

CADERNO DIDÁTICO

FORMAÇÃO E ATUALIZAÇÃO DO OPERADOR DE SISTEMA ELETRÔNICO DE SEGURANÇA

EDIÇÃO 01



CURSO DE FORMAÇÃO DE OPERADOR DE SISTEMA ELETRÔNICO DE SEGURANÇA (CFOP) PLANO DE CURSO

NOÇÕES DE SEGURANÇA PRIVADA (NSP)

Objetivos: Desenvolver conhecimentos sobre a segurança privada.

Os serviços de segurança privada serão prestados por pessoas jurídicas especializadas ou por meio das empresas e dos condomínios edilícios possuidores de serviços orgânicos de segurança privada, neste último caso, em proveito próprio, com ou sem utilização de armas de fogo e com o emprego de profissionais habilitados e de tecnologias e equipamentos de uso permitido. É vedada a prestação de serviços de segurança privada de forma cooperada ou autônoma (Brasil, 2024).

Segurança Privada: É a atividade de proteção de pessoas, bens, estabelecimentos e transportes exercida por pessoas jurídicas de direito privado, devidamente autorizadas e fiscalizadas pela Polícia Federal. Ela possui caráter complementar às atividades de segurança pública e é exercida exclusivamente nos termos da lei, sendo vedada qualquer atuação de natureza político-partidária ou paramilitar.

Serviços de Segurança Privada: Diz respeito à classificação da execução da atividade, que se divide em duas modalidades principais:

- **Prestação de Serviços a Terceiros (Empresas Especializadas):** Empresas constituídas com o fim exclusivo de comercializar e prestar serviços de segurança para outros clientes.
- **Serviço Próprio de Segurança (Segurança Orgânica):** Empresas de outros ramos (bancos, indústrias, comércios) que optam por criar seu próprio departamento de segurança, contratando diretamente os vigilantes para proteger apenas o seu próprio patrimônio, sem comercializar o serviço.

ADMINISTRAÇÃO, GESTÃO E COMANDO

Para os serviços de segurança privada e da segurança das instituições financeiras, por meio da Lei nº 14.967/24 e do Decreto nº 13.012/26, estão regulamentados a autorização, ao controle e à fiscalização:

Empresa de serviços de segurança privada: Pessoa jurídica de direito privado autorizada a prestar os serviços de vigilância patrimonial; de transporte de numerário, bens ou valores; de escolta de numerário, bens ou valores; de segurança pessoal e de gerenciamento de riscos em operações de transporte de numerário, bens ou valores;

Escola de Formação de Profissionais de Segurança Privada: São empresas especializadas cuja atividade exclusiva é a capacitação, formação, aperfeiçoamento e atualização periódica de vigilantes. Nenhuma pessoa pode exercer a profissão de vigilante sem o certificado emitido por uma escola devidamente autorizada pelo Ministério da Justiça/Polícia Federal.

Empresas de Monitoramento de Sistemas Eletrônicos de Segurança Privada: Uma das grandes inovações de inclusão do novo Estatuto. Compreende a prestação de serviços voltados ao desenho de projetos, instalação, manutenção e, principalmente, o monitoramento remoto de sinais de alarme, circuitos fechados de televisão (CFTV – Circuito Fechado de Televisão) e controle de acesso eletrônico.

- *Nota de prova:* As empresas que fazem apenas o monitoramento eletrônico (sem resposta física armada) possuem regras de fiscalização diferenciadas das empresas de segurança armada.

Gerenciamento de Riscos em Operações de Transporte de Numerários, Bens ou Valores: É a atividade de planejamento estratégico, análise e mitigação de ameaças voltada especificamente para a logística de valores. Envolve o desenho de rotas alternativas, monitoramento via satélite, definição de horários de saída, uso de cofres com fechadura randômica/retardo de tempo e o acionamento de planos de contingência caso ocorra um sinistro ou tentativa de assalto (como o Novo Cangaço).

EXECUÇÃO OPERACIONAL DE SEGURANÇA FÍSICA (ARMADA/DESARMADA)

Gestor de Segurança Privada: profissional especializado, de nível superior, registrado na Polícia Federal, responsável pela: a) realização da análise de riscos e definição e integração dos recursos físicos, humanos, técnicos e organizacionais a serem utilizados na mitigação de riscos; b) elaboração dos projetos de segurança para a implementação das estratégias de proteção; c) realização de auditorias de segurança em organizações públicas e privadas; ou d) execução do serviço de gerenciamento de riscos em operações de transporte de numerário, bens ou valores, realizado por empresa de gerenciamento de risco em operações de transporte de numerário, bens ou valores.

Vigilante Supervisor: profissional habilitado em curso de formação específico, registrado na Polícia Federal, possuidor de vínculo empregatício com empresa de serviço de segurança privada ou empresas e condomínios edifícios possuidores de serviço orgânico de segurança privada, encarregado do controle operacional dos serviços prestados por sua empregadora

Vigilante Patrimonial: Profissional habilitado em curso de formação específico, registrado na Polícia Federal, possuidor de vínculo empregatício com empresa de serviço de segurança privada ou empresas e condomínios edifícios possuidores de serviço orgânico de segurança privada, responsável pela execução dos serviços prestados por sua empregadora.

Transporte de Numerários, Bens ou Valores: É o serviço especializado de movimentação física de dinheiro (numerário), barras de ouro, joias, obras de arte ou documentos de alto valor. Exige a utilização de veículos blindados (carros-fortes) especialmente equipados e homologados pela Polícia Federal, contando com tripulação mínima armada.

Escolta de Numerários, Bens ou Valores: Diferente do transporte (onde o valor vai *dentro* do veículo blindado), a escolta é a atividade que visa garantir a incolumidade da carga de terceiros em movimento (seja um caminhão de eletrônicos ou um veículo de transporte de valores). É realizada por vigilantes embarcados em veículos próprios de escolta, devidamente identificados e armados, que acompanham o comboio ao longo do trajeto.

Segurança Pessoal: É a atividade de vigilância exercida com a finalidade de garantir a integridade física de uma pessoa específica (dignitários, executivos, celebridades, testemunhas protegidas). É executada por vigilantes especializados que atuam de forma próxima ao protegido, podendo atuar com trajes civis (discretos), desde que autorizados.

Segurança de Eventos: Atuação em espaços fechados ou comuns, públicos ou privados, onde ocorram eventos sociais, esportivos, culturais ou corporativos. É realizada predominantemente de forma **desarmada**, focando no controle de multidões, gerenciamento de crises e revista de público.

EXECUÇÃO OPERACIONAL DE SEGURANÇA ELETRÔNICA (DECRETO Nº 13.012, DE 9 DE JUNHO DE 2026)

Supervisor de Monitoramento de Sistemas Eletrônicos: Profissional habilitado em curso de formação específico, registrado na Polícia Federal, possuidor de vínculo empregatício com empresa de monitoramento de sistema eletrônico de segurança privada ou empresa de serviço de segurança privada, encarregado do controle operacional dos serviços de monitoramento de sistemas eletrônicos de segurança.

Operador de Sistemas Eletrônicos: profissional habilitado em curso de formação específico, registrado na Polícia Federal, possuidor de vínculo empregatício com empresa de monitoramento de sistema eletrônico de segurança privada ou empresa de serviço de segurança privada, encarregado de realizar o monitoramento de sistemas eletrônicos de segurança e dos equipamentos que o integram.

Técnico Externo de Sistemas Eletrônicos: Profissional habilitado em curso de formação específico, registrado na Polícia Federal, possuidor de vínculo empregatício com empresa de monitoramento de sistema eletrônico de segurança privada ou empresa de serviço de segurança privada, encarregado de prestar os serviços de inspeção técnica decorrente dos sinais emitidos pelos equipamentos da sua empregadora.

A Lei nº 14.967/2024 (Estatuto da Segurança Privada) e o Decreto nº 13.012/2026 expandiram e modernizaram o rol de **atividades de segurança privada** autorizadas no Brasil. O novo marco regulatório define os limites operacionais, requisitos e o uso de armamento para cada uma dessas onze vertentes.

Todas elas são de **interesse nacional**, e sua execução sem a devida autorização da Polícia Federal constitui atividade clandestina ilícita.

Segurança Física Geral e de Proteção Direta das Pessoas e do Patrimônio:

Infraestrutura Crítica e Áreas Estratégicas

- **Segurança Perimetral nas Muralhas e Guaritas:** Atuação em perímetros externos de alta periculosidade, como indústrias de infraestrutura estratégica e/ou de bens de alto valor.
- **Controle de Acesso em Portos e Aeroportos:** Fiscalização de pessoas, veículos e cargas nas chamadas zonas secundárias e áreas controladas de terminais portuários e aeroportuários. Realizada em estreita cooperação com a Receita Federal e a PF, fazendo uso intensivo de tecnologia de inspeção e raio-X.
- **Segurança em Unidades de Conservação:** Proteção de parques nacionais, reservas ecológicas e florestas protegidas. Os vigilantes atuam no combate à invasão de terras, desmatamento ilegal e caça/pesca predatória. Exige treinamento tático em ambiente de selva/bacia hidrográfica.
- **Segurança nos Transportes Coletivos Terrestres, Aquaviários e Marítimos:** Proteção interna e nas estações/terminais de ônibus, trens, metrô, balsas e navios de passageiros. O foco principal é coibir o vandalismo, furtos, assaltos e garantir a ordem pública de forma integrada com a segurança pública.

Tecnologia Avançada e Análise Estratégica

- **Segurança com Equipamentos Especiais de Observação e Operação:** Atividade focada no uso civil de tecnologias de ponta para varredura e monitoramento, operação de câmeras termais, analíticos de vídeo com inteligência artificial e varredura de escutas eletrônicas, a utilização de Drones (VANTs) dependerá de normas específicas do Ministério da Defesa, da Aeronáutica, da ANAC e/ou de outro órgão regulador.
- **Inteligência:** Atividade de coleta, análise e salvaguarda de dados para a produção de conhecimentos estratégicos. Visa antecipar ameaças corporativas, realizar a análise prévia de riscos e desenhar planos de contingência estruturados para blindar a operação dos clientes contra espionagem, sabotagem ou fraudes.

LEGISLAÇÃO APLICADA (LAP)

Objetivos: Desenvolver conhecimentos básicos de Direito, Direito Constitucional, Direito Penal e Lei Geral de Proteção de Dados.

A Legislação de Segurança Privada regula as atividades econômicas de segurança exercidas por empresas privadas, visando à proteção de pessoas e patrimônios, funcionando de forma complementar à segurança pública e sob controle e fiscalização da Polícia Federal.

LEGISLAÇÃO APLICADA DE SEGURANÇA PRIVADA

O novo marco regulatório da segurança privada no Brasil é estruturado por três pilares normativos fundamentais que organizam, detalham e executam as regras do setor:

Lei nº 14.967/2024 (Estatuto da Segurança Privada)

A Lei nº 14.967/2024 instituiu o **Estatuto da Segurança Privada e da Segurança das Instituições Financeiras**, revogando a antiga Lei nº 7.102/1983. Ela estabelece que a segurança privada é matéria de interesse nacional.

- **Principais Inovações:** Ampliou o rol de atividades permitidas, incluindo oficialmente o monitoramento eletrônico, rastreamento, segurança de eventos em espaços comuns e controle de acesso em portos e aeroportos.
- **Proibições:** É expressamente vedada a prestação de serviços de forma autônoma ou cooperada; apenas empresas jurídicas autorizadas podem atuar.
- **Responsabilidade do Contratante:** Quem contrata o serviço passa a ter a obrigação legal de fiscalizar previamente a regularidade formal da empresa prestadora junto à Polícia Federal.
- **Prazo de Adaptação:** O mercado recebeu um prazo de até 3 anos para se adequar integralmente às novas exigências.

Decreto Regulamentar (Decreto nº 13.012/2026)

O Decreto nº 13.012/2026 detalha a aplicação prática do Estatuto.

- **Função:** Define os ritos e procedimentos exatos para a concessão de autorizações, vistorias, fiscalizações e aplicação de penalidades administrativas.

- **Tecnologia e Operações:** Consolida as regras para portaria remota, videomonitoramento e o uso de carros-fortes e escolta armada. Ele também estabelece os parâmetros técnicos para a emissão de certificados eletrônicos de formação com validade nacional.
- **Foco Econômico e Social:** Objetiva reprimir o mercado clandestino e formalizar mais de 300 mil postos de trabalho no setor.

INSTRUÇÃO NORMATIVA DA POLÍCIA FEDERAL

A Polícia Federal é a autoridade central de controle e fiscalização do setor, conforme determinado pelo artigo 40 da lei. Suas Instruções Normativas (IN) e Portarias servem para operacionalizar o dia a dia das empresas:

- a) **Padronização:** Define os modelos de uniformes, o currículo mínimo dos cursos de formação de vigilantes (incluindo o uso progressivo da força e direitos humanos) e os critérios para testes de aptidão psicológica.
- b) **Controle de Armas:** Regula os atos de compra, custódia, transporte e destruição do armamento e munições utilizados pelas empresas especializadas.
- c) **Prazos de Renovação:** Sistematiza os processos de renovação de alvarás, que ocorrem a cada **2 anos** para empresas de segurança tradicional e escolas, e a cada **5 anos** para empresas de monitoramento eletrônico.

A Polícia Federal (PF) detém a competência exclusiva de autorizar, controlar e fiscalizar as atividades de segurança privada e das instituições financeiras no Brasil. Sob o regime da Lei nº 14.967/2024 e do Decreto nº 13.012/2026, esse papel fiscalizador foram substancialmente ampliado e enrijecido.

Requisitos para Constituição e Autorização de Funcionamento: Para abrir uma empresa e obter o Alvará de Funcionamento da Polícia Federal, a pessoa jurídica deve cumprir obrigatoriamente os seguintes critérios legais antes e durante o registro empresarial:

Aprovação Prévia de Atos: A minuta dos atos constitutivos (contrato social) deve ser submetida e aprovada pela PF através do Sistema GESP/SEI da Polícia Federal antes do registro na Junta Comercial.

Capital Social Mínimo: Comprovação de integralização de capital compatível com o ramo (ex: R\$ 730.000,00 para a maioria dos serviços comuns). Serviços armados exigem o valor integral; serviços sem arma de fogo (patrimonial/eventos) usufruem de redução de 1/4 do valor exigido.

Origem Lícita dos Recursos: É obrigatório demonstrar a idoneidade financeira e a procedência lícita de todo o capital investido.

Idoneidade dos Sócios e Administradores: Ausência de antecedentes criminais (certidões negativas da Justiça Federal, Estadual, Militar e Eleitoral) e inexistência de condenações por crimes dolosos.

Garantia Financeira (Seguro ou Provisão): Obrigatoriedade de contratar seguro-garantia ou constituir provisão financeira voltada ao adimplemento de verbas trabalhistas, previdenciárias e civis.

Infraestrutura Física: Instalações físicas adequadas e aprovadas em vistoria prévia pela PF, contendo cofres específicos, alarmes e monitoramento para a guarda segura de armas e munições.

Controle e Fiscalização Praticados pela Polícia Federal: A atuação cotidiana e operacional da Polícia Federal sobre os prestadores envolve o monitoramento de ativos técnicos, documentais e humanos:

[Cadastro no GESP] → [Vistoria de Instalações] → [Emissão de Alvará (2 ou 5 anos)]
→ [Fiscalização de Campo & Auditoria de Armas]

Homologação de Profissionais: Cadastro obrigatório de todo o efetivo (vigilantes, operadores de monitoramento e gestores). O registro profissional possui **validade de 2 anos** e exige atualização periódica e certidões criminais limpas.

Controle Estrito de Armamento: Centralização absoluta na PF para autorizar a compra, posse, transporte, estoque e eventual descarte de armas, munições e coletes balísticos.

Validade e Renovação de Alvarás: Emissão de alvarás de funcionamento com prazos de validade específicos — sendo renovados a **cada 2 anos** para vigilância armada e escolas de formação, e a **cada 5 anos** para empresas focadas estritamente em monitoramento eletrônico.

Fiscalização de Eventos de Grande Porte: Planos de segurança para eventos que reúnam mais de 1.000 pessoas dependem de análise de risco e validação prévia dos órgãos controladores.

PODER-DEVER SANCIONATÓRIO E REPRESSÃO À CLANDESTINIDADE

A legislação pune severamente desvios administrativos e a prestação irregular de serviços:

Penalidades Administrativas: Empresas regulares que violarem normas operacionais estão sujeitas a advertências, multas administrativas que variam de **R\$ 1.000,00 a R\$ 30.000,00**, suspensão temporária ou cassação definitiva do alvará.

Combate ao Mercado Clandestino: Empresas que atuam sem autorização da PF sofrem sanções imediatas de interdição e encerramento de atividades, além da apreensão e destruição de materiais.

Criminalização da Segurança Armada Irregular: Organizar, oferecer ou prestar serviços de segurança privada com o uso de armas de fogo sem autorização expressa da Polícia Federal constitui **crime**, com pena de **1 a 3 anos de detenção**, além de multa criminal aos sócios e proprietários

O novo marco regulatório da segurança privada no Brasil estabelece de forma clara a hierarquia, as funções e as responsabilidades de cada elo da cadeia operacional. Com base na Lei nº 14.967/2024 e no Decreto nº 13.012/2026, os profissionais do setor dividem-se em dois grandes grupos: a **administração e gestão**, e a **execução operacional** (dividida entre segurança física e eletrônica).

CONCLUSÃO

A legislação finalmente absorveu dinâmicas tecnológicas e de mercado que antes eram tratadas apenas por portarias temporárias da Polícia Federal.

Com o Decreto nº 13.012, de 9 de junho de 2026, o papel da Polícia Federal como órgão fiscalizador foi fortalecido para exigir capitais sociais mínimos elevados das empresas operantes.

Estima-se que as sanções administrativas e criminais, ou seja, as previsões legais preventivas e repressivas à informalidade e à clandestinidade, promova a busca de milhares de trabalhadores pela regularização, proporcionando mais segurança à sociedade mediante profissionais devidamente habilitados e fiscalizados, além de oportunizar aos trabalhadores outrora informais garantias sociais e previdenciárias, entre outras.

DIREITOS HUMANOS (DHU)

Objetivos: Ampliar o conhecimento objetivando coibir a prática de preconceito, discriminação, racismo e desrespeito aos direitos humanos, especialmente na perspectiva de combate a todo tipo de violência, ressaltando os seguintes temas:

Os direitos humanos na segurança privada representam o conjunto de princípios éticos, jurídicos e operacionais que garantem que a proteção do patrimônio e das pessoas nunca viole a dignidade humana, a integridade física e as liberdades individuais. Longe de ser apenas uma teoria, o respeito aos direitos humanos é um pilar prático e obrigatório de atuação para vigilantes, supervisores e gestores do setor.

CONSTITUIÇÃO FEDERAL.

É a lei suprema e mais importante de um país. Ela serve como a base de todo o ordenamento jurídico, o que significa que nenhuma outra lei ou decreto pode contrariá-la.

- **Garantir Direitos Fundamentais:** Define os direitos e deveres de todos os cidadãos. Exemplos: direito à vida, liberdade, igualdade, saúde, educação, segurança e propriedade.
- **Organizar o Estado:** Define como o país é estruturado politicamente. Ela divide e organiza os poderes em Executivo (Presidente, Governadores, Prefeitos), Legislativo (Deputados, Senadores, Vereadores) e Judiciário (Juízes e Tribunais).
- **Limitar o Poder do Governo:** Estabelece regras claras para que governantes não abusem do poder, protegendo o cidadão comum contra decisões arbitrárias do Estado.
- **Rígida:** Modificar o seu texto é um processo difícil e demorado. Alterações só podem ser feitas por meio de **Propostas de Emenda à Constituição (PECs)**, que exigem aprovação de grande maioria no Congresso.
- **Cláusulas Pétreas:** Existem pontos centrais da Constituição que **nunca podem ser apagados** ou reduzidos por nenhuma emenda. Exemplos: a forma federativa de Estado, o voto direto, secreto, universal e periódico, a separação dos Poderes e os direitos e garantias individuais.

PRINCÍPIOS FUNDAMENTAIS:

Direitos fundamentais da pessoa humana: São prerrogativas jurídicas historicamente conquistadas, positivadas na Constituição da República Federativa do Brasil (CRFB/88). Eles buscam proteger a dignidade da pessoa humana e limitar o arbítrio estatal. Suas principais características incluem a **universalidade** (aplicáveis a todos), a **irrenunciabilidade** (não se pode abrir mão deles) e a **inalienabilidade** (não possuem caráter comercial ou transferível)

b) direitos e garantias fundamentais (tortura, provas ilícitas, direito ao silêncio e o princípio da presunção da inocência);

Direitos e Garantias Fundamentais

A Constituição da República Federativa do Brasil (CRFB/88) diferencia os direitos (bens jurídicos protegidos em si) das garantias (instrumentos assecuratórios para exercer esses direitos). No bloco penal-processual, destacam-se quatro pilares:

- **Vedação à Tortura:** Proteção absoluta à integridade física e mental. Ninguém será submetido a tortura nem a tratamento desumano ou degradante (Art. 5º, III).
- **Provas Ilícitas:** São inadmissíveis no processo as provas obtidas por meios ilícitos (Art. 5º, LVI). Isso veda interceptações ilegais ou confissões extraídas sob coação física ou psicológica.
- **Direito ao Silêncio:** O preso será informado de seus direitos, entre os quais o de permanecer calado (Art. 5º, LXIII). Origina o princípio do *nemo tenetur se detegere* (ninguém é obrigado a produzir prova contra si mesmo).
- **Princípio da Presunção de Inocência:** Ninguém será considerado culpado até o trânsito em julgado de sentença penal condenatória (Art. 5º, LVII). O ônus da prova cabe inteiramente à acusação.

DIREITOS FUNDAMENTAIS DA PESSOA DETIDA

- O indivíduo sob custódia do Estado mantém todos os seus direitos não atingidos pela perda da liberdade. O texto constitucional e a Lei de Execução Penal (LEP) asseguram:
- **Respeito à Integridade:** É assegurado aos presos o respeito à integridade física e moral (Art. 5º, XLIX).
- **Identificação dos Responsáveis:** O preso tem direito à identificação dos responsáveis por sua prisão ou por seu interrogatório policial (Art. 5º, LXIV).
- **Comunicação Imediata:** A prisão de qualquer pessoa e o local onde se encontre serão comunicados imediatamente ao juiz competente e à família do preso ou à pessoa por ele indicada (Art. 5º, LXII).

O CRIME DE TORTURA E A LEI Nº 9.455/1997

- A tortura possui um mandato de criminalização explícito na Constituição da República Federativa do Brasil (CRFB/88).

Tratamento Constitucional (Art. 5º, XLIII)

- A lei considerará crimes **inafiançáveis e insuscetíveis de graça ou anistia** a prática da tortura. Nota de extrema relevância para provas: a tortura **é prescritível**. Os únicos crimes imprescritíveis na Constituição da República Federativa do Brasil (CRFB/88) são o racismo e a ação de grupos armados contra a ordem constitucional.

Aspectos Penais da Lei nº 9.455/1997

A lei tipifica as seguintes modalidades de tortura:

- **Tortura-Prova:** Constranger alguém com violência ou grave ameaça para obter informação, declaração ou confissão.
- **Tortura-Crime:** Constranger alguém para provocar ação ou omissão de natureza criminoso.
- **Tortura Discriminatória:** Constranger alguém em razão de discriminação racial ou religiosa.
- **Tortura-Castigo:** Submeter alguém sob sua guarda, poder ou autoridade, com emprego de violência ou grave ameaça, a intenso sofrimento físico ou mental, como forma de aplicar castigo pessoal ou medida preventiva.
- **Tortura do Preso:** Submeter pessoa presa ou sujeita a medida de segurança a sofrimento físico ou mental, por intermédio de ato não previsto em lei ou não resultante de medida legal.

- **Tortura por Omissão:** Aquele que se omite em face dessas condutas, quando tinha o dever de evitá-las ou apurá-las (pena menor: detenção de 1 a 4 anos).

Prisão e o Direito à Imagem

A Constituição da República Federativa do Brasil (CRFB/88) garante que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas" (Art. 5º, X). No contexto da prisão, o abuso na exposição do preso gera sanções severas:

- **Lei de Abuso de Autoridade (Lei nº 13.869/2019):** Considera crime constranger o preso ou detento, mediante violência, grave ameaça ou redução de sua capacidade de resistência, a exhibir-se ou ter seu corpo exibido à curiosidade pública, bem como divulgar trechos ou imagens de sua prisão de forma vexatória.
- **Garantia de Dignidade:** O preso não perde o direito de não ser exposto como "troféu" ou espetáculo midiático pela força policial.

Terrorismo, Segurança e Direitos Humanos

O Estado possui o dever de garantir a segurança pública e a ordem institucional, reprimindo o terrorismo de forma enérgica (conforme balizado pela Lei nº 13.260/2016). No entanto, o combate a ameaças à segurança nacional **não autoriza a suspensão total dos direitos humanos**.

- O terrorismo também é equiparado a hediondo (inafiançável e insuscetível de graça/anistia).
- Mesmo em estados de exceção legal (como o Estado de Defesa ou Estado de Sítio), o núcleo essencial dos direitos humanos fundamentais — como o direito à vida, à proibição de tortura e à dignidade — permanece **intocável**. A segurança do cidadão e do Estado deve coexistir sob o império da lei

Responsabilidade Civil e o Crime de Tortura

Quando um agente público comete o crime de tortura ou tratamento desumano/degradante, há dupla repercussão na esfera civil de indenizações:

Tipo de Responsabilidade: Responsabilidade Objetiva

Aplicada a Quem: Ao Estado (Pessoa Jurídica)

Regra de Configuração: Baseada no Art. 37, § 6º da CRFB/88. A vítima (ou seus familiares) precisa comprovar apenas o **fato administrativo** (conduta do agente), o **dano** sofrido e o **nexo causal**. Não é necessário provar que o Estado agiu com dolo ou culpa.

Tipo de Responsabilidade: Responsabilidade Subjetiva

Aplicada a Quem: Ao Agente Público (Indivíduo)

Regra de Configuração: O Estado, após indenizar a vítima, possui o **direito de regresso** contra o servidor público causador do dano. Nesse processo regressivo, exige-se a comprovação de **dolo ou culpa** do agente (o que é inerente e evidente no crime de tortura).

- **Tratamento Desumano:** Envolve a imposição de grave sofrimento físico ou mental, mas que não atinge o patamar de severidade absoluta da tortura, ou que não possui a finalidade específica exigida pelos tipos penais da tortura.
- **Tratamento Degradante:** É aquele focado em humilhar, menosprezar ou aviltar o indivíduo perante terceiros ou perante si mesmo. Visa quebrar a resistência moral ou física da vítima, gerando sentimentos de medo, angústia e inferioridade, independentemente de causar dor física.

PREVENÇÃO E COMBATE À VIOLÊNCIA CONTRA A MULHER

Este conteúdo aborda a legislação nacional para a Prevenção e o Combate à Violência Contra a Mulher, tópico recorrente em editais de Direito Penal, Processual Penal e Legislação Extravagante.

Lei Maria da Penha (Lei nº 11.340/2006)

A Lei Maria da Penha cria mecanismos para coibir e prevenir a violência doméstica e familiar contra a mulher, nos termos do art. 226, § 8º da CRFB/88.

- **Âmbito de Aplicação:** Configura violência doméstica qualquer ação ou omissão baseada no gênero que cause morte, lesão, sofrimento físico, sexual ou psicológico e dano patrimonial ou moral.
- **Espaços de Ocorrência:**
 - ✚ **Unidade Doméstica:** Espaço de convívio permanente de pessoas, com ou sem vínculo familiar, inclusive as esporadicamente agregadas.
 - ✚ **Âmbito da Família:** Comunidade formada por indivíduos que são ou se consideram aparentados, unidos por laços naturais, por afinidade ou por vontade expressa.
 - ✚ **Relação Íntima de Afeto:** Qualquer relação na qual o agressor conviva ou tenha convivido com a ofendida, independentemente de coabitação (Súmula 600 do STJ).
- **Medidas Protetivas de Urgência (MPUs):** Podem ser concedidas pelo juiz de imediato, sem audiência das partes. Podem obrigar o agressor (ex: afastamento do lar, proibição de aproximação) ou proteger a ofendida (ex: encaminhamento a programa de proteção, restituição de bens). O descumprimento de MPU constitui crime autônomo (Art. 24-A), sendo o único crime da lei que admite prisão preventiva decretada de ofício.
- **Ação Penal na Lesão Corporal:** A ação penal no crime de lesão corporal leve praticado com violência doméstica é **pública incondicionada** (Súmula 542 do STJ). A vítima não pode "retirar a queixa".

Tipos de Violência Contra a Mulher (Art. 7º da Lei Maria da Penha)

A lei elenca cinco formas de violência doméstica e familiar, cuja diferenciação é frequentemente cobrada em provas através de casos práticos:

- **Violência Física:** Entendida como qualquer conduta que ofenda a integridade ou saúde corporal da mulher (ex: socos, empurrões, queimaduras).
- **Violência Psicológica:** Qualquer conduta que cause danos emocional e diminuição da autoestima, ou que vise degradar ou controlar suas ações, comportamentos, crenças e decisões (ex: ameaças, humilhações, isolamento forçado, perseguição).
- **Violência Sexual:** Conduta que constranja a mulher a presenciar, a manter ou a participar de relação sexual não desejada, mediante intimidação, ameaça, coação ou uso da força (ex: estupro marital, impedimento do uso de métodos contraceptivos, aborto forçado).
- **Violência Patrimonial:** Conduta que configure retenção, subtração, destruição parcial ou total de seus objetos, instrumentos de trabalho, documentos pessoais, bens, valores e direitos ou recursos econômicos (ex: quebrar o celular da companheira, reter o cartão de salário).

- **Violência Moral:** Entendida como qualquer conduta que configure calúnia (imputar falsamente crime), difamação (imputar fato ofensivo à reputação) ou injúria (ofensa à dignidade ou decoro).
- *Nota: Deu origem ao crime autônomo de violência psicológica contra a mulher (Art. 147-B do Código Penal).*

Feminicídio (Lei nº 13.104/2015)

O feminicídio qualifica o crime de homicídio (Art. 121, § 2º, VI do CP) e está incluído no rol de **crimes hediondos** (Lei nº 8.072/1990).

- **Definição:** É o assassinato de mulher cometido por razões da condição de sexo feminino.
- **Razões da Condição de Sexo Feminino:** A lei considera que há essas razões quando o crime envolve:
 1. **Violência doméstica e familiar;**
 2. **Menosprezo ou discriminação à condição de mulher.**
- **Natureza da Qualificadora:** O STJ firmou entendimento de que o feminicídio possui natureza **objetiva**, pois se liga às condições da vítima (gênero). Portanto, é perfeitamente possível a coexistência do feminicídio com qualificadoras de natureza subjetiva, como o motivo torpe ou fútil.
- **Causas de Aumento de Pena:** A pena do feminicídio é aumentada de 1/3 até a metade se o crime for praticado durante a gestação ou nos 3 meses posteriores ao parto; contra menor de 14 anos, maior de 60 anos ou com deficiência; ou na presença física ou virtual de descendente ou de ascendente da vítima.

Protocolo "Não é Não" (Lei nº 14.786/2023)

Esta legislação foi criada para prevenir o constrangimento e a violência contra a mulher e para proteger a vítima em ambientes específicos onde há venda de bebidas alcoólicas.

- **Locais de Aplicação:** Casas noturnas, boates, espetáculos musicais em locais fechados e shows (eventos festivos em geral). **Não se aplica** a eventos de natureza estritamente religiosa.

Conceitos Importantes:

- **Constrangimento:** Qualquer insistência, física ou verbal, sofrida pela mulher depois de manifestada a sua discordância.
- **Violência:** Uso da força que resulte em lesão, morte ou danos psicológicos, entre outros, conforme a legislação penal.

Deveres dos Estabelecimentos:

- Manter pelo menos um funcionário qualificado para atender ao protocolo.
- Afastar a vítima do agressor e garantir o seu acompanhamento até o transporte se ela desejar deixar o local.
- Isolar o local onde existam vestígios da violência para perícia policial.
- Disponibilizar as imagens do sistema de segurança caso haja requisição policial ou judicial.

DIREITOS DAS CRIANÇAS E ADOLESCENTES (ECA - LEI Nº 8.069/1990)

O Estatuto da Criança e do Adolescente consolida a **Doutrina da Proteção Integral**, superando a antiga doutrina do menor em situação irregular.

Este estudo detalha o arcabouço jurídico de proteção a grupos vulneráveis, o combate ao racismo e à discriminação por orientação sexual, identidade de gênero, idade, religião e procedência nacional.

Princípios Matrizes:

- **Prioridade Absoluta:** Preferência na formulação de políticas públicas, destinação de recursos e atendimento nos serviços públicos (Art. 227 da CRFB/88).
- **Melhor Interesse da Criança:** Toda interpretação da lei deve visar o máximo bem-estar do menor
- **Definições Etárias:** Criança é a pessoa de até **12 anos incompletos**. Adolescente é aquela entre **12 e 18 anos**. Excepcionalmente, o ECA aplica-se a pessoas de até 21 anos.
- **Atos Infracionais e Medidas:** Crianças que cometem atos análogos a crimes recebem apenas **medidas protetivas** (Art. 101). Adolescentes estão sujeitos a **medidas socioeducativas** (Art. 112), sendo a internação a mais gravosa (prazo máximo de 3 anos).

DIREITOS DA PESSOA IDOSA (ESTATUTO DA PESSOA IDOSA - LEI Nº 10.741/2003)

Destina-se a regular os direitos assegurados às pessoas com idade **igual ou superior a 60 anos**.

- **Prioridade Especial:** A Lei nº 14.423/2022 alterou o termo "Estatuto do Idoso" para "Estatuto da Pessoa Idosa". Dentre os idosos, há prioridade especial para os **maiores de 80 anos**, que têm preferência sobre os demais idosos em atendimentos médicos e processos judiciais (exceto emergências de saúde).
- **Crimes em Espécie:** O estatuto tipifica crimes específicos, como discriminar a pessoa idosa (impedir acesso a cargos, recusar atendimento), abandonar em hospitais ou casas de saúde, e apropriar-se de proventos ou pensões (Art. 102).

ESTATUTO DA IGUALDADE RACIAL (LEI Nº 12.288/2010)

Este diploma formula políticas públicas e ações afirmativas para garantir a igualdade de oportunidades à população negra.

- **Ações Afirmativas:** Programas e medidas especiais adotados pelo Estado e pela iniciativa privada para a correção das desigualdades históricas.
- **Saúde e Educação:** Garante o direito à saúde integral da população negra (com diretrizes para patologias específicas, como a anemia falciforme) e a obrigatoriedade do ensino da história geral da África e da história da população negra no Brasil no ensino fundamental e médio.

CRIMES DE PRECONCEITO DE RAÇA OU DE COR (LEI Nº 7.716/1989)

Esta lei pune os atos de discriminação decorrentes de raça, cor, etnia, religião ou procedência nacional.

- **Inafiançabilidade e Imprescritibilidade:** Conforme o mandado constitucional (Art. 5º, XLII), a prática do racismo constitui crime inafiançável e imprescritível, sujeito à pena de reclusão.
- **Injúria Racial (Lei nº 14.532/2023):** A injúria racial (ofensa à dignidade associando elementos de raça, cor ou etnia) foi equiparada ao crime de racismo. Portanto, tornou-se **imprescritível, inafiançável** e passou a integrar o texto da Lei nº 7.716/1989.
- **Consequências do Racismo:**
 - ✓ **Materiais:** Perpetuação da desigualdade salarial, barreiras no acesso a cargos de chefia, segregação espacial (favelização) e maior letalidade policial.
 - ✓ **Psíquicas:** Estresse crônico por vigilância social, baixa autoestima, traumas por humilhação pública e depressão decorrente da exclusão sistemática.

OUTRAS DISCRIMINAÇÕES (ETÁRIA, RELIGIOSA, PROCEDÊNCIA NACIONAL)

O preconceito manifesta-se por diversas vertentes jurídicas protegidas pela Lei nº 7.716/1989 e pelo Código Penal:

- **Discriminação Religiosa:** O Art. 208 do Código Penal pune o ultraje a culto e impedimento de ato religioso. A Lei nº 7.716/1989 pune a discriminação religiosa com reclusão, protegendo fortemente as religiões de matriz africana contra a intolerância.
- **Procedência Nacional e Antissemitismo:** A discriminação contra indivíduos devido ao seu país de origem ou região do Brasil (ex: xenofobia contra nordestinos) é crime. O antissemitismo (preconceito contra judeus) e a islamofobia são processados criminalmente dentro desta vertente.

LGBTFOBIA: TRATAMENTO JURÍDICO E CONSEQUÊNCIAS

No Brasil, os atos de homofobia e transfobia são punidos penalmente por meio da **equiparação ao crime de racismo**, conforme tese fixada pelo STF na ADO 26 e no MI 4733.

- **Enquadramento Legal:** Enquanto o Congresso Nacional não edita lei específica, condutas homofóbicas e transfóbicas que envolvem aversão odiosa à orientação sexual ou identidade de gênero enquadram-se nos tipos penais da Lei nº 7.716/1989.

Consequências da LGBTfobia:

- **Materiais:** Expulsão do núcleo familiar com consequente evasão escolar; exclusão do mercado de trabalho formal (especialmente para pessoas trans, empurradas majoritariamente para a informalidade ou prostituição); e desamparo habitacional.
- **Psíquicas:** Altos índices de ideação suicida e automutilação; ansiedade gerada pelo medo constante de agressão física em vias públicas (hipervigilância); e sofrimento decorrente do não reconhecimento da própria identidade de gênero (disforia social induzida pelo preconceito).

A análise sistemática dos tópicos abordados consolida a centralidade dos **Direitos Humanos** como o eixo norteador de todo o ordenamento jurídico e da atuação do Estado, especialmente na segurança pública.

Podem-se extrair três conclusões fundamentais desse conjunto de normas:

O Princípio da Dignidade Humana como Limite Absoluto: A vedação à tortura, o controle sobre as provas ilícitas, os direitos da pessoa detida e a proteção à imagem demonstram que a persecução penal não possui poderes ilimitados. A eficiência policial e a segurança do Estado devem, obrigatoriamente, coexistir com o respeito aos direitos e garantias fundamentais.

Especial Proteção aos Grupos Vulneráveis: A existência de diplomas específicos — como a Lei Maria da Penha, o Estatuto da Pessoa Idosa, o Estatuto da Criança e Adolescente, o Estatuto da Igualdade Racial e o Protocolo "Não é Não" — reflete o compromisso de promover a igualdade material. O Estado reconhece as vulnerabilidades históricas e sociais de mulheres, crianças, idosos, populações negras e comunidade LGBTQIA+, editando normas repressivas e preventivas para mitigar as consequências materiais e psíquicas da discriminação.

Crescente Rigor Penal e Responsabilização: A evolução legislativa demonstra um endurecimento contra crimes de ódio e de abuso de poder. Isso se reflete na equiparação da homofobia e da injúria racial ao crime de racismo (tornando-os inafiançáveis e imprescritíveis), na hediondez do feminicídio e na aplicação da responsabilidade civil objetiva do Estado em casos de tratamentos degradantes.

Em suma, a compreensão dessas leis vai além do conhecimento técnico-jurídico; ela estabelece o padrão ético e operacional exigido para que o uso da força e a aplicação da lei ocorram sempre sob o império da democracia e dos Direitos Humanos.

RELAÇÕES HUMANAS NO TRABALHO (RHT)

Objetivos: Dotar o aluno de conhecimentos que o capacitem a desenvolver hábitos de sociabilidade que permitam aprimorar seu relacionamento no trabalho.

Constituem o conjunto de interações, comportamentos e atitudes que ocorrem entre as pessoas no ambiente corporativo. Na segurança privada, a RHT é uma ferramenta operacional crítica: o vigilante lida diretamente com o público, autoridades e clientes, onde a empatia, o controle emocional e a comunicação evitam o uso da força e garantem a integridade física de todos.

Evolução Histórica: Originada na Teoria das Relações Humanas (Elton Mayo), que provou que o bem-estar psicológico e a integração social influenciam diretamente a produtividade e o foco.

Objetivo na Segurança: Substituir a postura puramente truculenta ou reativa por um modelo focado em **comunicação assertiva**, mediação de conflitos e atendimento ao cliente, humanizando o serviço sem perder a autoridade

A. Comunicação Interpessoal

Trata-se da interação direta entre duas ou mais pessoas, detalhamos abaixo a mecânica técnica, os fluxos de mensagens e os desafios de expressão no ambiente da segurança privada.

Princípios da Comunicação Interpessoal: A comunicação interpessoal eficaz é regida por regras fundamentais que garantem a clareza e o respeito profissional no ambiente de trabalho:

- **Inevitabilidade:** É impossível não se comunicar. Mesmo em silêncio, a postura corporal, a expressão facial e o posicionamento do vigilante transmitem uma mensagem de atenção, desleixo ou hostilidade.
- **Irreversibilidade:** Uma palavra dita ou uma ordem expressa não podem ser apagadas. Na segurança, um comando verbal mal colocado pode escalar um conflito de forma irreversível.
- **Contextualização:** A comunicação depende do ambiente e dos envolvidos. A forma de falar com um colega de equipe em uma frequência de rádio restrita é diferente da abordagem utilizada com um cliente ou com uma autoridade policial.
- **Objetividade:** A mensagem deve ser direta e sem ambiguidades. No meio operacional, instruções prolixas ou confusas geram falhas graves na execução de procedimentos de segurança.

O Processo de Comunicação: A comunicação é um processo dinâmico composto por elementos interdependentes. Se um deles falhar, ocorre a quebra do entendimento:

[Emissor] -> (Codificação) -> [Mensagem / Canal] -> (Decodificação) -> [Receptor] ----- (Feedback / Retorno) -----
--

- ✓ **Emissor:** Quem inicia a comunicação (ex: o Vigilante Líder transmitindo uma ordem).
- ✓ **Codificação:** A transformação da ideia em símbolos compreensíveis (palavras, gestos, códigos de rádio como o Código Q).
- ✓ **Mensagem:** O conteúdo da informação que está sendo transmitida.

- ✓ **Canal:** O meio físico por onde a mensagem trafega (a fala direta, o aparelho de rádio HT, uma mensagem de texto no sistema).
- ✓ **Decodificação:** A interpretação dos símbolos feita por quem recebe a mensagem.
- ✓ **Receptor:** O destinatário final da informação (ex: o vigilante do posto de perímetro).
- ✓ **Feedback (Retorno):** A confirmação de que a mensagem foi compreendida. Na segurança, o famoso "Ciente" ou "QSL" é o feedback que fecha o circuito com segurança.
- ✓ **Ruído:** Qualquer interferência que prejudique a transmissão ou a compreensão da mensagem (barulho do ambiente, sinal de rádio ruim, uso de gírias)

Linguagem e Problemas da Fala: O uso correto da linguagem e a identificação de barreiras de fala são essenciais para manter o profissionalismo e a acessibilidade em postos de atendimento ao público:

Tipos de Linguagem na Segurança:

- **Linguagem Verbal:** Palavras faladas ou escritas. Deve primar pela norma culta simples, clareza técnica e ausência de gírias ou jargões excessivos que o público comum não entenda.
- **Linguagem Não Verbal:** Gestos, postura, tom de voz e expressões faciais. Um vigilante com os braços cruzados e testa franzida transmite uma barreira agressiva, enquanto uma postura ereta com os braços relaxados ao lado do corpo transmite prontidão e acessibilidade.

Problemas e Barreiras da Fala: No dia a dia operacional, o profissional deve estar atento a fatores que prejudicam a dicção e a recepção da mensagem:

- **Problemas Fisiológicos e de Dicção:** Gagueira, rouquidão extrema ou velocidade excessiva na fala (*taquilalia*). Em momentos de estresse ou sob o efeito da adrenalina, a tendência natural é falar rápido demais, o que torna as ordens incompreensíveis pelo rádio ou para o público.
- **Vícios de Linguagem e Gírias:** O uso excessivo de termos informais destrói a autoridade técnica da segurança e pode ser interpretado como falta de respeito ou deboche pelo interlocutor.
- **Barreiras Psicológicas:** O medo, a raiva ou o nervosismo alteram o tom de voz e o vocabulário utilizado, prejudicando o autocontrole exigido pela função.

B. Ética Profissional

Na segurança privada é o conjunto de princípios morais e regras de conduta que guiam as ações de empresas e profissionais. Ela serve para garantir que a força, a autoridade e as informações sigilosas confiadas ao setor sejam utilizadas estritamente dentro da legalidade e do respeito aos direitos humanos.

Sob as diretrizes do Estatuto da Segurança Privada (Lei nº 14.967/2024), o desenvolvimento da ética divide-se em duas frentes de governança e *compliance* corporativo: os colaboradores internos e os parceiros de negócios.

Desenvolver a Ética nos Colaboradores: Desenvolver a ética na equipe interna (vigilantes, supervisores, fiscais e gestores) exige a transformação de conceitos teóricos em atitudes práticas no posto de serviço [14.967/2024]:

- **Código de Conduta Claro:** A empresa deve instituir um Código de Ética e Conduta objetivo. Ele deve detalhar o que é esperado do profissional em relação ao sigilo de informações, uso de redes sociais e comportamento com o público.
- **Treinamento em Direitos Humanos e Cidadania:** Integrar à atualização bienal debates práticos sobre o combate à discriminação, racismo estrutural, homofobia e preconceito de classe em abordagens.

- **Canais de Denúncia Anônimos:** Manter um canal seguro e sem retaliações para que os próprios colaboradores possam reportar desvios de conduta, corrupção, maus-tratos ou uso excessivo da força por parte de colegas ou superiores.
- **Liderança pelo Exemplo:** Supervisores e gestores devem praticar a ética diariamente. Uma liderança que tolera pequenos desvios perde a autoridade moral para cobrar a postura dos vigilantes da linha de frente.

Aplicação Prática no Posto de Serviço:

- **Princípio da Legalidade:** O vigilante atua estritamente dentro do que a lei permite, recusando ordens ilegais de clientes (como realizar revistas abusivas ou aplicar punições físicas).
- **Princípio do Sigilo Profissional:** Não compartilhar em grupos de mensagens ou redes sociais imagens de câmeras de segurança (CFTV), rotas de carros-fortes ou rotinas de executivos protegidos.

C. Desenvolver a Ética nos Parceiros

Os parceiros comerciais — que englobam os **clientes contratantes**, fornecedores de tecnologia/armamento e empresas terceirizadas prestadoras de serviços complementares — também devem estar alinhados com os padrões éticos exigidos pela legislação, sobretudo pela CRFB/1988, pela Lei nº 14.967/2024 e demais normas citadas nesta obra.

Alinhamento de Expectativas Contratuais: Deixar claro em contrato que a empresa de segurança privada obedece rigidamente à Lei nº 14.967/2024 e à Instrução Normativa e Portarias da Polícia Federal. O cliente não pode exigir que o vigilante atue fora de suas prerrogativas legais (como fazer segurança externa na rua ou atuar como "leão de chácara" agressivo).

Homologação e Compliance de Fornecedores: Comprar armamento, munição, coletes balísticos e sistemas de CFTV apenas de fornecedores devidamente autorizados, auditados e que emitam notas fiscais regulares, combatendo o mercado ilegal de equipamentos.

Repressão Coletiva à Clandestinidade: Firmar um compromisso ético com parceiros de mercado para denunciar empresas clandestinas (seguranças informais ou "bicos" armados). A clandestinidade precariza o trabalho e mancha a reputação de todo o setor.

Responsabilidade Social Compartilhada: Desenvolver com os clientes protocolos de atendimento inclusivos, garantindo que o ambiente do contratante (seja um shopping, banco ou indústria) seja monitorado de forma justa, transparente e sem vieses preconceituosos.

D. Princípios de Disciplina

Os princípios disciplinares guiam o comportamento diário do vigilante, garantindo a ordem hierárquica e a eficiência operacional em campo:

- **Hierarquia e Disciplina:** A segurança privada adota uma estrutura de subordinação clara (Vigilante → Líder → Fiscal → Supervisor → Gestor) [14.967/2024]. O cumprimento das ordens legais dos superiores deve ser imediato e exato.
- **Apresentação Pessoal Impecável:** O uso do uniforme padrão homologado pela PF deve ser rigoroso. Isso inclui calçados limpos, barba feita ou aparada, cabelos alinhados e postura ereta. O uniforme limpo e bem cuidado transmite autoridade técnica e previne ameaças pela simples presença visual.

- **Manutenção e Cuidado com Equipamentos:** Zelar pelo armamento, munições, coletes e rádios transmissores sob sua cautela. Toda irregularidade ou falha técnica no equipamento deve ser registrada de imediato no livro de ocorrências para manutenção.
- **Respeito e Urbanidade:** Tratar colegas de equipe, superiores, autoridades públicas e o público geral com a máxima cortesia, independentemente da situação de estresse do momento.

Horários (Pontualidade e Assiduidade): Na segurança privada, o tempo é medido em vidas e patrimônios protegidos. A quebra de horários compromete diretamente a segurança do posto de serviço:

- **Rendição de Posto:** O vigilante **nunca** deve abandonar o seu posto de serviço antes da chegada de seu substituto (rendição). O abandono de posto sem cobertura configura falta gravíssima e, dependendo do caso, crime.
- **Pontualidade Rigorosa:** Chegar ao posto de serviço com antecedência mínima de 15 minutos do início oficial do turno. Esse tempo é indispensável para realizar a passagem de serviço, conferir as armas e munições em carga e ler as novidades no livro de ocorrências.
- **Assiduidade:** Faltas não justificadas desorganizam as escalas de serviço da empresa, sobrecarregam os colegas de turno que deverão permanecer no posto até serem substituídos e geram multas contratuais junto aos clientes.

Assuntos Confidenciais (Sigilo Profissional): O operador de segurança tem acesso constante a vulnerabilidades, dados financeiros e rotinas privadas de alto valor comercial ou pessoal. O vazamento de informações destrói a confiança na empresa de segurança:

- **Segurança da Informação:** É proibido repassar a terceiros, parentes ou amigos quaisquer detalhes sobre a rotina do posto (horários de abertura e fechamento, rotas de viaturas, número de vigilantes escalados ou posicionamento de câmeras de CFTV).
- **Vedações Digitais:** Não capturar fotos ou vídeos de incidentes operacionais, do interior de bases blindadas ou de carros-fortes para postagem em redes sociais ou compartilhamento em aplicativos de mensagens.
- **Sigilo Bancário e Comercial:** No transporte de valores e vigilância bancária, informações sobre quantias transportadas, datas de abastecimento de caixas eletrônicos e dados de clientes internos devem ser tratados como segredo legalmente protegido.

Compromisso Profissional: O compromisso profissional representa o pacto de responsabilidade que o operador assume com a proteção de vidas e com a legalidade de suas ações:

- **Consciência do Dever:** Entender que a função exige prontidão contínua. O vigilante deve manter-se em estado de alerta durante todo o turno de serviço, evitando distrações como o uso recreativo de celulares ou leituras alheias à função.
- **Legalidade Prática:** Manter o compromisso de atuar rigorosamente dentro dos limites legais [14.967/2024]. O vigilante deve se recusar a executar ordens manifestamente ilegais ou abusivas passadas por clientes (como aplicar castigos físicos ou realizar revistas vexatórias).
- **Treinamento Contínuo:** Manter o compromisso com o autodesenvolvimento técnico, participando de forma ativa das atualizações obrigatórias, treinamentos de tiro defensivo e atualizações normativas fornecidas pela empresa ou escola de formação.

E. Princípios de Disciplina

A disciplina na segurança privada não é apenas uma conduta de comportamento, mas um fator de sobrevivência e eficiência tática. Ela se fundamenta em quatro pilares práticos:

- **Princípio da Hierarquia:** Acatamento integral e imediato das ordens legais emanadas de superiores (Vigilante Líder, Fiscal, Supervisor e Gestor) [14.967/2024]. Ordens manifestamente ilegais devem ser recusadas e reportadas.
- **Apresentação Visual e Uniformização:** Uso rigoroso do uniforme padrão homologado pela Polícia Federal, limpo e bem alinhado. A imagem do vigilante é o primeiro nível do *Uso Progressivo da Força* (Presença Física), transmitindo autoridade e desestimulando ações criminosas por vias visuais.
- **Zelo pelo Material de Carga:** Manutenção preventiva e cuidado com o armamento, munições, colete balístico e rádio transmissor (HT) sob sua cautela. Qualquer avaria ou extravio deve ser comunicado imediatamente à empresa.
- **Urbanidade e Controle Emocional:** Tratar com absoluto respeito e cortesia os colegas de trabalho, funcionários do cliente e o público em geral, mantendo a sobriedade mesmo diante de provocações ou desacatos.

Horários (Pontualidade e Assiduidade): Na segurança, o tempo é medido pela continuidade da proteção. A quebra de horários gera vulnerabilidades críticas que comprometem o posto e a empresa:

- **A Regra de Ouro da Rendição:** O vigilante **nunca** desocupa ou abandona seu posto de serviço sem a chegada física e a efetiva assunção do seu substituto de turno. O abandono de posto sem cobertura configura falta gravíssima e pode gerar demissão por justa causa.
- **Margem de Antecedência:** Apresentar-se ao posto com antecedência mínima de 15 a 20 minutos do início oficial da escala. Esse período é obrigatório para a correta passagem de serviço, leitura das novidades no livro de ocorrências e conferência física das munições e armas em carga.
- **Assiduidade:** O cumprimento rigoroso da escala de repouso (folgas) e plantões evita dobras forçadas de horário dos colegas de equipe, reduzindo a fadiga física e prevenindo falhas de atenção causadas pelo cansaço extremo.

Assuntos Confidenciais (Sigilo Profissional): O operador de segurança lida diariamente com dados sensíveis, pontos vulneráveis e rotinas de alto valor financeiro ou estratégico. O vazamento de informações é uma falha disciplinar gravíssima e responsabilização civil e criminal.

- **Segurança da Informação Físico-Digital:** É expressamente proibido tirar fotos ou filmar o interior de bases operacionais, tesourarias, carros-fortes ou sistemas de CFTV para publicação em redes sociais ou compartilhamento em aplicativos de mensagens particulares.
- **Compartimentação de Dados:** Não discutir com familiares, amigos ou terceiros estranhos ao serviço as rotinas de abastecimento de caixas eletrônicos, horários de abertura e fechamento de agências, quantidade de vigilantes armados no posto ou pontos cegos de câmeras.
- **Proteção de Ativos Intangíveis:** Tratar dados cadastrais de funcionários, visitantes ou clientes internos como segredos corporativos sigilosos, impedindo o acesso visual ou físico de pessoas não autorizadas às pranchetas ou telas de controle de acesso.

Compromisso Profissional: Representa a dedicação técnica e a responsabilidade social que o profissional assume ao portar uma credencial de segurança chancelada pelo Estado [14.967/2024]:

- **Estado de Alerta Contínuo:** Manter a atenção focada integralmente nas linhas de varredura visual do posto durante o turno de serviço. Dispositivos eletrônicos

particulares (smartphones) só devem ser utilizados em horários de intervalo regulamentares, eliminando distrações que facilitem ações criminosas por surpresa.

- **Responsabilidade no Porte de Arma:** Consciência técnica sobre o uso do armamento e do colete balístico. O vigilante assume o compromisso de utilizar a arma estritamente em legítima defesa própria ou de terceiros, aplicando os princípios de proporcionalidade e estrita necessidade jurídica.
- **Atualização e Capacitação:** Compromisso pessoal com o aperfeiçoamento contínuo, demonstrando proatividade durante as atualizações obrigatórias bienais, treinamentos de tiro tático defensivo e simulações de gerenciamento de crise promovidas pela empresa.

F. Comando e Subordinação

Na segurança privada estabelecem a estrutura de governança tática necessária para que as operações funcionem sem falhas ou conflitos de autoridade. Devido à natureza da profissão — que lida com riscos reais, uso de armamento e proteção de vidas —, a cadeia de comando precisa ser tão clara e respeitada quanto a de uma força de segurança pública [Decreto nº 13.012/2026].

Unidade de Comando: O princípio da Unidade de Comando determina que cada colaborador deve responder a apenas um único superior direto.

- **O que evita:** Conflitos de ordens e dubiedade nas ações. Se dois supervisores derem ordens diferentes ao mesmo tempo para um vigilante em uma crise, a operação entra em colapso.
- **Aplicação Prática no Posto:** O vigilante que atua em um cliente terceirizado (ex: uma agência bancária ou shopping) deve seguir as ordens e procedimentos técnicos ditados pela sua **empresa de segurança privada** (através do Vigilante Líder, Fiscal ou Supervisor) e não de funcionários aleatórios do cliente [14.967/2024].
- **Fluxo de Decisão:** O cliente reporta a demanda ao Supervisor da empresa de segurança, e este traduz e transmite a ordem legal para a equipe de vigilantes em campo.

Necessidade da Subordinação: A subordinação não significa submissão pessoal ou humilhação, mas sim o **acatamento técnico e profissional às diretrizes de quem detém a responsabilidade legal** sobre a operação [14.967/2024].

- **Sincronia Tática:** Em situações de emergência (como um assalto com reféns ou incêndio), não há tempo para debates ou votações. A subordinação garante que o plano de contingência desenhado pela Gestão de Segurança seja executado de forma imediata e coordenada por toda a equipe.
- **Segurança Jurídica:** Ao cumprir estritamente as ordens e manuais de procedimentos passados pela liderança, o vigilante resguarda a si mesmo perante a lei. Se ele agir por conta própria e fora das normas, responderá individualmente pelos excessos civis e penais cometidos.
- **Manutenção da Ordem Interna:** Garante a estabilidade da empresa, a padronização no cumprimento das escalas de trabalho, o uso correto dos equipamentos de carga e o respeito às normas da Polícia Federal.

Acompanhamento do Profissional: O comando não se limita a dar ordens; ele exige o acompanhamento contínuo e a supervisão do desempenho de cada integrante da equipe de segurança.

- **Avaliação de Desempenho Operacional:** O Supervisor e o Fiscal avaliam periodicamente se o vigilante mantém o estado de alerta, cumpre as normas do posto, manuseia o armamento corretamente e atende o público com urbanidade
- **Feedback e Alinhamento Técnico:** Apontar de forma construtiva os pontos cegos que o vigilante está deixando no posto (ex: distração com o celular, falha na varredura visual) e reforçar as condutas exemplares para motivar a equipe.
- **Apoio Psicológico e Comportamental:** Identificar sinais de fadiga extrema, estresse severo ou problemas pessoais que possam comprometer a atenção do profissional. Na segurança privada, um operador psicologicamente abalado portando uma arma representa um risco para si e para terceiros.
- **Planejamento de Carreira e Treinamento:** Identificar quais vigilantes demonstram perfil de liderança e disciplina para indicações a cursos de extensão, reciclagens específicas ou promoções para cargos de Vigilante Líder ou Supervisor [14.967/2024].

G. **Princípios de Apresentação e Asseio Pessoal**

Na segurança privada vão muito além da vaidade ou da estética. Eles fazem parte da estratégia de prevenção e controle operacional do posto de serviço. A imagem do vigilante é o primeiro nível do **Uso Progressivo da Força (Presença Física)**: um profissional alinhado, asseado e postado corretamente transmite autoridade técnica, organização e prontidão, o que desestimula ações criminosas por vias visuais [Decreto nº 13.012/2026].

Apresentação Pessoal: A apresentação pessoal diz respeito aos elementos visuais e uniformização que caracterizam a autoridade do vigilante no posto [18.045/2023]:

- **Uso Rigoroso do Uniforme Homologado:** O uniforme é de uso obrigatório em serviço e deve ser estritamente aquele aprovado pela Polícia Federal para a empresa. Deve estar sempre limpo, passado e sem rasgos. É proibido misturar peças civis (como bonés ou jaquetas particulares) com a uniformização
- **Calçados e Coturnos:** Devem estar limpos e engraxados. Calçados sujos ou desgastados transmitem desleixo e passam a impressão de falta de fiscalização no posto.
- **Colete de Proteção Balística:** Item de segurança obrigatório nas modalidades com uso de arma. Deve estar ajustado perfeitamente ao corpo, limpo e com a capa de tecido conservada, garantindo a proteção e a imagem de prontidão.

Identificação Visível: O uso do crachá da empresa e da Carteira Nacional de Vigilante (CNV) em local visível é obrigatório para identificação imediata pelo cliente e pelos órgãos de fiscalização.

Asseio Pessoal: O asseio pessoal refere-se à higiene e aos cuidados corporais que garantem uma convivência profissional harmoniosa nas Relações Humanas no Trabalho (RHT):

- **Higiene Corporal Diária:** O banho diário e o uso de desodorante neutro são indispensáveis. Devido à carga horária extensa (escalas de 12h) e ao esforço físico das rondas, a higiene rigorosa previne odores desagradáveis no posto ou nas viaturas.
- **Barba e Cabelo:** O cabelo deve estar curto ou preso de forma discreta (no caso de cabelos longos), para não obstruir a visão ou virar um ponto de vulnerabilidade em uma luta corporal. A barba deve estar feita ou aparada de forma alinhada e discreta.
- **Unhas:** Devem estar cortadas e limpas. Unhas compridas acumulam sujeira e podem ferir o próprio profissional ou terceiros durante procedimentos de revista pessoal ou contenção física.

- **Uso de Adornos e Acessórios:** Anéis, pulseiras, correntes chamativas e brincos grandes devem ser evitados em serviço. Além de quebrarem a padronização visual, representam um risco tático grave, pois podem enroscar em equipamentos ou ser usados por um agressor para machucar o vigilante em um confronto físico.

Cuidados com sua Imagem Profissional: A imagem profissional é a reputação técnica construída pelo operador por meio de seu comportamento e postura, dentro e fora do posto de serviço:

- **Postura Corporal no Posto:** Evitar ficar escorado em paredes, sentado de forma relaxada em locais de passagem ou com as mãos nos bolsos. A postura deve ser ereta, com os braços relaxados ao lado do corpo ou na linha da cintura (posição de entrevista), demonstrando que o profissional está em pleno estado de alerta.
- **Comportamento em Público:** Evitar conversas informais longas e risadas excessivas com funcionários do cliente ou transeuntes. O vigilante deve ser focado, cortês e direto, mantendo o distanciamento profissional necessário para não perder o foco da vigilância.
- **Conduta Fora de Serviço (O Uniforme na Rua):** O uniforme e a credencial carregam o nome da empresa e a chancela da Polícia Federal. O vigilante não deve frequentar bares, consumir bebidas alcoólicas ou se envolver em discussões públicas utilizando a uniformização, mesmo que esteja fora do horário de trabalho.
- **Presença Digital:** Cuidado com postagens em redes sociais. Publicar fotos uniformizado portando armamento, expondo instalações do cliente ou emitindo opiniões agressivas destrói a imagem profissional e viola os códigos de conduta e disciplina das empresas de segurança

H. Posturas Desejadas do Profissional de Segurança Privada

Representam o conjunto de atitudes práticas que diferenciam um operador técnico de um executor comum. Em um setor dinâmico, monitorado pela Polícia Federal e pautado pelo cumprimento da legislação vigente, a postura adotada no dia a dia é o fator decisivo para a eficácia das operações de proteção [Lai nº 14.967/2024].

Conhecimento da Profissão: O domínio técnico é o alicerce de toda e qualquer ação de segurança. Um profissional sem conhecimento atua baseado em palpites, gerando riscos jurídicos e operacionais graves.

- **O que abrange:** Compreensão detalhada da legislação (como a Lei nº 14.967/2024 e o Código Penal), das normas internas do posto de serviço e das técnicas operacionais de sua função (tiro defensivo, primeiros socorros, controle de acesso) [Lai nº 14.967/2024].
- **Aplicação Prática:** Saber exatamente os limites legais do direito de retenção de um suspeito e os critérios do *Uso Progressivo da Força*, evitando cometer o crime de abuso de autoridade ou constrangimento ilegal.

Comprometimento: É o envolvimento real e responsável com a missão de proteger vidas e o patrimônio alheio. O profissional comprometido não trabalha apenas pelo cumprimento do horário, mas pela integridade do ambiente.

- **O que abrange:** Dedicção mútua com a empresa e com o cliente do posto, respeito aos horários de escala, cuidado rigoroso com os materiais de carga e manutenção do estado de prontidão permanente.
- **Aplicação Prática:** Recusar-se a ceder às distrações, mantendo o smartphone guardado durante o turno e focando integralmente na varredura visual de seu perímetro de vigilância.

Bom Senso: O bom senso é a capacidade de avaliar cenários com equilíbrio, razoabilidade e inteligência prática. Nem todas as situações do dia a dia estão previstas em manuais rígidos, cabendo ao operador tomar a decisão mais sensata.

- **O que abrange:** Analisar a gravidade de uma situação antes de agir, escolhendo a resposta menos danosa e mais eficiente para conter uma crise.
- **Aplicação Prática:** Ao deparar-se com uma gestante ou um idoso tentando acessar uma agência bancária com pertences metálicos permitidos por lei, orientá-los de forma calma, conduzindo-os pelo acesso lateral assistido em vez de tratá-los de forma hostil ou ríspida na porta giratória.

Imparcialidade: O operador de segurança privada representa a lei, a ordem técnica e as normas do estabelecimento. Suas ações nunca podem ser influenciadas por simpatias, antipatias ou vieses pessoais.

- **O que abrange:** Tratar todas as pessoas sob os mesmos critérios e regras estabelecidos pelo posto, combatendo rigorosamente qualquer tipo de preconceito de raça, gênero, orientação sexual, idade ou classe social.
- **Aplicação Prática:** Aplicar os rigorosos procedimentos de revista e controle de crachá com o mesmo nível de exigência técnica tanto para o funcionário terceirizado da limpeza quanto para o diretor do alto escalão da empresa contratante.

Empenho Profissional: É a busca voluntária pela excelência na prestação do serviço e pelo autodesenvolvimento contínuo. Reflete a proatividade do vigilante em ir além do básico exigido pelo dia a dia.

- **O que abrange:** Dedicção máxima durante as reciclagens obrigatórias bienais, atenção especial às simulações de evacuação de emergência e proatividade para identificar vulnerabilidades físicas antes que um crime aconteça.
- **Aplicação Prática:** Perceber uma lâmpada queimada ou uma cerca perimetral danificada nos fundos do pátio industrial e gerar um relatório técnico imediato para a supervisão, antecipando-se a uma possível intrusão noturna.

I. Gerenciamento de Conflitos

É uma das competências comportamentais mais críticas na segurança privada contemporânea. Em um setor pautado pelo cumprimento estrito da legalidade e dos direitos humanos, a capacidade de identificar, mediar e neutralizar atritos por meio do diálogo é a principal ferramenta do operador para evitar a escalada da violência e o uso desnecessário da força física ou de armamentos [Decreto nº 13.012/2026].

Conceito de Conflito: O conflito ocorre quando há uma quebra de harmonia devido a uma divergência de interesses, necessidades, valores ou percepções entre duas ou mais partes. Na segurança privada, os conflitos no posto de serviço geralmente se originam de três fatores principais:

- **Conflito de Normas vs. Desejos:** Ocorre quando o vigilante precisa aplicar uma regra de segurança (ex: proibição de entrada sem crachá ou exigência de revista de sacolas) e o cidadão se recusa a cumprir, sentindo-se contrariado ou ofendido.
- **Falhas e Ruídos de Comunicação:** O uso de tons de voz agressivos, gírias inadequadas ou comandos confusos por parte da equipe de segurança, transformando um atendimento rotineiro em um embate pessoal.
- **Fatores Externos e Emocionais:** Situações em que o cliente ou usuário já chega ao estabelecimento sob forte estresse, nervosismo ou frustração (ex: filas longas em bancos, atrasos em portões de embarque), tornando-se agressivo diante de qualquer imposição de barreira.

Regra de Ouro: O conflito não é necessariamente negativo; ele é uma característica das interações humanas. O problema reside na forma como ele é conduzido. Se for mal gerenciado, evolui para a agressão física; se for bem mediado, resolve a situação mantendo a ordem e o respeito mútuo.

Como Gerenciar Conflitos (Técnicas de Mediação): Para gerenciar um atrito de forma técnica, o profissional de segurança deve adotar o modelo de **Verbalização Assertiva e Desescalada**, estruturado em cinco etapas operacionais consecutivas:

1. Manter o Autocontrole e a Inteligência Emocional

- **Ação:** Diante de insultos ou gritos, o vigilante não deve revidar no mesmo tom. Ele deve respirar fundo, manter a voz baixa, firme e pausada.
- **Fundamento:** O operador deve compreender que a insatisfação do cidadão é contra a regra ou contra a instituição, e não um ataque pessoal ao indivíduo por trás do uniforme. Revidar anula a autoridade técnica do profissional.

2. Adotar a Escuta Ativa e a Empatia

- **Ação:** Permitir que a pessoa fale e exponha sua frustração sem interrupções imediatas. Manter o contato visual e demonstrar que está prestando atenção à demanda.
- **Fundamento:** Muitas vezes, o simples ato de desabafar diminui a carga de adrenalina do interlocutor. Dizer frases neutras como *"Entendo a sua frustração, o senhor tem razão em estar chateado, mas..."* ajuda a desarmar a postura defensiva da pessoa

3. Cuidar da Linguagem Não Verbal (Postura Corporal)

- **Ação:** Manter as mãos visíveis na altura da cintura (Postura de Entrevista ou de Prontidão Discreta), evitar apontar o dedo em riste, cruzar os braços ou aproximar-se excessivamente do espaço pessoal do cidadão.
- **Fundamento:** Gestos agressivos fecham canais de negociação e geram reações de ataque ou defesa. A postura correta transmite segurança, transparência e profissionalismo.

4. Apresentar a Solução Técnica com Foco na Norma

- **Ação:** Explicar o motivo da restrição de forma clara, educada e impessoal, transferindo o peso da decisão para o regulamento ou para a lei, e oferecendo uma alternativa viável quando houver.
- **Fundamento:** Em vez de dizer *"O senhor não vai entrar porque eu não quero"*, a postura correta é *"Senhor, por normas de segurança bancária da Polícia Federal, o acesso com esse objeto só é permitido através do canal lateral assistido. Vamos contornar por ali para que eu possa liberar o seu acesso com segurança?"*.

5. Acionamento do Uso Progressivo da Força (Se necessário)

- **Ação:** Se a verbalização falhar e a pessoa evoluir para a agressão física iminente ou tentativa de invasão violenta, o vigilante deve progredir de forma proporcional para as técnicas de controle de contato, defesa pessoal não letal ou, em caso de risco de morte, uso do armamento.
- **Fundamento:** O uso da força física é o último recurso. O gerenciamento de conflitos busca exaurir a etapa da verbalização para resolver a crise de forma pacífica, segura e juridicamente adequada.

J. Atendimento a pessoas portadoras de necessidades especiais

Na segurança privada baseia-se nos princípios constitucionais da dignidade humana, da acessibilidade e da inclusão. O operador de segurança deve garantir a proteção e o cumprimento das normas do posto, mas sempre eliminando barreiras com respeito, empatia e sem assistencialismo excessivo ou discriminação

Atendimento a Pessoas de Baixa Mobilidade: Compreende indivíduos que, temporária ou permanentemente, possuem dificuldade de movimentação (como gestantes, pessoas com muletas, bengalas ou próteses).

- **Conduta Prática:** Identificar a aproximação e, proativamente, facilitar o acesso abrindo portões laterais ou portas automáticas, evitando que a pessoa precise fazer esforço excessivo.
- **Tática de Segurança:** Oferecer apoio ou assento se houver tempo de espera na triagem. Nunca tocar na pessoa ou em seus apoios (muletas/bengalas) sem antes pedir permissão.

Atendimento a Cadeirantes: A cadeira de rodas deve ser tratada como uma extensão do espaço corporal da própria pessoa.

- **Conduta Prática:** Ao falar com um cadeirante por mais de alguns instantes, flexione os joelhos ou sente-se para **ficar ao mesmo nível dos olhos dele**, evitando que ele precise tensionar o pescoço para cima.
- **Tática de Segurança:** Em postos com portas giratórias ou catracas, conduza o cadeirante imediatamente para o portão lateral de acessibilidade. Nunca empurre a cadeira de rodas sem o consentimento ou pedido expresso do usuário.

Atendimento a Idosos: O envelhecimento pode trazer limitações motoras, visuais ou auditivas, exigindo paciência redobrada no posto de serviço.

- **Conduta Prática:** Fale de forma clara, pausada e de frente para a pessoa, garantindo que as instruções de segurança sejam compreendidas sem pressa.
- **Tática de Segurança:** Garanta a prioridade legal no atendimento e nas filas. Ao orientar um idoso a retirar objetos metálicos em portas giratórias, faça-o de forma discreta e paciente, evitando expô-lo ao constrangimento perante terceiros.

Atendimento a Pessoas com Problemas na Fala: Inclui pessoas com gagueira, sequelas de AVC, paralisia cerebral ou outras condições que afetam a expressão verbal.

- **Conduta Prática:** Pratique a **escuta ativa total**. Nunca termine as frases pela pessoa, não demonstre impaciência e não tente adivinhar o que ela vai dizer.
- **Tática de Segurança:** Se a comunicação verbal falhar ou for muito difícil, ofereça alternativas neutras, como o uso de papel e caneta, ou peça para a pessoa apontar para as opções de identificação

Atendimento a Pessoas com Baixa Audição / Surdas: A comunicação dependerá de estímulos visuais e da clareza nos gestos técnicos.

- **Conduta Prática:** Antes de começar a falar, acene discretamente ou toque de leve no ombro da pessoa para chamar sua atenção. Fale de frente, articulando bem as palavras (sem gritar), permitindo a **leitura labial**.
- **Tática de Segurança:** Se o usuário não fizer leitura labial ou utilizar exclusivamente a Língua Brasileira de Sinais (LIBRAS), utilize gestos universais e profissionais, escrita ou o apoio de sinalizações visuais do próprio posto para indicar os procedimentos de acesso.

Atendimento a Pessoas com Autismo (TEA): O Transtorno do Espectro Autista afeta a comunicação, a interação social e pode gerar hipersensibilidade sensorial (a barulhos, luzes e toques).

- **Conduta Prática:** Utilize uma linguagem direta, literal e sem metáforas ou ironias. Se a pessoa demonstrar sinais de agitação, mantenha o tom de voz calmo, reduza os estímulos ao redor e dê espaço físico a ela.
- **Tática de Segurança:** Evite contato físico abrupto ou sem aviso prévio. Em postos como agências bancárias ou aeroportos, o som alto de alarmes de portas ou detectores pode

gerar crises de sobrecarga sensorial; se notar a fita ou cordão com desenho de **quebra-cabeça ou girassóis**, antecipe o atendimento facilitado para reduzir o tempo de estresse em locais barulhentos.

CONCLUSÃO

A análise aprofundada deste módulo de **Relações Humanas no Trabalho (RHT)** reafirma que o domínio das competências comportamentais e interpessoais é tão indispensável para o profissional de segurança privada quanto o seu preparo técnico ou o uso de armamentos. Sob a ótica do **Estatuto da Segurança Privada (Lei nº 14.967/2024)** e das normativas de campo da **Polícia Federal**, a conduta do operador no posto de serviço deixou de ser puramente reativa para se tornar eminentemente preventiva e inclusiva.

O estudo permitiu consolidar três pilares essenciais para a atuação profissional:

1. **A Comunicação como Instrumento de Força:** Compreender o processo de comunicação interpessoal — blindando o fluxo de mensagens contra ruídos, monitorando a linguagem não verbal e superando problemas da fala — capacita o vigilante a exercer sua autoridade com clareza. A verbalização assertiva atua como a ferramenta primária e mais eficaz do *Uso Progressivo da Força*, capaz de desescalar e gerenciar conflitos antes que haja necessidade de contato físico ou uso de armas.
2. **Ética, Disciplina e Cadeia de Comando:** O desenvolvimento de uma postura ética perante colaboradores e parceiros comerciais, aliado ao cumprimento rigoroso da disciplina operacional (com foco em horários, assiduidade e sigilo confidencial), confere sustentação jurídica e credibilidade ao trabalho executado. A subordinação técnica à unidade de comando e o asseio pessoal impecável funcionam como vetores de dissuasão visual, transmitindo prontidão e desencorajando ações criminosas por surpresa no posto de serviço.
3. **Cidadania e Inclusão na Linha de Frente:** Adotar as posturas desejadas de bom senso, imparcialidade e empenho profissional reflete diretamente na qualidade do atendimento prestado a idosos, cadeirantes, autistas e demais pessoas com deficiência ou mobilidade reduzida. Eliminar barreiras atitudinais e acolher a diversidade sem assistencialismo assegura a conformidade com os direitos humanos e mitiga riscos de processos por discriminação ou abuso de autoridade.

Em suma, as Relações Humanas no Trabalho transformam o profissional de segurança privada em um verdadeiro agente de preservação da ordem pública e privada. Unir a rigidez dos protocolos operacionais à humanização do atendimento ao público é a fórmula que garante a excelência técnica, a proteção de vidas e o pleno sucesso da governança corporativa no cenário contemporâneo.

SISTEMA NACIONAL DE SEGURANÇA PÚBLICA E CRIME ORGANIZADO (SSP)

Objetivos: Desenvolver conhecimentos sobre o Sistema Nacional de Segurança Pública, atribuições constitucionais de cada corporação policial e das Forças Armadas e atribuições da guarda municipal. Apresentar conceitos e modalidades de crime organizado.

Sistema Único de Segurança Pública (SUSP), frequentemente associado ao conceito de Sistema Nacional de Segurança Pública, é a estrutura criada pela Lei nº 13.675/2018 para integrar polícias, guardas municipais, sistemas prisionais e perícia. Ele visa unificar ações, padronizar dados e promover inteligência conjunta entre União, Estados e Municípios para prevenir e combater a criminalidade de forma eficiente. As informações a seguir possuem compilações do livro Segurança Privada no Brasil: Fundamentos Históricos & Formação Multiprofissional (Soares, 2026).

PRINCIPAIS OBJETIVOS DO SUSP

O sistema visa acabar com a fragmentação entre as instituições, permitindo que elas trabalhem de forma sistêmica:

- 1) **Integração e Cooperação:** Promove o compartilhamento de dados e operações conjuntas entre as diferentes forças de segurança.
- 2) **Padronização:** Cria uma arquitetura uniforme para registros de ocorrência e procedimentos em todo o país.
- 3) **Gestão de Dados:** Utiliza o Sinesp (Sistema Nacional de Informações de Segurança Pública) para unificar consultas operacionais e estratégicas.

ÓRGÃOS QUE COMPÕEM O SISTEMA

O SUSP abrange uma ampla rede de instituições, conforme definido no Portal da Câmara:

- 1) **Forças Policiais:** Polícias Federal, Rodoviária Federal, Civis e Militares.
- 2) **Corpos de Bombeiros Militares.**
- 3) **Guardas Municipais e Guardas Portuárias.**
- 4) **Agentes Penitenciários/Polícia penal (EC 104/2019) e institutos de perícia/medicina legal.**
- 5) **Força Nacional de Segurança Pública.**

Fundo Nacional de Segurança Pública (FNSP): Principal fonte de recursos para equipamentos, tecnologias e treinamento, repassando verbas para estados e municípios que cumprem metas e planos de segurança.

Plano Nacional: Define estratégias e metas a cada 10 anos, servindo de guia para que cada ente federativo crie seu próprio plano individual

O Artigo 144 da Constituição Federal brasileira estabelece que a segurança pública é dever do Estado, direito e responsabilidade de todos, exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio. Os órgãos de segurança pública previstos são: Polícia Federal, Rodoviária Federal, Ferroviária Federal, Civis, Militares, Bombeiros e Polícias Penais. Sendo:

- 1) **Polícia Federal (PF):** Apura infrações contra a ordem política, social ou bens da União.

- 2) **Polícia Rodoviária Federal (PRF):** Patrulhamento ostensivo das rodovias federais.
- 3) **Polícia Ferroviária Federal (PFF):** Patrulhamento ostensivo das ferrovias federais.
- 4) **Polícias Cíveis:** Polícia judiciária e apuração de infrações penais (exceto militares).
- 5) **Polícias Militares (PM):** Polícia ostensiva e preservação da ordem pública.
- 6) **Corpos de Bombeiros Militares:** Atividades de defesa civil, prevenção e combate a incêndios.
- 7) **Polícias Penais:** Segurança dos estabelecimentos penais (Federal, Estadual e Distrital).

Observação: O STF (Superior Tribunal Federal) reconhece que as Guardas Municipais devidamente instituídas integram o sistema de segurança pública, podendo realizar prisões em flagrante (art. 301 do CPP), mas não possuem as mesmas atribuições de polícia ostensiva das polícias militares.

PODER DE POLÍCIA:

Faculdade de que dispõe a Administração Pública para restringir o uso e gozo de bens, atividades e direitos individuais, em benefício da coletividade ou do próprio Estado. Trata-se do mecanismo de frenagem da Administração Pública para conter os abusos do direito individual.

No entanto, se os representantes da Administração Pública extrapolarem os limites da legalidade, deverão ser punidos pelo crime de abuso de autoridade, conforme a Lei 4898 /1965, observados o direito de ampla defesa e contraditório. Consiste em síntese, no Poder da Administração Pública em restringir a conduta do particular em favor da coletividade. Saliente-se que de acordo com o Direito Administrativo, todos os agentes públicos, dentro de sua competência e atribuições, tem poder de polícia.

Exemplo: fiscal de posturas do município de Belo Horizonte ao fiscalizar um estabelecimento comercial e constatar a falta de alvará de funcionamento, após o prazo de adequação e constatar novamente a irregularidade, terá o poder de polícia de embargar o estabelecimento até que sejam retirados tais alvarás.

RECORDANDO:

Flagrante compulsório: O Código de Processo Penal rege em seu Art. 302 que se considera em flagrante delito quem:

- I - Está cometendo a infração penal;
- II - Acaba de cometê-la;
- III - É perseguido, logo após, pela autoridade, pelo ofendido ou por qualquer pessoa, em situação que faça presumir ser autor da infração;
- IV - É encontrado, logo depois, com instrumentos, armas, objetos ou papéis que façam presumir ser ele autor da infração.

Flagrante facultativo: De acordo com o Código de Processo Penal, em seu Art. 301 que qualquer do povo poderá e as autoridades policiais e seus agentes deverão prender quem quer que seja encontrado em flagrante delito.

Uso de algemas: É lícito o uso de algemas em casos de resistência e de fundado receio de fuga ou de perigo à integridade física própria ou alheia, por parte do preso ou de terceiros, justificada a excepcionalidade por escrito, sob pena de responsabilidade disciplinar, civil e penal do agente ou da autoridade e de nulidade da prisão ou do ato processual a que se refere, sem prejuízo da responsabilidade civil do Estado.

O uso de algemas por vigilantes é um tema controverso, mas geralmente permitido em situações excepcionais de **flagrante delito** (Art. 301 CPP), seguindo os critérios da Súmula Vinculante 11 do STF: resistência, receio de fuga ou perigo à integridade física. A contenção deve ser proporcional, temporária e justificada, visando apenas a segurança até a chegada da polícia. É de amplo conhecimento que a Segurança Privada é complementar e subsidiária da Segurança

Pública, sendo assim a necessidade do Estado (Administração Pública) ser o fundamento de existência da segurança privada, tendo competência de fiscalização e controle de tal atividade através da Polícia Federal.

- 1) **Fundamentação Legal:** Baseia-se no direito de qualquer pessoa realizar prisão em flagrante (Art. 301 do CPP), sendo o uso de algemas uma ferramenta de apoio para manter a segurança do local e dos envolvidos.
- 2) **Casos Permitidos (Súmula Vinculante 11):**
 - a) Resistência: ativa à prisão.
 - b) Fundado receio de **fuga**.
 - c) Perigo à integridade física do próprio detido, do vigilante ou de terceiros.
- 3) **Limitações:** O uso indevido, sem necessidade, pode configurar abuso, gerando responsabilização civil, penal e administrativa para o vigilante e a empresa. Não é um item de uso rotineiro, mas sim de exceção.
- 4) **Divergência:** Embora a interpretação da Súmula 11 permita, alguns entendimentos focam na ausência de poder de polícia, limitando severamente o uso de algemas por segurança privada

A ação deve sempre ser pautada pela necessidade imediata de segurança e, preferencialmente, acionar as forças de segurança pública (Polícia Militar/Civil) imediatamente.

APROFUNDANDO OS CONCEITOS:

POLÍCIA ADMINISTRATIVA OU PREVENTIVA: Tem por objetivo prevenir as infrações penais, evitar perigos, proteger a coletividade, assegurar o direito de seus componentes, manter a ordem e o bem estar públicos. Sua ação é exercida antes do cometimento da infração penal. Sua atuação é eminentemente preventiva, embora exerçam a parte repressiva também, após o cometimento dos delitos ou desastres. Formada pelas Polícias Militares, Corpos de Bombeiros Militares, Polícia Rodoviária Federal e Polícia Ferroviária Federal.

POLÍCIA JUDICIÁRIA: Destinada a investigar as infrações penais que não puderam ser prevenidas, de cobrir-lhe os autores e reunir provas da materialidade do delito. Sua atividade é predominantemente repressiva, e tem por objetivo encaminhar ao Poder Judiciário, provas contra os autores. É formada pela Polícia Federal e Polícias Civis.

ATRIBUIÇÕES DOS ÓRGÃOS DE SEGURANÇA PÚBLICA:

POLÍCIA MILITAR: A Polícia Militar (PM) é uma força pública estadual no Brasil, uniformizada e ostensiva, responsável pela preservação da ordem pública e segurança interna. Atua na prevenção de crimes através de rondas (patrulhamento), abordagens e atendimento de emergências, visando proteger cidadãos e bens. Está subordinada aos governos estaduais, sendo considerada força auxiliar do Exército.

PRINCIPAIS ATUAÇÕES E CARACTERÍSTICAS:

- 1) **Policamento Ostensivo:** Identificável pelo uso de uniforme e viaturas, sua presença busca inibir ilícitos penais
- 2) **Preventiva:** Atua antes que o crime ocorra, patrulhando ruas e comunidades.
- 3) **Primeira Resposta:** Geralmente é a primeira força a chegar em ocorrências de acidentes, conflitos e emergências.
- 4) **Estrutura Hierarquizada:** Baseada em hierarquia e disciplina.

- 5) **Especializações:** Além do patrulhamento geral, inclui unidades como polícia ambiental, rodoviária, de trânsito e Choque/BOPE.

Art. 142 CRFB/88: da Constituição Estadual; A Polícia Militar e o Corpo de Bombeiros Militar, forças públicas estaduais, são órgãos permanentes, organizados com base na hierarquia e disciplina militares e comandados, preferencialmente, por Oficial da ativa do último posto, competindo: I - à Polícia Militar, a polícia ostensiva de prevenção criminal, de segurança e de trânsito urbano e rodoviário, de florestas e de mananciais e a atividades relacionadas com a preservação e restauração da ordem pública, além do exercício do poder de polícia dos órgãos e entidades públicos, especialmente da área fazendária, sanitária, de proteção ambiental, de uso e ocupação do solo e patrimônio cultural; § 1º - A Polícia Militar e o Corpo de Bombeiros Militar são forças auxiliares e reserva do Exército

Art. 144 CRFB/1988 - § 5º: às Polícias Militares cabem a polícia ostensiva e a preservação da Ordem Pública; aos Corpos de Bombeiros Militares, além das atribuições definidas em lei, incumbe a execução das atividades de defesa civil (BRASIL, 1988).

COMO ACIONAR OS ÓRGÃOS DE SEGURANÇA PÚBLICA

Acione a Polícia Militar (PM) ligando 190 para emergências imediatas (crimes em andamento, risco à vida ou propriedade). Para denúncias anônimas sobre crimes já ocorridos ou suspeitos, utilize o 181. O atendimento 190 é gratuito e funciona 24h, idealmente com endereço exato e características dos envolvidos.

MODALIDADES DE POLICIAMENTO

AÉREO:

- 1) Salvamentos e resgate;
- 2) Acompanhamento tático e policiamento ostensivo em geral;
- 3) Patrulhamento ambiental;
- 4) Transporte de emergência;

AMBIENTAL, PREVENÇÃO E REPRESSÃO A CRIMES AMBIENTAIS:

- 1) Combate ao tráfico de drogas (cães farejadores) –
- 2) Controle de distúrbios civis –
- 3) Resgate de pessoas perdidas, soterradas, etc;

DE CHOQUE: Restabelecimento da ordem social;

DE GUARDA: Segurança a presídios, consulados, prédios públicos, etc;

ESCOLAR: Segurança às escolas e universidades;

ESCOLTA: Proteção especial a pessoas ou bens;

FLUVIAL: lacustre e marítimo - patrulhamento com embarcações.

MOTORIZADO: Patrulhamento com veículos automóveis e motocicletas;

OSTENSIVO A PÉ: Patrulhamento básico, em geral com o uso de radiotransmissores;

RODOVIÁRIO: Controle do trânsito em estradas rodoviárias;

TURÍSTICO: Segurança e apoio a turistas;

MONTADO: Destinado principalmente a patrulhamento de parques, áreas rurais, regiões de acesso restrito, etc;

DE TRÂNSITO: POLICIAMENTO E CONTROLE DO TRÂNSITO URBANO E EM VIAS SOB COMPETÊNCIA ESTADUAL;

VELADO: Sem uniforme e descaracterizado, para a preservação da ordem pública.

POLÍCIA CIVIL: É um órgão estadual de segurança pública, de natureza investigativa e administrativa (polícia judiciária), responsável por apurar infrações penais (exceto militares) e auxiliar a justiça. Ela atua após a ocorrência de crimes, realizando inquéritos, colhendo provas e identificando autores para combater o crime organizado e a criminalidade geral.

PRINCIPAIS CARACTERÍSTICAS E FUNÇÕES:

- 1) **Polícia Judiciária:** Auxilia o Poder Judiciário na elucidação de crimes através de investigações.
- 2) **Investigação Criminal:** Responsável por inquéritos, coleta de provas, escutas e depoimentos para descobrir autoria e materialidade de delitos.
- 3) **Atuação Especializada:**
- 4) Possui delegacias especializadas (homicídios, narcóticos, crimes cibernéticos, violência doméstica, etc.).
- 5) **Diferença da Polícia Militar (PM):** A Polícia Civil é investigativa e age *após* o crime (repressiva), não utiliza uniforme no dia a dia. A PM é ostensiva, uniformizada e atua na prevenção, patrulhando as ruas.
- 6) **Estrutura Estadual:** Cada estado brasileiro tem a sua própria Polícia Civil, subordinada ao governador.

Art. 142 § 4º: Às polícias civis, dirigidas por delegados de polícia de carreira, incumbem, ressalvada a competência da União, as funções de polícia judiciária e a apuração de infrações penais, exceto as militares (BRASIL, 1988).

São atividades privativas da Polícia Civil:

- 1) Polícia Técnico-científica;
- 2) Processamento e arquivo de identificação civil e criminal;
- 3) Registro e licenciamento de veículo automotor;
- 4) Habilitação de condutores;
- 5) Proteção à vida e aos bens;
- 6) Apuração das infrações penais, exercício da polícia judiciária e cooperação com as autoridades judiciárias, civis e militares, em assuntos de Segurança Interna.

POLÍCIA RODOVIÁRIA FEDERAL: É uma instituição policial brasileira voltada ao patrulhamento ostensivo das rodovias e estradas federais (as chamadas BRs). Subordinada ao Ministério da Justiça e Segurança Pública, sua missão principal é **preservar a ordem pública e proteger vidas** em mais de 75 mil quilômetros de malha federal.

CRFB/88, Art. 144 - § 2º: Órgão permanente, organizado e mantido pela União e estruturado em carreira, destina-se, na forma da lei, ao patrulhamento ostensivo das rodovias federais (BRASIL, 1988).

São atividades privativas da Polícia Rodoviária Federal:

- 1) Exercer os poderes de polícia de trânsito nas rodovias federais, fiscalização de produtos perigosos (substâncias tóxicas, explosivos, corrosivos) etc.
- 2) Executa o patrulhamento ostensivo, executando operações com o objetivo de preservar a ordem nas rodovias federais;
- 3) Inspecciona e fiscaliza o trânsito em todas as rodovias Federais do País, cumprindo e fazendo cumprir o Código de Trânsito Brasileiro;
- 4) Aplica e arrecada as multas impostas por infrações de trânsito e os valores decorrentes da prestação de serviço de estadia e remoção de veículos, atendimento a acidentes e salvamento de vítimas nas rodovias federais em apoio a órgãos de resgate;
- 5) Planejamento e escoltas nos deslocamentos do Presidente da República, Ministros de Estado, diplomatas estrangeiros e outras autoridades
- 6) Responsável pela regulamentação do credenciamento e fiscalização das empresas que realizam os serviços especializados de escolta.

POLÍCIA FERROVIÁRIA FEDERAL: É um órgão constitucional (Art. 144) destinado ao patrulhamento ferroviário, mas atualmente não existe de fato, sem quadro de funcionários ativo. Criada em

1852, teve atuação relevante, mas foi descontinuada com a privatização das ferrovias em 1996, a categoria busca reconhecimento e incorporação, com propostas para torná-la parte de uma "Polícia Viária Federal".

CRFB/88, Art. 144, §3º: A polícia ferroviária federal, órgão permanente, organizado e mantido pela União e estruturado em carreira, destina-se, na forma da lei, ao patrulhamento ostensivo das ferrovias federais (BRASIL, 1988).

Órgão permanente, como as demais polícias federais, organizado e mantido pela União e estruturado em carreira. Destinado ao patrulhamento ostensivo das ferrovias federais. Também é considerado como “a menor polícia do mundo”. Com a privatização das ferrovias e o desenvolvimento do policiamento nelas realizado pelos batalhões ferroviários das polícias militares, as atividades da corporação federal permanecem estagnadas.

Prevista no art. 144 da Constituição Federal, sua função é o patrulhamento ostensivo das ferrovias federais. Não há policiais ferroviários federais na ativa. A segurança ferroviária é feita por guardas de empresas privadas ou, em alguns casos, por guardas de transição da CBTU.

POLÍCIA FEDERAL: É uma instituição de estado brasileira, subordinada ao Ministério da Justiça e Segurança Pública, responsável por investigar crimes contra a ordem política e social ou em detrimento de bens, serviços e interesses da União.

Art. 144 CRFB/88 § 1º A polícia federal, instituída por lei como órgão permanente, organizado e mantido pela União estruturado em carreira, destina-se a: I - apurar infrações penais contra a ordem política e social ou em detrimento de bens, serviços e interesses da União ou de suas entidades autárquicas e empresas públicas, assim como outras infrações cuja prática tenha repercussão interestadual ou internacional e exija repressão uniforme, segundo se dispuser em lei; II - prevenir e reprimir o tráfico ilícito de entorpecentes e drogas afins, o contrabando e o descaminho, sem prejuízo da ação fazendária e de outros órgãos públicos nas respectivas áreas de competência; III - exercer as funções de polícia marítima, aeroportuária e de fronteiras; IV - exercer, com exclusividade, as funções de polícia judiciária da União. IV - Exercer, com exclusividade, as funções de polícia judiciária da União (BRASIL, 1988).

Subordinada ao Ministério da Justiça, é responsável por investigações dos crimes julgados pela Justiça Federal, como por exemplo, os crimes cometidos contra os bens, serviços e interesses da União, assim como os crimes cometidos a bordo de aeronaves e navios, além também de exercer a função de Polícia Judiciária. Exerce ainda funções de polícia marítima, aeroportuária, responsável pela fiscalização de fronteiras, alfândegas e emissão de passaporte.

Com base na Lei nº 14.967/2024, que institui o Estatuto da Segurança Privada, a Polícia Federal (PF) é o órgão central de controle, fiscalização e autorização de todas as atividades de segurança privada e transporte de valores no Brasil. A PF atua na regulação de empresas e profissionais, na repressão à segurança clandestina e na aplicação de penalidades administrativas.

As principais atribuições da Polícia Federal, conforme a nova legislação, incluem:

- 1) **Autorização e Registro:** Autorizar o funcionamento de empresas de segurança privada, escolas de formação e cadastrar os profissionais da área, conforme o artigo 40 da lei.
- 2) **Fiscalização e Controle:** Exercer a fiscalização permanente sobre as atividades, incluindo o uso de armas e o transporte de valores.
- 3) **Repressão à Clandestinidade:** Reprimir empresas e serviços de segurança irregulares ou ilegais.
- 4) **Processo Administrativo:** Aplicar penalidades como advertência, multa e cancelamento de autorização em caso de infrações.
- 5) **Atualização do Sistema:** Gerenciar o sistema informatizado de cadastramento para organizar, de forma digital e centralizada, as informações sobre empresas e vigilantes.

A nova lei fortalece o papel da PF como polícia administrativa do setor, substituindo a legislação anterior e focando na segurança das instituições financeiras e na profissionalização da segurança armada e desarmada.

OUTRAS ATRIBUIÇÕES:

- 1) Combate ao trabalho escravo;
- 2) Apuração de Crimes eleitorais;
- 3) Combate a crimes ambientais;
- 4) Conflitos fundiários;
- 5) Fiscalização e controle da Segurança Privada;
- 6) Representante da Interpol no país e responsável pela segurança dos Chefes de Estado em visita ao Brasil.

LEMBRETE: Embora adiante seja comentado sobre contrabando e descaminho, vale descrever as principais distinções entre os tipos penais. São duas modalidades de crimes parecidas, mas não idênticas, embora comumente se chame tudo de contrabando, este consiste na introdução no território nacional ou na retirada dele de mercadorias proibidas; se proíbe a importação ou exportação de determinada mercadoria no interesse da política econômica, mas alguém assim mesmo, atravessa as fronteiras nacionais com tal mercadoria, aí está cometendo o crime de contrabando; se essa pessoa, no entanto, introduz ou retira mercadorias, cuja importação ou exportação é permitida mediante pagamento de tributos, mas, no caso, enganou o fisco e não pagou o imposto pertinente, então cometeu o crime de descaminho.

Guarda Municipal (GM) ou Guarda Civil Municipal (GCM): É uma instituição de caráter civil, armada (conforme lei) e uniformizada, subordinada ao prefeito, com a função de proteção municipal preventiva. Ela atua na segurança urbana, protegendo bens, serviços e instalações municipais, além de realizar policiamento comunitário e atuar na fiscalização do trânsito.

Art. 144 CRFB/88 § 8º- Os Municípios poderão constituir guardas municipais destinadas à proteção de seus bens, serviços e instalações, conforme dispuser a lei. Sob a autoridade suprema do prefeito da cidade. Destinadas à proteção dos bens, serviços, interesses, instalações e patrimônios públicos do município (BRASIL, 1988).

Segundo o artigo da Constituição Federal, a Guarda Municipal tem como missão a proteção do patrimônio, bens, serviços e instalações públicas municipais. É uma corporação de caráter civil que trabalha uniformizada e aparelhada com treinamento específico estabelecida em Lei. Seus integrantes são considerados agentes de segurança dentro do âmbito municipal, cabendo-lhes exercer o policiamento municipal para todos os efeitos legais. Cabe ao poder executivo de cada município decidir atuação de sua Guarda Civil, variando sua forma de atuação em cada município que a contem. Cerca de 20% das cidades brasileiras têm Guardas Municipais.

A GM pode exercer as competências de trânsito nas vias e logradouros municipais, de acordo com o Código de Trânsito Brasileiro.

O Artigo 16 da Lei nº 13.022/2014 (Estatuto Geral das Guardas Municipais) trata especificamente da autorização e das restrições ao **porte de arma de fogo** para os guardas municipais.

Poder de Polícia dentro das suas esferas de atribuições, no que tange à proteção dos bens, serviços, interesses, instalações do patrimônio público municipal. É tão clara a intenção do constituinte de admitir uma atividade de polícia pelas guardas municipais, que houve por bem inseri-las no

O Art. 144 CRFB/88 - § 8º: Os Municípios poderão constituir guardas municipais destinadas à proteção de seus bens, serviços e instalações, conforme dispuser a lei. Assim, a atuação das guardas se resume a uma atividade comunitária de segurança urbana, e apoiando os órgãos policiais estaduais e federais quando solicitadas.

CORPOS DE BOMBEIRO MILITAR (CBM): É uma instituição pública, geralmente militarizada (Força Auxiliar e Reserva do Exército), focada em defesa civil, prevenção e combate

a incêndios, além de busca e salvamento de pessoas e bens. Atua no resgate em acidentes, emergências pré-hospitalares e situações de risco. Integra a Polícia Militar, atua no serviço público, acionado pelo telefone 193.

Artigo 144 § 5º aos corpos de bombeiros militares, além das atribuições definidas em lei, incumbe a execução de atividades de defesa civil (BRASIL, 1988).

OUTRAS ATRIBUIÇÕES:

- 1) Intervenção em incidentes com produtos perigosos; tais como: gases, inflamáveis, substâncias tóxicas, etc.
- 2) Vistorias técnicas de segurança em edificações, estádios, ou qualquer outro local de grande concentração de público.
- 3) Serviço de Atendimento Pré-Hospitalar.
- 4) Coordenar e executar as ações de defesa civil, proteção e socorro públicos, prevenção e combate a incêndio, perícias de incêndio e explosão em locais de sinistro, busca e salvamento.
- 5) Combate a Incêndios: Urbanos (residências/comércios) e florestais.
- 6) Busca e Salvamento: Resgates em altura, espaços confinados, água e veículos.
- 7) Atendimento Pré-Hospitalar (APH): Primeiros socorros em acidentes.
- 8) Prevenção: Vistorias de segurança e educação pública.

FORÇA NACIONAL DE SEGURANÇA PÚBLICA (FNSP): Criada em 2004, é um programa de cooperação federativa do Ministério da Justiça e Segurança Pública. Composta por policiais militares, civis, bombeiros e peritos estaduais, atua temporariamente em estados com crises de segurança, calamidades ou grandes eventos, mediante solicitação dos governadores.

Composto por profissionais qualificados das forças estaduais cedidos à União. Apoio em operações de inteligência, policiamento ostensivo, Polícia Judiciária e perícia forense; atua no combate a crimes ambientais, conflitos agrários, proteção de terras indígenas e unidades prisionais; apoiar estados que não conseguem controlar situações de emergência sozinhos, não sendo uma força de intervenção autônoma e seus agentes permanecem ligados aos seus estados de origem, mas recebem diárias federais durante a missão.

Força reserva estratégica do Poder executivo formada em sua maioria por POLICIAIS MILITARES das Unidades da Federação. São Policiais emprestados voluntariamente ao governo federal por suas respectivas corporações. A FNS é um programa de cooperação de Segurança Pública brasileira, empregada nas situações de crise na segurança pública dos Estados e evita o envio das Forças Armadas. Composta por:

- 1) Policiais Militares
- 2) Bombeiros militares dos Estados
- 3) Policiais rodoviários
- 4) Policiais federais

Foi inspirada nas forças de paz da Organização das Nações Unidas (ONU) e disciplinada na Lei 11.473/2007. Foi criada para evitar o envio das Forças Armadas nas situações de crise nos Estados.

A FNS 80 é empregada em situações emergenciais, a partir do pedido oficial do Governador e sob determinação do Ministro da Justiça, bem como Operações de Força Tarefa de alto risco, eventos internacionais como Copa do Mundo, Olimpíadas, etc.

Sua atuação é autorizada, a partir do pedido oficial do governador do Estado e sob determinação do Ministro da Justiça.

Entretanto, a Força Nacional de Segurança Pública só pode atuar em um determinado município do Brasil se for solicitada pelo governador do respectivo estado ou do Distrito Federal, e se esse pedido for autorizado pelo Ministro da Justiça e Segurança Pública (MJSP).

Dessa forma, a Força Nacional poderá apoiar a Polícia Militar, a Polícia Civil, o Corpo de Bombeiros ou os órgãos oficiais de Perícia Forense.

Também mediante autorização do MJSP, a Força Nacional de Segurança Pública poderá apoiar operações específicas de outros órgãos federais - a exemplo da Polícia Federal, da Polícia Rodoviária Federal ou do Instituto Brasileiro do Meio Ambiente e dos Recursos Naturais Renováveis, ou mesmo outros ministérios do governo federal.

O Departamento da Força Nacional de Segurança Pública está subordinado à Secretaria Nacional de Segurança Pública do Ministério da Justiça (SENASP/MJSP).

FORÇAS ARMADAS: são instituições nacionais permanentes e regulares, compostas pela **Marinha, Exército e Aeronáutica**. Sob a autoridade do Presidente da República e vinculadas ao Ministério da Defesa, destinam-se a defender a Pátria, garantir os poderes constitucionais e, por iniciativa destes, a lei e a ordem.

- 1) **Marinha do Brasil:** Responsável pela defesa das águas (mares e rios), protegendo a costa e o mar territorial.
- 2) **Exército Brasileiro:** Focado em operações terrestres, atuando na proteção e controle do solo nacional.
- 3) **Força Aérea Brasileira (Aeronáutica):** Encarregada da vigilância e defesa do espaço aéreo brasileira.

Art. 142 CRFB/88: As Forças Armadas, constituídas pela Marinha, pelo Exército e pela Aeronáutica, são instituições nacionais permanentes e regulares, organizadas com base na hierarquia e na disciplina, sob a autoridade suprema do Presidente da República, e destinam-se à defesa da Pátria, à garantia dos poderes constitucionais e, por iniciativa de qualquer destes, da lei e da ordem (BRASIL, 1988).

As Forças Armadas exercem um papel fundamental na continuidade da estabilidade das instituições, no equilíbrio do pacto federativo, bem como, subsidiariamente, em atividades de segurança pública e humanitária. Nas relações internacionais do Estado brasileiro, contribuem para a busca incessante da paz, como instrumentos de afirmação dos ideais pacifistas do presente momento.

Sempre, desde a Constituição de 1824, os textos constitucionais autorizam o emprego das Forças Armadas na garantia da lei e da ordem interna do país, com características de excepcionalidade como regra. Isto posto, a arquitetura constitucional de segurança aponta para o emprego e atuação das Forças Armadas em quatro destinações, que são:

- a) na defesa da pátria;
- b) na garantia dos poderes constitucionais;
- c) na garantia da lei e da ordem;
- d) em operações humanitárias e de cooperação internacional.

O Ministro de Estado da Defesa exerce a direção superior das Forças Armadas. Ele é responsável pela direção superior das Forças Armadas (Marinha, Exército e Aeronáutica), focando na soberania nacional, fortalecimento da base industrial de defesa e promoção de produtos como o cargueiro KC-390.

EMPREGO DAS FORÇAS ARMADAS

Na defesa da Pátria e na garantia dos poderes constitucionais, da lei e da ordem, e na participação em operações de paz, é de responsabilidade do Presidente da República, que determinará ao Ministro de Estado da Defesa a Ativação de órgãos operacionais.

A atuação das Forças Armadas, na garantia da lei e da ordem, por iniciativa de quaisquer dos poderes constitucionais, ocorrerá de acordo com as diretrizes baixadas em ato do Presidente da República, depois de esgotados os instrumentos destinados à preservação da ordem pública e da incolumidade das pessoas e do patrimônio. Consideram-se esgotados os instrumentos relacionados no art. 144 da Constituição Federal, quando, em determinado momento, forem eles formalmente reconhecidos pelo respectivo Chefe do Poder Executivo Federal ou Estadual como indisponíveis inexistentes ou insuficientes ao desempenho regular de sua missão constitucional. Nessas condições, após mensagem do Presidente da República, serão ativados os órgãos operacionais das Forças Armadas, que desenvolverão, de forma episódica, em área previamente estabelecida e por tempo limitado, as ações de caráter preventivo e repressivo necessárias para assegurar o resultado das operações na garantia da lei e da ordem.

Em resumo, as Forças Armadas têm por missão essencial a defesa da Pátria e a garantia dos poderes constitucionais, o que vale dizer defesa, por um lado, contra egressões estrangeiras em caso de guerra externa e, por outro lado, defesa das instituições democráticas, pois a isso corresponde a garantia dos poderes constitucionais, que, nos termos da Constituição, emanam do povo. Só subsidiária e eventualmente lhes incumbe à defesa da lei e da ordem, porque essa defesa é de competência primária das forças de segurança pública, que compreendem a polícia federal e os polícias civis e militares dos Estados e do Distrito Federal. Sua interferência na defesa da lei e da ordem depende, além do mais, de convocação dos legítimos representantes de qualquer dos poderes federais: Presidente da Mesa do Congresso Nacional, Presidente da República ou Presidente do Supremo Tribunal Federal.

ATRIBUIÇÕES DE CADA ÓRGÃO DAS FORÇAS ARMADAS:

MARINHA DO BRASIL (MB): É a força armada responsável pela defesa e proteção das águas brasileiras, território estrategicamente chamado de Amazônia Azul, que abrange cerca de 5,7 milhões de km².

É o ramo das Forças Armadas responsável pela defesa da soberania nacional no mar, rios e lagos, além de proteger a "Amazônia Azul" (área marítima rica em recursos). Suas principais funções incluem patrulhar fronteiras, fiscalizar o tráfego aquaviário, realizar resgates (SAR), garantir a lei e a ordem, e prover segurança à navegação.

Principais Atividades e Responsabilidades:

- 1) **Defesa Nacional:** Protege o litoral de 7,4 mil km, a infraestrutura marítima (como plataformas de pré-sal) e as águas jurisdicionais.
- 2) **Segurança Aquaviária:** Atua através da Capitania dos Portos na fiscalização de embarcações, emissão de habilitações para amadores (carteira de arrais, motonauta, etc.) e na segurança de banhistas.
- 3) **Autoridade Marítima:** Responsável pela segurança do tráfego aquaviário, combate à poluição hídrica e monitoramento de rios, lagos e mar.
- 4) **Apoio à População:** Realiza missões de assistência hospitalar em áreas remotas (como a Amazônia), buscas e salvamentos (SAR), e ajuda humanitária.
- 5) **Desenvolvimento Tecnológico:** Envolvida na construção de submarinos e fragatas para aumentar a capacidade operacional.

EXÉRCITO BRASILEIRO: É o componente terrestre das Forças Armadas de uma nação, sendo responsável por operações militares em solo. Diferente da Marinha (mar) e da Força Aérea (ar), o exército foca na defesa do território, das fronteiras e na manutenção da soberania nacional por terra.

Funções do Exército Brasileiro

No Brasil, o Exército Brasileiro (EB) é uma instituição permanente organizada sob hierarquia e disciplina. Suas principais funções incluem:

- 1) **Defesa Externa:** Proteção do território e das fronteiras contra ameaças estrangeiras;

- 2) **Garantia da Lei e da Ordem (GLO):** Atuação interna para assegurar a ordem pública e o respeito à Constituição quando solicitado pelos poderes constituídos;
- 3) **Ações Subsidiárias:** Apoio ao desenvolvimento nacional e à Defesa Civil em casos de desastres naturais, além de obras de infraestrutura realizadas pelo seu corpo de engenharia;
- 4) **Missões de Paz:** Participação em operações internacionais de ajuda humanitária e manutenção da paz sob a égide de organismos como a ONU.

O exército é comandado pelo Comandante do Exército e está subordinado ao Ministério da Defesa.

FORÇA AÉREA BRASILEIRA (FAB): É o ramo aeronáutico das Forças Armadas do Brasil, responsável pela manutenção da soberania do espaço aéreo e pela integração do território nacional. Fundada em **20 de janeiro de 1941**, ela atua na defesa das fronteiras, missões de busca e salvamento, transporte logístico e ajuda humanitária.

Além da defesa militar, a FAB desempenha papéis civis essenciais:

- 1) **Controle do Espaço Aéreo:** Gerenciado pelo DECEA, garante a segurança de voos civis e militares em 22 milhões de km²;
- 2) **Integração Nacional:** Através do Correio Aéreo Nacional (CAN), transporta órgãos para transplante, urnas eleitorais e suprimentos para comunidades isoladas, como na Amazônia;
- 3) **Busca e Salvamento (SAR):** O sistema SISSAR é responsável por resgates em terra e mar, tendo salvado 56 vidas apenas em 2025.

Principais Funções e Missões da FAB:

- 1) **Defesa Aeroespacial:** A principal função é controlar e defender o espaço aéreo brasileiro contra ameaças externas.
- 2) **Patrulha e Segurança:** Combate ao tráfico de drogas e armas, além de vigilância nas fronteiras.
- 3) **Busca e Salvamento (SAR):** O Esquadrão PARA-SAR é especializado em busca e resgate em situações de emergência.
- 4) **Logística e Transporte:** A FAB promove a integração nacional com o Correio Aéreo Nacional (CAN), transportando pessoas e cargas em áreas remotas.
- 5) **Controle de Tráfego Aéreo:** A FAB é responsável por orientar, coordenar e controlar as atividades de aviação civil e militar.
- 6) **Ações Humanitárias:** Apoio em regiões afetadas por desastres naturais.
- 7) **Treinamento e Preparo:** Realização de exercícios para manter a prontidão operacional das tropas.

A FAB, como ramo aeronáutico das Forças Armadas, foi criada em 1941. Informações sobre a estrutura de postos e graduações e a doutrina básica da FAB podem ser encontradas em seus canais oficiais.

AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL (ANAC): É a autarquia especial responsável por regular e fiscalizar as atividades da aviação civil no Brasil. Criada em 2005 e operante desde 2006, ela substituiu o antigo DAC (Departamento de Aviação Civil).

A sede oficial fica em **Brasília (DF)**, mas a agência possui representações regionais no **Rio de Janeiro, São Paulo e São José dos Campos**. Informações detalhadas sobre serviços, legislação e consultas ao Registro Aeronáutico Brasileiro (RAB) podem ser acessadas no portal oficial.

Funções e Atribuições Principais:

- 1) **Regulação e Fiscalização:** Normatiza e supervisiona a segurança técnica (*safety*), a segurança contra atos ilícitos (*security*) e os aspectos econômicos do setor, como concessões aeroportuárias e o mercado de transporte aéreo.
- 2) **Certificação:** Responsável por emitir licenças e certificados para aeronaves, pilotos e outros profissionais da aviação.

- 3) **Direitos do Passageiro:** Monitora a qualidade do serviço prestado pelas companhias aéreas e protege os direitos dos viajantes.

CRIME ORGANIZADO NO BRASIL

O crime organizado no Brasil é caracterizado pela atuação de grandes facções criminosas, como o PCC e o Comando Vermelho, que dominam territórios, gerenciam o tráfico de drogas/armas e lavam dinheiro em negócios legais. A estimativa é que cerca de 31 milhões de pessoas vivam em áreas sob influência dessas facções, evidenciando uma "governança criminal" que afeta a segurança e a política.

O Surgimento do crime organizado no Brasil ocorreu no final dos anos 60, os ativistas políticos começaram a assaltar bancos para financiar a guerrilha urbana contra a ditadura militar. Caetano Veloso e Gilberto Gil, exilados na Inglaterra, Chico Buarque, exilado na França.

Na década de 1980, a ditadura brasileira entrou em decadência quando o governo não conseguiu mais controlar e equilibrar os vários setores do seu poder. O governo decidiu enquadrar todos os ladrões de bancos na Lei de Segurança 85 Nacional; qualquer pessoa que pratique delitos como assalto, sequestro ou roubo, será punida, independentemente de seu crime ter ou não intenções políticas. Todos os assaltantes de bancos, integrantes de organizações políticas clandestinas e os chamados bandidos comuns foram para o mesmo presídio, o Instituto Penal Cândido Mendes, na Ilha Grande, do Estado do Rio de Janeiro.

Graças à aproximação de presos políticos com prisioneiros comuns, que nasceu uma das primeiras e maiores organizações criminosas do país: O Comando Vermelho.

COMANDO VERMELHO - ANOS 70: Na década de 70, dentro do Presídio Cândido Mendes, o Comando Vermelho, proliferou-se para outras penitenciárias e aglomerados do Rio de Janeiro. Primeiro conceito de crime organizado que se teve no Brasil foi a criação do comando vermelho nos complexos prisionais de Bangu I e II, no Estado do Rio de Janeiro, no ano de 1970, no qual pregavam a liberdade, paz e justiça no cárcere.

Entretanto, com passar dos anos, o slogan COMANDO VERMELHO alcançou os morros do Rio de Janeiro, o qual passou a financiar o tráfico de drogas e outros crimes. A partir daí o Estado brasileiro passou a reconhecer o Comando Vermelho como sendo uma facção criminosa, daí surgindo outras facções criminosas, como Comando vermelho jovem, Amigo dos Amigos, Terceiro Comando da Capital, todas predominantes do Estado do Rio de Janeiro e no Estado de São Paulo temos a predominância do PCC (PRIMEIRO COMANDO DA CAPITAL) que teve origens no massacre do Carandiru.

O Comando Vermelho (CV) surgiu no final da década de 1970 no Instituto Penal Cândido Mendes, em Ilha Grande (RJ), fruto da convivência entre presos políticos de esquerda e criminosos comuns. Presos políticos, sob a Lei de Segurança Nacional, ensinaram organização e estratégias de sobrevivência a presos comuns, influenciando a criação da facção.

Origem e Dinâmica:

- 1) **Berço:** A facção, inicialmente chamada de "Falange da Segurança Nacional" e depois "Falange Vermelha", uniu presos da "Galeria B" da prisão de Ilha Grande.
- 2) **Influência:** Presos políticos, com maior escolaridade, organizaram os comuns, criando caixa comunitária e normas para a galeria.
- 3) **Legado:** Após a anistia e saída dos presos políticos, os criminosos comuns mantiveram a estrutura organizada, consolidando o CV.

Líderes Notáveis da Facção (Histórico):

- 1) Luiz Fernando da Costa (Fernandinho Beira-Mar)
- 2) Elias Pereira da Silva (Elias Maluco)
- 3) Márcio Nepomuceno dos Santos (Marcinho VP)

- 4) William da Silva Lima (O Professor) (Apontado como um dos fundadores)

Transferência de Lideranças Recentes (2025): Sete líderes de alto escalão do CV foram transferidos para prisões federais, incluindo:

- 1) Arnaldo da Silva Dias (Naldinho)
- 2) Marco Antônio Pereira Firmino da Silva (*My Thor*)
- 3) Fabrício de Melo Jesus (Bicinho)
- 4) Alexander de Jesus Carlos (Choque)

O crime organizado no Brasil é atualmente um dos maiores desafios à segurança pública e à estabilidade institucional, caracterizando-se por uma rede complexa de cerca de **88 facções criminosas** que controlam territórios e influenciam a economia formal.

Principais Organizações e Atuação:

O cenário é dominado por grandes facções que operam com diferentes modelos de gestão e expansão:

- 1) **Primeiro Comando da Capital (PCC):** A maior organização do país, presente em 26 estados. Adota um modelo de "matriz e filial", com forte foco em logística nacional e internacional.
- 2) **Comando Vermelho (CV):** Segunda maior força, operando em um sistema de "franquias". Tem apresentado uma expansão acelerada, especialmente em estados onde desafia o domínio de grupos locais.
- 3) **Terceiro Comando Puro (TCP):** Recentemente consolidado como a **terceira força do crime no Brasil**, expandindo-se para estados como BA, CE e RS. É marcado pelo fenômeno do **narcopentecostalismo**, onde lideranças criminosas utilizam retórica religiosa para justificar disputas territoriais.
- 4) **Grupos Locais e Milícias:** Facções regionais, como a **Família do Norte (FDN)** e o **Guardiões do Estado (GDE)**, frequentemente estabelecem alianças ou conflitos com as grandes facções nacionais.

Além do tráfico de drogas e armas, o crime organizado diversificou suas operações para setores legais para facilitar a lavagem de dinheiro:

- 1) **Infiltração Econômica:** Controle de postos de gasolina, usinas de açúcar e etanol, empresas de transporte e até lojas de brinquedos;
- 2) **Contrabando Rentável:** Em 2025, estudos indicaram que o **contrabando de combustíveis** chegou a ser mais lucrativo para certas organizações do que o tráfico de cocaína;
- 3) **Controle Social:** Estima-se que mais de **28 milhões de brasileiros** vivam em territórios sob influência direta ou parcial dessas organizações.

O Estado brasileiro tem endurecido as medidas de combate, com destaque para atualizações recentes:

- ✓ **Lei 15.358/2026 (Marco Legal):** Sancionada em março de 2026, define e pune condutas de organizações criminosas ultraviolentas e milícias privadas, focando no domínio social estruturado.
- ✓ **Foco na Descapitalização:** A estratégia atual do governo prioriza atingir o braço financeiro das facções e reforçar a inteligência nas fronteiras e portos.

- ✓ **Debate sobre "Narcoterrorismo":** Existe uma discussão no Congresso para classificar o narcotráfico como terrorismo, embora especialistas alertem para riscos de soberania e mudanças de regime jurídico.

A ciência criminológica, de qualquer modo, já conta com incontáveis estudos sobre as organizações criminosas. Dentre tantas outras, são apontadas como suas características marcantes: hierarquia estrutural, planejamento empresarial, claro objetivo de lucros, uso de meios tecnológicos avançados, recrutamento de pessoas, divisão funcional de atividades, conexão estrutural ou funcional com o poder público e/ou com o poder político, oferta de prestações sociais, divisão territorial das atividades, alto poder de intimidação, alta capacitação para a fraude, conexão local, regional, nacional ou internacional com outras organizações etc.

A "criminalidade organizada" constitui verdadeiro flagelo mundial que, além de retirar enormes lucros das diferentes ações criminosas, tem consequências humanas e sociais dramáticas. As organizações criminosas perturbam não só o livre mercado e a concorrência leal, mas também as próprias regras da convivência social.

As principais características do crime organizado referem-se à forma como esses grupos se estruturam para garantir a continuidade de suas atividades ilícitas e maximizar lucros. No Brasil, a definição legal é estabelecida pela Lei nº 12.850/2013, que define organização criminosa pela associação de quatro ou mais pessoas.

ESTRUTURA E ORGANIZAÇÃO

- 1) **Hierarquia e Cadeia de Comando:** Existe uma estrutura piramidal com lideranças claras e níveis de subordinação;
- 2) **Divisão de Tarefas:** Os membros possuem funções específicas (logística, financeira, operacional), muitas vezes operando de forma compartimentada para proteger a cúpula.
- 3) **Estabilidade e Permanência:** Diferente de uma quadrilha comum, o grupo visa a continuidade no tempo, sobrevivendo mesmo com a prisão ou morte de líderes.

MÉTODOS DE OPERAÇÃO

- 1) **Objetivo de Lucro:** A finalidade principal é a obtenção de vantagem econômica, tratando o crime como um "negócio";
- 2) **Uso de Violência e Intimidação:** Utilizam o medo para controlar territórios, garantir o silêncio de testemunhas e resolver conflitos internos;
- 3) **Poder de Corrupção:** Infiltração em órgãos do Estado para obter informações privilegiadas, proteção ou impunidade;
- 4) **Lavagem de Dinheiro:** Necessidade constante de "legalizar" os lucros obtidos ilicitamente através de empresas de fachada ou investimentos legítimos.

ATUAÇÃO TERRITORIAL E TRANSNACIONAL

- 1) **Controle Territorial:** Domínio sobre áreas geográficas específicas, onde o grupo pode atuar como um "Estado paralelo".
- 2) **Conexões Internacionais:** Muitos grupos operam de forma transnacional, colaborando com cartéis e máfias estrangeiras para o tráfico de drogas e armas.

PRINCIPAIS CARACTERÍSTICAS DO CRIME ORGANIZADO

- 1) Participação de agentes estatais;
- 2) Alto grau de operacionalidade;
- 3) Constante mutação;
- 4) Pouca visibilidade de danos. Seguem abaixo características possíveis de estarem presentes em uma organização criminosa:
- 5) Hierarquia estrutural;
- 6) Planejamento empresarial;
- 7) Uso de meios tecnológicos avançados;

- 8) Recrutamento de pessoas;
- 9) Divisão funcional das atividades;
- 10) Conexão estrutural ou funcional com o poder público ou com agente do poder público;
- 11) Oferta de prestações sociais; Divisão territorial das atividades ilícitas;
- 12) Alto poder de intimidação;
- 13) Alta capacidade para a prática de fraudes;
- 14) Conexão local, regional, nacional ou internacional com outra organização criminosa.

MODALIDADES DO CRIME ORGANIZADO:

TRÁFICO ILEGAL: Geralmente são praticados paralelamente a um comércio legalizado: restaurantes, hotéis, etc. Em alguns casos corrompem agentes públicos para conseguirem o objetivo almejado. O tráfico pode ser de drogas, de armas, de seres humanos para prostituição, animais silvestres, além do comércio de órgãos.

LAVAGEM DE DINHEIRO: O termo “lavagem de dinheiro” é a transformação do dinheiro ilícito em aparentemente lícito. Exemplo: “paraísos fiscais” entre eles, Ilhas Virgens Britânicas, Uruguai, Panamá; criação de empresas de fachada; movimentações financeiras em diversas contas “laranjas”.

FALSIFICAÇÃO DE PRODUTOS: Dotada de estrutura empresarial com maquinário e pessoal qualificado, a organização produz falsificações perfeitas de diversos produtos no mercado, sobretudo os que mais estão destacando nas vendas. Exemplo: Comércio de produtos piratas; CDs, calçados, falsificação de diplomas, clonagem de cartões, etc.

ROUBO DE CARGAS: São contratados assaltantes que têm como missão roubar o caminhão entregar a terceiros, que levarão a carga para um local desconhecido pelos criminosos, para estancar as informações da organização. A distribuição é feita através de empresas legalizadas e conveniadas a varejistas relativos à carga (supermercados, farmácias, calçados).

TRÁFICO DE ENTORPECENTES: Considerada a modalidade mais lucrativa e preocupante pela Polícia Federal.

TRÁFICO DE ARMAS: Segunda maior fonte de renda, abastecendo conflitos locais e facções.

TRÁFICO DE PESSOAS E ÓRGÃOS: Exploração de indivíduos vulneráveis para fins de prostituição ou trabalho escravo.

CRIMES AMBIENTAIS: Extração ilegal de madeira, mineração em terras protegidas e tráfico de animais selvagens.

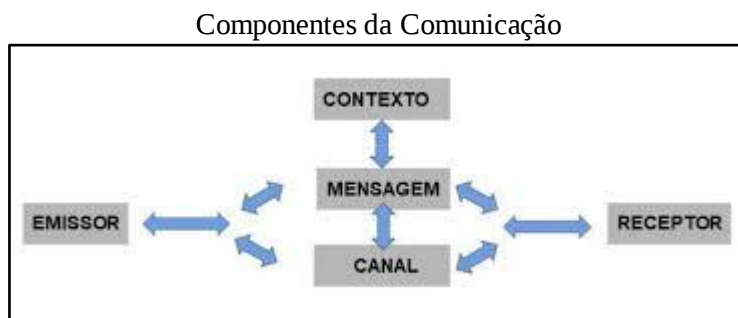
CRIMES CIBERNÉTICOS: Ataques a sistemas bancários e infraestruturas para extorsão e roubo de dados.

A modalidade do crime organizado refere-se à forma como grupos estruturados planejam e executam atividades ilegais de maneira contínua para obter lucro e poder. No Brasil, a Lei nº 12.850/2013 define organização criminosa como a associação de **4 ou mais pessoas** com estrutura ordenada, divisão de tarefas e foco em crimes com penas superiores a 4 anos ou de caráter transnacional

SISTEMA DE COMUNICAÇÃO (SIC)

Objetivos: Desenvolver conhecimentos sobre Sistemas de comunicação.

A comunicação por multimeios refere-se ao uso integrado de diversos canais e linguagens (texto, som, imagem estática e em movimento) para transmitir uma mensagem de forma estratégica. Em vez de se limitar a um único meio, ela explora a intersecção e a convergência entre mídias tradicionais e digitais. As informações a seguir possuem compilações do livro Segurança Privada no Brasil: Fundamentos Históricos & Formação Multiprofissional (Soares, 2026).



Fonte: <https://brainly.com.br>

1. **Emissor:** é o sujeito que gera a ideia ou sinal;
2. **Mensagem:** é o conteúdo, a informação, o fato a ser comunicado ao receptor;
3. **Receptor, Decodificador, Destinatário:** é aquele (s) para quem se dirige a mensagem;
4. **Canal da Comunicação ou Meio de Comunicação:** trata-se do meio utilizado para transmissão da mensagem. Os meios são mais variados, tais como sons, cheiro, imagem, palavras, etc.
5. **Código:** é o conjunto de símbolos organizados na elaboração da mensagem, o emissor codifica o que o receptor deve decodificar e, para tanto, é necessário o conhecimento do código por ambas as partes;
6. **Contexto:** situação, objeto ou ser a que mensagem se refere.

O campo de Multimeios é interdisciplinar e prepara profissionais para atuar em um mercado que exige versatilidade tecnológica e criativa.

Linguagens Integradas: Combina elementos visuais (gráficos, vídeos), sonoros (podcasts, trilhas) e textuais para criar narrativas complexas em plataformas digitais e analógicas.

Convergência Digital: Foca na adaptação de conteúdo para diferentes dispositivos (computadores, smartphones, tablets) e plataformas, como redes sociais e webseries.

Gestão Estratégica: Além da criação, envolve o planejamento e a gestão de processos comunicativos em instituições governamentais, empresas ou escolas.

Segurança nas Comunicações: Todas as medidas são tomadas para proteger os sistemas de comunicações de modo a impedir ou pelo menos dificultar a obtenção de informações por terceiros, não destinatários da mensagem. A segurança é considerada em todos os seus aspectos, abrangendo a segurança do material e sua exploração.

Meios de Comunicação: São agentes e equipamentos especializados interligados para transmitir e receber mensagens escritas, impressas ou faladas; com rapidez, segurança, confiabilidade e continuidade exigidas pelas operações policiais e de segurança privada. Exemplos: rádios, telefone, fax, computador, etc.

Canal: É a frequência em que a rede ou transceptor de radiocomunicação está operando.

Posto: Menor órgão de comunicação, onde se instala ou funciona qualquer meio.

Rede de comunicação: Conjunto de postos de uma mesma espécie, operando num mesmo processo de frequência.

Órgão de comunicação: Conjunto de pessoal e material organizado administrativamente para planejar, coordenar, controlar, apoiar ou explorar as redes de comunicações. Também chamado de posto diretor ou PDR (posto diretor da rede).

SISTEMAS DE COMUNICAÇÕES: Radiocomunicação

Conjunto de órgão e meios de comunicações estruturados em redes de diferentes espécies e níveis hierárquicos que se inter-relacionam e se completam, facilitando as ligações. Podem ser divididos em dois grandes grupos, Sistemas via Cabo e os Sistemas via Rádio. O Sistema via Cabo, se utiliza um cabo condutor, denominado linha de transmissão.

Características principais: Excelente confiabilidade, pouca flexibilidade para ampliações que não tenham um cuidadoso estudo e planejamento, necessitando de grandes investimentos com a implantação de cabos e da central de comutação. Como necessita de cabos, torna-se impossível a comunicação móvel.

Os Sistemas via Rádio utilizam ondas eletromagnéticas como elemento de ligação entre transmissor e o receptor. Ondas irradiam-se pelo espaço, dispensando a existência de quaisquer meios físicos para sua transmissão, sendo a implantação deste sistema grandemente facilitada.

Comparando ao sistema via cabo, o sistema via rádio utiliza equipamentos eletrônicos relativamente complexos para o processamento dos sinais necessários à operação do sistema. Possui baixa confiabilidade, dependendo da propagação das ondas eletromagnéticas; podem atingir dezenas de quilômetros, possuindo ótima flexibilidade para ampliações. Pelas características tornam o sistema via rádio adequado para comunicações à longa distância para comunicações móveis.

São exemplos de Sistema via Cabo: a) Telefone; b) Fac-símile; c) Microinformática (rede de dados);

São exemplos de Sistema via Rádio: a) Rádio VHF/FM; b) Rádio HF/SSB; c) Telefonia Celular; d) Internet de alto desempenho.

Mensagem: É qualquer ordem, informação, fotografia ou sinal expresso convenientemente, em linguagem clara ou não, de modo a permitir a transmissão por meio de comunicação.

Conceito de radiocomunicação e sua finalidade: é a comunicação entre pessoas e postos, que utilizam o rádio como meio para estabelecerem trocas de informações com a finalidade da transmissão de mensagens, estabelecendo uma comunicação bidirecional. Cada posto estação deverá estar equipado com um transmissor e um receptor.

Estas mensagens ou informações são transformadas pelo transmissor, em sinais de radiofrequência, e enviadas até uma antena de uma linha de transmissão que são enviadas ao receptor. Para transformar as informações, que se encontra em seu estado original em forma de som ou imagem, em sinais elétricos, os sistemas de telecomunicações, utilizam transdutores eletroacústicos, eletromecânicos eletrônicos, tais como microfones, alto-falantes e câmeras de vídeo.

TECNOLOGIAS EXISTENTES

Os sistemas de rádio são compostos basicamente de:

Estação fixa base: Terminal geralmente colocado junto a central de comando, junto ao gestor de comunicação. A base é constituída por terminal de rádio, fonte de alimentação e antenas direcionais ou antena onidirecional.



Fonte: <https://www.tecsolbh.com.br>

Estação Móvel ou Veicular: Terminal colocado no interior da viatura possuindo uma antena no exterior do veículo.



Fonte: <https://www.tecsolbh.com.br>

Terminal Portátil ou HT (HandieTalk): Terminal pessoal transportável.



Fonte: <https://intelisense.com.br>

Um rádio comunicador (ou transceptor) funciona convertendo sinais de voz em **ondas eletromagnéticas** que viajam pelo ar e são capturadas por outro aparelho na mesma frequência. Diferente dos celulares, eles permitem comunicação direta sem depender de torres de operadoras ou internet.

Frequência: É o número de oscilações por segundo, ou seja, é o número de ciclos na unidade de tempo, unidade de medida é o Hertz ou Hz.

Antena: É o elemento essencial do rádio. Irradia e capta as ondas eletromagnéticas (ondas de rádio e vídeo). O tamanho da antena depende do comprimento de onda seja das frequências de operação.

Repetidoras: são rádio transmissores que retransmitem, num nível mais alto, sinais de rádio no instante em que eles são recebidos, automaticamente, aumentando o alcance das comunicações. De acordo com o sistema de operação, as repetidoras podem ser do tipo Cruzada (recebe/transmite) ou paralelas (recebe/aciona).

Características de emprego das comunicações são:

- I. Tempo integral;
- II. Amplitude e desdobramento;
- III. Integração;
- IV. Flexibilidade;
- V. Apoio.

Tempo Integral: Para sua finalidade, um sistema de comunicações deve ser mantido e explorado durante 24 horas por dia. Para isso, o sistema deve ser dotado de pessoal e material de todos os níveis operacionais e de apoio.

Amplitude e desdobramento: Os meios de comunicação se estendem administrativamente e operacionalmente do 167 escalão superior ao subordinado.

Integração: O sistema de comunicações deve funcionar integrado, de forma a harmonizar os órgãos.

Flexibilidade: Um sistema de comunicações deve apresentar alternativas para atender à multiplicidade de ligações pré-estabelecidas. Situações vagas e emergenciais.

Apoio: É exercido em profundidade. Da atividade meio à atividade fim. Prioridade de atendimento dos meios de comunicações disponíveis. Emprego criterioso das reservas técnicas e remanejamento de recursos existentes.

Orientações Gerais para uso:

A exploração das comunicações deve ser feita através dos transceptores VHF/FM e obedecem às instruções contidas nas Instruções para Explorações das Comunicações (IECOM)ZVHF-FM. A eficiência das comunicações, nesta área, dependerá da correta utilização do equipamento, o que só ocorrerá se foram executados certos procedimentos de operação. As comunicações obedecerão aos seguintes pressupostos:

1. Rapidez;
2. Continuidade;
3. Confiabilidade;
4. Segurança.

Rapidez: Os Meios de Comunicações devem ser instalados explorados e mantidos de forma a assegurar as ligações sem perder o princípio da oportunidade. As mensagens são classificadas quanto à precedência.

Continuidade: As Comunicações devem ser mantidas e exploradas de forma contínua, em todos os níveis dos escalões envolvidos. O fluxo de mensagem em volume normal entre os órgãos.

Confiabilidade: A confiabilidade de uma rede de comunicações é um índice percentual que avalia o desempenho da mesma. Confiabilidade define a qualidade da rede ou sistema de comunicações.

Segurança: Consiste nas medidas tomadas visando a impedir ou dificultar a escuta e a obtenção de informações por parte de pessoas não autorizadas. Abrange os aspectos: material, 168 exploração e codificação.

Segurança das Comunicações: Consiste e todas as medidas tomadas visando a proteção do material e da mensagem, quanto a sua preparação, processamento, transmissão e recebimento, a fim de impedir ou retardar que pessoas não autorizadas tomem conhecimento do seu conteúdo. Temos a segurança do material e a segurança da exploração.

Segurança do material: Consiste na proteção que se deve dar aos materiais e documentos sigilosos de comunicações contra furto, roubo, extravio ou simples conhecimento por pessoas não credenciadas.

Segurança da exploração: São cuidados relativos à forma ou maneira de transmissão de mensagens e que, juntamente com proteção do material, protegem nossas mensagens contra a escuta e análise por pessoas inidôneas e evitam que tirem conclusões sobre nosso tráfego, volume, direção e origem.

Responsabilidade: a) O diretor da empresa é o responsável pela manutenção da segurança das comunicações no âmbito de sua unidade ou área; b) A classificação quanto à segurança é de responsabilidade e atribuição do expedidor da mensagem; c) A disciplina das redes de radiocomunicações é de responsabilidade da estação diretora geral das redes.

Rede de radiocomunicação (CONCEITO): Conjunto de postos que operam na mesma frequência e são coordenados por um dos postos que é o Posto Diretor da Rede (PDR). Temos como exemplo de um PDR o Centro de Operações (COPOM) na PMMG e a (CECOGE) na Guarda Municipal de Belo Horizonte (GMBH). Os postos são os locais onde se instalou e se explora os sistemas de comunicação via rádio. O posto pode ser fixo, móvel ou portátil.

- A. **Fixo** - quando o rádio é instalado em prédio ou ambiente similar, tal como casa ou 'trailer', sendo a designação do posto em função do local de instalação.
- B. **Móvel** - quando o rádio é instalado em veículos ou barcos, a designação do posto será ao correspondente ao veículo/barco ou pela função da autoridade.
- C. **Portátil** - quando o rádio é do tipo Hand-Talk (HT), e a designação do posto será determinada pelo órgão responsável pelo posto lançado na atividade.

Posto Diretor de Rede (PDR): Com a finalidade de coordenar a rede, um posto, normalmente aquele que serve ao escalão mais elevado, de que faz parte a rede, é designada como Posto Diretor da Rede (PDR), enquanto que os demais são designados Postos Secundários (PS). A autoridade do PDR abrange os aspectos operacionais da rede e sua disciplina, 169 quanto em funcionamento e durante o período de silêncio da rede de rádio.

Considerando que o PDR possui a responsabilidade da manutenção da disciplina de exploração da rede, o rádio operador possui também autoridade para exercer o controle operacional necessário para utilização das frequências dentro do mais alto padrão de rendimento. Entretanto, não possui capacidade de decisão sobre os problemas administrativos internos dos órgãos integrantes da rede.

Autoridade e funções do PDR: É absoluta em tudo a que se referirem as normas técnicas de operação de rede. O PDR abre e fecha a rede, controla e regula o tráfego de mensagens, corrige erros de exploração. Concede e nega permissão para postos secundários e, sobretudo, mantém a disciplina e técnica de exploração da rede rádio.

Abertura de rede - Para abrir a rede, o PDR obedece às normas contidas na IECOM, utilizando o indicativo de chamada de rede, o PDR faz a chamada de todos os postos secundários, em seguida, identifica-se através de seu indicativo. Tais indicativos constam da IECOM, depois que os postos chamados responderem na ordem alfabética ou numérica. O PDR, posteriormente, acusa o recebimento das transmissões determinando a seguir as condições de funcionamento da rede (livre ou controlada), e as prescrições quanto ao uso do rádio.

Fechamento de rede - Obedecendo as normas contidas na IECOM, o PDR para fechar a rede, utiliza o indicativo de chamada desta e determina o fechamento dos postos. Caso a rede tenha que ser reaberta mais tarde, o PDR informará aos postos a que horas e em que frequência a rede será reaberta. Esta informação poderá ser transmitida por mensagem preestabelecida ou fazendo-se menção à instrução da IECOM.

Entrada de um posto na rede - Quando um posto desejar entrar na rede, será obrigado a pedir permissão prévia ao PDR. Primeiramente, o posto transmite o indicativo de chamada do PDR e logo depois da identificação da chamada, o posto chamador esclarece as razões do seu desejo de entrar na rede. O PDR autenticará este posto de acordo com a IECOM e então dará ou negará a permissão de pedido de entrada na rede. Esta decisão será tomada depois que o PDR julgar a validade das razões do posto, ao pedir a entrada na rede.

Saída de um posto da rede - O posto que desejar deixar a rede chamará o PDR e solicitará a permissão para sair na rede.

Escuta da rede - O PDR manterá o seu receptor em escuta permanente, com a finalidade de escutar a 170 rede. O PDR também manterá constante atenção no escoamento do tráfego das mensagens, devendo sempre estar preparado para tomar as providências necessárias, caso ocorram problemas de interferência ou conflitos entre os postos.

Controle e escala das transmissões - Quando o tráfego numa rede se torna volumoso, o PDR poderá interferir, mantendo cerrado e disciplinado controle, evitando deste modo transmissões desnecessárias.

Direção da rede - Quando o tráfego de mensagens se tornarem excessivamente volumosos ou o rádio operador não possuir a devida experiência de exploração da rede de rádio, neste caso, nenhum posto pode transmitir sem primeiro chamar o PDR e solicitar permissão para transmitir.

Ainda dentro das condições de rede controlada, o PDR poderá estabelecer normas a serem seguidas por todos os postos da rede.

Imposição ou suspensão de silêncio-rádio - Dada a permissão por autoridade competente, o PDR poderá impor ou suspender a prescrição de silêncio-rádio, quando houver necessidade tática.

O PDR imporá o silêncio-rádio, chamando todos os postos da rede informando-os da prescrição em vigor. Cabe ao PDR a fiscalização desta prescrição.

Exploração da rede de rádio - Para se obter um bom atendimento de um sistema de rádio comunicações torna-se imperioso adotar critérios que evitem perda de tempo e má interpretação das mensagens, empregue corretamente os códigos e expressões adotadas, bem como evitar linguagem inadequado e prolixo. A comunicação via rádio, recorrem a um alfabeto fonético e

empregam expressões convencionais de serviço bem como códigos específicos, tomando as comunicações mais rápidas e claras.

Legibilidade - entende-se por legibilidade a clareza, compreensão da mensagem (sinais) recebida.

Intensidade - entende-se por intensidade o volume, tonalidade da mensagem (sinais) recebida.

Tabela de Legibilidade dos sinais - Classificação

ESCALA	LEGIBILIDADE	INTENSIDADE
1	Ilegível	Muito fraca
2	Legível com intermitência	Fraca
3	Legível com dificuldade	Regular
4	Legível	Boa
5	Legibilidade perfeita	Ótima

Elaboração: Amilson Soares, 2026

É utilizada a classificação acima, quando existe um pedido de como a recepção está ocorrendo. O posto deseja saber como está sendo recebido, em virtude de a comunicação estar se procedendo com dificuldade. Pra isto o operador deverá fazer o pedido usando a expressão convencional: “como me recebe?”. E como resposta o operador que está no outro rádio deve responder: “recebo 4 pontos 2”. Isto significa que a mensagem está LEGÍVEL (Escala 4) e de intensidade FRACA (Escala 2).

Disciplina da rede-rádio: As prescrições mais importantes a serem seguidas que fortalecem a manutenção da disciplina da rede são:

1. Empregar unicamente as regras de exploração em vigor;
2. Eliminar as transmissões desnecessárias ou não autorizadas;
3. Enviar indicativos de chamada com clareza e precisão;
4. Evitar o vício de desenvolvimento de expressões pessoais;
5. Saber usar as frequências estabelecidas para as redes;
6. Transmitir uma cadência a altura da capacidade de recepção do operador mais fraco da rede; não transmitir sem autorização do órgão coordenador. São responsáveis nas respectivas instituições, visando disciplinar a rede e estabelecer prioridade;
7. Responder prontamente a todos os chamados.
8. Só transmitir quando a rede estiver em silêncio, devendo o operador escutar antes de transmitir; Não interromper as transmissões de outro posto, exceto em casos excepcionais, quando a situação for grave e assim exigir.
9. Não acrescentar à mensagem termos, adjetivos, conjunções desnecessárias à compreensão da mensagem. A transmissão deve ser curta e precisa quando possível; l)
10. Cada posto deverá ter sempre um de seus integrantes, na escuta do rádio;
11. A linguagem deve ser clara, precisa, pausada, com ênfase natural;
12. Não permitir conversações informais entre operadores;

13. Dar o recebimento de todas as mensagens. Encerrada a transmissão, o posto receptor dará confirmação do recebimento ou solicitará a retransmissão, quando a mensagem não foi compreendida;
14. Não fazer chamada insistentemente a um mesmo posto. Em certas oportunidades, é comum um posto não receber as transmissões, face à sua localização.

ALFABETO E NÚMEROS FONÉTICOS NA RADIOCOMUNICAÇÃO

O termo "Alfabeto Fonético Internacional" pode se referir a dois sistemas distintos, dependendo do contexto: o **IPA (*International Phonetic Alphabet*)**, usado na linguística para representar sons, e o **Alfabeto Radiofônico da OTAN**, usado para soletração clara em comunicações.

O **alfabeto fonético da OTAN** permite transmitir eficazmente uma informação substituindo cada letra por uma palavra. É o que se chama **acrofonia**. Por exemplo, certamente já teve de soletrar o seu apelido ou o do seu interlocutor ao telefone, substituindo cada letra por outra palavra para ter a certeza de que se compreenderam bem e não cometer erros. Para transmitir o apelido DUPONT, por exemplo, poderia dizer « D » como Denis, « U » como Ursule, « P » como Pierre, « O » como Orange, « N » como Nicolas e « T » como *Thérèse* ». A OTAN simplesmente uniformizou as palavras utilizadas para substituir as letras do alfabeto. Assim, toda a gente consegue compreender-se. Este alfabeto é aliás o único reconhecido internacionalmente pela **União Internacional das Telecomunicações (UIT)**.

TABELA DO ALFABETO FONÉTICO

ALFABETO (Código) MORSE E FONÉTICO INTERNACIONAL					
Criado por Samuel Finley Breese Morse , ao inventar o telégrafo, em 1838.					
A	• –	Alfa	N	– •	November
B	– • • •	Bravo	O	– – –	Oscar
C	– • • •	Charlie	P	• – – •	Papa
D	– • •	Delta	Q	– – • –	Quebec
E	•	Echo	R	• – •	Romeo
F	• • – •	Foxtrot	S	• • •	Sierra
G	– – •	Golf	T	–	Tango
H	• • • •	Hotel	U	• • –	Uniform
I	• •	India	V	• • • –	Victor
J	• – – –	Juliett	W	• – –	Whiskey
K	– • –	Kilo	X	– • • –	X-Ray
L	• – • •	Lima	Y	– • – –	Yankee
M	– –	Mike	Z	– – • •	Zulu

“Dit” (•) - “Dah” (–)

Fonte: <https://www.pdias.com.br>

Os números no sistema fonético brasileiro (utilizado principalmente em comunicações aeronáuticas e via rádio) são adaptados para garantir que cada dígito seja compreendido sem ambiguidades, mesmo sob interferências ou ruídos.

A principal diferença para o uso cotidiano é a substituição dos números **1** e **6**, para evitar que soem parecidos com outros comandos ou palavras.

Alfabeto (Código) Morse e Fonético Internacional

1	• — — — —	Uno
2	• • — — —	Dois
3	• • • — —	Três
4	• • • • —	Quatro
5	• • • • •	Cinco
6	— • • • •	Meia
7	— — • • •	Sete
8	— — — • •	Oito
9	— — — — •	Nove
0	— — — — —	Zero

“Dit” (•) - “Dah” (—)

Fonte: <https://www.pdias.com.br>

O código civil internacional “Q”, abreviadamente “Q”, foi aprovado em 21 de dezembro do ano de 1959, em Genebra, na convenção internacional de Telecomunicações, da qual o Brasil é país signatário. Trata-se de um recurso que visa simplificar e dar maior rapidez às comunicações, pela substituição de palavras, frase ou informações por um conjunto de três letras. Código “Q”, alguns aspectos devem ser lembrados:

- a) A utilização dessa codificação por quem não a domina razoavelmente poderá causar transtornos ao invés de benefícios;
- b) Os sinais do código “Q”, não têm caráter sigiloso, são considerados como linguagem clara e corrente;
- c) O mesmo grupo de letras pode ter sentido afirmativo ou negativo;
- d) Desde que não se utilizem abreviaturas, e não sendo possível outro sinal ou método convencional, permite-se o emprego de palavras ou expressões em linguagem corrente para complementar ou ampliar o significado dos sinais “Q”.

CÓDIGO “Q”

QAP - na escuta	QTO - saindo da base	A - alfa	O - oscar
QRA -qual o nome	QTP - retornando á base	B - bravo	P - papa
QRM -interferência	QTE -qual minha orientação	C - charlie	Q - quebec
QRT -finalizar a transmissão	QTK -velocidade do veículo	D - delta	R - romeo
QRX -aguarde	QTW -como estão as vítimas?	E - echo	S - sierra
QRV - está preparado?	QTY -seguindo pro local do acidente	F - foxtrot	T - tango
QRD - rota	QUD -sinal de emergência	G - golf	U -uniform
QRL - você está ocupado?	QUE -usar telefone	H - hotel	V - victor
QRU - tem algo para mim?	QUR -foram atendidos	I - índia	W - whisky
QRZ -quem está me chamando	QUS - você já avistou avítima?	J - juliett	X - x-ray
QTA -cancelar a mensagem	QUT -local do acidente	K - kilo	Y - yankee
QTC -mensagem	QSF -final de atendimento	L - lima	Z - zulu
QTH -localização	QSI -dinheiro	M - mike	
QTI - a caminho/em direção	QSL -entendido	N - november	
QTR - hora certa	QSN -está me ouvindo		
QTT - identificação	QSQ -téc. Enfermagem		
QTI - qual a sua velocidade?	QSO -contato baixa frequência		

Fonte: <https://pt.scribd.com>

CÓDIGO “10”

CÓDIGO	DESCRIÇÃO	
10-70	incêndio em...	ECHO BRAVO - estação bombeiro
10-4	mensagem recebida	BRAVOS - bombeiros
10-18	tem alguma coisa para mim?	BRAVO CHARLIE - bombeiro coordenador
10-23	esteja atento ou de prontidão	BRAVO LIMA - bombeiro líder
10-24	tarefa terminada	BRAVO SIERRA - bombeiro supervisor
10-30	tem clandestino na faixa	TST - tec. de segurança
10-34	com problemas; preciso de ajuda	TKS - obrigado
10-35	assunto urgente; não pode ser tratado pelo rádio.	QSQ - téc. Enfermagem
10-37	desastre ou óbito	DELTA - operador CECOM
10-38	envie socorros médicos; pessoas feridas	
10-42	acidente de tráfego em...	
10-54	animais na estrada	
10-57	atropelamento e fuga de motorista	
10-200	solicitando apoio da polícia	

Em radiocomunicação (usada por policiais, bombeiros ou segurança), o **Código 10** faz parte do sistema americano "Ten-Code".

A comunicação por telefone é um dos meios mais diretos e eficazes para resolver problemas e estabelecer conexões, seja em contextos pessoais ou profissionais. Diferente de mensagens de texto, o telefone permite o uso do **tom de voz**, que transmite emoção e reduz mal-entendidos

SISTEMAS DE COMUNICAÇÕES: Telefonia



Fonte: <https://altoastral.joaobidu.com.br>

A comunicação por telefone é um dos meios mais diretos e eficazes para resolver problemas e estabelecer conexões, seja em contextos pessoais ou profissionais. Diferente de mensagens de texto, o telefone permite o uso do tom de voz, que transmite emoção e reduz mal-entendidos.

O dia 10 de março de 1876 está marcado na história como a data da primeira ligação telefônica registrada. O inventor britânico naturalizado norte-americano Alexander Graham Bell, de sua casa em Boston, nos Estados Unidos (EUA), chamou seu assistente, Thomas Watson, que estava em outro cômodo da residência, e disse a frase que entrou para a história: “Senhor Watson, venha aqui. Preciso vê-lo”. A data acabou sendo celebrada como o Dia do Telefone.

Três dias antes da primeira ligação, Bell havia obtido a patente da invenção do telefone, após disputa histórica sobre a autoria do aparelho com outros inventores, entre eles Antonio Meucci. Poucos meses depois, em junho daquele mesmo ano, o então imperador do Brasil, Dom Pedro II, experimentou pessoalmente a invenção durante uma exposição internacional na cidade de Filadélfia (EUA).

No ano seguinte, em 1877, a tecnologia chegou ao Brasil, com a instalação de um dos primeiros telefones do país no Palácio Imperial da Quinta da Boa Vista, no Rio de Janeiro, onde hoje funciona o Museu Nacional.

Para garantir uma comunicação eficiente e profissional ao telefone, considere as seguintes diretrizes:

1. **Tom de Voz e Dicção:** Mantenha um tom de voz moderado (nem muito alto, nem muito baixo) e fale de forma pausada para facilitar a compreensão.
2. **Apresentação e Cordialidade:** Identifique-se logo no início da chamada e demonstre interesse real em ajudar.
3. **Escuta Ativa:** Dê sinais de que está acompanhando a fala da outra pessoa (como "sim", "entendo") e evite interromper.
4. **Clareza e Agilidade:** Seja objetivo, tenha as informações necessárias à mão e anuncie claramente as ações que irá realizar.
5. **Uso Correto da Gramática:** Lembre-se que o termo gramaticalmente sugerido é falar "**ao telefone**", indicando aproximação do aparelho

No Brasil, existem cerca de 20 milhões de assinantes do serviço de telefonia fixa, enquanto a telefonia móvel soma aproximadamente 270 milhões de acessos. A implantação do 5G, a limpeza da faixa de 3,5 GHz e os novos leilões de espectro são instrumentos para garantir que o país acompanhe a evolução tecnológica e amplie a conectividade.

UNIVERSALIZAÇÃO TELEFÔNICA

Tecnologia	Período de expansão	Impacto tecnológico	O que mudou para o usuário
Telefonia fixa	Final do século XIX e século XX	Redes de voz baseadas em cabos e centrais telefônicas	Possibilidade de falar à distância de forma imediata entre residências, empresas e governos
2G / 3G	Final dos anos 1990 e anos 2000	Digitalização da telefonia móvel e início da internet no celular	Popularização do celular, envio de SMS e primeiros acessos à internet móvel
4G	A nos 2010	Banda larga móvel de alta velocidade	Uso massivo de aplicativos, redes sociais, streaming de vídeo e serviços digitais no celular
5G	Anos 2020	Alta velocidade, baixa latência e grande capacidade de conexão	Expansão da Internet das Coisas, cidades inteligentes, automação industrial e novos serviços digitais

Fonte: <https://www.gov.br>

O Futuro da telefonia: Embora o 5G ainda esteja em fase de expansão para cidades menores, o 6G já aparece no horizonte. O conselheiro Octavio Pieranti comenta que a nova geração de redes móveis deve começar a chegar ao mercado por volta de 2030. Ele ressalta que, em relação à implantação dessa tecnologia, o Brasil parte de uma posição favorável, pois o país já acumula experiência com redes 5G *standalone* (SA).

Na segurança privada, o telefone (especialmente o smartphone) evoluiu de um simples meio de comunicação para uma ferramenta tecnológica central que integra gestão, monitoramento e resposta a emergências.

Controle de Rondas Eletrônicas: Aplicativos instalados em smartphones substituem os antigos bastões de ronda. Eles permitem que o vigilante registre sua passagem por pontos específicos via geolocalização ou leitura de QR Codes, enviando os dados em tempo real para a central.

Comunicação *Push-to-Talk* (PTT): Softwares que transformam o celular em um rádio comunicador digital. Essa tecnologia é preferida por oferecer som mais claro, sem interferências de rádio comum, e ser mais econômica para a empresa.

Monitoramento de Imagens: Profissionais podem visualizar câmeras de CFTV diretamente na palma da mão, permitindo a verificação remota de alarmes ou a vigilância de áreas enquanto estão em deslocamento.

Senhas e Contrassenhas: O telefone é usado para validações discretas em situações de emergência. Em caso de coação, o vigilante ou o cliente pode fornecer uma contrassenha específica que indica perigo à central sem alertar o agressor.

SISTEMAS DE COMUNICAÇÕES: Redes (Mídias) Sociais.



Fonte: <https://brasilescola.uol.com.br>

As redes sociais na segurança privada funcionam como uma faca de dois gumes: são ferramentas poderosas para marketing e inteligência, mas representam riscos críticos de vulnerabilidade operacional se usadas sem rigorosa política de conduta.

O profissional da segurança privada deve se atentar para os riscos e cuidados. O comportamento digital do vigilante impacta diretamente a segurança do posto e sua própria carreira. Deve atentar-se:

1. **Sigilo Operacional:** É proibido postar fotos uniformizado, em postos de serviço ou exibindo armamento e rotinas. Isso expõe vulnerabilidades que podem ser usadas por criminosos.
2. **Geolocalização:** O compartilhamento de localização em tempo real pode facilitar o planejamento de ataques contra o profissional ou o patrimônio protegido.
3. **Consequências Jurídicas:** Postagens inadequadas podem servir como prova em processos trabalhistas ou levar a demissões por justa causa por violação de normas internas.
4. **Imagem Profissional:** Redes sociais são consideradas o "cartão de visitas" do vigilante; manter uma postura ética online é fundamental para a empregabilidade.

O Uso Estratégico pelas Empresas de segurança que utilizam as plataformas digitais para fortalecer a operação e o negócio, precisa atentar-se para:

1. **Monitoramento de Ameaças:** Ferramentas de Inteligência Artificial analisam dados de redes sociais para identificar padrões de comportamento, discursos de ódio ou planos de atos violentos, permitindo ações preventivas.
2. **Marketing Digital:** Plataformas como Instagram e LinkedIn são usadas para atrair clientes, demonstrar tecnologias (como drones e sistemas eletrônicos) e construir autoridade no setor.
3. **Gestão de Crise:** O monitoramento de mídias sociais ajuda a entender a percepção de segurança do público e a reagir rapidamente a *fake news* ou incidentes que viralizam.

Para mitigar riscos, recomenda-se que as empresas implementem uma política interna de uso de mídias sociais:

1. **Treinamento:** Educar colaboradores sobre os perigos da exposição da rotina e dados do trabalho.
2. **Privacidade:** Incentivar o uso de perfis privados e a ativação de autenticação em duas etapas para evitar invasões.
3. **Configuração de Perfil:** Orientar para que não se compartilhem informações sensíveis, como endereço residencial ou documentos confidenciais.

As **redes sociais** são plataformas digitais que permitem a conexão entre pessoas, grupos ou empresas, facilitando a troca de informações e o compartilhamento de conteúdo como fotos, vídeos e textos. Diferente do conceito tradicional de "rede social" da sociologia — que estuda as relações humanas há décadas —, as redes sociais virtuais são ambientes onde a interação ocorre em tempo real, independentemente da distância geográfica.

De acordo com dados de 2026 e relatórios recentes de plataformas como Brasil Escola e *Serasa Experian*, as plataformas dominantes incluem:

- **WhatsApp:** O principal meio de comunicação instantânea, com milhões de usuários ativos para conversas privadas e profissionais.
- **YouTube:** A maior plataforma de compartilhamento de vídeos, utilizada tanto para entretenimento quanto para educação.
- **Instagram:** Focado no compartilhamento visual (fotos e *Reels*), é central para o marketing de influência.
- **Facebook:** Continua sendo uma das redes mais populosas, integrando grupos e eventos.
- **TikTok:** Conhecido pelos vídeos curtos e virais, com crescimento acelerado entre o público jovem.

Embora ofereçam benefícios como a democratização da informação e o estreitamento de laços, especialistas alertam para os riscos do uso excessivo. Debates atuais, como os apresentados no podcast De Repente CRINGE¹, destacam o impacto na saúde mental de jovens e a formação de "bolhas" ideológicas causadas pelos algoritmos de personalização.

SISTEMA ELETRÔNICOS DE SEGURANÇA (SEL)

Objetivo

Dotar o aluno de conhecimentos sobre sistema eletrônicos de segurança utilizados no monitoramento de sistemas eletrônicos de segurança e no rastreamento de numerário, bens ou valores.

¹ O **De Repente CRINGE** é um podcast apresentado pelas irmãs e influenciadoras **Luisa Accorsi** e **Marianna Accorsi**. O projeto surgiu quando ambas, ao completarem 30 anos, perceberam que haviam se tornado "cringe" (termo usado para algo que causa vergonha alheia ou que é ultrapassado para as gerações mais novas) e começaram a se sentir um pouco perdidas nessa nova fase da vida

Conteúdo programático

Sistemas eletrônicos de segurança

Componentes do sistema eletrônico de segurança;

Contexto:

Os sistemas eletrônicos de segurança são constituídos por um conjunto integrado de equipamentos, dispositivos, softwares e meios de comunicação que atuam de forma coordenada para prevenir, detectar, registrar e responder a eventos que possam comprometer a segurança de pessoas, patrimônios, informações e processos. O conhecimento sobre esses componentes é essencial para que o operador de monitoramento compreenda a origem dos eventos recebidos na central, identifique possíveis falhas operacionais e execute corretamente os protocolos estabelecidos para cada situação.

Neste conteúdo serão apresentados os principais elementos que compõem um sistema eletrônico de segurança, incluindo centrais de alarme, detectores, sensores, câmeras de videomonitoramento, gravadores digitais, controladoras de acesso, dispositivos de identificação, rastreadores, equipamentos de comunicação, fontes de alimentação, nobreaks, servidores e plataformas de gerenciamento. Também serão abordadas as funções desempenhadas por cada componente dentro da arquitetura do sistema e sua importância para a continuidade operacional.

Será demonstrado como esses equipamentos se interligam por meio de redes cabeadas e sem fio, protocolos de comunicação e plataformas integradas, formando uma infraestrutura capaz de transmitir informações em tempo real para uma Central de Monitoramento. O aluno compreenderá que o desempenho global do sistema depende da correta instalação, configuração, integração e manutenção de todos os seus componentes, sendo suficiente que um único elemento apresente falha para comprometer a eficiência do conjunto.

Ao final deste conteúdo, o profissional deverá reconhecer os principais componentes presentes em sistemas modernos de segurança eletrônica, compreender sua finalidade operacional e identificar sua participação no fluxo de geração, transmissão e tratamento dos eventos monitorados, estabelecendo uma base sólida para os conteúdos técnicos que serão desenvolvidos nas disciplinas subsequentes.

Equipamentos de monitoramento: câmeras, alarmes, sensores e outras tecnologias;

Contexto:

Os equipamentos de monitoramento constituem a principal fonte de informações utilizadas pelas Centrais de Monitoramento/rastreamento para identificar situações de risco, acompanhar ocorrências em tempo real e apoiar a tomada de decisões operacionais. O correto entendimento do funcionamento desses dispositivos permite que operadores e supervisores interpretem adequadamente os eventos recebidos, reduzam falsas ocorrências e adotem procedimentos compatíveis com os protocolos operacionais definidos pela empresa.

Neste tópico serão estudadas as características técnicas e operacionais das principais tecnologias empregadas no monitoramento eletrônico, incluindo sistemas de CFTV, câmeras IP, gravadores digitais, sensores infravermelhos, sensores magnéticos, detectores de quebra de vidro, sensores de fumaça, detectores de temperatura, sensores perimetrais, botões de pânico, alarmes monitorados, cercas elétricas, sensores micro-ondas, radares, analíticos de vídeo e demais dispositivos empregados na proteção patrimonial.

Também será abordado o princípio de funcionamento desses equipamentos, os tipos de eventos que podem gerar, suas limitações técnicas, fatores que influenciam seu desempenho e os cuidados necessários para minimizar alarmes indevidos. Serão discutidas situações reais em que fatores ambientais, falhas de instalação ou configurações inadequadas podem comprometer a confiabilidade do monitoramento.

Ao término deste conteúdo, o aluno estará apto a compreender como cada tecnologia contribui para o processo de monitoramento eletrônico, reconhecendo as informações fornecidas pelos equipamentos e sua relevância para a análise dos eventos recebidos pela Central de Monitoramento.

Equipamentos de controle de acesso: fechaduras eletrônicas, raio-x, identificação biométrica, catracas, cartões, portaria remota e outras tecnologias;

Contexto:

Os sistemas de controle de acesso têm como finalidade administrar, registrar e restringir a circulação de pessoas, veículos e materiais em áreas protegidas, garantindo que apenas indivíduos previamente autorizados tenham acesso aos ambientes monitorados. Atualmente, esses sistemas representam um dos principais recursos tecnológicos empregados em condomínios, empresas, instituições financeiras, órgãos públicos, instalações industriais e infraestruturas críticas.

Durante este conteúdo serão apresentados os diferentes equipamentos utilizados em soluções de controle de acesso, como fechaduras eletromagnéticas, controladoras, leitores de cartões de proximidade, cartões inteligentes, biometria facial, biometria digital, reconhecimento de íris, QR Codes, leitores veiculares, cancelas automáticas, catracas eletrônicas, torniquetes, detectores de metais, equipamentos de inspeção por raios X, interfones IP, videoporteiros e sistemas de portaria remota.

O aluno compreenderá como essas tecnologias se integram às plataformas de monitoramento, possibilitando o gerenciamento remoto de acessos, a validação de credenciais, a geração de registros de auditoria e o acionamento automático de protocolos diante de tentativas de acesso não autorizado, coação, violação de dispositivos ou falhas operacionais. Também serão abordados aspectos relacionados à rastreabilidade das operações e à preservação da segurança física e lógica das instalações.

Ao concluir este tópico, o profissional estará apto a compreender o funcionamento dos sistemas de controle de acesso, interpretar os eventos gerados por essas tecnologias e executar procedimentos operacionais compatíveis com as políticas de segurança estabelecidas para cada ambiente monitorado.

Equipamentos de rastreamento de numerários, bens ou valores: sistemas de geolocalização (GPS) e telemetria embarcada.

Contexto:

O rastreamento de numerários, bens e valores constitui uma atividade estratégica para a gestão de riscos em operações logísticas, transporte de cargas de alto valor agregado e transporte de numerário. O uso de tecnologias de geolocalização e telemetria permite acompanhar continuamente a posição dos veículos, monitorar condições operacionais e identificar situações de risco que demandem intervenção imediata da Central de Monitoramento/rastreamento.

Neste conteúdo serão apresentados os fundamentos dos sistemas de posicionamento por satélite (GPS e demais sistemas globais de navegação), tecnologias de comunicação móvel, dispositivos rastreadores, módulos embarcados, sensores instalados em compartimentos de carga, cofres inteligentes e demais equipamentos utilizados para monitoramento remoto de ativos móveis. Também serão abordados conceitos relacionados à precisão do posicionamento, disponibilidade do sinal, redundância das comunicações e confiabilidade das informações transmitidas.

Serão estudados os recursos de telemetria embarcada empregados para monitorar velocidade, ignição, abertura de portas, acionamento de botão de pânico, desengate de carretas, violação de compartimentos, comportamento do condutor, consumo de combustível, paradas não autorizadas, desvios de rota e outras variáveis relevantes para a gestão operacional e a mitigação de riscos. O aluno compreenderá como essas informações subsidiam decisões rápidas e fundamentadas durante situações críticas.

Ao final deste conteúdo, o profissional deverá compreender o funcionamento dos sistemas de rastreamento e telemetria, interpretar corretamente os eventos gerados pelos equipamentos embarcados e reconhecer a importância dessas tecnologias para a proteção de pessoas, cargas, numerários e demais ativos monitorados.

Demonstração de equipamentos de CFTV, alarmes, sensores e controle de acesso.

Contexto:

A demonstração prática dos equipamentos constitui uma etapa essencial do processo de aprendizagem, permitindo que o aluno relacione os conceitos teóricos apresentados ao funcionamento real das tecnologias empregadas nas Centrais de Monitoramento/rastreamento. A familiarização com os dispositivos amplia a capacidade de interpretação dos eventos operacionais e reduz a ocorrência de erros durante o atendimento das ocorrências.

Durante esta atividade serão apresentados equipamentos reais ou demonstrativos de sistemas de videomonitoramento, centrais de alarme, sensores, detectores, controladoras de acesso, leitores biométricos, gravadores digitais, câmeras IP, módulos de comunicação, rastreadores e demais dispositivos empregados na segurança eletrônica. Sempre que possível, os participantes terão contato direto com os equipamentos, observando sua instalação, configuração básica, operação e geração de eventos.

Também serão realizadas simulações de situações operacionais, demonstrando o comportamento dos sistemas diante de ocorrências como invasões, acionamentos de botão de pânico, falhas de comunicação, abertura de portas, alarmes técnicos, violações de sensores e eventos de controle de acesso. Os participantes acompanharão o processamento dessas informações nas plataformas de monitoramento, compreendendo a sequência de tratamento operacional adotada pelas centrais.

Ao término desta atividade, espera-se que o aluno seja capaz de identificar visualmente os principais equipamentos utilizados na segurança eletrônica, compreender sua finalidade operacional e correlacionar os eventos observados em campo com aqueles recebidos pelos softwares de monitoramento, fortalecendo a integração entre conhecimento técnico e prática profissional.

Plataformas de gestão de segurança **softwares de CFTV e gestão de vídeo;**

Contexto:

Os softwares de gerenciamento de vídeo, conhecidos internacionalmente como Video Management Systems (VMS), constituem o núcleo operacional dos sistemas modernos de Circuito Fechado de Televisão (CFTV). Essas plataformas permitem centralizar, visualizar, gravar, pesquisar e administrar imagens provenientes de centenas ou milhares de câmeras distribuídas em diferentes locais, proporcionando aos operadores uma visão integrada do ambiente monitorado. A evolução dessas soluções transformou o videomonitoramento em uma ferramenta estratégica para prevenção de perdas, proteção patrimonial, segurança pública e gestão operacional.

Neste conteúdo serão apresentados os princípios de funcionamento dos softwares de gestão de vídeo, abordando sua arquitetura, recursos e aplicações em Centrais de Monitoramento/rastreamento. O aluno compreenderá como ocorre a comunicação entre câmeras IP, codificadores, gravadores de vídeo, servidores e estações de operação, bem como a importância da infraestrutura de rede, do armazenamento digital e dos mecanismos de redundância para garantir a disponibilidade contínua das imagens.

Serão estudadas funcionalidades como monitoramento em tempo real, gravação contínua ou por eventos, reprodução de imagens gravadas, pesquisa inteligente, controle de câmeras móveis (PTZ), mapas sinóticos, videowall, alarmes de vídeo, integração com sensores, notificações automáticas e recursos de análise inteligente de imagens. Também serão apresentados conceitos relacionados à inteligência artificial aplicada ao videomonitoramento, incluindo detecção de intrusão, cruzamento de linha virtual, permanência em área restrita, reconhecimento facial, classificação de objetos e análise comportamental.

Ao final deste conteúdo, o aluno compreenderá o papel estratégico dos softwares de gestão de vídeo nas operações de monitoramento eletrônico, reconhecendo suas funcionalidades, limitações e benefícios para a tomada de decisões em tempo real. Também estará apto a interpretar corretamente os eventos gerados pelo sistema, compreender os fluxos operacionais da Central de Monitoramento/rastreamento e atuar de forma integrada com os demais sistemas eletrônicos de segurança.

softwares de monitoramento;

Contexto:

Os softwares de monitoramento representam a principal ferramenta utilizada pelos operadores das Centrais de Monitoramento/rastreamento para recepção, processamento, classificação e tratamento dos eventos provenientes dos sistemas eletrônicos de segurança. Essas plataformas concentram informações oriundas de sistemas de alarme, sensores, dispositivos de automação, rastreamento, controle de acesso e videomonitoramento, permitindo que as ocorrências sejam analisadas e tratadas de acordo com protocolos operacionais previamente estabelecidos.

Durante este conteúdo serão apresentados os conceitos fundamentais relacionados ao funcionamento dos softwares de monitoramento/rastreamento, destacando sua arquitetura, banco de dados, mecanismos de comunicação, gerenciamento de eventos e integração com equipamentos instalados em campo. O aluno compreenderá como ocorre o fluxo completo de um evento, desde sua geração pelo equipamento até sua apresentação ao operador, incluindo processos de validação, classificação, priorização e encerramento da ocorrência.

Também serão estudadas funcionalidades como cadastro de clientes, gerenciamento de contratos, monitoramento de múltiplas contas, tratamento de eventos técnicos, registro de ocorrências, histórico operacional, geração de relatórios estatísticos, gerenciamento de operadores, auditoria de ações e monitoramento da disponibilidade dos sistemas. Serão

abordadas ainda práticas para redução de alarmes falsos, gerenciamento de filas de atendimento, rastreabilidade das ações executadas e padronização dos procedimentos operacionais.

Ao concluir este conteúdo, o aluno compreenderá como os softwares de monitoramento suportam as atividades desenvolvidas em uma Central de Monitoramento/rastreamento, reconhecendo sua importância para a eficiência operacional, para a rastreabilidade das ocorrências e para a tomada de decisões fundamentadas em informações confiáveis e atualizadas em tempo real.

softwares de controle de acesso;

Contexto:

Os softwares de controle de acesso são responsáveis pelo gerenciamento das credenciais, dispositivos e regras que controlam a circulação de pessoas e veículos em ambientes protegidos. Essas plataformas permitem administrar permissões de acesso, monitorar eventos em tempo real, registrar todas as movimentações realizadas e integrar informações provenientes de diferentes dispositivos eletrônicos, contribuindo para o fortalecimento da segurança física das instalações.

Neste tópico serão apresentados os principais recursos dessas plataformas, incluindo cadastramento de usuários, gerenciamento de perfis de acesso, programação de horários, definição de áreas restritas, administração de dispositivos, emissão de credenciais, monitoramento remoto e geração de relatórios gerenciais. O aluno compreenderá como essas funcionalidades são utilizadas para garantir que apenas pessoas autorizadas tenham acesso aos ambientes monitorados.

Serão abordados também os mecanismos de integração entre os softwares de controle de acesso e outros sistemas de segurança, como videomonitoramento, alarmes, detecção de incêndio, portarias remotas e plataformas PSIM. Essa integração permite validar eventos automaticamente, associar imagens às tentativas de acesso, registrar evidências das ocorrências e executar respostas automáticas diante de situações previamente configuradas.

Ao final deste conteúdo, o aluno compreenderá a importância dos softwares de controle de acesso como ferramenta de gestão da segurança patrimonial, reconhecendo seu papel na prevenção de acessos não autorizados, na rastreabilidade das operações e na geração de informações estratégicas para auditorias, investigações e tomada de decisões.

outras tecnologias.

Contexto:

A constante evolução tecnológica vem ampliando significativamente as capacidades dos sistemas eletrônicos de segurança, incorporando novas soluções capazes de aumentar a eficiência operacional, reduzir custos e proporcionar respostas mais rápidas aos eventos monitorados. Além dos sistemas tradicionais de CFTV, alarmes, controle de acesso e rastreamento, diversas tecnologias complementares vêm sendo incorporadas às Centrais de Monitoramento/rastreamento, promovendo maior integração entre pessoas, processos e equipamentos.

Neste conteúdo serão apresentadas tecnologias emergentes utilizadas no setor de segurança eletrônica, incluindo computação em nuvem, Internet das Coisas (IoT), inteligência artificial, aprendizado de máquina, análise de dados, plataformas móveis, armazenamento distribuído, redes de comunicação de alta disponibilidade, sensores inteligentes, drones, robôs de

patrulhamento, dispositivos vestíveis (wearables) e soluções baseadas em computação de borda (Edge Computing). O aluno compreenderá como essas tecnologias contribuem para ampliar a capacidade de monitoramento e resposta das organizações.

Também serão discutidos aspectos relacionados à interoperabilidade entre sistemas, padronização de protocolos de comunicação, escalabilidade das soluções, continuidade operacional, cibersegurança, proteção de dados e tendências futuras da segurança eletrônica. Serão apresentados exemplos de aplicações em ambientes corporativos, cidades inteligentes, infraestrutura crítica, logística, transporte de valores, condomínios, indústrias e órgãos públicos, evidenciando os benefícios proporcionados pela transformação digital do setor.

Ao término deste conteúdo, o profissional compreenderá o impacto das novas tecnologias sobre os serviços de monitoramento eletrônico e estará apto a identificar oportunidades de inovação aplicáveis às Centrais de Monitoramento/rastreamento. Também desenvolverá uma visão sistêmica da evolução da segurança eletrônica, reconhecendo que a integração tecnológica representa um dos principais fatores para o aumento da eficiência operacional, da capacidade de prevenção e da qualidade dos serviços prestados.

Plataformas de Integração (PSIM - Physical Security Information Management): CFTV, alarmes, controle de acesso, sensores, rastreamento e comunicação em uma única central.

Contexto:

O crescimento da complexidade das operações de segurança patrimonial e logística tornou necessária a adoção de plataformas capazes de integrar diferentes sistemas tecnológicos em um único ambiente operacional. Nesse contexto, as soluções de Physical Security Information Management (PSIM) representam uma evolução significativa na gestão da segurança eletrônica, permitindo consolidar informações provenientes de múltiplos subsistemas, automatizar processos e fornecer aos operadores uma visão abrangente das ocorrências em tempo real.

Neste conteúdo serão apresentados os fundamentos das plataformas PSIM, sua arquitetura, funcionalidades e aplicações em Centros de Controle e Operações. O aluno compreenderá como essas plataformas integram sistemas de videomonitoramento, alarmes de intrusão, controle de acesso, rastreamento veicular, detecção e alarme de incêndio, automação predial, sensores perimetrais e sistemas de comunicação, centralizando o gerenciamento operacional em uma única interface. Essa integração reduz a necessidade de alternância entre diferentes softwares, aumenta a produtividade da equipe e melhora a qualidade da tomada de decisão.

Serão abordados os conceitos de interoperabilidade, integração por protocolos padronizados, gerenciamento unificado de eventos, correlação automática de informações, mapas sinóticos, georreferenciamento, dashboards operacionais, automação de fluxos de trabalho e procedimentos guiados (Standard Operating Procedures – SOP). Também serão apresentados exemplos práticos de como um único evento pode desencadear ações automáticas, como a exibição imediata de imagens, o bloqueio de acessos, o envio de notificações e a abertura de chamados para equipes externas.

Ao longo do estudo, será destacada a importância do PSIM para ambientes de alta criticidade, como instituições financeiras, centros logísticos, aeroportos, portos, indústrias, órgãos governamentais, concessionárias de infraestrutura e empresas de transporte de numerário e valores. O aluno compreenderá como essas plataformas contribuem para reduzir o tempo de resposta, aumentar a confiabilidade das operações e apoiar a gestão estratégica da segurança.

Ao final deste conteúdo, o profissional será capaz de compreender o funcionamento das plataformas de integração, reconhecer seus benefícios operacionais e identificar sua aplicação como ferramenta de apoio à coordenação das atividades desenvolvidas em Centrais de Monitoramento/rastreamento modernas.

Central de Monitoramento

Recepção e tratamento de sinais (alarme, vídeo, sensores e rastreadores em tempo real);

Contexto:

A recepção e o tratamento de sinais constituem a atividade central de qualquer Central de Monitoramento/rastreamento. Todos os eventos gerados pelos dispositivos instalados em campo são transmitidos continuamente para a central, onde são processados, classificados e apresentados aos operadores para análise e adoção das medidas previstas nos protocolos operacionais. A confiabilidade dessa etapa é determinante para a efetividade dos serviços prestados e para a mitigação dos riscos associados às ocorrências monitoradas.

Neste conteúdo serão estudados os diferentes tipos de sinais recebidos pelas plataformas de monitoramento/rastreamento, incluindo eventos provenientes de sistemas de alarme, videomonitoramento, controle de acesso, sensores ambientais, rastreamento veicular, dispositivos de telemetria e sistemas de automação. O aluno compreenderá como essas informações são codificadas, transmitidas por diferentes meios de comunicação e processadas pelos softwares de monitoramento, respeitando critérios de prioridade, criticidade e disponibilidade.

Também serão abordados os procedimentos utilizados para validação de eventos, eliminação de registros duplicados, identificação de falhas de comunicação, tratamento de alarmes técnicos e diferenciação entre eventos operacionais e ocorrências críticas. Serão apresentados conceitos relacionados à redundância de comunicação e disponibilidade dos sistemas.

Ao final deste conteúdo, o profissional compreenderá o fluxo operacional desde a geração do evento até sua apresentação ao operador, desenvolvendo competências para interpretar corretamente os sinais recebidos, reconhecer possíveis inconsistências e iniciar o atendimento das ocorrências conforme os procedimentos estabelecidos pela organização.

Identificação de situações suspeitas, intrusões, vandalismo ou ocorrências;

Contexto:

A capacidade de identificar corretamente situações suspeitas representa uma das competências mais importantes para operadores e supervisores de Centrais de Monitoramento/rastreamento. A interpretação adequada dos eventos permite diferenciar ocorrências reais de alarmes indevidos, reduzindo o tempo de resposta e aumentando a eficiência das ações de prevenção e proteção patrimonial.

Neste conteúdo serão apresentados os critérios utilizados para análise e classificação de ocorrências relacionadas a intrusões, tentativas de acesso não autorizado, vandalismo, sabotagem, violação de perímetros, movimentações atípicas, falhas operacionais, perda de comunicação, eventos técnicos e demais situações que possam representar risco à integridade das pessoas, do patrimônio ou das operações monitoradas. O aluno compreenderá a importância da análise contextual das informações, utilizando dados provenientes de diferentes sistemas para aumentar a confiabilidade da avaliação.

Serão estudadas técnicas de verificação por vídeo, correlação de eventos, confirmação por múltiplos sensores, utilização de recursos de inteligência artificial, análise de histórico operacional e aplicação de critérios objetivos para classificação das ocorrências. Também serão discutidos os fatores humanos que podem influenciar o processo decisório, destacando a necessidade de manter postura técnica, atenção concentrada e estrita observância aos procedimentos operacionais padronizados.

Ao término deste conteúdo, o aluno será capaz de reconhecer indícios de situações suspeitas, avaliar corretamente os eventos recebidos e adotar as medidas previstas nos protocolos operacionais, contribuindo para uma resposta rápida, segura e tecnicamente fundamentada.

Gestão de eventos e protocolos operacionais (alarmes, imagens suspeitas e falhas técnicas): autoriza ou bloqueia acessos em portarias virtuais e empresas, aciona o técnico externo, comunica o cliente e chama as forças de segurança pública.

Contexto:

A gestão de eventos compreende o conjunto de procedimentos adotados para controlar, registrar, acompanhar e encerrar todas as ocorrências tratadas pela Central de Monitoramento/Rastreamento. Essa atividade deve ser executada de forma padronizada, seguindo protocolos previamente definidos pela organização e alinhados às características de cada cliente, garantindo uniformidade nas decisões e rastreabilidade das ações executadas.

Neste conteúdo serão apresentados os fundamentos dos Procedimentos Operacionais Padrão (POP), das Instruções de Trabalho (IT) e dos fluxos de atendimento utilizados nas Centrais de Monitoramento/rastreamento. O aluno compreenderá como cada tipo de evento possui um protocolo específico, definindo a sequência de ações a serem executadas, os responsáveis pelo atendimento, os critérios para escalonamento das ocorrências e as condições para encerramento de cada chamado.

Serão estudadas situações que envolvem autorização e bloqueio remoto de acessos em portarias remotas, confirmação de alarmes por vídeo, despacho de equipes técnicas, comunicação com o técnico externo, contato com responsáveis cadastrados, acionamento de empresas de apoio e solicitação de atendimento às forças públicas de segurança quando confirmada a ocorrência. Também serão abordados os critérios para priorização de eventos simultâneos, gerenciamento de incidentes múltiplos e preservação das evidências digitais.

Ao final deste conteúdo, o profissional compreenderá que o cumprimento rigoroso dos protocolos operacionais é um dos principais fatores para garantir a qualidade dos serviços prestados, reduzir riscos operacionais, assegurar conformidade com as políticas da empresa e preservar a confiabilidade das informações registradas durante o atendimento das ocorrências.

Comunicação com técnico externo, clientes e forças públicas de segurança via rádio, telefone, aplicativos ou despacho online.

Contexto:

A comunicação operacional é um elemento indispensável para o funcionamento eficiente das Centrais de Monitoramento/rastreamento. A rapidez, precisão e confiabilidade na transmissão das informações influenciam diretamente a capacidade de resposta diante das ocorrências, tornando essencial a utilização de procedimentos padronizados e meios de comunicação adequados a cada situação operacional.

Neste conteúdo serão apresentados os diferentes canais utilizados para comunicação entre a Central de Monitoramento/rastreamento, equipes técnicas de manutenção, técnicos externos, gestores de segurança, clientes, empresas parceiras e órgãos públicos.

O aluno estudará técnicas de comunicação profissional, padronização da linguagem, transmissão objetiva das informações, confirmação de mensagens, registro das comunicações realizadas e procedimentos destinados a evitar ambiguidades ou interpretações equivocadas durante situações críticas. Também serão apresentados aspectos relacionados ao sigilo das informações, à proteção de dados sensíveis e à observância das políticas de confidencialidade da organização.

Ao concluir este conteúdo, o profissional estará apto a realizar comunicações operacionais de forma clara, objetiva, segura e compatível com os protocolos da Central de Monitoramento, contribuindo para a coordenação eficiente das equipes envolvidas na resposta às ocorrências.

Registro e relatório de ocorrências;

Contexto:

O registro das ocorrências representa uma das atividades mais importantes desenvolvidas em uma Central de Monitoramento/rastreamento, pois constitui a documentação oficial de todas as ações executadas durante o atendimento dos eventos. Esses registros subsidiam auditorias, análises estatísticas, investigações, avaliações de desempenho e processos judiciais, quando aplicáveis, tornando indispensável sua elaboração com precisão, clareza e objetividade.

Neste conteúdo serão apresentados os princípios técnicos aplicáveis ao registro de ocorrências, enfatizando a necessidade de documentar cronologicamente os fatos observados, os horários de cada ação, os responsáveis envolvidos, as comunicações realizadas, as decisões adotadas e os resultados obtidos durante o atendimento. O aluno compreenderá que o relatório deve refletir fielmente os acontecimentos, sem interpretações subjetivas, opiniões pessoais ou informações não verificadas.

Serão estudadas boas práticas para elaboração de registros em sistemas informatizados, utilização de linguagem técnica padronizada, preservação de evidências digitais, anexação de imagens, vídeos e demais documentos relacionados à ocorrência. Também serão abordados aspectos relacionados à rastreabilidade das informações, integridade dos registros, confidencialidade dos dados e conformidade com as políticas internas da organização e com a legislação aplicável.

Ao término deste conteúdo, o profissional compreenderá que a qualidade dos registros operacionais influencia diretamente a eficiência da gestão da segurança, a melhoria contínua dos processos e a capacidade da organização de demonstrar, de forma técnica e documental, todas as ações executadas durante o tratamento das ocorrências monitoradas.

Rastreamento de Numerário, Bens ou Valores

Acompanhamento de veículos e cargas em tempo real.

Contexto:

O acompanhamento em tempo real de veículos utilizados no transporte de numerário, bens e valores constitui uma das principais atividades desempenhadas pelas Centrais de Monitoramento/rastreamento e Gerenciamento de Riscos. Essa atividade tem como objetivo proporcionar supervisão contínua da operação logística, permitindo identificar rapidamente situações que possam representar ameaças à segurança da carga, da equipe de transporte ou do

patrimônio transportado. A utilização de tecnologias de rastreamento aumenta significativamente a capacidade de prevenção e resposta diante de eventos críticos.

Neste conteúdo serão apresentados os fundamentos do monitoramento/rastreamento em tempo real, abordando o funcionamento dos sistemas de posicionamento por satélite, das redes de comunicação de dados e das plataformas de rastreamento utilizadas para acompanhar veículos durante todo o percurso operacional. O aluno compreenderá como as informações de localização, velocidade, direção, tempo de deslocamento e status operacional são transmitidas continuamente à Central de Monitoramento/rastreamento para subsidiar a tomada de decisão.

Também serão estudadas as metodologias empregadas para acompanhamento de rotas planejadas, monitoramento de pontos de controle, identificação de atrasos operacionais, acompanhamento de entregas, supervisão de áreas de risco e gerenciamento de deslocamentos em ambientes urbanos e rodoviários. Serão apresentados conceitos relacionados ao georreferenciamento, cercas eletrônicas (geofences), mapas digitais e monitoramento simultâneo de múltiplas operações logísticas.

Ao final deste conteúdo, o aluno compreenderá a importância do acompanhamento contínuo das operações de transporte, reconhecendo como o monitoramento em tempo real contribui para reduzir riscos, aumentar a eficiência operacional e proporcionar maior segurança às atividades de transporte de numerário, bens e valores.

Integração com a gestão de riscos em operações de transporte de numerário, bens ou valores.

Contexto:

O rastreamento eletrônico representa apenas um dos componentes de um programa estruturado de gerenciamento de riscos. Para que as operações de transporte sejam executadas com elevados níveis de segurança, torna-se necessário integrar informações provenientes de diferentes tecnologias, procedimentos operacionais e análises estratégicas, permitindo que a Central de Monitoramento/rastreamento atue de forma preventiva e coordenada diante das diversas ameaças existentes.

Neste conteúdo serão apresentados os princípios da gestão de riscos aplicada às operações de transporte de numerário, bens e valores, enfatizando a identificação, análise, avaliação, tratamento e monitoramento contínuo dos riscos operacionais. O aluno compreenderá que fatores como características da carga, perfil das rotas, índices de criminalidade, horários de circulação, condições climáticas e vulnerabilidades operacionais influenciam diretamente o planejamento das medidas de proteção.

Serão estudadas as formas de integração entre plataformas de rastreamento, sistemas de comunicação, bancos de dados, softwares de rastreamento, ferramentas de inteligência e recursos de análise geoespacial. Também serão abordadas metodologias para classificação de eventos por criticidade, definição de níveis de resposta, acompanhamento de indicadores de desempenho e avaliação da efetividade dos controles implementados.

Ao término deste conteúdo, o profissional compreenderá que a gestão de riscos é um processo contínuo, baseado em informações atualizadas e na integração entre pessoas, tecnologias e procedimentos, contribuindo para a redução das perdas e para o aumento da segurança das operações monitoradas.

Geração de alertas de desvios de rota, paradas não autorizadas ou violação de compartimento de carga.

Contexto:

Os sistemas modernos de rastreamento possuem mecanismos capazes de identificar automaticamente situações que possam indicar riscos operacionais ou ações criminosas durante o transporte de numerário, bens e valores. Esses mecanismos permitem gerar alertas em tempo real sempre que determinados parâmetros previamente configurados forem ultrapassados, possibilitando que a Central de Monitoramento/rastreamento inicie imediatamente os procedimentos previstos para cada tipo de ocorrência.

Neste conteúdo serão apresentados os principais eventos monitorados pelas plataformas de rastreamento, incluindo desvios de rota, permanência excessiva em determinado local, entrada ou saída de áreas restritas, perda de comunicação, abertura não autorizada de compartimentos de carga, acionamento de botão de pânico, desligamento indevido de equipamentos, remoção de dispositivos de rastreamento e alterações inesperadas nas condições operacionais do veículo.

Serão estudados os critérios técnicos utilizados para configuração desses alertas, considerando aspectos como horários autorizados, rotas previamente aprovadas, limites de velocidade, áreas de risco, zonas de exclusão, cercas eletrônicas e regras específicas definidas pelo plano operacional de cada cliente. O aluno compreenderá a importância de calibrar corretamente esses parâmetros para reduzir alarmes desnecessários e aumentar a confiabilidade do monitoramento/rastreamento.

Ao final deste conteúdo, o profissional será capaz de compreender o funcionamento dos sistemas automáticos de geração de alertas, interpretar corretamente os eventos apresentados pelas plataformas de rastreamento e adotar as medidas previstas nos protocolos operacionais sempre que identificadas situações de risco.

Gestão de eventos e protocolos operacionais (alarmes, imagens suspeitas, perda de sinal e falhas técnicas): aciona o técnico externo, comunica o cliente e, se confirmado, chama as forças de segurança pública.

Contexto:

A resposta eficiente aos eventos gerados pelos sistemas de rastreamento depende da existência de protocolos operacionais claramente definidos, padronizados e previamente conhecidos pelos operadores da Central de Monitoramento/rastreamento. Esses protocolos estabelecem a sequência de ações que deve ser executada diante de cada tipo de ocorrência, reduzindo o tempo de resposta e garantindo uniformidade na condução dos atendimentos.

Neste conteúdo serão abordados os procedimentos aplicáveis ao tratamento de eventos como perda de sinal, violação de equipamentos, acionamento de botão de emergência, desvio de rota, abertura de compartimentos, falhas de comunicação, eventos de telemetria e demais ocorrências relacionadas às operações de transporte. O aluno compreenderá como analisar as informações recebidas, confirmar a ocorrência, registrar as evidências disponíveis e executar o fluxo operacional previsto para cada situação.

Também serão apresentados os critérios para acionamento de equipes técnicas, comunicação com gestores da operação, contato com clientes, escalonamento das ocorrências e solicitação de apoio das forças de segurança pública quando houver confirmação de ameaça à integridade das pessoas ou da carga. Serão enfatizados aspectos relacionados à preservação das evidências digitais e à documentação das decisões adotadas durante todo o atendimento.

Ao concluir este conteúdo, o profissional compreenderá que a correta aplicação dos protocolos operacionais constitui um dos principais fatores para assegurar eficiência, rastreabilidade, conformidade e qualidade na gestão das ocorrências relacionadas ao rastreamento de numerário, bens e valores.

Comunicação com técnico externo, clientes e forças públicas de segurança via rádio, telefone, aplicativos ou despacho online.

Contexto:

Durante uma ocorrência envolvendo operações de transporte, a comunicação eficiente entre a Central de Monitoramento/rastreamento e os diversos atores envolvidos é essencial para coordenar as ações de resposta e minimizar os impactos do evento. A precisão das informações transmitidas influencia diretamente a velocidade das decisões e a eficácia das medidas adotadas para proteção da carga, da equipe e do patrimônio.

Neste conteúdo serão estudados os procedimentos de comunicação entre operadores, supervisores, motoristas, técnicos externos, gestores de risco, clientes e órgãos de segurança pública. Serão apresentados os diferentes meios tecnológicos utilizados nessas comunicações, incluindo rádio digital, telefonia móvel, aplicativos corporativos, plataformas de despacho eletrônico e sistemas integrados de gerenciamento operacional.

O aluno compreenderá a importância da utilização de linguagem objetiva, padronizada e tecnicamente adequada, evitando ambiguidades que possam comprometer o atendimento da ocorrência. Também serão abordados procedimentos para confirmação das mensagens, registro das comunicações realizadas, proteção das informações sensíveis e observância das políticas de confidencialidade da organização.

Ao final deste conteúdo, o profissional estará apto a realizar comunicações operacionais de forma segura, eficiente e alinhada aos procedimentos institucionais, contribuindo para a coordenação integrada das equipes envolvidas nas operações de monitoramento e gerenciamento de riscos.

Uso da telemetria: sensores em portas de baú/cofre, alarme de pânico acionado pelo motorista, bloqueio remoto do veículo em caso de furto ou roubo, registro de paradas não autorizadas, monitoramento de condições do veículo, gestão de comportamento do condutor, localização em tempo real, histórico de rotas percorridas e alerta de desvio de rota.

Contexto:

A telemetria embarcada amplia significativamente a capacidade de monitoramento das operações de transporte ao fornecer informações detalhadas sobre o comportamento do veículo, das condições operacionais e das ações executadas durante todo o deslocamento. Diferentemente do rastreamento convencional, que informa principalmente a localização do veículo, a telemetria permite monitorar diversos parâmetros que auxiliam na prevenção de riscos, na proteção da carga e na gestão da frota.

Neste conteúdo serão apresentados os principais sensores e dispositivos utilizados em sistemas de telemetria, incluindo sensores de abertura de portas e compartimentos, sensores de ignição, botão de pânico, bloqueadores remotos, sensores de temperatura, acelerômetros, giroscópios, leitores do barramento eletrônico do veículo (CAN Bus), dispositivos de identificação do motorista e módulos de monitoramento do comportamento da condução.

Serão estudadas as informações geradas por esses equipamentos, como excesso de velocidade, frenagens bruscas, acelerações agressivas, curvas acentuadas, marcha lenta prolongada, consumo de combustível, tempo de operação, abertura de compartimentos, desligamento do rastreador, tentativas de sabotagem, desvios de rota e permanência em áreas de risco. O aluno compreenderá como essas informações contribuem para a análise preventiva dos riscos e para o aumento da eficiência operacional.

Ao término deste conteúdo, o profissional compreenderá que a telemetria constitui uma importante ferramenta de apoio à gestão operacional, permitindo que a Central de Monitoramento atue de forma preventiva, baseada em indicadores objetivos e informações atualizadas sobre toda a operação logística.

Registro e relatório de ocorrências;

Contexto:

A documentação das ocorrências relacionadas ao rastreamento de numerário, bens e valores é uma etapa indispensável para garantir rastreabilidade, transparência e confiabilidade às operações desenvolvidas pela Central de Monitoramento/rastreamento. Os registros produzidos durante o atendimento constituem evidências formais das ações executadas, servindo de apoio para auditorias, análises operacionais, investigações, processos administrativos e demandas judiciais.

Neste conteúdo serão apresentados os procedimentos para elaboração de registros técnicos completos, contemplando informações sobre horários, localização dos eventos, histórico de deslocamentos, comunicações realizadas, decisões operacionais, acionamentos efetuados, evidências coletadas e encerramento da ocorrência. O aluno compreenderá que todos os registros devem ser objetivos, precisos, cronológicos e baseados exclusivamente em fatos observáveis e verificáveis.

Também serão abordadas boas práticas para elaboração de relatórios gerenciais, consolidação de indicadores de desempenho, análise estatística de ocorrências, identificação de tendências e proposição de ações corretivas e preventivas. Será enfatizada a importância da integridade dos registros, da preservação das evidências digitais e da conformidade com os requisitos legais, regulatórios e contratuais aplicáveis ao setor de segurança privada.

Ao final deste conteúdo, o profissional estará apto a elaborar registros e relatórios técnicos que contribuam para a melhoria contínua das operações, para a avaliação dos processos de gerenciamento de riscos e para a produção de informações confiáveis destinadas ao apoio das decisões operacionais e estratégicas da organização.

Técnicas de Elaboração de Relatórios

Objetivo

Dotar o aluno de conhecimento sobre as técnicas de elaboração de relatórios.

Conteúdo programático

Relatório Técnico

Conceito.

Contexto:

O relatório técnico é um documento formal destinado ao registro sistemático de informações relativas a atividades, ocorrências, inspeções, análises ou eventos operacionais. Nas Centrais de Monitoramento/rastreamento, esse documento representa o principal instrumento de comunicação entre operadores, supervisores, gestores, clientes e demais partes interessadas, permitindo registrar de forma organizada todas as ações executadas durante o atendimento das ocorrências. Sua correta elaboração assegura que as informações sejam preservadas de maneira íntegra, possibilitando consultas futuras e subsidiando processos decisórios.

Durante este conteúdo serão apresentados os conceitos fundamentais relacionados aos relatórios técnicos, destacando suas características, finalidades e aplicações no contexto da segurança eletrônica. O aluno compreenderá que o relatório deve ser elaborado com base em fatos objetivos e verificáveis, utilizando linguagem técnica, impessoal e precisa, evitando interpretações subjetivas, opiniões pessoais ou informações não confirmadas.

Também será enfatizada a diferença entre registros operacionais, anotações de atendimento, comunicados internos e relatórios técnicos, demonstrando que cada documento possui objetivos específicos dentro da rotina operacional da Central de Monitoramento. Serão apresentados exemplos de situações em que o relatório técnico se torna indispensável para documentar eventos relevantes, comprovar procedimentos executados e preservar evidências relacionadas às ocorrências atendidas.

Ao final deste conteúdo, o aluno compreenderá o papel do relatório técnico como instrumento essencial para a gestão da segurança, reconhecendo sua importância para a rastreabilidade das operações, a transparência das atividades desenvolvidas e a produção de informações confiáveis que apoiem a tomada de decisões estratégicas e operacionais.

Estrutura conforme a Associação de Normas Técnicas (ABNT) para a elaboração de relatório técnico.

Contexto:

A padronização documental constitui um requisito fundamental para garantir qualidade, uniformidade e confiabilidade na produção de documentos técnicos. A utilização das diretrizes estabelecidas pela Associação Brasileira de Normas Técnicas (ABNT) contribui para que os relatórios apresentem organização lógica, clareza na exposição das informações e facilidade de interpretação pelos diferentes públicos envolvidos nas operações de segurança.

Neste conteúdo serão apresentados os princípios gerais aplicáveis à elaboração de relatórios técnicos conforme as normas da ABNT, abordando aspectos relacionados à estrutura documental, identificação do documento, organização do conteúdo, apresentação das informações e utilização de linguagem técnica adequada. Embora as empresas possam adotar modelos próprios, a observância dessas diretrizes promove maior padronização e profissionalismo na documentação produzida.

Serão estudados os principais elementos estruturais de um relatório técnico, incluindo identificação da ocorrência, objetivo do documento, contextualização dos fatos, descrição cronológica dos eventos, procedimentos executados, recursos utilizados, resultados obtidos, conclusão e recomendações, quando aplicáveis. Também serão abordados aspectos relacionados à identificação do responsável pela elaboração, controle de versões, anexação de evidências digitais e procedimentos de arquivamento.

Ao término deste conteúdo, o aluno compreenderá a importância da padronização documental para a gestão da qualidade, reconhecendo que a adoção de estruturas organizadas facilita a

comunicação entre equipes, melhora a rastreabilidade das informações e fortalece a credibilidade dos documentos produzidos pela Central de Monitoramento.

Objetivos: relatar ocorrências, vulnerabilidades, status de equipamentos e outros.

Contexto:

Os relatórios técnicos produzidos em uma Central de Monitoramento/rastreamento possuem diferentes finalidades, todas voltadas à documentação de informações relevantes para a continuidade das operações, para a gestão dos riscos e para a melhoria contínua dos serviços prestados. A definição clara do objetivo do relatório orienta sua estrutura, o nível de detalhamento necessário e o público ao qual se destina.

Neste conteúdo serão abordadas as diversas aplicações dos relatórios técnicos no contexto da segurança eletrônica, incluindo o registro de ocorrências operacionais, falhas de equipamentos, indisponibilidade de sistemas, vulnerabilidades identificadas, acionamentos de equipes externas, atendimentos técnicos, inspeções, auditorias, testes operacionais e demais situações relevantes para a gestão da segurança.

O aluno compreenderá que um relatório bem elaborado não se limita à descrição dos fatos, mas fornece informações suficientes para permitir a análise das causas, a avaliação dos impactos e a definição de ações corretivas ou preventivas. Também será enfatizada a necessidade de registrar informações objetivas, consistentes e verificáveis, assegurando que o documento possa servir como fonte confiável para consultas futuras.

Ao final deste conteúdo, o profissional compreenderá que os relatórios técnicos representam instrumentos de gestão indispensáveis para acompanhar o desempenho operacional, identificar oportunidades de melhoria e apoiar decisões relacionadas à manutenção da segurança, da disponibilidade dos sistemas e da qualidade dos serviços prestados.

Tipos de relatórios (de serviço, de qualidade, de não conformidade, de manutenção, de ocorrências e outros).

Contexto:

As atividades desenvolvidas pelas Centrais de Monitoramento/rastreamento geram informações de diferentes naturezas, exigindo a elaboração de relatórios específicos para cada finalidade. A correta classificação desses documentos permite organizar as informações produzidas pela organização, facilitando seu gerenciamento, arquivamento e utilização em processos operacionais, administrativos e estratégicos.

Neste conteúdo serão apresentados os principais tipos de relatórios utilizados no setor de segurança eletrônica, incluindo relatórios de ocorrência, atendimento operacional, manutenção preventiva e corretiva, inspeção técnica, auditoria, não conformidade, desempenho operacional, qualidade dos serviços, disponibilidade dos sistemas, atendimento ao cliente, gerenciamento de riscos e análise estatística de eventos.

Serão discutidas as características específicas de cada modalidade documental, destacando os objetivos, o público destinatário, o nível de detalhamento exigido e os critérios técnicos para sua elaboração. O aluno compreenderá que cada tipo de relatório atende a necessidades distintas, devendo conter informações compatíveis com sua finalidade e obedecer aos procedimentos internos estabelecidos pela organização.

Ao concluir este conteúdo, o profissional será capaz de identificar o tipo de relatório mais adequado para cada situação operacional, compreendendo sua importância para a gestão da segurança, para o controle da qualidade e para a melhoria contínua dos processos desenvolvidos pela Central de Monitoramento.

Recomendações: ações corretivas, ações preventivas e melhorias.

Contexto:

Além de registrar fatos e descrever ocorrências, os relatórios técnicos podem constituir importantes instrumentos para a melhoria contínua dos processos organizacionais. A análise das informações registradas permite identificar causas de falhas, recorrência de eventos, vulnerabilidades operacionais e oportunidades de aperfeiçoamento dos sistemas e procedimentos adotados pela organização.

Neste conteúdo serão apresentados os conceitos de ações corretivas, ações preventivas e ações de melhoria contínua, demonstrando como essas iniciativas contribuem para reduzir a probabilidade de recorrência das ocorrências e aumentar a eficiência operacional das Centrais de Monitoramento/rastreamento. O aluno compreenderá que as recomendações técnicas devem ser fundamentadas em evidências objetivas e alinhadas às políticas e procedimentos institucionais.

Também serão abordados critérios para elaboração de recomendações claras, viáveis e tecnicamente justificadas, contemplando aspectos relacionados à atualização de procedimentos operacionais, capacitação das equipes, manutenção de equipamentos, aperfeiçoamento tecnológico, revisão de protocolos e fortalecimento dos controles internos. Será enfatizada a importância de distinguir fatos observados das propostas de melhoria, preservando a objetividade do documento.

Ao final deste conteúdo, o profissional compreenderá como a elaboração de recomendações técnicas contribui para a evolução dos processos organizacionais, fortalecendo a cultura da qualidade, da prevenção de riscos e da melhoria contínua nas operações de monitoramento eletrônico.

Modelos de Relatórios Técnicos.

Contexto:

A utilização de modelos padronizados de relatórios constitui uma prática consolidada nos sistemas de gestão da qualidade e nas organizações que atuam com segurança eletrônica. A padronização facilita o preenchimento das informações, reduz inconsistências, melhora a qualidade dos registros e assegura que todos os dados necessários sejam devidamente documentados durante as atividades operacionais.

Neste conteúdo serão apresentados diferentes modelos de relatórios técnicos utilizados em Centrais de Monitoramento/rastreamento, contemplando documentos destinados ao registro de ocorrências, atendimento de alarmes, videomonitoramento, controle de acesso, rastreamento veicular, atendimento técnico, inspeções, auditorias e demais atividades relacionadas à gestão da segurança eletrônica. O aluno compreenderá a estrutura desses documentos e os critérios para seu correto preenchimento.

Serão desenvolvidas atividades práticas de elaboração e análise de relatórios, permitindo que os participantes exercitem a organização lógica das informações, a utilização de linguagem técnica adequada e o correto registro cronológico das ações executadas. Também serão abordados

aspectos relacionados ao uso de formulários eletrônicos, sistemas informatizados de registro e integração das informações com plataformas de gestão operacional.

Ao término deste conteúdo, o aluno estará apto a elaborar relatórios técnicos completos, claros, objetivos e padronizados, compatíveis com as exigências operacionais das Centrais de Monitoramento/rastreamento e com as boas práticas de gestão documental adotadas pelas organizações do setor de segurança privada.

Gerenciamento de crises (GEC)

Objetivo

Desenvolver conhecimentos sobre gerenciamento de crise.

Conteúdo Programático

Identificação de emergências, crises, ou qualquer evento crítico:

Contexto:

A identificação precoce de uma emergência ou de um evento crítico constitui uma das principais responsabilidades do operador da Central de Monitoramento. A correta interpretação das informações recebidas permite avaliar a gravidade da ocorrência e iniciar rapidamente os procedimentos operacionais previstos para cada situação.

Neste conteúdo serão apresentados os critérios para reconhecimento de eventos críticos, utilizando informações provenientes de sistemas de alarme, videomonitoramento, controle de acesso, rastreamento e demais recursos tecnológicos disponíveis. Também serão abordados os fatores que auxiliam na diferenciação entre eventos rotineiros e situações que exigem resposta imediata.

Ao final deste conteúdo, o aluno compreenderá como identificar ocorrências críticas e classificá-las de acordo com os protocolos operacionais da Central de Monitoramento.

medidas imediatas e mediatas;

Contexto:

Após a confirmação de uma situação crítica, as ações executadas pela Central de Monitoramento devem obedecer a uma sequência previamente estabelecida, diferenciando as medidas que precisam ser adotadas imediatamente daquelas executadas durante o desenvolvimento da ocorrência.

Neste conteúdo serão apresentados os procedimentos iniciais de atendimento, comunicação, registro, acionamento de recursos e acompanhamento da ocorrência, bem como as ações posteriores destinadas ao controle da situação, restabelecimento das operações e documentação dos fatos ocorridos.

Ao final deste conteúdo, o profissional compreenderá a importância da correta sequência das ações para reduzir riscos e aumentar a eficiência da resposta operacional.

critérios de ação no gerenciamento de crises;

Contexto:

As decisões adotadas durante uma crise devem basear-se em critérios técnicos previamente definidos pela organização, evitando improvisações e garantindo uniformidade na condução das ocorrências. Esses critérios orientam a priorização dos eventos, o acionamento dos recursos disponíveis e a definição das medidas de resposta.

Neste conteúdo serão estudados os fatores utilizados para apoiar a tomada de decisão, considerando o nível de risco, o impacto potencial da ocorrência, a disponibilidade de recursos e os procedimentos operacionais padronizados estabelecidos pela Central de Monitoramento.

Ao final deste conteúdo, o aluno compreenderá como aplicar critérios técnicos na condução de situações críticas, assegurando respostas consistentes e alinhadas aos protocolos institucionais.

objetivos do gerenciamento de crises;

Contexto:

O gerenciamento de crises tem como finalidade reduzir os impactos provocados por eventos críticos, preservar vidas, proteger o patrimônio, manter a continuidade operacional e restabelecer a normalidade das atividades no menor tempo possível.

Neste conteúdo serão apresentados os objetivos do gerenciamento de crises aplicados às operações de monitoramento eletrônico, destacando a importância do planejamento, da coordenação das equipes, da comunicação eficiente e da adoção de procedimentos previamente definidos para cada tipo de ocorrência.

Ao término deste conteúdo, o aluno compreenderá que todas as ações desenvolvidas durante uma crise devem estar orientadas para a proteção das pessoas, dos ativos e da continuidade dos serviços.

classificação dos graus de risco ou ameaça;

Contexto:

A classificação do grau de risco permite estabelecer a prioridade de atendimento das ocorrências e definir o nível de resposta necessário para cada situação. Esse processo contribui para a utilização eficiente dos recursos disponíveis e para a adoção de medidas compatíveis com a gravidade do evento.

Neste conteúdo serão apresentados os critérios utilizados para classificação dos níveis de risco, considerando fatores como probabilidade de ocorrência, impacto operacional, vulnerabilidade dos ativos protegidos e potencial de agravamento da situação.

Ao final deste conteúdo, o profissional compreenderá como a classificação adequada dos riscos auxilia na gestão das ocorrências e na tomada de decisões durante situações críticas.

níveis de resposta e fatores que influenciam na classificação de eventos críticos e na gradação de sua periculosidade;

Contexto:

Nem todas as ocorrências exigem o mesmo nível de resposta operacional. A definição da intensidade das ações depende da análise das características do evento, dos riscos envolvidos e das informações disponíveis no momento do atendimento.

Neste conteúdo serão estudados os diferentes níveis de resposta utilizados nas Centrais de Monitoramento/rastreamento, bem como os fatores que influenciam a classificação dos eventos críticos, incluindo localização, tipo de ameaça, pessoas envolvidas, impacto potencial, disponibilidade de recursos e evolução da ocorrência.

Ao término deste conteúdo, o aluno compreenderá como adequar a resposta operacional ao grau de criticidade de cada evento, observando os procedimentos estabelecidos pela organização.

autoridades locais que devam ser imediatamente comunicadas;

Contexto:

Determinadas ocorrências exigem a comunicação imediata às autoridades competentes, conforme a natureza do evento, os protocolos da organização e a legislação aplicável. Essa comunicação deve ocorrer de forma rápida, objetiva e baseada em informações confirmadas pela Central de Monitoramento.

Neste conteúdo serão apresentados os critérios para acionamento dos órgãos públicos competentes, incluindo forças policiais, serviços de emergência, defesa civil, corpo de bombeiros e demais instituições responsáveis pelo atendimento das diferentes categorias de ocorrência. Também serão abordados os procedimentos para registro das comunicações realizadas.

Ao final deste conteúdo, o profissional compreenderá a importância do correto acionamento das autoridades competentes como parte integrante do gerenciamento de crises e da resposta coordenada às ocorrências críticas.

Cibersegurança e Inteligência Artificial (CIA)

Objetivo

Dotar o aluno de conhecimentos para utilizar cibersegurança e inteligência artificial nos serviços de monitoramento de sistemas eletrônicos de segurança e no rastreamento de numerário, bens ou valores.

Conteúdo programático

Fundamentos de cibersegurança em segurança privada:

Conceitos de segurança cibernética e sua importância;

Contexto:

A crescente digitalização dos sistemas eletrônicos de segurança transformou as Centrais de Monitoramento/rastreamento em ambientes altamente dependentes de redes de computadores, serviços em nuvem, dispositivos conectados e plataformas de gerenciamento integradas. Embora essa evolução tecnológica tenha proporcionado maior eficiência operacional, também ampliou significativamente a superfície de exposição a ameaças cibernéticas, tornando a cibersegurança um componente essencial para a continuidade das operações.

Neste conteúdo serão apresentados os conceitos fundamentais de segurança cibernética, destacando sua aplicação no contexto da segurança privada. O aluno compreenderá que a cibersegurança compreende o conjunto de políticas, processos, tecnologias e controles destinados a proteger sistemas, equipamentos, redes, aplicações e informações contra acessos

não autorizados, alterações indevidas, indisponibilidade dos serviços e outras formas de comprometimento dos ativos digitais.

Serão abordados os princípios da gestão de riscos cibernéticos, enfatizando que a proteção dos sistemas de monitoramento não depende exclusivamente de soluções tecnológicas, mas também da adoção de boas práticas operacionais, capacitação contínua dos profissionais e observância rigorosa das políticas de segurança da informação estabelecidas pela organização.

Ao término deste conteúdo, o aluno compreenderá que a cibersegurança constitui um elemento indispensável para garantir a confiabilidade dos sistemas eletrônicos de segurança, assegurando que as informações tratadas pela Central de Monitoramento permaneçam protegidas durante todo o seu ciclo de vida.

Principais ameaças digitais a serviços de segurança privada.

Contexto:

As organizações que atuam no segmento da segurança privada administram diariamente informações estratégicas relacionadas a clientes, imagens de videomonitoramento, registros de controle de acesso, dados de rastreamento, plantas de instalações, protocolos operacionais e outros ativos de elevado valor. Em razão dessa característica, tornam-se alvos potenciais de ataques cibernéticos que podem comprometer a disponibilidade dos serviços e a integridade das operações.

Neste conteúdo serão estudadas as principais ameaças digitais que afetam sistemas de segurança eletrônica, incluindo malware, ransomware, phishing, engenharia social, ataques de negação de serviço (DDoS), exploração de vulnerabilidades, roubo de credenciais, invasão de redes, comprometimento de dispositivos IoT, ataques a câmeras IP e tentativas de acesso não autorizado às plataformas de monitoramento.

Também serão apresentados exemplos de incidentes envolvendo sistemas de videomonitoramento, controle de acesso, automação predial e rastreamento, demonstrando como falhas de configuração, utilização de senhas fracas, softwares desatualizados e ausência de políticas de segurança podem comprometer toda a infraestrutura tecnológica da organização.

Ao final deste conteúdo, o profissional será capaz de reconhecer as principais ameaças cibernéticas aplicáveis ao setor de segurança eletrônica, compreendendo a importância da prevenção, da detecção precoce e da adoção de medidas de proteção compatíveis com os riscos existentes.

Proteção de dados e privacidade em sistemas de segurança:

Legislação aplicável à proteção de dados (LGPD);

Contexto:

As atividades desenvolvidas pelas Centrais de Monitoramento/rastreamento envolvem o tratamento contínuo de dados pessoais, imagens, registros biométricos, informações de localização e diversos outros dados capazes de identificar pessoas físicas. Em razão disso, as organizações do setor devem observar rigorosamente a legislação brasileira referente à proteção de dados pessoais, garantindo que suas operações sejam conduzidas de forma ética, transparente e compatível com os direitos fundamentais dos titulares das informações.

Neste conteúdo serão apresentados os fundamentos da Lei Geral de Proteção de Dados Pessoais (LGPD), abordando seus princípios, objetivos e impactos sobre os serviços de monitoramento

eletrônico. O aluno compreenderá conceitos como dado pessoal, dado pessoal sensível, tratamento de dados, controlador, operador, encarregado pelo tratamento de dados e bases legais que autorizam o processamento das informações.

Serão discutidas as responsabilidades das empresas de segurança privada na coleta, armazenamento, compartilhamento, utilização e descarte de dados pessoais, bem como os cuidados necessários para preservar a privacidade dos clientes, colaboradores e demais indivíduos cujas informações sejam tratadas pelos sistemas eletrônicos de segurança. Também serão abordadas as consequências administrativas, civis e reputacionais decorrentes do tratamento inadequado dessas informações.

Ao término deste conteúdo, o aluno compreenderá a importância da conformidade com a LGPD como requisito indispensável para a atuação profissional em Centrais de Monitoramento/rastreamento, reconhecendo que a proteção de dados constitui parte integrante da gestão da segurança das organizações.

Sistemas de Gestão da Segurança da Informação (SGSI);

Contexto:

A proteção das informações exige a adoção de processos estruturados capazes de identificar riscos, implementar controles, monitorar resultados e promover a melhoria contínua das práticas de segurança. Nesse contexto, os Sistemas de Gestão da Segurança da Informação (SGSI) representam um conjunto organizado de políticas, procedimentos, recursos tecnológicos e responsabilidades voltados à proteção dos ativos informacionais das organizações.

Neste conteúdo serão apresentados os fundamentos de um SGSI, destacando seus objetivos, estrutura e benefícios para empresas que operam Centrais de Monitoramento/rastreamento. O aluno compreenderá que um sistema de gestão permite estabelecer diretrizes claras para classificação das informações, controle de acessos, gestão de ativos, tratamento de incidentes, continuidade de negócios e conscientização dos colaboradores.

Também serão discutidos conceitos relacionados à análise de riscos, inventário de ativos, políticas de segurança, auditorias internas, monitoramento de conformidade e melhoria contínua dos controles implantados. Serão apresentados exemplos de aplicação desses princípios em ambientes de videomonitoramento, controle de acesso, rastreamento e gerenciamento integrado da segurança.

Ao concluir este conteúdo, o profissional compreenderá como um SGSI contribui para fortalecer a governança da segurança da informação, reduzir vulnerabilidades e aumentar a confiabilidade dos serviços prestados pelas organizações do setor de segurança privada.

Métodos de criptografia e controle de acesso digital.

Contexto:

A proteção das informações armazenadas e transmitidas pelos sistemas eletrônicos de segurança depende da adoção de mecanismos capazes de impedir acessos não autorizados e preservar a confidencialidade dos dados. Entre esses mecanismos destacam-se as técnicas de criptografia e os controles de autenticação, que constituem elementos essenciais da arquitetura de segurança das plataformas utilizadas nas Centrais de Monitoramento/rastreamento.

Neste conteúdo serão apresentados os conceitos fundamentais de criptografia, certificados digitais, autenticação multifator, gerenciamento de identidades, controle de privilégios, políticas

de senhas, segregação de funções e registro de auditoria. O aluno compreenderá como essas tecnologias protegem as comunicações entre equipamentos, usuários e servidores, reduzindo a possibilidade de interceptação, alteração ou utilização indevida das informações.

Serão abordadas boas práticas para administração de contas de usuários, definição de perfis de acesso, gestão de credenciais privilegiadas, utilização de autenticação forte e monitoramento das atividades executadas pelos operadores. Também será enfatizada a importância da revisão periódica dos acessos concedidos e da adoção do princípio do menor privilégio como medida preventiva contra incidentes de segurança.

Ao término deste conteúdo, o profissional compreenderá como os mecanismos de criptografia e controle de acesso contribuem para proteger os ativos digitais da organização, preservando a confidencialidade, a integridade e a disponibilidade das informações tratadas pela Central de Monitoramento.

Cibersegurança em centros de controle e monitoramento:

Boas práticas para proteção de infraestruturas críticas;

Contexto:

As Centrais de Monitoramento/rastreamento frequentemente integram sistemas responsáveis pela proteção de instalações estratégicas, infraestruturas críticas e operações essenciais para organizações públicas e privadas. A indisponibilidade desses sistemas pode gerar impactos significativos sobre a segurança patrimonial, a continuidade operacional e a prestação de serviços essenciais, exigindo a adoção de medidas rigorosas de proteção cibernética.

Neste conteúdo serão apresentadas as principais boas práticas para proteção das infraestruturas tecnológicas utilizadas em Centros de Controle e Monitoramento. O aluno compreenderá a importância da segmentação de redes, atualização periódica de softwares, gestão de vulnerabilidades, utilização de antivírus corporativos, monitoramento contínuo, backups seguros, redundância de equipamentos e planos de continuidade de negócios.

Também serão discutidos aspectos relacionados à segurança física dos ambientes tecnológicos, controle de acesso às salas de servidores, proteção das estações de trabalho, monitoramento de dispositivos conectados e adoção de políticas de resposta rápida diante da identificação de vulnerabilidades ou incidentes.

Ao final deste conteúdo, o profissional compreenderá que a proteção das infraestruturas críticas depende da integração entre controles físicos, tecnológicos e administrativos, contribuindo para garantir a disponibilidade contínua dos serviços de monitoramento.

Procedimentos para responder a incidentes cibernéticos.

Contexto:

Mesmo em ambientes protegidos por múltiplas camadas de segurança, a possibilidade de ocorrência de incidentes cibernéticos nunca pode ser totalmente eliminada. Dessa forma, torna-se indispensável que as organizações possuam procedimentos estruturados para identificar, conter, tratar, registrar e recuperar-se rapidamente desses eventos, reduzindo seus impactos operacionais.

Neste conteúdo serão apresentados os fundamentos da resposta a incidentes cibernéticos, contemplando as etapas de preparação, identificação, contenção, erradicação, recuperação e análise pós-incidente. O aluno compreenderá como os operadores da Central de Monitoramento

participam desse processo, identificando comportamentos anormais dos sistemas, comunicando rapidamente os responsáveis e seguindo rigorosamente os procedimentos definidos pela organização.

Serão abordados exemplos de incidentes envolvendo indisponibilidade de sistemas, comprometimento de credenciais, infecção por malware, falhas em servidores, ataques a dispositivos de segurança eletrônica e interrupções de comunicação. Também serão discutidos os procedimentos para preservação de evidências digitais e registro das ações executadas durante o tratamento do incidente.

Ao término deste conteúdo, o profissional compreenderá que a resposta eficiente aos incidentes depende da atuação coordenada entre equipes técnicas, gestores, operadores e demais áreas envolvidas na proteção da infraestrutura tecnológica da organização.

Confidencialidade, integridade e disponibilidade das informações.

Contexto:

A proteção das informações baseia-se em três princípios fundamentais universalmente reconhecidos pela segurança da informação: confidencialidade, integridade e disponibilidade, frequentemente denominados como a "Tríade CID". Esses princípios orientam o desenvolvimento de políticas, controles e procedimentos destinados a assegurar que as informações permaneçam protegidas durante todo o seu ciclo de vida.

Neste conteúdo serão apresentados os conceitos de confidencialidade, integridade e disponibilidade, demonstrando sua aplicação prática nas operações de monitoramento eletrônico, videomonitoramento, controle de acesso e rastreamento. O aluno compreenderá que a confidencialidade visa impedir o acesso não autorizado às informações; a integridade assegura que os dados permaneçam completos e livres de alterações indevidas; e a disponibilidade garante que os sistemas e informações estejam acessíveis sempre que necessários às operações.

Também serão estudadas medidas técnicas e administrativas utilizadas para preservar esses princípios, incluindo controles de acesso, criptografia, backups, redundância, monitoramento contínuo, gestão de mudanças, registros de auditoria e políticas de continuidade de negócios. Serão apresentados exemplos práticos de como falhas em qualquer um desses pilares podem comprometer a segurança das operações e gerar impactos significativos para clientes e organizações.

Ao final deste conteúdo, o profissional compreenderá que a observância da Tríade CID constitui um dos fundamentos da segurança da informação e um requisito indispensável para garantir a confiabilidade, a continuidade e a credibilidade dos serviços prestados pelas Centrais de Monitoramento/rastreamento.

Uso de inteligência artificial em segurança privada:

Aplicações de IA em monitoramento e análise de riscos;

Contexto:

A Inteligência Artificial (IA) tem ampliado significativamente a capacidade dos sistemas eletrônicos de segurança ao permitir a análise automatizada de grandes volumes de dados e a identificação de padrões que auxiliam na prevenção e resposta a incidentes. Sua aplicação contribui para aumentar a eficiência operacional das Centrais de Monitoramento/rastreamento e apoiar a tomada de decisões baseada em informações em tempo real.

Neste conteúdo serão apresentados os principais conceitos relacionados ao emprego da IA no monitoramento eletrônico, abordando sua utilização na análise de riscos, detecção de anomalias, priorização de eventos e apoio à gestão operacional. Também serão discutidos os benefícios, limitações e boas práticas para utilização dessas tecnologias em ambientes de segurança privada.

Ao final deste conteúdo, o aluno compreenderá como a Inteligência Artificial pode contribuir para aumentar a confiabilidade das operações e otimizar os processos de monitoramento eletrônico.

Reconhecimento facial, análise de comportamento e automação.

Contexto:

As tecnologias de reconhecimento facial e análise comportamental utilizam algoritmos de Inteligência Artificial para identificar pessoas, reconhecer padrões de movimentação e detectar comportamentos que possam representar situações de risco. Esses recursos ampliam a capacidade dos sistemas eletrônicos de segurança na prevenção de incidentes e no apoio às atividades de monitoramento.

Neste conteúdo serão apresentados os fundamentos do reconhecimento facial, da análise inteligente de comportamento e dos processos de automação associados aos sistemas de videomonitoramento. Também serão abordados aspectos relacionados à precisão das tecnologias, aos critérios para sua utilização e às limitações operacionais e legais aplicáveis ao tratamento de dados e imagens.

Ao final deste conteúdo, o aluno compreenderá as aplicações dessas soluções na segurança eletrônica e sua importância como ferramentas de apoio às atividades de monitoramento e gerenciamento de riscos.

Integração de IA com sistemas de monitoramento eletrônico:

Contexto:

A integração da Inteligência Artificial com os sistemas eletrônicos de segurança permite ampliar a capacidade de análise das informações provenientes de câmeras, alarmes, controle de acesso, rastreamento e demais dispositivos conectados às Centrais de Monitoramento/rastreamento. Essa integração favorece uma visão mais abrangente das operações e melhora a eficiência dos processos de resposta às ocorrências.

Neste conteúdo serão apresentados os princípios de integração entre plataformas de monitoramento eletrônico e soluções baseadas em Inteligência Artificial, abordando o compartilhamento de informações, a interoperabilidade entre sistemas e o apoio à tomada de decisões operacionais. Também serão discutidos os requisitos básicos para implementação dessas tecnologias em ambientes de segurança.

Ao término deste conteúdo, o profissional compreenderá como a integração entre diferentes sistemas contribui para o fortalecimento da gestão operacional e para o aumento da capacidade de prevenção e resposta a incidentes.

Processamento de imagens em tempo real;

Contexto:

O processamento de imagens em tempo real permite que sistemas inteligentes analisem continuamente os fluxos de vídeo captados pelas câmeras, identificando automaticamente eventos previamente configurados e reduzindo a necessidade de monitoramento exclusivamente manual. Essa tecnologia aumenta a velocidade de detecção de ocorrências e auxilia na priorização dos eventos relevantes.

Neste conteúdo serão apresentados os conceitos fundamentais do processamento inteligente de imagens, incluindo detecção de objetos, cruzamento de linhas virtuais, reconhecimento de movimentos, classificação de eventos e geração automática de notificações. Também serão abordados fatores que influenciam a qualidade das análises, como iluminação, posicionamento das câmeras e condições ambientais.

Ao final deste conteúdo, o aluno compreenderá como o processamento de imagens em tempo real contribui para tornar as operações de monitoramento mais eficientes, precisas e proativas.

Automação de alertas e respostas a incidentes.

Contexto:

A automação de alertas permite que os sistemas eletrônicos de segurança executem ações previamente programadas quando determinados eventos são identificados, reduzindo o tempo de resposta e aumentando a padronização dos procedimentos operacionais. Essa capacidade representa um importante recurso para as Centrais de Monitoramento/rastreamento modernas.

Neste conteúdo serão apresentados os princípios da automação aplicada à segurança eletrônica, contemplando a geração automática de alertas, acionamento de dispositivos, notificações aos operadores, integração com plataformas de monitoramento e execução de fluxos operacionais previamente definidos. Também serão discutidos os critérios para configuração dessas rotinas e os cuidados necessários para minimizar falsos alarmes e garantir a confiabilidade das respostas automáticas.

Ao término deste conteúdo, o profissional compreenderá como a automação pode apoiar as equipes de monitoramento, proporcionando maior agilidade na gestão das ocorrências e contribuindo para a eficiência dos sistemas eletrônicos de segurança.

QUALIDADE DE VIDA NO TRABALHO (QVT)

Objetivo da Disciplina

Desenvolver nos profissionais de segurança privada a consciência da importância da prática contínua de atividades físicas e da adoção de hábitos saudáveis, promovendo saúde, qualidade de vida, bem-estar físico, psicológico e social, além de contribuir para um melhor desempenho das atividades profissionais.

1. Qualidade de Vida e Saúde no Trabalho

Qualidade de vida é o equilíbrio entre saúde física, mental e social. Para o profissional de segurança privada, significa estar preparado para enfrentar longas jornadas, situações de risco e momentos de pressão emocional.

Ter qualidade de vida envolve:

Dormir adequadamente;

Alimentar-se de forma equilibrada;

Praticar exercícios físicos regularmente;

Controlar o estresse;

Reservar momentos para lazer e convivência familiar.

Exemplo prático

Um profissional que trabalha 12 horas em um posto de serviço e não pratica atividade física tende a sentir mais dores musculares, fadiga e dificuldade de concentração. Já aquele que realiza caminhadas, musculação ou outro exercício regularmente apresenta melhor disposição e menor risco de adoecimento.

2. Exercício Físico: Um Aliado da Segurança

A atividade física melhora o desempenho profissional, aumenta a capacidade de reação e reduz o risco de lesões durante a execução das atividades.

Principais benefícios

- Aumento da força muscular;
 - Melhora da resistência física;
 - Maior flexibilidade;
 - Melhor capacidade cardiorrespiratória;
 - Redução da ansiedade e do estresse;
-
- Melhora da autoestima.

Exemplos de atividades

- Caminhada;
- Corrida;
- Musculação;
- Ciclismo;
- Natação;
- Alongamentos diários.

O ideal é praticar exercícios pelo menos 150 minutos por semana, respeitando sempre os limites individuais.

3. Os Riscos do Sedentarismo

Sedentarismo é a ausência ou insuficiência de atividade física.

Pessoas sedentárias apresentam maior probabilidade de desenvolver:

- Hipertensão arterial;
- Diabetes;
- Obesidade;
- Colesterol elevado;
- Doenças cardiovasculares;
- Dores na coluna e articulações;
- Redução da resistência física.

Exemplo prático

Um profissional que permanece muitas horas sentado na central de monitoramento pode desenvolver dores lombares e problemas circulatórios. **Importante:** Pequenas pausas para caminhar e alongar-se já ajudam a reduzir esses riscos.

4. Alimentação Saudável

Uma alimentação equilibrada fornece energia para o trabalho e auxilia na recuperação muscular após os exercícios.

Recomendações

- Consumir frutas, verduras e legumes diariamente;
- Dar preferência a carnes magras;
- Beber entre 2 e 3 litros de água por dia;
- Evitar excesso de refrigerantes, frituras e alimentos ultraprocessados;
- Não permanecer muitas horas sem se alimentar.

Exemplo prático

Durante um plantão de 12 horas, substituir salgados e refrigerantes por frutas, sanduíches naturais e água melhora a disposição e reduz a sensação de cansaço.

5. Frequência Cardíaca e Índice de Massa Corporal (IMC)

Frequência Cardíaca

A frequência cardíaca corresponde ao número de batimentos do coração por minuto.

Ela aumenta durante a atividade física e diminui quando o corpo está em repouso.

Como medir:

Localize o pulso no punho ou pescoço;

Conte os batimentos durante 15 segundos;

Multiplique o resultado por quatro.

Exemplo

20 batimentos em 15 segundos = 80 batimentos por minuto (bpm).

Esse controle ajuda a verificar se o treinamento está sendo realizado de forma segura.

Índice de Massa Corporal (IMC)

O IMC é um indicador utilizado para relacionar peso e altura.

Fórmula:

$$\text{IMC} = \text{Peso (kg)} \div \text{Altura}^2 \text{ (m)}$$

Exemplo

Peso: 80 kg

Altura: 1,75 m

$$\text{IMC} = 80 \div (1,75 \times 1,75)$$

$$\text{IMC} = 26,1$$

Esse resultado indica necessidade de atenção ao peso corporal, associado sempre à avaliação de um profissional de saúde.

6. Orientações para um Treinamento Seguro

Antes de iniciar qualquer atividade física:

Faça aquecimento de 5 a 10 minutos;

Utilize roupas e calçados adequados;

Respeite seus limites;

Mantenha boa hidratação;

Alongue-se ao término da atividade.

Um treinamento completo deve trabalhar:

Resistência cardiovascular;

Força muscular;

Flexibilidade;

Coordenação motora;

Equilíbrio.

Exemplo prático

Um profissional pode organizar sua semana da seguinte forma:

Segunda: caminhada de 40 minutos;

Quarta: musculação;

Sexta: corrida leve ou bicicleta;

Diariamente: alongamentos de 10 minutos.

7. Doenças Relacionadas ao Trabalho

As atividades repetitivas, o uso constante de equipamentos e as posturas inadequadas podem causar doenças ocupacionais.

As mais comuns são:

LER – Lesões por Esforços Repetitivos

São lesões causadas pela repetição contínua de movimentos.

DORT – Distúrbios Osteomusculares Relacionados ao Trabalho

Afetam músculos, tendões, ligamentos e articulações.

Sintomas

- Dor;
- Formigamento;
- Dormência;
- Perda de força;
- Limitação dos movimentos.

Exemplos práticos

Vigilante que permanece várias horas digitando relatórios pode desenvolver tendinite.

Operador de monitoramento que trabalha sentado durante todo o turno pode apresentar dores na coluna cervical e lombar.

Vigilante armado que permanece muito tempo em pé pode desenvolver dores nos joelhos e tornozelos.

8. Ginástica Laboral

A ginástica laboral consiste em exercícios rápidos realizados durante a jornada de trabalho para prevenir lesões e reduzir a fadiga.

Ela pode ser realizada antes, durante ou após o expediente.

Benefícios

Melhora da postura;

Redução das dores musculares;

Diminuição da fadiga;

Prevenção de LER e DORT;

Aumento da disposição;

Maior integração entre os colaboradores.

Exemplos de exercícios

Alongamento do pescoço;

Rotação dos ombros;

Alongamento dos braços;

Flexão e extensão dos punhos;

Alongamento das pernas;

Caminhada de 3 a 5 minutos durante intervalos.

A prática diária de apenas 10 minutos já proporciona benefícios significativos.

Considerações Finais

O preparo físico é uma ferramenta indispensável para o profissional de segurança privada. Um organismo saudável responde melhor às situações de emergência, reduz o risco de acidentes, melhora a tomada de decisões e aumenta a qualidade do serviço prestado.

Lembre-se: atividade física regular, alimentação equilibrada, hidratação, descanso adequado e cuidados preventivos são investimentos na sua saúde e na sua carreira.

Um profissional preparado protege melhor a si mesmo, seus colegas, o patrimônio e a sociedade.

REFERÊNCIA TÉCNICAS E BIBLIOGRÁFICAS

ABCFAV - ASSOCIAÇÃO BRASILEIRA DOS CURSOS DE FORMAÇÃO E APERFEIÇOAMENTO DE VIGILANTES. **Guia Prático ABCFAV**. São Paulo: ABCFAV, 2024.

ABCFAV; FENAVIST. **Cartilha Segurança Sem Preconceito**. Brasília: Fenavist, 2025. 2ª Edição.

ABCFAV; FENAVIST. **Cartilha Segurança Sem Preconceito**. Brasília: Fenavist, 2021. Disponível em: site oficial da Fenavist. Acesso em: 5 maio 2026.

ASSOCIAÇÃO BRASILEIRA DAS EMPRESAS DE TRANSPORTE DE VALORES (ABTV). **Relatório de Atividades 2024**. Brasília, 2024. Disponível em: abtv.org.br. Acesso em: 5 maio 2026.

ASSOCIAÇÃO BRASILEIRA DAS EMPRESAS DE VIGILÂNCIA E SEGURANÇA (ABREVIS). **Revista Abrevis**. São Paulo: Abrevis, 2024. Disponível em: abrevis-seg.com.br. Acesso em: 5 maio 2026.

ASSOCIAÇÃO BRASILEIRA DE CURSOS E APERFEIÇOAMENTO DE VIGILANTES (ABCFAV). **10º Encontro Nacional de Escolas de Formação e Aperfeiçoamento de Vigilantes (ENEFAV)**. São Paulo, 2023.

ASSOCIAÇÃO BRASILEIRA DE CURSOS E APERFEIÇOAMENTO DE VIGILANTES (ABCFAV). **11º Encontro Nacional de Escolas de Formação e Aperfeiçoamento de Vigilantes (ENEFAV)**. São Paulo, 2024.

ASSOCIAÇÃO BRASILEIRA DE CURSOS E APERFEIÇOAMENTO DE VIGILANTES (ABCFAV). **12º Encontro Nacional de Escolas de Formação e Aperfeiçoamento de Vigilantes (ENEFAV)**. São Paulo, 2025.

BRASIL. Polícia Federal. **Portaria nº 22-CGCSP/DPA/PF, de 15 de junho de 2026**. Estabelece os planos de curso, contendo conteúdo programático, carga horária e demais requisitos dos cursos de formação, aperfeiçoamento e atualização dos profissionais de segurança privada, no âmbito da Polícia Federal. Diário Oficial da União, Brasília, DF, 17 jun. 2026.

BRASIL. Polícia Federal. **Portaria nº 23 - CGCSP/DPA/PF, de 10 de junho de 2026**. Dispõe sobre o procedimento para o registro do gestor de segurança privada pela Polícia Federal e para a emissão da carteira nacional de gestor de segurança privada. Disponível no Portal da Polícia Federal. Acesso em: 08 jul. 2026.

BRASIL. Polícia Federal. **Portaria nº 24-CGCSP/DPA/PF, de 10 de junho de 2026**. Dispõe sobre a modalidade de ensino semipresencial nas escolas de formação de profissionais de segurança privada. Disponível em: Portal da Polícia Federal. Acesso em: 8 jul. 2026.

BRASIL. Polícia Federal. **Portaria nº 25-CGCSP/DPA/PF, de 10 de junho de 2026**. Dispõe sobre as normas relacionadas ao credenciamento de instrutores das escolas de formação de

profissionais de segurança privada. *Diário Oficial da União*, Brasília, DF, 12 jun. 2026. Seção 1, p. XX

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2022]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 20 de janeiro de 2026.

BRASIL. **Lei nº 13.146, de 6 de julho de 2015**. Estatuto da pessoa com deficiência. Brasília: Senado Federal, Coordenação de Edições Técnicas, 2015. 65 p. ISBN 978-85-7018-634-8.

BRASIL. **Decreto nº 4.503, de 20 de dezembro de 2001**. Regulamenta a Lei nº 10.257, de 10 de julho de 2001, que estabelece diretrizes gerais da política urbana, e dá outras providências. *Diário Oficial da União*, Brasília, DF, 21 dez. 2001.

BRASIL. **Decreto nº 98.380, de 9 de novembro de 1989**. Institui o emblema do Departamento de Polícia Federal, dispõe sobre a identificação de seus servidores e dá outras providências. Brasília, DF: Presidência da República. Disponível em: <https://www.planalto.gov.br>. Acesso em: 20 de junho de 2025.

BRASIL. **Decreto-Lei nº 6.378, de 28 de março de 1944**. Dispõe sobre a criação do Departamento Federal de Segurança Pública. *Diário Oficial da União*, Rio de Janeiro, 6 abr. 1944.

BRASIL. **Ética e cidadania: construindo valores na escola e na sociedade / Secretaria de Educação Básica, Fundo Nacional de Desenvolvimento da Educação**. Brasília: Ministério da Educação, Secretaria de Educação Básica, 2007.

BRASIL. **Lei nº 11.340, de 7 de agosto de 2006**. Cria mecanismos para coibir a violência doméstica e familiar contra a mulher [...]. Brasília, DF: Presidência da República, [2006]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/11340.htm. Acesso em: 02 de fevereiro de 2026.

BRASIL. **Lei nº 11.473, de 10 de maio de 2007**. Dispõe sobre cooperação federativa no âmbito da segurança pública e revoga a Lei nº 10.277, de 10 de setembro de 2001. *Diário Oficial da União*, Brasília, DF, 11 maio 2007. Disponível em: Portal da Presidência/Planalto. Acesso em: 4 abril 2026.

BRASIL. **Lei nº 12.037, de 1º de outubro de 2009**. Dispõe sobre a identificação criminal do civilmente identificado, regulamentando o art. 5º, inciso LVIII, da Constituição Federal. Brasília, DF: Presidência da República, [2009]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2009/lei/12037.htm. Acesso em: 10 de agosto de 2025.

BRASIL. **Lei nº 12.288, de 20 de julho de 2010**. Institui o Estatuto da Igualdade Racial; altera as Leis nos 7.716, de 5 de janeiro de 1989, 9.029, de 13 de abril de 1995, 7.347, de 24 de julho de 1985, e 10.778, de 24 de novembro de 2003. Brasília, DF: Presidência da República, [2010]. Disponível em: planalto.gov.br. Acesso em: 01 de junho de 2025.

BRASIL. **Lei nº 12.711, de 29 de agosto de 2012**. Dispõe sobre o ingresso nas universidades federais e nas instituições federais de ensino técnico de nível médio e dá outras providências. Brasília, DF: *Diário Oficial da União*, 30 ago. 2012. Disponível em: planalto.gov.br. Acesso em: 15 abr. 2026

BRASIL. **Lei nº 13.104, de 9 de março de 2015**. Altera o art. 121 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, para prever o feminicídio como circunstância qualificadora do crime de homicídio, e o art. 1º da Lei nº 8.072, de 25 de julho de 1990, para incluir o feminicídio no rol dos crimes hediondos. *Diário Oficial da União*, Brasília, DF, 10 mar. 2015.

BRASIL. **Lei nº 13.146, de 6 de julho de 2015**. Institui a Lei Brasileira de Inclusão da Pessoa com Deficiência (Estatuto da Pessoa com Deficiência). Brasília, DF: Presidência da República,

[2015]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/113146.htm. Acesso em: 1 maio 2025.

BRASIL. Lei nº 13.675, de 11 de junho de 2018. Institui o Sistema Único de Segurança Pública (Susp) e cria a Política Nacional de Segurança Pública e Defesa Social (PNSPDS). Diário Oficial da União: seção 1, Brasília, DF, ano 155, n. 111, p. 1-6, 12 jun. 2018. Disponível em: www.planalto.gov.br. Acesso em: 4 mai. 2025.

BRASIL. Lei nº 14.532, de 11 de janeiro de 2023. Altera a Lei nº 7.716, de 5 de janeiro de 1989 (Lei do Crime Racial), e o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tipificar como crime de racismo a injúria racial. Brasília, DF: Presidência da República, [2023]. Disponível em: www.planalto.gov.br. Acesso em: 01 de junho de 2025.

BRASIL. Lei nº 14.786, de 28 de dezembro de 2023. Cria o protocolo “Não é Não”, para prevenção ao constrangimento e à violência contra a mulher e para proteção à vítima... Diário Oficial da União, Brasília, DF, 28 dez. 2023.

BRASIL. Lei nº 14.967, de 9 de setembro de 2024. Institui o Estatuto da Segurança Privada e da Segurança das Instituições Financeiras; altera a Lei nº 10.826, de 22 de dezembro de 2003 (Estatuto do Desarmamento), a Lei nº 10.446, de 8 de maio de 2002, a Lei nº 10.637, de 30 de dezembro de 2002, a Lei nº 10.833, de 29 de dezembro de 2003, e o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal); revoga a Lei nº 7.102, de 20 de junho de 1983, a Lei nº 8.863, de 28 de março de 1994, e dispositivos da Lei nº 11.718, de 20 de junho de 2008, da Lei nº 9.017, de 30 de março de 1995, e da Medida Provisória nº 2.184-23, de 24 de agosto de 2001; e dá outras providências., 09 de setembro de 2024.

BRASIL. Lei nº 15.142, de 3 de junho de 2025. Reserva às pessoas pretas e pardas, indígenas e quilombolas o percentual de 30% das vagas oferecidas nos concursos públicos federais.

Diário Oficial da União: seção 1, Brasília, DF, ano 162, n. 105, p. 1-3, 4 jun. 2025

BRASIL. Lei nº 15.245, de 29 de outubro de 2025. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para dispor sobre o crime de associação criminosa, a Lei nº 12.694, de 24 de julho de 2012, e a Lei nº 12.850, de 2 de agosto de 2013. Brasília, DF: Presidência da República, [2025]. Disponível em: <https://www2.camara.leg.br/legin/fed/lei/2025/lei-15245-29-outubro-2025-798213-publicacaooriginal-176869-pl.html>. Acesso em: 5 mai. 2026.

BRASIL. Lei nº 3.353, de 13 de maio de 1888. Declara extinta a escravidão no Brasil. Rio de Janeiro, 1888. Disponível em: Planalto.gov.br. Acesso em: 4 mai. 2025.

BRASIL. Lei nº 4.483, de 16 de novembro de 1964. Diário Oficial da União, Brasília, DF, 10 dez. 1964.

BRASIL. Lei nº 4.878, de 3 de dezembro de 1965. Dispõe sobre o regime jurídico peculiar aos funcionários policiais civis da União e do Distrito Federal. Brasília, DF: Diário Oficial da União, 6 dez. 1965. Disponível em: <https://www2.camara.leg.br/legin/fed/lei/1960-1969/lei-4878-3-dezembro-1965-368395-norma-pl.html>. Acesso em: 20 de julho de 2025.

BRASIL. Lei nº 5.553, de 6 de dezembro de 1968. Dispõe sobre a apresentação e uso de documentos de identificação pessoal. Brasília, DF: Diário Oficial da União, 10 dez. 1968. Disponível em: www.planalto.gov.br. Acesso em: 03 de julho de 2025.

BRASIL. Lei nº 601, de 18 de setembro de 1850. Dispõe sobre as terras devolutas do Império. Rio de Janeiro, [1850]. Disponível em: www.planalto.gov.br. Acesso em: 5 mai. 2025.

BRASIL. Lei nº 7.716, de 5 de janeiro de 1989. Define os crimes resultantes de preconceito de raça ou de cor. Brasília, DF: Presidência da República, [1989]. Disponível em: planalto.gov.br. Acesso em: 4 abril 2026.

BRASIL. Lei nº 7.716, de 5 de janeiro de 1989. Define os crimes resultantes de preconceito de raça ou de cor. **Diário Oficial da União:** seção 1, Brasília, DF, ano 127, n. 4, p. 369, 6 jan. 1989.

BRASIL. Lei nº 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Brasília, DF: Presidência da República, [1990].

Disponível em: https://www.planalto.gov.br/ccivil_03/leis/18069.htm. Acesso em: 01 de maio de 2026.

BRASIL. **Lei nº 9.017, de 30 de março de 1995**. Estabelece normas de controle e fiscalização sobre produtos e insumos químicos [...]. Brasília, DF: Diário Oficial da União, 1995. Disponível no Portal da Legislação da Presidência. Acesso em: 5 maio 2026.

BRASIL. **Lei nº 9.296, de 24 de julho de 1996**. Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal. Brasília, DF: Presidência da República, [1996]. Disponível em: [planalto.gov.br](https://www.planalto.gov.br). Acesso em: 01 de junho 2025.

BRASIL. **Lei nº 9.453, de 20 de março de 1997**. Acrescenta parágrafo ao art. 2º da Lei nº 5.553, de 6 de dezembro de 1968, que dispõe sobre a apresentação e uso de documentos de identificação pessoal. Brasília, DF: Presidência da República, [1997]. Disponível em: [planalto.gov.br](https://www.planalto.gov.br). Acesso em: 01 de junho 2025.

BRASIL. **Ministério da Educação. Secretaria de Educação Básica. Ética e cidadania**: construindo valores na escola e na sociedade. Brasília: MEC, SEB, 2007. 84 p.

BRASIL. Ministério da Justiça e Segurança Pública. Polícia Federal. Portaria nº 6-CGCSP/DIREX/PF, de 22 de abril de 2021. Dispõe sobre a modalidade de ensino semipresencial nas empresas de curso de formação. **Diário Oficial da União**: seção 1, Brasília, DF, p. 204, 26 abr. 2021.

BRASIL. Ministério da Justiça. Gabinete do Ministro. **Portaria nº 796, de 8 de setembro de 2000**. Dispõe sobre classificação de diversões públicas e de programas de rádio e de televisão, a exceção dos transmitidos ao vivo. **Diário Oficial da União**: seção 1, Brasília, DF, n. 177, p. 1, 13 set. 2000.

BRASIL. Ministério do Trabalho e Emprego. **Norma Regulamentadora nº 01 (NR-01)**: Disposições Gerais e Gerenciamento de Riscos Ocupacionais. Brasília, DF: Ministério do Trabalho e Emprego, 2022. Disponível em: <https://www.gov.br/trabalho-e-emprego/pt-br/aceso-a-informacao/participacao-social/conselhos-e-orgaos-colegiados/comissao-tripartite-partitaria-permanente/normas-regulamentadora/normas-regulamentadoras-vigentes/nr-1>. Acesso em: 6 maio 2026.

BRASIL. Ministério do Trabalho e Emprego. **Setor de vigilância pode gerar até 25 mil vagas para jovens aprendizes**. Brasília, DF, 18 jun. 2024. Disponível em:

<https://www.gov.br/trabalho-e-emprego/pt-br/noticias-e-conteudo/2024/Junho/setor-de-vigilancia-pode-gerar-ate-25-mil-vagas-para-jovens-aprendizes>. Acesso em: 24 jun. 2024.

BRASIL. Ministério do Trabalho e Previdência. **Norma Regulamentadora nº 07 - Programa de Controle Médico de Saúde Ocupacional (PCMSO)**. Brasília, DF: Portaria SEPRT nº 6.734, de 9 de março de 2020. Disponível no Portal Gov.br.

BRASIL. Ministério do Trabalho e Previdência. **Norma Regulamentadora nº 23 - Proteção Contra Incêndios**. Brasília, DF: 2022. Disponível no Portal Gov.br. Acessado em 01 de fevereiro de 2026.

BRASIL. Ministério do Trabalho e Previdência. **Norma Regulamentadora nº 07 - Programa de Controle Médico de Saúde Ocupacional (PCMSO)**. Brasília, DF: Portaria SEPRT nº 6.734, de 9 de março de 2020. Disponível no Portal Gov.br.

BRASIL. Ministério do Trabalho e Previdência. **Norma Regulamentadora nº 23 - Proteção Contra Incêndios**. Brasília, DF: 2022. Disponível no Portal Gov.br. Acessado em 01 de fevereiro de 2026.

BRASIL. Polícia Federal. **Instrução Normativa nº 111, de 31 de janeiro de 2017**. Estabelece normas e procedimentos para o credenciamento de instrutores de armamento e tiro. Brasília, 2017. Disponível em: <https://www.gov.br/pf/pt-br/assuntos/armas/instrutores-de-armamento-e-tiro/orientacao-para-credenciamento/in-111-2017>. Acesso em: 23 de abril de 2026.

BRASIL. Polícia Federal. **Manual do Vigilante**. 2. ed. retif. Brasília, DF: Academia Nacional de Polícia, 2020. Disponível em: <https://www.gov.br/pf/pt-br/assuntos/seguranca-privada/legislacao-normas-e-orientacoes/manual-do-vigilante>. Acesso em: 05 fevereiro 2026.

BRASIL. Polícia Federal. **Segurança Privada**. Brasília: Polícia Federal, [202-?]. Disponível em: <https://www.gov.br/pf/pt-br/assuntos/carta-de-servicos/arquivos/livretos/livreto-Seg%20Privada.pdf>. Acesso em: 5 maio 2026.

CAMPIDELLI, Cristiano. **Novos rumos para as escolas de formação em segurança**. In: ENCONTRO NACIONAL DAS ESCOLAS DE FORMAÇÃO E APERFEIÇOAMENTO DE VIGILANTES, 11., 2024. **Anais**. São Paulo, SP, Brasil: ABCFAV, 2024.

CNTV - CONFEDERAÇÃO NACIONAL DOS TRABALHADORES VIGILANTES E PRESTADORES DE SERVIÇOS. **Quem Somos**. Brasília, [2026]. Disponível em: <https://www.cntv.org.br/quem-somos.html>. Acesso em: 05 maio 2026

CORREA, Ricardo Tadeu; ABCFAV. **Segurança sem Preconceito: cartilha educativa**. São Paulo: ABCFAV/Fenavist, 2022. Disponível em: <https://www.gov.br/pf/pt-br/assuntos/seguranca-privada/legislacao-normas-e-orientacoes/cartilha-seguranca-sem-preconceito/cartilha-seguranca-sem-preconceito>. Acesso em: 05 de janeiro de 2026.

ESCOLA BRASIL DE SEGURANÇA. **CURSO DE SUPERVISOR**. Belo Horizonte: Escola Brasil, 2009. Apostila interna destinada ao Curso de Formação de Vigilantes.

SOARES, Amilson Santos. **Segurança privada no Brasil: Fundamentos Históricos & Formação Multiprofissional** / Amilson Santos Soares. – Veranópolis, RS: Laurea, 2026.

TOCCHETTO, Domingos. **Balística Forense: aspectos técnicos e jurídicos**. 12. ed. Campinas: Millennium Editora, 2026.