentários:

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

Gabarito: C

44.CESPE – TCE-PA/Auditor de Controle Externo – Informática/2016

Na metodologia de desenvolvimento seguro de software SDL (Security Development Lifecycle), a modelagem de ameaças é realizada na fase de requisitos.

Comentários:

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

- Definir as diretivas de design e arquitetura de segurança;
- Documentar os elementos da superfície de ataque do software;

- Realizar a modelagem de ameaças;
- Definir critérios de fornecimento complementar.

Gabarito: E

45.CESPE – CNJ/Analista Judiciário – Análise de Sistemas/2013

O SDL é um processo de desenvolvimento de software seguro, que envolve a adição de produtos e atividades, como o desenvolvimento de modelos de ameaças.

Comentários:

Essa é a definição básica do processo contemplado pelo SDL.

Gabarito: C

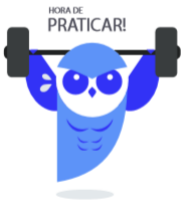
46.CESPE – Polícia Federal/Perito Criminal Federal – Cargo 3/2013

O CLASP (Comprehensive, Lightweight Application Security Process) fornece uma taxonomia de vulnerabilidades que podem ocorrer no código-fonte e que podem ser verificadas com o uso de ferramentas automatizadas para análise estática de código.

Comentários:

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

Gabarito: C



EXERCÍCIOS COMENTADOS COMPLEMENTARES

PRINCÍPIOS DE SEGURANÇA

1. 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

---

2. 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

---

3. 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

---

4. 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

---

5. 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

---

6. 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

---

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

Pedro trabalha na área que cuida da Segurança da Informação de uma empresa. Frente ao risco de indisponibilidade de uma aplicação, criou um servidor de backup para tentar

garantir que as informações sejam replicadas, automaticamente, do servidor principal para o servidor backup de forma redundante. A estratégia utilizada por Pedro para tratar o risco é considerada como
A) aceitação do risco.
B) transferência do risco.
C) eliminação do risco.
D) especificação do risco.
E) mitigação do risco.

Comentário:

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

Gabarito: E

---

8. 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

---

9. FCC – TRF – 4ª Região/Técnico Judiciário/2014

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

a) datiloscópica ou fingerprint.

b) da íris

c) da retina.

d) cognitiva.

e) teclar.

Comentários:

Como vimos em nossa teoria:

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

Gabarito: C

10.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



Bom pessoal, para a nossa primeira aula (AULA 00 - demonstrativa) é isso!

Creio que vocês já puderam identificar um pouco da forma como serão os materiais. Entretanto, é fundamental saber a perspectiva de vocês.

Portanto, o que acharam? Precisamos acrescentar mais exercícios? Mais teoria? Mudar a estruturação dos tópicos? Enfim, estou aberto a sugestões e críticas com o intuito de tornar a nossa aula cada vez mais completa.

As demais aulas estarão disponíveis em breve conforme cronograma proposto e espero poder caminhar junto com vocês em busca da aprovação.

Aguardo vocês nas próximas aulas!

Vamos juntos?!?!?

Um grande abraço.

Instagram

@ProfAndreCastro

Telegram

t.me/ProfessorAndreCastro





LISTA DE EXERCÍCIOS

PRINCÍPIOS DE SEGURANÇA

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

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

---

2. CESPE – TCE-PR/Analista de Controle – Área TI/2016

A integridade de dados que detecta modificação, inserção, exclusão ou repetição de quaisquer dados em sequência, com tentativa de recuperação, é a integridade

A conexão com recuperação.

B autenticação da origem de dados.

C entidade par a par.

D conexão com campo selecionado.

E fluxo de tráfego.

---

3. CESPE – TJDFT/Analista Judiciário – Análise de Sistemas/2015

Possíveis dificuldades apresentadas por colaboradores para acessar as informações do sistema da organização por mais de dois dias indicam de violação da autenticidade das informações.

---

4. CESPE – TJDFT/Analista Judiciário – Análise de Sistemas/2015

Se, para cometer o incidente, o colaborador usou software sem licenciamento regular e sem autorização formal da política de segurança da organização, então houve violação da integridade das informações da organização.

---

5. CESPE – TJDFT/Analista Judiciário – Análise de Sistemas/2015

Se um colaborador conseguiu visualizar informações das quais ele não possuía privilégios, então houve violação da confidencialidade das informações.

---

6. CESPE – ANTAQ/Analista Administrativo – Infraestrutura de TI/2014

Confidencialidade diz respeito à propriedade da informação que não se encontra disponível a pessoas, entidades ou processos não autorizados.

---

7. CESPE – TCE-RO/Analista de Informática/2013

Considere que um arquivo que esteja sendo transferido entre dois usuários tenha sido interceptado e seu conteúdo tenha sido visualizado e encaminhado a outros usuários. Nessa situação, caracterizou-se a ocorrência do comprometimento da integridade do arquivo

---

8. CESPE – TCE-RO/Analista de Informática/2013

Se um sítio da web sofrer comprometimento devido a problemas de hardware no servidor, impossibilitando a visualização do conteúdo pelos usuários, esse fato poderá ser considerado como comprometimento da disponibilidade do serviço.

---

9. CESPE – CNJ/Técnico Judiciário – Programação de Sistemas/2013

A proteção aos recursos computacionais inclui desde aplicativos e arquivos de dados até utilitários e o próprio sistema operacional.

---

10. CESPE – CNJ/Técnico Judiciário – Programação de Sistemas/2013

O princípio da autenticidade é garantido quando o acesso à informação é concedido apenas a pessoas explicitamente autorizadas.

---

11. CESPE – TRE-RJ/Analista Judiciário – Análise de Sistemas/2012

Na atualidade, os ativos físicos de uma organização são mais importantes para ela do que os ativos de informação.

12.CESPE – TRE-RJ/Analista Judiciário – Análise de Sistemas/2012

O termo de confidencialidade, de acordo com norma NBR ISO/IEC, representa a propriedade de salvaguarda da exatidão e completude de ativos.

13.CESPE – TRE-RJ/Analista Judiciário – Análise de Sistemas/2012

Na área de segurança da informação, vulnerabilidade representa causa potencial de um incidente indesejado.

14.CESPE – TRE-RJ/Analista Judiciário – Análise de Sistemas/2012

A contratação de grande quantidade de novos empregados para a empresa é um incidente grave para a segurança da informação, que deve ser comunicado ao setor competente e tratado rapidamente.

15.CESPE – TRE-RJ/Analista Judiciário – Análise de Sistemas/2012

Considere que um usuário armazenou um arquivo nesse servidor e, após dois dias, verificou que o arquivo está modificado, de forma indevida, uma vez que somente ele tinha privilégios de gravação na área em que armazenou esse arquivo. Nessa situação, houve problema de segurança da informação relacionado à disponibilidade do arquivo.

16.CESPE – TRE-RJ/Analista Judiciário – Análise de Sistemas/2012

Se as mídias das cópias de segurança são enviadas para outro local, fisicamente distante do servidor de arquivos, pelo menos uma vez a cada cinco dias úteis e tendo em vista que o transporte desses dados é feito por uma empresa terceirizada, uma forma de aumentar a segurança dessa informação é efetuar procedimento para criptografar os dados armazenados nas mídias.

17.CESPE – TJ-ES/Analista Judiciário – Análise de Sistemas/2012

Para o controle lógico do ambiente computacional, deve-se considerar que medidas de segurança devem ser atribuídas aos sistemas corporativos e aos bancos de dados, formas de proteção ao código-fonte, preservação de arquivos de log de acesso ao sistema, incluindo-se o sistema de autenticação de usuários.

18.CESPE – TJ-AC/Técnico Judiciário – Informática/2012

Para garantir a segurança da informação, é recomendável não apenas a instalação de procedimentos relacionados a sistemas e manipulação de dados eletrônicos, mas também daqueles pertinentes ao controle de acesso físico.

19.CESPE – TJ-SE/Analista Judiciário – Segurança da Informação/2014

Considere que uma empresa tenha introduzido sistema de autenticação biométrica como controle de acesso de seus funcionários às suas instalações físicas. Nessa situação, o uso desse tipo de controle é um procedimento de segurança da informação.

20.CESPE – TJ-SE/Analista Judiciário – Segurança da Informação/2014

Separação de tarefas, privilégio mínimo e necessidade de saber são conceitos que identificam os três principais tipos de controle de acesso.

21.CESPE – TJ-SE/Analista Judiciário – Segurança da Informação/2014

O controle de acesso RBAC (role-based access control) indica, com base em uma engenharia de papéis, o método de acesso, de modo que o nível de acesso de um colaborador, por exemplo, possa ser determinado a partir do tipo de atividade que este exerce.

22.CESPE – TJ-SE/Analista Judiciário – Segurança da Informação/2014

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

23.CESPE – SUFRAMA/Analista de Sistemas – Desenvolvimento/2014

O controle de acesso refere-se à verificação da autenticidade de uma pessoa ou de dados. As técnicas utilizadas, geralmente, formam a base para todas as formas de controle de acesso a sistemas ou dados da organização.

24.CESPE – TCE-RN/Assessor Técnico De Informática – Controle Externo/2015

A prática de contratação de seguro para equipamentos de alto custo de TIC, tais como servidores de alto desempenho e sistemas de armazenamento em escala, caracteriza transferência de risco.

25.CESPE - TCE-ES/Informática/2013

Tendo em vista que a segurança da informação tem importância estratégica, contribuindo para garantir a realização dos objetivos da organização e a continuidade dos negócios, assinale a opção correta.

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

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

c) A privacidade constitui uma preocupação do comércio eletrônico e da sociedade da informação, não estando inserida como atributo de segurança da informação, uma vez que é prevista no Código Penal brasileiro.
d) A área de segurança da informação deve preocupar-se em proteger todos os ativos de informação de uma organização, governo, indivíduo ou empresa, empregando, em todas as situações, o mesmo nível de proteção.
e) Entre as características básicas da segurança da informação estão a confidencialidade, a disponibilidade e a integridade.

26.CESPE - TCE-ES/Informática/2013

Assinale a opção correta acerca dos mecanismos de segurança disponíveis para a implementação da segurança da informação.
a) A seleção de mecanismos e controles a serem implementados para promover a segurança da informação deve seguir critérios com base na avaliação do que se deseja proteger, dos riscos associados e do nível de segurança que se pretende atingir.
b) Todos os mecanismos de segurança disponíveis devem ser utilizados, tendo em vista que a segurança da informação exige sempre o grau máximo de proteção dos ativos de informação.
c) Controles físicos, barreiras que limitem o contato ou acesso direto a informação ou à infraestrutura para garantir a existência da informação, não são geridos pela área de segurança da informação.
d) Mecanismos de cifração ou encriptação que permitem a transformação reversível da informação, de forma a torná-la ininteligível a terceiros, em geral, são suficientes para apoiar uma boa estratégia de segurança da informação.
e) Os mais importantes mecanismos de segurança da informação incluem, necessariamente, o emprego de firewalls, detectores de intrusões, antivírus, filtros anti-spam e controle de acesso.

27.CESPE - TCE-RO/Ciências da Computação/2013

As ações referentes à segurança da informação devem focar estritamente a manutenção da confidencialidade e a integridade e disponibilidade da informação.

28.CESPE - SUFRAMA/Analista de Sistemas/2014

A utilização de algoritmos de criptografia garante a disponibilidade e a autenticidade de informações em ambientes de tecnologia da informação.

29.CESPE - SUFRAMA/Analista de Sistemas/2014

A lentidão e a paralisação do funcionamento de um sítio de comércio eletrônico que provê transações para venda de produtos é considerado incidente que viola a confidencialidade das informações do sítio.

30.CESPE - TRT8/Analista Judiciário - Tecnologia da Informação/2013

Considere que, em uma organização, uma planilha armazenada em um computador (o servidor de arquivos) tenha sido acessada indevidamente por usuários que visualizaram as informações contidas na planilha, mas não as modificaram. O princípio da segurança da informação comprometido com esse incidente foi
a) a disponibilidade
b) a autenticidade
c) o não repúdio
d) a confidencialidade
e) a integridade

31.CESPE – TRT17/Técnico Judiciário – TI/2013

A segurança da informação tem por objetivo proteger as organizações dos vários tipos de ameaças, não se destinando a garantir a continuidade do negócio.

32.CESPE – ANCINE/Analista Administrativo/2013

No que tange à autenticação, a confiabilidade trata especificamente da proteção contra negação, por parte das entidades envolvidas em uma comunicação, de ter participado de toda ou parte desta comunicação.

33.CESPE – ANTAQ/Analista de Infraestrutura/2014

A utilização adequada dos mecanismos de criptografia permite que se descubra qualquer alteração em um documento por partes não autorizadas, o que garante a confidencialidade do documento.

34.CESPE – DEPEN/Área 07/2015

O principal objetivo da segurança da informação é preservar a confidencialidade, a autenticidade, a integridade e a disponibilidade da informação.

35.CESPE – TCU/Auditor Federal de Controle Externo – TI/2015

Confidencialidade é a garantia de que somente pessoas autorizadas tenham acesso à informação, ao passo que integridade é a garantia de que os usuários autorizados tenham acesso, sempre que necessário, à informação e aos ativos correspondentes.

36.CESPE - 2018 - EBSERH - Analista de Tecnologia da Informação

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

37.CESPE - 2018 - ABIN - Oficial de Inteligência - Área 4

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

38.CESPE - 2015 - Telebras - Engenheiro - Engenharia de Redes

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

39.CESPE - 2015 - MEC - Gerente de Suporte

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

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

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

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

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

42.CESPE - 2014 - TJ-SE - Analista Judiciário - Segurança da Informação

Atividades de usuários, exceções e outros eventos são registros ou logs de eventos produzidos e mantidos pela instituição, mas, por constituírem eventos qualitativos, não são objetos apropriados para futuras investigações ou auditorias.

DIRETRIZES PARA SOFTWARE SEGURO

43.CESPE – CNJ/Técnico Judiciário – Programação de Sistemas/2013

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

44.CESPE – TCE-PA/Auditor de Controle Externo – Informática/2016

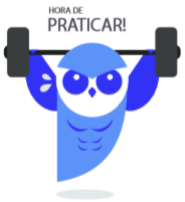
Na metodologia de desenvolvimento seguro de software SDL (Security Development Lifecycle), a modelagem de ameaças é realizada na fase de requisitos.

45.CESPE – CNJ/Analista Judiciário – Análise de Sistemas/2013

O SDL é um processo de desenvolvimento de software seguro, que envolve a adição de produtos e atividades, como o desenvolvimento de modelos de ameaças.

46.CESPE – Polícia Federal/Perito Criminal Federal – Cargo 3/2013

O CLASP (Comprehensive, Lightweight Application Security Process) fornece uma taxonomia de vulnerabilidades que podem ocorrer no código-fonte e que podem ser verificadas com o uso de ferramentas automatizadas para análise estática de código.



LISTA DE EXERCÍCIOS COMPLEMENTARES

PRINCÍPIOS DE SEGURANÇA

1. 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.

---

2. FCC – TRE-CE/Analista Judiciário – Análise de Sistemas/2012

Em relação à segurança da informação, considere:

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

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

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

Os itens I, II e III, associam-se, direta e respectivamente, aos princípios de
a) confidencialidade, integridade e autenticidade.
b) autenticidade, confidencialidade e irretratabilidade.
c) confidencialidade, confidencialidade e irretratabilidade.
d) autenticidade, confidencialidade e autenticidade.
e) integridade, confidencialidade e integridade.

---

3. 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.

---

4. 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.

---

5. 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.

---

6. 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.

---

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

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

D) especificação do risco.
E) mitigação do risco.

---

8. 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.

---

9. FCC – TRF – 4ª Região/Técnico Judiciário/2014

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

a) datiloscópica ou fingerprint.

b) da íris

c) da retina.

d) cognitiva.

e) teclar.

10.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 :

F) acesso lógico.
G) acesso físico.
H) programas.
I) conteúdo.
J) entrada e saída de dados.



GABARITO

GABARITO – QUESTÕES CESPE

1	C
2	A
3	E
4	E
5	C
6	C
7	E
8	C
9	C
10	E
11	E
12	E
13	E
14	E
15	E
16	C
17	C

18	C
19	C
20	E
21	C
22	C
23	C
24	C
25	E
26	A
27	E
28	E
29	E
30	D
31	E
32	E
33	E
34	C
35	E
36	C
37	E
38	C
39	E
40	C
41	C



42	E
43	C
44	E
45	C
46	C

GABARITO – QUESTÕES FCC

1	E
2	A
3	C
4	A
5	D
6	B
7	E
8	B
9	C
10	B

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.