DEFINIÇÃO

Conceitos básicos de segurança da informação, tipos de segurança e controle de acesso.

PROPÓSITO

Apresentar os conceitos de segurança da informação e os tipos de segurança, assim como a aplicação deles.

OBJETIVOS

MÓDULO 1

Empregar os conceitos básicos da área de segurança e informação, assim como seu valor, sua propriedade e seu ciclo de vida

MÓDULO 2

Formular segurança física, lógica e controle de acesso

MÓDULO 1

⦿ **Empregar os conceitos básicos da área de segurança e informação, assim como seu valor, sua propriedade e seu ciclo de vida**

DADO E INFORMAÇÃO

As primeiras figuras rupestres datam de mais de 70 mil anos antes de Cristo. Dos manuscritos do Mar Morto até o último livro disponibilizado pela Amazon, a humanidade sempre precisou armazenar seus conhecimentos de alguma forma.

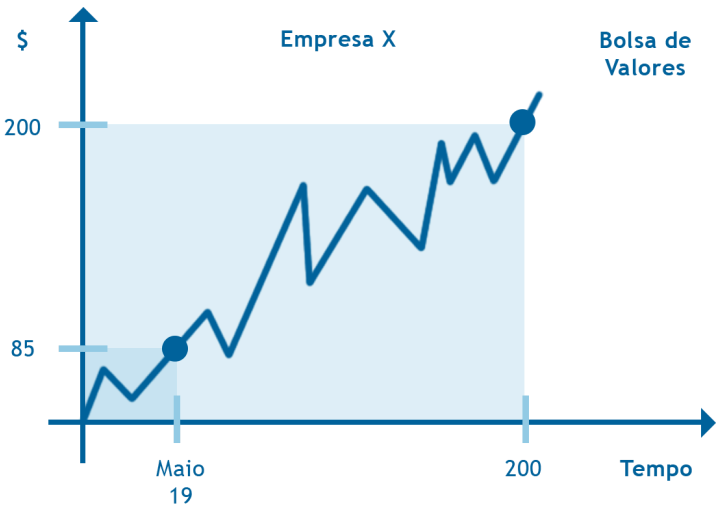
Isso nos remete ao conceito de conhecimento – ou, mais especificamente, de **informação**. Já o conceito fundamental que dá origem à informação é o **dado**.

Mas como podemos defini-lo?

O dado pode ser considerado o valor de determinada medida sem uma contextualização e, portanto, sem valor para ser aplicado ou tratado. No momento em que um dado é contextualizado, ou seja, é atribuído a um contexto ou a uma situação, torna-se uma informação, consequentemente

obtendo valor.

Consideremos, por exemplo, o gráfico de uma empresa na Bolsa de Valores. Na abscissa, ele apresenta o eixo temporal; na ordenada, o valor da ação na Bolsa.



Suponhamos que ela tenha registrado um crescimento durante a pandemia gerada pelo Covid-19. O valor das ações desta empresa praticamente dobrou na Bolsa de Valores.

Analisemos agora estas duas situações:

SITUAÇÃO 1

Em meados de maio de 2019, o valor da ação girava em torno de US$85; um ano depois, ele já era aproximadamente de US$200. Isso significa um aumento de mais de 100%.

SITUAÇÃO 2

Coloquemos agora tais valores em determinado contexto: suponhamos que, em meados de dezembro de 2019, fossemos informados dos dois valores dessa ação registrados nos meses de maio de 2019 e 2020.

Normalmente, uma situação do tipo não ocorre. Afinal, é muito difícil existir uma valorização tão grande em um curto espaço de tempo.

Na **situação 1**, os valores US$85 e US$200 são dados – e não contextualizados. Portanto, não é possível auferir ganhos financeiros ou elaborar uma percepção monetária a respeito deles. Mesmo que o maior *expert* em investimentos da Bolsa de Valores tivesse ciência de ambos, ele nada poderia fazer para lucrar com tais dados.

Na **situação 2**, esses valores são dados contextualizados; por isso, conhecê-los configuraria uma informação passível de se auferir ganhos monetários.

OBSERVANDO O EXEMPLO APRESENTADO, COMO PODEMOS DEFINIR UMA INFORMAÇÃO?

RESPOSTA

RESPOSTA

Ela pode ser definida como um dado contextualizado no qual existe uma percepção de valor. Dessa forma, é necessário haver uma atenção quanto à sua preservação.

CICLO DE VIDA DA INFORMAÇÃO

Por se tratar de um dado contextualizado, a informação possui o seguinte ciclo de vida:

CRIAÇÃO

TRANSPORTE

MANUSEIO

DESCARTE

Após a primeira etapa (criação), o dado pode ser transportado ou manuseado. Esta figura representa o transporte antes do manuseio por tal procedimento ser o mais comum nesses casos, porém é perfeitamente possível que ele seja manuseado anteriormente. Na etapa final, a informação é descartada.

Durante todas essas etapas, a informação deve ser protegida. Seu vazamento em quaisquer etapas pode provocar problemas em vários aspectos.

Vamos analisar alguns exemplos disso:

1º

Transporte inadequado de dados por uma transportadora que não realiza todos os procedimentos de segurança necessários.

Um *laptop* é levado para a manutenção sem que os dados do disco rígido dele sejam protegidos. Não é raro haver casos de roubos de unidades que possuíam informações sensíveis de empresas.

Fonte: (FREIRE, 2008)

2º

3º

Um analista de dados tem um *laptop* e um disco rígido externo roubados em sua residência com informações não criptografadas de 26,5 milhões veteranos do exército americano. O analista informou que **rotineiramente** levava os dados para a sua residência. Neste caso, o problema ocorreu no manuseio da informação.

Fonte: (GUSMÃO, 2014)

Empresa forense de Nova Iorque, a Kessler International realizou o seguinte estudo: durante seis meses, ela foi adquirindo discos rígidos usados no portal eBay. Cerca de 40% deles continham informações de seus usuários.

Fonte: (MEARIAN, 2009)

4º

5º

Exemplos simples e clássicos como os apresentados acima não correspondem apenas a empresas que não sejam de tecnologia da informação (TI). Até mesmo o Facebook, uma das companhias mais novas do mercado de tecnologia e com um altíssimo valor agregado, sendo usado por milhões de pessoas no mundo, teve um disco rígido furtado de um veículo. Ele continha informações de aproximadamente 29.000 empregados norte-americanos.

Fonte: (BE COMPLIANCE, 2019)

Que conclusão podemos tirar dos casos apresentados?

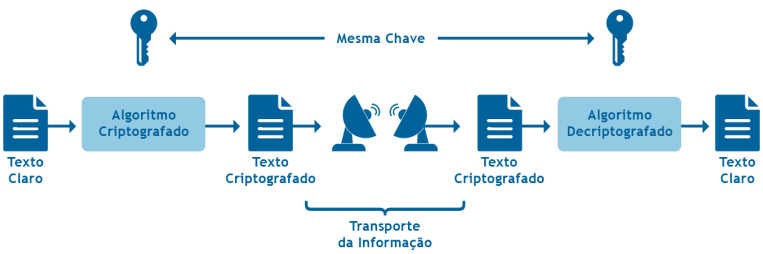
A informação, que é o dado contextualizado, precisa de proteção em todo o seu ciclo de vida. A partir dos exemplos citados, conseguimos entender a necessidade de **sempre** estabelecer uma proteção adequada dela em qualquer etapa do seu ciclo de vida.

No caso do transporte de mídias magnéticas contendo informações sigilosas de usuários de determinada empresa, por exemplo, uma boa proteção é o emprego da **criptografia**. Esta chave é usada para embaralhar (criptografar) e desembaralhar (decriptografar) as informações.

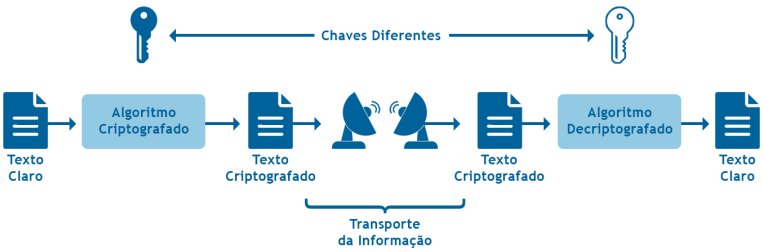
Quando a mesma chave é usada nas duas etapas, a criptografia é dita **simétrica**; quando são usadas chaves distintas, ela é **assimétrica**. Vejamos seus dois tipos nas figuras a seguir:

CRIPTOGRAFIA

Ela pode ser definida como o embaralhamento das informações por meio de uma sequência de dados que utiliza uma chave e um algoritmo.



CRIPTOGRAFIA SIMÉTRICA.



CRIPTOGRAFIA ASSIMÉTRICA.

Como você manuseia seu *pen drive*?

Hoje em dia, por estarmos na era da informação, é comum sempre levarmos um desses dispositivos no bolso, mochila ou na carteira.

Afinal, como você cuida das suas informações?

Certamente, seu *pen drive* contém alguns arquivos nos quais você ainda deve estar trabalhando. Ele pode servir para várias pessoas e diferentes tipos de trabalho:

Se você é um programador, pode estar mexendo em alguma parte de um sistema que está desenvolvendo;

Se você trabalha na direção, pode estar atualizando alguma planilha com os dados financeiros da sua empresa.

Uma prática simples – mas eficiente – nestes casos é simplesmente compactar os seus arquivos usando uma senha.

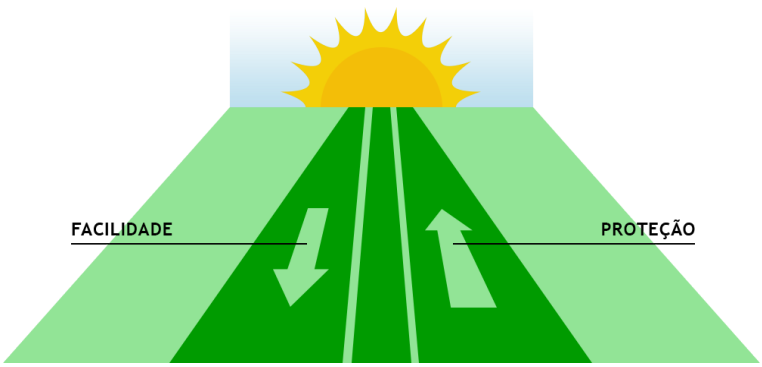
ARQUIVOS NO *PEN DRIVE* SEM SENHA.

ARQUIVO COMPACTADO CONTENDO TODOS OS ARQUIVOS COM SENHA.

Praticamente todas as ferramentas (até mesmo as gratuitas) possuem essa funcionalidade. Cada uma conta com uma metodologia para acrescer a senha ao processo de compactação. Um bom exemplo disso é a ferramenta 7-zip.

Essas ferramentas utilizam os melhores algoritmos de criptografia existentes no mercado. Além de economizar o espaço do *pen drive*, essa simples prática cria ainda uma camada de proteção para as informações contidas no dispositivo.

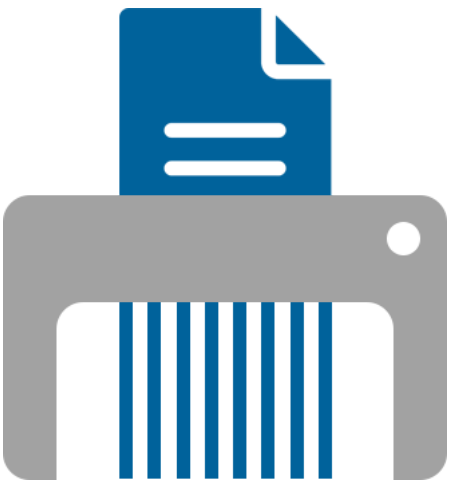
Devemos observar que a **proteção** e a **facilidade** caminham em direções contrárias. Por isso, o processo de compactar com senha gera um aumento de tempo no manuseio da informação, pois ele sempre torna necessária a tarefa de descompactar e compactar para tratar a informação.



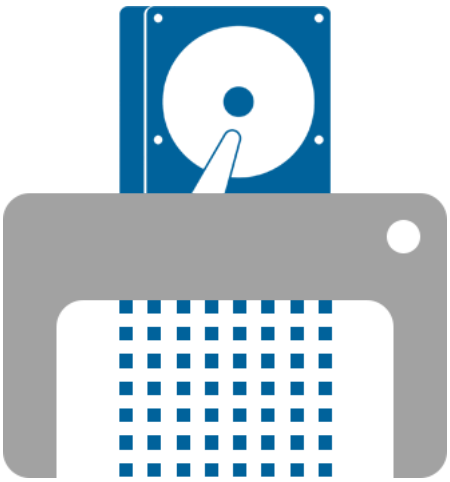
A proteção e a facilidade sempre caminham em sentidos opostos.

Dessa forma, seu descarte deve ser realizado de forma padronizada, já que o propósito é evitar a recuperação de suas informações. Exemplo: *pen drives*, discos rígidos e outras mídias usadas precisam ser descartadas com o uso de trituradores adequados.

Nas figuras a seguir, exibiremos dois tipos de trituradores:



TRITURADOR DE PAPEL.



TRITURADOR DE DISCO RÍGIDO.

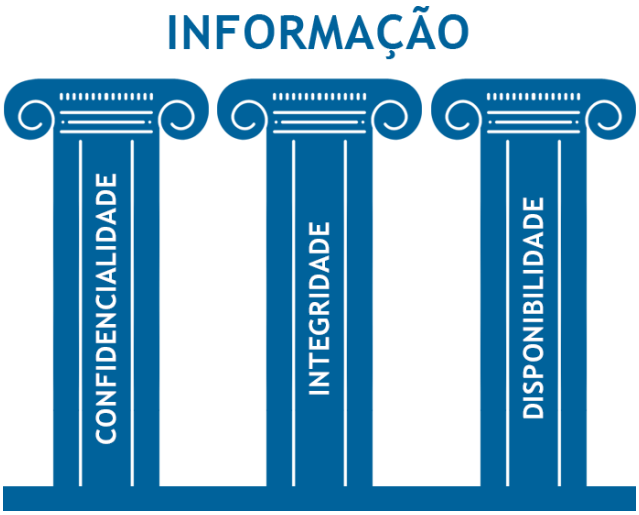
ASPECTOS DA SEGURANÇA DA INFORMAÇÃO

Dos aspectos da informação, seus três principais requerem cuidados especiais:

Confidencialidade;

Integridade;

Disponibilidade.



Principais pilares da informação: confidencialidade, integridade e disponibilidade.

Confidencialidade

Capacidade do acesso à informação apenas por quem possui autorização.

Integridade

Possibilidade de alteração da informação por pessoas ou sistemas autorizados.

Disponibilidade

Faculdade de a informação poder ser acessada, em qualquer tempo, por pessoas ou sistemas autorizados para tal.

Citados por diversos autores como pilares, estes três aspectos, conforme indica a imagem acima, correspondem à prioridade do que deve ser protegido em relação à informação. Todos os exemplos citados correspondem, portanto, à confidencialidade da informação em três momentos diferentes do seu ciclo de vida.

Portanto, a **segurança da informação** pode ser definida como as atividades, os procedimentos e as metodologias que objetivam a proteção da informação, principalmente no que tange à confidencialidade, à integridade e à disponibilidade (CID).

Os seguintes aspectos, contudo, também são considerados importantes:

AUTENTICIDADE

Assegura que a informação foi gerada por pessoa ou sistema autorizado para isso.

LEGALIDADE

Trata-se do alinhamento da informação e/ou dos processos com normas, portarias, leis e quaisquer outros documentos normativos, cada um na sua respectiva esfera de atribuição e abrangência.

NÃO REPÚDIO

Também conhecido como **irretratabilidade**, ele está relacionado ao fato de o emissor negar a autoria de uma informação divulgada.

Juntos, todos eles compõem os principais aspectos empregados pelos controles – ou pelas ferramentas que proporcionam a segurança da informação – para proteger a informação.

Resumo dos aspectos da segurança:

D	V	F	T	Y	H	E	A	C	V	D	A	D	E	A	Z	C	U	I	O	K
A	D	E	D	A	D	D	A	D	E	D	A	D	E	D	A	**D**	D	A	D	E
E	R	E	D	V	F	T	Y	H	E	A	C	V	D	A	D	**I**	A	C	V	D
D	A	D	A	D	E	D	A	D	D	A	D	E	D	A	D	**S**	D	A	D	V
A	C	V	A	A	A	C	V	S	A	C	V	D	D	A	D	**P**	D	V	F	D
S	V	F	T	Y	H	E	A	C	V	D	A	D	D	V	F	**O**	V	D	V	D
P	D	E	D	A	D	D	A	D	E	D	A	D	A	D	E	**N**	D	F	D	A
O	S	E	D	V	A	T	Y	H	E	A	C	V	D	A	D	**I**	F	A	F	A
N	P	D	A	A	V	D	A	D	D	A	D	E	D	A	D	**B**	A	E	A	V
R	O	S	A	V	D	**I**	**R**	**R**	**E**	**T**	**R**	**A**	**T**	**A**	**B**	**I**	**L**	**I**	**D**	**A**

A	N	P	V	D	A	F	T	Y	H	F	T	Y	H	A	S	**L**	F	T	Y	H
D	R	O	D	A	Y	E	D	A	D	E	D	A	D	Z	C	**I**	E	D	A	D
C	A	N	A	Y	A	F	T	Y	H	A	**C**	**O**	**N**	**F**	**I**	**D**	**E**	**N**	**C**	**I**
D	D	R	Y	A	V	E	D	A	D	S	F	G	H	J	K	**A**	Q	W	E	R
A	D	A	A	V	D	A	**A**	**U**	**T**	**E**	**N**	**T**	**I**	**C**	**I**	**D**	**A**	**D**	**E**	D
A	C	D	V	D	T	Y	H	F	T	Y	H	E	A	A	A	**E**	F	T	Y	D
A	D	D	D	F	T	Y	H	F	T	Y	H	E	A	C	V	D	E	D	A	E
V	D	C	P	E	D	A	D	E	D	A	D	D	A	D	E	D	A	D	Q	D
E	D	D	O	A	A	C	V	A	A	A	C	V	D	A	D	E	D	A	D	C
C	V	A	N	F	T	Y	H	V	F	T	Y	H	E	A	C	V	D	A	D	D
D	E	A	D	E	D	A	D	D	E	D	A	D	D	A	D	E	D	A	D	A
E	D	D	O	A	A	B	D	E	D	D	O	A	A	C	V	A	A	A	C	V
C	V	A	N	F	T	A	A	C	V	A	N	F	T	Y	H	V	F	T	Y	H
D	E	A	D	E	D	Q	A	D	E	A	D	E	D	A	D	D	E	D	A	D

Atenção! Para visualizaçãocompleta da tabela utilize a rolagem horizontal

DISPONIBILIDADE

Capacidade de a informação poder ser acessada, em qualquer tempo, por pessoas ou sistemas autorizados para tal.

IRRETRATABILIDADE

Está relacionada ao emissor negar a autoria de uma informação divulgada.

CONFIDENCIALIDADE

Capacidade do acesso à informação apenas por quem possui autorização.

AUTENTICIDADE

Assegura que a informação foi gerada por pessoa ou sistema autorizado para isso.

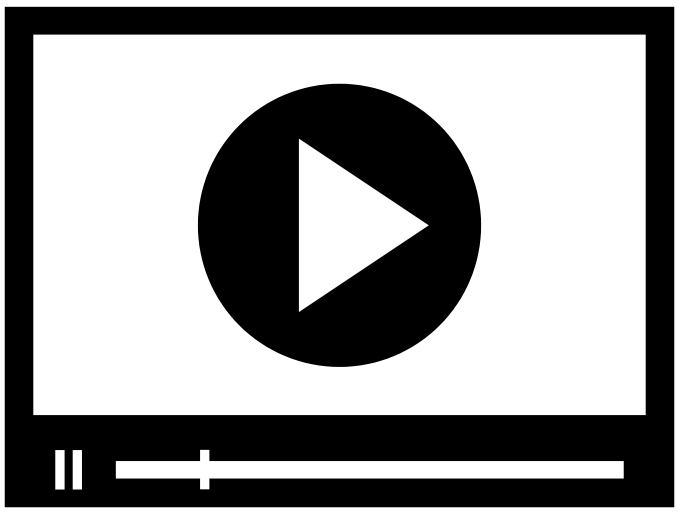
INTEGRIDADE

Possibilidade de alteração da informação por pessoas ou sistemas autorizados.

LEGALIDADE

Alinhamento da informação ou dos processos com normas, portarias, leis e quaisquer outros documentos normativos.

Palavras cruzadas dos aspectos da segurança.



Neste vídeo, empregaremos os conceitos básicos da área de segurança e informação, citando seu valor, propriedade e ciclo de vida.

MÃO NA MASSA

TEORIA NA PRÁTICA

Todas as profissões possuem suas características. Nós, que somos de TIC, precisaremos, uma hora ou outra, interagir com elas e assegurar que tais características sejam cumpridas.

Uma das mais antigas profissões do mundo é a do médico. Aqueles que já fizeram o juramento de Hipócrates e sabem quão árdua esta profissão é estão cientes de que um de seus fundamentos é o sigilo entre médico e paciente.

Esse sigilo aparece transcrito no CFM 1605/2000 em adição ao Código de Processo Penal (1941, art. 207), que dispõe o seguinte: “São proibidas de depor as pessoas que, em razão de função, ministério, ofício ou profissão, devam guardar segredo, salvo se, desobrigadas pela parte interessada, quiserem dar o seu testemunho”. Isso reforça ainda mais a necessidade de proteção desses dados não apenas quanto à confidencialidade deles, mas também em relação à sua integridade.

No tocante à confidencialidade, como os administradores de banco de dados devem fazer para gerenciá-los, uma vez que eles podem manusear quaisquer dados armazenados em um SGBD?

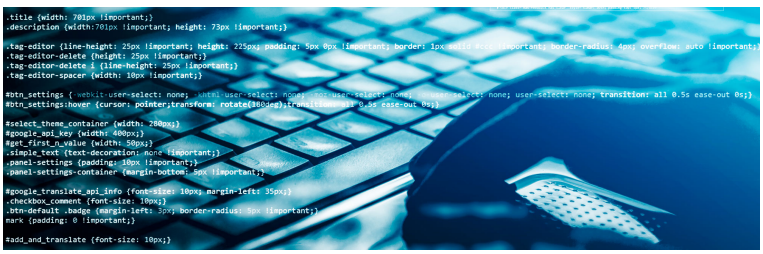
RESPOSTA

A resposta padrão a este questionamento cada vez mais comum é o uso de criptografia na base de dados sem que a chave (simétrica, pública ou privada) esteja em *hard code*, tampouco armazenada no BD ou no arquivo de computador.

VERIFICANDO O APRENDIZADO

MÓDULO 2

Formular segurança física, lógica e controle de acesso



SEGURANÇA FÍSICA

No módulo anterior, vimos o exemplo de roubo de dados no seu transporte. Mesmo que eles estivessem criptografados, a ação poderia ocorrer da mesma forma, pois ela foi uma consequência de vulnerabilidades na segurança física das mídias em questão.

Aspecto integridade

A informação foi totalmente impactada, pois a mídia poderia ser destruída.

Aspecto confidencialidade

Dependeria, por exemplo, da informação armazenada ter ou não algum controle de proteção, como, por exemplo, a criptografia.

A família de normas ABNT ISO/IEC 27.000 divide a segurança física em dois aspectos: um é relacionado aos equipamentos e outro, ao ambiente.

A segurança da informação age dessa forma. Ela é entendida como camadas justapostas que permitem à informação ficar cada vez mais protegida, como, por exemplo, uma cebola e suas camadas.

Quanto ao ambiente, em uma instalação empresarial, por exemplo, é possível observar as camadas de segurança físicas e, a partir daí, estabelecer um paralelo com a imagem da cebola.

📷 Nossa informação deve receber camadas de proteção como se fosse uma cebola.

Ao nos aproximarmos de uma instalação, alcançamos a cancela para automóveis, que, normalmente, conta com dois seguranças. Sua função é solicitar alguma identificação ou verificar se o veículo possui algum selo de identificação.

Normalmente, esse selo é único para aquela instituição. Em alguns casos, essa verificação pode ser feita de forma automatizada com alguma tecnologia de emissão de sinal de baixa frequência, como o RFID.

Após a ultrapassagem dessa primeira barreira (camada mais externa à nossa cebola de segurança), geralmente existe mais uma etapa: catraca e elevador. Ela está vinculada a algum controle biométrico ou de crachá. O RFID novamente surge como um exemplo.

Físicos, esses controles são justapostos, permitindo que a vulnerabilidade de um deles possa ser recoberta por outro controle. Isso funciona de forma similar nas salas de servidores, *data centers* e salas-cofres, criando camadas de segurança que dificultam o acesso físico ao servidor.

Outro aspecto que deve ser levado em consideração é a proteção contra ameaças da natureza, como enchentes, incêndios e outras calamidades provocadas pela natureza e/ou pelo homem.

Tendo isso em vista, certos controles de monitoramento e prevenção devem ser instalados e controlados.

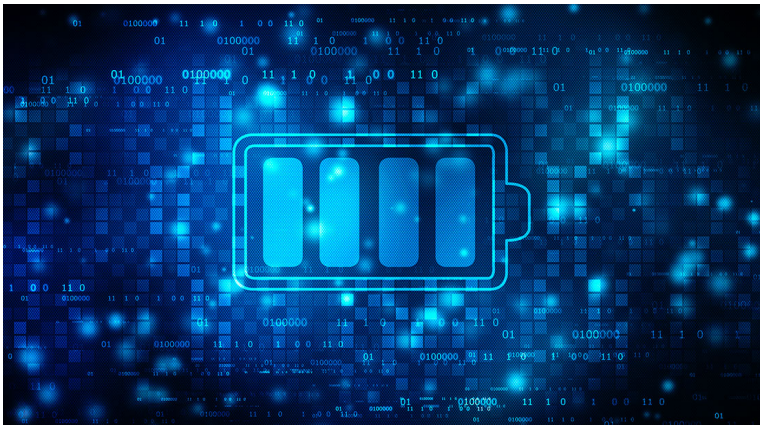
★ EXEMPLO

Câmeras de segurança, controles de temperatura, extintores de incêndio e *sprinkles* (algumas vezes traduzidos como chuveiros automáticos).

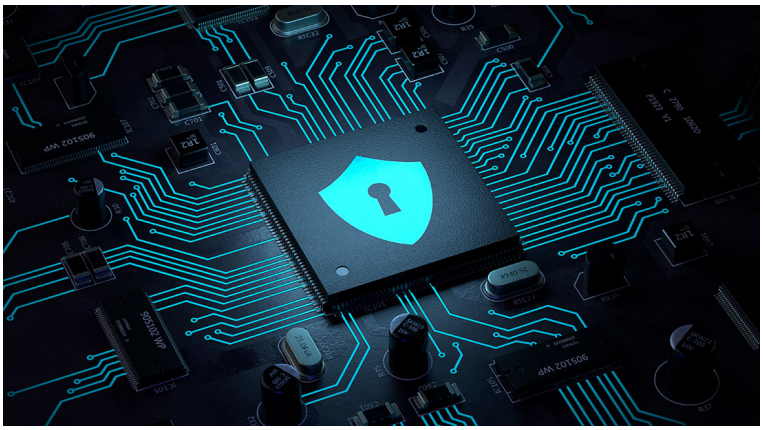
O cabeamento e o acesso à rede externa (internet), bem como ao fornecimento de energia, são fatores fundamentais nesse processo. Como eles dependem de um fornecimento feito por terceiros, certos aspectos contratuais e de redundância precisam ser estabelecidos.

Além disso, políticas e instruções normativas devem ser instituídas, treinadas e simuladas visando à prontidão. Nesse sentido, é razoável haver uma redundância no fornecimento de rede (internet), bem como uma independência física desse fornecimento no que tange ao tipo de conexão estipulada.

É necessário evitar o uso compartilhado de conexões entre fornecedores distintos. Desse modo, se, para um fornecedor, a conexão é feita por meio de fibra ótica, para o outro ela poderia ser realizada por intermédio de link rádio.



Sobre a parte de energia elétrica, o uso de bancos de bateria (e/ou no-breaks) e de geradores revela ser algo fundamental na maioria dos casos. Quanto aos geradores, deve-se levar em consideração o fornecimento de insumos necessários e periódicos, como o combustível.



Em relação aos equipamentos, a ideia de segurança tem relação com o acesso físico aos componentes de *hardware* e aos dispositivos de entrada. Devem ser adotadas medidas como senha na BIOS e configuração de botões físicos e de ordem de execução na inicialização dos computadores.

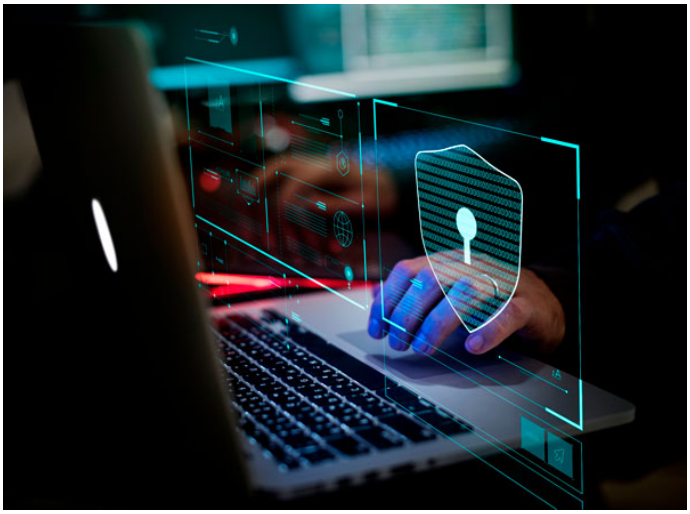
Os maiores computadores do mundo são organizados em uma lista conhecida como Top 500 (top500.org). Pelo custo e poder computacional deles, esses equipamentos requerem uma série de recursos de proteção.

Maior recurso computacional do Brasil, o supercomputador Santos Dumont consta na referida lista. Para prover os recursos necessários de segurança, uma série de medidas foi tomada e, em seguida, publicada no Youtube.

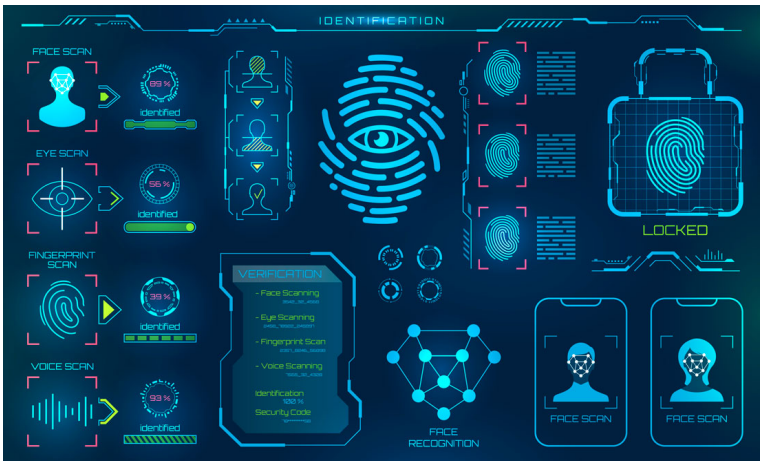
SEGURANÇA LÓGICA

Em adição às medidas de segurança física, há as de segurança lógica, que correspondem às medidas baseadas em *software*. Dessa lista, podemos destacar as senhas, as listas de controle de acesso, a criptografia, e o *firewall*.

Repetindo o padrão apresentado anteriormente, esses mecanismos estão justapostos; com isso, a demanda de uma camada pode criar uma adicional a outra que possua alguma vulnerabilidade particular.



Como exemplo disso, existem no próprio equipamento controles de acessos biométricos, como a leitura de digital e o reconhecimento facial. Esses sistemas de controle biométricos são caracterizados pela captura da geometria humana, a qual, em grande parte, difere em cada pessoa.



Atualmente, os leitores de digitais têm dado espaço para o reconhecimento facial pela disseminação dos sensores e da tecnologia empregada. Há diversas APIs disponibilizadas para uso gratuito e comercial, como a do Amazon Rekognition. Esses controles atuam na proteção da confidencialidade da informação.

A criptografia corresponde ao conjunto de técnicas que permite o embaralhamento de dados por intermédio do uso de chaves e de algoritmos computacionais baseados em funções matemáticas. Essas funções propiciam, em linhas gerais, a presença de duas grandes classes de algoritmos: os **simétricos** e os **assimétricos**.

CRIPTOGRAFIA SIMÉTRICA

Utiliza funções matemáticas mais simples e uma única chave para criptografar e decriptografar. Esta classe de algoritmos é composta por, entre outros exemplos, Cifra de César, Blowfish, Twofish e Rijnadel. Graças a esse controle, é possível assegurar a confidencialidade da informação.

Algoritmo	Tamanho da chave
AES (Rijnadel)	128, 192 e 256 bits
Twofish	128, 192 e 256 bits

Serpent	128, 192 e 256 bits
Blowfish	32 a 448-bits
RC4	40-128 bits
3DES (baseado no DES)	168 bits
IDEA	128 bits

Atenção! Para visualizaçãocompleta da tabela utilize a rolagem horizontal

CRIPTOGRAFIA ASSIMÉTRICA

Caracteriza-se por algoritmos que normalmente envolvem técnicas matemáticas mais sofisticadas, como a fatoração de números grandes e o logaritmo discreto.

Esta família emprega duas chaves: uma é utilizada para cifrar; a outra, para decifrar. Essas chaves são conhecidas como:

Pública

Normalmente, ela fica disponibilizada em um servidor de confiança.

Privada

Ela está sob a posse do usuário.

Com a combinação dessas duas chaves, é possível assegurar não somente a confidencialidade, mas também o não repúdio ou irretratabilidade. Afinal, pode-se combinar o uso desse controle tanto com a chave privada do emissor (não repúdio) quanto com a pública do destinatário (confidencialidade).

Diffie-Hellman, El Gamal e Curvas Elípticas são alguns dos algoritmos desta família. Quanto aos controles aplicados às redes, destacam-se os ***firewalls***, os sistemas detectores de intrusão e os VPNs.

Esses controles permitem a criação de zonas de segurança dentro e fora da instituição. Tais zonas, por sua vez, possibilitam a criação de segregações de funcionalidades.

Das zonas de segurança, a mais comumente encontrada é a DMZ. Zona desmilitarizada, ela limita, conforme demonstra a figura a seguir, a região onde os servidores *web* e de aplicação podem ficar.

FIREWALLS

Equipamentos que filtram o tráfego de rede relacionado à troca de dados entre clientes e servidores.

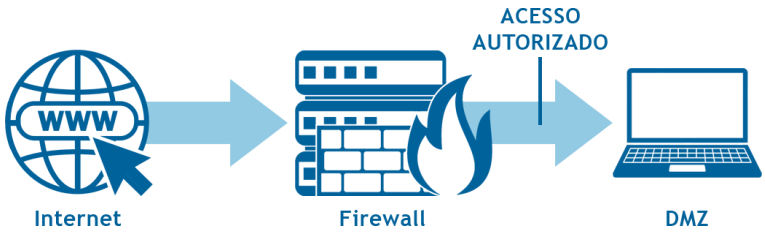


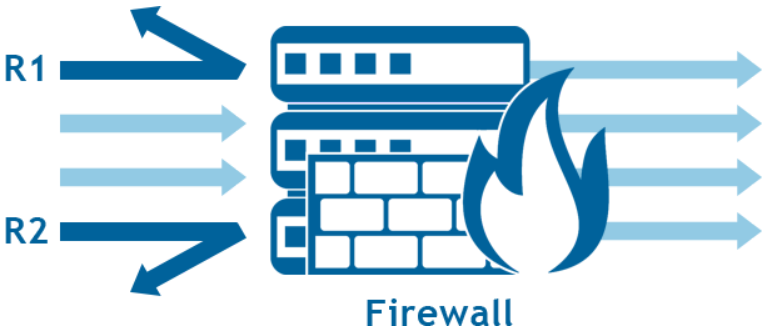
Diagrama simplificado de uma DMZ.

As regras dos *firewalls* podem seguir duas políticas:

NEGAR POR PADRÃO

Todo o tráfego é negado. Apenas os servidores e os protocolos são autorizados.

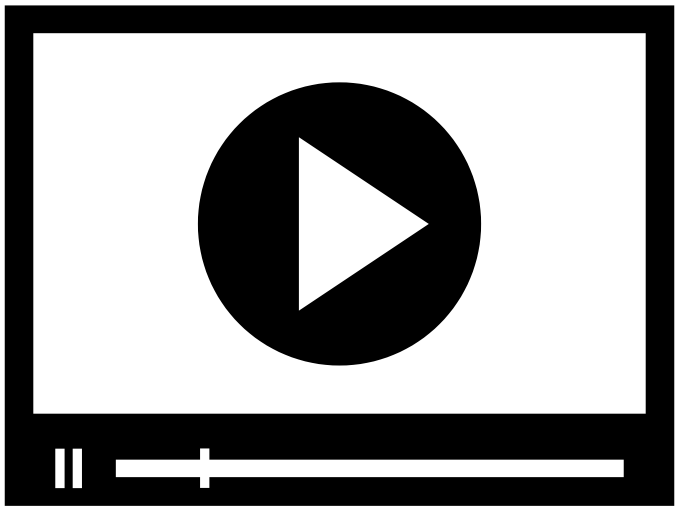
Trata-se da política normalmente encontrada e recomendada no mercado. Como todos os tráfegos são negados, apenas podem trafegar aqueles cujas regras (R1) são aceitas.



ACEITAR POR PADRÃO

Nesta política, todo o tráfego é autorizado, embora o destinado para determinados servidores seja negado.

Qualquer tráfego é aceito por padrão. Regras específicas (R1 e R2) definem quais serão negados.



Neste vídeo, conceituaremos a segurança física e a lógica, além do controle de acesso.

MÃO NA MASSA

VERIFICANDO O APRENDIZADO

CONCLUSÃO

CONSIDERAÇÕES FINAIS

Neste tema, elencamos os conceitos básicos da área de segurança e informação, citando seu valor, sua propriedade e seu ciclo de vida, além dos conceitos de segurança física, lógica e controle de acesso.

No módulo 1, abordamos o ciclo de vida e os problemas relacionados em cada etapa. Em seguida, apresentamos os principais mecanismos de segurança, como a criptografia, além destes pilares de segurança: confidencialidade, integridade e disponibilidade.

No módulo seguinte, falamos sobre a segurança física, que se relaciona com o acesso físico às instalações, e a lógica, que está ligada aos algoritmos. Também verificamos conceitos importantes, como o do *firewall* e das zonas delimitadas por ele.

PODCAST

⚠ PODCAST

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Norma ABNT ISO/IEC 27.0002/2013** – boas práticas para gestão em segurança da informação. Código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2005.

BARRETO, J. dos S.; ZANIN, A.; MORAIS, I. S. de; VETTORAZZO, A. de S. **Fundamentos de segurança da informação**. São Paulo: Sagah, 2018.

BE COMPLIANCE. **Ladrão rouba HDs com dados de 29 mil funcionários do Facebook**. Publicado em: 19 dez. 2019.

BRASIL. **Decreto-lei nº 3.689, de 3 de outubro de 1941**. Código de Processo Penal.

FREIRE, A. **Notebooks furtados da Petrobras estavam na Bacia de Santos, diz PF**. *In*: G1. Publicado em: 5 fev. 2008.

GUSMÃO, G. **Os 15 maiores vazamentos de dados da década**. *In*: Exame. Publicado em: 21 fev. 2014.

MEARIAN, L. **Survey**: 40% of hard drives bought on eBay hold personal, corporate data. *In*: Computerworld. Publicado em: 10 fev. 2009.

RODRIGUES, F. N. **Segurança da informação** – princípios e controles de ameaças. São Paulo: Érica, 2019.

EXPLORE+

Pesquise em canais do Youtube vídeos sobre:

IBM Cloud e Amazon Web Services: A nuvem ou *cloud computing* é um processo que vem mostrando muita força;

Supercomputador Santos Dumont: Como frisamos, ele é o maior recurso computacional do país. Conhecê-lo é uma ótima forma de analisar as medidas de segurança.

CONTEUDISTA

Anderson Fernandes Pereira dos Santos

🔗 CURRÍCULO LATTES