



CÓD: OP-133JN-23
7908403547869

ITABERABA-BA

PREFEITURA MUNICIPAL DE ITABERABA - BAHIA

Fiscal Administrativo

EDITAL Nº 001/2024

Língua Portuguesa

1. Leitura e interpretação de textos (ficcionais e/ou não ficcionais)	5
2. Gêneros discursivos e tipologia textual	5
3. Ortografia.....	6
4. acentuação.....	7
5. pontuação.....	7
6. Formação de palavras	11
7. Léxico: adequação no emprego das palavras.....	12
8. Verbos: conjugação, emprego dos tempos, modos e vozes verbais; as palavras de relação	12
9. morfossintaxe; estrutura do período, da oração e da frase.....	15
10. regência nominal e verbal.....	22
11. colocação pronominal.....	23
12. formas de tratamento (usos e adequações)	23
13. Noções de fonética; Noções de prosódia.....	26
14. Estrutura do parágrafo.....	27
15. Coesão e coerência textuais	28
16. Estilística: denotação e conotação; Semântica: sinonímia, antonímia, homonímia, paronímia, polissemia e figuras de linguagem.	29
17. figuras de linguagem.....	29
18. Níveis de linguagem.....	32
19. Manual de Redação da Presidência da República (3ª edição, revista, atualizada e ampliada).....	33

Matemática

1. Conjuntos; Problemas e Sistemas	53
2. Teoria dos Conjuntos	62
3. Progressão Geométrica e Aritmética	65
4. Razão; Proporção	69
5. Regra de Três.....	70
6. Porcentagem	72
7. Equações e Inequações do 1º e 2º grau.....	73
8. Sistemas de equações.....	76
9. Funções do 1º e 2º grau.....	78
10. Trigonometria	90
11. Logaritmo.....	97
12. Probabilidade.....	97
13. Análise Combinatória; Permutação	99
14. Geometria Plana, Espacial e Analítica.....	102
15. Matrizes e Determinantes	112

Conhecimentos Gerais

1. Temas relevantes e atuais de diversas áreas: Segurança, Política, Economia, Educação, Saúde, Cultura, Tecnologia e Desenvolvimento sustentável.....	123
2. Princípios Constitucionais da Administração Pública (Constituição Federal: art. 37 a 40)	123
3. Poderes administrativos. Poder de polícia e abuso de poder	128
4. Princípios norteadores dos Serviços Públicos	135
5. Princípios do Processo Administrativo.....	147
6. Atos administrativos: requisitos, vícios, revogação e anulação	156
7. Lei da improbidade administrativa (Lei nº 8.429, de 2 de junho de 1992 e alterações posteriores).....	167
8. Crimes contra Administração pública	182
9. Lei Orgânica do Município de Itaberaba e alterações posteriores.....	192

Conhecimentos Específicos

Fiscal Administrativo

1. Conceitos básicos de dados, informação, conhecimento, sistemas de informação	229
2. Conceitos básicos de informática, os componentes funcionais de computadores (hardware e software), periféricos e dispositivos de entrada, saída e armazenamento de dados.....	230
3. Conceitos e funções de aplicativos de editores de texto, planilhas eletrônicas, apresentações	233
4. gerenciadores de banco de dados	238
5. Conceitos de organização e de Gerenciamento de arquivos e pastas	246
6. Conceitos básicos de segurança da informação, sistemas antivírus	249
7. sistemas de backup.....	253
8. criptografia, assinatura digital e autenticação	254
9. Intranet e internet: conceitos básicos e utilização de tecnologias, ferramentas e aplicativos associados à internet: navegação	254
10. correio eletrônico	258
11. busca e pesquisa.....	262
12. Conceitos básicos de rede, componentes, topologias, estação e servidor, LAN e WAN.....	263

- **Visão:** nível de abstração mais alto (considerada a visão do grupo de usuários) descreve apenas parte do banco de dados, muitos usuários não precisam de todas as informações sobre o banco de dados.
- **Nível Lógico (Visão Conceitual):** nível de abstração intermediário, descreve quais dados estão armazenados e que relação existe entre eles (descreve o bando de dados inteiro).
- **Nível Físico (Visão Interna):** nível de abstração mais baixo, visão do responsável pela manutenção e desenvolvimento do SGBD. Neste nível existe a preocupação de como os dados serão armazenados.

Banco de dados

Analisando como um conceito geral de banco de dados, podemos dizer que uma planilha do Microsoft Excel ou uma lista de contatos (nome, telefone e e-mail) de uma agenda configuram um banco de dados, ou seja, toda organização e armazenagem de informações sobre um mesmo assunto ou assuntos relacionados entre si é um banco de dados¹⁵.

Um banco de dados é uma coleção de dados relacionados¹⁶. Entende-se por dado, toda a informação que pode ser armazenada e que apresenta algum significado dentro do contexto ao qual ele se aplica. Por exemplo, em um sistema bancário, uma pessoa é identificada pelo seu CPF (cliente). Em um sistema escolar a pessoa é identificada pelo seu número de matrícula (aluno). Em um sistema médico a pessoa (paciente) é identificada pelo número do plano de saúde ou cartão SUS.

Um banco de dados informatizado é usualmente mantido e acessado por meio de um software conhecido como Sistema Gerenciador de Banco de Dados (SGBD), que é muitas vezes o termo banco de dados é usado como sinônimo de SGBD.

Um SGBD é uma coleção de programas que permitem ao usuário definir, construir e manipular Bases de Dados para as mais diversas finalidades.



Exemplos de SGBDs.

Modelagem de dados

A modelagem de dados é a criação de uma estrutura de dados eletrônica (banco de dados) que representa um conjunto de informações. Esta estrutura permite ao usuário recuperar dados de forma rápida e eficiente. O objetivo é incluir dados em uma estrutura que possibilite transformar os dados originais em vários tipos de saídas como formulários, relatórios, etiquetas ou gráficos.

Entretanto, para que possamos implementar, de forma correta, um BD utilizando algum SGBD, temos que passar por uma fase intermediária, chamada modelagem de dados. Observe o exemplo:

CLIENTES		
CÓDIGO	NOME	DATA DE NASCIMENTO
1	Regilan Meira Silva	13/02/1983
2	Aline Araujo Freitas	27/08/1986
3	Joaquim José Pereira da Silva	12/05/1967
4	Maria Aparecida Gomes da Costa	06/01/1995

TELEFONES		
CÓDIGO	NUMERO	TIPO
1	(73)9158-9683	Celular
2	(71)3458-5112	Residencial
3	(73)8874-9681	Celular
4	(77)8841-2563	Celular

¹⁵ <https://centraldefavoritos.com.br/2017/12/27/banco-de-dados/>

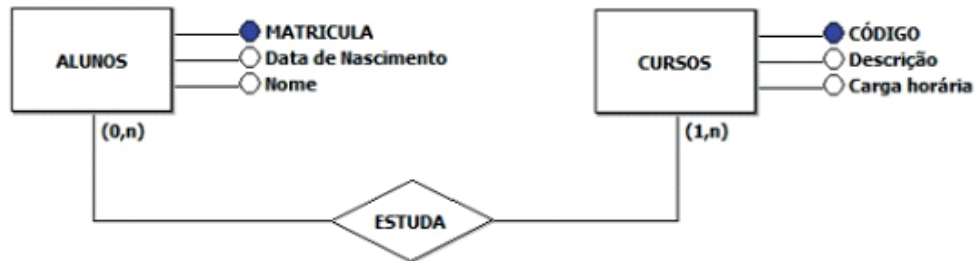
¹⁶ <http://www.regilan.com.br/wp-content/uploads/2013/10/Apostila-Banco-de-Dados.pdf>

Certos conceitos são utilizados na modelagem conceitual para descrever os papéis de cada componente do domínio analisado. Dentre eles, podemos citar:

- **Instância:** denomina uma ocorrência, um registro que existe ou passou a existir de uma entidade;
- **Entidade:** define qualquer coisa que seja identificável, singular e tenha existência bem delimitada, podendo ser classificada entre “fraca” e “forte” de acordo com sua cardinalidade e representada por um retângulo no DER;

Entidade pode ser entendida como uma “coisa” ou algo da realidade modelada onde deseja-se manter informações no banco de dados (BD).

Por exemplo, em um sistema escolar, algumas entidades podem ser os alunos, professores, horário, disciplinas e avaliações. Note que uma entidade pode representar tanto objetos concretos (alunos), quanto objetos abstratos (horário). A entidade é representada por um retângulo. Uma entidade se transformará em uma tabela no modelo físico de banco de dados.



DER Alunos x Curso.

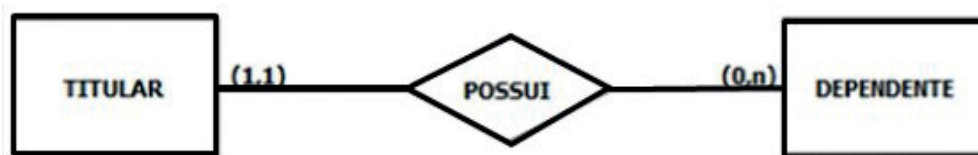
A entidade ALUNO representa todos os estudantes sobre as quais se deseja manter informações no BD. Relacionamento é um conjunto de associações entre entidades. O relacionamento é representado por um LOSANGO e o nome do relacionamento (POSSUI, ESTUDA). Esse losango é ligado por linhas aos retângulos que representam as entidades participantes do relacionamento.

- **Atributo:** é usado para referir-se à cada característica possuída pelas instâncias de uma entidade ou de um relacionamento e sua representação no DER se dá em forma de balões — embora seja desencorajada por poluí-lo facilmente;
- **Relacionamento:** descreve um evento significativo que ocorre entre instâncias de duas entidades e é representado por um losango, sendo considerado e representado a partir da modelagem lógica como uma entidade no DER quando tem cardinalidade N:N (surpresa!);
- **Cardinalidade:** conceito usado para dizer quantas vezes uma instância de uma entidade pode se relacionar com instâncias de outra entidade, também referenciado como “grau de relacionamento”.

A cardinalidade é um número que expressa o comportamento (número de ocorrências) de determinada entidade associada a uma ocorrência da entidade em questão através do relacionamento.

Existem dois tipos de cardinalidade: mínima e máxima. A cardinalidade máxima, expressa o número máximo de ocorrências de determinada entidade, associada a uma ocorrência da entidade em questão, através do relacionamento. A cardinalidade mínima, expressa o número mínimo de ocorrências de determinada entidade associada a uma ocorrência da entidade em questão através do relacionamento.

Observe as cardinalidades mínima e máxima representadas no modelo abaixo:



DER Titular x Dependente: cardinalidade

Para fazermos a leitura do modelo, partimos de determinada entidade e a cardinalidade correspondente a essa entidade é representada no lado oposto. Em nosso exemplo, a cardinalidade (0:N) faz referência a TITULAR, já a cardinalidade (1:1), faz referência a DEPENDENTE. Isso significa que:

- Uma ocorrência de empregado pode não estar associada a uma ocorrência de dependente ou pode estar associada a várias ocorrências dele (determinado empregado pode não possuir dependentes ou pode possuir vários);
- Uma ocorrência de dependente está associada a apenas uma ocorrência de empregado (determinado dependente possui apenas um empregado responsável).

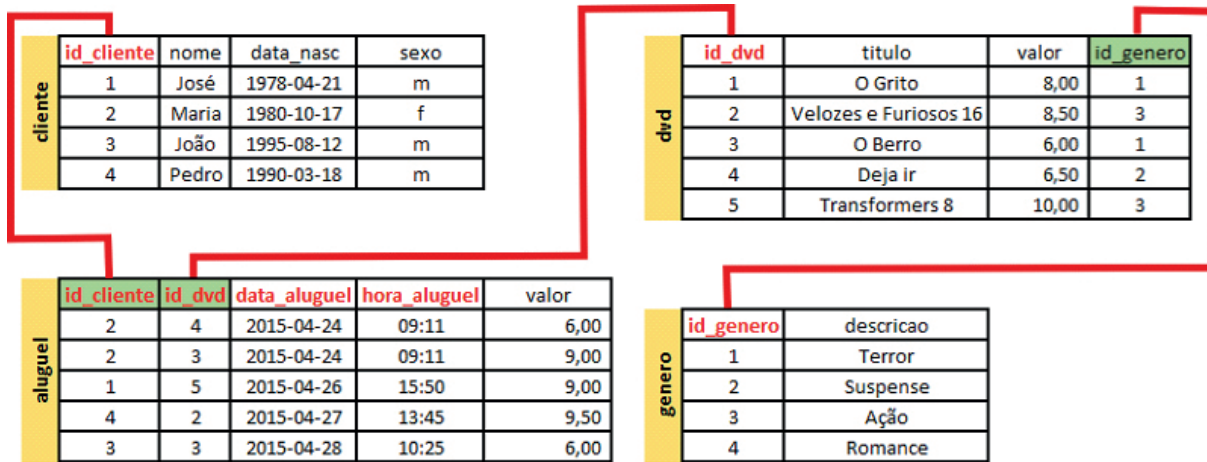
Observação: na prática, para as cardinalidades máximas, costumamos distinguir dois tipos: 1 (um) e N (cardinalidades maiores que 1). Já para as cardinalidades mínimas, costumamos distinguir dois tipos: 0 (zero) e 1 (um).

- **Condicionalidade:** responsável por comunicar se a existência de uma instância de uma entidade está condicionada à existência de uma instância de outra entidade, não sendo muito representada no DER.

• Chaves

São regras que definem comportamentos específicos sobre uma tabela¹⁹. Estas, são a base para estabelecer relacionamentos. Em uma base de dados relacional podemos considerar três tipos de chaves: chave primária, chave estrangeira e chave alternativa.

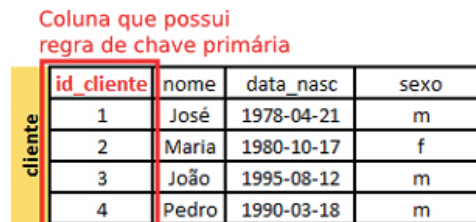
Para explicar os conceitos referente aos tipos de chaves existentes, será utilizado o modelo que segue na figura abaixo.



Tabelas para exemplificar chaves.

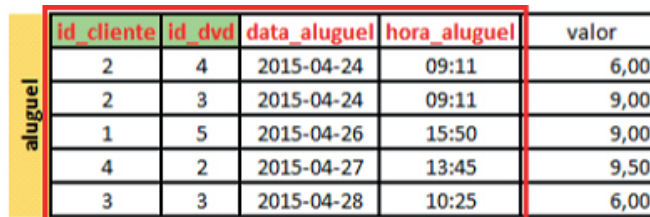
• Chave Primária - (Primary Key - PK)

Uma chave primária é uma regra implementada em uma coluna ou em um conjunto de colunas de forma a garantir que os valores contidos nesta (s) sejam únicos, ou seja, estes valores nunca irão se repetir.



Regra de chave primária.

Na figura anterior a coluna ID_CLIENTE contém a regra de chave primária de forma que estes valores identificaram cada um dos clientes cadastrados. Esta é a única coluna que possui informações que podem distinguir uma linha das demais, pois elas não se repetem. As colunas NOME, DATA_NASC e SEXO podem possuir informações repetidas de forma que não são bons identificadores. Como foi dito, em algumas tabelas podemos ter mais de uma coluna recebendo a regra de chave primária.



Colunas que possuem regra de chave primária composta

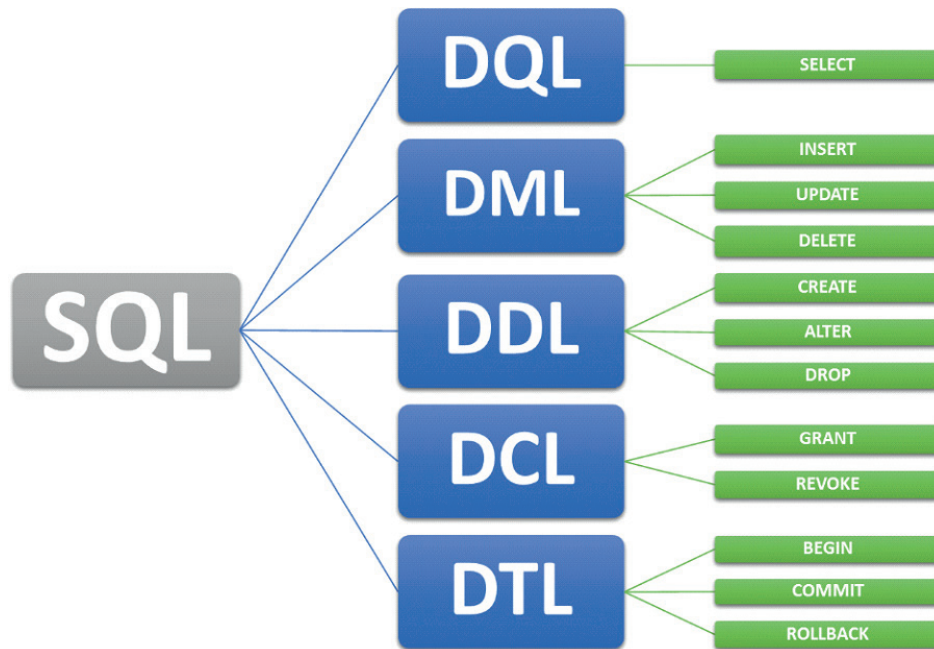
Regra de chave primária composta.

Na figura acima temos quatro colunas recebendo a regra de chave primária. Cada tabela só pode ter uma regra de chave primária, independente da quantidade de colunas que a compõem. Então podemos dizer que o cliente que possui o código (id_cliente) número 2, por exemplo, locou no dia 24 de abril 2015 os DVDs de código número 3 e 4 exatamente as 09:11. Como a regra de chave primária envolve

¹⁹ <http://thiagocury.eti.br/disciplinas/banco-de-dados-relacional/conceito-de-chaves-no-banco-de-dados-relacional.php>

É por meio dela que criamos tabelas, colunas, índices, garantimos e removemos privilégios a usuários e, principalmente, consultamos os dados armazenados em tabelas²⁰.

A linguagem SQL é organizada em subconjuntos, cada um com propósitos bem definidos²¹:



Subdivisões da linguagem SQL.

- **DQL - Linguagem de Consulta de Dados:** define o comando utilizado para que possamos consultar (SELECT) os dados armazenados no banco;
- **DML - Linguagem de Manipulação de Dados:** define os comandos utilizados para manipulação de dados no banco (INSERT, UPDATE e DELETE);
- **DDL - Linguagem de Definição de Dados:** define os comandos utilizados para criação (CREATE) de tabelas, views, índices, atualização dessas estruturas (ALTER), assim como a remoção (DROP);
- **DCL - Linguagem de Controle de Dados:** define os comandos utilizados para controlar o acesso aos dados do banco, adicionando (GRANT) e removendo (REVOKE) permissões de acesso;
- **DTL - Linguagem de Transação de Dados:** define os comandos utilizados para gerenciar as transações executadas no banco de dados, como iniciar (BEGIN) uma transação, confirmá-la (COMMIT) ou desfazê-la (ROLLBACK).

CONCEITOS DE ORGANIZAÇÃO E DE GERENCIAMENTO DE ARQUIVOS E PASTAS

Pasta

São estruturas que dividem o disco em várias partes de tamanhos variados as quais podem armazenar arquivos e outras pastas (subpastas)²².



²⁰ <https://www.devmedia.com.br/introducao-a-linguagem-sql/40690>

²¹ <https://www.devmedia.com.br/guia/guia-completo-de-sql/38314>

²² <https://docente.ifrn.edu.br/eliezioares/disciplinas/informatica/aula-05-manipulacao-de-arquivos-e-pastas>

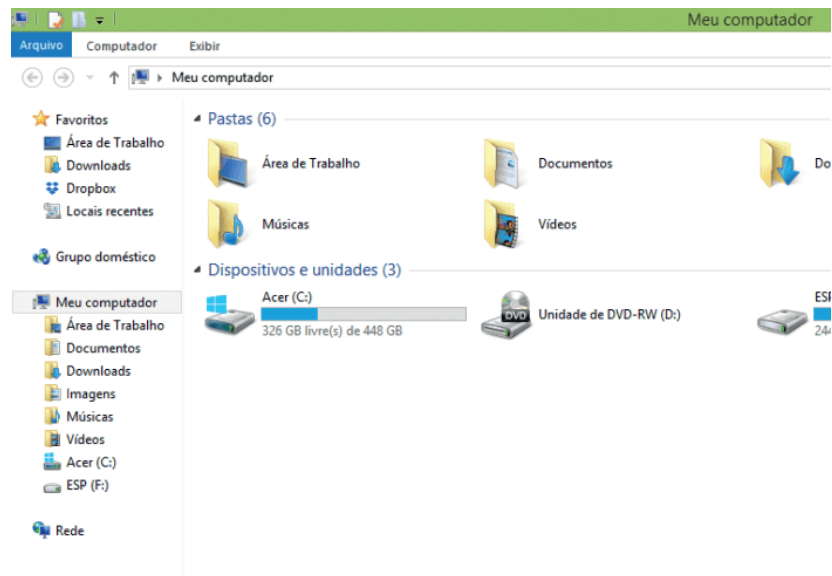
Windows Explorer

O Windows Explorer é um gerenciador de informações, arquivos, pastas e programas do sistema operacional Windows da Microsoft²³. Todo e qualquer arquivo que esteja gravado no seu computador e toda pasta que exista nele pode ser vista pelo Windows Explorer. Possui uma interface fácil e intuitiva.

Na versão em português ele é chamado de Gerenciador de arquivo ou Explorador de arquivos.

O seu arquivo é chamado de Explorer.exe

Normalmente você o encontra na barra de tarefas ou no botão Iniciar > Programas > Acessórios.



Na parte de cima do Windows Explorer você terá acesso a muitas funções de gerenciamento como criar pastas, excluir, renomear, excluir históricos, ter acesso ao prompt de comando entre outras funcionalidades que aparecem sempre que você selecionar algum arquivo.

A coluna do lado esquerdo te dá acesso direto para tudo que você quer encontrar no computador. As pastas mais utilizadas são as de Download, documentos e imagens.

Operações básicas com arquivos do Windows Explorer

- **Criar pasta:** clicar no local que quer criar a pasta e clicar com o botão direito do mouse e ir em novo > criar pasta e nomear ela. Você pode criar uma pasta dentro de outra pasta para organizar melhor seus arquivos. Caso você queira salvar dentro de uma mesma pasta um arquivo com o mesmo nome, só será possível se tiver extensão diferente. Ex.: maravilha.png e maravilha.doc

Independente de uma pasta estar vazia ou não, ela permanecerá no sistema mesmo que o computador seja reiniciado

- **Copiar:** selecione o arquivo com o mouse e clique Ctrl + C e vá para a pasta que quer colar a cópia e clique Ctrl +V. Pode também clicar com o botão direito do mouse selecionar copiar e ir para o local que quer copiar e clicar novamente como o botão direito do mouse e selecionar colar.

- **Excluir:** pode selecionar o arquivo e apertar a tecla delete ou clicar no botão direito do mouse e selecionar excluir

- **Organizar:** você pode organizar do jeito que quiser como, por exemplo, ícones grandes, ícones pequenos, listas, conteúdos, lista com detalhes. Estas funções estão na barra de cima em exibir ou na mesma barra do lado direito.

- **Movimentar:** você pode movimentar arquivos e pastas clicando Ctrl + X no arquivo ou pasta e ir para onde você quer colar o arquivo e Clicar Ctrl + V ou clicar com o botão direito do mouse e selecionar recortar e ir para o local de destino e clicar novamente no botão direito do mouse e selecionar colar.

Localizando Arquivos e Pastas

No Windows Explorer tem duas:

Tem uma barra de pesquisa acima na qual você digita o arquivo ou pasta que procura ou na mesma barra tem uma opção de Pesquisar. Clicando nesta opção terão mais opções para você refinar a sua busca.

²³ <https://centraldefavoritos.com.br/2019/06/05/conceitos-de-organizacao-e-de-gerenciamento-de-informacoes-arquivos-pastas-e-programas/>

– **Ativos:** neste momento, faz-se a utilização dos dados coletados no ataque passivo para, por exemplo, derrubar um sistema, infectar o sistema com malwares, realizar novos ataques a partir da máquina-alvo ou até mesmo destruir o equipamento (Ex.: interceptação, monitoramento, análise de pacotes).

Política de Segurança da Informação

Este documento irá auxiliar no gerenciamento da segurança da organização através de regras de alto nível que representam os princípios básicos que a entidade resolveu adotar de acordo com a visão estratégica da mesma, assim como normas (no nível tático) e procedimentos (nível operacional). Seu objetivo será manter a segurança da informação. Todos os detalhes definidos nelas serão para informar sobre o que pode e o que é proibido, incluindo:

- **Política de senhas:** define as regras sobre o uso de senhas nos recursos computacionais, como tamanho mínimo e máximo, regra de formação e periodicidade de troca.
- **Política de backup:** define as regras sobre a realização de cópias de segurança, como tipo de mídia utilizada, período de retenção e frequência de execução.
- **Política de privacidade:** define como são tratadas as informações pessoais, sejam elas de clientes, usuários ou funcionários.
- **Política de confidencialidade:** define como são tratadas as informações institucionais, ou seja, se elas podem ser repassadas a terceiros.

Mecanismos de segurança

Um mecanismo de segurança da informação é uma ação, técnica, método ou ferramenta estabelecida com o objetivo de preservar o conteúdo sigiloso e crítico para uma empresa.

Ele pode ser aplicado de duas formas:

- **Controle físico:** é a tradicional fechadura, tranca, porta e qualquer outro meio que impeça o contato ou acesso direto à informação ou infraestrutura que dá suporte a ela
- **Controle lógico:** nesse caso, estamos falando de barreiras eletrônicas, nos mais variados formatos existentes, desde um antivírus, firewall ou filtro anti-spam, o que é de grande valia para evitar infecções por e-mail ou ao navegar na internet, passa por métodos de criptografia, que transformam as informações em códigos que terceiros sem autorização não conseguem decifrar e, há ainda, a certificação e assinatura digital, sobre as quais falamos rapidamente no exemplo antes apresentado da emissão da nota fiscal eletrônica.

Todos são tipos de mecanismos de segurança, escolhidos por profissional habilitado conforme o plano de segurança da informação da empresa e de acordo com a natureza do conteúdo sigiloso.

Criptografia

É uma maneira de codificar uma informação para que somente o emissor e receptor da informação possa decifrá-la através de uma chave que é usada tanto para criptografar e descriptografar a informação²⁷.

Tem duas maneiras de criptografar informações:

- **Criptografia simétrica (chave secreta):** utiliza-se uma chave secreta, que pode ser um número, uma palavra ou apenas uma sequência de letras aleatórias, é aplicada ao texto de uma mensagem para alterar o conteúdo de uma determinada maneira. Tanto o emissor quanto o receptor da mensagem devem saber qual é a chave secreta para poder ler a mensagem.
- **Criptografia assimétrica (chave pública):** tem duas chaves relacionadas. Uma chave pública é disponibilizada para qualquer pessoa que queira enviar uma mensagem. Uma segunda chave privada é mantida em segredo, para que somente você saiba. Qualquer mensagem que foi usada a chave pública só poderá ser descriptografada pela chave privada. Se a mensagem foi criptografada com a chave privada, ela só poderá ser descriptografada pela chave pública correspondente. A criptografia assimétrica é mais lenta o processamento para criptografar e descriptografar o conteúdo da mensagem. Um exemplo de criptografia assimétrica é a assinatura digital.
- **Assinatura Digital:** é muito usado com chaves públicas e permitem ao destinatário verificar a autenticidade e a integridade da informação recebida. Além disso, uma assinatura digital não permite o repúdio, isto é, o emitente não pode alegar que não realizou a ação. A chave é integrada ao documento, com isso se houver alguma alteração de informação invalida o documento.
- **Sistemas biométricos:** utilizam características físicas da pessoa como os olhos, retina, dedos, digitais, palma da mão ou voz.

Firewall

Firewall ou “parede de fogo” é uma solução de segurança baseada em hardware ou software (mais comum) que, a partir de um conjunto de regras ou instruções, analisa o tráfego de rede para determinar quais operações de transmissão ou recepção de dados podem ser executadas. O firewall se enquadra em uma espécie de barreira de defesa. A sua missão, por assim dizer, consiste basicamente em bloquear tráfego de dados indesejado e liberar acessos bem-vindos.

27 <https://centraldefavoritos.com.br/2016/11/19/conceitos-de-protecao-e-seguranca-da-informacao-parte-2/>

Vírus

Vírus é um programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos.

Para que possa se tornar ativo e dar continuidade ao processo de infecção, o vírus depende da execução do programa ou arquivo hospedeiro, ou seja, para que o seu computador seja infectado é preciso que um programa já infectado seja executado.

O principal meio de propagação de vírus costumava ser os disquetes. Com o tempo, porém, estas mídias caíram em desuso e começaram a surgir novas maneiras, como o envio de e-mail. Atualmente, as mídias removíveis tornaram-se novamente o principal meio de propagação, não mais por disquetes, mas, principalmente, pelo uso de pen-drives.

Há diferentes tipos de vírus. Alguns procuram permanecer ocultos, infectando arquivos do disco e executando uma série de atividades sem o conhecimento do usuário. Há outros que permanecem inativos durante certos períodos, entrando em atividade apenas em datas específicas. Alguns dos tipos de vírus mais comuns são:

- Vírus propagado por e-mail: recebido como um arquivo anexo a um e-mail cujo conteúdo tenta induzir o usuário a clicar sobre este arquivo, fazendo com que seja executado.

- Vírus de script: 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.

- Vírus de macro: tipo específico de vírus de script, escrito em linguagem de macro, que tenta infectar arquivos manipulados por aplicativos que utilizam esta linguagem como, por exemplo, os que compõem o Microsoft Office (Excel, Word e PowerPoint, entre outros).

- Vírus de telefone celular: vírus que se propaga de celular para celular por meio da tecnologia bluetooth ou de mensagens MMS (Multimedia Message Service). A infecção ocorre quando um usuário permite o recebimento de um arquivo infectado e o executa.

Worm

Worm é um programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador.

Diferente do vírus, o worm não se propaga por meio da inclusão de cópias de si mesmo em outros programas ou arquivos, mas sim pela execução direta de suas cópias ou pela exploração automática de vulnerabilidades existentes em programas instalados em computadores.

Worms são notadamente responsáveis por consumir muitos recursos, devido à grande quantidade de cópias de si mesmo que costumam propagar e, como consequência, podem afetar o desempenho de redes e a utilização de computadores.

Bot e botnet

Bot é um programa que dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente. Possui processo de infecção e propagação similar ao do worm, ou seja, é capaz de se propagar automaticamente, explorando vulnerabilidades existentes em programas instalados em computadores.

A comunicação entre o invasor e o computador infectado pelo bot pode ocorrer via canais de IRC, servidores Web e redes do tipo P2P, entre outros meios. Ao se comunicar, o invasor pode enviar instruções para que ações maliciosas sejam executadas, como desferir ataques, furtar dados do computador infectado e enviar spam.

Um computador infectado por um bot costuma ser chamado de zumbi (zombie computer), pois pode ser controlado remotamente, sem o conhecimento do seu dono. Também pode ser chamado de spam zombie quando o bot instalado o transforma em um servidor de e-mails e o utiliza para o envio de spam.

Botnet é uma rede formada por centenas ou milhares de computadores zumbis e que permite potencializar as ações danosas executadas pelos bots.

Quanto mais zumbis participarem da botnet mais potente ela será. O atacante que a controlar, além de usá-la para seus próprios ataques, também pode alugá-la para outras pessoas ou grupos que desejem que uma ação maliciosa específica seja executada.

Algumas das ações maliciosas que costumam ser executadas por intermédio de botnets são: ataques de negação de serviço, propagação de códigos maliciosos (inclusive do próprio bot), coleta de informações de um grande número de computadores, envio de spam e camuflagem da identidade do atacante (com o uso de proxies instalados nos zumbis).

Spyware

Spyware é um programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros.

Pode ser usado tanto de forma legítima quanto maliciosa, dependendo de como é instalado, das ações realizadas, do tipo de informação monitorada e do uso que é feito por quem recebe as informações coletadas. Pode ser considerado de uso:

- **Legítimo:** quando instalado em um computador pessoal, pelo próprio dono ou com consentimento deste, com o objetivo de verificar se outras pessoas o estão utilizando de modo abusivo ou não autorizado.

- **Malicioso:** quando executa ações que podem comprometer a privacidade do usuário e a segurança do computador, como monitorar e capturar informações referentes à navegação do usuário ou inseridas em outros programas (por exemplo, conta de usuário e senha).

Alguns tipos específicos de programas spyware são:

- **Keylogger:** capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador.

- **Screenlogger:** similar ao keylogger, capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o mouse é clicado, ou a região que circunda a posição onde o mouse é clicado.

- **Adware:** projetado especificamente para apresentar propagandas.

Backdoor

Backdoor é um programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim.

Pode ser incluído pela ação de outros códigos maliciosos, que tenham previamente infectado o computador, ou por atacantes, que explorem vulnerabilidades existentes nos programas instalados no computador para invadi-lo.

Após incluído, o backdoor é usado para assegurar o acesso futuro ao computador comprometido, permitindo que ele seja acessado remotamente, sem que haja necessidade de recorrer novamente aos métodos utilizados na realização da invasão ou infecção e, na maioria dos casos, sem que seja notado.