Estratégia Concursos

Aula 07

SERPRO (Analista - Especialização: Tecnologia) Bizu Estratégico - 2023 (Pós-Edital)

Autor:
Elizabeth Menezes de Pinho Alves, Leonardo Mathias, Paulo Júnior, Aline Calado Fernandes

23 de Maio de 2023

BIZU ESTRATÉGICO DE SEGURANÇA DA INFORMAÇÃO – SERPRO

Olá, concurseiro! Tudo certo?

Neste material, traremos uma seleção de *bizus* da disciplina de **Segurança da Informação** para o concurso **SERPRO**.

O objetivo é proporcionar uma revisão rápida e de alta qualidade aos alunos por meio de tópicos que possuem as maiores chances de incidência em prova.

Vale lembrar que todos os *bizus* destinam-se àqueles que já estejam na fase final de revisão, ou seja, que já estudaram bastante o conteúdo teórico da disciplina e, nos últimos dias, precisam revisar por algum material bem curto e objetivo. Este *bizu* foi elaborado com base no curso de **Segurança da Informação** do professor **André Castro.**

Aline Calado

@alinecalado.f

Leonardo Mathias

@profleomathias

ANÁLISE ESTATÍSTICA

Pessoal, segue abaixo uma análise estatística dos assuntos mais exigidos pela Banca **CEBRASPE** no âmbito da disciplina de **Segurança da Informação** em concursos. Com base nessa análise, podemos focar nos pontos mais importantes para revisar e detonar na prova!

Assunto	% de cobrança
Mecanismos de segurança (Criptografia, Assinatura Digital, arantia de Integridade, Controle de Acesso, Certificação Digital, ICP-Brasil) – parte I	46,43%
Mecanismos de segurança (Criptografia, Assinatura Digital, arantia de Integridade, Controle de Acesso, Certificação Digital, ICP-Brasil) – parte II	
Políticas de segurança (NBR ISO/IEC 27002:2005, NBR ISO/IEC 27001:2013, Políticas de senhas)	26,79%

MAPA DO BIZU

Segue abaixo tabela contendo a numeração dos *Bizus* referentes a cada tópico abordado e os respectivos cadernos de questões selecionadas no nosso SQ:

Os cadernos de questões foram montados utilizando questões específicas de concursos realizados pela banca **CEBRASPE** nos últimos anos.

Como já mencionado, neste material abordaremos **apenas os temas mais importantes do edital,** considerando tanto o percentual de incidência nas provas, quanto a extensão e complexidade do assunto. Veja como está estruturado o seu *Bizu*.

Assunto	Bizus	Caderno de Questões
Mecanismos de segurança (Criptografia, Assinatura Digital, Garantia de Integridade, Controle de Acesso, Certificação Digital, ICP-Brasil) – parte I	1	http://questo.es/0lz3hq
Mecanismos de segurança (Criptografia, Assinatura Digital, Garantia de Integridade, Controle de Acesso, Certificação Digital, ICP-Brasil) – parte II	2	
Políticas de segurança (NBR ISO/IEC 27002:2005, NBR ISO/IEC 27001:2013, Políticas de senhas)	3	http://questo.es/gqzdv1

Apresentação

Antes de começarmos, gostaria de me apresentar. Meu nome é **Aline Calado**, tenho 30 anos e sou natural de Pernambuco. Sou graduada em Ciências Contábeis pela UFPE e Pós-Graduada em Contabilidade Pública e Auditoria.

Atualmente, exerço o cargo de Auditora de Controle Externo (Agente da Fiscalização) no Tribunal de Contas do Estado de São Paulo (TCE-SP).

Serei a responsável pelo seu **Bizu Estratégico de Segurança da Informação** e, com ele, pretendo abordar os tópicos mais cobrados nessa disciplina, de maneira concisa e objetiva, por meio de uma linguagem bem clara!

Espero que gostem!

Um grande abraço e bons estudos!

1. Mecanismos de segurança (Criptografia, Assinatura Digital, Garantia de Integridade, Controle de Acesso, Certificação Digital, ICP-Brasil) – parte I.

Criptografia

A criptografia é uma ciência que tem como objetivo "embaralhar" as informações. Desse modo, ainda que um atacante obtenha acesso aos dados, este não será capaz de lê-la e em alguns casos, alterá-la.

-***Análysis*** = decomposição;
-***Logo*** = estudo.
-Criptoanálise = Ciência de quebrar códigos e decifrar mensagens. Então o simples fato de você buscar quebrar o código e não somente interpretar a informação já é uma forma de ataque.
-Criptologia = Ciência que agrega a criptografia e a criptoanálise.
-Cifra = Método de codificação de mensagens com vista à sua ocultação.

Ao codificarmos uma mensagem, podemos utilizar, basicamente, três métodos de cifragem, quais sejam: substituição, transposição e esteganografia.

Substituição

A substituição é um método de codificação que busca alterar um caractere, símbolo ou dado em algum outro. É o método mais simples e fácil de executar. Porém, tende a ser o mais fácil de ser quebrado.

Transposição

A transposição foca no simples embaralhamento das letras segundo alguma rotina. Um exemplo simples seria transpor cada sílaba de cada palavra (bloco) para esquerda, mantendo a rotação de cada bloco.

Esteganografia

A esteganografia que tem como objetivo esconder uma mensagem dentro de outra. Tipicamente, busca-se enviar uma mensagem de texto embutido no código de uma imagem.

Cifragem de Bloco – Cipher Block

A ideia é quebrar a mensagem a ser enviada em blocos de tamanho fixo antes de se aplicar as diversas operações matemáticas de determinado algoritmo.

Em regra, temos que todos os modos buscam garantir aspectos de confidencialidade.

Alguns deles são capazes de tratar aspectos de autenticidade e integridade, ou seja, não podemos generalizar e afirmar que a cifragem por bloco garante os princípios de segurança de forma geral.
-***Eletronic Code Book – ECB:*** É o método mais simples que utiliza como conceito a independência dos blocos sendo aplicada a mesma chave. É uma técnica não randômica pela simples concatenação dos blocos resultado da fragmentação da mensagem original.
-***Cipher Block Chaining – CBC:*** É o método mais utilizado. Utiliza a operação XOR devidamente representada na imagem a seguir pelo círculo em volta do sinal de "+".
A cifragem de cada bloco depende da cifragem de todos os blocos anteriores.
-***Cipher FeedBack – CFB:*** Suporta qualquer tamanho de entrada, independentemente do bloco.
Por esse motivo, se torna útil para aplicações que dependem de transmissão imediata.

Cifragem de Fluxo – Stream Cipher

Diferentemente da cifra de bloco, a cifra de fluxo não necessita aguardar o processamento de toda a mensagem para se aplicar o algoritmo. Como o próprio nome nos remete, a ideia é ser algo mais dinâmico e ágil de tal forma que, à medida que os dados vão chegando, vai se aplicando o algoritmo de forma contínua.

Identificação de Dados Criptografados

a. Criptoanálise

A criptoanálise tem foco no entendimento de como funciona o algoritmo de criptografia. Desse modo, a realização da criptoanálise depende da quantidade
de informações que se tem à disposição e quão possível é manipulá-las.
A partir daí, podemos elencar cincos tipos de ataques, que recorrentemente caem em provas, quais sejam:
1. **Apenas Texto Cifrado – CypherText-Only:** Nesse contexto, há conhecimento apenas do algoritmo de criptografia utilizado e do próprio texto cifrado;
2. **Texto Claro Conhecido – Known-plaintext:** Além dos itens acima, o atacante tem a informação dos pares de texto claro de entrada e seu respectivo texto cifrado de saída;
3. **Texto Claro Escolhido – Choosen-Plaintext:** Agora o atacante não se restringe apenas a saber o par de entrada e saída, mas ele é capaz de manipular a entrada e avaliar a sua respectiva saída;
4. **Texto Cifrado Escolhido – Choosen-CypherText:** Agora o atacante é capaz de fazer o caminho reverso, onde a partir de um texto cifrado escolhido, ele é capaz de verificar qual o texto em claro correspondendo;
5. **Texto Escolhido – Choosen-Text** – Há plena capacidade de manipulação dos textos de entrada e saída, e vice versa;

b. Métodos de Decifragem de Dados

1. Método da Recuperação Direta: O intuito desse método é conseguir obter a senha de maneira direta, ou seja, a partir de algum ponto de armazenamento ou a chave utilizada como referência para armazenar o dado criptografado.

2. Método Pré-Computado: Neste método, busca-se criar uma lista, bem extensa por sinal (aumentando a chance de quebra), que correlaciona, para um determinado algoritmo, os textos em claro e os resultados gerados. Por isso o termo "pré-computado".

3. Método da Força Bruta: Aqui, busca-se, a partir de um grande poder computacional, processar todas as possibilidades de senhas para determinado ambiente ou algoritmos.

4. Método de Dicionário: Sem dúvida, no contexto atual, é uma das técnicas mais utilizadas. O procedimento a ser realizado é muito semelhante com o método da Força Bruta. Entretanto, a invés de se testar todas as possibilidades possíveis dentro de uma quantidade limitada de caracteres, testasse as senhas conforme uma lista pré-definida de "possíveis senhas" para o contexto em análise.

5. Método probabilístico: Por fim, temos o método probabilístico. Como o nome já diz, busca-se por intermédio de algoritmos e análises estatísticas, aquelas sequências de caracteres que possuem maior probabilidade de ocorrência dado um contexto. Este método pode ser derivado em duas subespécies, quais sejam: **probabilidade condicional e gramática especializada**.

Importante destacar a eficiência de cada um dos métodos. No caso da Força Bruta sendo eficiente contra as senhas pequenas e homogêneas, já o dicionário para senhas comuns que ainda possuem alguma regra de alteração e a probabilística para os casos mais complexos a serem tratados.

Criptografia Simétrica

A criptografia simétrica possui como princípio o fato de se utilizar a mesma chave para o procedimento de criptografia e descriptografia.

A criptografia simétrica visa garantir apenas o princípio da confidencialidade.
Atenção: Alguns autores assumem que o fato de apenas os envolvidos na comunicação terem acesso à chave, vale o princípio da autenticidade.

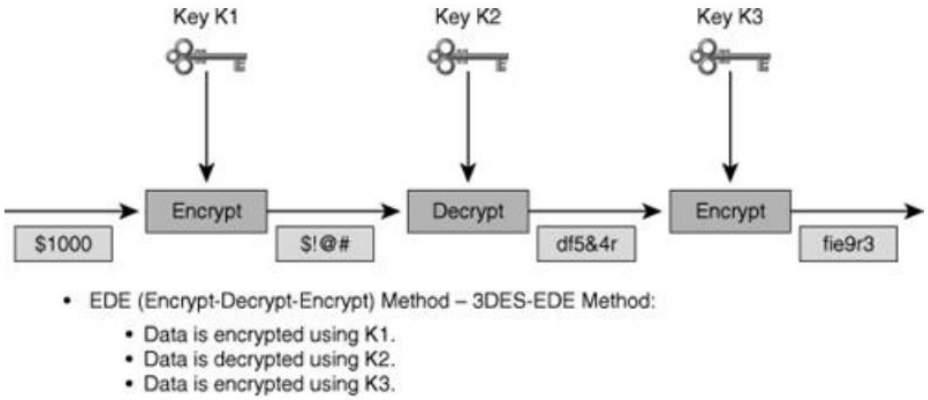
Vamos conhecer agora os principais algoritmos de criptografia simétrica:

DES

Durante muitos anos o DES foi o algoritmo padrão utilizado na criptografia simétrica. Foi criado pela IBM em 1977 com tamanho de chaves relativamente pequenas, quando comparada com as demais. Apesar do tamanho da chave ser de 64 bits, a robustez para efeito de quebra de chave era de 56 bits, uma vez que os 8 são derivados dos 56 bits.

3DES

Na tentativa de dar uma sobrevida ao DES, criou-se o 3DES, que nada mais é do que a aplicação do DES três vezes, com o detalhe de que na segunda vez, faz-se o processo de decriptação.



Desse modo, ao se utilizar três chaves distintas, tem-se uma robustez de 56 bits por chave, totalizando 168 bits de tamanho de chave.

AES – Advanced Encryption Standard

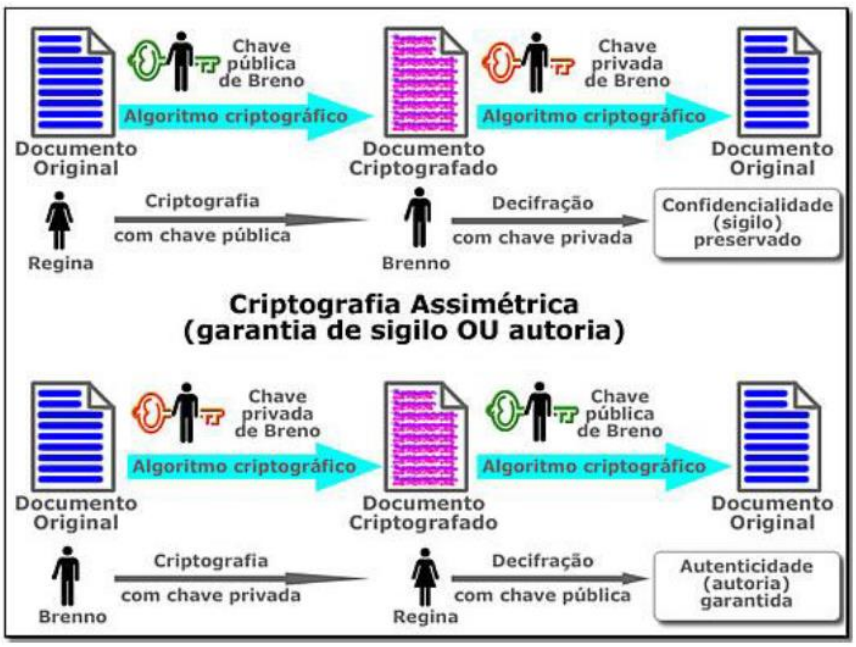
Foi desenvolvido para substituir o DES como padrão do governo americano. Suporta tamanhos de chaves variáveis. Entretanto, por padrão, utiliza-se o tamanho de bloco de 128 bits, podendo ser utilizado chaves de 128, 192 e 256 bits. Não utiliza a tão conhecida rede de Feistel disseminada pelo DES.
Seu funcionamento pode ser resumido em quatro estágios, quais sejam:
SubBytes – Utiliza uma caixa-S para substituição operada byte a byte de acordo com uma tabela;
ShiftRows – Permutação Simples;
Seu funcionamento pode ser resumido em quatro estágios, quais sejam:
SubBytes – Utiliza uma caixa-S para substituição operada byte a byte de acordo com uma tabela;
ShiftRows – Permutação Simples;

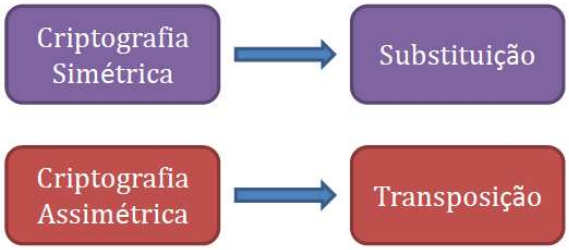
Outros exemplos de algoritmos de criptografia simétrica são: o Blowfish, Twofish e IDEA.

Criptografia Assimétrica

A criptografia Assimétrica, também conhecida como criptografia de chaves públicas é caracterizada pelo fato de se utilizar duas chaves no processo criptográfico, ou seja, caso seja utilizada uma para criptografar os dados, deve-se, necessariamente, usar a outra para descriptografar. As duas chaves utilizadas são conhecidas como privada e pública.
O processo de criptografia de chave pública não se restringe a uma única sequência, isto é, não necessariamente se criptografa com a chave privada e decriptografa com a pública.
É possível usar algoritmos de criptografia assimétrica para trocar informações de chaves simétricas. Essa característica é a base das soluções de certificação digital.

Se o objetivo é garantir a confidencialidade, deve-se cifrar com a chave pública do RECEPTOR e decifrar com a chave privada do RECEPTOR!
Se o objetivo é garantir a autenticidade, deve-se cifrar com a chave privada do EMISSOR e decifrar com a chave pública do EMISSOR!





Diffie-Hellman – DH

Principal algoritmo quando se fala no propósito de troca de chaves simétricas em um meio inseguro sem conhecimento prévio do segredo.
A sua estrutura e robustez reside na complexidade e problema do logaritmo discreto.

RSA – Rivest, Shamir and Adelman

Possui a característica de ser utilizado tanto para processos de cifragem como para produzir hashes. Foi baseado na proposta apresentada pelo algoritmo DH.
Sua robustez reside na dificuldade de se fatorar números extensos. Sugere-se, atualmente, que sejam utilizadas chaves de 2048 a 4096 bits para aumentar a robustez contra ataques de força bruta.

El Gamal

- O El Gamal possui como segurança de seu sistema a dificuldade do cálculo de logaritmos discretos em um corpo finito.

Sua principal aplicação é na transferência de assinaturas digitais e trocas de chaves no estabelecimento de comunicações. Possui três componentes básicos: gerador de chaves, algoritmo de cifragem e algoritmo decifragem.

Funções HASH

As funções HASH são algoritmos criptográficos unidirecionais. Utiliza-se funções matemáticas que permitem gerar um resultado de tamanho fixo independentemente do tamanho do conteúdo de entrada.
Outras características que surgem nas funções de HASH é que estas devem apresentar modelos matemáticos e cálculos simples que exijam pouco processamento das informações. Além disso, o conceito de difusão diz que deve ser impossível modificar a mensagem original sem modificar o resultado do HASH desta mensagem.
O resultado de um cálculo de uma função HASH também é bastante referenciada como “message digest”.

MD5

Esse algoritmo produz um tamanho de HASH de 128 bits.

MD4

O MD4 produz HASH de tamanho de 128 bits, dependendo de entradas de tamanho múltiplos de 512 bits.

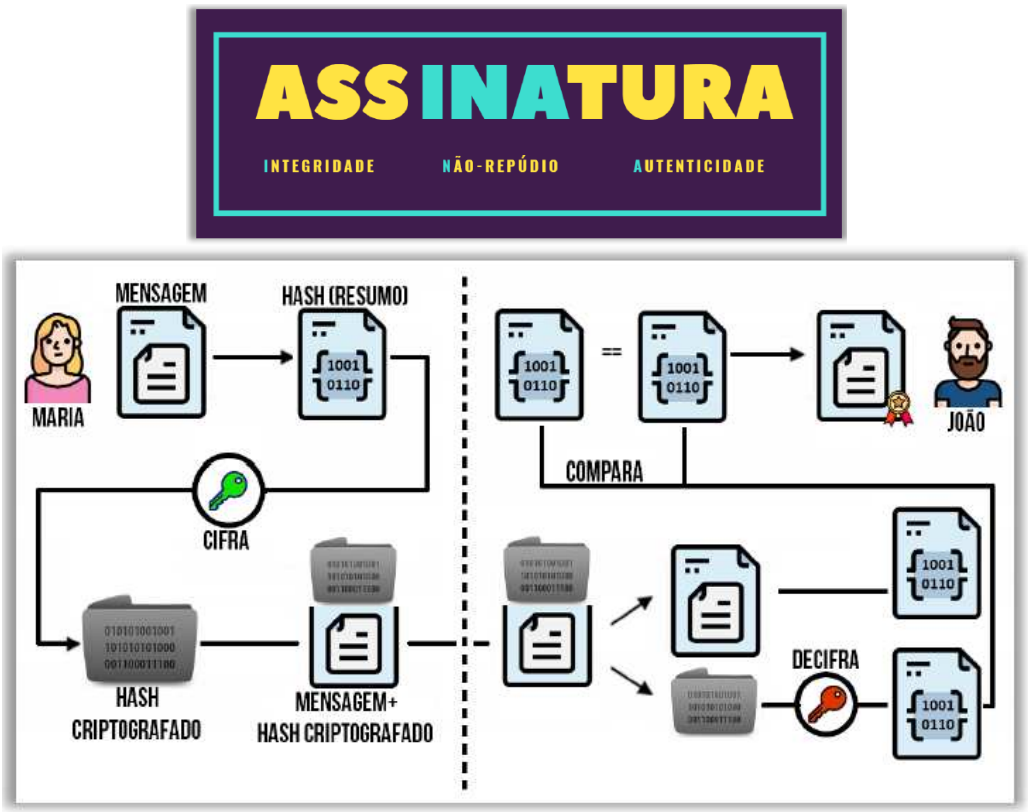
SHA

O algoritmo SHA possui diversas versões de implementação que produzem resultados distintos. Atualmente, temos os algoritmos abaixo e seus respectivos tamanhos de HASH:
SHA1 – 160 bits de HASH;
SHA-224 – 224 bits de HASH. É uma versão truncada do SHA-256;
SHA-256 – 256 bits de HASH, com palavras de entrada de 256 bits;
SHA-384 – 384 bits de HASH. É uma versão truncada do SHA-512;
SHA-512 – 512 bits de HASH, com palavras de entrada de 512 bits;

2. Mecanismos de segurança (Criptografia, Assinatura Digital, Garantia de Integridade, Controle de Acesso, Certificação Digital, ICP-Brasil) – parte II.

Assinatura Digital

Trata-se de um método matemático de autenticação de informação digital tipicamente tratado como substituto à assinatura física, já que elimina a necessidade de ter uma versão em papel do documento que necessita ser assinado. Por meio de um Algoritmo de Hash, é possível garantir a integridade dos dados.



Principais algoritmos: SHA-1 (Hash de 160 bits), MD5 (Hash de 128 bits), etc

FUNCIONAMENTO da Assinatura Digital
Maria possui uma mensagem em claro (sem criptografia). Ela gera um hash dessa mensagem, depois criptografa esse hash utilizando sua chave privada. Em seguida, ela envia para João tanto a mensagem original quanto o seu hash. João gera um hash da mensagem original e obtém um resultado, depois descriptografa o hash da mensagem utilizando a chave pública de Maria e obtém outro resultado. Dessa forma, ele tem dois hashes para comparar: o que ele gerou a partir da mensagem em claro e o que ele descriptografou a partir da mensagem criptografada. Se forem iguais, significa que Maria realmente enviou a mensagem, significa que ela não pode negar que enviou a mensagem e, por fim, significa que a mensagem está íntegra.

A Assinatura Digital possui uma autenticação relativamente frágil, porque não é possível saber se a chave pública que foi utilizada é realmente de quem diz ser.
Para resolver esse problema, é necessária uma terceira parte confiável chamada Autoridade Certificadora (AC).
A Autoridade Certificadora é uma entidade responsável por emitir certificados digitais – ela é uma espécie de Cartório Digital.
A Autoridade Certificadora é responsável por emitir, distribuir, renovar, revogar e gerenciar certificados digitais.
Esse cadeado significa que essa página web fornece um serviço possivelmente crítico em que trafegam informações sigilosas, portanto ela oferece um canal de comunicação criptografado e seguro.
Essa camada adicional de segurança permite que os dados possam ser transmitidos por meio de uma conexão criptografada/segura e que se verifique a autenticidade do servidor web por meio do uso de certificados digitais (é a autenticidade do servidor e, não, do cliente).

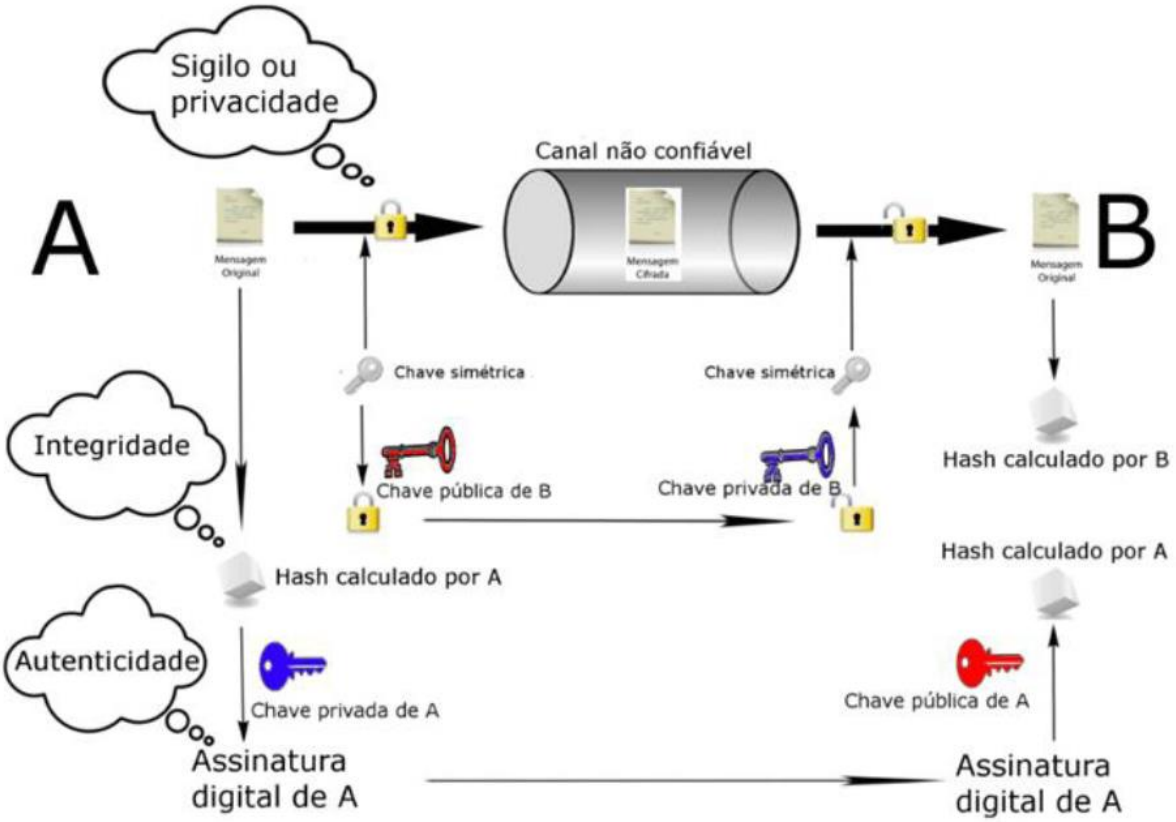
Certificado Digital

Certificado Digital é um documento eletrônico assinado digitalmente por uma terceira parte confiável – chamada Autoridade Certificadora – e que cumpre a função de associar uma entidade (pessoa, processo, servidor) a um par de chaves criptográficas com o intuito de tornar as comunicações mais confiáveis e auferindo maior confiabilidade na autenticidade. Ele é capaz de garantir a autenticidade, integridade e não-repúdio, e até confidencialidade.

As principais informações contidas em um certificado digital são:
- Chave pública do usuário ou sistemas;
- Dados relativos à sua identidade;
- Prazo de validade;
- Assinatura Digital da Entidade Certificadora que gerou o certificado;
- Chave pública da CA
- Cadeia de certificados hierarquicamente superiores;

Além disso, por seguir o padrão X.509 do ITU-t, consta ainda:
- Versão do X.509 e número de série do certificado;
- Informação do algoritmo gerador do certificado;
- Identificação do gerador do certificado;

● Informações sobre o algoritmo assimétrico da chave pública do usuário;



● **Tipos de Certificados Digitais:**

o **Certificado de Assinatura Digital (A1, A2, A3 e A4)**

▪ São os certificados usados para confirmação da identidade na web, correio eletrônico, transações online, redes privadas virtuais, transações eletrônicas, informações eletrônicas, cifração de chaves de sessão e assinatura de documentos com verificação da integridade de suas informações.

o **Certificado de Sigilo (S1, S2, S3 e S4)**

▪ São os certificados usados para cifração de documentos, bases de dados, mensagens e outras informações eletrônicas.

o **Certificado do Tipo A1 e S1**

▪ É o certificado em que a geração das chaves criptográficas é feita por software e seu armazenamento pode ser feito em hardware ou repositório protegido por senha, cifrado por software. Sua validade máxima é de um ano, sendo a frequência de publicação da LCR no máximo de 48 horas e o prazo máximo admitido para conclusão do processo de revogação de 72 horas.

o **Certificado do Tipo A2 e S2**

▪ É o certificado em que a geração das chaves criptográficas é feita em software e as mesmas são armazenadas em Cartão Inteligente ou Token, ambos sem capacidade de geração de chave e protegidos por senha. As chaves criptográficas têm no mínimo 1024 bits. A validade máxima do certificado é de dois anos, sendo a frequência de publicação da LCR no máximo de 36 horas e o prazo máximo admitido para conclusão do processo de revogação de 54 horas.

o **Certificado do Tipo A3 e S3**

▪ É o certificado em que a geração e o armazenamento das chaves criptográficas são feitos em cartão Inteligente ou Token, ambos com capacidade de geração de chaves e protegidos por senha, ou hardware criptográfico aprovado pela ICPBrasil.
As chaves criptográficas têm no mínimo 1024 bits. A validade máxima do certificado é de três anos, sendo a frequência de publicação da LCR no máximo de 24 horas e o prazo máximo admitido para conclusão do processo de revogação de 36 horas.

o **Certificado do Tipo A4 e S4**

▪ É o certificado em que a geração e o armazenamento das chaves criptográficas são feitos em cartão Inteligente ou Token, ambos com capacidade de geração de chaves e protegidos por senha, ou hardware criptográfico aprovado pela ICPBrasil.
As chaves criptográficas têm no mínimo 2048 bits. A validade máxima do certificado é de três anos, sendo a frequência de publicação da LCR no máximo de 12 horas e o prazo máximo admitido para conclusão do processo de revogação de 18 horas.

O certificado digital é público, logo a chave privada não pode estar inserida nele. **As chaves privadas podem ficar armazenadas em um computador, token ou smartcard protegidas por alguma senha.**

Exemplo de chave privada:
MDJKoZIAQ5MCAhvcNAQEBBQADKgAwDXcZ3OBJwlgYjDE7cZ83SO3QZZSfTiwvXqBezakBQsjQVZ1h5MCfTiwvwlgYAwEAAQ==XVOAoZIhvcNgEAAiBimNdWkSET

Comparação Assinatura Digital x Certificado Digital

ASSINATURA DIGITAL	CERTIFICADO DIGITAL
Trata-se um método matemático utilizado para verificar a autenticidade e integridade de uma entidade (mensagem, software, servidor, documento, etc).	Trata-se de um documento eletrônico assinado digitalmente por uma terceira parte confiável para vincular uma chave pública a uma entidade.
Garante a autenticidade do emissor, a integridade do documento e o não-repúdio.	Garante a confidencialidade ou a autenticidade do proprietário do certificado. Em combinação com outros recursos, pode garantir integridade e não repúdio.

ICP - INFRAESTRUTURA DE CHAVES PÚBLICAS – PKI (PUBLIC KEY INFRASTRUCTURE)

Todo o conjunto de hardware e software, pessoal, políticas e procedimentos necessários para criar e implementar uma infraestrutura de certificação digital chama-se PKI ou ICP. É uma estrutura hierárquica que permite uma melhor organização e gerenciamento dos certificados, além de tratar aspectos de auditabilidade e controle.

Esta pode ser composta por quatro componentes básicos:
Autoridade Certificadora – (CA – Certificate Authority)
Autoridade Registradora – (RA – Registration Authority)
Certificados Digitais
Lista de Certificados Revogados (CRL – Certification Revocation List)

3. Políticas de segurança (NBR ISO/IEC 27002:2005, NBR ISO/IEC 27001:2013, Políticas de senhas).

ISO 27001 E ISO 27002

A norma ISO 27001 de define os **requisitos de um Sistema de Gestão de Segurança da Informação – SGSI.**

Essa norma é um padrão e referência Internacional para a gestão da Segurança da Informação.
Possui como objetivo a provisão de requisitos para **ESTABELECER, IMPLEMENTAR, MANTER E MELHORAR CONTINUAMENTE** um SGSI

A norma é dividida em 10 tópicos e 1 anexo de referência. Os tópicos são os seguintes:
1. ESCOPO;
2. REFERÊNCIA NORMATIVA;
3. TERMOS e DEFINIÇÕES;
4. Contexto da ORGANIZAÇÃO;
5. LIDERANÇA;
6. PLANEJAMENTO;
7. APOIO;
8. OPERAÇÃO;
9. AVALIAÇÃO do DESEMPENHO;
10. MELHORIA;

Estrutura da Norma:

1. Políticas de segurança da informação
a. Orientação da Direção para segurança da informação
i. Políticas para segurança da Informação
ii. Análise crítica das políticas para Segurança da Informação;

2. Organização da Segurança da Informação
a. Organização Interna
i. Responsabilidades e papéis pela Segurança da Informação;
ii. Segregação de Funções;
iii. Contato com Autoridades;
iv. Contato com grupos Especiais;
v. Segurança da Informação no gerenciamento de projetos;
b. Dispositivos móveis e trabalho remoto
i. Política para uso de dispositivo móvel
ii. Trabalho Remoto

3. Segurança em Recursos Humanos
a. Antes da Contratação
i. Seleção
ii. Termos e Condições de Contratação;

b. Durante a Contratação
i. Responsabilidades da Direção
ii. Conscientização, educação e treinamento em segurança da informação;
iii. Processo disciplinar;
c. Encerramento e mudança da contratação
i. Responsabilidades pelo encerramento ou mudança da contratação;

4. Gestão de Ativos

a. Responsabilidade pelos ativos (OBJETIVO: Identificar os ativos da organização e definir as devidas responsabilidades pela proteção dos ativos.)
i. Inventário dos ativos (CONTROLE: Convém que os ativos associados à informação e aos recursos de processamento da informação sejam identificados, e um inventário destes ativos seja estruturado e mantido.)
ii. Proprietário dos ativos (CONTROLE: Convém que os ativos mantidos no inventário tenham um proprietário.)
iii. Uso aceitável dos ativos (CONTROLE: Convém que regras para o uso aceitável das informações, dos ativos associados com a informação e dos recursos de processamento da informação sejam identificadas, documentadas e implementadas.)
iv. Devolução dos ativos (CONTROLE: Convém que todos os funcionários e partes externas devolvam todos os ativos da organização que estejam em sua posse, após o encerramento de suas atividades, do contrato ou acordo.)
b. Classificação da Informação (OBJETIVO: Assegurar que a informação receba um nível adequado de proteção, de acordo com a sua importância para a organização.)
i. Classificação da Informação (CONTROLE: Convém que a informação seja classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada.)
ii. Rótulos e tratamento da Informação (CONTROLE: Convém que um conjunto apropriado de procedimento para rotular e tratar a informação seja desenvolvido e implementado de acordo com o esquema de classificação da informação adotada pela organização.)
iii. Tratamento dos Ativos (CONTROLE: Convém que procedimentos para o tratamento dos ativos sejam desenvolvidos e implementados de acordo com o esquema de classificação da informação adotado pela organização.)
c. Tratamento de Mídias (OBJETIVO: Prevenir a divulgação não autorizada, modificação, remoção ou destruição da informação armazenada nas mídias.)
i. Gerenciamento de mídias removíveis (CONTROLE: Convém que existam procedimentos implementados para o gerenciamento de mídias removíveis de acordo com o esquema de classificação adotado pela organização.)
ii. Descarte de mídias (CONTROLE: Convém que as mídias sejam descartadas de forma segura, quando não forem mais necessárias, por meio de procedimentos formais.)
iii. Transferência física de mídias (CONTROLE: Convém que mídias contendo informações sejam protegidas contra acesso não autorizado, uso impróprio ou corrupção, durante o transporte.)

5. Controle de Acesso

a. Requisitos do negócio para controle de acesso
i. Política de controle de acesso
ii. Acesso às redes e aos serviços de rede
b. Gerenciamento de acesso do usuário

i. Registro e cancelamento de usuário
ii. Provisionamento para acesso de usuário
iii. Gerenciamento de direitos de acesso privilegiados
iv. Gerenciamento da informação de autenticação secreta de usuários
v. Análise crítica dos direitos de acesso de usuário
vi. Retirada ou ajuste dos direitos de acesso
c. Responsabilidades dos usuários
i. Uso da informação de autenticação secreta
d. Controle de acesso ao sistema e à aplicação
i. Restrição de acesso à informação
ii. Procedimentos seguros de entrada no sistema (log-on)
iii. Sistema de Gerenciamento de senha
iv. Uso de programas utilitários privilegiados
v. Controle de acesso ao código-fonte de programas

6. Criptografia
a. Controles criptográficos
i. Política para o uso de controles criptográficos
ii. Gerenciamento de chaves

7. Segurança física e do ambiente
a. Áreas Seguras
i. Perímetro de segurança física
ii. Controles de entrada física
iii. Segurança em escritórios, salas e instalações
iv. Proteção contra ameaças externas e do meio ambiente
v. Trabalhando em áreas seguras
vi. Áreas de entrega e de carregamento
b. Equipamento
i. Localização e proteção do equipamento
ii. Utilidades
iii. Segurança do cabeamento
iv. Manutenção dos equipamentos
v. Remoção de ativos
vi. Segurança de equipamentos e ativos fora das dependências da organização
vii. Reutilização ou descarte seguro de equipamentos
viii. Equipamento de usuário sem monitoração
ix. Política de mesa limpa e tela limpa

8. Segurança nas operações
a. Responsabilidades e procedimentos operacionais
i. Documentação dos procedimentos de operação
ii. Gestão de mudanças
iii. Gestão de capacidade
iv. Separação dos ambientes de desenvolvimento, teste e produção
b. Proteção contra malware
i. Controles contra malware

c. Cópias de Segurança
i. Cópias de segurança das informações
d. Registros e monitoramento
i. Registros de eventos
ii. Proteção das informações dos registros de eventos (logs)
iii. Registros de eventos (log) de administrador e operador
iv. Sincronização dos relógios
e. Controle de software operacional
i. Instalação de software nos sistemas operacionais
f. Gestão de vulnerabilidades técnicas
i. Gestão de vulnerabilidades técnicas
ii. Restrições quanto à instalação de software
g. Considerações quanto à auditoria de sistemas da informação
i. Controles de auditoria de sistemas de informação

9. Segurança das comunicações
a. Gerenciamento da segurança em redes
i. Controles de redes
ii. Segurança dos serviços de rede
iii. Segregação de redes
b. Transferência de informação
i. Políticas e procedimentos para transferência de informações
ii. Acordos para transferência de informações
iii. Mensagens eletrônicas
iv. Acordos de confidencialidade e não divulgação

10. Aquisição, Desenvolvimento e Manutenção de Sistemas
a. Requisitos de Segurança de sistemas de informação
i. Análise e especificação dos requisitos de segurança da informação
ii. Serviços de aplicação seguros em redes públicas
iii. Protegendo as transações nos aplicativos de serviços
b. Segurança em processos de desenvolvimento e de suporte
i. Política de desenvolvimento seguro
ii. Procedimentos para controle de mudanças de sistemas
iii. Análise crítica técnica das aplicações após mudanças nas plataformas operacionais
iv. Restrições sobre mudanças em pacotes de software
v. Princípios para projetar sistemas seguros
vi. Ambiente seguro para desenvolvimento
vii. Desenvolvimento terceirizado
viii. Teste de segurança do sistema
ix. Teste de aceitação de sistemas
c. Dados para teste
i. Proteção dos dados para teste

11. Relacionamento na Cadeia de Suprimento
a. Segurança da informação na cadeia de suprimento

i. Política de segurança da informação no relacionamento com os fornecedores
ii. Identificando segurança da informação nos acordos com fornecedores
iii. Cadeia de suprimento na tecnologia da informação e comunicação
b. Gerenciamento da entrega do serviço do fornecedor
i. Monitoramento e análise crítica de serviços com fornecedores
ii. Gerenciamento de mudanças para serviços com fornecedores

12. Gestão de Incidentes de Segurança da Informação

a. Gestão de incidentes de segurança da informação e melhorias
i. Responsabilidades e procedimentos
ii. Notificação de eventos de segurança da informação
iii. Notificando fragilidades de segurança da informação
iv. Avaliação e decisão dos eventos de segurança da informação
v. Resposta aos incidentes de segurança da informação
vi. Aprendendo com os incidentes de segurança da informação
vii. Coleta de evidências

13. Aspectos da Segurança da Informação na Gestão da Continuidade do Negócio

a. Continuidade da Segurança da Informação
i. Planejando a continuidade da segurança da informação
ii. Implementando a continuidade da segurança da informação
iii. Verificação, análise crítica e avaliação da continuidade da segurança da informação
b. Redundâncias
i. Disponibilidade dos recursos de processamento da informação

14. Conformidade

a. Conformidade com requisitos legais e contratuais
i. Identificação da legislação aplicável e de requisitos contratuais
ii. Direitos de propriedade intelectual
iii. Proteção de registros
iv. Proteção e privacidade de informações de identificação pessoal
v. Regulamentação de controles de criptografia
b. Análise crítica da segurança da informação
i. Análise crítica independente da segurança da informação
ii. Conformidade com as políticas e procedimentos de segurança da informação
iii. Análise crítica da conformidade técnica

Então é isso pessoal, vamos ficando por aqui.

Esperamos que tenha gostado do nosso Bizu!

Bons estudos!

Aline Calado

@alinecalado.f

Leonardo Mathias

@profleomathias

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.