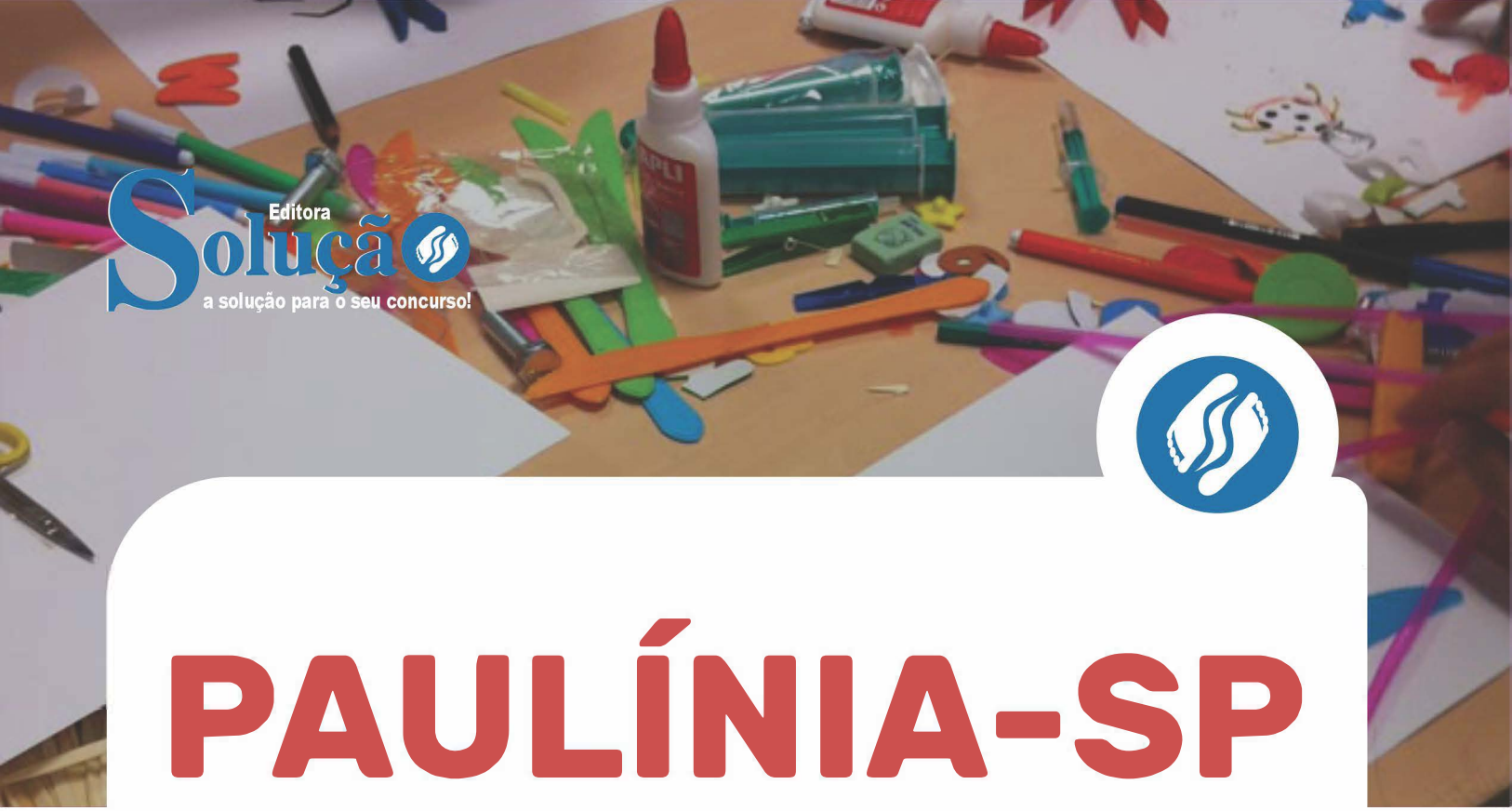

Editora Soluçã
a solução para o seu concurso!

PAULÍNIA-SP

PREFEITURA MUNICIPAL DE PAULÍNIA - SÃO PAULO

PROFESSOR DE EDUCAÇÃO BÁSICA - PEB II - ARTE

- Língua Portuguesa
- Raciocínio Lógico
- Conhecimentos Educacionais
- Conhecimentos Específicos

INCLUI QUESTÕES GABARITADAS

EDITAL DE ABERTURA Nº 001/2026

BÔNUS
ÁREA DO CONCURSEIRO

- **Português**: Ortografia, Fonologia, Acentuação Gráfica, Concordância, Regência, Crase e Pontuação.
- **Informática:** Computação na Nuvem, Armazenamento em Nuvem, Intranet, Internet, Conceitos, Protocolos e Segurança da informação.

41 ANOS
A SOLUÇÃO PARA O SEU CONCURSO

AVISO IMPORTANTE:

Este é um Material de Demonstração

Este arquivo é apenas uma amostra do conteúdo completo da Apostila.

Aqui você encontrará algumas páginas selecionadas para que possa conhecer a qualidade, estrutura e metodologia do nosso material. No entanto, esta não é a apostila completa.

POR QUE INVESTIR NA APOSTILA COMPLETA?

- Conteúdo totalmente alinhado ao edital
- Teoria clara, objetiva e sempre atualizada
- Questões gabaritadas
- Diferentes práticas que otimizam seus estudos

Ter o material certo em mãos transforma sua preparação e aproxima você da APROVAÇÃO.

Garanta agora o acesso completo e aumente suas chances de aprovação:
https://www.editorasolucao.com.br/

Editora Solução
a solução para o seu concurso!

TRANSPETRO

PETROBRAS TRANSPORTE S.A

Análise de Sistemas – Segurança Cibernética e da Informação

COM BASE NO EDITAL Nº 02 – TRANSPETRO/PSP/ TERRA/NÍVELSUPERIOR-2023.2

CÓD: SL-206JL-26
7901183003938

Língua Portuguesa

Língua Inglesa

Segurança Ofensiva

Segurança Defensiva

Compliance de Segurança e Privacidade

LÍNGUA PORTUGUESA

COMPREENSÃO DE TEXTOS

A compreensão e a interpretação de textos são habilidades essenciais para que a comunicação alcance seu objetivo de forma eficaz. Em diversos contextos, como na leitura de livros, artigos, propagandas ou imagens, é necessário que o leitor seja capaz de entender o conteúdo proposto e, além disso, atribuir significados mais amplos ao que foi lido ou visto.

Para isso, é importante distinguir os conceitos de compreensão e interpretação, bem como reconhecer que um texto pode ser verbal (composto por palavras) ou não-verbal (constituído por imagens, símbolos ou outros elementos visuais).

Compreender um texto implica decodificar sua mensagem explícita, ou seja, captar o que está diretamente apresentado. Já a interpretação vai além da compreensão, exigindo que o leitor utilize seu repertório pessoal e conhecimentos prévios para gerar um sentido mais profundo do texto. Dessa forma, dominar esses dois processos é essencial não apenas para a leitura cotidiana, mas também para o desempenho em provas e concursos, onde a análise de textos e imagens é frequentemente exigida.

Essa distinção entre compreensão e interpretação é crucial, pois permite ao leitor ir além do que está explícito, alcançando uma leitura mais crítica e reflexiva.

Conceito de Compreensão

A compreensão de um texto é o ponto de partida para qualquer análise textual. Ela representa o processo de decodificação da mensagem explícita , ou seja, a habilidade de extrair informações diretamente do conteúdo apresentado pelo autor, sem a necessidade de agregar inferências ou significados subjetivos. Quando compreendemos um texto, estamos simplesmente absorvendo o que está dito de maneira clara, reconhecendo os elementos essenciais da comunicação, como o tema , os fatos e os argumentos centrais.

▸ A Compreensão em Textos Verbais

Nos textos verbais , que utilizam a linguagem escrita ou falada como principal meio de comunicação, a compreensão passa pela habilidade de ler com atenção e reconhecer as estruturas linguísticas. Isso inclui:

- **Vocabulário :** O entendimento das palavras usadas no texto é fundamental. Palavras desconhecidas podem comprometer a compreensão, tornando necessário o uso de dicionários ou ferramentas de pesquisa para esclarecer o significado.
- **Sintaxe:** A maneira como as palavras estão organizadas em frases e parágrafos também influencia o processo de compreensão. Sentenças complexas, inversões sintáticas ou o uso de conectores como conjunções e preposições requerem atenção redobrada para garantir que o leitor compreenda as relações entre as ideias.
- **Coesão e coerência:** são dois pilares essenciais da compreensão. Um texto coeso é aquele cujas ideias estão bem conectadas, e a coerência se refere à lógica interna do texto, onde as ideias se articulam de maneira fluida e compreensível.

Ao realizar a leitura de um texto verbal, a compreensão exige a decodificação de todas essas estruturas. É a partir dessa leitura atenta e detalhada que o leitor poderá garantir que absorveu o conteúdo proposto pelo autor de forma plena.

▸ A Compreensão em Textos Não-Verbais

Além dos textos verbais, a compreensão se estende aos textosnão-verbais , que utilizam símbolos, imagens, gráficos ou outras representações visuais para transmitir uma mensagem. Exemplos de textos não-verbais incluem obras de arte, fotografias, infográficos e até gestos em uma linguagem de sinais.

A compreensão desses textos exige uma leitura visual aguçada, na qual o observador decodifica os elementos presentes, como:

- **Cores:** As cores desempenham um papel comunicativo importante em muitos contextos, evocando emoções ou sugerindo informações adicionais. Por exemplo, em um gráfico, cores diferentes podem representar categorias distintas de dados.
- **Formas e símbolos:** Cada forma ou símbolo em um texto visual pode carregar um significado próprio, como sinais de trânsito ou logotipos de marcas. A correta interpretação desses elementos depende do conhecimento prévio do leitor sobre seu uso.
- **Gestos e expressões:** Em um contexto de comunicação corporal, como na linguagem de sinais ou em uma apresentação oral acompanhada de gestos, a compreensão se dá ao identificar e entender as nuances de cada movimento.

▸ Fatores que Influenciam a Compreensão

A compreensão, seja de textos verbais ou não-verbais, pode ser afetada por diversos fatores, entre eles:

- **Conhecimento prévio:** Quanto mais familiarizado o leitor estiver com o tema abordado, maior será sua capacidade de compreender o texto. Por exemplo, um leitor que já conhece o contexto histórico de um fato poderá compreender melhor uma notícia sobre ele.

▪ **Contexto:** O ambiente ou a situação em que o texto é apresentado também influencia a compreensão. Um texto jornalístico, por exemplo, traz uma mensagem diferente dependendo de seu contexto histórico ou social.

▪ **Objetivos da leitura:** O propósito com o qual o leitor aborda o texto impacta a profundidade da compreensão. Se a leitura for para estudo, o leitor provavelmente será mais minucioso do que em uma leitura por lazer.

▸ **Compreensão como Base para a Interpretação**

A compreensão é o primeiro passo no processo de leitura e análise de qualquer texto. Sem uma compreensão clara e objetiva, não é possível seguir para uma etapa mais profunda, que envolve a interpretação e a formulação de inferências. Somente após a decodificação do que está explicitamente presente no texto, o leitor poderá avançar para uma análise mais subjetiva e crítica, onde ele começará a trazer suas próprias ideias e reflexões sobre o que foi lido.

A compreensão textual é um processo que envolve a decodificação de elementos verbais e não-verbais, permitindo ao leitor captar a mensagem essencial do conteúdo. Ela exige atenção, familiaridade com as estruturas linguísticas ou visuais e, muitas vezes, o uso de recursos complementares, como dicionários. Ao dominar a compreensão, o leitor cria uma base sólida para interpretar textos de maneira mais profunda e crítica.

Textos Verbais e Não-Verbais

Na comunicação, os textos podem ser classificados em duas categorias principais:verbais e não-verbais . Cada tipo de texto utiliza diferentes recursos e linguagens para transmitir suas mensagens, sendo fundamental que o leitor ou observador saiba identificar e interpretar corretamente as especificidades de cada um.

▸ **Textos Verbais**

Os textos verbais são aqueles constituídos pela linguagem escrita ou falada, onde as palavras são o principal meio de comunicação. Eles estão presentes em inúmeros formatos, como livros, artigos, notícias, discursos, entre outros. A linguagem verbal se apoia em uma estrutura gramatical, com regras que organizam as palavras e frases para transmitir a mensagem de forma coesa e compreensível.

Características dos Textos Verbais:

▪ **Estrutura Sintática:** As frases seguem uma ordem gramatical que facilita a decodificação da mensagem.

▪ **Uso de Palavras:** As palavras são escolhidas com base em seu significado e função dentro do texto, permitindo ao leitor captar as ideias expressas.

▪ **Coesão e Coerência:** A conexão entre frases, parágrafos e ideias deve ser clara, para que o leitor compreenda a linha de raciocínio do autor.

Exemplos de textos verbais incluem:

▪ **Livros e artigos:** Onde há um desenvolvimento contínuo de ideias, apoiado em argumentos e explicações detalhadas.

▪ **Diálogos e conversas:** Que utilizam a oralidade para interações mais diretas e dinâmicas.

▪ **Panfletos e propagandas:** Usam a linguagem verbal de forma concisa e direta para transmitir uma mensagem específica.

A compreensão de um texto verbal envolve a decodificação de palavras e a análise de como elas se conectam para construir significado. É essencial que o leitor identifique o tema, os argumentos centrais e as intenções do autor, além de perceber possíveis figuras de linguagem ou ambiguidades.

▸ **Textos Não-Verbais**

Os textos não-verbais utilizam elementos visuais para se comunicar, como imagens, símbolos, gestos, cores e formas. Embora não usem palavras diretamente, esses textos transmitem mensagens completas e são amplamente utilizados em contextos visuais, como artes visuais, placas de sinalização, fotografias, entre outros.

Características dos Textos Não-Verbais:

▪ **Imagens e símbolos:** Carregam significados culturais e contextuais que devem ser reconhecidos pelo observador.

▪ **Cores e formas:** Podem ser usadas para evocar emoções ou destacar informações específicas. Por exemplo, a cor vermelha em muitos contextos pode representar perigo ou atenção.

▪ **Gestos e expressões:** Na comunicação corporal, como na linguagem de sinais ou na expressão facial, o corpo desempenha o papel de transmitir a mensagem.

Exemplos de textos não-verbais incluem:

▪ **Obras de arte:** Como pinturas ou esculturas, que comunicam ideias, emoções ou narrativas através de elementos visuais.

▪ **Sinais de trânsito:** Que utilizam formas e cores para orientar os motoristas, dispensando a necessidade de palavras.

▪ **Infográficos:** Combinações de gráficos e imagens que transmitem informações complexas de forma visualmente acessível.

A interpretação de textos não-verbais exige uma análise diferente da dos textos verbais. É necessário entender os códigos visuais que compõem a mensagem, como as cores, a composição das imagens e os elementos simbólicos utilizados. Além disso, o contexto cultural é crucial, pois muitos símbolos ou gestos podem ter significados diferentes dependendo da região ou da sociedade em que são usados.

▸ **Relação entre Textos Verbais e Não-Verbais**

Embora sejam diferentes em sua forma, textos verbais e não-verbais frequentemente se complementam. Um exemplo comum são as propagandas publicitárias , que utilizam tanto textos escritos quanto imagens para reforçar a mensagem. Nos livros ilustrados , as imagens acompanham o texto verbal, ajudando a criar um sentido mais completo da história ou da informação.

LÍNGUA INGLESA

COMPREENSÃO DE TEXTO ESCRITO EM LÍNGUA INGLESA

A compreensão e interpretação de textos em língua inglesa vão muito além da simples tradução de palavras. Esse processo envolve a capacidade de entender o significado global do texto, reconhecer relações entre suas partes e identificar como ele dialoga com outros textos e contextos. Para que isso ocorra de forma eficiente, é fundamental desenvolver tanto o domínio do vocabulário e da estrutura da língua quanto a habilidade de perceber relações intratextuais e intertextuais.

O processo de leitura em inglês requer não apenas o reconhecimento de palavras isoladas, mas a capacidade de entender como essas palavras se organizam para construir significados complexos. Além disso, é essencial que o leitor consiga identificar relações internas no texto, como a coesão entre parágrafos e a progressão de ideias, bem como conexões externas, que envolvem referências a outros textos, contextos históricos, culturais ou literários.

A seguir, o tema será explorado em três partes: o domínio do vocabulário e da estrutura da língua, as relações intratextuais e a intertextualidade no processo de leitura.

Domínio do vocabulário e da estrutura da língua

O primeiro passo para uma compreensão eficaz de textos em inglês é o domínio do vocabulário. O vocabulário pode ser dividido em dois tipos principais:

- **Active vocabulary (vocabulário ativo):** composto por palavras que o leitor é capaz de usar em sua própria produção oral e escrita.
- **Passive vocabulary (vocabulário passivo):** formado por palavras que o leitor reconhece e compreende quando encontra em um texto, mas que pode não usar com frequência em suas próprias falas ou escritas.

Para interpretar textos com precisão, é necessário ampliar o vocabulário passivo, pois ele representa uma grande parte das palavras encontradas em leituras acadêmicas, jornalísticas, literárias e técnicas. Estratégias como a leitura regular de diferentes tipos de textos, o uso de flashcards, a prática de contextos de uso e o estudo de sinônimos e antônimos ajudam a expandir esse repertório.

Além do vocabulário isolado, é fundamental compreender o uso de expressões idiomáticas (idiomatic expressions), phrasal verbs, collocations (combinações de palavras que ocorrem naturalmente) e false cognates (falsos cognatos), que podem levar a interpretações equivocadas se não forem bem conhecidos. Por exemplo, o termo “actually” em inglês significa “na verdade” e não “atualmente”, o que é um erro comum entre estudantes de inglês.

O domínio da estrutura da língua (grammar structures) também é essencial. Isso inclui o conhecimento de tempos verbais (verb tenses), vozes ativa e passiva (active and passive voice), uso de modais (modal verbs), estruturas condicionais (conditional sentences) e conjunções (conjunctions) que conectam ideias. A compreensão da gramática permite que o leitor identifique o papel de cada elemento no texto, facilitando a interpretação de informações implícitas e explícitas.

Por exemplo, ao ler a frase “If I had known about the meeting, I would have attended,” o leitor deve reconhecer que se trata de uma third conditional sentence, que expressa uma situação hipotética no passado, indicando que o falante não sabia da reunião e, portanto, não compareceu. Esse entendimento é crucial para interpretar o significado além das palavras individuais.

O conhecimento gramatical também contribui para a identificação de referências anafóricas e catafóricas (quando um pronome ou termo faz referência a algo já mencionado ou que será mencionado no texto), o que é fundamental para manter a coesão e entender como as ideias se relacionam.

Assim, o domínio do vocabulário e da estrutura gramatical da língua inglesa é o alicerce para uma leitura eficiente, permitindo que o leitor vá além da decodificação de palavras para compreender o significado completo do texto.

Relações intratextuais: coesão e coerência no texto

As relações intratextuais referem-se à maneira como as ideias e informações estão conectadas dentro do próprio texto. Isso envolve mecanismos de coesão e coerência, que garantem a fluidez da leitura e a clareza das ideias.

A coesão textual é construída por meio de elementos linguísticos que criam ligações entre frases, parágrafos e seções do texto. Os principais recursos de coesão incluem:

- **Conjunctions and linking words (conjunções e palavras de ligação):** termos como “however,” “therefore,” “although,” “in addition” ajudam a estabelecer relações de causa e efeito, contraste, adição, etc.
- **Reference words (pronomes e expressões referenciais):** pronomes como “he,” “she,” “it,” “this,” “that” mantêm a continuidade do texto, referindo-se a elementos mencionados anteriormente.
- **Substitution and ellipsis (substituição e elipse)**: permitem evitar repetições desnecessárias, substituindo termos ou omitindo partes do texto que são facilmente inferíveis.
- **Lexical cohesion (coesão lexical):** uso de sinônimos, antônimos e termos relacionados semanticamente para reforçar o tema e criar unidade no texto.

Por exemplo, em um texto sobre o meio ambiente, termos como “pollution,” “contamination,” “environmental damage,” e “ecosystem degradation” criam coesão lexical ao abordar o mesmo campo semântico.

A coerência textual, por sua vez, está relacionada ao sentido global do texto. Um texto coerente apresenta ideias organizadas de forma lógica, com progressão temática clara e relações de causa, consequência e temporalidade bem definidas. A coerência depende não apenas da estrutura do texto, mas também do conhecimento prévio do leitor, que deve ser capaz de relacionar as informações apresentadas com seus próprios conhecimentos e experiências.

Por exemplo, ao ler um texto que começa com “Global warming has severe impacts on biodiversity” e continua explicando como o aumento da temperatura afeta espécies animais e vegetais, o leitor espera que o texto mantenha essa linha de raciocínio, apresentando exemplos, causas e possíveis soluções para o problema. Se o texto mudar abruptamente para um tema sem relação, a coerência será comprometida.

Entender as relações intratextuais é fundamental para interpretar textos em inglês de forma eficaz, pois permite identificar como as informações estão organizadas e como cada parte contribui para o todo.

Intertextualidade no processo de leitura

A intertextualidade refere-se à relação entre diferentes textos. Trata-se da capacidade de reconhecer como um texto faz referência a outros textos, obras, eventos históricos, contextos culturais ou até mesmo a discursos sociais amplos. Esse fenômeno é comum em textos literários, jornalísticos, publicitários e acadêmicos, e sua identificação enriquece a interpretação do texto.

Existem diferentes formas de intertextualidade:

- **Citação direta ou indireta (quotation or paraphrase):** ocorre quando um texto menciona explicitamente outro, usando aspas ou reformulando uma ideia já conhecida.
- **Alusão (allusion):** uma referência sutil a outro texto, evento ou figura histórica, que o leitor deve reconhecer para compreender completamente o significado. Por exemplo, a expressão “to be or not to be” remete imediatamente à obra de Shakespeare, mesmo fora do contexto da peça.
- **Paródia e pastiche:** quando um texto imita ou faz uma releitura de outro, seja para homenageá-lo, seja para criticar ou modificar seu sentido original.
- **Interdiscursividade:** quando um texto incorpora elementos de diferentes gêneros discursivos, como um artigo acadêmico que inclui trechos de entrevistas, notícias e gráficos.

A intertextualidade é uma estratégia poderosa para enriquecer o significado de um texto. Por exemplo, um anúncio publicitário pode usar uma referência bíblica ou literária para criar um impacto emocional no público, enquanto um artigo de opinião pode citar estudos acadêmicos para reforçar sua argumentação.

Para identificar relações intertextuais em textos em inglês, o leitor precisa estar atento a pistas linguísticas, como aspas, expressões idiomáticas conhecidas, nomes próprios e eventos históricos mencionados. Além disso, o background knowledge (conhecimento prévio) é fundamental para fazer essas conexões de forma eficiente.

O reconhecimento da intertextualidade amplia a compreensão do texto, pois permite ao leitor perceber camadas de significado que vão além da superfície, enriquecendo a interpretação e promovendo uma leitura mais crítica e reflexiva.

A compreensão e interpretação de textos em inglês envolvem uma combinação de habilidades linguísticas e cognitivas. O domínio do vocabulário e da estrutura da língua fornece a base para decodificar o texto, enquanto a identificação das relações intratextuais e intertextuais permite uma compreensão mais profunda e crítica do conteúdo.

Desenvolver essas competências é essencial para leitores que desejam não apenas entender textos em inglês, mas também analisá-los de forma reflexiva, reconhecendo as conexões entre diferentes ideias, contextos e discursos. Esse processo contribui para o aprimoramento da proficiência linguística e para a formação de leitores mais autônomos e críticos em qualquer área do conhecimento.

ITENS GRAMATICAIS RELEVANTES PARA A COMPREENSÃO DOS CONTEÚDOS SEMÂNTICOS

Dentre os muitos tópicos gramaticais da língua inglesa, alguns se fazem primordiais para a compreensão textual e a contextualização da comunicação no idioma. Os tempos verbais são as principais gramáticas a serem estudadas para uma melhor compreensão do idioma por completo. Ao realizar a interpretação de um texto, deve-se levar o tempo verbal em consideração para que se possa contextualizar o momento ao qual a fala se refere. Confira a seguir.

Simple present

O *simple present* ou o presente simples é marcado por dois verbos auxiliares específicos DO e DOES. A conjugação verbal no tempo presente da língua inglesa é simples e se divide entre grupos de sujeitos. No infinitivo, ou seja, quando terminados em “ar”, “er”, “ir” no português, o verbo leva “to” em inglês, veja a seguir.

- Comer – to *eat*
- Beber – to *drink*
- Andar – to *walk*

Todos os verbos no presente mantêm uma conjugação básica, muito mais simples que a do português para cada sujeito. Basta retirar o “to” do infinitivo para serem conjugados com os sujeitos *I, you, we, they* e *you* (plural). Veja:

- I **eat** – Eu como
- You **eat** – Você come/ Tu comes
- We **eat** – Nós comemos
- They **eat** – Eles comem
- You **eat** – Vocês comem/ Vós comeis

SEGURANÇA OFENSIVA

CONCEITOS BÁSICOS: VULNERABILIDADES, AMEAÇAS E ATAQUES

Segurança ofensiva é o conjunto de práticas destinadas a avaliar sistemas, aplicações, redes, identidades e processos a partir da perspectiva de um possível atacante. Seu objetivo não é provocar danos, mas identificar antecipadamente condições que poderiam ser utilizadas em um incidente real. Dessa forma, a organização consegue compreender sua exposição, validar controles de segurança e corrigir fragilidades antes que sejam exploradas por agentes maliciosos.

Relação entre segurança ofensiva e defensiva

A segurança ofensiva e a segurança defensiva atuam sobre o mesmo problema por perspectivas diferentes. Enquanto a abordagem defensiva busca impedir, detectar e responder a atividades maliciosas, a abordagem ofensiva procura verificar se essas proteções realmente resistem a cenários plausíveis de ataque.

Essa relação pode ser compreendida pelos seguintes papéis complementares:

- **Segurança ofensiva:** identifica fragilidades, simula comportamentos adversários e testa a efetividade dos controles existentes.
- **Segurança defensiva:** monitora ambientes, reduz superfícies de ataque, detecta atividades suspeitas e responde a incidentes.
- **Gestão de riscos:** transforma os resultados técnicos dessas atividades em decisões sobre prioridade, tratamento e investimento.

Um programa maduro de segurança combina essas perspectivas. Encontrar uma vulnerabilidade possui valor limitado se a organização não conseguir compreender seu impacto, definir prioridade e implementar medidas de redução de risco.

▸ Ativos, exposição e superfície de ataque

O conceito de ativo

Um ativo é qualquer recurso que possua valor para uma organização e que, por esse motivo, necessite de proteção. Servidores, estações de trabalho, aplicações, bancos de dados, contas de usuários, informações confidenciais, equipamentos de rede e serviços em nuvem são exemplos comuns.

A análise ofensiva precisa compreender quais ativos existem, como estão conectados e quais consequências podem resultar de seu comprometimento.

Superfície de ataque

A superfície de ataque corresponde ao conjunto de pontos pelos quais um sistema ou organização pode ser alcançado ou influenciado por um possível atacante. Quanto maior e mais complexa essa superfície, maior tende a ser a quantidade de condições que precisam ser protegidas.

Alguns componentes frequentemente presentes nessa superfície incluem:

- Serviços de rede expostos à Internet ou a redes internas.
- Aplicações web, APIs e interfaces administrativas.
- Contas, credenciais, permissões e mecanismos de autenticação.
- Estações de trabalho, dispositivos móveis e equipamentos conectados.
- Usuários suscetíveis a engenharia social ou manipulação.
- Integrações com fornecedores, parceiros e serviços externos.

▸ Risco, vulnerabilidade, ameaça e ataque

Uma relação fundamental

Esses conceitos não são sinônimos. Uma vulnerabilidade representa uma fraqueza; uma ameaça representa algo capaz de causar dano; um ataque é uma ação realizada para produzir determinado efeito; e o risco representa a possibilidade de que uma situação indesejada efetivamente ocorra e gere impacto.

Por exemplo, considere um sistema administrativo acessível pela Internet que utiliza credenciais fracas. As credenciais inadequadas constituem uma vulnerabilidade. Um agente interessado em obter acesso não autorizado representa uma ameaça. As tentativas realizadas contra o mecanismo de autenticação constituem um ataque. O possível acesso indevido a informações sensíveis representa parte do risco associado ao cenário.

▸ Autorização, escopo e ética

O limite fundamental da segurança ofensiva

Atividades ofensivas legítimas dependem de autorização explícita. Um teste de segurança deve possuir objetivos, ativos autorizados, restrições, período de execução, responsáveis e regras de comunicação claramente definidos.

Escopo técnico

O escopo estabelece o que pode e o que não pode ser testado. Essa definição evita que uma avaliação tecnicamente válida produza impactos indevidos sobre sistemas não autorizados, ambientes de terceiros ou operações críticas.

Portanto, a diferença essencial entre uma avaliação profissional e uma atividade maliciosa não está apenas nas técnicas utilizadas, mas principalmente na autorização, no propósito, no controle operacional e na responsabilidade envolvidos.

Vulnerabilidades: conceitos, origens e classificação

O que é uma vulnerabilidade

Uma vulnerabilidade é uma fraqueza que pode comprometer a confidencialidade, a integridade, a disponibilidade ou outros requisitos de segurança de um ativo. Ela pode existir no código de uma aplicação, na configuração de um servidor, na arquitetura de uma rede, em processos organizacionais ou até mesmo na forma como pessoas utilizam determinado sistema.

Vulnerabilidade não significa comprometimento

A existência de uma vulnerabilidade não indica automaticamente que um ataque ocorreu. Ela representa uma condição que, dependendo do contexto, pode ser explorada ou combinada com outras condições.

É importante diferenciar alguns conceitos próximos:

Conceito	Significado
Vulnerabilidade	Fraqueza capaz de afetar a segurança de um ativo
Exploração	Utilização prática de uma vulnerabilidade para produzir determinado efeito
Exposição	Condição que torna um ativo acessível ou sujeito a determinada interação
Mitigação	Medida que reduz a probabilidade ou o impacto associado à vulnerabilidade
Correção	Alteração que elimina ou resolve diretamente a causa da vulnerabilidade

Principais origens das vulnerabilidades

Falhas de software

Vulnerabilidades podem surgir durante o desenvolvimento de aplicações quando entradas não são adequadamente tratadas, permissões são incorretamente aplicadas ou mecanismos de autenticação e autorização são implementados de maneira inadequada.

Configurações inseguras

Mesmo softwares tecnicamente seguros podem tornar-se vulneráveis quando são configurados incorretamente. Serviços desnecessários expostos, permissões excessivas, interfaces administrativas acessíveis e configurações padrão inadequadas são exemplos frequentes.

Arquitetura e processos

Algumas fragilidades não estão concentradas em um único componente. Uma arquitetura pode permitir movimentação excessiva entre sistemas, enquanto um processo organizacional pode autorizar modificações sensíveis sem verificações suficientes.

As origens podem, portanto, ser resumidas em diferentes categorias:

- **Software:** erros de implementação, bibliotecas vulneráveis ou controles insuficientes.
- **Configuração:** parâmetros inadequados, serviços desnecessários e permissões excessivas.
- **Arquitetura:** segmentação insuficiente, relações de confiança excessivas ou ausência de isolamento.
- **Identidade:** senhas fracas, privilégios elevados ou mecanismos de autenticação inadequados.
- **Processos:** procedimentos que permitem ações sensíveis sem validações suficientes.
- **Fator humano:** decisões, comportamentos ou manipulações que podem resultar em exposição.

Identificação e classificação

CVE, CWE e CVSS

Na gestão técnica de vulnerabilidades, alguns conceitos auxiliam na padronização das informações. CVE é utilizado para identificar publicamente vulnerabilidades conhecidas de maneira única. CWE organiza tipos de fraquezas que podem resultar em vulnerabilidades. CVSS, por sua vez, fornece um modelo para estimar a severidade técnica de determinadas vulnerabilidades.

Esses mecanismos cumprem funções diferentes. Uma vulnerabilidade pode possuir um identificador CVE, estar relacionada a determinada categoria de fraqueza descrita por uma CWE e receber uma pontuação de severidade calculada com CVSS.

Severidade não é o mesmo que risco

Uma vulnerabilidade tecnicamente grave não será necessariamente a maior prioridade de uma organização. O contexto precisa ser considerado. Uma falha severa localizada em um sistema isolado e sem informações relevantes pode representar menor risco organizacional do que uma vulnerabilidade moderada existente em um sistema crítico diretamente exposto.

Ciclo de vida de uma vulnerabilidade

Da descoberta ao tratamento

O gerenciamento adequado exige continuidade. Depois da identificação, a vulnerabilidade precisa ser analisada, priorizada, tratada e posteriormente verificada.

As principais possibilidades de tratamento incluem:

- **Correção:** eliminar diretamente a causa da vulnerabilidade.
- **Mitigação:** implementar controles que reduzam sua exploração ou impacto.
- **Controle compensatório:** utilizar outra proteção quando a correção direta não for imediatamente possível.
- **Aceitação:** reconhecer formalmente o risco quando ele estiver dentro da tolerância estabelecida pela organização.

Na segurança ofensiva, identificar uma vulnerabilidade é apenas o início. O valor real está em demonstrar seu contexto, possíveis consequências e prioridade de tratamento.

Ameaças e agentes de ameaça

O conceito de ameaça

Uma ameaça é qualquer circunstância, evento ou agente capaz de explorar uma vulnerabilidade ou provocar um resultado prejudicial. Diferentemente da vulnerabilidade, que é uma

SEGURANÇA DEFENSIVA

DEFESA EM PROFUNDIDADE: PERÍMETRO DE SEGURANÇA (FILTRO DE PACOTES, FIREWALL DE ESTADO, FIREWALL PROXY, IDS, IPS, VPN).

Defesa em profundidade é uma estratégia de segurança baseada na utilização coordenada de múltiplas camadas de proteção. O princípio central é evitar que a segurança de uma organização dependa exclusivamente de um único mecanismo. Caso determinado controle seja contornado, apresente falha ou esteja configurado incorretamente, outros controles permanecem disponíveis para limitar, detectar ou interromper a progressão de uma ameaça.

Essa abordagem reconhece que nenhum mecanismo de segurança é perfeito. Firewalls podem possuir regras inadequadas, credenciais podem ser comprometidas, vulnerabilidades podem ainda não ter sido corrigidas e usuários podem cometer erros. Por isso, a proteção deve ser distribuída entre redes, dispositivos, identidades, aplicações, dados e mecanismos de monitoramento.

Tipos de controles

As camadas de defesa podem exercer funções diferentes e complementares. Essa diferenciação é importante porque impedir uma ação e detectá-la são capacidades distintas.

- Controles preventivos procuram impedir que atividades inadequadas sejam executadas.
- Controles detectivos procuram identificar atividades suspeitas ou violações que estejam ocorrendo ou já tenham ocorrido.
- Controles corretivos procuram limitar consequências e restaurar o ambiente após um problema.

Um firewall, por exemplo, pode bloquear determinada comunicação, enquanto um IDS pode gerar um alerta sobre um padrão suspeito. Procedimentos de resposta a incidentes e restauração atuam posteriormente para controlar os danos.

▸ Perímetro de segurança

Fronteira entre zonas com diferentes níveis de confiança

Tradicionalmente, o perímetro de segurança representava a fronteira entre a rede interna de uma organização e redes externas, especialmente a Internet. Firewalls eram posicionados nesse ponto para controlar quais comunicações poderiam entrar ou sair.

Esse modelo permanece importante, mas tornou-se insuficiente como única estratégia. Organizações modernas utilizam serviços em nuvem, aplicações distribuídas, dispositivos móveis, trabalho remoto e integrações com terceiros. Consequentemente, não existe necessariamente uma única fronteira claramente definida.

O conceito moderno de perímetro deve considerar diversas zonas e níveis de confiança.

▸ Zonas de segurança e segmentação

Separação de ambientes

Segmentação divide a infraestrutura em áreas com diferentes requisitos e permissões. Dessa forma, um dispositivo comprometido em determinado segmento não deve possuir acesso irrestrito aos demais ambientes.

Uma arquitetura pode separar, por exemplo, estações de usuários, servidores internos, sistemas críticos, equipamentos administrativos, serviços publicados e dispositivos de terceiros.

Essa separação permite aplicar controles específicos de acordo com o risco.

Tráfego de entrada, saída e lateral

A defesa não deve analisar somente conexões vindas da Internet. Comunicações internas também podem representar riscos.

O tráfego pode ser observado em três perspectivas principais:

- **Entrada:** comunicações originadas externamente e destinadas a recursos da organização.
- **Saída:** comunicações iniciadas internamente em direção a redes externas.
- **Lateral:** comunicações realizadas entre sistemas ou segmentos internos.

O controle de tráfego de saída pode revelar comportamentos inesperados, enquanto a análise do tráfego lateral ajuda a limitar movimentações após um eventual comprometimento.

▸ Princípio do menor privilégio aplicado à rede

Uma rede segura não deve permitir comunicações simplesmente porque tecnicamente são possíveis. Cada fluxo deve existir por uma necessidade operacional identificada.

Essa abordagem favorece uma política de bloquear por padrão e permitir apenas comunicações justificadas. O objetivo é reduzir a superfície de ataque e dificultar que sistemas comprometidos utilizem serviços que nunca deveriam estar acessíveis.

▸ Limitações do perímetro isolado

Um firewall de borda não protege sozinho contra todos os cenários. Um usuário autenticado pode possuir credenciais comprometidas, um dispositivo autorizado pode estar infectado e um serviço em nuvem pode estar fora do perímetro tradicional.

Por isso, filtros de pacotes, firewalls, IDS, IPS e VPN devem ser vistos como componentes de uma arquitetura maior. Defesa em profundidade surge exatamente da combinação entre esses controles, políticas de identidade, proteção de endpoints, segmentação, monitoramento e resposta a incidentes.

Filtro de Pacotes, Firewall de Estado e Firewall Proxy

Filtro de pacotes

Análise baseada em características da comunicação

O filtro de pacotes é uma das formas mais fundamentais de controle de tráfego. Seu funcionamento consiste em examinar informações presentes nos cabeçalhos dos pacotes e compará-las com regras previamente definidas.

Entre os critérios normalmente considerados estão endereço de origem, endereço de destino, protocolo, porta de origem, porta de destino e direção da comunicação.

As regras podem ser estruturadas para permitir ou bloquear determinados fluxos. Isso possibilita estabelecer políticas relativamente simples e eficientes.

Filtragem stateless

Um filtro stateless analisa cada pacote de maneira predominantemente independente, sem manter conhecimento detalhado sobre a conexão à qual ele pertence.

Essa abordagem pode apresentar alto desempenho e baixa complexidade, porém possui pouca capacidade de interpretar o contexto da comunicação.

Firewall de estado

Stateful inspection

Um firewall de estado mantém informações sobre conexões em andamento. Em vez de avaliar cada pacote completamente isolado, ele procura compreender se determinado tráfego faz parte de uma comunicação previamente estabelecida.

Esse comportamento permite diferenciar, por exemplo, uma resposta legítima associada a uma conexão iniciada internamente de um pacote inesperado que apenas apresenta características semelhantes.

Tabela de estados

O equipamento mantém registros temporários das conexões observadas. Esses registros possibilitam acompanhar elementos necessários para determinar se o tráfego recebido corresponde ao contexto esperado.

A diferença fundamental entre as duas abordagens pode ser visualizada da seguinte maneira:

Característica	Filtro de Pacotes	Firewall de Estado
Análise de cabeçalhos	Sim	Sim
Conhecimento da conexão	Limitado	Sim
Controle contextual	Menor	Maior
Complexidade	Menor	Maior
Consumo de recursos	Geralmente menor	Geralmente maior

Firewall Proxy

Intermediação da comunicação

Um firewall proxy atua como intermediário entre cliente e servidor. Em vez de simplesmente encaminhar a conexão original, ele recebe a comunicação de uma parte e estabelece outra comunicação com o destino.

Essa separação lógica oferece maior capacidade de controle porque o proxy pode compreender determinadas características do protocolo utilizado.

Inspeção em camada de aplicação

Firewalls proxy podem analisar elementos que não seriam suficientemente compreendidos por filtros tradicionais baseados apenas em endereços e portas.

Dependendo da tecnologia e do protocolo, essa abordagem possibilita avaliar comandos, métodos, conteúdos ou comportamentos específicos da aplicação.

Algumas vantagens são particularmente importantes:

- Maior compreensão do protocolo utilizado.
- Separação lógica entre clientes e servidores.
- Possibilidade de aplicar políticas específicas de aplicação.
- Maior capacidade de registrar detalhes das comunicações.

Essa profundidade, entretanto, aumenta complexidade e consumo de recursos.

Controles complementares

Não existe uma tecnologia universalmente superior. Filtros simples podem ser adequados para determinadas fronteiras, firewalls stateful oferecem controle contextual eficiente e proxies são úteis quando a compreensão da aplicação é importante.

Em defesa em profundidade, essas tecnologias podem ser combinadas em diferentes pontos. O objetivo não é acumular controles indiscriminadamente, mas posicioná-los de acordo com o risco, o tipo de tráfego e a importância dos ativos protegidos.

IDS e IPS: Detecção e Prevenção de Intrusões

Intrusion Detection System

Conceito de IDS

IDS é um sistema destinado a identificar comportamentos que possam indicar ataques, violações de políticas ou atividades anormais. Seu propósito predominante é detectivo: observar eventos ou comunicações e gerar alertas que possam ser analisados.

Um IDS pode ser posicionado na rede ou instalado diretamente em sistemas.

NIDS e HIDS

Um NIDS analisa tráfego de rede e procura identificar padrões relacionados a comunicações suspeitas. Um HIDS observa elementos do próprio host, como eventos, alterações e comportamentos de processos.

As duas abordagens fornecem perspectivas diferentes:

- NIDS oferece visibilidade sobre comunicações entre diferentes dispositivos.
- HIDS proporciona maior contexto sobre atividades realizadas dentro de determinado equipamento.

COMPLIANCE DE SEGURANÇA E PRIVACIDADE

NORMAS: ABNT NBR ISO/IEC 27001:2013, ABNT NBR ISO/IEC 27002:2013, ABNT NBR ISO/IEC 27005:2019, ABNT NBR ISO/IEC 29100:2020, ABNT NBR ISO/IEC 29134:2020

Sistema de Gestão da Segurança da Informação: ABNT NBR ISO/IEC 27001:2013 e ABNT NBR ISO/IEC 27002:2013

Família ISO/IEC 27000 e o SGSI

A família ISO/IEC 27000 reúne normas relacionadas à gestão da segurança da informação. Dentro desse conjunto, a ABNT NBR ISO/IEC 27001:2013 estabelece requisitos para criação, implementação, manutenção e melhoria contínua de um Sistema de Gestão da Segurança da Informação, denominado SGSI.

O SGSI não deve ser entendido apenas como um conjunto de ferramentas técnicas. Trata-se de um sistema de gestão que integra políticas, responsabilidades, processos, pessoas, recursos tecnológicos, avaliação de riscos e mecanismos de controle.

Segurança orientada a riscos

A organização precisa compreender quais informações devem ser protegidas, quais ameaças e vulnerabilidades são relevantes e quais consequências podem ocorrer. A partir dessa análise, são escolhidos controles proporcionais aos riscos.

As propriedades tradicionalmente associadas à proteção são confidencialidade, integridade e disponibilidade. Dependendo do contexto, outras propriedades, como autenticidade e irretratabilidade, também podem ser relevantes.

Estrutura do SGSI

A ISO/IEC 27001:2013 organiza os requisitos de gestão em cláusulas que abrangem desde o contexto organizacional até a melhoria contínua.

Os principais elementos podem ser compreendidos da seguinte forma:

- **Contexto da organização:** compreensão do ambiente interno, externo e das partes interessadas.
- **Liderança:** comprometimento da direção, estabelecimento da política e definição de responsabilidades.
- **Planejamento:** avaliação de riscos, tratamento de riscos e definição de objetivos de segurança.
- **Apoio:** recursos, competências, conscientização, comunicação e documentação.
- **Operação:** execução dos processos planejados de avaliação e tratamento de riscos.
- **Avaliação de desempenho:** monitoramento, medição, auditorias internas e análise crítica pela direção.
- **Melhoria:** tratamento de não conformidades e aperfeiçoamento contínuo do SGSI.

Anexo A e tratamento dos riscos

O Anexo A da edição de 2013 apresenta um conjunto de objetivos de controle e controles que podem ser considerados durante o tratamento dos riscos. A edição de 2013 organiza esses controles em 14 domínios e contém 114 controles.

A seleção não deve ocorrer de maneira automática. A organização deve avaliar seus riscos e justificar quais controles são necessários.

Declaração de Aplicabilidade

A Declaração de Aplicabilidade, frequentemente chamada de SoA, documenta os controles considerados necessários, sua situação de implementação e as justificativas relacionadas à inclusão ou exclusão.

Ela estabelece uma conexão importante entre avaliação de riscos e controles efetivamente adotados.

ABNT NBR ISO/IEC 27002:2013

Enquanto a ISO/IEC 27001 apresenta requisitos para o SGSI e pode servir como base para certificação, a ISO/IEC 27002:2013 possui caráter orientativo e detalha boas práticas relacionadas aos controles de segurança.

Na edição de 2013, seus domínios abrangem:

- Políticas de segurança da informação e organização da segurança.
- Segurança em recursos humanos e gestão de ativos.
- Controle de acesso e criptografia.
- Segurança física e ambiental.
- Segurança das operações e das comunicações.
- Aquisição, desenvolvimento e manutenção de sistemas.
- Relacionamento com fornecedores e gestão de incidentes.
- Continuidade de negócios e conformidade.

As duas normas, portanto, cumprem papéis complementares: a ISO/IEC 27001 estrutura o sistema de gestão e seus requisitos, enquanto a ISO/IEC 27002 auxilia a organização a compreender e implementar controles apropriados.

Gestão de Riscos de Segurança da Informação: ABNT NBR ISO/IEC 27005:2019

Finalidade da gestão de riscos

A ABNT NBR ISO/IEC 27005:2019 fornece orientações para a gestão dos riscos de segurança da informação. Sua aplicação complementa o SGSI porque permite transformar decisões de segurança em escolhas fundamentadas na identificação, análise, avaliação e tratamento dos riscos.

A gestão de riscos não procura eliminar todo risco. Em muitos contextos isso seria tecnicamente impossível ou economicamente inviável. O objetivo é compreender os riscos e mantê-los dentro de níveis considerados aceitáveis pela organização.

- **Estabelecimento do contexto**

Antes de analisar riscos, a organização precisa estabelecer seu contexto. Isso envolve compreender escopo, ativos, processos, responsabilidades, requisitos e critérios que serão utilizados para decidir se determinado risco pode ou não ser aceito.

Critérios de risco

Os critérios definem como probabilidade e consequências serão avaliadas e quais níveis exigirão tratamento.

Uma organização pode considerar, entre outros aspectos:

- Impactos financeiros e operacionais.
- Consequências jurídicas ou regulatórias.
- Danos à imagem ou confiança das partes interessadas.
- Comprometimento da confidencialidade, integridade ou disponibilidade.

- **Identificação e análise de riscos**

A identificação procura determinar quais situações podem comprometer os objetivos de segurança. Isso normalmente exige conhecimento dos ativos, ameaças, vulnerabilidades, controles existentes e consequências possíveis.

Uma ameaça pode explorar determinada vulnerabilidade e produzir impacto sobre um ativo. O risco representa esse cenário dentro de determinado contexto.

Na análise, procura-se compreender a probabilidade ou possibilidade de ocorrência e a magnitude de suas consequências. A organização pode utilizar métodos qualitativos, quantitativos ou combinações dos dois.

- **Avaliação de riscos**

Após a análise, os resultados são comparados aos critérios estabelecidos. Dessa forma, riscos podem ser priorizados conforme sua importância.

Essa etapa permite direcionar recursos para situações que realmente exigem atenção, em vez de tratar todas as vulnerabilidades ou ameaças como equivalentes.

- **Tratamento de riscos**

Quando um risco não é considerado aceitável, diferentes estratégias podem ser adotadas.

As principais possibilidades incluem:

- Modificar o risco mediante implementação ou fortalecimento de controles.
- Evitar a atividade ou condição que produz o risco.
- Compartilhar determinadas consequências com outras partes.
- Reter ou aceitar conscientemente o risco quando compatível com os critérios estabelecidos.

O tratamento deve resultar em decisões documentadas, responsabilidades e ações definidas.

Risco inerente e risco residual

Risco inerente representa o nível de risco considerado antes da aplicação dos controles relevantes. Após a implementação das medidas de tratamento, permanece o risco residual.

A existência de risco residual é normal. A organização precisa avaliar se esse nível pode ser formalmente aceito ou se novas medidas são necessárias.

- **Monitoramento e revisão**

Riscos não são estáticos. Novas tecnologias, vulnerabilidades, fornecedores, processos e ameaças podem modificar significativamente um cenário.

Por isso, a gestão de riscos deve incluir comunicação, consulta, monitoramento e revisão periódica. Essa característica permite integrar a ISO/IEC 27005 ao ciclo de melhoria contínua do SGSI: a ISO/IEC 27001 estabelece a necessidade de gerenciar riscos, a ISO/IEC 27005 orienta esse processo e a ISO/IEC 27002 contribui para a escolha e compreensão dos controles.

Privacidade e Proteção de Informações Pessoais: ABNT NBR ISO/IEC 29100:2020

- **Estrutura de privacidade**

A ABNT NBR ISO/IEC 29100:2020 estabelece uma estrutura conceitual para proteção da privacidade relacionada a informações de identificação pessoal. Seu objetivo é fornecer terminologia comum, papéis, princípios e elementos que auxiliem organizações a compreender e organizar a governança da privacidade.

Segurança da informação e privacidade são relacionadas, mas não equivalentes. Segurança busca proteger informações contra diferentes formas de comprometimento. Privacidade também considera se a coleta, utilização, retenção e divulgação de informações pessoais são apropriadas ao contexto e às finalidades declaradas.

- **Informações de identificação pessoal**

Informações de identificação pessoal são dados que podem estar associados a uma pessoa identificada ou identificável. A proteção deve considerar não apenas informações diretamente identificadoras, mas também dados que, quando combinados, possam permitir associação a uma pessoa.

Papéis no tratamento

A estrutura distingue diferentes participantes envolvidos no ecossistema de privacidade. Entre eles encontram-se o titular das informações, entidades que determinam sua finalidade de tratamento, entidades que processam essas informações e terceiros envolvidos nas operações.

Compreender esses papéis é necessário para atribuir responsabilidades e definir controles.

- **Ciclo de vida das informações pessoais**

A privacidade deve ser considerada durante todo o ciclo de vida da informação. O risco não existe apenas durante o armazenamento.

O ciclo pode envolver:

- Coleta de informações pessoais.
- Utilização para finalidades definidas.
- Armazenamento e proteção durante o período necessário.
- Compartilhamento ou divulgação quando aplicável.
- Retenção conforme requisitos legítimos.

Editora Solução
a solução para o seu concurso!

GOSTOU DESSE MATERIAL?

Então não pare por aqui: a versão **COMPLETA** vai te deixar ainda mais perto da sua aprovação e da tão sonhada estabilidade. Aproveite o **DESCONTO EXCLUSIVO** que liberamos para Você!

EU QUERO DESCONTO!