

Aula 00

MPU (Analista - Desenvolvimento de Sistema) Passo Estratégico de Conhecimentos Específicos

Autor:

Thiago Rodrigues Cavalcanti

06 de Janeiro de 2023

SEGURANÇA DA INFORMAÇÃO. CONFIABILIDADE. INTEGRIDADE. DISPONIBILIDADE. MECANISMOS DE SEGURANÇA: CRIPTOGRAFIA, ASSINATURA DIGITAL, GARANTIA DE INTEGRIDADE, CONTROLE DE ACESSO E CERTIFICAÇÃO DIGITAL. GERÊNCIA DE RISCOS: AMEAÇA, VULNERABILIDADE E IMPACTO

Sumário

Análise Estatística.....	2
Roteiro de revisão e pontos do assunto que merecem destaque	2
Segurança da Informação.....	2
Conceitos Básicos	2
Noções de vírus, worms e pragas virtuais	6
Ferramentas para segurança	9
Noções de Criptografia.....	12
Assinatura Digital.....	15
Certificação Digital	16
Auditoria, Vulnerabilidade e Conformidade	21
Aposta Estratégica.....	24
Questões estratégicas	26
Questionário de revisão e aperfeiçoamento.....	33
Perguntas	33
Perguntas com respostas.....	35



ANÁLISE ESTATÍSTICA

A análise estatística estará disponível a partir da próxima aula.

ROTEIRO DE REVISÃO E PONTOS DO ASSUNTO QUE MERECEM DESTAQUE

A ideia desta seção é apresentar um roteiro para que você realize uma revisão completa do assunto e, ao mesmo tempo, destacar aspectos do conteúdo que merecem atenção.

Para revisar e ficar bem preparado no assunto, você precisa, basicamente, seguir os passos a seguir:

Segurança da Informação

A segurança de redes é um tema muito discutido por gestores e analistas de TI. A cada ano que passa, grandes investimentos são feitos para proteger a privacidade, integridade e disponibilidade das informações. Tudo isso por causa dos crescentes ataques e sequestros de dados que atingem diversas pessoas e empresas ao redor do mundo – que duplicaram no ano de 2017, segundo pesquisa da ISOC (Internet Society).

Conceitos Básicos

Os conceitos de segurança da informação estão diretamente relacionados com proteção de um conjunto de informações, no sentido de preservar o valor que possuem para um indivíduo ou uma organização.

De acordo com a norma ISO 17799:2005, “segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio”.

A informação é um ativo que deve ser protegido e cuidado por meio de regras e procedimentos das políticas de segurança, do mesmo modo que protegemos nossos recursos financeiros e patrimoniais. Entretanto, “muitas vezes é difícil obter o apoio da própria alta administração da organização para realizar os investimentos necessários em segurança da informação. Os custos elevados das soluções contribuem para esse cenário, mas o desconhecimento da importância do tema é provavelmente ainda o maior problema”. (CAMPOS, 2007)¹

O Decreto Nº 3.505 de 13 de junho de 2000 instituído pelo presidente da República Federativa do Brasil, define segurança da informação como:

¹ CAMPOS, A. Sistema de segurança da informação: controlando os riscos. Florianópolis: Visual Books, 2ª ed, 2007.



Art. 2. Para efeitos da Política de Segurança da Informação, ficam estabelecidas as seguintes conceituações:

II – Segurança da Informação: proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento.

Dessa forma, a segurança da informação é imprescindível para qualquer organização tanto do ponto de vista estratégico, quanto do tático e operacional.

Antes de falar sobre as políticas de segurança, precisamos entender que na segurança da informação existem quatro princípios básicos, definidos na norma ABNT NBR ISO/IEC 27002:2005, que fundamentam a proteção dos dados. A partir do quadro abaixo vamos citar e definir cada um destes princípios.



O dicionário Aurélio nos dá, entre os dezesseis significados de princípio, dois que se encaixam bem dentro deste contexto: 1 - Frase ou raciocínio que é base de uma arte, de uma ciência ou de uma teoria; 2 - Regras ou conhecimentos fundamentais e mais gerais. Ou seja, um princípio é uma definição sobre algo que se almeja.

Princípio	Definição
D isponibilidade	- Princípio que garante que a informação estará sempre disponíveis.
I ntegridade	- Princípio que garante que as informações serão guardadas ou enviadas em sua forma original, sem sofrer alterações.
C onfidencialidade	- Princípio que garante o sigilo da informação com a capacidade de controlar o acesso, assegurando que elas só serão acessadas por pessoas autorizadas. Ou seja, é a garantia que as informações só serão acessadas através de uma senha.
A utenticidade	- Princípio que permite verificar a identidade de uma pessoa em um sistema, garantindo a veracidade das informações.

Note que foi formado o mnemônico **DICA** para facilitar a memorização e associação das definições.

É importante notar que nos princípios sempre está presente a partícula “...idade”. Por exemplo: caso a banca cite o princípio da autenticação, estará incorreto. O correto é “Princípio da Autenticidade”.



Algumas bancas indicam o Não Repúdio como parte dos princípios de segurança da informação, porém ele só é efetivamente usado junto com o princípio da Autenticidade que garante que as informações são verdadeiras e por este motivo não podem ser refutadas.

Não Repúdio - Incapacidade de negação da autoria de uma informação.
(Irrefutabilidade) (Este princípio está ligado diretamente ao princípio da Autenticidade)

Princípios

Disponibilidade

O operacional de uma organização depende diretamente desse princípio, pois ele está relacionado ao tempo e à acessibilidade que se tem dos dados e sistemas, ou seja, se eles podem ser consultados a qualquer momento pelos colaboradores.

Praticamente todos os processos de trabalho de uma organização dependem da chegada ou busca de uma informação. Quando a informação está indisponível, os processos que dependem dela ficam impedidos de serem executados.

Integridade

Esse princípio é absolutamente crítico do ponto de vista operacional, pois valida todo o processo de comunicação em uma organização. Conforme vimos na tabela acima, é importante que os dados circulem ou sejam armazenados do mesmo modo como foram criados, sem que haja interferência externa para corrompê-los ou comprometê-los.

Toda organização se comunica interna e externamente o tempo todo, transmitindo números, resultados, projeções, estratégias, regras, procedimentos e dados em todas as direções; e a comunicação efetiva só acontece quando o emissor e o receptor da informação a interpretam da mesma maneira.

Informação sem integridade demanda verificação, correção e retrabalho, que causa desperdício de energia, traduzido em perda de recursos, seja tempo, pessoal ou financeiro.

Confidencialidade

A norma ISO/IEC 17799 define confidencialidade como “garantir que a informação seja acessível apenas àqueles autorizados a ter acesso”. Com isso, chegamos à conclusão que a confidencialidade tem a ver com a privacidade dos dados de uma organização. Esse conceito se relaciona às ações tomadas para assegurar que informações confidenciais e críticas não sejam roubadas dos sistemas organizacionais por meio de cyber ataques, espionagem, entre outras práticas.

Para que a confidencialidade seja reforçada, as organizações adotam medidas preventivas, como por exemplo a definição dos níveis de acesso às informações. Isso garante que apenas pessoas autorizadas terão acesso a



dados sensíveis para a organização. Os níveis também precisam ser limitados conforme as áreas a que se relacionam (marketing, vendas, financeiro, administração, etc.).

Além de níveis de acesso para as pessoas, os dados são classificados de acordo com o potencial de impacto, caso sejam acessados por pessoas indevidas. Dessa forma as organizações criam modelos de contingência que abrangem todas as possibilidades.

Autenticidade

Esse princípio identifica e registra as ações de envio ou edição de uma informação, realizadas pelo usuário. Toda ação é documentada, garantido a autenticidade da informação proveniente de uma fonte confiável. Acima citei que esse princípio torna a informação irrefutável, ou seja, a pessoa que cria, edita ou exclui um dado, não pode negar a sua ação.

Métodos Relacionados aos Princípios

Disponibilidade

Um exemplo de disponibilidade é o site para inscrição em um concurso. Dependendo do concurso pode acontecer de o site ficar "fora do ar", ferindo o princípio e causando uma indisponibilidade. Isso normalmente ocorre quando os recursos acessados estão ultrapassando o limite fornecido pelo servidor.

Integridade

Em um arquivo é utilizada uma função hash, que mapeia os dados de comprimento variável para dados de comprimento fixo, criando, a partir dos valores retornados, um código *hash* ou *checksum*. Os algoritmos da função *hash* mais utilizados são MD5 e SHA-1. Os códigos gerados são únicos para cada arquivo, possuem tamanho entre 20 e 256 caracteres e a partir do código gerado não é possível retornar ao arquivo, ou seja, é um processo de via única.

Confidencialidade

O uso de criptografia garante o sigilo quando a informação é confidencial. Existem dois métodos de criptografia: chaves simétricas e chaves assimétricas (com ou sem certificado digital). Além desses métodos, pode ser implantada a autenticação de dois fatores, a verificação biométrica e o uso de token.

Autenticidade

O reconhecimento de firma em um cartório é um exemplo de um método de autenticidade. Em informática o uso de certificado digital é o que garante a autenticidade.





Chave Simétrica está relacionada diretamente a uma senha única.

Chave Assimétrica está relacionada a duas chaves diferentes que são correspondentes – chave pública e chave privada. A chave pública, como o próprio no diz, qualquer pessoa possui acesso. A chave privada apenas o próprio dono tem acesso. Quando um arquivo é criptografado com a chave pública, apenas o proprietário da chave privada poderá ter acesso a informação.

Noções de vírus, worms e pragas virtuais

Uma ameaça acontece quando há uma ação sobre uma pessoa ou sobre um processo fazendo uso de uma fraqueza, causando um problema ou consequência.

A partir das ameaças podem surgir ataques. Um ataque pode ser decorrente da invasão de um sistema de segurança com intuito de tornar vulnerável os sistemas e serviços. Eles são divididos em ativo, passivo e destrutivo; o ativo modifica os dados, o passivo libera os dados e o destrutivo impede qualquer acesso aos dados. Os ataques podem ser realizados a partir da ação de um vírus ou do uso de técnicas específicas.

Malware

Malware é um termo abreviado para *malicious software* (software malicioso). Esse software é criado especificamente para obter acesso ou danificar um computador, sem o conhecimento do seu proprietário. Existem vários tipos de malware, incluindo spyware, keyloggers, vírus verdadeiros, worms ou qualquer outro tipo de código malicioso que se infiltra em um computador.

Normalmente um software é considerado malware com base na intenção de seu criador e não nas funcionalidades para as quais foi criado. Originalmente ele foi criado para experimentos e pegadinhas, mas acabou resultando em vandalismo e destruição dos computadores alvo. Atualmente, a maioria do malware é criada para a obtenção de lucros por meio de publicidade forçada (adware), roubo de informações confidenciais (spyware), propagação de spam ou pornografia infantil por e-mail (computadores zumbi) ou propagação de extorsões financeiras (ransomware).

Vírus

Um vírus de computador é um programa ou código malicioso criado para alterar a forma como um computador funciona. Ele atua se inserindo ou se anexando a um programa ou documento legítimo, que tenha suporte para macros, a fim de executar o seu código. Durante esse processo, um vírus pode potencialmente causar efeitos inesperados ou prejudiciais, como danificar o sistema, corrompendo ou destruindo os dados.



Para que o vírus contamine o computador, será necessário executar o programa infectado, o que por sua vez obriga o código do vírus a ser executado. Isso significa que um vírus pode permanecer inativo em seu computador, sem demonstrar nenhum sinal ou sintoma. Porém, quando o vírus contamina o computador, ele pode também contaminar outros computadores na mesma rede. Roubar senhas ou dados, registrar o uso do teclado, corromper arquivos, enviar spam aos seus contatos de e-mail e até mesmo controlar o seu computador são apenas algumas das ações irritantes e devastadoras que um vírus pode executar.

Os vírus podem se propagar através de anexos de e-mail ou mensagens de texto, downloads de arquivos da Internet e links para golpes em mídias sociais. Até mesmo os dispositivos móveis e smartphones podem ser infectados com vírus através do download de aplicativos duvidosos nesses dispositivos. Os vírus podem se esconder disfarçados como anexos de conteúdos compartilhados socialmente, como imagens humorísticas, cartões comemorativos ou arquivos de áudio e vídeo.

Existem muitos tipos de vírus e eles são classificados de acordo com a sua ação sobre o computador. Vamos entender como cada um deles funciona.

Spyware

De forma simples e direta, é um software de espionagem, isto é, sua função é coletar informações sobre uma ou mais atividades realizadas em um computador. Normalmente entra em seu computador sem o seu conhecimento ou permissão e é executado em segundo plano.

O spyware é conhecido por capturar e transmitir informações altamente pessoais como contas bancárias online e senhas, ou informações de cartão de crédito.

As formas como o spyware captura as informações subdivide sua classificação.

Registro de toques nas teclas

Chamados de “keyloggers”, esse tipo de spyware é usado para coletar senhas e rastrear comunicações em que o teclado é utilizado.

Acompanhamento das atividades

Alguns cookies de rastreamento podem, indiscutivelmente, ser considerados spyware, no sentido que eles acompanham seus movimentos online e relatam o que você visita aos publicitários, para que eles possam servir informações mais pertinentes a você.

Redução da velocidade do dispositivo

Frequentemente, o único sinal que denuncia que você está infectado com spyware será a maneira parasita com que ele rouba potência de processamento e largura de banda de Internet para comunicar o que foi roubado.

Cavalo de Tróia

O cavalo de Tróia é um malware disfarçado de software legítimo para obter acesso aos sistemas dos usuários. Uma vez ativados, os cavalos de Tróia permitem que os criminosos espionem, roubem dados confidenciais e



obtenham acesso ao sistema através de uma backdoor. Ele se confunde em algumas características com o spyware. Os principais tipos de cavalo de Tróia são:

Backdoor

Com um cavalo de Tróia backdoor, usuários maliciosos controlam remotamente o computador infectado. Os cavalos de Tróia backdoor costumam ser usados para reunir um conjunto de computadores e formar uma rede zumbi, que pode ser usada para fins criminosos.

Exploit

Exploits são programas que contêm dados ou códigos que tiram proveito de uma vulnerabilidade do software de um aplicativo executado no computador.

Rootkit

Os rootkits têm como objetivo ocultar certos objetos ou atividades no sistema. Geralmente, o principal objetivo é evitar a detecção de programas maliciosos para estender o período em que os programas são executados em um computador infectado.

Trojan-Banker

Programas Trojan-Banker são criados para roubar dados de contas de sistemas de bancos on-line, pagamentos eletrônicos e cartões de débito e crédito.

Spam

O spam é o equivalente eletrônico das correspondências indesejadas enviadas pelo correio e das ligações de telemarketing. Apesar de certos tipos de spam serem apenas publicidade indesejada, porém legítima, outros são muito piores. Eles podem incluir todo tipo de golpe, desde ofertas falsas até códigos maliciosos, criados para causar destruição na sua situação financeira ou em seu computador, pois podem ser usados para transmitir Cavalos de Tróia, vírus, worms, spywares e ataques de phishing direcionados. O spam representa aproximadamente 80% do volume de e-mails em todo o mundo.

Phishing

É basicamente um golpe on-line de falsificação. Os phishers enviam e-mails que tentam imitar mensagens de empresas financeiras legítimas ou de outras empresas e instituições que você talvez até utilize. O e-mail de phishing do spam solicitará que você acesse um site falso para reinserir o número do seu cartão de crédito ou verificar sua senha. A partir da inserção desses dados eles têm acesso a todas as informações necessárias para aplicar golpes.

Worm

Um worm é um software malicioso capaz de se autorreplicar em computadores ou por redes de computadores sem que você desconfie que sua máquina foi infectada. Como cada cópia subsequente do worm também consegue se autorreplicar, as infecções podem se disseminar muito rapidamente. Há diversos tipos de worms,



sendo que muitos deles podem causar altos níveis de destruição. Eles podem explorar erros de configuração da rede (por exemplo, copiar a si mesmos em um disco totalmente acessível) ou explorar brechas na segurança do sistema operacional e dos aplicativos. Muitos worms usam mais de um método para propagar cópias pelas redes.

Ransomware

O ransomware é um tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate (ransom) para restabelecer o acesso ao usuário. O pagamento do resgate geralmente é cobrado em bitcoins.

O ransomware pode se propagar de diversas formas, embora as mais comuns sejam: através de e-mails com o código malicioso em anexo ou que induzam o usuário a seguir um link; ou explorando vulnerabilidades em sistemas que não tenham recebido as devidas atualizações de segurança.

Botnet

Botnet é uma palavra formada pelos termos robot e network que indica um grupo de computadores conectados à Internet, cada um deles rodando um ou mais bots que se comunicam com outros dispositivos, a fim de executar determinada tarefa. O termo também pode ser aplicado a uma rede de agentes de software ou bots que executam tarefas de maneira autônoma e automática. Pode se referir, ainda, a uma rede de computadores que utilizam software de computação distribuída.

Entretanto a palavra botnet geralmente é associada ao uso de software malicioso, para realizar ataques distribuídos de negação de serviço (ataque DDoS), seja mediante o envio de spam, seja permitindo que o invasor acesse o dispositivo e sua conexão, a fim de furtrar dados. Esses ataques geralmente utilizam computadores infectados para atacar outros computadores sem que o usuário perceba essa ação.

Ferramentas para segurança

Existem várias formas para promover a proteção dos arquivos e o controle de segurança. Abaixo vamos listar algumas das mais cobradas em concursos.

Autenticação e Autorização

De acordo com o dicionário Aurélio, autenticação é o ato de autenticar, que significa “validar; reconhecer algo como verdadeiro; admitir a autenticidade, a veracidade de algo. Legitimar; reconhecer como verídico; validar de modo jurídico: o notório autenticou o documento”.

Para Huntington², o processo de autenticação é aquele capaz de determinar se alguém é quem está dizendo ser. Tal procedimento pode ser realizado a partir de uma senha, um token, cartão ID ou uma leitura biométrica e é realizado com base em uma medida de riscos onde sistemas aplicações e informações de alto risco exigem

² Huntington, Guy. The Business of Authentication. 27-Jun-2009. disponível em <<http://www.authenticationworld.com/>>.



diferentes formas de autenticação que confirmem de forma mais precisa a identidade digital do usuário enquanto aplicações de baixo risco onde a confirmação da identidade digital não é tão importante. Este conceito é normalmente referido como “autenticação forte”. O autor enumera diversos tipos de autenticação tal como PKI, biométrica, senha entre outras, mas nota-se que todas elas possuem similaridades que nos permite agrupá-las nos chamados fatores de autenticação.

Fatores e Métodos de Autenticação

Os fatores de autenticação, são de forma geral classificados em três categorias distintas: **O que você tem, o que você é e o que você sabe.**

“O que você sabe” – Autenticação baseada no conhecimento

Para se autenticar é necessário saber previamente alguma informação para ser validado, a senha é o melhor exemplo deste método. Você precisa informar ela corretamente, do contrário não será autenticado, e terá o acesso barrado.

A vantagem deste método é que ele já é amplamente difundido e simples de ser utilizado. Já o grande problema é que outra pessoa pode saber ou até mesmo descobrir a sua senha, ao realizar diversas tentativas.

“O que você tem” – Autenticação baseada na propriedade

Nesta categoria você só é autenticado se você possuir algum dispositivo. Um bom exemplo deste tipo é o token, o dispositivo gera uma nova senha a cada período de tempo, desta maneira, é preciso ter o token para se autenticar. Caso outra pessoa observe a senha enquanto você digita a senha para entrar no site bancário, em questão de minutos esta senha será trocada, e a senha observada não servirá mais.

Esta categoria já se mostra mais segura que a anterior, pois é necessário ter a posse do cartão ou do token, e caso outra pessoa consiga estes dispositivos o proprietário notaria a falta, o usuário pode solicitar um novo cartão ou token.

Mas, mesmo esta categoria apresenta alguns riscos, no caso do cartão de senhas, os criminosos criam páginas falsas de bancos que pedem todas as senhas do cartão da vítima. No caso dos tokens, existe a possibilidade da empresa que cria os tokens ter suas chaves roubadas, e com isto permite que os criminosos se passem pela vítima.

“O que você é” – Autenticação baseada na característica

Nesta categoria a autenticação é mais rigorosa, apenas a princípio apenas a própria pessoa pode ser autenticada, isto porque é utilizado a biometria, um bom exemplo deste tipo é a leitura da impressão digital.

Há também outros tipos de biometria não tão populares, como escaneamento de veias, identificação da íris, reconhecimento da voz, e outros.

Note que os métodos de autenticação que utilizam a biometria são mais seguros que os demais, mas mesmo assim não garante 100% de segurança, como já foi noticiado que pessoas utilizavam um molde de silicone da digital de outra pessoa para passar pelo leitor de impressão digital.



Autorizar

É o mecanismo responsável por garantir que apenas usuários autorizados consumam os recursos protegidos de um sistema computacional. Os recursos incluem arquivos, programas de computador, dispositivos de hardware e funcionalidades disponibilizadas por aplicações instaladas em um sistema.

Prevenção Contra Riscos e Códigos Maliciosos

Antivírus

Com a finalidade de garantir um nível de segurança, é necessário instalar um programa de antivírus. Os antivírus e anti-malwares são programas desenvolvidos para prevenir, detectar e eliminar vírus de computador e outros tipos de softwares nocivos ao sistema operacional. Ele funciona identificando, bloqueando e alertando ao usuário sobre a ação de um vírus em e-mails e outros arquivos. Caso algum seja encontrado, o antivírus coloca em quarentena (isola) o vírus ou o exclui completamente, antes que ele danifique o computador e os arquivos.

A principal diferença entre antivírus pago e antivírus gratuito é que as versões pagas oferecem proteções extras, que em sua grande maioria não disponíveis nas versões grátis.

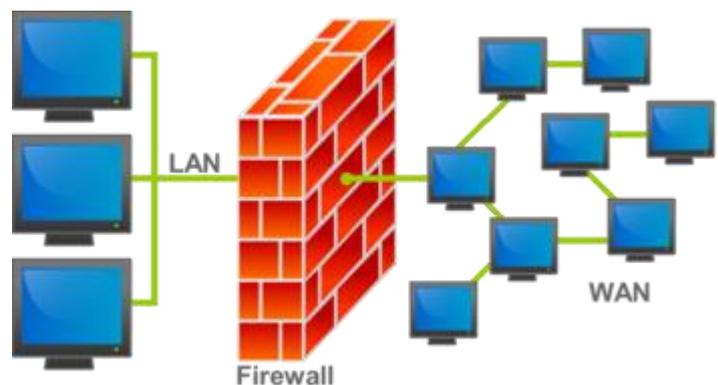
Como exemplos de antivírus gratuitos mais conhecidos temos: AVG, Avast, Avira e Microsoft Security Essential.

Como exemplos de antivírus pagos temos: Kaspersky, BitDefender, McAfee e Norton.

Firewall

Um firewall é um dispositivo de segurança da rede que monitora o tráfego de rede. Traduzindo de forma literal ele é uma “parede de fogo” que de acordo com regras pré-definidas decide permitir ou bloquear tráfegos específicos. Ele pode ser tanto um software quanto um hardware, onde a combinação de ambos é chamada tecnicamente de “appliance”.

Sua complexidade depende do tamanho da rede, da política de segurança, da quantidade de regras que controlam o fluxo de entrada e saída de informações e do grau de segurança desejado. A partir das regras, o firewall pode ajudar a impedir o acesso de hackers e softwares mal-intencionados aos computadores conectados na rede.



Na sua forma mais simples de implementação, o firewall funciona como um filtro de pacotes (stateless) que pode ser configurado tanto para a rede interna, quanto para a rede externa (Internet). A outra forma de configuração é a de estado de sessão (statefull), onde o firewall analisa os pacotes e guarda o estado de cada conexão de maneira que seja possível para identificar e fazer uma previsão das respostas legítimas, de forma a impedir o tráfego de pacotes ilegítimos.



Normalmente o firewall é implementado em dispositivos que fazem a separação das redes interna e externa, tornando-se assim um roteador.

Noções de Criptografia

De acordo com o CERT.br/NIC.br³, “a criptografia, considerada como a ciência e a arte de escrever mensagens em forma cifrada ou em código, é um dos principais mecanismos de segurança que você pode usar para se proteger dos riscos associados ao uso da Internet”.

A criptografia abrange desde a elaboração até a implementação de sistemas de computação relacionado a diversos elementos da segurança.

Ela diz respeito a conceitos e técnicas usadas para codificar uma informação, de tal forma que apenas seu real destinatário e o emissor da mensagem possam acessá-la, com o objetivo de evitar que terceiros capturem e interpretem a mensagem.



Entre os principais objetivos do uso da criptografia temos:

- proteger os dados sigilosos armazenados em seu computador, como o seu arquivo de senhas e a sua declaração de Imposto de Renda;
- criar uma área (partição) específica no seu computador, na qual todas as informações que forem lá gravadas serão automaticamente criptografadas;
- proteger seus backups contra acesso indevido, principalmente aqueles enviados para áreas de armazenamento externo de mídias;
- proteger as comunicações realizadas pela Internet, como os e-mails enviados/recebidos e as transações bancárias e comerciais realizadas.

História

³ <https://cartilha.cert.br/criptografia/>



A criptografia tem uma história longa e complexa. Seu primeiro uso conhecido foi encontrado em hieróglifos irregulares esculpidos em monumentos do Antigo Império do Egito (a cerca de 4500 anos). Porém foi na Segunda Guerra Mundial que a criptografia se tornou famosa e teve papel decisivo.

Os alemães e seus aliados, que formavam o grupo chamado Eixo, utilizavam máquinas eletromecânicas de criptografia com rotores (Enigma) em praticamente todas as suas comunicações, tornando impossível a decodificação das mensagens. Dessa forma, os Aliados (EUA, União Soviética, Reino Unido e França) precisaram buscar ajuda de criptógrafos e matemáticos que descobriram que existia uma quase indetectável falha no código, que consistia no fato de que uma letra nunca era criptografada de forma que fosse representada como ela mesma depois de ser codificada.

A partir dessa descoberta, a equipe comandada por Alan Turing desenvolveu uma máquina (*Bombe*) capaz de decifrar as mensagens alemãs e conseguiu descobrir como o código funcionava.

Toda a história a respeito da criptografia na Segunda Grande Guerra é contada no filme O Jogo da Imitação, que eu indico para você assistir.

Tipos de Criptografia

Existem diversas técnicas de criptografia, entretanto as mais conhecidas envolvem o conceito das chaves criptográficas, que são um conjunto de bits, baseados em um algoritmo capaz de interpretar a informação, ou seja, capaz de codificar e decodificar. Se a chave do receptor não for compatível com a do emissor, a informação então não será extraída.



Antes de continuarmos, é importante que você se acostume com alguns termos que são comuns em criptografia e podem estar presentes na sua prova de concurso.

Termo	Significado
Texto claro	Informação legível (original) que será protegida, ou seja, que será codificada
Texto codificado (cifrado)	Texto ilegível, gerado pela codificação de um texto claro
Codificar (cifrar)	Ato de transformar um texto claro em um texto codificado
Decodificar (decifrar)	Ato de transformar um texto codificado em um texto claro
Método criptográfico	Conjunto de programas responsável por codificar e decodificar informações
Chave	Similar a uma senha, é utilizada como elemento secreto pelos métodos criptográficos. Seu tamanho é geralmente medido em quantidade de bits
Canal de comunicação	Meio utilizado para a troca de informações



Remetente	Pessoa ou serviço que envia a informação
Destinatário	Pessoa ou serviço que recebe a informação

De acordo com o tipo de chave usada, os métodos de criptografia podem ser divididos em duas categorias: criptografia de chave simétrica e criptografia de chaves assimétricas.

Criptografia de chave simétrica (secreta ou única)

Esse método utiliza a mesma chave tanto para codificar como para decodificar as informações. É muito empregado para **garantir a confidencialidade dos dados**, onde uma mesma pessoa codificada e decodificada a informação e por isso não há necessidade de compartilhamento da chave. Entretanto, quando estas operações envolvem pessoas ou equipamentos diferentes, é necessário que a chave secreta seja previamente combinada por meio de um canal de comunicação seguro, para não comprometer sua confidencialidade. Como exemplo desse método temos os algoritmos: AES, Blowfish, RC4, 3DES e IDEA.

Criptografia de chave assimétrica (pública)

Utiliza duas chaves distintas: uma pública, que pode ser livremente divulgada, e uma privada, que deve ser mantida em segredo por seu dono. Quando uma informação é codificada com uma das chaves, somente a outra chave do par pode decodificá-la. Qual chave usar para codificar depende da proteção que se deseja, se **confidencialidade ou autenticação**, integridade e não-repúdio. A chave privada pode ser armazenada de diferentes maneiras, como um arquivo no computador, um *smartcard* ou um *token*. Como exemplo desse método temos os algoritmos: RSA, DSA, ECC e Diffie-Hellman.

Principais Algoritmos de Criptografia

- **DES (Data Encryption Standard)**: essa chave consiste nominalmente em 64 bits, porém utiliza apenas 56 bits, que corresponde à aproximadamente 72 quatrilhões de combinações, que apesar de ser um número absurdamente alto, em 1999, foi quebrado através do método de “tentativa e erro”, em um desafio na Internet. Ainda assim, foi aprovado pelo governo dos EUA como algoritmo padrão em 1976 e utilizado a partir de 1977 até 2002, tendo passado nesse período por 3 revisões que resultaram no último prescrito “Triplo DES” ou 3DES.
- **AES (Advanced Encryption Standard)**: criado a partir de um concurso do governo americano para definir um novo algoritmo padrão de chave simétrica, hoje em dia é um dos melhores e mais populares algoritmos de criptografia. O AES tem um tamanho de bloco fixo em 128 bits, mas diferentes comprimentos de chave: 128, 192 e 256 bits.
- **IDEA (International Data Encryption Algorithm)**: é um algoritmo de cifra de bloco que faz uso de chaves de 128 bits e que tem uma estrutura semelhante ao DES.
- **RSA (Rivest, Shamir and Adleman)**: É um dos algoritmos de chave assimétrica mais utilizados, onde dois números primos (aqueles números que só podem ser divididos por 1 e por eles mesmos) são multiplicados para a obtenção de um terceiro valor. A chave privada do RSA são os números que são multiplicados e a chave pública é o valor que será obtido. Para descobrir os dois primeiros números a partir do terceiro, é preciso fazer fatoração. Dessa forma, se forem utilizados números grandes, será praticamente impossível descobrir o código.



Assinatura Digital

A assinatura digital é um método que permite comprovar a autenticidade e a integridade de uma informação, ou seja, que ela foi realmente gerada por quem diz ter feito e que ela não foi alterada. Podemos comparar a assinatura digital a assinatura física com firma reconhecida em cartório, pois possui validade jurídica inquestionável e equivale a uma assinatura de próprio punho.

A validade e admissibilidade legal da assinatura digital são garantidas pelo artigo 10 da MP nº 2.200-2/2001⁴, que instituiu a Infraestrutura de Chaves Públicas Brasileiras - ICP-Brasil, conferindo presunção de veracidade jurídica em relação aos signatários nas declarações constantes dos documentos em forma eletrônica.

A assinatura digital se baseia no fato de que apenas o dono conhece a chave privada e que, se ela foi usada para codificar uma informação, então apenas seu dono poderia ter feito isto. A verificação da assinatura é feita com o uso da chave pública, pois se o texto foi codificado com a chave privada, somente a chave pública correspondente pode decodificá-lo.

Ela utiliza uma ID digital baseada em certificado e emitida por uma autoridade de certificação (CA) ou um provedor de serviços confiável (TSP) credenciado. Desse modo, quando você assina um documento digitalmente, sua identidade é associada exclusivamente a você, a assinatura é vinculada ao documento com criptografia, e tudo pode ser confirmado por meio de uma tecnologia subjacente conhecida como infraestrutura de chave pública (PKI).

Para contornar a baixa eficiência característica da criptografia de chaves assimétricas, a codificação é feita sobre o hash e não sobre o conteúdo em si, pois é mais rápido codificar o hash (que possui tamanho fixo e reduzido) do que a informação toda.

Após gerar o hash, ele deve ser criptografado através de um sistema de chave pública, para garantir a autenticação e a irretratibilidade. O autor da mensagem deve usar sua chave privada para assinar a mensagem e armazenar o hash criptografado junto à mensagem original.



Hash é uma função de resumo, um método criptográfico que, quando aplicado sobre uma informação, independentemente do tamanho que ela tenha, gera um resultado único e de tamanho fixo.

Para verificar a integridade de um arquivo, por exemplo, você pode calcular o hash dele e, quando julgar necessário, gerar novamente este valor. Se os dois hashes forem iguais então você pode concluir

⁴ http://www.receita.fazenda.gov.br/Acsrf/MP_ICP_22002.pdf



que o arquivo não foi alterado. Caso contrário, este pode ser um forte indício de que o arquivo esteja corrompido ou que foi modificado. Exemplos de métodos de hash são: SHA-1, SHA-256 e MD5.



O termo "**assinatura eletrônica**" tem um significado diferente: refere-se a qualquer mecanismo, não necessariamente criptográfico, para identificar o remetente de uma mensagem eletrônica.

Basicamente, toda assinatura digital é eletrônica, mas nem toda assinatura eletrônica é digital. Seja com a digitação de um código de segurança para confirmar uma transferência bancária ou por meio de certificado digital para efetuar operações no site da Receita Federal, a validação eletrônica assegura mais proteção às operações, velocidade no fechamento de negócios, praticidade e economia de custos — com papéis, toners e demais materiais de escritório.

As assinaturas eletrônicas podem ser aplicadas nos mais diversos tipos de documento. Por também possuírem valor jurídico, podem ser utilizadas no fechamento de contratos de aluguel, seguros, planos de saúde, formulários de RH, contratos de compra e venda com fornecedores, assinatura de serviços, operações bancárias, notificações jurídicas, contratação de planos de saúde, além de inúmeras outras possibilidades.

Certificação Digital

Segundo o SERPRO⁵, certificado digital é o documento eletrônico que possibilita a troca segura de informações entre duas partes, com a garantia da identidade do emissor, da integridade da mensagem e, opcionalmente, de sua confidencialidade.

Na prática, o certificado digital funciona como uma identidade virtual que permite a identificação segura e inequívoca do autor de uma mensagem ou transação feita em meios eletrônicos. Esse documento eletrônico é gerado e assinado por uma Autoridade Certificadora (AC) que, seguindo regras estabelecidas pelo Comitê Gestor da ICP-Brasil, associa uma entidade (pessoa, processo, servidor) a um par de chaves criptográficas. Os

⁵ Serviço Federal de Processamento de Dados, é a maior empresa pública de prestação de serviços em tecnologia da informação do Brasil. Foi criado pela Lei nº 4.516, para modernizar e dar agilidade a setores estratégicos da administração pública. É uma empresa vinculada ao Ministério da Fazenda e cresceu desenvolvendo programas e serviços que permitiram maior controle e transparência sobre a receita e os gastos públicos. Consolidou-se aprimorando tecnologias adotadas por diversos órgãos públicos federais, estaduais e municipais, e incorporadas à vida do cidadão brasileiro.



certificados contêm os dados de seu titular conforme detalhado na Política de Segurança de cada Autoridade Certificadora.



ICP-Brasil

A Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil é uma cadeia hierárquica de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão.

Diante disso, precisamos entender a diferença entre assinatura digital e certificado digital. A assinatura digital é uma tecnologia que utiliza a criptografia e vincula um certificado digital ao documento eletrônico que está sendo assinado. Assim dá garantias de integridade e autenticidade do documento. Logo, a questão não está na diferença entre uma e outra, mas sim no tipo de certificado digital que cada assinatura vincula. O certificado digital é uma chave, um arquivo eletrônico que contém variadas informações de identificação de uma pessoa/empresa (chave pública do titular, nome, e-mail, validade do certificado, número de série e outros).

De forma geral, os dados básicos que compõem um certificado digital são:

- versão e número de série do certificado;
- dados que identificam a AC que emitiu o certificado;
- dados que identificam o dono do certificado (para quem ele foi emitido);
- chave pública do dono do certificado;
- validade do certificado (quando foi emitido e até quando é válido);
- assinatura digital da AC emissora e dados para verificação da assinatura.

Uso do Certificado Digital

Assinatura de documentos e contratos digitais: os documentos assinados digitalmente com certificado digital ICP-Brasil têm a mesma validade que os documentos assinados em papel. Além de proporcionar economia de insumos, já que não há necessidade de realizar impressões, os documentos assinados digitalmente agilizam processos, pois podem ser enviados por email e assinados de qualquer lugar facilmente;

Autenticação em sistemas: existem vários sistemas com informações confidenciais, especialmente de governo, que só podem ser acessados presencialmente, através da confirmação de identidade. Como o certificado digital garante autenticidade, ele proporciona o acesso à esses sistemas e informações através da internet, não havendo necessidade de comparecimento presencial;

Atualização de informações em sistemas: Além de garantir acesso seguro à sistemas, o certificado também permite a alteração rápida de informações, evitando longos processos burocráticos;



Categorias profissionais: diversas categorias profissionais (médicos, advogados, contadores, militares, entre outros) já utilizam o certificado digital em suas rotinas. Com o certificado, as classes profissionais têm a possibilidade de trabalhar com sistemas virtuais unificados e seguros, proporcionando integração e desburocratização de processos relativos ao setor.

Hierarquia e Emissão do Certificado Digital

De acordo com o Instituto Nacional de Tecnologia da Informação, o ICP-Brasil possui 6 entes, dos quais destacamos 3:

AC - Raiz

A Autoridade Certificadora Raiz da ICP-Brasil – AC-Raiz é a primeira autoridade da cadeia de certificação. Executa as Políticas de Certificados e as normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil. Portanto, compete à AC-Raiz emitir, expedir, distribuir, revogar e gerenciar os certificados das autoridades certificadoras de nível imediatamente subsequente ao seu.

A AC-Raiz também está encarregada de emitir a Lista de Certificados Revogados – LCR e de fiscalizar e auditar as Autoridades Certificadoras – ACs, Autoridades de Registro – ARs e demais prestadores de serviço habilitados na ICP-Brasil. Além disso, verifica se as ACs estão atuando em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor da ICP-Brasil.

AC - Autoridade Certificadora

Uma Autoridade Certificadora – AC é uma entidade, pública ou privada, subordinada à hierarquia da ICP-Brasil, responsável por emitir, distribuir, renovar, revogar e gerenciar certificados digitais. Tem a responsabilidade de verificar se o titular do certificado possui a chave privada que corresponde à chave pública que faz parte do certificado. Cria e assina digitalmente o certificado do assinante, onde o certificado emitido pela AC representa a declaração da identidade do titular, que possui um par único de chaves (pública/privada).

Cabe também à AC emitir Listas de Certificados Revogados – LCR e manter registros de suas operações sempre obedecendo às práticas definidas na Declaração de Práticas de Certificação – DPC. Além de estabelecer e fazer cumprir, pelas Autoridades de Registro – ARs a ela vinculadas, as políticas de segurança necessárias para garantir a autenticidade da identificação realizada.

AR - Autoridade de Registro

Uma Autoridade de Registro – AR é responsável pela interface entre o usuário e a Autoridade Certificadora – AC. Vinculada a uma AC, tem por objetivo o recebimento, a validação, o encaminhamento de solicitações de emissão ou revogação de certificados digitais e identificação, de forma presencial, de seus solicitantes. É responsabilidade da AR manter registros de suas operações. Pode estar fisicamente localizada em uma AC ou ser uma entidade de registro remota.



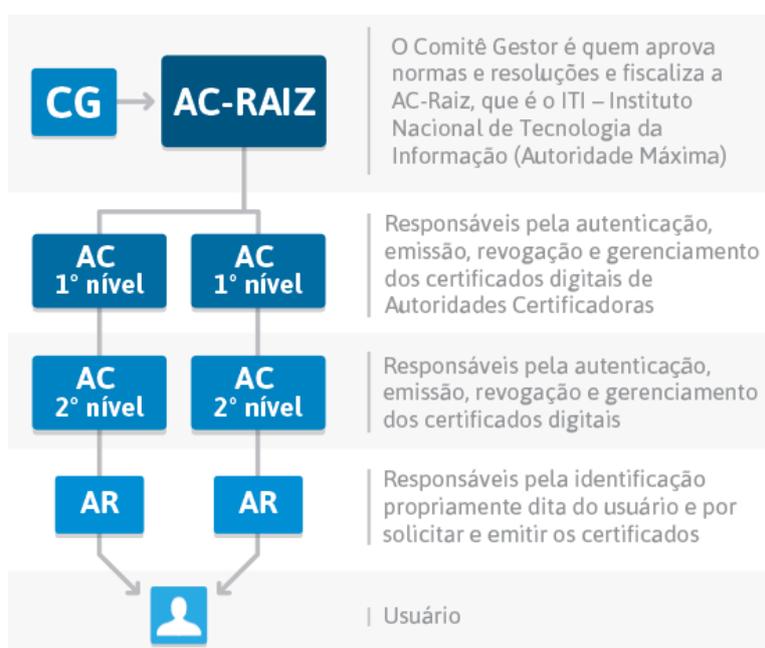


CURIOSIDADE

Mas quem emite o certificado para uma Autoridade Certificadora?

O certificado digital de uma AC é emitido, geralmente, por outra AC, estabelecendo uma hierarquia conhecida como "cadeia de certificados" ou "caminho de certificação". A AC raiz, primeira autoridade da cadeia, é a âncora de confiança para toda a hierarquia e, por não existir outra AC acima dela, possui um certificado auto assinado (mais detalhes a seguir). Os certificados das ACs raízes publicamente reconhecidas já vêm inclusos, por padrão, em grande parte dos sistemas operacionais e navegadores e são atualizados juntamente com os próprios sistemas. Alguns exemplos de atualizações realizadas na base de certificados dos navegadores são: inclusão de novas ACs, renovação de certificados vencidos e exclusão de ACs não mais confiáveis.

Abaixo temos uma imagem de como funciona esse processo no Brasil.



Neste [link](#) você encontra a lista e a estrutura hierárquica de todas as Autoridades Certificadoras – ACs de 1º e 2º nível e Autoridades de Registro – ARs da ICP-Brasil.

Categorias e Tipos de Certificado Digital

Existem vários modelos e tipos de certificado digital, sendo que cada um deles se aplica em um caso específico, sendo 8 relacionados com Assinatura Digital (A1,A2,A3,A4,T3,T4,A CF-e-SAT e OM-BR) e 4 com sigilo (S1/S2/S3 e S4).

Categoria A (certificado de assinatura digital)



Esse é o tipo mais utilizado de certificado digital e pode ser aplicado para conferir autenticidade a qualquer tipo de documento e arquivo virtual. Seu principal objetivo é identificar o assinante, confirmar a integridade do documento e atestar a autenticidade da operação realizada. Ou seja, tudo o que for feito por meio do Certificado tem validade jurídica, similar a sua assinatura de próprio punho, só que do mundo virtual.

Categoria S (certificado de sigilo/confidencialidade)

O certificado tipo S é um modelo que busca trazer sigilo para uma determinada transação, já que, por meio de sua utilização, é possível criptografar os dados de um documento, que, a partir desse momento, só poderá ser acessado por meio de um certificado autorizado, evitando, assim, o vazamento de informações.

Ou seja, ao utilizar o tipo S, o conteúdo do documento assinado se torna inacessível para pessoas que não tenham autorização e, com isso, é muito mais seguro transmitir informações sigilosas pela rede. Empresas que precisam trocar informações de cunho sigiloso constantemente podem se valer dessa proteção.

Categoria T (certificado de tempo)

O certificado digital tipo T é mais conhecido como carimbo de tempo, uma vez que seu objetivo é atestar quando um documento digital foi emitido, tornando evidente a data e a hora que determinada informação digital passou a existir.

Como esses dados poderiam ser facilmente adulterados para beneficiar uma das partes, em uma ação judicial, por exemplo, o tipo T utiliza uma terceira parte certificadora para atestar o exato instante em que o documento foi emitido, evitando fraudes. Pode ser utilizado em conjunto com os demais certificados para garantir ainda mais segurança às transações.

Categoria A CF-e-SAT

Só podem ser emitidos para equipamentos integrantes do Sistema de Autenticação e Transmissão do Cupom Fiscal Eletrônico – SAT-CF-e, seguindo a regulamentação do CONFAZ.

Categoria OM-BR – Certificados do tipo Objeto Metrológico

Certificados do tipo Objeto Metrológico – OM-BR só podem ser emitidos para equipamentos metrológicos regulados pelo Inmetro.

No Brasil, os dois tipos mais comuns, de certificado digital são: A1 e A3.

Certificado A1

O Certificado A1 é gerado em software, ou seja, não precisa de nenhum leitor, pois fica instalado diretamente no computador. As extensões desse tipo de arquivo costumam ser .P12 ou .PFX. A vantagem do A1 é que ele pode ser instalado simultaneamente em diversos computadores. Geralmente tem o custo menor que um A3, porém tem prazo de validade de 1 ano.



Certificado A3

O Certificado A3 é baseado em hardware, seja em Token (USB) ou cartão com leitor específico em conformidade com a legislação da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). Entre suas vantagens podemos considerar a validade, que dependendo do tipo de mídia, pode ter duração de três a cinco anos. A desvantagem deste tipo de certificado é que ele só pode ser utilizado em um computador e um programa por vez, diminuindo sua versatilidade. Além de exigir a digitação do PIN (senha) toda vez que for necessário verificar sua identidade.

Auditoria, Vulnerabilidade e Conformidade

Existem algumas definições que permeiam o conceito de auditoria. Entretanto, vamos nos basear na NBR ISO 19011⁶ que define auditoria como um processo sistemático, documentado e independente para obter evidências de auditoria e avaliá-las objetivamente de modo a determinar a extensão na qual os critérios de auditoria são atendidos.

As evidências de auditoria: são registros, apresentação de fatos ou outras informações, pertinentes aos critérios de auditoria. A auditoria pode ser quantitativa ou qualitativa. Já os critérios de auditoria: consistem em um conjunto de políticas, procedimentos ou requisitos. Os critérios de auditoria são usados como uma referência contra a qual a evidência da auditoria é comparada.

A NBR ISO 19011 apresenta alguns princípios, relacionados aos auditores, possibilitando que sejam fornecidas conclusões de auditoria relevantes e suficientes e permitindo que auditores trabalhem de forma independente e cheguem a conclusões semelhantes em situações semelhantes.

Conduta ética: consiste na alma do profissional, confiança, integridade, confidencialidade e discrição. A ética consiste em uma característica inerente às ações do ser humano, tornando-se um componente fundamental à sociedade.

Obrigaç o: existe a obrigaç o de reportar com veracidade e exatid o todas as informaç es pertinentes   auditoria, relacionadas com as constataç es e as conclus es da auditoria e seus respectivos relat rios.

Consci ncia profissional: os auditores devem ter a preocupaç o de realizar as tarefas da forma mais profissional, de acordo com a import ncia e a confianç a depositada em uma auditoria.

Independ ncia:   a base para a imparcialidade e objetividade das conclus es de uma auditoria, porque os auditores s o independentes em relaç o ao que ser  auditado, assim como n o se ligam aos interesses e  s tend ncias apresentadas.

Evid ncia: a evid ncia de auditoria pode ser verificada, pois ela   realizada com base em amostras de informaç es que se encontram dispon veis.

⁶ NBR ISO 19011. Diretrizes para auditorias de sistema de gest o da qualidade, NBR. 2002.



Tipos de Auditoria

Os autores Neto e Solonca (2007)⁷ apresentam um quadro com os tipos de auditoria, separando-os em 3 classes abrangentes: forma de abordagem; órgão fiscalizador e área envolvida.

QUANTO A FORMA DE ABORDAGEM

Auditoria Horizontal – Auditoria com tema específico, realizada em várias entidades ou serviços, paralelamente.

Auditoria Orientada – Foca em uma atividade específica qualquer ou atividades com fortes indícios de fraudes ou erros.

QUANTO AO ÓRGÃO FISCALIZADOR:

Auditoria Interna – Auditoria realizada por um departamento interno, responsável pela verificação e avaliação dos sistemas e procedimentos internos de uma entidade. Um de seus objetivos é reduzir a probabilidade de fraudes, erros, práticas ineficientes ou ineficazes. Esse serviço deve ser independente e prestar contas diretamente à classe executiva da corporação.

Auditoria Externa – Auditoria realizada por uma empresa externa e independente da entidade que está sendo fiscalizada, com o objetivo de emitir um parecer sobre a gestão de recursos da entidade, sua situação financeira, a legalidade e regularidade de suas operações.

Auditoria Articulada – Trabalho conjunto de auditorias internas e externas, devido à superposição de responsabilidades dos órgãos fiscalizadores, caracterizado pelo uso comum de recursos e comunicação recíproca dos resultados.

QUANTO A ÁREA ENVOLVIDA:

Auditoria de programas de governo – Acompanhamento, exame e avaliação da execução de programas e projetos governamentais. Auditoria do planejamento estratégico – verifica se os principais objetivos da entidade são atingidos e se as políticas e estratégias são respeitadas.

Auditoria Administrativa – Engloba o plano da organização, seus procedimentos, diretrizes e documentos de suporte à tomada de decisão.

Auditoria Contábil – É relativa à fidedignidade das contas da instituição. Essa auditoria, conseqüentemente, tem como finalidade fornecer alguma garantia de que as operações e o acesso aos ativos se efetuam de acordo com as devidas autorizações.

⁷ NETO, Abílio Bueno; SOLONCA, Davi. Auditoria de sistemas informatizados. Palhoça: UnisulVirtual, 2007.



Auditoria Financeira – Conhecida também como auditoria das contas. Consiste na análise das contas, da situação financeira, da legalidade e regularidade das operações e aspectos contábeis, financeiros, orçamentários e patrimoniais, verificando se todas as operações foram corretamente autorizadas, liquidadas, ordenadas, pagas e registradas. Auditoria de legalidade – conhecida como auditoria de conformidade. Consiste na análise da legalidade e regularidade das atividades, funções, operações ou gestão de recursos, verificando se estão em conformidade com a legislação em vigor.

Auditoria Operacional – Incide em todos os níveis de gestão, nas fases de programação, execução e supervisão, sob a ótica da economia, eficiência e eficácia. Analisa também a execução das decisões tomadas e aprecia até que ponto os resultados pretendidos foram atingidos.

Auditoria da Tecnologia da Informação – Tipo de auditoria essencialmente operacional, por meio da qual os auditores analisam os sistemas de informática, o ambiente computacional, a segurança de informações e o controle interno da entidade fiscalizada, identificando seus pontos fortes e deficiências.

Termos Utilizados em Auditoria

Vamos nos basear nos termos apresentados por DIAS (2000)⁸ no livro Segurança e auditoria da tecnologia da informação.

- Campo: está relacionado ao objeto a ser fiscalizado, período e tipo da auditoria.
- Âmbito: define o grau de alcance e a profundidade dos trabalhos.
- Área de verificação: dá limites aos temas da auditoria, em função da organização a ser fiscalizada e do tipo da auditoria.
- Controle: é a fiscalização exercida sobre as atividades das pessoas, departamentos, produtos, e outros, de forma que as atividades executadas ou produtos estejam dentro das normas preestabelecidas.

Três tipos de controle são exercidos:

Preventivo – previne erros e invasões. (Exemplo: identificação e autenticação de usuários do sistema a partir da utilização de senhas);

Detector – detecta erros, tentativas de invasões, etc. (arquivos logs, realização de controle de acesso de usuários);

Corretivo – reduz o impacto causado por falhas ou erros, fazendo a correção necessária (política de segurança, plano de contingência).

- Objetivos de controle: são as finalidades de controle a serem atingidas, ou aspectos negativos a serem evitados em cada transação, atividade ou função fiscalizada.
- Procedimentos de auditoria: é o conjunto de verificações e investigações que permitem obter e analisar as informações necessárias ao parecer do auditor.
- Achados de auditoria: são fatos a serem considerados como importantes para o auditor.
- Papéis de trabalho: são registros que evidenciam atos e fatos observados pelo auditor.

⁸ DIAS, Cláudia. Segurança e auditoria da tecnologia da informação. Rio de Janeiro: Excel Books, 2000.



- Recomendações de auditoria: realizadas na fase de relatório, são as medidas corretivas que podem ou devem ser executadas para corrigir as falhas detectadas.

APOSTA ESTRATÉGICA

A ideia desta seção é apresentar os pontos do conteúdo que mais possuem chances de serem cobrados em prova, considerando o histórico de questões da banca em provas de nível semelhante à nossa, bem como as inovações no conteúdo, na legislação e nos entendimentos doutrinários e jurisprudenciais⁹.



Um vírus de computador é um programa ou código malicioso criado para alterar a forma como um computador funciona. Ele atua se inserindo ou se anexando a um programa ou documento legítimo, que tenha suporte para macros, a fim de executar o seu código. Durante esse processo, um vírus pode potencialmente causar efeitos inesperados ou prejudiciais, como danificar o sistema, corrompendo ou destruindo os dados.

Para que o vírus contamine o computador, será necessário executar o programa infectado, o que por sua vez obriga o código do vírus a ser executado. Isso significa que um vírus pode permanecer inativo em seu computador, sem demonstrar nenhum sinal ou sintoma. Porém, quando o vírus contamina o computador, ele pode também contaminar outros computadores na mesma rede. Roubar senhas ou dados, registrar o uso do teclado, corromper arquivos, enviar spam aos seus contatos de e-mail e até mesmo controlar o seu computador são apenas algumas das ações irritantes e devastadoras que um vírus pode executar.

Os vírus podem se propagar através de anexos de e-mail ou mensagens de texto, downloads de arquivos da Internet e links para golpes em mídias sociais. Até mesmo os dispositivos móveis e smartphones podem ser infectados com vírus através do download de aplicativos duvidosos nesses dispositivos. Os vírus podem se esconder disfarçados como anexos de conteúdos compartilhados socialmente, como imagens humorísticas, cartões comemorativos ou arquivos de áudio e vídeo.

Fatores e Métodos de Autenticação

Os fatores de autenticação, são de forma geral classificados em três categorias distintas: O que você tem, o que você é e o que você sabe.

⁹ Vale deixar claro que nem sempre será possível realizar uma aposta estratégica para um determinado assunto, considerando que às vezes não é viável identificar os pontos mais prováveis de serem cobrados a partir de critérios objetivos ou minimamente razoáveis.



“O que você sabe” – Autenticação baseada no conhecimento

Para se autenticar é necessário saber previamente alguma informação para ser validado, a senha é o melhor exemplo deste método. Você precisa informar ela corretamente, do contrário não será autenticado, e terá o acesso barrado.

A vantagem deste método é que ele já é amplamente difundido e simples de ser utilizado. Já o grande problema é que outra pessoa pode saber ou até mesmo descobrir a sua senha, ao realizar diversas tentativas.

“O que você tem” – Autenticação baseada na propriedade

Nesta categoria você só é autenticado se você possuir algum dispositivo. Um bom exemplo deste tipo é o token, o dispositivo gera uma nova senha a cada período de tempo, desta maneira, é preciso ter o token para se autenticar. Caso outra pessoa observe a senha enquanto você digita a senha para entrar no site bancário, em questão de minutos esta senha será trocada, e a senha observada não servirá mais.

Esta categoria já se mostra mais segura que a anterior, pois é necessário ter a posse do cartão ou do token, e caso outra pessoa consiga estes dispositivos o proprietário notaria a falta, o usuário pode solicitar um novo cartão ou token.

Mas, mesmo esta categoria apresenta alguns riscos, no caso do cartão de senhas, os criminosos criam páginas falsas de bancos que pedem todas as senhas do cartão da vítima. No caso dos tokens, existe a possibilidade da empresa que cria os tokens ter suas chaves roubadas, e com isto permite que os criminosos se passem pela vítima.

“O que você é” – Autenticação baseada na característica

Nesta categoria a autenticação é mais rigorosa, apenas a princípio apenas a própria pessoa pode ser autenticada, isto porque é utilizado a biometria, um bom exemplo deste tipo é a leitura da impressão digital.

Há também outros tipos de biometria não tão populares, como escaneamento de veias, identificação da íris, reconhecimento da voz, e outros.

Note que os métodos de autenticação que utilizam a biometria são mais seguros que os demais, mas mesmo assim não garante 100% de segurança, como já foi noticiado que pessoas utilizavam um molde de silicone da digital de outra pessoa para passar pelo leitor de impressão digital.

De acordo com o tipo de chave usada, os métodos de criptografia podem ser divididos em duas categorias: criptografia de chave simétrica e criptografia de chaves assimétricas.

Criptografia de chave simétrica (secreta ou única)

Esse método utiliza a mesma chave tanto para codificar como para decodificar as informações. É muito empregado para **garantir a confidencialidade dos dados**, onde uma mesma pessoa codificada e decodificada a informação e por isso não há necessidade de compartilhamento da chave. Entretanto, quando estas operações envolvem pessoas ou equipamentos diferentes, é necessário que a chave secreta seja previamente combinada por meio de um canal de comunicação seguro, para não comprometer sua confidencialidade. Como exemplo desse método temos os algoritmos: AES, Blowfish, RC4, 3DES e IDEA.



Criptografia de chave assimétrica (pública)

Utiliza duas chaves distintas: uma pública, que pode ser livremente divulgada, e uma privada, que deve ser mantida em segredo por seu dono. Quando uma informação é codificada com uma das chaves, somente a outra chave do par pode decodificá-la. Qual chave usar para codificar depende da proteção que se deseja, se **confidencialidade ou autenticação**, integridade e não-repúdio. A chave privada pode ser armazenada de diferentes maneiras, como um arquivo no computador, um *smartcard* ou um *token*. Como exemplo desse método temos os algoritmos: RSA, DSA, ECC e Diffie-Hellman.

Principais Algoritmos de Criptografia

- **DES (Data Encryption Standard):** essa chave consiste nominalmente em 64 bits, porém utiliza apenas 56 bits, que corresponde à aproximadamente 72 quatrilhões de combinações, que apesar de ser um número absurdamente alto, em 1999, foi quebrado através do método de “tentativa e erro”, em um desafio na Internet. Ainda assim, foi aprovado pelo governo dos EUA como algoritmo padrão em 1976 e utilizado a partir de 1977 até 2002, tendo passado nesse período por 3 revisões que resultaram no último prescrito “Triplo DES” ou 3DES.
- **AES (Advanced Encryption Standard):** criado a partir de um concurso do governo americano para definir um novo algoritmo padrão de chave simétrica, hoje em dia é um dos melhores e mais populares algoritmos de criptografia. O AES tem um tamanho de bloco fixo em 128 bits, mas diferentes comprimentos de chave: 128, 192 e 256 bits.
- **IDEA (International Data Encryption Algorithm):** é um algoritmo de cifra de bloco que faz uso de chaves de 128 bits e que tem uma estrutura semelhante ao DES.
- **RSA (Rivest, Shamir and Adleman):** É um dos algoritmos de chave assimétrica mais utilizados, onde dois números primos (aqueles números que só podem ser divididos por 1 e por eles mesmos) são multiplicados para a obtenção de um terceiro valor. A chave privada do RSA são os números que são multiplicados e a chave pública é o valor que será obtido. Para descobrir os dois primeiros números a partir do terceiro, é preciso fazer fatoração. Dessa forma, se forem utilizados números grandes, será praticamente impossível descobrir o código.

Imprima o capítulo Aposta Estratégica separadamente e dedique um tempo para absolver tudo o que está destacado nessas duas páginas. Caso tenha alguma dúvida, volte ao Roteiro de Revisão e Pontos do Assunto que Merecem Destaque. Se ainda assim restar alguma dúvida, não hesite em me perguntar no fórum.

QUESTÕES ESTRATÉGICAS

Nesta seção, apresentamos e comentamos uma amostra de questões objetivas selecionadas estrategicamente: são questões com nível de dificuldade semelhante ao que você deve esperar para a sua prova e que, em conjunto, abordam os principais pontos do assunto.

A ideia, aqui, não é que você fixe o conteúdo por meio de uma bateria extensa de questões, mas que você faça uma boa revisão global do assunto a partir de, relativamente, poucas questões.





1. (CESPE / SEFAZ-RS – 2019)

Para o estabelecimento de padrões de segurança, um dos princípios críticos é a necessidade de se verificar a legitimidade de uma comunicação, de uma transação ou de um acesso a algum serviço. Esse princípio refere-se à

- a) confidencialidade.
- b) autenticidade.
- c) integridade.
- d) conformidade.
- e) disponibilidade.

Comentários

Legitimidade está interligada diretamente a autenticidade. Esse princípio identifica e registra as ações de envio ou edição de uma informação, realizadas pelo usuário. Toda ação é documentada, garantido a autenticidade da informação proveniente de uma fonte confiável. Portanto, a alternativa correta é a letra B.

Gabarito: alternativa B.

2. (CESPE / PRF – 2019)

Acerca de proteção e segurança da informação, julgue o seguinte item.

No acesso a uma página web que contenha o código de um vírus de script, pode ocorrer a execução automática desse vírus, conforme as configurações do navegador.

Comentários

De acordo com a cartilha de segurança para Internet, o vírus de script é escrito em linguagem de script, como VBScript e JavaScript, e recebido ao acessar uma página Web ou por e-mail, como um arquivo anexo ou como parte do próprio e-mail escrito em formato HTML. Pode ser automaticamente executado, dependendo da configuração do navegador Web e do programa leitor de e-mails do usuário. Portanto, assertiva correta.

Gabarito: certo.

3. (CESPE / Polícia Federal – 2018)



Julgue o próximo item, a respeito de proteção e segurança, e noções de vírus, worms e pragas virtuais.

A infecção de um sistema por códigos maliciosos pode ocorrer por meio da execução de arquivos infectados obtidos de anexos de mensagens eletrônicas, de mídias removíveis, de páginas web comprometidas, de redes sociais ou diretamente de outros equipamentos.

Comentários

As formas citadas pela assertiva são as mais comuns, mas apenas algumas das possíveis para infecção de um sistema. Portanto, assertiva correta.

Gabarito: certo.

4. (CESPE / Polícia Federal – 2018)

Julgue o próximo item, a respeito de proteção e segurança, e noções de vírus, worms e pragas virtuais.

Um ataque de ransomware comumente ocorre por meio da exploração de vulnerabilidades de sistemas e protocolos; a forma mais eficaz de solucionar um ataque desse tipo e recuperar os dados “sequestrados” (criptografados) é a utilização de técnicas de quebra por força bruta da criptografia aplicada.

Comentários

Em um ataque ransomware é praticamente impossível recuperar os dados criptografados e o esforço exigido para tal processo não compensa o retorno. Dessa forma, a melhor maneira de recuperar os dados é através do backup.

Gabarito: errado.

5. (CESPE / Polícia Federal – 2018)

Julgue o item subsecutivo a respeito de redes de computadores e conceitos de proteção e segurança.

Um firewall é uma combinação de hardware e software que isola da Internet a rede interna de uma organização, permitindo o gerenciamento do fluxo de tráfego e dos recursos da rede e o controle, pelo administrador de rede, do acesso ao mundo externo.

Comentários

Em termos mais técnicos o elaborador descreveu o conceito de firewall que inserimos na aula. O firewall é um dispositivo de segurança da rede que monitora o tráfego de rede. Traduzindo de forma literal ele é uma “parede de fogo” que de acordo com regras pré-definidas decide permitir ou bloquear tráfegos específicos. Ele pode ser tanto um software quanto um hardware, onde a combinação de ambos é chamada tecnicamente de “appliance”.

Gabarito: certo.



6. (CESPE / PC-MA – 2018)

Determinado tipo de vírus eletrônico é ativado quando um documento por ele infectado é aberto, podendo então, nesse momento, infectar não apenas outros documentos, mas também um gabarito padrão de documento, de modo que cada novo documento criado sob esse gabarito seja infectado. Tal vírus, cuja propagação ocorre quando documentos por ele infectados são remetidos por correio eletrônico para outros usuários, é conhecido como

- a) vírus de setor de carga (boot sector).
- b) vírus de programa.
- c) vírus de macro.
- d) backdoor.
- e) hoax.

Comentários

De acordo com o site, <https://www.kaspersky.com.br/resource-center/definitions/macro-virus>, um macro vírus é um vírus de computador que altera ou substitui uma macro, que é um conjunto de comandos usados por programas para executar ações comuns. Por exemplo, a ação "documento aberto" em muitos programas de processamento de texto se baseia em uma macro para funcionar, uma vez que existem várias etapas distintas no processo. Os macros vírus mudam esse conjunto de comandos, permitindo que sejam executados sempre que a macro é executada. Essa definição se encaixa perfeitamente com o enunciado da questão e portanto nossa resposta está na alternativa B.

Gabarito: alternativa B.

7. (CESPE / TCE-PB – 2018)

Entre os vários tipos de programas utilizados para realizar ataques a computadores, aquele capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo entre computadores, é conhecido como

- a) botnet.
- b) spyware.
- c) backdoor.
- d) trojan.
- e) worm.

Comentários

Conforme vimos na aula, o software malicioso capaz de se autorreplicar através das redes é o worm. Portanto, a alternativa correta é a letra E.



Gabarito: alternativa E.

8. (CESPE / TRT-7ª Região (CE) – 2018)

Assinale a opção que apresenta um tipo de malware capaz de registrar as teclas que são digitadas em uma estação de trabalho, fazer capturas de tela e até mesmo acessar arquivos em drives locais e(ou) compartilhados.

- a) boot
- b) cavalo de troia
- c) macro
- d) melissa

Comentários

Vimos na aula que o cavalo de troia, também conhecido como spyware, são softwares maliciosos de espionagem que capturaram e transmitem informações altamente pessoais como contas bancárias online e senhas, ou informações de cartão de crédito. Portanto a alternativa correta é a letra B.

Gabarito: alternativa B.

9. (CESPE / TRE-BA – 2017)

Assinale a opção que apresenta a solução que permite filtrar tentativas de acessos não autorizados oriundos de outros ambientes e redes externas, contribuindo para a melhora do estado de segurança da informação de ambientes computacionais.

- a) certificado digital
- b) chave de criptografia
- c) rootkits
- d) firewall
- e) antivírus

Comentários

Sempre que uma questão mencionar o termo filtro de acesso, ou controle de acesso, ela está relacionada ao firewall. Portanto, a alternativa correta é a letra D.

Gabarito: alternativa D.



10. (CESPE / SERES-PE – 2017)

Praga virtual que informa, por meio de mensagem, que o usuário está impossibilitado de acessar arquivos de determinado equipamento porque tais arquivos foram criptografados e somente poderão ser recuperados mediante pagamento de resgate denomina-se

- a) ransomware.
- b) trojan.
- c) spyware.
- d) backdoor.
- e) vírus.

Comentários

Conforme vimos na aula, o malware ou software malicioso que criptografa arquivos e envia mensagem cobrando resgate para que possam ser novamente acessados é ransomware. Portanto, a alternativa correta é a letra A.

Gabarito: alternativa A.

11. (CESPE / TRE-PE – 2017)

Os mecanismos que contribuem para a segurança da informação em ambientes computacionais incluem

- a) certificado digital, criptografia e cavalo de troia.
- b) *backdoor*, *firewall* e criptografia.
- c) *rootkits*, arquivos de configuração e becape.
- d) *firewall*, *worm* e *proxy*.
- e) VPN, *honeypot* e senha.

Comentários

Vamos analisar todas as alternativas:

a) certificado digital (CORRETO) / criptografia (CORRETO) / cavalo de troia (ERRADO – O Cavalo de Troia é um *malware* do tipo spyware)

b) backdoor (ERRADO – vulnerabilidade explorada por spywares / firewall (CORRETO) / criptografia (CORRETO)

c) ROOTKITS (ERRADO – Rootkit é um tipo de praga virtual de difícil detecção, visto que é ativado antes que o sistema operacional tenha sido completamente inicializado / arquivos de configuração (ERRADO – sem relação com a segurança da informação) / becape (CORRETO)



- d) firewall (CORRETO) / worm (ERRADO) / proxy (CORRETO)
- e) VPN (CORRETO – virtual private network) / honeypot (CORRETO – pote de mel, é uma ferramenta que tem a função de propositadamente simular falhas de segurança de um sistema e colher informações sobre o invasor. Uma espécie de armadilha para invasores.) / senha (CORRETO)

Portanto a alternativa correta é a letra E.

Gabarito: alternativa E.

12. (CESPE / TRE-PI – 2017)

A remoção de códigos maliciosos de um computador pode ser feita por meio de

- a) *anti-spyware*.
- b) detecção de intrusão.
- c) *anti-spam*.
- d) *anti-phishing*.
- e) filtro de aplicações.

Comentários

Vamos analisar as alternativas:

- a) Correto. Anti-spyware é um programa cujo objetivo é tentar eliminar do sistema operacional, spywares, adwares, keyloggers, trojans e outros *malwares*. Apesar das funções serem semelhantes as do antivírus, devemos tomar cuidado para não confundi-los.
- b) Errado. A detecção de intrusão funciona através de um IDS (Intrusion detection System) que é um sistema de detecção de intrusão na rede.
- c) Errado. Um anti-spam funciona como um filtro bloqueando as mensagens de e-mail detectadas como spam.
- d) Errado. Anti-phishing é um programa que bloqueia códigos maliciosos que tentam realizar o phishing, capturando os dados do usuário.
- e) Errado. Filtro de aplicações funciona controlando o acesso a determinadas aplicações.

Gabarito: alternativa A.



QUESTIONÁRIO DE REVISÃO E APERFEIÇOAMENTO

A ideia do questionário é elevar o nível da sua compreensão no assunto e, ao mesmo tempo, proporcionar uma outra forma de revisão de pontos importantes do conteúdo, a partir de perguntas que exigem respostas subjetivas.

São questões um pouco mais desafiadoras, porque a redação de seu enunciado não ajuda na sua resolução, como ocorre nas clássicas questões objetivas.

O objetivo é que você realize uma autoexplicação mental de alguns pontos do conteúdo, para consolidar melhor o que aprendeu ;)

Além disso, as questões objetivas, em regra, abordam pontos isolados de um dado assunto. Assim, ao resolver várias questões objetivas, o candidato acaba memorizando pontos isolados do conteúdo, mas muitas vezes acaba não entendendo como esses pontos se conectam.

Assim, no questionário, buscaremos trazer também situações que ajudem você a conectar melhor os diversos pontos do conteúdo, na medida do possível.

É importante frisar que não estamos adentrando em um nível de profundidade maior que o exigido na sua prova, mas apenas permitindo que você compreenda melhor o assunto de modo a facilitar a resolução de questões objetivas típicas de concursos, ok?

Nosso compromisso é proporcionar a você uma revisão de alto nível!

Vamos ao nosso questionário:

Perguntas

- 1) O que é um vírus e como ele afeta um sistema?**
- 2) Qual a definição de cada princípio da segurança da informação? Cite exemplos relacionados a cada princípio.**
- 3) O que é um firewall? Quais os tipos de firewall? Como eles funcionam?**
- 4) Qual a diferença entre phishing, worm e ransomware?**



5) Quais os fatores e métodos de autenticação e como eles são aplicados?



Perguntas com respostas

1) O que é um vírus e como ele afeta um sistema?

Um vírus de computador é um programa ou código malicioso criado para alterar a forma como um computador funciona. Ele atua se inserindo ou se anexando a um programa ou documento legítimo, que tenha suporte para macros, a fim de executar o seu código. Durante esse processo, um vírus pode potencialmente causar efeitos inesperados ou prejudiciais, como danificar o sistema, corrompendo ou destruindo os dados.

2) Qual a definição de cada princípio da segurança da informação? Cite exemplos relacionados a cada princípio.

Disponibilidade - Princípio que garante que a informação estará sempre disponível.

Integridade - Princípio que garante que as informações serão guardadas ou enviadas em sua forma original, sem sofrer alterações.

Confidencialidade - Princípio que garante o sigilo da informação com a capacidade de controlar o acesso, assegurando que elas só serão acessadas por pessoas autorizadas. Ou seja, é a garantia que as informações só serão acessadas através de uma senha.

Autenticidade - Princípio que permite verificar a identidade de uma pessoa em um sistema, garantindo a veracidade das informações.

3) O que é um firewall? Quais os tipos de firewall? Como eles funcionam?

Um firewall é um dispositivo de segurança da rede que monitora o tráfego de rede. Traduzindo de forma literal ele é uma “parede de fogo” que de acordo com regras pré-definidas decide permitir ou bloquear tráfegos específicos. Ele pode ser tanto um software quanto um hardware, onde a combinação de ambos é chamada tecnicamente de “appliance”. Na sua forma mais simples de implementação, o firewall funciona como um filtro de pacotes (stateless) que pode ser configurado tanto para a rede interna, quanto para a rede externa (Internet). A outra forma de configuração é a de estado de sessão (statefull), onde o firewall analisa os pacotes e guarda o estado de cada conexão de maneira que seja possível para identificar e fazer uma previsão das respostas legítimas, de forma a impedir o tráfego de pacotes ilegítimos.

4) Qual a diferença entre phishing, worm e ransomware?

O phishing é um golpe on-line de falsificação. Os phishers enviam e-mails que tentam imitar mensagens de empresas financeiras legítimas ou de outras empresas solicitando que o usuário acesse um site falso para reinserir o número do seu cartão de crédito ou verificar sua senha. A partir da inserção desses dados eles têm acesso a todas as informações necessárias para aplicar golpes. Um worm é um software malicioso capaz de se autorreplicar em computadores ou por redes de computadores sem que você desconfie que sua máquina foi infectada. Eles podem explorar erros de configuração da rede (por exemplo, copiar a si mesmos em um disco totalmente acessível) ou explorar brechas na segurança do sistema operacional e dos aplicativos. O ransomware é um tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate (ransom) para restabelecer o acesso ao usuário.



5) Quais os fatores e métodos de autenticação e como eles são aplicados?

“O que você sabe” – Autenticação baseada no conhecimento. Exemplo: senha; “O que você tem” – Autenticação baseada na propriedade. Exemplo: token, certificado digital; “O que você é” – Autenticação baseada na característica Exemplo: biometria.

Existe um material desenvolvido pelo Comitê Gestor da Internet no Brasil - CGI.br, que aborda os principais pontos cobrados em concursos. Esse material está disponível em: <https://cartilha.cert.br/> e serve como base para o seu estudo sobre Segurança da Informação. Não é um material extenso e os textos são bastante didáticos para facilitar a compreensão.

...

Forte abraço e bons estudos!

"Hoje, o 'Eu não sei', se tornou o 'Eu ainda não sei'"

(Bill Gates)

Thiago Cavalcanti



Face: www.facebook.com/profthiogocavalcanti
Insta: www.instagram.com/prof.thiago.cavalcanti
YouTube: youtube.com/profthiogocavalcanti



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.