Editora Solução
a solução para o seu concurso!

# DATAPREV

**EMPRESA DE TECNOLOGIA E INFORMAÇÕES DA PREVIDÊNCIA**

## Comum aos Cargos de Ensino Médio/Técnico e Superior

**EDITAL Nº 1 - DATAPREV, DE 28 DE JULHO DE 2023**

CÓD: SL-041AG-23
7908433240129

# Língua Portuguesa



# Língua Inglesa



# Raciocínio Lógico

# Atualidades



# Legislação acerca de Segurança de Informações e Proteção de Dados

## IDENTIFICANDO O TEMA DE UM TEXTO

O tema é a ideia principal do texto. É com base nessa ideia principal que o texto será desenvolvido. Para que você consiga identificar o tema de um texto, é necessário relacionar as diferentes informações de forma a construir o seu sentido global, ou seja, você precisa relacionar as múltiplas partes que compõem um todo significativo, que é o texto.

Em muitas situações, por exemplo, você foi estimulado a ler um texto por sentir-se atraído pela temática resumida no título. Pois o título cumpre uma função importante: antecipar informações sobre o assunto que será tratado no texto.

Em outras situações, você pode ter abandonado a leitura porque achou o título pouco atraente ou, ao contrário, sentiu-se atraído pelo título de um livro ou de um filme, por exemplo. É muito comum as pessoas se interessarem por temáticas diferentes, dependendo do sexo, da idade, escolaridade, profissão, preferências pessoais e experiência de mundo, entre outros fatores.

Mas, sobre que tema você gosta de ler? Esportes, namoro, sexualidade, tecnologia, ciências, jogos, novelas, moda, cuidados com o corpo? Perceba, portanto, que as temáticas são praticamente infinitas e saber reconhecer o tema de um texto é condição essencial para se tornar um leitor hábil. Vamos, então, começar nossos estudos?

Propomos, inicialmente, que você acompanhe um exercício bem simples, que, intuitivamente, todo leitor faz ao ler um texto: reconhecer o seu tema. Vamos ler o texto a seguir?

CACHORROS

Os zoólogos acreditam que o cachorro se originou de uma espécie de lobo que vivia na Ásia. Depois os cães se juntaram aos seres humanos e se espalharam por quase todo o mundo. Essa amizade começou há uns 12 mil anos, no tempo em que as pessoas precisavam caçar para se alimentar. Os cachorros perceberam que, se não atacassem os humanos, podiam ficar perto deles e comer a comida que sobrava. Já os homens descobriram que os cachorros podiam ajudar a caçar, a cuidar de rebanhos e a tomar conta da casa, além de serem ótimos companheiros. Um colaborava com o outro e a parceria deu certo.

Ao ler apenas o título "Cachorros", você deduziu sobre o possível assunto abordado no texto. Embora você imagine que o texto vai falar sobre cães, você ainda não sabia exatamente o que ele falaria sobre cães. Repare que temos várias informações ao longo do texto: a hipótese dos zoólogos sobre a origem dos cães, a associação entre eles e os seres humanos, a disseminação dos cães pelo mundo, as vantagens da convivência entre cães e homens.

As informações que se relacionam com o tema chamamos de subtemas (ou ideias secundárias). Essas informações se integram, ou seja, todas elas caminham no sentido de estabelecer uma unidade de sentido. Portanto, pense: sobre o que exatamente esse texto fala? Qual seu assunto, qual seu tema? Certamente você chegou à conclusão de que o texto fala sobre a relação entre homens e cães. Se foi isso que você pensou, parabéns! Isso significa que você foi capaz de identificar o tema do texto!

*Fonte: https://portuguesrapido.com/tema-ideia-central-e-ideias-secundarias/*

## IDENTIFICAÇÃO DE EFEITOS DE IRONIA OU HUMOR EM TEXTOS VARIADOS

**Ironia**

Ironia *é o recurso pelo qual o emissor diz o contrário do que está pensando ou sentindo (ou por pudor em relação a si próprio ou com intenção depreciativa e sarcástica em relação a outrem).*

A ironia consiste na utilização de determinada palavra ou expressão que, em um outro contexto diferente do usual, ganha um novo sentido, gerando um efeito de humor.

Exemplo:



Na construção de um texto, ela pode aparecer em três modos: ironia verbal, ironia de situação e ironia dramática (ou satírica).

*Ironia verbal*

Ocorre quando se diz algo pretendendo expressar outro significado, normalmente oposto ao sentido literal. A expressão e a intenção são diferentes.

Exemplo: Você foi tão bem na prova! Tirou um zero incrível!

*Ironia de situação*

A intenção e resultado da ação não estão alinhados, ou seja, o resultado é contrário ao que se espera ou que se planeja.

Exemplo: Quando num texto literário uma personagem planeja uma ação, mas os resultados não saem como o esperado. No livro "Memórias Póstumas de Brás Cubas", de Machado de Assis, a personagem título tem obsessão por ficar conhecida. Ao longo da vida, tenta de muitas maneiras alcançar a notoriedade sem suces-

• *To fry – John **fries** potatoes in oil.* (John frita batatas no óleo)
• *To copy – Lucy **copies** the text.* (Lucy copia o texto)
• *To reply – He **replies** with a text.* (Ele responde com uma mensagem)

Há, porém, uma exceção para a regra do "y". Em verbos que seguem a ordem de consoante, vogal e consoante (cvc) em sua terminação, acrescenta-se apenas o "*s*". Confira:
• *To play - She **plays** the guitar*. (Ela toca violão)
• *To stay* – It **stays** there (Fica lá)
• *To enjoy* – He **enjoys** playing the piano. (Ele gosta de tocar o violão)

Verbos terminados em ch, sh, s, z ou x, terminam "*es*". Observe:
• *To touch – He **touches** his nose*. (Ele toca seu nariz)
• *To press – Mary **presses** the button.* (Maria aperta o botão)
• *To buzz – The noise **buzzes** across the room.* (O barulho zumbe pela sala)
• *To crash* – The bus **crashes** against the wall (O ônibus bate contra o muro)
• *To fix* – The man **fixes** the sink. (O homem conserta a pia)

Observe que apenas no caso dos pronomes em terceira pessoa (he, she, it), o verbo se modificou. Nos demais sujeitos o verbo mantem sua forma original do infinitivo.

Há ainda o uso dos verbos auxiliares DO e DOES em frases negativas e interrogativas no presente simples do inglês. E, assim como a conjugação verbal, os auxiliares são divididos em dois grupos de acordo com os sujeitos:
• **DO** para *I, You, We, They e You* (plural).
• **DOES** para *He, She e It.*

Na negativa, o verbo auxiliar do ou does é somado ao not (não), podendo sofrer uma contração, comum da linguagem informal.
• Do not = **don't**
• Does not = **doesn't**

Sendo assim, no presente acrescentam-se estes auxiliares ao modo negativo para formular uma frase negativa. O verbo que o segue, porém, retorna ao seu estado primário (infinitivo sem "to") em todos os casos quando as frases estão na forma negativa. Veja:
• *You **do not** <u>enjoy</u> this song. / You **don't** <u>enjoy</u> this song*
(Você não gosta desta canção)
• *She **does not** <u>understand</u> English / She **doesn't** <u>understand</u> English.*
(Ela não entende inglês)

Em frases interrogativas os verbos auxiliares do presente são postos no início da frase e o verbo retorna para seu estado infinitivo sem o "to". Confira:
• ***Do** you enjoy watching TV?* (Você gosta de assistir TV?)
• ***Do** Anna and Joe undertand the text?* (Anna e John entendem o texto?)
• ***Does** she work at a store?* (Ela trabalha em uma loja?)
• ***Does** Matt speak Mandarin?* (Matt fala mandarim?)
E assim formamos as bases das estruturas do tempo presente na língua inglesa.

**Simple past**
O passado simples no inglês segue uma estrutura ainda mais simplificada do que o próprio presente simples. O auxiliar DID é responsável por formular frases negativas e interrogativas. E os verbos são divididos entre verbos regulares e irregulares.

**Verbos regulares**
Os verbos regulares da língua inglesa possuem uma terminação padrão -ED. No tempo passado, todas as regras se aplicam a todos os sujeitos, sem diferenciação.
• *She lov**ed** the movie.*
• *We learn**ed** a new lamguage.*
• *Joseph cook**ed** a tasty dish.*

**Verbos irregulares**
Os verbos irregulares possuem variações diversas e não seguem uma regra. São, portanto, um tema que precisa de mais atenção e estudo para que a memorização seja efetiva. O uso cotidiano dos verbos pode auxiliar a aprender sua forma no passado, quando verbo irregular. Confira a seguir uma tabela de verbos irregulares em inglês.

| INFINITIVO | PASSADO SIMPLES | SIGNIFICADO |
|---|---|---|
| to arise | arose | erguer, levantar |
| to awake | awoke | acordar, despertar |
| to be | was / were | ser, estar, ficar |
| to bear | bore | suportar, aguentar |
| to beat | beat | bater, espancar, superar, vibrar, palpitar |
| to become | became | tornar-se |
| to begin | began | começar, iniciar |
| to bend | bent | curvar, entortar, franzir, dirigir, desistir |
| to bet | bet | apostar |
| to bid | bade | oferecer, convidar, ordenar, desejar, leiloar |
| to bind | bound | atar, amarrar, obrigar |
| to bite | bit | morder, engolir a isca |
| to bleed | bled | sangrar, perder sangue; |
| to blow | blew | soprar, assobiar, fazer soar |
| to break | broke | quebrar, romper, violar |
| to breed | bred | procriar, gerar, fazer criação, educar, ensinar |
| to buy | bought | comprar |
| to cast | cast | arremessar, jogar, derrubar, moldar |
| to catch | caught | pegar, capturar, entender, adquirir |

Por fim, estabelecemos que uma proposição ou é verdadeira ou é falsa, não havendo mais nenhuma opção, ou seja, excluindo uma nova (como são duas, uma terceira) opção).

**DICA:** Vimos então as principais estruturas lógicas, como lidamos com elas e quais as regras para *jogarmos este jogo*. Então, escreva várias frases, julgue se são proposições ou não e depois tente traduzi-las para a linguagem simbólica que aprendemos.

## LÓGICA DE ARGUMENTAÇÃO: ANALOGIAS, INFERÊNCIAS, DEDUÇÕES E CONCLUSÕES

Quando falamos sobre lógica de argumentação, estamos nos referindo ao processo de argumentar, ou seja, através de argumentos é possível convencer sobre a veracidade de certo assunto.

No entanto, a construção desta argumentação não é necessariamente correta. Veremos alguns casos de argumentação, e como eles podem nos levar a algumas respostas corretas e outras falsas.

**Analogias:** Argumentação pela semelhança (analogamente)
Todo ser humano é mortal
Sócrates é um ser humano
Logo Sócrates é mortal

**Inferências:** Argumentar através da dedução
Se Carlos for professor, haverá aula
Se houve aula, então significa que Carlos é professor, caso contrário, então Carlos não é professor

**Deduções:** Argumentar partindo do todo e indo a uma parte específica
Roraima fica no Brasil
A moeda do Brasil é o Real
Logo, a moeda de Roraima é o Real

**Indução:** É a argumentação oposta a dedução, indo de uma parte específica e chegando ao todo
Todo professor usa jaleco
Todo médico usa jaleco
Então todo professor é médico

Vemos que nem todas as formas de argumentação são verdades universais, contudo, estão estruturadas de forma a parecerem minimamente convincentes. Para isso, devemos diferenciar uma argumentação verdadeira de uma falsa. Quando a argumentação resultar num resultado falso, chamaremos tal argumentação de sofismo[1].

No sofismo temos um encadeamento lógico, no entanto, esse encadeamento se baseia em algumas sutilezas que nos conduzem a resultados falsos. Por exemplo:
A água do mar é feita de água e sal
A bolacha de água e sal é feita de água e sal
Logo, a bolacha de água e sal é feita de mar (ou o mar é feito de bolacha)

Esta argumentação obviamente é falsa, mas está estruturada de forma a parecer verdadeira, principalmente se vista com pressa.

Convidamos você, caro leitor, para refletir sobre outro exemplo de sofismo:
Queijo suíço tem buraco
Quanto mais queijo, mais buraco
Quanto mais buraco, menos queijo
Então quanto mais queijo, menos queijo?

## LÓGICA SENTENCIAL (OU PROPOSICIONAL). PROPOSIÇÕES SIMPLES E COMPOSTAS. TABELAS-VERDADE

A lógica proposicional é baseada justamente nas *proposições* e suas relações. Podemos ter dois tipos de proposições, simples ou composta.

Em geral, uma proposição simples não utiliza conectivos (*e*; *ou*; *se*; *se, e somente se*). Enquanto a proposição composta são duas ou mais proposições (simples) ligadas através destes conectivos.

Mas às vezes uma proposição composta é de difícil análise. "Carlos é professor e a moeda do Brasil é o Real". Se Carlos não for professor e a moeda do Brasil for o real, a proposição composta é verdadeira ou falsa? Temos uma proposição verdadeira e falsa? Como podemos lidar com isso?

A melhor maneira de analisar estas proposições compostas é através de tabelas-verdades.

A *tabela verdade* é montada com todas as possibilidades que uma proposição pode assumir e suas combinações. Se quiséssemos saber sobre uma proposição e sua negativa, teríamos a seguinte tabela verdade:

| p | ~p |
|---|---|
| V | F |
| F | V |

A tabela verdade de uma conjunção (p ^ q) é a seguinte:

| *p* | *q* | p ^ q |
|---|---|---|
| V | V | V |
| V | F | F |
| F | V | F |
| F | F | F |

*1 O termo sofismo vem dos Sofistas, pensadores não alinhados aos movimentos platônico e aristotélico na Grécia dos séculos V e IV AEC, sendo considerados muitas vezes falaciosos por essas linhas de pensamento. Desta forma, o termo sofismo se refere a quando a estrutura foge da lógica tradicional e se obtém uma conclusão falsa.*

I - orientação sobre os procedimentos para a consecução de acesso, bem como sobre o local onde poderá ser encontrada ou obtida a informação almejada;

II - informação contida em registros ou documentos, produzidos ou acumulados por seus órgãos ou entidades, recolhidos ou não a arquivos públicos;

III - informação produzida ou custodiada por pessoa física ou entidade privada decorrente de qualquer vínculo com seus órgãos ou entidades, mesmo que esse vínculo já tenha cessado;

IV - informação primária, íntegra, autêntica e atualizada;

V - informação sobre atividades exercidas pelos órgãos e entidades, inclusive as relativas à sua política, organização e serviços;

VI - informação pertinente à administração do patrimônio público, utilização de recursos públicos, licitação, contratos administrativos; e

VII - informação relativa:

a) à implementação, acompanhamento e resultados dos programas, projetos e ações dos órgãos e entidades públicas, bem como metas e indicadores propostos;

b) ao resultado de inspeções, auditorias, prestações e tomadas de contas realizadas pelos órgãos de controle interno e externo, incluindo prestações de contas relativas a exercícios anteriores.

VIII – (VETADO). (Incluído pela Lei nº 14.345, de 2022)

§ 1º O acesso à informação previsto no caput não compreende as informações referentes a projetos de pesquisa e desenvolvimento científicos ou tecnológicos cujo sigilo seja imprescindível à segurança da sociedade e do Estado.

§ 2º Quando não for autorizado acesso integral à informação por ser ela parcialmente sigilosa, é assegurado o acesso à parte não sigilosa por meio de certidão, extrato ou cópia com ocultação da parte sob sigilo.

§ 3º O direito de acesso aos documentos ou às informações neles contidas utilizados como fundamento da tomada de decisão e do ato administrativo será assegurado com a edição do ato decisório respectivo.

§ 4º A negativa de acesso às informações objeto de pedido formulado aos órgãos e entidades referidas no art. 1º , quando não fundamentada, sujeitará o responsável a medidas disciplinares, nos termos do art. 32 desta Lei.

§ 5º Informado do extravio da informação solicitada, poderá o interessado requerer à autoridade competente a imediata abertura de sindicância para apurar o desaparecimento da respectiva documentação.

§ 6º Verificada a hipótese prevista no § 5º deste artigo, o responsável pela guarda da informação extraviada deverá, no prazo de 10 (dez) dias, justificar o fato e indicar testemunhas que comprovem sua alegação.

Art. 8º É dever dos órgãos e entidades públicas promover, independentemente de requerimentos, a divulgação em local de fácil acesso, no âmbito de suas competências, de informações de interesse coletivo ou geral por eles produzidas ou custodiadas.

§ 1º Na divulgação das informações a que se refere o caput, deverão constar, no mínimo:

I - registro das competências e estrutura organizacional, endereços e telefones das respectivas unidades e horários de atendimento ao público;

II - registros de quaisquer repasses ou transferências de recursos financeiros;

III - registros das despesas;

IV - informações concernentes a procedimentos licitatórios, inclusive os respectivos editais e resultados, bem como a todos os contratos celebrados;

V - dados gerais para o acompanhamento de programas, ações, projetos e obras de órgãos e entidades; e

VI - respostas a perguntas mais frequentes da sociedade.

§ 2º Para cumprimento do disposto no caput, os órgãos e entidades públicas deverão utilizar todos os meios e instrumentos legítimos de que dispuserem, sendo obrigatória a divulgação em sítios oficiais da rede mundial de computadores (internet).

§ 3º Os sítios de que trata o § 2º deverão, na forma de regulamento, atender, entre outros, aos seguintes requisitos:

I - conter ferramenta de pesquisa de conteúdo que permita o acesso à informação de forma objetiva, transparente, clara e em linguagem de fácil compreensão;

II - possibilitar a gravação de relatórios em diversos formatos eletrônicos, inclusive abertos e não proprietários, tais como planilhas e texto, de modo a facilitar a análise das informações;

III - possibilitar o acesso automatizado por sistemas externos em formatos abertos, estruturados e legíveis por máquina;

IV - divulgar em detalhes os formatos utilizados para estruturação da informação;

V - garantir a autenticidade e a integridade das informações disponíveis para acesso;

VI - manter atualizadas as informações disponíveis para acesso;

VII - indicar local e instruções que permitam ao interessado comunicar-se, por via eletrônica ou telefônica, com o órgão ou entidade detentora do sítio; e

VIII - adotar as medidas necessárias para garantir a acessibilidade de conteúdo para pessoas com deficiência, nos termos do art. 17 da Lei nº 10.098, de 19 de dezembro de 2000, e do art. 9º da Convenção sobre os Direitos das Pessoas com Deficiência, aprovada pelo Decreto Legislativo nº 186, de 9 de julho de 2008.

§ 4º Os Municípios com população de até 10.000 (dez mil) habitantes ficam dispensados da divulgação obrigatória na internet a que se refere o § 2º , mantida a obrigatoriedade de divulgação, em tempo real, de informações relativas à execução orçamentária e financeira, nos critérios e prazos previstos no art. 73-B da Lei Complementar nº 101, de 4 de maio de 2000 (Lei de Responsabilidade Fiscal).

Art. 9º O acesso a informações públicas será assegurado mediante:

I - criação de serviço de informações ao cidadão, nos órgãos e entidades do poder público, em local com condições apropriadas para:

a) atender e orientar o público quanto ao acesso a informações;

b) informar sobre a tramitação de documentos nas suas respectivas unidades;

c) protocolizar documentos e requerimentos de acesso a informações; e

II - realização de audiências ou consultas públicas, incentivo à participação popular ou a outras formas de divulgação.

§ 2º A decisão de reconhecimento de que trata o caput será precedida de publicação de extrato da informação, com descrição resumida do assunto, origem e período do conjunto de documentos a serem considerados de acesso irrestrito, com antecedência de no mínimo trinta dias.

§ 3º Após a decisão de reconhecimento de que trata o § 2º , os documentos serão considerados de acesso irrestrito ao público.

§ 4º Na hipótese de documentos de elevado valor histórico destinados à guarda permanente, caberá ao dirigente máximo do Arquivo Nacional, ou à autoridade responsável pelo arquivo do órgão ou entidade pública que os receber, decidir, após seu recolhimento, sobre o reconhecimento, observado o procedimento previsto neste artigo.

Art. 60. O pedido de acesso a informações pessoais observará os procedimentos previstos no Capítulo IV e estará condicionado à comprovação da identidade do requerente.

Parágrafo único. O pedido de acesso a informações pessoais por terceiros deverá ainda estar acompanhado de:

I - comprovação do consentimento expresso de que trata o inciso II do caput do art. 55, por meio de procuração;

II - comprovação das hipóteses previstas no art. 58;

III - demonstração do interesse pela recuperação de fatos históricos de maior relevância, observados os procedimentos previstos no art. 59; ou

IV - demonstração da necessidade do acesso à informação requerida para a defesa dos direitos humanos ou para a proteção do interesse público e geral preponderante.

Art. 61. O acesso à informação pessoal por terceiros será condicionado à assinatura de um termo de responsabilidade, que disporá sobre a finalidade e a destinação que fundamentaram sua autorização, sobre as obrigações a que se submeterá o requerente.

§ 1º A utilização de informação pessoal por terceiros vincula-se à finalidade e à destinação que fundamentaram a autorização do acesso, vedada sua utilização de maneira diversa.

§ 2º Aquele que obtiver acesso às informações pessoais de terceiros será responsabilizado por seu uso indevido, na forma da lei.

Art. 62. Aplica-se, no que couber, a Lei nº 9.507, de 12 de novembro de 1997, em relação à informação de pessoa, natural ou jurídica, constante de registro ou banco de dados de órgãos ou entidades governamentais ou de caráter público.

## CAPÍTULO VIII
## DAS ENTIDADES PRIVADAS SEM FINS LUCRATIVOS

Art. 63. As entidades privadas sem fins lucrativos que receberem recursos públicos para realização de ações de interesse público deverão dar publicidade às seguintes informações:

I - cópia do estatuto social atualizado da entidade;

II - relação nominal atualizada dos dirigentes da entidade; e

III - cópia integral dos convênios, contratos, termos de parcerias, acordos, ajustes ou instrumentos congêneres realizados com o Poder Executivo federal, respectivos aditivos, e relatórios finais de prestação de contas, na forma da legislação aplicável.

§ 1º As informações de que trata o caput serão divulgadas em sítio na Internet da entidade privada e em quadro de avisos de amplo acesso público em sua sede.

§ 2º A divulgação em sítio na Internet referida no §1º poderá ser dispensada, por decisão do órgão ou entidade pública, e mediante expressa justificação da entidade, nos casos de entidades privadas sem fins lucrativos que não disponham de meios para realizá-la.

§ 3º As informações de que trata o caput deverão ser publicadas a partir da celebração do convênio, contrato, termo de parceria, acordo, ajuste ou instrumento congênere, serão atualizadas periodicamente e ficarão disponíveis até cento e oitenta dias após a entrega da prestação de contas final.

Art. 64. Os pedidos de informação referentes aos convênios, contratos, termos de parcerias, acordos, ajustes ou instrumentos congêneres previstos no art. 63 deverão ser apresentados diretamente aos órgãos e entidades responsáveis pelo repasse de recursos.

Parágrafo único . (Revogado pelo Decreto nº 11.527, de 2023)

Art. 64-A. As entidades com personalidade jurídica de direito privado constituídas sob a forma de serviço social autônomo, que sejam destinatárias de contribuições ou de recursos públicos federais decorrentes de contrato de gestão, e os conselhos de fiscalização profissional deverão observar o disposto na Lei nº 12.527, de 2011, e: (Redação dada pelo Decreto nº 11.527, de 2023)

I - divulgar, independentemente de requerimento, as informações de interesse coletivo ou geral por eles produzidas ou custodiadas, inclusive aquelas a que se referem os incisos I a VIII do § 3º do art. 7º, em local de fácil visualização, em sítios eletrônicos oficiais, observado o disposto no § 1º do art. 7º e no art. 8º; e (Incluído pelo Decreto nº 11.527, de 2023)

II - criar SIC, observado o disposto nos art. 9º e art. 10. (Incluído pelo Decreto nº 11.527, de 2023)

§ 1º As informações previstas no inciso I do caput devem ser fornecidas diretamente pelas entidades e pelos conselhos de que trata o caput e referem-se à parcela dos recursos provenientes das contribuições e dos demais recursos públicos recebidos e à sua destinação, sem prejuízo das prestações de contas a que estejam legalmente obrigadas. (Redação dada pelo Decreto nº 11.527, de 2023)

§ 2º Aplica-se o disposto nos art. 55 e art. 58 às informações pessoais relativas à intimidade, à vida privada, à honra e à imagem detidas pelas entidades e pelos conselhos de que trata o caput. (Redação dada pelo Decreto nº 11.527, de 2023)

§ 3º A divulgação das informações previstas no inciso I do caput não exclui outras hipóteses de publicação e divulgação de informações previstas na legislação, inclusive na Lei de Diretrizes Orçamentárias. (Redação dada pelo Decreto nº 11.527, de 2023)

§ 4º O sistema recursal e de monitoramento deste Decreto não se aplica às entidades e aos conselhos de que trata o caput, salvo quanto à possibilidade de o requerente, no caso de omissão de resposta ao pedido de acesso à informação, apresentar a reclamação prevista no art. 22, que será encaminhada à autoridade máxima da entidade ou do conselho demandado. (Incluído pelo Decreto nº 11.527, de 2023)

§ 5º As entidades de que trata o caput estão sujeitas, no que couber, às sanções e aos procedimentos previstos no art. 66. (Incluído pelo Decreto nº 11.527, de 2023)

Art. 64-B . (Revogado pelo Decreto nº 11.527, de 2023)

Parágrafo único. (Revogado pelo Decreto nº 11.527, de 2023)

Art. 64-C (Revogado pelo Decreto nº 11.527, de 2023)

IV - áreas prioritárias - áreas definidas no Plano Nacional de Segurança de Infraestruturas Críticas para a aplicação da Política Nacional de Segurança de Infraestruturas Críticas, nos termos do disposto no inciso I do caput do art. 9º do Anexo ao Decreto nº 9.573, de 2018;

V - incidente cibernético - ocorrência que comprometa, real ou potencialmente, a disponibilidade, a integridade, a confidencialidade ou a autenticidade de sistema de informação ou das informações processadas, armazenadas ou transmitidas por esse sistema, que poderá também ser caracterizada pela tentativa de exploração de vulnerabilidade de sistema de informação que constitua violação de norma, política de segurança, procedimento de segurança ou política de uso;

VI - plano de gestão de incidentes cibernéticos para a administração pública federal - plano que orienta as equipes dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional, exceto das agências reguladoras, do Banco Central do Brasil e da Comissão Nacional de Energia Nuclear, sobre a coordenação de atividades referentes à prevenção, ao tratamento e à resposta a incidentes cibernéticos; e

VII - planos setoriais de gestão de incidentes cibernéticos - planos que orientam as equipes nas agências reguladoras, no Banco Central do Brasil, na Comissão Nacional de Energia Nuclear ou nas suas entidades reguladas sobre a coordenação de atividades referentes à prevenção, ao tratamento e à resposta a incidentes cibernéticos inerentes ao setor específico.

## CAPÍTULO II
## DA COMPOSIÇÃO

Art. 5º A Rede Federal de Gestão de Incidentes Cibernéticos será composta pelo Gabinete de Segurança Institucional da Presidência da República, pelos órgãos e pelas entidades da administração pública federal direta, autárquica e fundacional e, observado o disposto nos § 2º do art. 1º, pelas empresas públicas e sociedades de economia mista e pelas suas subsidiárias que aderirem à Rede.

§ 1º O Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República coordenará a Rede Federal de Gestão de Incidentes Cibernéticos por meio do Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo.

§ 2º Os órgãos e as entidades da administração pública federal direta, autárquica e fundacional atuarão na Rede Federal de Gestão de Incidentes Cibernéticos por meio das suas equipes de prevenção, tratamento e resposta a incidentes cibernéticos, nos termos do disposto nos inciso I a III do caput do art. 4º.

§ 3º Observado o interesse do Estado em relação à segurança cibernética nacional, outras entidades públicas ou privadas poderão ser convidadas pelo Gabinete de Segurança Institucional da Presidência da República para integrar a Rede Federal de Gestão de Incidentes Cibernéticos, por meio de ofício, desde que cumpridos os requisitos de que trata o art. 7º.

Art. 6º No âmbito do Ministério da Defesa e das Forças Singulares, a articulação com o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo será feita prioritariamente por meio da equipe de coordenação setorial, operada pelo Comando de Defesa Cibernética, na condição de órgão central do Sistema Militar de Defesa Cibernética.

§ 1º Excepcionalmente, as equipes de prevenção, tratamento e resposta a incidentes cibernéticos do Ministério da Defesa e das Forças Singulares poderão articular-se diretamente com o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo, hipótese em que deverão informar a equipe de coordenação setorial do Ministério da Defesa.

§ 2º As informações compartilhadas pelas equipes de prevenção, tratamento e resposta a incidentes cibernéticos de que trata o § 1º com o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo observarão as restrições legais de acesso a dados em razão das necessidades de segurança do Estado.

Art. 7º A adesão das entidades de que trata o § 2º do art. 1º será formalizada por ato do dirigente máximo do órgão da administração pública federal direta ao qual estejam vinculadas ou subordinadas.

§ 1º Quando da elaboração do ato de que trata o caput, o órgão da administração pública federal direta avaliará se há necessidade de dispor sobre requisitos adicionais às normas de segurança da informação estabelecidas pelo Gabinete de Segurança Institucional da Presidência da República em decorrência das atividades desenvolvidas pelas entidades de que trata o § 2º do art. 1º, principalmente quando essas atividades estiverem relacionadas com infraestrutura crítica.

§ 2º As entidades de que trata o § 2º do art. 1º que solicitarem a adesão à Rede Federal de Gestão de Incidentes Cibernéticos deverão cumprir os seguintes requisitos para serem aprovadas pelo Gabinete de Segurança Institucional da Presidência da República:

I - possuir equipe de prevenção, tratamento e resposta a incidentes cibernéticos implementada de acordo com as normas de segurança da informação estabelecidas pelo Gabinete de Segurança Institucional da Presidência da República; e

II - encaminhar ao Gabinete de Segurança Institucional da Presidência da República, por meio de sua equipe de prevenção, tratamento e resposta a incidentes cibernéticos ou de sua equipe de coordenação setorial, termo de adesão à Rede Federal de Gestão de Incidentes Cibernéticos assinado pelo dirigente máximo ou representante legal.

§ 3º A adesão à Rede Federal de Gestão de Incidentes Cibernéticos dependerá da aprovação formal pelo Gabinete de Segurança Institucional da Presidência da República, que poderá recusá-la motivadamente, mesmo que tenham sido cumpridos os requisitos estabelecidos neste artigo.

§ 4º O disposto neste artigo se aplica, no que couber, a outras pessoas jurídicas de direito privado e às pessoas jurídicas de direito público interno de outros Poderes e entes federativos que forem convidadas pelo Gabinete de Segurança Institucional da Presidência da República para integrar a Rede Federal de Gestão de Incidentes Cibernéticos.

§ 5º A colaboração espontânea, caso a caso, das entidades de que trata o § 2º do art. 1º com o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo ou com quaisquer de seus integrantes independerá da adesão à Rede Federal de Gestão de Incidentes Cibernéticos.

Art. 8º As pessoas jurídicas que não pertencerem à administração pública federal direta, autárquica e fundacional e que tiverem firmado termo de adesão com o Gabinete de Segurança Institucional da Presidência da República para integrar a Rede Federal de Gestão de Incidentes Cibernéticos deverão reportar-se à

CRIPTOGRAFIA BASEADA NA IDENTIDADE (IBE) - também conhecida por criptografia baseada em identidade (identity-based encryption), trata-se de um tipo de criptografia de chave pública, no qual um usuário pode gerar uma chave pública a partir de um identificador único conhecido (como por exemplo um endereço dee-mail), em que um servidor confiável de terceiros calcula a chave privada correspondente, a partir da chave pública. Dessa forma, não há necessidade de distribuir chaves públicas antes da troca de dados criptografados;

CRIPTOGRAFIA DE CHAVE PÚBLICA - também conhecida como criptografia assimétrica, é qualquer sistema criptográfico que usa pares de chaves: chaves públicas, que podem ser amplamente disseminadas, e chaves privadas, que são conhecidas apenas pelo proprietário. Isto realiza duas funções: autenticação, em que a chave pública verifica se um portador da chave privada aparelhada enviou a mensagem; e encriptação, em que apenas o portador da chave privada aparelhada pode decriptar a mensagem encriptada com a chave pública;

CROSS-SITE SCRIPTING(XSS) - método de ataque que explora vulnerabilidades descriptingentresites, que visa contornar controles de acesso, como a política de mesma origem. Ao injetar umscriptmalicioso em uma entrada desprotegida ou não validada do navegador, o invasor faz com que oscriptseja devolvido pelo aplicativo e executado no navegador. Um ataque XSS bem-sucedido pode permitir ao invasor assumir o controle das funcionalidades do aplicativo, manipular dados ou implantar códigos maliciosos adicionais. Os ataques XSS também permitem que os invasores injetemscriptsdo lado do cliente, em páginas dawebvisualizadas por outros usuários;

CSA - sigla decloud security alliance;

CSIRT (COMPUTER SECURITY INCIDENT RESPONSE TEAM) - sigla internacional para designar um grupo de resposta a incidentes de segurança, responsável por tratar incidentes de segurança para um público alvo específico;

CTIR GOV - Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo, subordinado ao Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República;

CUSTÓDIA - consiste na responsabilidade de guardar um ativo para terceiros. A custódia não permite automaticamente o acesso ao ativo e nem o direito de conceder acesso a outros;

CUSTODIANTE - aquele que, de alguma forma, total ou parcialmente, zela pelo armazenamento, operação, administração e preservação de um sistema estruturante, ou dos ativos de informação que compõem o sistema de informação, que não lhe pertence, mas que está sob sua custódia;

CUSTODIANTE DA INFORMAÇÃO - qualquer indivíduo ou estrutura de órgão ou entidade da administração pública federal, direta e indireta, que tenha responsabilidade formal de proteger a informação e aplicar os níveis de controles de segurança, em conformidade com as exigências de segurança da informação, comunicadas pelo proprietário da informação;

CVE - sigla decommon vulnerabilities and exposures;

Letra D

DADO ANONIMIZADO - dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

DADO EM REPOUSO - informação armazenada. A proteção dos dados em repouso não deve ser subestimada, pois informações valiosas podem não ser transmitidas por canais de comunicação, mas apenas serem imóveis;

DADO PESSOAL - informação relacionada à pessoa natural identificada ou identificável;

DADO PESSOAL SENSÍVEL - dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

DADOS PROCESSADOS - dados submetidos a qualquer operação ou tratamento, por meio de processamento eletrônico ou por meio automatizado, com o emprego de tecnologia da informação;

DATAGRAMA (PACOTE DE DADOS) - trata-se de dados encapsulados, ou seja, dados aos quais são acrescentados cabeçalhos com informações sobre o seu transporte (como o endereço IP de destino). Os dados contidos nos datagramas são analisados e eventualmente alterados pelosswitches(roteadores) que permitem o seu trânsito. Os dados circulam na Internet na forma de datagramas;

DC - sigla de documento controlado;

DDoS - sigla de negação de serviço distribuída (distributed denial of service);

DECIFRAÇÃO - ato de decifrar, mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para reverter processo de cifração original;

DEEPFAKE- forma de vídeo manipulado, utilizando técnicas de síntese de imagem humana, que criam renderizações artificiais hiper-realistas de um ser humano. Esses vídeos geralmente são criados pela mistura de um vídeo já existente com novas imagens, áudio e vídeo, para criar a ilusão da fala. Esse processo é realizado por meio de redes contraditórias generativas (GAN). A consequência mais perigosa da popularidade dosdeepfakesé que eles podem facilmente convencer as pessoas a acreditarem em uma determinada história ou teoria, o que pode resultar em comportamentos com grande impacto na vida política, social ou financeira;

DEFESA CIBERNÉTICA - ações realizadas no espaço cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com as finalidades de proteger os ativos de informação de interesse da defesa nacional, obter dados para a produção de conhecimento de inteligência e buscar superioridade sobre os sistemas de informação do oponente;

DESASTRE - evento, ação ou omissão, repentino e não planejado, que tenha permitido acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica, gerando sérios impactos em sua capacidade de entregar serviços essenciais ou críticos por um período de tempo superior ao tempo objetivo de recuperação;

DESCARTE - eliminação correta de informações, documentos, mídias e acervos digitais;

**GABARITO**

| | |
|---|---|
| 1 | CERTO |
| 2 | CERTO |
| 3 | ERRADO |
| 4 | ERRADO |
| 5 | C |
| 6 | D |
| 7 | E |
| 8 | D |
| 9 | B |
| 10 | B |
| 11 | C |
| 12 | C |
| 13 | C |
| 14 | B |
| 15 | A |
| 16 | E |
| 17 | E |
| 18 | C |
| 19 | A |
| 20 | C |

## ANOTAÇÕES