DEFINIÇÕES TÉCNICAS DOS SISTEMAS

Lei nº 14.133, de 1º de abril de 2021

Instrução Normativa SGD/ME n° 94, de 23 de dezembro de 2022

VOLUME 6

Contrato n° 04.043.10.2024

Processo Administrativo n° 0016551-52.2024.4.03.8000

Tribunal Regional Federal da 3ª Região

Secretaria de Segurança Institucional

Seção de Inteligência - RINA

CREA-SP - ART 2620250540031

SOLUÇÃO DE EXPANSÃO E MODERNIZAÇÃO DO SISTEMA DE SEGURANÇA ELETRÔNICA

M.Sc. Rodrigo Sagaseta de Oliveira Souza

Mestre em Engenharia Elétrica – Dissertação sobre uso de IA (Deep Learning)

Engenheiro Eletricista, Segurança do Trabalho e Segurança contra Incêndio e Pânico

Perito Técnico Judiciário – Assistência Judicial Gratuita

CREA-SP: 5070834495

São Paulo, abril de 2025

DEFINIÇÕES TÉCNICAS DOS SISTEMAS

(Referência: Inciso XI, do art. 2º e art. 11 da IN SGD/ME nº 94/2022)

HISTÓRICO DE VERSÕES

DATA	VERSÃO	DESCRIÇÃO	AUTOR
23/03/2025	1.00	Criação do documento	M.Sc Rodrigo Sagaseta de Oliveira Souza
01/04/2025	1.01	Finalização do documento	M.Sc Rodrigo Sagaseta de Oliveira Souza
02/04/2025	1.02	Divisão em Volumes	M.Sc Rodrigo Sagaseta de Oliveira Souza

SUMÁRIO

Histórico de Versões 2
Sumário 2
1. Informações básicas 7
2. Design da nova solução 7
2.1. Diagrama ilustrativo dos compontentes dos novos sistemas 7
2.2. Infraestrutura 7
2.3. Controle de acesso 8
2.4. Videomonitoramento 8
2.4.4. Sistema de reconhecimento facial 8
2.5. Alarme perimetral 10
2.6. Sistemas interdependentes 10
2.7. Sistemas independentes 11
3. Análise técnica para definições do novo sistema 11
3.1. Diagrama da arquitetura do sistema VMS inteligente 11
3.1.1. Diagrama ilustrativo da arquitetura (SOC) 11
3.1.2. Firewall 12
3.1.3. Servidores 12
3.1.4. IDS/IPS 12

3.1.5. VPN 12
3.1.6. Alarmes 12
3.2. Centro de Comando e Operações (CCO) 12
3.2.1. Monitoramento 13
3.2.2. Operadores 13
3.2.3. Alertas 13
3.2.4. Resposta rápida 13
3.3. Fluxo de operação 13
3.3.1. Detecção de eventos 13
3.3.2. Análise 13
3.3.3. Ação 13
3.3.4. Resposta 13
4. Serviços e necessidades tecnológicas 13
4.3. Serviços de engenharia e treinamento 14
4.4. Integração com sistemas existentes 14
4.5. Implementação de soluções de redundância 14
4.6. Substituição e modernização do parque de câmeras 15
4.7. Implementação de sistema de videomonitoramento inteligente 15
4.7.2. Funcionalidades essenciais de um VMS inteligente 15
4.7.3. Benefícios da implementação de um VMS inteligente 16
4.8. Implementação de sistema de leitura de placas (LPR) 17
4.9. Implementação de sistema de reconhecimento facial 17
4.9.5. Diagrama de funcionamento 17
4.9.6. Possibilidades funcionais 18

4.9.7. Detecção de máscaras 19
4.9.8. Áreas restritas 19
4.9.9. Relatórios analíticos 19
4.10. Aprimoramento da infraestrutura de rede 19
4.11. Implementação de um centro de operações de segurança (SOC) 20
4.12. Aquisição de software de análise de vídeo inteligente (IVA) 20
4.13. Implementação de um sistema de gestão de identidade e acesso (IAM) 20
4.14. Aquisição de cofre de acautelamento de armas 20
4.15. Diagrama ilustrativo da topologia de rede dos novos sistemas 20
4.16. Integração com sistema de controle de acesso 21
4.16.2. Arquitetura e compatibilidade 21
4.16.3. Integração com sistemas associados 21
4.16.4. Funcionalidades avançadas de integração 22
4.16.5. Segurança e resiliência 23
4.16.6. Conformidade e certificações 23
4.16.7. Resiliência operacional e monitoramento reativo 23
4.16.8. Funcionalidades recomendadas para operadores 23
4.16.9. Integração de metadados com IA 23
4.16.10. API Aberta 24
4.17. Integração do sistema de controle de acesso com sistema de alarme de incêndio 24
4.17.2. Comunicação e interoperabilidade 24
4.17.3. Automação de respostas 24
4.17.4. Monitoramento e notificação 24
4.17.5. Prioridades de resposta 25

4.17.6. Conformidade com normas técnicas 25
4.17.7. Rastreamento e localização 25
4.17.8. Funcionalidades adicionais para cenários de emergência 25
4.17.9. API Aberta 25
5. Demais requisitos necessários e suficientes à escolha da solução de TIC 26
5.4. Integração e interoperabilidade 26
5.5. Escalabilidade e flexibilidade 26
5.6. Segurança cibernética 26
5.7. Desempenho e confiabilidade 27
5.8. Usabilidade e acessibilidade 27
5.9. Manutenção e suporte técnico 27
5.10. Treinamento 27
5.11. Conformidade com normas e regulamentações 27
5.12. garantia 27
6. Processo de despacho de ocorrências automatizado 28
6.2. Registro e recebimento de ocorrências 29
6.3. Cadastro detalhado de ocorrências 29
6.4. Fluxo de atendimento e ações 29
6.5. Visualização em Mapa 30
6.6. Análise de incidências 30
6.7. Integração com sistemas de câmeras 30
6.8. Cadastros e relatórios 30
6.9. Monitoramento de agentes 30
6.10. Painel e indicadores 31

6.11. Localização referenciada 31
6.12. Ordem de serviço 31
6.13. Tecnologia de análises inteligentes 31
6.14. Integração com leitura de placas, CFTV e reconhecimento facial 32
6.15. Integração com sistema de telefonia 32
6.16. Aplicação nos ambientes do TRF3 32
6.16.2. Torres norte e sul 32
6.16.3. Heliporto 33
6.16.4. Depósito judicial Presidente Wilson 33
6.16.5. Considerações adicionais 33
7. Responsabilidade técnica e direitos autorais 34
8. Aprovação e declaração de conformidade 34

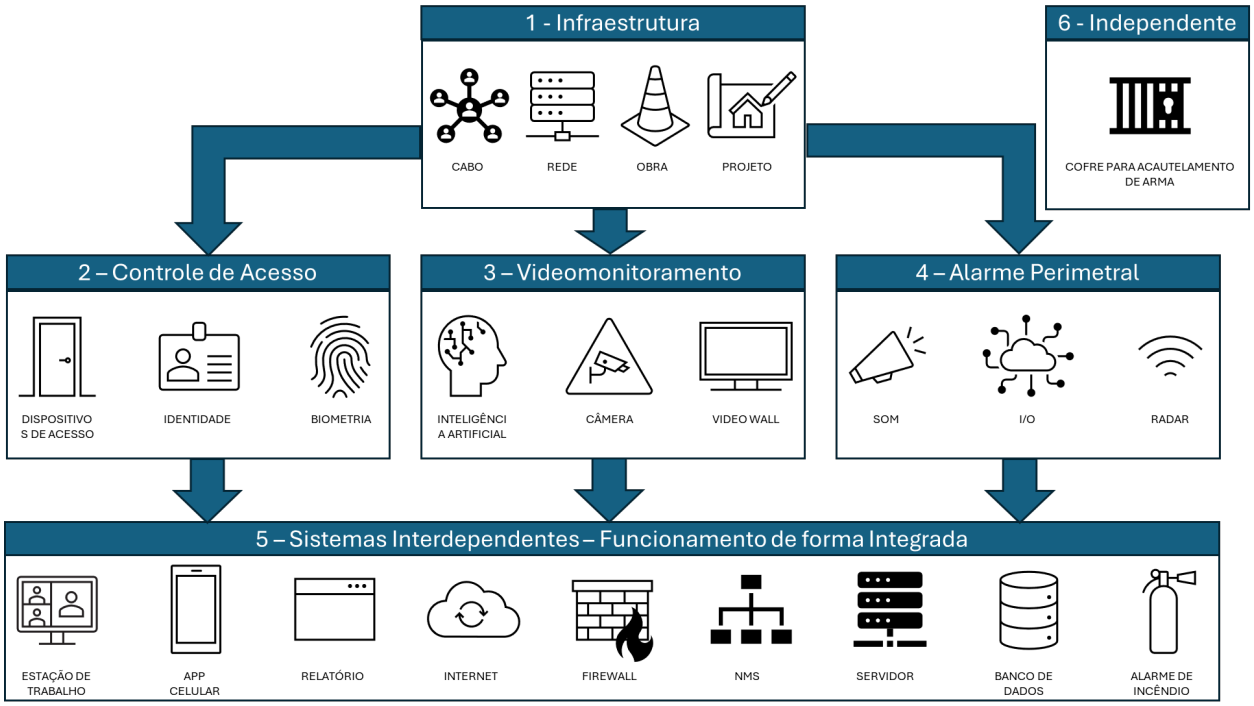
1. INFORMAÇÕES BÁSICAS

1.1. Este estudo, foi elaborado conforme termos do Processo Administrativo nº 0016551-52.2024.4.03.8000, sob número de contrato 04.043.10.2024, devidamente registrado no CREA-SP - ART 2620250540031 sob responsabilidade técnica do M.Sc Rodrigo Sagaseta de Oliveira Souza.

1.2. As Definições Técnicas dos Sistemas tem por objetivo apresentar todas as definições técnicas e funcionalidades do conjunto de sistemas da contratação de Solução de Expansão e Modernização do Sistema de Segurança Eletrônica, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação.

2. DESIGN DA NOVA SOLUÇÃO

2.1. DIAGRAMA ILUSTRATIVO DOS COMPONTENTES DOS NOVOS SISTEMAS



2.2. INFRAESTRUTURA

2.2.1. **Cabo:** Essencial para a transmissão de dados entre os diversos dispositivos. A escolha do tipo de cabo (fibra óptica, par trançado, etc.) deve considerar a largura de banda necessária e a distância entre os pontos.

2.2.2. **Rede:** Conjunto de equipamentos (switches, roteadores, etc.) que permitem a comunicação entre os dispositivos. A arquitetura da rede deve ser projetada para garantir a redundância e a segurança dos dados.

2.2.3. **Obra:** Refere-se às adaptações físicas necessárias para a instalação dos sistemas, como a passagem de cabos, a

instalação de suportes para câmeras, etc.

2.2.4. **Projeto:** Engloba o planejamento, projeto executivo, As-built e a documentação de toda a infraestrutura e demais subsistemas trabalhando de forma integrada, incluindo diagramas, especificações técnicas e cronogramas.

2.3. CONTROLE DE ACESSO

2.3.1. Dispositivos de Acesso: Leitoras de cartão, teclados, leitores biométricos, etc. São os equipamentos que autenticam os usuários e liberam o acesso.

2.3.2. **Identidade:** Refere-se aos métodos de identificação utilizados, como cartões de acesso, senhas, biometria (impressão digital, reconhecimento facial, etc.).

2.3.3. **Biometria:** Utilização de características físicas únicas para identificação, oferecendo um nível de segurança mais elevado.

2.3.4. **Inteligência Artificial:** Utilização de algoritmos de IA para análise de padrões de acesso, detecção de anomalias e prevenção de fraudes.

2.4. VIDEOMONITORAMENTO

2.4.1. **Câmeras:** Dispositivos que capturam imagens e vídeos. A escolha do tipo de câmera (fixa, móvel, infravermelho, etc.) deve considerar as características do ambiente e as necessidades de monitoramento.

2.4.2. **Video Wall:** Conjunto de monitores que exibem as imagens capturadas pelas câmeras, permitindo uma visão ampla do ambiente.

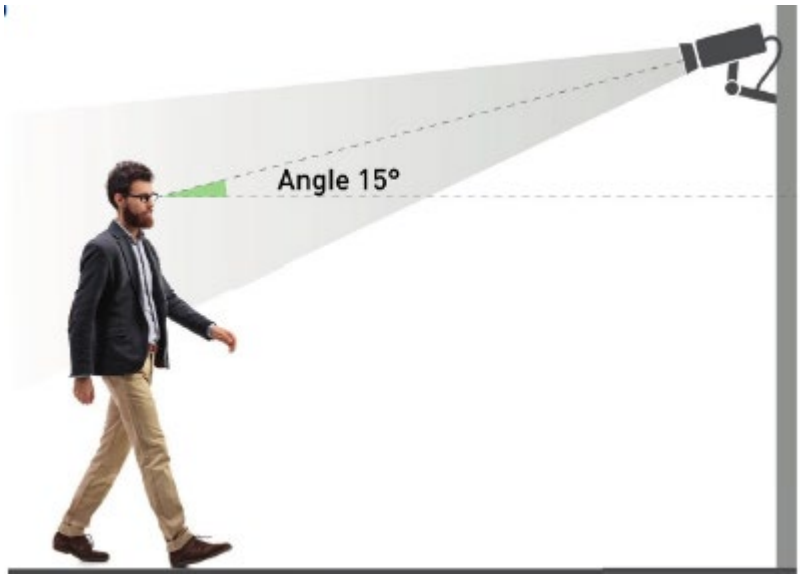
2.4.3. **Analíticos de Inteligência Artificial:** Conjunto de funcionalidades analíticas que permitem uma ação automatizada e garantida no monitoramento de áreas, evitando erros e falhas humanas. Estes sistemas tornam-se essenciais pois evitam viés por trabalharem sobre regras bem definidas de ações enviando as notificações e os vídeos assim que detectados para a tela do operador, evitando que fatos possam passar desapercebidos. Estas funcionalidades analíticas, além de permitirem uma interação e monitoramento mais assertivo em tempo real, possibilita a identificação de indivíduos, veículos e objetos suspeitos, e através de recursos de machine learning, permitem a implementação de um sistema de investigação forense baseados em um conjunto de características que tenham sido identificadas pelo sistema de inteligência artificial, de forma simples e rápida.

2.4.4. SISTEMA DE RECONHECIMENTO FACIAL

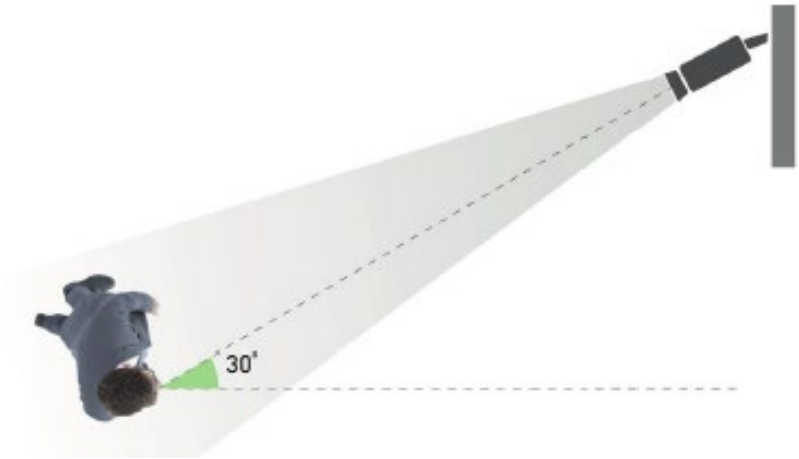
2.4.4.1. Em condições ideais (o sistema funciona em diversas condições, com diminuição de sua assiduidade) para a detecção perfeita (superior a 99% de acerto) de faces, no fluxo de vídeo, as câmeras devem ser instaladas de modo que o campo de visão inclua, de maneira direta, as faces dos indivíduos que entram no local ou se encontrem em um determinado perímetro.

2.4.4.2. O ângulo de inclinação vertical da câmera não deve exceder 15° (o ajuste do foco da câmera a partir do plano

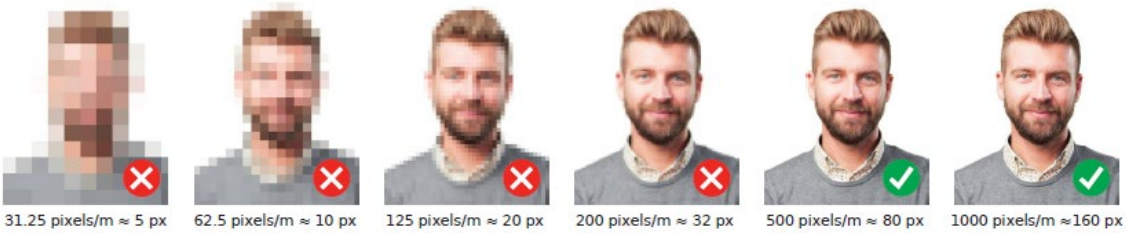
horizontal, construído no nível médio da altura de uma pessoa - 160 cm). Sendo que o ângulo da deflexão horizontal não deve exceder 30° (desvio do eixo óptico da câmera do vetor de movimento do fluxo principal dos objetos de reconhecimento). Veja figura abaixo:

2.4.4.3. 

2.4.4.4. O ângulo da deflexão horizontal não deve exceder 30° (desvio do eixo óptico da câmera do vetor de movimento do fluxo principal para realizar o reconhecimento). Veja a figura abaixo:

2.4.4.5. 

2.4.4.6. É importante que o Sistema de Reconhecimento Facials, seja compatível com qualquer marca/fabricante de câmeras HD respeitando a densidade de pixels para nosso engenho de “deep learning” realizar a identificação, sendo o mínimo de 500 pixels/m (aproximadamente, sendo à largura da face em 80 pixels). Conforme exemplo abaixo:

2.4.4.7. 

2.5. ALARME PERIMETRAL

2.5.1. **Dispositivos de I/O (Entrada/Saída):** Os dispositivos de I/O atuam como a interface entre os sensores de detecção (radares) e o sistema de alarme central. Eles recebem os sinais dos radares indicando a presença de uma pessoa ou veículo, processam essas informações e, em seguida, acionam os alarmes sonoros (cornetas de áudio) e enviam notificações para a central de segurança.

2.5.2. **Radar para Detecção de Presença de Pessoas e Veículos:** O radar é o sensor primário do sistema, responsável por detectar a presença de pessoas e veículos dentro do perímetro protegido, através da emissão de ondas de rádio que, ao atingirem um objeto (pessoa ou veículo), são refletidas de volta ao sensor. O sistema analisa as características dessas ondas refletidas para determinar a distância, velocidade e direção do objeto. A análise do deslocamento Doppler permite determinar a velocidade do objeto com alta precisão.

2.5.3. **Cornetas de Áudio:** As cornetas de áudio têm a função de emitir sinais sonoros de alerta em caso de detecção de intrusão. Quando os dispositivos de I/O recebem um sinal de intrusão, eles acionam as cornetas de áudio que emitem um som alto e estridente, ou mensagens de voz gravadas, alertando as pessoas na área sobre a ameaça e dissuadindo potenciais invasores. O volume das cornetas pode ser ajustado para ser audível em toda a área protegida, mas sem causar desconforto excessivo ou violações das normas de ruído.

2.5.4. **Melhores Práticas:** As cornetas devem ser instaladas em locais estratégicos para maximizar a cobertura sonora e minimizar a possibilidade de serem danificadas ou desativadas. A alimentação das cornetas deve ser protegida contra cortes de energia, utilizando baterias de backup ou geradores.

2.6. SISTEMAS INTERDEPENDENTES

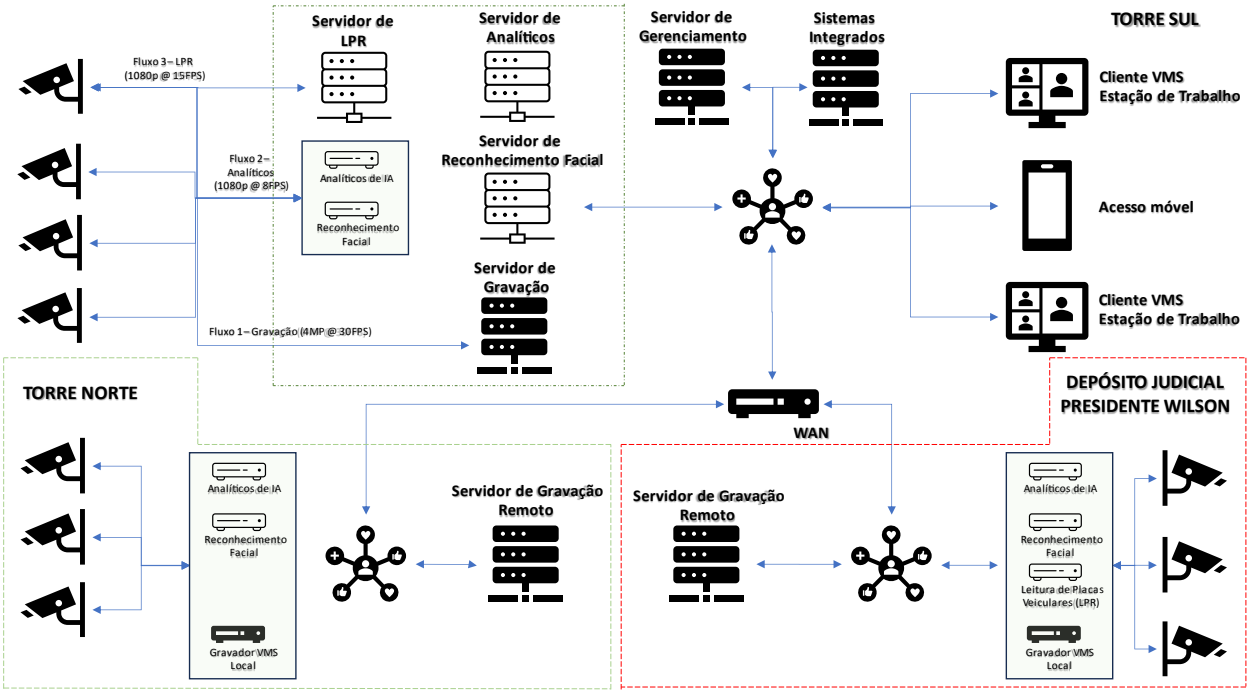
2.6.1. A interdependência entre os sistemas é algo fundamental a ser observado para garantir a segurança e a eficiência do local. Por exemplo, o controle de acesso pode ser integrado ao videomonitoramento, permitindo que as câmeras capturem imagens das pessoas que acessam áreas restritas. Proporcionar a integração com o alarme perimetral, permite que o sistema alerte os operadores em caso de invasão. A aquisição e a instalação desses sistemas deve considerar suas interdependências, exigindo que sejam apresentadas soluções integradas e eficientes e principalmente que possam ser comprovadas por seus respectivos fabricantes, treinamentos de especialização e corpo técnico com graduação e atribuições compatíveis que permitam a plena execução de todas as atividades necessárias.

2.7. SISTEMAS INDEPENDENTES

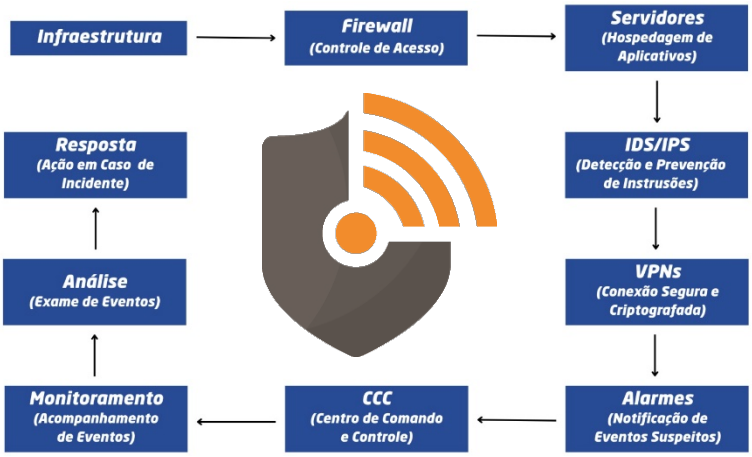
2.7.1. São sistemas que não podem depender de nenhum outro sistema para garantir o seu completo funcionamento. Neste ETP, é previsto um cofre para acautelamento de armas, que deve ser um local seguro para guarda de armas de fogo, evitando o acesso não autorizado e que apesar de ser um sistema independente também deve possuir uma integração para garantia de sua manutenção e atualização segura com os sistemas de controle de acesso, videomonitoramento e alarme.

3. ANÁLISE TÉCNICA PARA DEFINIÇÕES DO NOVO SISTEMA

3.1. DIAGRAMA DA ARQUITETURA DO SISTEMA VMS INTELIGENTE



3.1.1. DIAGRAMA ILUSTRATIVO DA ARQUITETURA (SOC)



3.1.1.1.

3.1.2. FIREWALL

3.1.2.1. Um firewall é um sistema de segurança que monitora e controla o tráfego de rede entre uma rede interna e a internet, tendo como função bloquear tráfego indesejado, permitir tráfego autorizado e proteger a rede contra ameaças.

3.1.3. SERVIDORES

3.1.3.1. Um servidor é uma unidade de processamento computacional que fornece serviços ou recursos a outras unidades denominadas computadores, em um ambiente de rede. Sua função principal consiste em hospedar aplicativos, armazenar dados, gerenciar e fornecer serviços de rede.

3.1.4. IDS/IPS

3.1.4.1. O IDS (Intrusion Detection System), é um sistema que detecta tentativas de intrusão em uma rede. O IPS (Intrusion Prevention System), é um sistema que detecta e previne tentativas de intrusão. Suas funções consistem em prevenir ameaças, tais como ataques de negação de serviço, malwares e etc.

3.1.5. VPN

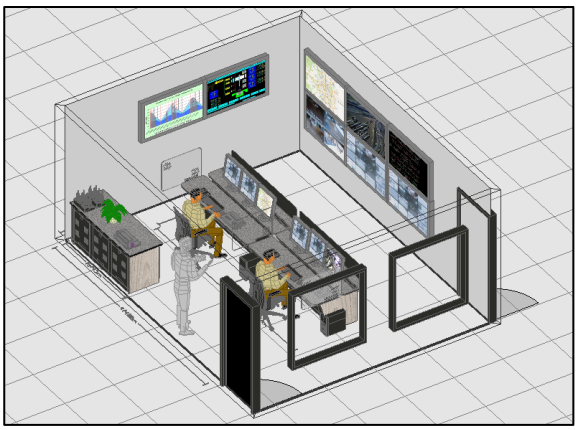
3.1.5.1. Uma VPN (Virtual Private Network) é uma rede privada que utiliza a internet para realizar a conexão à dispositivos remotos. Sua função consistem em fornecer uma conexão segura e criptografada entre dispositivos remotos e a rede interna local.

3.1.6. ALARMES

3.1.6.1. Um alarme é um sistema que notifica quando um evento suspeito ocorre. Sua função consiste em notificar administradores de rede sobre eventos suspeitos, como tentativas de intrusão, falhas de hardware e etc.

3.2. CENTRO DE COMANDO E OPERAÇÕES (CCO)

O Centro de Comando e Operações é o ponto central onde as decisões de ações proativas ou reações são iniciadas. Por este motivo é muito importante que este seja bem implementado de forma a dispor para os operadores as informações mais importantes em tempo real. Desta forma, apresentamos abaixo um design conceitual da solução que deverá ser montada neste ambiente.



3.2.1. MONITORAMENTO

3.2.1.1. Monitoramento é o processo de acompanhar e analisar eventos em tempo real. Sua função consiste em acompanhar eventos de rede, sistemas e aplicativos para detectar problemas ou ameaças.

3.2.2. OPERADORES

3.2.2.1. Os operadores são os profissionais responsáveis por analisar e responder aos eventos. Sua função consiste em analisar estes eventos, identificar problemas ou ameaças e responder a estes incidentes.

3.2.3. ALERTAS

3.2.3.1. Alertas são as notificações geradas de forma automática, que são enviadas quando um evento suspeito ocorre. Sua função consiste em notificar de forma automatizada os operadores e administradores de rede sobre eventos suspeitos.

3.2.4. RESPOSTA RÁPIDA

3.2.4.1. A resposta rápida é um processo que envolve a resposta de forma imediata a incidentes. Sua função é responder de forma imediata a incidentes buscando minimizar seus impactos e prevenindo danos.

3.3. FLUXO DE OPERAÇÃO

3.3.1. DETECÇÃO DE EVENTOS

3.3.1.1. A detecção de eventos é o processo de identificar eventos suspeitos. Sua função é identificar estes eventos suspeitos, tais como, tentativas de intrusão, malware e etc.

3.3.2. ANÁLISE

3.3.2.1. A análise é o processo de examinar eventos para determinar a gravidade e o impacto. Sua função consiste em examinar eventos para determinar sua gravidade e impacto.

3.3.3. AÇÃO

3.3.3.1. A ação é o processo de responder aos eventos. Sua função é responder a eventos, como incidentes, para minimizar seus impactos e proporcionar a prevenção a danos.

3.3.4. RESPOSTA

3.3.4.1. Resposta é o processo de responder aos incidentes. Sua função é responder de forma proativa ou reativa diante de um incidente.

4. SERVIÇOS E NECESSIDADES TECNOLÓGICAS

4.1. As necessidades tecnológicas a seguir definem os bens e serviços de Tecnologia da Informação e Comunicação (TIC) necessários ao atendimento da demanda de segurança integrada do TRF3 - Tribunal Regional Federal da 3ª Região. Estas necessidades levam em conta padrões, capacidades, metodologias, processos, competências das equipes, cuidados com a segurança da informação, entre outros aspectos que a

solução deve satisfazer para atingir o desempenho e os resultados de negócio esperados. Essas definições são inerentes ao ambiente computacional da instituição, envolvem características de infraestrutura, capacidade, organização, boas práticas implementadas e decisões tomadas pela área de TIC ao longo dos anos, além de projetos para o futuro. Como resultado da definição das necessidades, obtém-se uma lista de bens e serviços que obrigatoriamente devem compor a solução e serão detalhados na definição dos requisitos. Em geral, correspondem a itens a serem contratados ou adquiridos, podendo incluir: equipamentos necessários ao funcionamento da solução, serviços que devem ser executados (mesmo em aquisições de bens pode haver serviços de instalação ou de configuração envolvidos), produtos que devem ser entregues, capacitações, demandas de outras áreas envolvidas no processo em que a solução vai intervir ou que necessitam da mesma solução. Essas necessidades ou componentes podem variar a depender da solução específica ou da alternativa adotada.

4.2. Ao atender a essas necessidades tecnológicas, a solução de segurança integrada para o TRF-3 estará preparada para enfrentar os desafios atuais e futuros, garantindo a proteção das instalações, dos servidores, magistrados e visitantes, e a integridade das informações e processos sob sua responsabilidade.

4.3. SERVIÇOS DE ENGENHARIA E TREINAMENTO

4.3.1. Contratação de serviços de engenharia especializada para realizar um projeto executivo detalhado, instalação, configuração e implementação das novas tecnologias, juntamente com o treinamento do pessoal existente para operar e manter os sistemas de segurança e a entrega de documentação As-built detalhada contendo todas as informações técnicas das instalações e do ambiente instalado. Isso garantira que as novas tecnologias possam ser implementadas de forma eficaz e documentada, e permitindo que a equipe de operação possa ser corretamente treinada e capacitada dentro do ambiente operacional, para utilizá-las de forma segura e eficiente.

4.4. INTEGRAÇÃO COM SISTEMAS EXISTENTES

4.4.1. Garantir a integração das novas tecnologias com os sistemas existentes, como os sistemas de alarme e controle de acesso.

4.4.2. A integração dos sistemas permitirá a automação de tarefas, a coordenação da resposta a incidentes e a geração de relatórios detalhados sobre a segurança institucional.

4.5. IMPLEMENTAÇÃO DE SOLUÇÕES DE REDUNDÂNCIA

4.5.1. Implementar soluções de redundância para garantir a disponibilidade dos sistemas em caso de falhas, como a duplicação de comutadores e roteadores e a utilização de links de comunicação redundantes.

4.5.2. A redundância garante que, em caso de falha de um componente da rede, outro componente assuma

automaticamente as funções do componente falho, minimizando o tempo de inatividade e garantindo a disponibilidade dos sistemas.

4.6. SUBSTITUIÇÃO E MODERNIZAÇÃO DO PARQUE DE CÂMERAS

4.6.1. Substituição das câmeras analógicas existentes por câmeras IP de alta resolução (mínimo 4MP) com funcionalidades avançadas de análise de vídeo e inteligência artificial (IA) realizadas por software, minimizando os custos tanto para aquisição quanto para substituição de câmeras, uma vez que a inteligência não estará embarcada nela, permitindo também a constante atualização de funcionalidades analíticas dos softwares, melhorando o aproveitamento de legado.

4.6.2. A solução deve incluir câmeras com diferentes tipos de lentes (fixas, varifocais, PTZ) para atender às necessidades específicas de cada área monitorada.

4.6.3. As câmeras analógicas apresentam limitações em termos de qualidade de imagem, capacidade de integração e funcionalidades avançadas de análise. A substituição por câmeras IP de alta resolução com IA permitirá a detecção proativa de ameaças, a identificação de pessoas de interesse e a automatização de tarefas.

4.7. IMPLEMENTAÇÃO DE SISTEMA DE VIDEOMONITORAMENTO INTELIGENTE

4.7.1. A implementação de um Sistema de Videomonitoramento Inteligente (VMS) representa um passo fundamental na modernização da segurança eletrônica do Tribunal Regional Federal da 3ª Região (TRF-3). Um VMS moderno não é apenas um sistema de gravação de vídeo, mas sim uma plataforma centralizada que integra diversas tecnologias e funcionalidades para aprimorar a vigilância, a detecção de ameaças e a resposta a incidentes.

4.7.2. FUNCIONALIDADES ESSENCIAIS DE UM VMS INTELIGENTE

4.7.2.1. Gestão centralizada de câmeras

a) Suporte para uma ampla variedade de câmeras IP de diferentes fabricantes e modelos.

b) Configuração remota das câmeras, incluindo ajustes de imagem, configurações de rede e agendamento de gravações.

c) Monitoramento do status das câmeras, com alertas automáticos em caso de falhas ou desconexões.

4.7.2.2. Gravação e armazenamento de vídeo

a) Gravação contínua, por agendamento ou por evento.

b) Suporte para diferentes codecs de vídeo (H.264, H.265) e resoluções (HD, 4K).

c) Armazenamento de vídeo em servidores locais, em nuvem ou em uma combinação de ambos.

d) Gestão eficiente do armazenamento, com políticas de retenção e arquivamento de vídeo.

4.7.2.3. Análise de vídeo inteligente (IVA)

a) Integração com algoritmos de inteligência artificial (IA) para detecção de anomalias comportamentais, reconhecimento facial avançado, leitura de placas veiculares inteligente e análise de objetos abandonados.

b) Configuração de regras e alertas para identificar eventos de interesse.

c) Visualização dos resultados da análise de vídeo em tempo real.

4.7.2.4. Gestão de alarmes e eventos

a) Integração com sistemas de alarme, controle de acesso e outros dispositivos de segurança.

b) Recebimento de alertas em tempo real sobre incidentes de segurança.

c) Visualização das imagens das câmeras associadas aos alarmes.

d) Gestão de alarmes, com atribuição de responsabilidades, acompanhamento do status e geração de relatórios.

4.7.2.5. Acesso remoto e mobile

a) Acesso seguro ao sistema a partir de qualquer dispositivo com acesso à internet (computadores, tablets, smartphones).

b) Visualização das imagens das câmeras em tempo real.

c) Reprodução de vídeos gravados.

d) Gestão de alarmes e eventos.

4.7.2.6. Integração com outros sistemas

a) Integração com sistemas de controle de acesso, sistemas de alarme, sistemas de gestão de edifícios e outros sistemas de segurança.

b) Troca de informações entre os diferentes sistemas para automatizar tarefas e coordenar a resposta a incidentes.

4.7.2.7. Segurança cibernética

a) Criptografia das comunicações e dos dados armazenados.

b) Autenticação multifator (MFA) para todos os usuários.

c) Controles de acesso rigorosos para proteger o sistema contra acessos não autorizados.

d) Auditoria de todas as atividades realizadas no sistema.

4.7.3. BENEFÍCIOS DA IMPLEMENTAÇÃO DE UM VMS INTELIGENTE

4.7.3.1. **Aumento da Eficiência da Vigilância:** A análise de vídeo inteligente permite que os operadores se concentrem em eventos de interesse, reduzindo a fadiga e aumentando a eficiência da vigilância.

4.7.3.2. **Detecção Proativa de Ameaças:** A IA permite a detecção precoce de ameaças, como comportamentos suspeitos e invasões de perímetro.

4.7.3.3. **Resposta Rápida a Incidentes:** A integração com outros sistemas e a automação de tarefas permitem uma resposta rápida e coordenada a incidentes.

4.7.3.4. **Melhoria da Gestão da Segurança:** A plataforma centralizada do VMS facilita a gestão da segurança, permitindo o monitoramento, o controle e a análise de dados a partir de um único local.

4.7.3.5. **Redução de Custos Operacionais:** A automação de tarefas e a melhoria da eficiência da vigilância reduzem os custos operacionais.

4.7.3.6. **Conformidade com Normas e Regulamentações:** Um VMS inteligente pode ajudar o TRF-3 a cumprir as normas e regulamentações de segurança, como a Lei Geral de Proteção de Dados (LGPD).

4.8. IMPLEMENTAÇÃO DE SISTEMA DE LEITURA DE PLACAS (LPR)

4.8.1. Implementação de sistemas de leitura de placas (LPR) para controlar o acesso a áreas restritas e monitorar o movimento de veículos. A solução deve incluir câmeras com alta capacidade de captura de imagem e software de análise de vídeo com algoritmos de IA para reconhecimento e leitura de placas.

4.8.2. Os sistemas de LPR aumentarão a segurança institucional, permitindo a identificação de veículos de interesse e a geração de alertas automáticos.

4.9. IMPLEMENTAÇÃO DE SISTEMA DE RECONHECIMENTO FACIAL

4.9.1. Além de identificar e monitorar pessoas, faz parte do escopo do sistema de reconhecimento facial estabelecer a Segurança Preventiva, com mecanismos para inibir e prevenir ações altamente perigosas:

a) Identifica itens suspeitos em meio a multidões (caso de passeatas e protestos nas proximidades);

b) Monitorar o comportamentos suspeitos em tempo real usando inteligência artificial, tais como brigas, roubos, sequestros, ou em casos da necessidade de ajuda iminente como crianças em situação de vulnerabilidade, superlotação, roubo, etc.

4.9.2. Uma vez detectada a pessoa ou grupo, o sistema emite um alarme para o Centro de Operações que em poucos segundos pode realizar a verificação da ocorrência.

4.9.3. Nessa verificação, o sistema pode identificar situações anômalas no banco de dados ou em caso da inexistência de registros, configurando que a pessoa pode estar custodiada, é inválida, é um estrangeiro ilegal, cuja permanência no país não é autorizada.

4.9.4. Em tais situações ou situações semelhantes, uma vez identificado o contexto da pessoa, esta pode ser introduzida no sistema, depois de devidamente identificada, ou pode ser conservada para posterior tratamento.

4.9.5. DIAGRAMA DE FUNCIONAMENTO

4.9.5.1.

1) **Seguimento de rosto ou face:** Encontra e reconhece rostos dentro de fluxos de vídeo.
2) **Identificação de pessoas:** Realiza a busca e similaridades de rostos e faces de uma base de dados em um fluxo de vídeo.
3) **Armazenamento e análise de dados:** Armazena todos os eventos de reconhecimento e disponibiliza informações.
4) **Notificação:** Notifica o operador das similaridades encontradas na base de dados.
5) **Ações de reação rápida:** Através da integração com sistemas de terceiros, proporciona uma ação de reação rápida que pode ser automatizada ou não.

4.9.6. POSSIBILIDADES FUNCIONAIS

4.9.6.1. 99% das pessoas estão corretamente identificadas durante testes realizados em ambiente real;

4.9.6.2. Cada câmera rastreia até 30 faces em um quadro de análise ao mesmo tempo;

4.9.6.3. O resultado da identificação deve ser obtido em menos de 1 segundo;

4.9.6.4. Deve possibilitar o armazena mais de 100.000.000 de amostras;

4.9.6.5. Deve ser resistente a várias alterações físicas e reconhecimento de características únicas (penteados, barbas, bigodes, chapéus, envelhecimento, etc.);

4.9.6.6. Com base na triangulação vetorial 3D deve gerar hash com assinatura de cada face.

4.9.6.7. Deve possuir tecnologia de Deep Learning de IA em cada reconhecimento bem-sucedido.

4.9.6.8. Deve possuir processo de autoaprendizagem por meio de experimentação de Deep Learning de várias etnias.

4.9.6.9. Deve possuir uma assertividade superior a 99%, comprovada pelo processo de autoaprendizagem através da

experimentação por processo de Deep Learning utilizando-se várias etnias.

4.9.6.10. Deve possuir reconhecimento não cooperativo do objeto focal em câmeras fixas e PTZ.

4.9.6.11. Deve possibilitar a gestão de listas (bandidos, Interpol, pessoas desaparecidas, mandados de detenção, etc.).

4.9.6.12. Deve gerar alertas em tempo real com indicação do perímetro de aproximação.

4.9.6.13. Deve possuir funcionalidade para controle de perímetro, para aplicação de medidas restritivas e protetivas.

4.9.6.14. Deve possibilitar a pesquisa de qualquer rosto que tenha aparecido, independentemente de estar registrado ou não.

4.9.7. DETECÇÃO DE MÁSCARAS

4.9.7.1. Os algoritmos devem ser adaptados para reconhecer máscaras e respiradores de vários modelos e cores;

4.9.7.2. Deve possibilitar o registro de cada caso mediante ausência de máscara no arquivo de foto;

4.9.7.3. Reconhecimento de pessoas sem máscaras;

4.9.7.4. Verificação se as máscaras são ou não usadas corretamente.

4.9.8. ÁREAS RESTRITAS

4.9.8.1. A integração com sistema GPS/GIS ou mapas que permita ver as câmeras instaladas em diferentes locais.

4.9.8.2. Deve possibilitar identificar a intrusão em uma área restrita ou que a pessoa não possua autorização conforme cadastro no sistema de controle de acesso, gerando alertas em tempo real.

4.9.8.3. A visualização no mapa deve permitir que centro de comando e controle tome medidas o mais rápido possível.

4.9.8.4. O sistema também deve permitir localizar pessoas desaparecidas e perdidas dentro das dependências monitoradas.

4.9.9. RELATÓRIOS ANALÍTICOS

4.9.9.1. Deve apresentar informações sobre os horários de chegada e partida de qualquer cidadão, viajante, funcionário ou imigrante;

4.9.9.2. Deve conter informação sobre a hora de chegada e partida, bem como o paradeiro de qualquer uma delas;

4.9.9.3. Deve possibilitar a gestão de relatórios em tempo real de cidadãos e imigrantes, bem como mandados de prisão ou outras situações legais relevantes, incluindo pessoas desaparecidas;

4.9.9.4. Deve fornecer estatísticas do perfil de visitantes.

4.10. APRIMORAMENTO DA INFRAESTRUTURA DE REDE

4.10.1. Aprimoramento da infraestrutura de rede com a substituição dos comutadores Cisco Catalyst 2950 e 2960-S PoE+ por modelos mais modernos (Cisco 9200L ou superior) e a implementação de um sistema de cabeamento estruturado. A solução deve garantir a capacidade, o desempenho, a confiabilidade e a segurança da rede.

4.10.2. A infraestrutura de rede atual apresenta limitações em termos de capacidade e desempenho, o que pode dificultar

a implementação de novas tecnologias e a garantia da confiabilidade dos sistemas de segurança. A modernização da infraestrutura de rede permitirá que o TRF-3 suporte as novas tecnologias de segurança e garanta a disponibilidade contínua dos sistemas.

4.11. IMPLEMENTAÇÃO DE UM CENTRO DE OPERAÇÕES DE SEGURANÇA (SOC)

4.11.1. Implementação de um Centro de Operações de Segurança (SOC) para monitorar continuamente os sistemas de segurança, detectar incidentes e coordenar a resposta. A solução deve incluir equipamentos de monitoramento, software de análise de segurança, sistemas de comunicação e pessoal treinado.

4.11.2. O SOC permitirá que o TRF-3 monitore continuamente os sistemas de segurança, detecte incidentes em tempo real e responda rapidamente a ameaças.

4.12. AQUISIÇÃO DE SOFTWARE DE ANÁLISE DE VÍDEO INTELIGENTE (IVA)

4.12.1. Aquisição de software de análise de vídeo inteligente (IVA) com algoritmos de IA para detecção de anomalias comportamentais, reconhecimento facial avançado, leitura de placas veiculares inteligente e análise de objetos abandonados, contagem de pessoas, detecção de fogo e fumaça, análise de aglomeração, investigação forense de vídeo em tempo real, e com a possibilidade de criar algoritmos personalizados com base em instruções de linguagem natural situacional que possam ser testados em imagens detectadas por câmeras de forma a permitir a categorização em regras de alarme de forma personalizada.

4.12.2. O software de IVA permitirá que o TRF-3 detecte proativamente ameaças, identifique pessoas de interesse e responda rapidamente a incidentes.

4.13. IMPLEMENTAÇÃO DE UM SISTEMA DE GESTÃO DE IDENTIDADE E ACESSO (IAM)

4.13.1. Implementação de um sistema de gestão de identidade e acesso (IAM) para controlar o acesso aos sistemas de segurança e garantir a autenticação multifator (MFA) para todos os usuários.

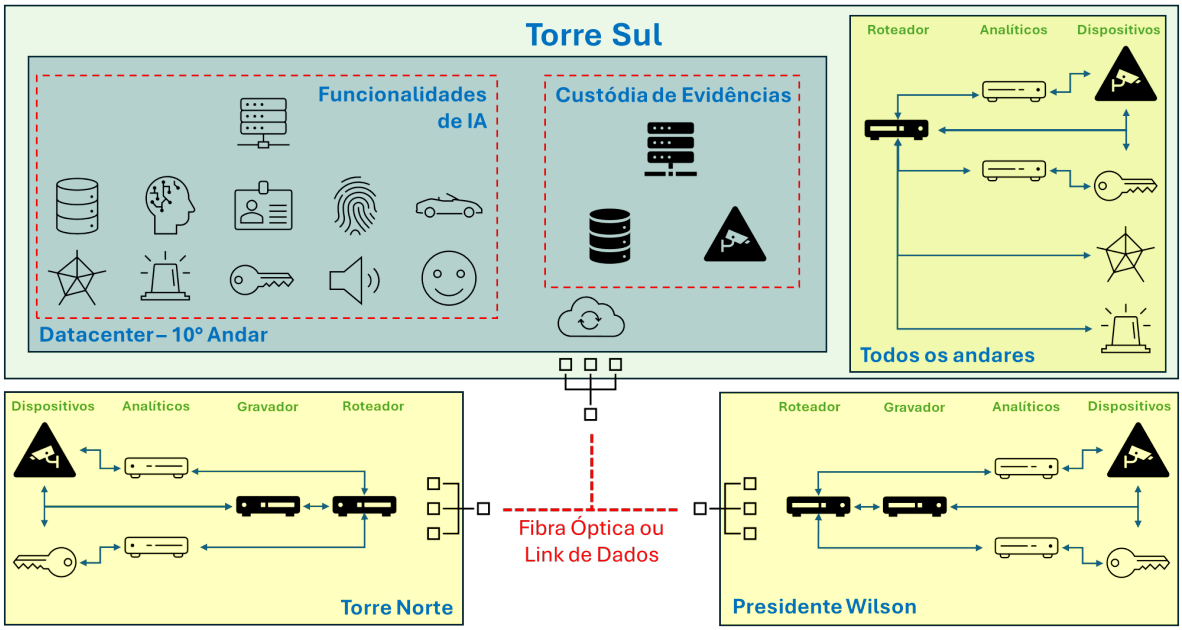
4.13.2. O sistema de IAM aumentará a segurança dos sistemas de segurança, garantindo que apenas pessoas autorizadas tenham acesso e que a autenticação seja realizada de forma segura.

4.14. AQUISIÇÃO DE COFRE DE ACAUTELAMENTO DE ARMAS

4.14.1. Aquisição de cofre de acautelamento de armas integrado ao sistema de controle de acesso com múltiplos níveis de autenticação (biometria digital, cartão de acesso, reconhecimento facial e senha).

4.14.2. O cofre de acautelamento de armas permitirá o armazenamento seguro das armas de fogo pertencentes a indivíduos com porte legal, mitigando o risco de ações de alto risco.

4.15. DIAGRAMA ILUSTRATIVO DA TOPOLOGIA DE REDE DOS NOVOS SISTEMAS



4.15.1.

4.16. INTEGRAÇÃO COM SISTEMA DE CONTROLE DE ACESSO

4.16.1. O sistema de controle de acesso a ser fornecido deve atender rigorosamente aos seguintes requisitos, garantindo interoperabilidade, segurança e escalabilidade:

4.16.2. ARQUITETURA E COMPATIBILIDADE

4.16.2.1. Deve suportar APIs abertas (RESTful, SOAP) para integração facilitada com sistemas externos, viabilizando a troca de dados e o acionamento de funcionalidades de forma padronizada.

4.16.2.2. Deve ser compatível com padrões industriais amplamente adotados, tais como ONVIF (para videomonitoramento), OSDP (dispositivos de controle de acesso), LPR (Reconhecimento de Placas) e SNMP (Monitoramento de Rede), garantindo a interoperabilidade com uma variedade de dispositivos e sistemas.

4.16.2.3. Deve suportar protocolos de segurança de comunicação robustos, incluindo HTTPS, TLS 1.2 (ou superior) e RTSP, para proteger a integridade e a confidencialidade dos dados transmitidos.

4.16.2.4. Deve centralizar todos os dados de eventos, como logs de acesso, registros de câmeras, leituras LPR e parâmetros de detecção facial, em uma base central unificada, permitindo a análise abrangente de metadados por sistemas de Business Intelligence (BI).

4.16.2.5. Deve adotar uma arquitetura modular baseada em microsserviços para suportar escalabilidade horizontal e vertical, facilitando a adição de novas funcionalidades e integrações futuras.

4.16.3. INTEGRAÇÃO COM SISTEMAS ASSOCIADOS

4.16.3.1. Deve, no contexto de Videomonitoramento Inteligente com Analíticos baseados em IA, permitir que pontos de entrada sejam vinculados ao sistema de videomonitoramento, de forma que a identificação de um usuário ou suspeito

acione o rastreamento progressivo em outros ambientes por meio das câmeras vinculadas.

4.16.3.2. Deve oferecer uma interface de troca de dados via API para vincular logs de acesso com capturas de vídeo em cada ponto de controle, fornecendo contexto visual para eventos de acesso.

4.16.3.3. Deve receber alertas gerados por sistemas de IA (por exemplo, detecção de comportamento suspeito em vídeo) para bloquear ou restringir dinamicamente zonas de acesso, aumentando a segurança proativamente.

4.16.3.4. Deve, no contexto de Sistema de Leitura de Placas (LPR), integrar-se aos dispositivos de LPR para controlar automaticamente cancelas e outras barreiras de acesso veicular.

4.16.3.5. Deve suportar consultas de placas e comparação com listas específicas (permitidos ou restritos), permitindo a gestão de acessos veiculares baseada em listas.

4.16.3.6. Deve enviar dados de eventos (por exemplo, veículo permitido, visitante cadastrado) ao módulo de Business Intelligence para análise e geração de relatórios.

4.16.3.7. Deve, no contexto de Sistema de Detecção e Reconhecimento Facial, associar imagens faciais capturadas em tempo real aos logs da controladora e aos registros pré-cadastrados, facilitando a identificação e o registro de acessos.

4.16.3.8. Deve implementar recursos de alerta instantâneo em caso de identificação positiva de pessoas em listas de suspeitos, permitindo uma resposta rápida a potenciais ameaças.

4.16.3.9. Deve possibilitar o rastreamento de indivíduos pelas câmeras vinculadas com base na triangulação entre pontos de identificação facial e logs de acesso, otimizando o rastreamento em ambientes monitorados.

4.16.3.10. Deve, no contexto de Sistema de Alarmes Perimetrais, registrar e tratar automaticamente eventos provenientes de alarmes perimetrais, como intrusões em áreas restritas, elevando o nível de segurança e resposta.

4.16.3.11. Deve automatizar respostas a eventos de alarme, incluindo o bloqueio de portas, a ativação de torniquetes ou cancelas, e o envio de alertas ao sistema de videomonitoramento, garantindo uma resposta coordenada a incidentes.

4.16.3.12. Deve, no contexto de Sistema de Detecção de Incêndio, monitorar continuamente os alertas de incêndio e permitir a abertura automática de portas e cancelas nas áreas impactadas em caso de emergência, seguindo um protocolo configurável.

4.16.3.13. Deve registrar eventos relacionados a incêndios e sincronizar os dados com a auditoria pós-incidente no sistema centralizado, fornecendo informações para análise e melhoria contínua.

4.16.4. FUNCIONALIDADES AVANÇADAS DE INTEGRAÇÃO

4.16.4.1. Deve habilitar o cercamento eletrônico, rastreando a movimentação de usuários e suspeitos em tempo real com base em dados de acesso, identificações por câmeras ou dispositivos de IA e alertas cruzados de alarmes perimetrais ou comportamentos irregulares.

4.16.4.2. Deve processar e analisar centralizadamente metadados para identificar padrões, tais como picos de movimentação em diferentes horários e zonas, tentativas de acesso de usuários em áreas restritas e análise preditiva de

movimentação e tendências comportamentais.

4.16.4.3. Deve emitir notificações inteligentes para os operadores via SMS, e-mail ou push notifications (dispositivos móveis) em casos de suspeitas, além de integrar-se com sistemas de monitoramento central para exibição em dashboards personalizados.

4.16.5. SEGURANÇA E RESILIÊNCIA

4.16.5.1. Deve proteger todos os dados com criptografia AES-256, tanto em trânsito quanto em repouso, garantindo a confidencialidade e a integridade das informações.

4.16.5.2. Deve registrar todos os eventos de comunicação entre sistemas integrados em logs detalhados para auditoria e rastreamento de atividades.

4.16.5.3. Deve garantir redundância para recuperação automática em caso de falha ou ataque, assegurando a continuidade das operações e a disponibilidade dos dados.

4.16.6. CONFORMIDADE E CERTIFICAÇÕES

4.16.6.1. Deve possuir a certificação ISO/IEC 27001 para garantir a implementação e a manutenção de boas práticas em segurança da informação.

4.16.6.2. Deve suportar requisitos legais como a LGPD, garantindo a confidencialidade e a proteção de dados pessoais envolvidos na integração.

4.16.7. RESILIÊNCIA OPERACIONAL E MONITORAMENTO REATIVO

4.16.7.1. Deve oferecer redundância completa na infraestrutura, com suporte para balanceamento de carga, failover automático e backup contínuo, garantindo a alta disponibilidade dos dados dos sistemas críticos.

4.16.7.2. Deve suportar o monitoramento contínuo de todos os sistemas e equipamentos conectados, com alertas automáticos para operadores em caso de falhas, exibindo o status em tempo real dos equipamentos.

4.16.7.3. Deve implementar protocolos rápidos para eventos de alto impacto, como evacuações devido a incêndios ou violações perimetrais detectadas, configurando automações adaptativas, como travamento de portas ou desligamento controlado de áreas.

4.16.8. FUNCIONALIDADES RECOMENDADAS PARA OPERADORES

4.16.8.1. Deve oferecer uma interface centralizada/dashboard para monitorar e controlar todos os sistemas integrados em um painel único e intuitivo, exibindo KPIs como alertas ativos, mapas de calor de movimentações e indicadores de presença de suspeitos e possíveis ameaças.

4.16.8.2. Deve permitir a personalização da interface por função, disponibilizando painéis ajustáveis para operadores, supervisores e equipes de segurança, cada um com o nível adequado de permissões e informações.

4.16.9. INTEGRAÇÃO DE METADADOS COM IA

4.16.9.1. Deve processar os dados capturados (acessos, leituras de placas, imagens de rostos, ativação de alarmes) por

algoritmos de inteligência artificial que correlacionam eventos em tempo real.

4.16.9.2. Deve utilizar a análise de dados para detectar anomalias comportamentais, como movimentações fora do padrão, aplicando machine learning para prever padrões e antecipar possíveis incidentes.

4.16.10. API ABERTA

4.16.10.1. Deve possuir uma API aberta, bem documentada e acessível, que permita a outros fabricantes e desenvolvedores de soluções a integração com o sistema de controle de acesso. A documentação da API deve incluir exemplos de código, esquemas de dados e guias de implementação para facilitar a integração.

4.17. INTEGRAÇÃO DO SISTEMA DE CONTROLE DE ACESSO COM SISTEMA DE ALARME DE INCÊNDIO

4.17.1. O sistema de controle de acesso a ser fornecido deve atender rigorosamente aos seguintes requisitos, garantindo interoperabilidade, segurança e escalabilidade, com ênfase na integração com sistemas de alarme de incêndio:

4.17.2. COMUNICAÇÃO E INTEROPERABILIDADE

4.17.2.1. Deve ser compatível com sistemas de alarme de incêndio que utilizam protocolos de comunicação amplamente aceitos, como BACnet, Modbus TCP/IP, ou OPC.

4.17.2.2. Deve suportar APIs abertas para troca de informações bidirecional em tempo real com o painel de incêndio.

4.17.2.3. Deve receber, processar e responder automaticamente a eventos de alarme de incêndio enviados pelo painel de detecção.

4.17.2.4. Deve manter comunicação contínua entre o controlador de acesso e os sensores de incêndio, proibindo zonas específicas à movimentação ou liberando acessos conforme os planos de contingência.

4.17.3. AUTOMAÇÃO DE RESPOSTAS

4.17.3.1. Deve destrancar automaticamente portas de emergência ou outras vias de saída na área afetada pelo alarme de incêndio, respeitando os padrões de execução do plano de evacuação.

4.17.3.2. Deve travar automaticamente zonas de risco identificadas, sinalizadas pelo alarme de incêndio, para evitar que indivíduos acessem áreas comprometidas.

4.17.3.3. Deve integrar dados gerados por sensores de presença ou videomonitoramento (via analíticos de IA) com alarmes de incêndio para localizar indivíduos que possam estar presos em zonas críticas.

4.17.3.4. Deve rastrear, em tempo real, a localização dos ocupantes e fornecer atualizações sobre a movimentação dentro das dependências, redirecionando rotas e facilitando o trabalho das equipes de resgate através de cercamento eletrônico.

4.17.4. MONITORAMENTO E NOTIFICAÇÃO

4.17.4.1. Deve exibir as informações de status do sistema de controle de acesso e do sistema de alarme de incêndio, incluindo alarmes ativos e rotas de evacuação, em um dashboard unificado.

4.17.4.2. Deve gerar mensagens automáticas, como envio de SMS, e-mails ou notificações no sistema central para

equipes de segurança e brigadas de incêndio, detalhando as ações tomadas pelo sistema de controle de acesso nas zonas afetadas.

4.17.4.3. Deve registrar logs detalhados de todos os eventos de acesso, bloqueios, aberturas e movimentações realizadas durante o incidente para auditoria e análise.

4.17.5. PRIORIDADES DE RESPOSTA

4.17.5.1. Deve permitir que operadores de emergência desativem, remotamente, regras de controle de acesso, como intertravamento entre portas, em caso de necessidade, priorizando ações automáticas previamente configuradas para situações críticas.

4.17.5.2. Deve haver sincronização entre o sistema de controle de acesso e dispositivos de sinalização sonora e luminosa (sirenes e luzes de evacuação), garantindo uma resposta coordenada.

4.17.6. CONFORMIDADE COM NORMAS TÉCNICAS

4.17.6.1. Deve ter certificação de conformidade com normas como:

a) NFPA 101 (Vida Segura): Prevenção de bloqueio de rotas de fuga.

b) ABNT NBR 9077: Saídas de emergência de edificações.

c) NFPA 72: Sistemas de detecção e alarme de incêndio.

4.17.6.2. Deve garantir contínuo funcionamento mesmo durante falhas de energia, utilizando baterias ou energia redundante conforme especificado pela ABNT NBR 17240.

4.17.7. RASTREAMENTO E LOCALIZAÇÃO

4.17.7.1. Deve, integrado ao alarme de incêndio, exibir em tempo real mapas de calor em uma planta das dependências, indicando a ocupação de áreas durante o incidente.

4.17.7.2. Deve localizar cada ocupante nas áreas seguras e inseguras, atualizando o ciclo de informações do controle, utilizando identidades associadas a crachás, biometria ou reconhecimento facial.

4.17.8. FUNCIONALIDADES ADICIONAIS PARA CENÁRIOS DE EMERGÊNCIA

4.17.8.1. Deve implementar comandos que liberam todas as portas de evacuação simultaneamente em caso de incidente crítico.

4.17.8.2. Deve oferecer função de busca de histórico para investigar o comportamento, acesso e trajetos seguidos por ocupantes durante ou antes do incidente de incêndio.

4.17.9. API ABERTA

4.17.9.1. Deve possuir uma API aberta, bem documentada e acessível, que permita a outros fabricantes e desenvolvedores de soluções a integração com o sistema de controle de acesso. A documentação da API deve incluir exemplos de código, esquemas de dados e guias de implementação para facilitar a integração.

5. DEMAIS REQUISITOS NECESSÁRIOS E SUFICIENTES À ESCOLHA DA SOLUÇÃO DE TIC

5.1. As definições de requisitos apresentadas neste Estudo Técnico Preliminar (ETP) constituem-se em uma versão simplificada das futuras especificações técnicas da solução a ser contratada. Todavia, de acordo com o artigo 11, inciso I, da IN SGD/ME nº 94/2022, devem possuir pelo menos a completude suficiente para selecionar adequadamente a natureza ou o tipo da solução e os recursos de TIC viabilizados.

5.2.

5.3. A tarefa de definir os requisitos da contratação com o detalhamento adequado para fazer uma boa escolha da solução nem sempre é fácil. Ela depende da complexidade da demanda e da colaboração entre os integrantes, a fim de garantir a compatibilidade entre os requisitos negociais e os tecnológicos e obter o melhor resultado possível. Assim sendo, os integrantes podem selecionar outros aspectos ou características relevantes com o objetivo de subsidiar as decisões e a escolha da melhor solução.

5.4. INTEGRAÇÃO E INTEROPERABILIDADE

5.4.1. A solução de segurança integrada deve ser capaz de se integrar e interoperar com os sistemas existentes no TRF-3, incluindo os sistemas de alarme, controle de acesso, gestão de edifícios e outros sistemas de segurança. A integração deve ser realizada de forma a garantir a troca de informações entre os diferentes sistemas e a automatização de tarefas.

5.4.2. A solução deve suportar protocolos de comunicação padronizados, como ONVIF, para facilitar a integração com câmeras e outros dispositivos de diferentes fabricantes. A solução deve oferecer APIs (Application Programming Interfaces) para permitir a integração com outros sistemas de software.

5.5. ESCALABILIDADE E FLEXIBILIDADE

5.5.1. A solução deve ser escalável e flexível para atender às necessidades futuras do TRF-3. A solução deve permitir a adição de novas câmeras, dispositivos e funcionalidades de forma fácil e econômica.

5.5.2. A solução deve ser baseada em uma arquitetura modular que permita a expansão gradual do sistema. A solução deve suportar diferentes tipos de câmeras, dispositivos e funcionalidades para atender às necessidades específicas de cada área monitorada.

5.6. SEGURANÇA CIBERNÉTICA

5.6.1. A solução deve garantir a segurança cibernética dos sistemas de videomonitoramento, protegendo as imagens gravadas e em tempo real contra acessos não autorizados, manipulação e ataques cibernéticos.

5.6.2. A solução deve implementar medidas de segurança para proteger as câmeras, a rede, os servidores de armazenamento e as estações de trabalho dos operadores. A solução deve seguir as melhores práticas de segurança cibernética e estar em conformidade com as normas e regulamentações aplicáveis.

5.7. DESEMPENHO E CONFIABILIDADE

5.7.1. A solução deve garantir o desempenho e a confiabilidade dos sistemas de videomonitoramento, garantindo a disponibilidade contínua das imagens e a resposta rápida a incidentes.

5.7.2. A solução deve ser projetada para suportar um grande número de câmeras e usuários simultâneos. A solução deve implementar soluções de redundância para garantir a disponibilidade dos sistemas em caso de falhas.

5.8. USABILIDADE E ACESSIBILIDADE

5.8.1. A solução deve ser fácil de usar e acessível para os operadores de segurança. A solução deve oferecer uma interface intuitiva e funcionalidades de busca e reprodução de vídeo eficientes.

5.8.2. A solução deve ser projetada para atender às necessidades dos operadores de segurança, com funcionalidades que facilitem a vigilância, a detecção de ameaças e a resposta a incidentes. A solução deve ser acessível para pessoas com deficiência, seguindo as diretrizes de acessibilidade web (WCAG).

5.9. MANUTENÇÃO E SUPORTE TÉCNICO

5.9.1. O fornecedor da solução deve oferecer serviços de manutenção e suporte técnico para garantir o bom funcionamento dos sistemas de videomonitoramento.

5.9.2. O fornecedor deve oferecer suporte técnico 24 horas por dia, 7 dias por semana. O fornecedor deve oferecer serviços de manutenção preventiva e corretiva. O fornecedor deve garantir a disponibilidade de peças de reposição.

5.10. TREINAMENTO

5.10.1. O fornecedor da solução deve oferecer treinamento para os operadores de segurança e outros usuários do sistema.

5.10.2. O treinamento deve abranger todos os aspectos da solução, incluindo a instalação, a configuração, a operação e a manutenção dos sistemas de videomonitoramento. O treinamento deve ser ministrado por profissionais qualificados e experientes.

5.11. CONFORMIDADE COM NORMAS E REGULAMENTAÇÕES

5.11.1. A solução deve estar em conformidade com as normas e regulamentações aplicáveis, incluindo a Lei Geral de Proteção de Dados (LGPD) e as normas do Conselho Nacional de Justiça (CNJ).

5.11.2. O fornecedor da solução deve garantir que a solução atenda aos requisitos de privacidade e segurança de dados estabelecidos pela LGPD e pelas normas do CNJ. O fornecedor deve fornecer documentação que comprove a conformidade da solução com as normas e regulamentações aplicáveis.

5.12. GARANTIA

5.12.1. A solução deve ser coberta por uma garantia que proteja o TRF-3 contra defeitos de fabricação e falhas de funcionamento.

5.12.2. A garantia deve ter uma duração mínima de 60 meses. A garantia deve cobrir todos os componentes da solução,

incluindo as câmeras, os servidores, o software e outros dispositivos.

5.12.2.1. O prazo de garantia contratual dos bens, complementar à garantia legal, é de, no mínimo, 60 (sessenta) meses, ou pelo prazo fornecido pelo fabricante, se superior, contado a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto.

5.12.2.2. A garantia será prestada com vistas a manter os equipamentos fornecidos em perfeitas condições de uso, sem qualquer ônus ou custo adicional para o Contratante.

5.12.2.3. A garantia abrange a realização da manutenção corretiva dos bens pelo próprio Contratado, ou, se for o caso, por meio de assistência técnica autorizada, de acordo com as normas técnicas específicas.

5.12.2.4. A garantia legal ou contratual do objeto tem prazo de vigência próprio e desvinculado daquele fixado no contrato, permitindo eventual aplicação de penalidades em caso de descumprimento de alguma de suas condições, mesmo depois de expirada a vigência contratual.

5.12.2.5. Entende-se por manutenção corretiva aquela destinada a corrigir os defeitos apresentados pelos bens, compreendendo a substituição de peças, a realização de ajustes, reparos e correções necessárias.

5.12.2.6. As peças que apresentarem vício ou defeito no período de vigência da garantia deverão ser substituídas por outras novas, de primeiro uso, e originais, que apresentem padrões de qualidade e desempenho iguais ou superiores aos das peças utilizadas na fabricação do equipamento.

5.12.2.7. Uma vez notificado, o Contratado realizará a reparação ou substituição dos bens que apresentarem vício ou defeito no prazo de até 5 (cinco) dias úteis, contados a partir da data de retirada do equipamento das dependências da Administração pelo Contratado ou pela assistência técnica autorizada.

5.12.2.8. O prazo indicado no subitem anterior, durante seu transcurso, poderá ser prorrogado uma única vez, por igual período, mediante solicitação escrita e justificada do Contratado, aceita pelo Contratante.

5.12.2.9. Na hipótese do subitem acima, o Contratado deverá disponibilizar equipamento equivalente, de especificação igual ou superior ao anteriormente fornecido, para utilização em caráter provisório pelo Contratante, de modo a garantir a continuidade dos trabalhos administrativos durante a execução dos reparos.

5.12.2.10. Decorrido o prazo para reparos e substituições sem o atendimento da solicitação do Contratante ou a apresentação de justificativas pelo Contratado, fica o Contratante autorizado a contratar fornecedor diverso para executar os reparos, ajustes ou a substituição do bem ou de seus componentes, bem como a exigir do Contratado o reembolso pelos custos respectivos, sem que tal fato acarrete a perda da garantia dos equipamentos.

5.12.2.11. O custo referente ao transporte dos equipamentos cobertos pela garantia será de responsabilidade do Contratado.

6. PROCESSO DE DESPACHO DE OCORRÊNCIAS AUTOMATIZADO

6.1. O sistema deverá permitir a gestão e controle para registro do recebimento e despacho de ocorrências, sejam as originadas na central de controle de ocorrência e atendimento manual, inseridas no sistema diretamente pelo agente da segurança interno do contratante através de dispositivo móvel (tablet, Celular) e Web, ou de gatilhos de alertas de blacklists de reconhecimento de placas, faces ou alarmes pré-configurados

6.2. REGISTRO E RECEBIMENTO DE OCORRÊNCIAS

6.2.1. **Automático:** Ocorrências registradas de forma automática por meio de notificações do sistema de videomonitoramento inteligente ou de controle de acesso, mediante regras pre-configuradas

6.2.2. **Central de controle:** Ocorrências registradas manualmente na central de controle

6.2.3. **Dispositivos móveis:** Inserção direta por agentes de segurança via tablets ou celulares

6.2.4. **Web:** Registro via interface web

6.2.5. **Gatilhos automáticos:** Alertas de blacklists de reconhecimento de placas, faces ou alarmes pré-configurados

6.2.6. **Integração de dados:** O sistema deve integrar dados de diversas fontes, como sistemas de alarme de incêndio, controle de acesso, videomonitoramento e leitura de placas, para gerar ocorrências automaticamente

6.3. CADASTRO DETALHADO DE OCORRÊNCIAS

6.3.1. Andar ou quadrante completo indicado no mapa

6.3.2. Natureza da ocorrência

6.3.3. Origem da ocorrência

6.3.4. Envolvidos (advertida, suspeita, testemunha, vítima, apreendida, presa ou somente envolvido)

6.3.5. Providências / ações tomadas

6.3.6. Armas apreendidas

6.3.7. Veículos e seus proprietários participantes da ocorrência

6.3.8. Agentes envolvidos

6.3.9. Cadastro de pessoas envolvidas

6.3.10. Outros órgãos

6.3.11. Fotos e imagens de CFTV

6.3.12. Imagens por dispositivos móveis

6.3.13. Leitura de placas e reconhecimento facial

6.3.14. Arquivos relativos anexados

6.3.15. Mapa referenciado e georreferenciado nativo integrado

6.4. FLUXO DE ATENDIMENTO E AÇÕES

6.4.1. **Registro de ações:** Registro de ações / providências tomadas durante o atendimento da ocorrência

6.4.2. **Bloqueio de alterações:** Após o encerramento da ocorrência, o sistema bloqueia a inserção e alteração de fatos / arquivos adicionais, permitindo apenas a consulta completa de alguns dados da ocorrência (Boletim, Entrega Envolvido, Entrega Objetos e outros)

6.5. VISUALIZAÇÃO EM MAPA

6.5.1. Mapa que exibe todas as ocorrências abertas com a sua respectiva localização e apresentação.

6.5.2. Permite traçar o mapa demonstrando as ocorrências em forma de marcadores.

6.5.3. Geração de mapa de calor das ocorrências encerradas

6.5.4. Localização para atender as ocorrências e apoiar o acesso a informação dos agentes integrados à central de controle.

6.5.5. Uso de dispositivo móvel para abertura e atendimento de ocorrências e suas providências

6.6. ANÁLISE DE INCIDÊNCIAS

6.6.1. **Separação por período:** Análise de incidências separando as ocorrências por período do dia, mês, ano e outras.

6.6.2. **Identificação de local e ocorrência:** Identificação do local e a ocorrência, agrupando as ocorrências por registros, tais como, envolvidos, tipos de apreensões, locais e outros órgãos ou instâncias.

6.6.3. **Integração e acompanhamento:** Objetivo de integrar operações e acompanhamento de serviços operacionais, através do sistema de mapas e georreferenciamento.

6.7. INTEGRAÇÃO COM SISTEMAS DE CÂMERAS

6.7.1. Permissão de cadastro de ocorrências pelo agente via sistema móvel integrado ao atendimento às ocorrências, com acesso a imagens e informações aos sistema de câmera com as imagens próximas ao local da ocorrência de forma georreferenciada.

6.7.2. Integração com CFTV, LPR, reconhecimento facial ou outros dispositivos de forma integrada, para apoiar o agente com informações.

6.8. CADASTROS E RELATÓRIOS

6.8.1. **Cadastros integrados:** O sistema deverá possuir todos os cadastros dos agentes, equipamentos de uso, acessórios de uso no apoio das atividades, fardamentos, armas, materiais consumíveis, cautelas, cursos, audiências, exames de rotina, boletim interno, escalas de serviços, prédios públicos, locais de ronda ou policiamento ostensivo, tabelas de uso.

6.8.2. **Relatórios e estatísticas:** Gerar relatórios, com apoio a gestão administrativa e gerar dados estatísticos para apoiar o gestor e ação dos agentes.

6.9. MONITORAMENTO DE AGENTES

6.9.1. **Integração com agentes:** Possuir no sistema uma forma integrada de análise das informações dos agentes com integração na computação embarcada, dispositivos móveis, com monitoramento contínuo dos agentes, que estão em uso

no atendimento das ocorrências.

6.9.2. **Análise de comportamento:** Análise e acompanhamento do comportamento, localização, habitualidade, desenho de rotas programadas e no atendimento e chegada em pontos com o registro de forma automática no sistema de gestão de forma a indicar no mapa, o andamento dos deslocamentos com os registros, localização e indicação das ocorrências nos mapas.

6.10. PAINEL E INDICADORES

6.10.1. Possuir, painel de indicador de ocorrência, com a identificação de indivíduos, tipos de ocorrências, prazos médios, categorização das ocorrências e gráficos representando as ações, com a distribuição das ocorrências e monitoramento.

6.11. LOCALIZAÇÃO REFERENCIADA

6.11.1. Possuir reconhecimento com geoprocessamento integrado para as ocorrências, agentes através de integração do sistema de rastreamento e aplicação móvel, pontos de videomonitoramento e leitura de placas, com mapas, de forma integrada.

6.12. ORDEM DE SERVIÇO

6.12.1. Possuir ordem de serviço, com pontos base para percorrer com tempo inicial e final

6.13. TECNOLOGIA DE ANÁLISES INTELIGENTES

6.13.1. **Análise de vínculo:** Possuir tecnologia para tratamento de dados de forma inteligente como análise de vínculo, apoio a atendimento de ocorrência, de forma integrada à solução de gestão.

6.13.2. **Inteligência com dados abertos:** Possuir a gestão de inteligência com base em dados abertos e dados dos convênios das instituições contratantes com outros órgãos de governos, Municipais, Estaduais, Federais e Internacionais.

6.13.3. **IA e processamento de dados:** Possuir na aplicação de técnicas de inteligência artificial e processamento de dados para identificação automática de entidades em conteúdos diversos como redes sociais, para apoiar no atendimento às ocorrências

6.13.4. **Monitoramento de redes sociais:** Possuir ao informar dados a leitura de redes sociais, o apoio ao atendimento de ocorrências abertura de eventos baseado nos contextos para verificação da situação.

6.13.5. **Regras de utilização:** Possuir regras de utilização do sistema de tratamento de dados de forma inteligente, para análise de veículo, pessoas físicas e jurídicas, de forma a gerenciar os perfis e permissões por usuários e grupos, e ter a análise do número de acessos a base de informações no uso do tratamento de dados de forma inteligente, para análise de vínculo, apoio a atendimento a ocorrência e integrado, conforme política de forma de uso do contratante.

6.13.6. **Busca de dados:** Possuir a busca de dados com as fontes de dados estruturados e não estruturados, com a extração de variáveis, análise de sentimentos com mineração de dados.

6.13.7. **Coleta e vinculação de dados:** Possuir a coleta e a vinculação de dados externos, inclusive redes sociais, com

informações de apoio a atendimento a ocorrências.

6.13.8. **Conformidade com LGPD:** Possuir os recursos para apoiar as atividades de origem de inteligência entre outras, através de fontes públicas e oficiais, 100% online e real time e podendo ser completamente integrada com o seu banco de dados Interno da instituição com apoio ao atendimento de ocorrências, com uso da tecnologia de análise de vínculos possibilita ao operador atendente a visualização de diferentes elementos funcionais e estruturais da apuração correspondente.

6.14. INTEGRAÇÃO COM LEITURA DE PLACAS, CFTV E RECONHECIMENTO FACIAL

6.14.1. A solução deve possuir integração, com o uso sistema de leitura de placa, circuito fechado de TV, reconhecimento facial, análise de objetos, com alertas, monitoramento automático, carros roubados, indícios de clonagem com alerta do proprietário, cadastro de veículo suspeito veículos monitorados, na lista de alerta, consulta a veículo, consulta de trajeto como linha do tempo, por placa, com a integração na solução proposta.

6.15. INTEGRAÇÃO COM SISTEMA DE TELEFONIA

6.15.1. A solução deve permitir a integração e através de APIs, com o sistema de gravação, de acordo com o padrão de comunicação do sistema de telefonia é composta por um servidor de aplicações interligado a um PABX e à rede de dados da instituição, o servidor de gravação é baseado em nuvem ou em um hardware PC Industrial no local, a ser configurado e já existentes no cliente, ou a ser fornecido ou ser contratado, mas a solução proposta está, preparada e apta às integrações, para o sistema de gravação das recepções das ligações, na central de atendimento e despacho, integrado com o sistema de gestão.

6.16. APLICAÇÃO NOS AMBIENTES DO TRF3

6.16.1. A solução deve permitir a integração e através de APIs, com o sistema de gravação, de acordo com o padrão de comunicação do sistema de telefonia é composta por um servidor de aplicações interligado a um PABX e à rede de dados da instituição, o servidor de gravação é baseado em nuvem ou em um hardware PC Industrial no local, a ser configurado e já existentes no cliente, ou a ser fornecido ou ser contratado, mas a solução proposta está, preparada e apta às integrações, para o sistema de gravação das recepções das ligações, na central de atendimento e despacho, integrado com o sistema de gestão.

6.16.2. TORRES NORTE E SUL

6.16.2.1. Integração com o sistema de controle de acesso para identificar e registrar a entrada e saída de pessoas e veículos.

6.16.2.2. Alertas automáticos em caso de acesso não autorizado ou tentativa de violação.

6.16.2.3. Monitoramento contínuo das áreas internas e externas das torres, com câmeras estrategicamente posicionadas.

6.16.2.4. Análise de vídeo inteligente para detectar comportamentos suspeitos, como aglomerações, invasões ou

vandalismo.

6.16.2.5. Integração com o sistema de alarme de incêndio para acionar automaticamente o despacho de equipes de emergência em caso de detecção de fumaça ou calor.

6.16.2.6. Visualização em tempo real das câmeras próximas ao foco do incêndio para auxiliar no combate e evacuação.

6.16.2.7. Utilização de reconhecimento facial para identificar pessoas procuradas ou com restrições de acesso, gerando alertas automáticos.

6.16.2.8. Despacho otimizado de agentes de segurança para atender às ocorrências, com base na localização, gravidade e recursos necessários.

6.16.3. HELIPORTO

6.16.3.1. Despacho otimizado de agentes de segurança para atender às ocorrências, com base na localização, gravidade e recursos necessários.

6.16.3.2. Monitoramento constante da área do heliporto, com câmeras de alta resolução e visão noturna.

6.16.3.3. Detecção automática de objetos estranhos na pista e alertas de aproximação de aeronaves não autorizadas.

6.16.3.4. Sistema de alarme de incêndio específico para ambientes com risco de explosão, com acionamento automático de sprinklers e espuma.

6.16.3.5. Comunicação direta com a torre de controle e equipes de resgate em caso de emergência.

6.16.4. DEPÓSITO JUDICIAL PRESIDENTE WILSON

6.16.4.1. Controle de acesso reforçado, com biometria, cartões de proximidade e senhas.

6.16.4.2. Monitoramento de alarmes de violação e tentativas de acesso não autorizado.

6.16.4.3. Cobertura total das áreas de armazenamento, com câmeras de alta resolução e sensores de movimento.

6.16.4.4. Análise de vídeo inteligente para detectar atividades suspeitas, como manipulação de objetos ou acesso a áreas restritas.

6.16.4.5. Sistema de alarme perimetral para detectar tentativas de invasão.

6.16.4.6. Realização de rondas virtuais por meio das câmeras, com agendamento automático e alertas em caso de desvios.

6.16.5. CONSIDERAÇÕES ADICIONAIS

6.16.5.1. **Integração com Outros Sistemas:** O sistema de despacho de ocorrências automatizado deve ser integrado com outros sistemas do TRF3, como o sistema de gestão de processos judiciais, o sistema de recursos humanos e o sistema de gestão de frotas.

6.16.5.2. **Privacidade e Segurança:** O sistema deve garantir a privacidade e a segurança dos dados, em conformidade com a Lei Geral de Proteção de Dados (LGPD).

6.16.5.3. **Capacitação:** É fundamental que os agentes de segurança e demais usuários do sistema recebam treinamento

adequado para operar e manter o sistema de forma eficiente.

6.16.5.4. **Manutenção:** O sistema deve ser submetido a manutenções preventivas e corretivas regulares para garantir seu bom funcionamento e prolongar sua vida útil.

7. RESPONSABILIDADE TÉCNICA E DIREITOS AUTORAIS

7.1. Este Definições Técnicas dos Sistemas foi elaborado em conformidade com as normas da Associação Brasileira de Normas Técnicas (ABNT) e considerando as melhores práticas de engenharia, com visão especializada nas áreas de segurança pública e privada. O estudo visa a viabilização técnica para a contratação de empresa especializada na execução da implementação da Solução de Expansão e Modernização do Sistema de Segurança Eletrônica , objeto deste termo de referência.

7.2. O conteúdo integral deste Estudo Técnico Preliminar é protegido por direitos autorais, sendo o Autor, M.Sc. Rodrigo Sagaseta de Oliveira Souza (CREA-SP: 5070834495), e a empresa RSSI Segurança e Tecnologia os detentores exclusivos de tais direitos. A utilização deste estudo é expressamente restrita ao órgão contratante, exclusivamente para fins de implementação da solução de expansão e modernização do sistema de segurança eletrônica, conforme Anotação de Responsabilidade Técnica (ART) CREA-SP - ART 2620250540031 e Contrato nº 04.043.10.2024, referente ao Processo Administrativo nº 0016551-52.2024.4.03.8000 do TRF3 - Tribunal Regional Federal da 3ª Região.

7.3. A reprodução, distribuição, divulgação ou utilização total ou parcial das informações contidas neste estudo para outros órgãos, entidades ou para finalidades distintas, somente poderão ser realizadas mediante prévia e expressa autorização por escrito do Autor, M.Sc. Rodrigo Sagaseta de Oliveira Souza, e da empresa RSSI Segurança e Tecnologia. O descumprimento desta disposição sujeitará o infrator às sanções legais cabíveis, nos termos da Lei nº 9.610/98 (Lei de Direitos Autorais).

8. APROVAÇÃO E DECLARAÇÃO DE CONFORMIDADE

8.1. Aprovo este volume que trata das Definições Técnicas dos Sistemas da Solução de Expansão e Modernização do Sistema de Segurança Eletrônica e atesto sua conformidade às disposições da Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022.

(assinado eletronicamente)
RAFAEL ANTUNES CHAGAS
Fiscal Técnico

(assinado eletronicamente)
UMBERTO MALAVOLTA JUNIOR
Fiscal Técnico