



SME MONTES CLAROS - MG

**SECRETARIA DE EDUCAÇÃO MUNICIPAL
DE MONTES CLAROS - MINAS GERAIS**

**Auxiliar de Docência,
Auxiliar de Secretaria de
Educação Básica e Agente
Administrativo**

**EDITAL DO CONCURSO PÚBLICO Nº 01/2024,
DE 02 DE ABRIL DE 2024**

**CÓD: SL-114AB-24
7908433252993**

Língua Portuguesa

1. Compreensão e interpretação de textos	7
2. Tipologia textual e gêneros textuais	8
3. Denotação e conotação. Sinonímia, antonímia e polissemia	15
4. Coesão e coerência textuais	15
5. Figuras de linguagem	16
6. Conhecimentos gerais sobre a norma-padrão da língua e a gramática tradicional	19
7. Classes de palavras	20
8. Concordância verbal e nominal	29
9. Regência verbal e nominal	30
10. Uso do sinal indicativo de crase	33
11. Pontuação	33
12. Ortografia	35
13. acentuação gráfica	36
14. Formação de palavras	37
15. Colocação pronominal	39
16. Ortografia Oficial	40

Matemática

1. Conjuntos numéricos: naturais, inteiros, racionais e reais. Operações com números reais: adição, subtração, multiplicação, divisão, potenciação e radiciação	51
2. Problemas envolvendo contagem dos elementos de um conjunto	60
3. Notação científica	64
4. Cálculo de porcentagem: acréscimos e decréscimos simples e sucessivos	64
5. Cálculo de área e perímetro de figuras geométricas planas. Polígonos regulares	65
6. Tratamento da informação: análise, leitura e interpretação de tabelas e gráficos	67
7. Problemas de contagem	73
8. Problemas envolvendo equação do 1º grau	74
9. Problemas envolvendo grandezas diretamente e inversamente proporcionais	75
10. Sistema monetário brasileiro	77

Legislação

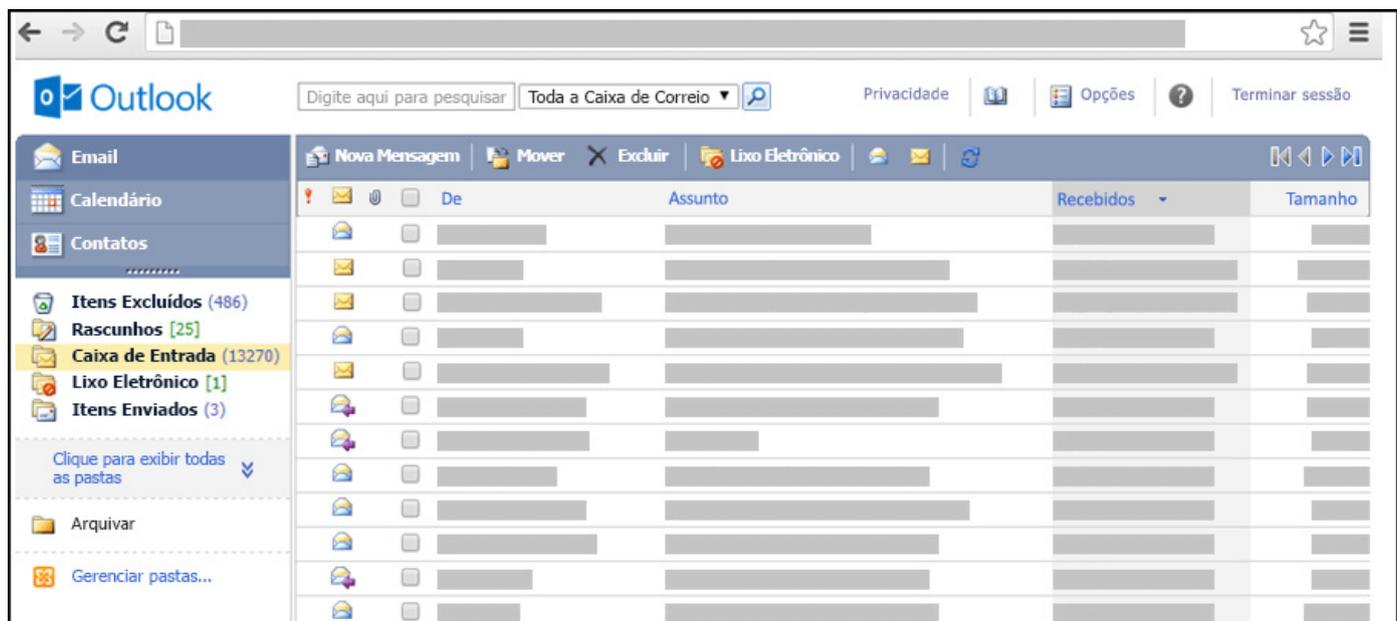
1. Constituição Federal de 1988; Direitos e garantias fundamentais – Artigo 5º	85
2. Lei nº 9.394/1996 – Lei de Diretrizes e Bases da Educação Nacional (LDB) e suas alterações	89
3. Lei nº 13.005/2014	106
4. Lei Federal nº 8.069/1990 – Estatuto da Criança e do Adolescente	120
5. Lei nº 13.146/2015 – Lei Brasileira de Inclusão da Pessoa com Deficiência (Estatuto da Pessoa com Deficiência)	158
6. Plano Nacional de Educação em Direitos Humanos – 2007	175

ÍNDICE

7. Lei nº 10.741/2003 (Estatuto da pessoa idosa)	176
8. Código de Ética do Servidor do Município de Montes Claros – Lei nº 3.177/2003.....	187
9. Estatuto do servidor público municipal de Montes Claros – Lei nº 3.175/2003	189
10. Estatuto do Magistério do Município de Montes Claros – Lei nº 3.176/2003	207

Informática Básica

1. Sistemas operacionais: conhecimentos do ambiente Windows 10: configurações básicas do Sistema Operacional (painel de controle); organização de pastas e arquivos; operações de manipulação de pastas e arquivos (criar, copiar, mover, excluir e renomear)	221
2. Editor de texto Microsoft Word (pacote Microsoft 365): criação, edição, formatação e impressão; criação e manipulação de tabelas; inserção e formatação de gráficos e figuras; geração de mala direta	232
3. Planilha eletrônica Microsoft Excel (pacote Microsoft 365): criação, edição, formatação e impressão; utilização de fórmulas; geração de gráficos; classificação e organização de dados	238
4. Software de Apresentações PowerPoint (pacote Microsoft 365): criação, edição, formatação e impressão das apresentações.....	242
5. Conhecimentos de internet: noções básicas	250
6. correio eletrônico (receber e enviar mensagens; anexos; catálogos de endereço; organização das mensagens)	253
7. Segurança. Conceitos de segurança da informação; Classificação da informação, segurança física e segurança lógica; Análise e gerenciamento de riscos; Ameaça, tipos de ataques e vulnerabilidade	256
8. Lei Geral de Proteção de Dados Pessoais (LGPD); Lei nº 13.709/2018 e LGPD.....	261
9. Decreto nº 2013/2003 - (Município de Montes Claros).....	274



Respondendo uma mensagem

Os ícones disponíveis para responder uma mensagem são:

- **Responder ao remetente:** responde à mensagem selecionada para o autor dela (remetente).
- **Responde a todos:** a mensagem é enviada tanto para o autor como para as outras pessoas que estavam na lista de cópias.
- **Encaminhar:** envia a mensagem selecionada para outra pessoa.

Clientes de E-mail

Um cliente de e-mail é essencialmente um programa de computador que permite compor, enviar e receber e-mails a partir de um servidor de e-mail, o que exige cadastrar uma conta de e-mail e uma senha para seu correto funcionamento. Há diversos clientes de e-mails no mercado que, além de manipular e-mails, podem oferecer recursos diversos.

– **Outlook:** cliente de e-mails nativo do sistema operacional Microsoft Windows. A versão Express é uma versão mais simplificada e que, em geral, vem por padrão no sistema operacional Windows. Já a versão Microsoft Outlook é uma versão que vem no pacote Microsoft Office possui mais recursos, incluindo, além de funções de e-mail, recursos de calendário.

– **Mozilla Thunderbird:** é um cliente de e-mails e notícias Open Source e gratuito criado pela Mozilla Foundation (mesma criadora do Mozilla Firefox).

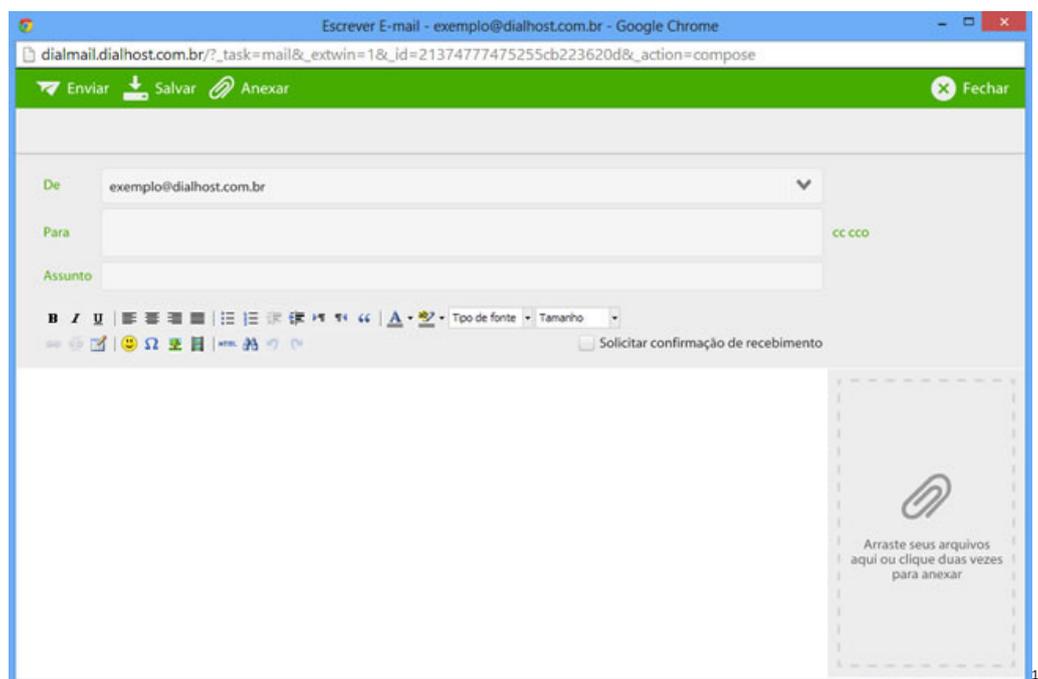
Webmails

Webmail é o nome dado a um cliente de e-mail que não necessita de instalação no computador do usuário, já que funciona como uma página de internet, bastando o usuário acessar a página do seu provedor de e-mail com seu login e senha. Desta forma, o usuário ganha mobilidade já que não necessita estar na máquina em que um cliente de e-mail está instalado para acessar seu e-mail. A desvantagem da utilização de webmails em comparação aos clientes de e-mail é o fato de necessitarem de conexão de Internet para leitura dos e-mails, enquanto nos clientes de e-mail basta a conexão para “baixar” os e-mails, sendo que a posterior leitura pode ser realizada desconectada da Internet.

Exemplos de servidores de webmail do mercado são:

- Gmail
- Yahoo!Mail
- Microsoft Outlook: versão on-line do Outlook. Anteriormente era conhecido como Hotmail, porém mudou de nome quando a Microsoft integrou suas diversas tecnologias.

12 <https://support.microsoft.com/pt-br/office/ler-e-enviar-emails-na-vers%C3%A3o-light-do-outlook-582a8fdc-152c-4b61-85fa-ba5ddf07050b>



Diferença entre webmail e correio eletrônico

O webmail (Yahoo ou Gmail) você acessa através de seu navegador (Firefox ou Google Chrome) e só pode ler conectado na internet. Já o correio eletrônico (Thunderbird ou Outlook) você acessa com uma conexão de internet e pode baixar seus e-mails, mas depois pode ler na hora que quiser sem precisar estar conectado na internet.

SEGURANÇA. CONCEITOS DE SEGURANÇA DA INFORMAÇÃO; CLASSIFICAÇÃO DA INFORMAÇÃO, SEGURANÇA FÍSICA E SEGURANÇA LÓGICA; ANÁLISE E GERENCIAMENTO DE RISCOS; AMEAÇA, TIPOS DE ATAQUES E VULNERABILIDADE

SEGURANÇA DA INFORMAÇÃO

Segurança da informação é o conjunto de ações para proteção de um grupo de dados, protegendo o valor que ele possui, seja para um indivíduo específico no âmbito pessoal, seja para uma organização¹⁴.

É essencial para a proteção do conjunto de dados de uma corporação, sendo também fundamentais para as atividades do negócio.

Quando bem aplicada, é capaz de blindar a empresa de ataques digitais, desastres tecnológicos ou falhas humanas. Porém, qualquer tipo de falha, por menor que seja, abre brecha para problemas.

A segurança da informação se baseia nos seguintes pilares¹⁵:

– **Confidencialidade:** o conteúdo protegido deve estar disponível somente a pessoas autorizadas.

– **Disponibilidade:** é preciso garantir que os dados estejam acessíveis para uso por tais pessoas quando for necessário, ou seja, de modo permanente a elas.

– **Integridade:** a informação protegida deve ser íntegra, ou seja, sem sofrer qualquer alteração indevida, não importa por quem e nem em qual etapa, se no processamento ou no envio.

– **Autenticidade:** a ideia aqui é assegurar que a origem e autoria do conteúdo seja mesmo a anunciada.

Existem outros termos importantes com os quais um profissional da área trabalha no dia a dia.

Podemos citar a legalidade, que diz respeito à adequação do conteúdo protegido à legislação vigente; a privacidade, que se refere ao controle sobre quem acessa as informações; e a auditoria, que permite examinar o histórico de um evento de segurança da informação, rastreando as suas etapas e os responsáveis por cada uma delas.

Alguns conceitos relacionados à aplicação dos pilares

– **Vulnerabilidade:** pontos fracos existentes no conteúdo protegido, com potencial de prejudicar alguns dos pilares de segurança da informação, ainda que sem intenção

– **Ameaça:** elemento externo que pode se aproveitar da vulnerabilidade existente para atacar a informação sensível ao negócio.

– **Probabilidade:** se refere à chance de uma vulnerabilidade ser explorada por uma ameaça.

¹³ <https://www.dialhost.com.br/ajuda/abrir-uma-nova-janela-para-escrever-novo-email>

¹⁴ <https://ecoit.com.br/seguranca-da-informacao/>

¹⁵ <https://bit.ly/2E5beRr>

Pode ser incluído pela ação de outros códigos maliciosos, que tenham previamente infectado o computador, ou por atacantes, que exploram 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.

Cavalo de troia (Trojan)

Cavalo de troia, trojan ou trojan-horse, é um programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário.

Exemplos de trojans são programas que você recebe ou obtém de sites na Internet e que parecem ser apenas cartões virtuais animados, álbuns de fotos, jogos e protetores de tela, entre outros. Estes programas, geralmente, consistem de um único arquivo e necessitam ser explicitamente executados para que sejam instalados no computador.

Trojans também podem ser instalados por atacantes que, após invadirem um computador, alteram programas já existentes para que, além de continuarem a desempenhar as funções originais, também executem ações maliciosas.

Rootkit

Rootkit é um conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido.

Rootkits inicialmente eram usados por atacantes que, após invadirem um computador, os instalavam para manter o acesso privilegiado, sem precisar recorrer novamente aos métodos utilizados na invasão, e para esconder suas atividades do responsável e/ou dos usuários do computador. Apesar de ainda serem bastante usados por atacantes, os rootkits atualmente têm sido também utilizados e incorporados por outros códigos maliciosos para ficarem ocultos e não serem detectados pelo usuário e nem por mecanismos de proteção.

Ransomware

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 usuário²¹.

O pagamento do resgate geralmente é feito via bitcoins.

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 e explorando vulnerabilidades em sistemas que não tenham recebido as devidas atualizações de segurança.

Engenharia Social

Engenharia social é uma técnica de manipulação psicológica utilizada para obter informações confidenciais. Ela explora a tendência natural das pessoas em confiar e pode envolver vários métodos, como pretexting, baiting e tailgating, para enganar indivíduos e acessar informações privilegiadas ou sistemas protegidos.

Phishing

É um tipo de fraude onde o atacante se disfarça como uma entidade confiável em comunicações eletrônicas para enganar as vítimas e fazê-las revelar informações pessoais, como senhas e números de cartão de crédito. Geralmente, isso é feito por meio de e-mails ou mensagens que parecem ser de bancos, redes sociais ou outros serviços online legítimos.

Smishing

Smishing é uma variante do phishing que utiliza mensagens de texto (SMS) como meio para enganar as vítimas e induzi-las a fornecer informações pessoais ou clicar em links maliciosos. Os atacantes costumam se passar por instituições financeiras ou outras organizações confiáveis para ganhar a confiança das vítimas.

Vishing

Vishing é uma forma de phishing realizada por meio de chamadas telefônicas ou mensagens de voz. Os criminosos se passam por representantes de instituições legítimas e tentam persuadir as vítimas a fornecer informações pessoais ou financeiras.

Antivírus

O antivírus é um software de proteção do computador que elimina programas maliciosos que foram desenvolvidos para prejudicar o computador.

O vírus infecta o computador através da multiplicação dele (cópias) com intenção de causar danos na máquina ou roubar dados.

O antivírus analisa os arquivos do computador buscando padrões de comportamento e códigos que não seriam comuns em algum tipo de arquivo e compara com seu banco de dados. Com isto ele avisa o usuário que tem algo suspeito para ele tomar providência.

O banco de dados do antivírus é muito importante neste processo, por isso, ele deve ser constantemente atualizado, pois todos os dias são criados vírus novos.

Uma grande parte das infecções de vírus tem participação do usuário. Os mais comuns são através de links recebidos por e-mail ou download de arquivos na internet de sites desconhecidos ou mesmo só de acessar alguns sites duvidosos pode acontecer uma contaminação.

Outro jeito de contaminar é através de dispositivos de armazenamento móveis como HD externo e pen drive. Nestes casos devem acionar o antivírus para fazer uma verificação antes.

Existem diversas opções confiáveis, tanto gratuitas quanto pagas. Entre as principais estão:

- Avast;
- AVG;
- Norton;
- Avira;
- Kaspersky;
- McAfee.

Filtro anti-spam

Spam é o termo usado para referir-se aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas.

Spam zombies são computadores de usuários finais que foram comprometidos por códigos maliciosos em geral, como worms, bots, vírus e cavalos de tróia. Estes códigos maliciosos, uma vez instalados, permitem que spammers utilizem a máquina para o envio

21 <https://cartilha.cert.br/ransomware/>

VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019) Vigência

IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

§1º (Revogado). (Redação dada pela Lei nº 13.853, de 2019) Vigência

§2º (Revogado). (Redação dada pela Lei nº 13.853, de 2019) Vigência

§3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.

§4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei.

§5º O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.

§6º A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.

§7º O tratamento posterior dos dados pessoais a que se referem os §§3º e 4º deste artigo poderá ser realizado para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei. (Incluído pela Lei nº 13.853, de 2019) Vigência

Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.

§1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais.

§2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.

§3º É vedado o tratamento de dados pessoais mediante vício de consentimento.

§4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.

§5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei.

§6º Em caso de alteração de informação referida nos incisos I, II, III ou V do art. 9º desta Lei, o controlador deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração.

Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:

- I - finalidade específica do tratamento;
- II - forma e duração do tratamento, observados os segredos comercial e industrial;
- III - identificação do controlador;
- IV - informações de contato do controlador;
- V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;
- VI - responsabilidades dos agentes que realizarão o tratamento; e
- VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

§1º Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.

§2º Na hipótese em que o consentimento é requerido, se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações.

§3º Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 desta Lei.

Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:

- I - apoio e promoção de atividades do controlador; e
- II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.

§1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.

§2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.

§3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

SEÇÃO II

DO TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS

Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

- I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
- II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

§6º As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

SEÇÃO IV DO TÉRMINO DO TRATAMENTO DE DADOS

Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:

I - verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;

II - fim do período de tratamento;

III - comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no §5º do art. 8º desta Lei, resguardado o interesse público; ou

IV - determinação da autoridade nacional, quando houver violação ao disposto nesta Lei.

Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:

I - cumprimento de obrigação legal ou regulatória pelo controlador;

II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou

IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

CAPÍTULO III DOS DIREITOS DO TITULAR

Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei.

Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

I - confirmação da existência de tratamento;

II - acesso aos dados;

III - correção de dados incompletos, inexatos ou desatualizados;

IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;

V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; (Redação dada pela Lei nº 13.853, de 2019) Vigência

VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;

VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;

IX - revogação do consentimento, nos termos do §5º do art. 8º desta Lei.

§1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional.

§2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei.

§3º Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento.

§4º Em caso de impossibilidade de adoção imediata da providência de que trata o §3º deste artigo, o controlador enviará ao titular resposta em que poderá:

I - comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente; ou

II - indicar as razões de fato ou de direito que impedem a adoção imediata da providência.

§5º O requerimento referido no §3º deste artigo será atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento.

§6º O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional. (Redação dada pela Lei nº 13.853, de 2019) Vigência

§7º A portabilidade dos dados pessoais a que se refere o inciso V do caput deste artigo não inclui dados que já tenham sido anonimizados pelo controlador.

§8º O direito a que se refere o §1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor.

Art. 19. A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular:

I - em formato simplificado, imediatamente; ou

II - por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular.

§1º Os dados pessoais serão armazenados em formato que favoreça o exercício do direito de acesso.

§2º As informações e os dados poderão ser fornecidos, a critério do titular:

I - por meio eletrônico, seguro e idôneo para esse fim; ou

II - sob forma impressa.

§3º Quando o tratamento tiver origem no consentimento do titular ou em contrato, o titular poderá solicitar cópia eletrônica integral de seus dados pessoais, observados os segredos comercial e industrial, nos termos de regulamentação da autoridade nacional, em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento.

§4º A autoridade nacional poderá dispor de forma diferenciada acerca dos prazos previstos nos incisos I e II do caput deste artigo para os setores específicos.

**CAPÍTULO VIII
DA FISCALIZAÇÃO**

**SEÇÃO I
DAS SANÇÕES ADMINISTRATIVAS**

Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: (Vigência)

I - advertência, com indicação de prazo para adoção de medidas corretivas;

II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R\$ 50.000.000,00 (cinquenta milhões de reais) por infração;

III - multa diária, observado o limite total a que se refere o inciso II;

IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;

V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;

VI - eliminação dos dados pessoais a que se refere a infração;

VII - (VETADO);

VIII - (VETADO);

IX - (VETADO).

X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; (Incluído pela Lei nº 13.853, de 2019)

XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; (Incluído pela Lei nº 13.853, de 2019)

XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. (Incluído pela Lei nº 13.853, de 2019)

§1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:

I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;

II - a boa-fé do infrator;

III - a vantagem auferida ou pretendida pelo infrator;

IV - a condição econômica do infrator;

V - a reincidência;

VI - o grau do dano;

VII - a cooperação do infrator;

VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do §2º do art. 48 desta Lei;

IX - a adoção de política de boas práticas e governança;

X - a pronta adoção de medidas corretivas; e

XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

§2º O disposto neste artigo não substitui a aplicação de sanções administrativas, civis ou penais definidas na Lei nº 8.078, de 11 de setembro de 1990, e em legislação específica. (Redação dada pela Lei nº 13.853, de 2019)

§3º O disposto nos incisos I, IV, V, VI, X, XI e XII do caput deste artigo poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei nº 8.112, de 11 de dezembro de 1990, na Lei nº 8.429, de 2 de junho de 1992, e na Lei nº 12.527, de 18 de novembro de 2011. (Promulgação partes vetadas)

§4º No cálculo do valor da multa de que trata o inciso II do caput deste artigo, a autoridade nacional poderá considerar o faturamento total da empresa ou grupo de empresas, quando não dispuser do valor do faturamento no ramo de atividade empresarial em que ocorreu a infração, definido pela autoridade nacional, ou quando o valor for apresentado de forma incompleta ou não for demonstrado de forma inequívoca e idônea.

§5º O produto da arrecadação das multas aplicadas pela ANPD, inscritas ou não em dívida ativa, será destinado ao Fundo de Defesa de Direitos Difusos de que tratam o art. 13 da Lei nº 7.347, de 24 de julho de 1985, e a Lei nº 9.008, de 21 de março de 1995. (Incluído pela Lei nº 13.853, de 2019)

§6º As sanções previstas nos incisos X, XI e XII do caput deste artigo serão aplicadas: (Incluído pela Lei nº 13.853, de 2019)

I - somente após já ter sido imposta ao menos 1 (uma) das sanções de que tratam os incisos II, III, IV, V e VI do caput deste artigo para o mesmo caso concreto; e (Incluído pela Lei nº 13.853, de 2019)

II - em caso de controladores submetidos a outros órgãos e entidades com competências sancionatórias, ouvidos esses órgãos. (Incluído pela Lei nº 13.853, de 2019)

§7º Os vazamentos individuais ou os acessos não autorizados de que trata o caput do art. 46 desta Lei poderão ser objeto de conciliação direta entre controlador e titular e, caso não haja acordo, o controlador estará sujeito à aplicação das penalidades de que trata este artigo. (Incluído pela Lei nº 13.853, de 2019)

Art. 53. A autoridade nacional definirá, por meio de regulamento próprio sobre sanções administrativas a infrações a esta Lei, que deverá ser objeto de consulta pública, as metodologias que orientarão o cálculo do valor-base das sanções de multa. (Vigência)

§1º As metodologias a que se refere o caput deste artigo devem ser previamente publicadas, para ciência dos agentes de tratamento, e devem apresentar objetivamente as formas e dosimetrias para o cálculo do valor-base das sanções de multa, que deverão conter fundamentação detalhada de todos os seus elementos, demonstrando a observância dos critérios previstos nesta Lei.

§2º O regulamento de sanções e metodologias correspondentes deve estabelecer as circunstâncias e as condições para a adoção de multa simples ou diária.

Art. 54. O valor da sanção de multa diária aplicável às infrações a esta Lei deve observar a gravidade da falta e a extensão do dano ou prejuízo causado e ser fundamentado pela autoridade nacional. (Vigência)

Parágrafo único. A intimação da sanção de multa diária deverá conter, no mínimo, a descrição da obrigação imposta, o prazo razoável e estipulado pelo órgão para o seu cumprimento e o valor da multa diária a ser aplicada pelo seu descumprimento.