Registro de Documentos Contratuais

HISAQ - Histórico de Aquisições

Registro Nº 257122	Fornecedor: INTELBRAS S/A – INDÚSTRIA DE TELECOMUNICAÇÃO ELETRÔNICA BRASILEIRA			
	Objeto: Termo de Comodato para empréstimos de equipamentos e Prova de Conceito			
	Tp Doc. Contratual: ACORDO SEM REPASSE FINANCEIRO			
	Data Registro: 04/11/2025	Data Assinatura: 30/10/2025	UG Emitente: BRASILIA SEDE	Vigência: 30/10/2025 a 28/03/2026
	UG Executora: SUPGA/GAADM	UG Responsável: SUPGL	Contrato: null	Valor: R$ 0,00
	Fundamentações Legais :	Art. 30, caput, da Lei n° 13.303/2016.		

CONTRATO DE COMODATO, que celebram entre si **INTELBRAS S.A. INDÚSTRIA DE TELECOMUNICAÇÃO ELETRÔNICA BRASILEIRA**, com sede na cidade de São José (SC), Distrito Industrial, BR 101, km 210, inscrita no CNPJ sob o nº 82.901.000/0001-27, doravante denominada "COMODANTE 1", **AIDC TECNOLOGIA LTDA**, com sede na Avenida Poços de Caldas, n. 148, Distrito Industrial, Itajubá (MG), inscrita no CNPJ 07.500.596/0001-38, doravante denominada "COMODANTE 2" e o – **SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS (SERPRO)**, empresa pública federal regida pela Lei nº 5.615, de 13/10/70, com sede em SGAN Quadra 601 Módulo "V", Brasília/Distrito Federal, inscrita no CNPJ sob o nº 33.683.111/0001-07, doravante designada "COMODATÁRIA", em conjunto denominadas PARTES, ajustam este Contrato de Comodato ("Contrato") de acordo com as seguintes cláusulas e condições:

CONSIDERANDO QUE:

- A COMODANTE 1 é a INTELBRAS S.A INDÚSTRIA DE TELECOMUNICAÇÃO ELETRÔNICA BRASILEIRA, esta ficará responsável por fornecer em caráter de empréstimo todos os softwares e hardwares (equipamentos) necessários à Prova de Conceito POC.
- A COMANDANTE 2 é a AIDC TECNOLOGIA LTDA, esta identificada como Integrador sugerido pela INTELBRAS considerando suas competências técnicas, ficará responsável por todos os serviços relacionados à implementação, instalação, configuração, integrações e sustentação da solução disponibilizada em regime de comodato.
- A COMODATÁRIA é a SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS (SERPRO) e deseja utilizar os produtos e serviços prestados pelas COMODANTES, firma-se o presente contrato.

CLÁUSULA PRIMEIRA – DO OBJETO

1.1. O objeto do presente Contrato é o empréstimo, não oneroso, pela COMODANTE 1 à COMODATÁRIA, dos bens e/ou do(s) software(s) especificados, todos em perfeito estado de conservação e uso, no Anexo 2 deste Contrato ("Bens e/ou do(s) software(s)").
1.2. Os Anexos 1, 2 e 3, rubricado pelas PARTES, integram este Contrato.
1.3. Este comodato tem como único objetivo a realização de Prova de Conceito (POC) para demonstrar as funcionalidades e desempenhos dos bens e/ou do(s) software(s) a serem testados pela COMODATÁRIA.
1.4. Dentro do Anexo 1, o COMODANTE 1 descreve de forma detalhada todos os requisitos necessários para que a COMODATÁRIA possa executar as atividades inerentes a esta POC dentro do ambiente esperado pela COMODATÁRIA.
1.5. A COMODATÁRIA declara disponibilidade em realizar os testes, comprometendo-se a responder aos questionamentos das COMODANTES e contribuir com insumos, com o intuito de contribuir para a correção e o aprimoramento da Solução em teste.
1.6. Todos os serviços relacionados à implementação, instalação, configuração~, integração e sustentação da solução disponibilizada em regime de comodato, bem como o fornecimento de possíveis acessórios, imprescindíveis a solução, que não sejam fornecidos pela INTELBRAS, serão de responsabilidade da empresa integradora AIDC TECNOLOGIA LTDA, inscrita no CNPJ sob o nº 07.500.596/0001-38, sem qualquer ônus para a COMODATÁRIA. À COMODANTE 1, caberá exclusivamente a disponibilização dos produtos em comodato e a substituição dos equipamentos, em caso de defeito de fabricação.

CLÁUSULA SEGUNDA – DA CONFIDENCIALIDADE

2.1. Este Contrato atenderá aos princípios da boa-fé, confiança e lealdade, devendo as PARTES, por si, seus empregados ou terceiros, abster-se de adotar conduta que prejudique os interesses da outra, seus clientes ou terceiros.
2.2. Nenhuma das PARTES divulgará, anunciará ou publicará os termos e condições deste Contrato sem o prévio consentimento por escrito da outra PARTE.
2.3. Os termos e condições deste Contrato, e demais documentos a ele relacionados, serão consideradas informações confidenciais, não podendo ser divulgadas a terceiros. O Acordo de Confidencialidade – Non Diclosure Agreement (NDA) assinado pelos COMODANTES e COMODATÁRIA, fará parte integrante desse contrato.

CLÁUSULA TERCEIRA – VIGÊNCIA

3.1. O prazo de vigência deste Contrato será de 150 (cento e cinquenta) dias a contar da data de sua assinatura.

3.2. O prazo de vigência poderá ser prorrogado somente mediante assinatura de termo aditivo.
3.3. Atingido o prazo de vigência deste Contrato ou em caso de rescisão, a COMODATÁRIA devolverá imediatamente à COMODANTE 1 a solução e os itens a ela vinculados.

CLÁUSULA QUARTA – CONDIÇÕES DO EMPRÉSTIMO

4.1. A instalação e desinstalação dos bens e do(s) software(s) serão feitas pela COMODANTE 2 e COMODATÁRIA.
4.2. A COMODATÁRIA se obriga a utilizar os bens e o(s) software(s) com observância das normas constantes do manual técnico, respondendo por eventuais danos causados.
4.3. A COMODATÁRIA concorda em utilizar os Bens, durante a vigência do presente, em conformidade com as disposições da Licença de Software fornecida juntamente com os Bens.
4.4. A COMODATÁRIA concorda que os Bens não serão licenciados, emprestados, cedidos, onerados ou vendidos ou de qualquer forma alterados durante a vigência do presente Contrato. Os Bens são entregues no estado em que se encontram, devidamente identificados como sendo de titularidade da COMODANTE, junto com materiais acessórios.
4.5. Após o término do prazo do Contrato, a COMODATÁRIA se obriga a tornar disponíveis os Bens para a COMODANTE 2, no prazo de 30 (trinta) dias úteis, em perfeitas condições de conservação e funcionamento, ressalvado o desgaste natural pelo uso.
4.6. A COMODANTE 1 confirma que detém os Direitos de Propriedade Intelectual da Solução ou atua como representante comercial legalmente autorizado do detentor dos Direitos de Propriedade Intelectual da Solução.
4.7. Eventuais softwares de propriedade de terceiros, ferramentas de interoperabilidade e condições adicionais aplicáveis que possam estar integrados à Solução serão devidamente identificados e caracterizados pela COMODANTE.
4.8. A COMODANTE 1 se declara ciente de que o referido comodato não configura compromisso de aquisição ou contratação da solução por parte da COMODATÁRIA.
4.9. A COMODANTE 1 se responsabiliza a fornecer à COMODATÁRIA suporte à realização das atividades de avaliação da Solução, durante todo o período previsto para sua duração, em horário comercial.
4.10. As despesas necessárias à plena execução do objeto disponibilizado à COMODATÁRIA, tais como desenvolvimento do sistema, serviços de terceiros, deslocamento, comunicação entre as Partes ou a órgãos fiscalizadores ou reguladores e outras que se fizerem necessárias, correrão por conta da COMODANTE 1.

CLÁUSULA QUINTA – OBRIGAÇÕES ESPECÍFICAS DO COMODATÁRIO

5.1. A COMODATÁRIA obriga-se a:

5.1.1. Conservar os Bens adequadamente, de modo a preservar a segurança e o perfeito funcionamento destes, notificando a COMODANTE 1 sempre que houver necessidade de reparos;

5.1.2. Proteger e defender a posse e a propriedade da COMODANTE 1 sobre os Bens, comunicando, imediatamente e por escrito, qualquer tentativa de esbulho ou turbação inclusive penhora ou qualquer tipo de ônus ou encargo, desse direito;

5.1.3. Fazer uso adequado dos Bens;

5.1.4. Não introduzir modificações de quaisquer espécies, ou remover as plaquetas de identificação e numeração, sem o consentimento prévio, por escrito, da COMODANTE 1;

5.1.5. Não transferir os Bens do local de instalação, reconhecendo que os Bens especificados no Anexo I são de propriedade da COMODANTE 1 e não poderão ser removidos do endereço da COMODATÁRIA sem a expressa concordância prévia da COMODANTE 1;

5.1.6. Responder pelos danos decorrentes do uso indevido ou da operação inadequada dos Bens.

5.1.7. Da Proteção de Dados Pessoais

5.1.7.1.A COMODATÁRIA e as COMODANTES se comprometem a proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, relativos ao tratamento de dados pessoais, inclusive nos meios digitais, garantindo que:

a) o tratamento de dados pessoais dar-se-á de acordo com as bases legais previstas nas hipóteses dos arts. 7º, 11 e/ou 14 da Lei 13.709/2018 às quais se submeterão os serviços, e para propósitos legítimos, específicos, explícitos e informados ao titular;

b) o tratamento seja limitado às atividades necessárias para o alcance das finalidades do serviço contratado ou, quando for o caso, ao cumprimento de obrigação legal ou regulatória, no exercício regular de direito, por determinação judicial ou por requisição da ANPD;

c) em caso de necessidade de coleta de dados pessoais dos titulares mediante consentimento, indispensáveis à própria prestação do serviço, esta será realizada após prévia aprovação da COMODATÁRIA, responsabilizando-se a COMODANTE 2 pela obtenção e gestão. Os dados assim coletados só poderão ser utilizados na execução dos serviços especificados neste contrato, e em hipótese alguma poderão ser compartilhados ou utilizados para outros finalidades;

c.1) eventualmente, podem as partes convencionar que a COMODATÁRIA será responsável por obter o consentimento dos titulares;

d) os sistemas que servirão de base para armazenamento dos dados pessoais coletados, seguem um conjunto de premissas, políticas, especificações técnicas, devendo estar alinhados com a legislação vigente e as melhores práticas de mercado;

e) os dados obtidos em razão deste contrato serão armazenados em um banco de dados seguro, com garantia de registro das transações realizadas na aplicação de acesso (log), adequado controle baseado em função (role based access control) e com transparente identificação do perfil dos credenciados, tudo estabelecido como forma de garantir inclusive a rastreabilidade de cada transação e a franca apuração, a qualquer momento, de desvios e falhas, vedado o compartilhamento desses dados com terceiros;

e.1) no caso de haver transferência internacional de dados pessoais pelas COMODANTES, para atender ao acima, estas garantem que:

e.1.1) a legislação do país para o qual os dados foram transferidos, asseguram o mesmo nível de proteção que a legislação brasileira em termos de privacidade e proteção de dados, sob pena de encerramento da relação contratual, em vista de restrição legal prevista no ordenamento jurídico brasileiro;

e.1.2) os dados transferidos serão tratados em ambiente da COMODANTE 1;

e.1.3) o tratamento dos dados pessoais, incluindo a própria transferência, foi e continuará a ser feito de acordo com as disposições pertinentes da legislação sobre proteção de dados aplicável e que não viola as disposições pertinentes do Brasil;

e.1.4) sempre que necessário, orientará a COMODATÁRIA durante o período de tratamento de dados pessoais, também em relação aos dados transferidos para país estrangeiro, para que ocorra em conformidade com a legislação sobre proteção de dados aplicável e com as cláusulas do contrato;

e.1.5) oferecerá garantias suficientes em relação às medidas de segurança técnicas e organizativas, e as especificará formalmente ao contratante, não compartilhando dados que lhe sejam remetidos com terceiros;

e.1.6) as medidas de segurança são adequadas para proteger os dados pessoais contra a destruição acidental ou ilícita, a perda acidental, a alteração, a divulgação ou o acesso não autorizados, nomeadamente quando o tratamento implicar a sua transmissão por rede, e contra qualquer outra forma de tratamento ilícito e que estas medidas asseguram um nível de segurança adequado em relação aos riscos que o tratamento representa e à natureza dos dados a proteger, atendendo aos conhecimentos técnicos disponíveis e aos custos resultantes da sua aplicação;

e.1.7) zelará pelo cumprimento das medidas de segurança;

e.1.8) tratará os dados pessoais apenas em nome da COMODATÁRIA e em conformidade com as suas instruções e as cláusulas do contrato; no caso de não poder cumprir estas obrigações por qualquer razão, concorda em informar imediatamente à COMODATÁRIA, que neste caso poderá suspender a transferência de dados e/ou de rescindir o contrato;

e.1.9) a legislação que lhe é aplicável não o impede de respeitar as instruções recebidas do SERPRO e as obrigações do contrato e que, no caso de haver uma alteração nesta legislação que possa ter efeito adverso substancial nas garantias e obrigações conferidas pelas cláusulas do contrato, comunicará imediatamente essa alteração à COMODATÁRIA, que neste caso poderá suspender a transferência de dados e/ou de rescindir o contrato;

e.1.10) notificará imediatamente a COMODATÁRIA sobre: qualquer solicitação juridicamente vinculativa de divulgação de dados pessoais por uma autoridade fiscalizadora responsável pela aplicação da lei, a menos que seja proibido de outra forma, como uma proibição da lei penal de preservar a confidencialidade de uma investigação policial; qualquer acesso acidental ou não autorizado;
e.1.11) responderá rápida e adequadamente todas as solicitações de informação da COMODATÁRIA, relacionadas ao tratamento dos dados pessoais objeto da transferência e que se submeterá aos conselhos da autoridade fiscalizadora no que diz respeito ao processamento dos dados transferidos;
e.1.12) a pedido da COMODATÁRIA, apresentará as informações necessárias sobre o tratamento relacionado com os dados pessoais objeto da transferência ou as informações solicitadas pela Autoridade fiscalizadora;
e.1.13) em caso de subcontratação, informará previamente a COMODATÁRIA que poderá anuir por escrito;
e.1.14) os serviços de processamento pelo subcontratado, serão executados de acordo com o disposto neste contrato;
e.1.15) enviará imediatamente à COMODATÁRIA uma cópia de qualquer acordo de subcontratação que celebrar sobre o objeto deste contrato.
5.1.7.2. As COMODANTES darão conhecimento formal aos seus empregados das obrigações e condições acordadas nesta cláusula, inclusive no tocante à Política de Privacidade da COMODATÁRIA.
5.1.7.3.O eventual acesso, pelas COMODANTES, às bases de dados que contenham ou possam conter dados pessoais ou segredos de negócio, implicará para as COMODANTES e para seus prepostos – devida e formalmente instruídos nesse sentido – o mais absoluto dever de sigilo, no curso do presente contrato e pelo prazo de até 10 anos contados de seu termo final.
5.1.7.4.As partes cooperarão entre si no cumprimento das obrigações referentes ao exercício dos direitos dos Titulares previstos na LGPD e nas Leis e Regulamentos de Proteção de Dados em vigor e também no atendimento de requisições e determinações do Poder Judiciário, Ministério Público, Órgãos de controle administrativo;
5.1.7.5.Uma parte deverá informar à outra, sempre que receber uma solicitação de um Titular de Dados, a respeito de Dados Pessoais da outra Parte, abstendo-se de responder qualquer solicitação, exceto nas instruções documentadas ou conforme exigido pela LGPD e Leis e Regulamentos de Proteção de Dados em vigor.
5.1.7.6.Os Encarregados das COMODANTES manterão contato formal com o Encarregado da COMODATÁRIA, no prazo de 24 (vinte e quatro) horas da ciência da ocorrência de qualquer incidente que implique violação ou risco de violação de dados pessoais de que venha a ter conhecimento ou suspeita, devendo a parte responsável, em até 10 (dez) dias corridos, tomar as medidas necessárias.
5.1.7.7. A critério do Encarregado de Dados da COMODATÁRIA, as COMODANTES poderão ser provocadas a colaborar na elaboração do relatório de impacto à proteção

de dados pessoais (RIPD), conforme a sensibilidade e o risco inerente dos serviços objeto deste contrato, no tocante a dados pessoais.
5.1.7.8.Encerrada a vigência do contrato ou não havendo mais necessidade de utilização dos dados pessoais, sensíveis ou não, as COMODANTES interromperão o tratamento e, em no máximo (30) dias, sob instruções e na medida do determinado pela COMODATÁRIA, eliminará completamente os Dados Pessoais e todas as cópias porventura existentes (em formato digital, físico ou outro qualquer), salvo quando necessite mantê-los para cumprimento de obrigação legal ou outra hipótese legal prevista na LGPD.
5.1.7.9.Eventuais responsabilidades das partes, serão apuradas conforme estabelecido neste contrato e de acordo com o que dispõe a Seção III, Capítulo VI da LGPD.

CLÁUSULA SEXTA – MANUTENÇÃO E TRANSPORTE DOS BENS

6.1. A COMODATÁRIA se compromete a realizar a calibração, a manutenção corretiva e preventiva dos Bens.
6.2. As despesas de embalagem e reembalagem, frete de transportes e seguro do transporte para entrega na COMODATÁRIA, correrão por conta da COMODANTE 1, que providenciará a retirada e transporte dos bens na comodatária, incluindo todos os encargos acessórios, no prazo máximo de 5 (cinco) dias úteis da solicitação da comodatária.

CLÁUSULA SÉTIMA – RESPONSABILIDADE CIVIL

7.1. As COMODANTES não assumem responsabilidade de qualquer natureza em razão do uso dos Bens pela COMODATÁRIA, desde que os Bens tenham sido comprovadamente entregues em perfeito estado de conservação e uso.
7.2. As PARTES não serão responsáveis por perdas e danos diretos, incidentes ou consequentes, incluindo lucros cessantes, ou quaisquer outras perdas e danos indiretos.
7.3. Quaisquer danos ocasionados aos Bens motivados pelo mau uso, abuso, desgaste ou alteração não autorizada, todos devidamente comprovados que foram ocasionados por culpa da COMODATÁRIA, deverão ser indenizados pela COMODATÁRIA à COMODANTE 1 pelo seu valor de nota fiscal na data de recebimento pela COMODATÁRIA, deduzida a depreciação proporcional ao tempo de utilização pela COMODATÁRIA, sem prejuízo da devolução à COMODANTE 1 dos respectivos Bens, ainda que danificados.
7.4. É devida indenização pela perda, deterioração total ou parcial, ou danos ocasionados aos Bens, enquanto estes estiverem na posse da COMODATÁRIA, se for comprovado que a COMODATÁRIA tenha dado causa.

CLÁUSULA OITAVA – RESCISÃO

8.1. Rescisão pela Comodante: as COMODANTES poderão, mediante aviso por escrito à COMODATÁRIA, rescindir motivadamente o Contrato no caso de a COMODATÁRIA cometer uma infração a este Contrato e não sanar a infração no prazo de 30 (trinta) dias após o recebimento da comunicação.
8.2. Rescisão pela Comodatária: a COMODATÁRIA poderá, mediante aviso por escrito às COMODANTES rescindir motivadamente o Contrato no caso de as COMODANTES cometerem uma infração a este Contrato e não sanar a infração no prazo de 30 (trinta) dias após o recebimento da comunicação.
8.3. Rescisão por Conveniência: Este Contrato poderá ser rescindido por qualquer das PARTES a qualquer tempo, independentemente de justo motivo e sem nenhum ônus, mediante envio de notificação à outra PARTE por escrito com 30 (trinta) dias de antecedência.

CLÁUSULA NONA – CONDIÇÕES GERAIS

9.1. A tolerância das PARTES não significará renúncia, perdão, novação ou alteração do pactuado.
9.2. É vedada a cessão deste Contrato bem como os direitos e obrigações dele decorrentes, sem o consentimento prévio e por escrito da outra PARTE.
9.3. Este Contrato constitui o integral acordo entre as Partes com relação ao seu objeto e sobrepõe-se a todos os acordos, propostas, informações, minutas e discussões anteriores, quer verbais, quer escritas, no tocante ao objeto contido neste Contrato. O presente Contrato somente poderá ser alterado por mútuo acordo por escrito entre as PARTES.
9.4. O atraso ou omissão, por qualquer das PARTES, em exercer qualquer direito ou poder decorrente deste Contrato não será considerado uma novação ou uma renúncia a tal direito ou poder. A tolerância por qualquer das Partes quanto ao não cumprimento de qualquer obrigação pelas demais, ou quanto a qualquer infração deste Contrato, não será considerada tolerância a qualquer outro descumprimento ou infração subsequente à mesma ou a qualquer outra obrigação contida neste Contrato.
9.5. Quaisquer direitos que não sejam concedidos à COMODATÁRIA sob este Contrato serão expressamente reservados à COMODANTE 1.
9.6. Toda e qualquer alteração contratual deverá ser formalizada por meio de termo aditivo específico submetido à análise jurídica, devidamente aprovado e assinado pelos seus respectivos representantes legais/prepostos.
9.7. Este Contrato deverá ser regido, interpretado e cumprido de acordo com as leis brasileiras e deverá ser tratado em todos os aspectos como contrato dessa jurisdição.
9.8. Ao formalizar o presente instrumento, as Partes se obrigam ao cumprimento dos seguintes documentos, disponíveis em https://www.intelbras.com/pt-br/contratos-clientes, sendo integrantes e indissociáveis do presente instrumento: Condições

Gerais de Contratação Intelbras - CGI; Política Intelbras de Proteção de Dados e Compliance.

CLÁUSULA DÉCIMA – FORO

10.1 Fica eleita a Legislação Brasileira como a que regerá os termos e condições deste Contrato.
10.2 Em caso de divergência, o idioma que deverá prevalecer para interpretação deste Contrato é o português.
10.3 Fica eleito o Foro da Justiça Federal da cidade de Brasília/DF para dirimir as dúvidas resultantes desse contrato.

E POR ESTAREM JUSTAS E CONTRATADAS, a COMODATÁRIA e as COMODANTES, qualificadas no preâmbulo assinam digitalmente o presente Contrato de Comodato.

INTELBRAS S.A. INDÚSTRIA DE TELECOMUNICAÇÃO ELETRÔNICA BRASILEIRA

Adriano Digiacomo

Gerente Executivo Administrativo e Jurídico

ASSINADO DIGITALMENTE
ADRIANO DIGIACOMO
DATA
30/10/2025
Data obtida do computador do assinante.
A conformidade com a assinatura pode ser verificada em:
https://serpro.gov.br/assinador-digital
Serpro

AIDC TECNOLOGIA LTDA

Emerson Ferreira da Fonseca

Diretor Geral

ASSINADO DIGITALMENTE
EMERSON FERREIRA DA FONSECA
DATA
29/10/2025
Data obtida de um servidor de tempo.
A conformidade com a assinatura pode ser verificada em:
https://serpro.gov.br/assinador-digital
Serpro

SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS (SERPRO)

Elayne Caroline Rosa Dal Col

Superintendente de Gestão Logística

ASSINADO DIGITALMENTE
ELAYNE CAROLINE ROSA DAL COL
CPF
32475100877
DATA
30/10/2025
A conformidade com a assinatura pode ser verificada em:
http://serpro.gov.br/assinador-digital
SERPRO

GESTOR DO CONTRATO (SERPRO)

Francisco Gualberto Santos Filho

Departamento de Obras e Infraestrutura de Instalações

ASSINADO DIGITALMENTE
FRANCISCO GUALBERTO SANTOS FILHO
CPF
63880792372
DATA
30/10/2025
Data obtida de um servidor de tempo.
A conformidade com a assinatura pode ser verificada em:
https://serpro.gov.br/assinador-digital
Serpro

ANEXO 1

ESPECIFICAÇÕES TÉCNICAS DA PROVA DE CONCEITO

1.Escopo

A Prova de Conceito (POC) para prospecção será focada na implementação e validação de um sistema integrado de gestão predial inteligente nos prédios do Serpro, utilizando tecnologias avançadas para monitoramento, segurança, eficiência operacional e sustentabilidade.

1.1. Componentes da PoC

1.1.1. Videomonitoramento e Controle de Acesso

- Implementação de um sistema moderno e integrado de videomonitoramento e controle de acesso para segurança predial;
- Controle de acesso eletrônico baseado em biometria facial, credenciais digitais e cartões, integrando câmeras e sensores para gerenciamento automatizado de entradas e saídas;
- Monitoramento das instalações em tempo real e geração de alertas para incidentes de segurança.
- Analíticos de vídeo para controles de perímetros e zonas.

1.1.2. Monitoramento Predial com IoT

- Instalação de sensores IoT para monitoramento em tempo real de variáveis como consumo de energia, temperatura, umidade, qualidade do ar e ocupação dos espaços.
- Coleta e análise de dados para otimizar a eficiência energética e melhorar a gestão dos recursos prediais.
- Implementação de dashboards para visualização e tomada de decisão baseada em dados.

1.1.3. Gerenciamento de Vagas de Estacionamento

- Utilização de câmeras e sensores para monitoramento da ocupação de vagas em tempo real.
- Implementação de um sistema de reserva e direcionamento de vagas para otimizar o uso do estacionamento.
- Integração com o sistema de controle de acesso para melhor gerenciamento do fluxo de veículos.

1.1.4. Carregamento de Veículos Elétricos

- Instalação de estações de carregamento para veículos elétricos no estacionamento.
- Monitoramento do uso e disponibilidade das estações via sistema integrado.
- Análise de consumo de energia e impacto na eficiência energética do prédio.

1.2. Integração e Gestão

1.2.1. Todos os componentes devem ser conectados a uma plataforma centralizada de gestão predial, permitindo o acompanhamento unificado das operações em tempo real.

1.2.2. O sistema integrará APIs e bases de dados corporativas para consolidar informações e otimizar a administração predial.

1.2.3. A POC avaliará a interoperabilidade entre os diferentes sistemas e a capacidade de escalabilidade da solução para futura implementação em larga escala.

2.Requisitos

2.1. Controle de acesso

Requisitos Gerais e Funcionais

2.1.1. O Sistema de Controle de Acesso deverá ser disponibilizado com todos os elementos necessários ao funcionamento do sistema, como controladores, leitores, estações de cadastramento, switches, servidor, infraestrutura completa, serviços de instalação e configuração.

2.1.2. O controle de acesso será composto de equipamentos de controle de acesso para portas e catracas, equipadas com leitoras de reconhecimento biométrico facial, leitoras de proximidade RFID (*Radio Frequency Identification* ou Identificação por Radiofrequência) com biometria e leitoras de proximidade RFID sem biometria.

2.1.3. A solução deverá ser capaz de controlar a passagem de elementos diversos, tais como: controle de veículos, empregados, prestadores de serviço, fornecedores e visitantes.

2.1.4. O sistema deve permitir:

a) O alerta para o operador quando o usuário tiver alguma restrição ao acesso;
b) O cadastramento de identificadores (cartões de proximidade) individualmente ou em lotes;
c) A configuração de servidor NTP;
d) A criação de status de usuários com a opção de bloqueio de acesso;
e) A captura de foto do momento do acesso;
f) Que o operador crie atalhos de funcionalidades para agilizar a operação.

2.1.5. O sistema deverá possuir perfeita integração com os dispositivos de reconhecimento facial.

2.1.6. O Sistema de Controle de Acesso deve ser concebido de tal forma que falhas locais não venham implicar falha de todo sistema. Controladores de acesso locais continuam a funcionar, mantendo a integridade dos níveis de acesso dos usuários, mesmo se a conexão de rede com o software de gerenciamento falhar.

2.1.7. Os dados necessários ao acesso deverão ser gravados nos equipamentos de borda de forma a realizar liberação e/ou bloqueio de usuários quando os equipamentos de borda estiverem operando off-line. Todos os registros de acesso (autorizados ou negados), incluindo data e hora, são armazenados na memória interna do equipamento e transferidos ao servidor tão logo a comunicação seja restabelecida. A base de dados de usuários deverá ficar armazenada na memória não-volátil local nos equipamentos de borda, sendo atualizada em tempo real pelo sistema de controle de acesso.

2.1.8. O Sistema de Controle de Acesso deve gerenciar datas de validade de usuários e cartões, e permitir a ativação de cartões provisórios.

2.1.9. O Sistema de Controle de Acesso deve fornecer uma maneira fácil de cadastrar cartões de acesso no banco de dados. Além dos dados básicos, como nome, sobrenome, número de crachá, foto e autorizações, as seguintes informações devem ser possíveis, mas não limitadas a:

a) Período de validade
b) Campos de tipos de usuários, no mínimo 6 classificações (empregados, conselheiros, visitantes etc.)
c) Campos de endereço
d) Dados Funcionais (matrícula, cargo e lotação)
e) Dados pessoais (nome e CPF)

2.1.10. Campos individuais podem ser adicionados, eliminados ou editados por administrador.

2.1.11. Prever diversas situações para controle de usuários, tais como ativos, inativos, férias, desligados.

2.1.12. O cadastramento biométrico (como impressões digitais e faciais) deve ser totalmente integrado no Sistema de Controle de Acesso, sem a necessidade de software de terceiros.

2.1.13. O cadastramento de biometria da falange e reconhecimento facial deve ser feito uma única vez, e propagado para os demais equipamentos.

2.1.14. O sistema de controle de acesso deve ter, no mínimo, as seguintes funcionalidades:

a) a capacidade de definir e gerenciar áreas lógicas arbitrárias no interior das instalações. Estas podem ser salas individuais, grupos de salas, andares inteiros ou áreas de estacionamento;
b) permitir a composição de níveis de acessos, agilizando o gerenciamento de múltiplos pontos de controle de uma mesma sala;
c) permitir a composição de níveis de acessos ilimitados;
d) permitir o controle do número máximo de elementos simultâneos em uma determinada área;
e) permitir a configuração de intertravamento entre as portas controladas;

2.1.15. A solução deverá conter rastreamento de pessoas para pesquisa forense, permitindo pesquisar uma pessoa em um banco de dados para todas as ações de entrada. Ex: uma porta pode ser pesquisada para todas as pessoas que passaram por esta, para a investigação de vídeo rápido.

2.1.16. Todas as gravações de imagens, sejam de videomonitoramento ou controle de acesso, devem ser mantidas em disco por pelo menos 30 dias corridos, após esse período o arquivo pode ser sobrescrito ou excluído automaticamente.

Controle de Acesso de Veículos

2.1.17. O controle de acesso de veículos deve ser realizado por meio de cancela automática, com sistema de leitura e reconhecimento de placas, permitindo:

a) Permitir configuração para controle de limite de vagas para veículos;
b) Permitir o acesso de veículos através da leitura da placa do veículo (LPR), com reconhecimento de placas de todo território nacional;
c) O sistema deve permitir liberação prévia a visitantes por meio de cadastramento de placa.
d) Permitir o cadastro de veículos, das placas e a associação com os respectivos proprietários.
e) Registrar e arquivar no banco de dados a imagem da placa, data, hora, número da placa e número de registro da placa (ID placa);
f) Deve possuir funcionalidades de compensação de distorção de vídeo e posição incorreta de placas capturadas de um veículo;
g) Deve ser capaz de armazenar uma sequência de vídeo completa associado ao resultado de reconhecimento de placas;

h) Deve fornecer ajuste de parâmetros de reconhecimento e grau de assertividade (permitir que o usuário insira uma placa não cadastrada ou não lida);
i) Permitir que o operador insira uma placa lida não cadastrada numa lista;
j) Extrair relatórios dos veículos capturados contendo informações de data, horário e número de placa, e
k) Analisar placas autorizadas e permitir passagem de veículo, abrindo cancelas de acesso aos estacionamentos, sem a intervenção de um operador.

Gestão de visitantes

2.1.18. Administração de visitantes deve ser fornecida pelo software de gerenciamento do sistema de controle de acesso no mesmo banco de dados.

2.1.19. A gestão de visitantes deve possuir os seguintes requisitos:

a) a solução deverá conter, ou possibilitar personalização, campos tais como: nome, documento oficial, foto, empresa de origem, cargo, telefone, e funcionário do SERPRO responsável pelo visitante.
b) permitir a captura de fotos de visitantes, com uso de câmeras nas portarias.
c) permitir controlar o número de trânsitos do visitante pelas catracas, tais como: apenas ida e ida-e-volta, e obrigatoriedade do uso da urna para saída de visitantes.
d) permitir a baixa automática do cartão do visitante após a passagem pela saída de visitantes, quando for utilizada urna associada à catraca.
e) permitir pelo menos 300.000 visitantes cadastrados ao sistema (na condição de inativos – dissociados de cartão RFID).
f) permitir a configuração de alarmes para visitas expiradas.
g) permitir o agendamento de visitas, a fim de agilizar a operação da recepção.
h) permitir identificar o motivo da visita.
i) permitir consultar ou sinalizar se o visitado está presente na empresa no momento da visita.
j) permitir o limite de visitantes por lotação ou faixa horária a uma área controlada;
k) permitir liberar uma visita a uma área controlada com capacidade total ou fora do horário programado mediante login e senha de operador com tal permissão.

Emergência

2.1.20. Permitir, em caso de emergência, a liberação e/ou bloqueio de controladoras de modo automático (sem intervenção de operador) ou manual (com intervenção de operador).

2.1.21. O Sistema de Controle de Acesso deve ser capaz de realizar o destravamento de todos os pontos através da interface cliente.

Monitoração

2.1.22. O software deve possuir tela de monitoramento de alarmes gerados por eventos da controladora e/ou dispositivos I/O's.

2.1.23. Permitir monitorar em tempo real o acesso dos usuários, mostrando os dados como:

a) Nome do usuário;
b) Foto do usuário
c) Número do crachá/identificador (se houver);
d) Nome da controladora/ponto de acesso;
e) Data e hora do acesso;
f) Método de identificação;

2.1.24. Permitir monitorar um ponto de acesso em tempo real com visualização de câmeras em tempo real.

2.1.25. A solução deverá ser capaz de personalizar as configurações de visualização de telas.

2.1.26. As configurações devem abranger no mínimo a permissão de emissão de som em caso de alarmes, tempo de atualização de informações na página de eventos e sobreposição de tela nos eventos com maior prioridade.

Segurança e Administração do sistema

2.1.27. O sistema de controle de acesso deve:

a) Ser capaz de cadastrar os administradores com diversos níveis de permissão.
b) Oferecer telas para o acompanhamento em tempo real de todas as transações efetivadas no Sistema e por níveis de prioridades, tais como: evento regular, alerta e erro.
c) Possibilitar o envio de e-mails automáticos em caso de eventos de alertas.
d) Utilizar criptografia na comunicação de todos dados trafegados.

e) Prover auditoria de ações dos usuários, inclusive os administradores, com possibilidade de filtro de pesquisa.
f) Possibilitar a customização dos perfis dos usuários, permitindo a criação de perfis de forma ilimitada.
g) Possibilitar inserção de permissões nos perfis de forma ilimitada, de forma que seja permitido restringir o acesso aos diferentes módulos e funcionalidades do sistema. Os perfis, inclusive, devem ser flexíveis de forma a possibilitar a restrição de acesso a campos e aos dispositivos do sistema, tais como leitoras e controladoras.

Ações Automatizadas

2.1.28. O sistema deverá possibilitar a configuração de ações iniciadas a partir de eventos ou através de agendamento.

2.1.29. As ações deverão abranger a possibilidade de rastrear o trânsito de uma pessoa, notificando todos os eventos de cartão gerado pela pessoa em específico.

2.1.30. As ações deverão permitir o envio de e-mails nas situações dos eventos de maior prioridade.

2.1.31. O sistema deve permitir o envio de e-mails para os responsáveis em caso de violação das políticas de horário de acesso às dependências do SERPRO.

2.1.32. Permitir a criação de alerta caso a quantidade de indivíduos ultrapasse o limite de ocupação da área.

Gestão de dispositivos

2.1.33. Quanto à gestão de dispositivos, o sistema de controle de acesso deverá:

a) Possibilitar o cadastro, consultas, alteração e exclusão dos equipamentos controladores e suas respectivas leitoras.
b) Além das informações básicas tais como: nome, descrição e endereço IP, o sistema deverá possibilitar vincular uma câmera ao equipamento.
c) Deverá possibilitar a verificação de status e controle do funcionamento em tempo real dos equipamentos.
d) A supervisão e controle desses dispositivos deverá ser realizada por meio de telas gráficas.

e) Deverá possibilitar o envio de comandos para os equipamentos cadastrados.
f) Os comandos devem possibilitar o bloqueio, desbloqueio e normalização dos equipamentos.
g) Permitir enviar e-mail de alerta sobre falha e retorno de comunicação com a controladora, para análise de manutenção preventiva.
h) Permitir o agendamento de abertura e/ou travamento do ponto de controle de acesso sem intervenção de operador.
i) Permitir gerar alerta na falta de alimentação AC.

2.2. Videomonitoramento

2.2.1. O Monitoramento por Circuito Fechado IP (CFTV IP) será composto por câmeras IP, servidor de gerenciamento, servidores de armazenamento, estações de monitoramento, switches, infraestrutura completa, serviços de instalação, configuração e capacitação técnica, com as devidas integrações aos demais sistemas.

2.2.2. A solução de CFTV baseada na tecnologia IP deve compreender a disponibilização, instalação, configuração e suporte técnico das câmeras de videomonitoramento IP, servidores de gerenciamento, servidor de armazenamento, estações de monitoramento, infraestrutura completa, serviços de instalação, configuração, softwares cliente e servidor, com as devidas integrações listadas nesse documento, e o licenciamento necessário.

2.2.3. A solução de CFTV deverá funcionar em operação contínua, 24 horas por dia e 07 dias por semana e possuir os seguintes requisitos mínimos:

a) Gerar imagens com ausência de distorções geométricas ou linearidade.
b) Deverá possibilitar a gravação local das imagens das câmeras fixas e móveis.
c) Deverá possibilitar a disponibilização remota de imagens em tempo real e gravadas, de sinais de alarmes e de áudio bidirecional.
d) Deverá trabalhar com sistema de licenciamento por câmeras que mesmo possuindo mais de uma stream, deve ser cobrada apenas uma licença, permitindo a expansão do sistema com licenças adicionais e de maneira ilimitada.
e) Permitir suporte para armazenamento de borda, diretamente em um armazenamento como um cartão microSD / SDHC ™ *.

f) Deverá permitir a tecnologia de redução de largura de banda e armazenamento, podendo realizar visualização ao vivo em taxa de quadros ajustáveis e em resoluções mais baixa que as configurações de gravação para um melhor balanceamento.
g) Deverá possuir capacidade de armazenamento de pelo menos 30 dias de gravação por evento, a uma taxa mínima de 30 fps (H.265 ou superior), resolução FULL HD (1920 x 1080) e gravação no mínimo de 10 horas por dia.
h) Deverá possibilitar que as câmeras sejam alimentadas pelo sistema PoE – Power over Ethernet.
i) Deverá suportar gravação por detecção de movimento e eventos, sejam estes eventos manuais, de análise de vídeo ou oriundos da integração com o sistema de acesso.

2.2.4. A monitoração e detecção de intrusão dos perímetros das regionais do Serpro deverá ser realizada por intermédio de análise inteligente de vídeo e câmeras.

Software de Videomonitoramento (VMS)

2.2.5. O sistema de gerenciamento de vídeo deve ser baseado em solução de vídeo IP, que suporta operação de imagens de vídeo, áudio e dados digitais dentro de uma rede IP, bem como apresentar os seguintes requisitos mínimos:

a) Rede e armazenamento otimizados, por multi-streaming, que otimiza a banda usando novos métodos de compressão, superiores ao padrão H.264 (H.265, H.264B, Zipstream, H.264+, H.264H, H.265+ ou similares).
b) Deverá gerar uma determinada foto da reprodução de vídeo com um descritivo, data e hora do evento ocorrido.
c) Deverá operar em forma de matriz digital assegurando chaveamento e controle das câmeras.
d) Deverá possuir topologia cliente–servidor, bem como servidores de gravação e estações clientes para operadores. Imagens de vídeo das localidades remotas devem ser acessíveis por diferentes estações de operação simultaneamente. Câmeras, gravadores e estações de visualização podem ser instalados em qualquer ponto dentro da rede.
e) Deverá permitir que o operador realize tarefas de recuperação de imagens dos servidores de gravação, bem como permitir o tratamento de eventos / alarmes recebidos, inserção de marcações nas gravações de maneira manual ou automática se devidas condições forem atendidas.

f) Deverá ter suporte em português em todas as operações.
g) Deverá permitir criação de grupos com direitos de acesso para câmeras específicas, prioridade de controle das câmeras, direito de exportação de imagens e acesso aos arquivos de log de eventos.

2.2.6. O sistema deve suportar operação (programação, visualização e recuperação) de funções de análise inteligente de vídeo.

2.2.7. O sistema deve dispor de API / SDK de forma gratuita, permitindo sua integração com sistemas de outros fabricantes.

2.2.8. O sistema especificado deve possibilitar tratamento dos alarmes gerados.

2.2.9. O sistema de gerenciamento deve ser capaz de combinar os alarmes gerados a partir das interfaces de alarmes dos servidores de vídeo com funções lógicas internas para criar gatilhos que permitam ao sistema reagir de acordo com um cenário de alarme pré-programado.

2.2.10. Possuir temporizadores internos e com os dias da semana, que podem ser programados para determinar com precisão quando os alarmes podem ser ativados.

2.2.11. O sistema deve aceitar entradas de eventos de alarmes e então colocá-los em uma pilha de alarmes para ser reconhecido ou a entrada de alarme pode automaticamente disparar uma série de operações no sistema (cenários).

2.2.12. O acionamento de entradas de alarme no sistema pode ser causado por qualquer uma das seguintes condições nos servidores remotos de vídeo:

a) Contato de entrada.
b) Detecção de movimento.
c) Perda de sinal de vídeo.
d) Perda de resposta dos servidores
e) Diversos eventos gerados pelas câmeras

2.2.13. O sistema deve ter capacidade de enviar e-mail em resposta à ocorrência de eventos de alarme.

2.2.14. O sistema deve ter capacidade, em caso de evento de alarmes, mostrar imagens de vídeo ao vivo, vídeo recuperado, documentos de texto, sistemas, arquivos HTML ou web sites (URLs).

2.2.15. O sistema deve suportar monitoramento do desempenho que inclui verificação das câmeras, computadores, software.

2.2.16. O sistema deve possuir possibilidade de integração com servidor de OPC, permitindo integração, quando necessário, com outras plataformas de automação.

2.2.17. O sistema deve suportar função de áudio bidirecional de sistemas de intercomunicação, diretamente da estação de operação com os codificadores remotos.

2.2.18. sistema deve permitir arranjo de imagens em mosaico, de 1 a 25 imagens simultaneamente, em formatos de 1x1, 2x2, 3x3, 4x4 e 5x5 (em monitor padrão 4:3), para monitores de formato 16:9, deverá suportar exibição do mosaico de 1 a 30 imagens em formatos de 1x1, 3x2, 4x3, 5x4 e 6x5. O sistema deve ainda permitir livre configuração no tamanho de cada imagem do mosaico, permitindo melhor visualização para a operação.

2.2.19. O sistema deve suportar sobre mapas ou plantas sinópticas com ícones dos dispositivos (câmeras, dispositivos etc.), inicialização de script de comandos, inicialização de sequência de câmeras, e links para outros mapas. Suportar ainda capacidade de zoom.

2.2.20. O sistema deve suportar operação com controles de joystick ou mouse, permitindo livre operação dos comandos em giros horizontal, vertical, zoom óptico, íris, foco e comandos auxiliares das câmeras. Deve ainda suportar zoom digital para qualquer imagem por meio de um controle gráfico na interface do usuário.

2.2.21. O sistema deve suportar barra de tempo permitindo visualização gráfico do tempo, com escala variável entre minutos e horas, através do uso de calendário, para todas as imagens gravadas.

2.2.22. O sistema deve permitir exportação de vídeo sincronizada de câmeras simultâneas.

2.2.23. O sistema deve suportar, por meio de módulo de analíticos ou metadados das câmeras, função de busca de eventos com pelo menos os seguintes critérios: definição da área de interesse para pesquisa do objeto, cor do objeto, bem como eventos de entrar ou sair de áreas designadas.

2.2.24. O sistema deverá suportar as seguintes opções de segurança:

a) Certificados digitais instalados em câmeras para verificação de dispositivos confiáveis.
b) Conexão segura (criptografada e verificação de origem) entre a câmera e o servidor de vídeo. O controle da câmera, incluindo sinais de PTZ, vídeo, áudio e comandos I/O, devem ser transferidos e criptografados (por meio de encapsulamento HTTPS).
c) Estabelecer sessões por HTTPS (autorização segura (por SSL / TLS) com certificado confiável instalado na câmera) para proteger os dados do usuário.

d) Conexões HTTPS seguras entre os servidores de vídeo e as instâncias do thin client (web e móvel).
e) Encapsulamento HTTPS ao recuperar vídeo do armazenamento de borda da câmera.
f) Assinatura digital do vídeo exportado para comprovar a autenticidade do vídeo. A assinatura digital deve ser feita pelo VMS e deverá possuir formas de validar o vídeo exportado.

2.3. Sistema de Monitoramento Predial por IoT

2.3.1. Deverão ser instalados dispositivos IoT para monitorar as condições ambientais da edificação, tais como temperatura, umidade, nível de iluminação, qualidade do ar etc.

2.3.2 Além do monitoramento das condições ambientais, deverá também o sistema monitorar as instalações elétricas, como o consumo, tensão e corrente.

2.3.3. O sistema deve ser capaz de:

a) Monitorar o consumo de energia das redes comum, estabilizada e climatização;
b) Monitorar o horário de acionamento e desligamento da climatização (maior responsável pelo consumo de energia;
c) Monitorar a Demanda e Fator de Potência da Regional;
d) Identificar as quedas de energia com precisão (dia, hora);
e) Realizar a análise de vários tipos de dispositivos na mesma interface;
f) Programar alertas de mudança de temperatura, queda de energia e outras variáveis de interesse;
g) Estabelecer limites de consumo para notificação em forma de alarme;
h) Planejar e racionalizar o uso da energia nos ambientes de trabalho (oportunidades de redução de consumo e de evitar o desperdício);
i) Possibilita verificar o consumo da Regional em tempo real e de diversos ambientes de trabalho;
j) Medir e registrar grandezas calculadas: Consumo consolidado (kWh), Consumo de hora de ponta (KWh), Consumo em (R$), Consumo de hora de ponta em (R$).
k) Realizar por meio de sensores a medição no mínimo das seguintes grandezas: Tensão, Frequência, Corrente, Potência Ativa, Potência Reativa, Potência Aparente, Fator de potência e Consumo.

l) Realizar por meio de sensores a medição de temperatura dos ambientes com range de -40 a 80ºC.
m) Realizar por meio de sensores a medição de umidade dos ambientes no range de 0 a 100% RH.
n) Deve permitir a transmissão dos dados do medidor para software de terceiros via protocolos HTTP e/ou MQTT nas suas revisões mais recentes.

Segurança da Informação

2.3.4. A empresa fornecedora deverá especificar nos projetos recursos que inibam a engenharia reversa de hardware e software, tais como mecanismos anti-violação física e lógica, como, por exemplo, Tampering, Auto-Destruction entre outros;

2.3.5. A empresa fornecedora deverá utilizar práticas de Security by design (a segurança deve ser planejada, executada e monitorada ao longo de todo o ciclo de vida de uma aplicação).

2.3.6. A empresa fornecedora deverá especificar nos projetos recursos de software e hardware que permitam a disponibilidade da solução, como os recursos de recuperação de erros (técnicas como o watchdog timer).

2.3.7. Os dispositivos deverão permitir inserção de senhas complexas, alfanuméricas e com caracteres especiais.

2.3.8. Os dispositivos devem se comunicar utilizando protocolos seguros e abolir protocolos com falhas de segurança já conhecidas ou comunicações em texto plano;

2.3.9. Os dispositivos devem permitir desabilitar/impedir acesso a serviços não utilizados.

2.3.10. A empresa não deve figurar ou dispor em seu parque, dispositivos que constam em listas relacionadas a problemas de segurança ou privacidade, como exemplo o PROCOM ou a Federal Trade Commission;

2.3.11. Os dispositivos devem prover atualizações e correções, estas devem ser assinadas e realizadas por meio seguro;

2.3.12. Os dispositivos devem apresentar proteção de no mínimo IP66;

2.3.13. Os dispositivos da solução devem poder executar reinicializações sob demanda remotamente de forma segura;

2.4. Gestão de Estacionamento

2.4.1. Deverá ser implantado um sistema de gestão de vagas de estacionamento, indicando o número de vagas livres e ocupadas, em tempo real.

2.4.2. O sistema abrangerá, no mínimo, as seguintes funcionalidades:

a) Monitoramento em tempo real da ocupação das vagas.
b) Interface de administração para gestores do estacionamento.
c) Geração de relatórios de uso e estatísticas.

2.4.3. O sistema deverá:

a) Detectar a presença de veículos em cada vaga utilizando sensores e/ou câmeras apropriados.
b) Atualizar o status de cada vaga (livre/ocupada) em tempo real.
c) Disponibilizar uma interface para que os gestores possam visualizar o estado atual do estacionamento e gerenciar as vagas.
d) Fornecer uma interface para que os usuários possam verificar a disponibilidade de vagas antes de entrar no estacionamento.
e) Gerar relatórios periódicos sobre a utilização das vagas, incluindo métricas como tempo médio de ocupação e taxa de rotatividade.
f) Ser responsivo e acessível a partir de diferentes dispositivos, incluindo desktops, tablets e smartphones.
g) Garantir a segurança dos dados dos usuários e do estacionamento, implementando medidas de proteção contra acessos não autorizados.
h) Ser escalável para suportar diferentes tamanhos de estacionamentos, desde pequenos até grandes complexos.
i) Possuir alta disponibilidade, garantindo que o sistema esteja operacional pelo menos 99,5% do tempo.

2.5 Estações de Carregamento de Veículos Elétricos

2.5.1. Deverá ser instalado um posto de carregamento de veículo elétrico, do tipo smart, com plataforma de gerenciamento.

2.5.2. O carregador deverá ser de carga lenta AC de 2,7kW até 22kW, com conector padrão europeu tipo 2.

2.5.3. Deverá ser montado em pedestal ou em parede, com cabo de pelo menos 4m de comprimento.

2.5.4. Deverá possuir uma plataforma completa de gestão, com registro e relatórios de uso, dados de energia consumida por cada veículo/usuário, data e hora da conexão, tempo de carregamento e tarifação.

2.5.5. O equipamento deve ser dotado de sistema de proteção elétrica, e ser adequado para instalação ao tempo, com no mínimo IP65.

2.5.6. A recarga deve ser liberada mediante app ou cartão RFID.

3.Integrações

Os sistemas devem integrar-se perfeitamente a sistemas internos e softwares do Serpro.

3.1. Login Único Serpro

3.1.1. Integração com Login Único do SERPRO com autenticação através de SSO (Single Sign-On) compatível com OpenID Connect 1.0 ou SAML 2.0, implementando as recomendações do protocolo OAuth, disponibilizando plenos direitos aos recursos do sistema aos usuários logados via SSO e com possibilidade de uso de SDK/API para adição, remoção, bloqueio e gestão de Usuários.

3.2. Sistema de Gestão de Identidades Serpro - GIA

3.2.1. A solução deve permitir a importação/sincronização dos dados de usuários à medida que forem cadastrados/atualizados na Solução de Gestão de Identidade e Acesso do SERPRO (GIA):

3.2.2. Deverão ser importados dados do cadastro, no mínimo: nome, foto, matrícula, identidade e lotação.

3.2.3. O conector entre o GIA será de responsabilidade do fornecedor da solução.

3.2.4. A solução deverá adicionar automaticamente permissão para passagem pelas catracas das portarias.

3.3. API Serpro de Reconhecimento Facial

3.3.1. O Serpro dispõe de API de Reconhecimento facial, capaz de alimentar uma base de dados biométricos, de validar faces coletadas e excluir os dados biométricos da referida base.

3.3.2. O sistema deverá coletar a face do indivíduo e utilizar a API Serpro para validação facial através do Datavalid.

3.3.3. O sistema deverá cadastrar a face e o identificador do indivíduo em uma base específica na API Serpro de reconhecimento facial, que tem seu próprio mecanismo de autenticação/autorização.

3.3.4. O sistema deverá ler a face do indivíduo, por meio de leitores faciais que detectem vivacidade, e validar sua identidade através da API Serpro de reconhecimento facial.

3.3.5. O sistema deverá gerenciar a remoção dos indivíduos através da API Serpro de reconhecimento facial.

3.3.6. As imagens enviadas ao sistema de reconhecimento facial devem possuir resolução mínima de 300x300 pixels, não ter problemas de super ou sub iluminação, nitidez nem oclusões.

3.4. Base de Placas Veiculares

3.4.1. O Serpro dispõe de APIs de consulta à base de dados do Senatran, que devem ser integradas ao sistema de gestão de controle de acesso e estacionamento.

3.4.2. Os sistemas que compõem a PoC deverão integrar-se a estas APIs para consulta dos dados básicos de cada veículo que adentra às instalações do Serpro, ou fazem uso da estação de carregamento veicular.

3.4.3. Todas as consultas a esta base devem ser realizadas mediante a informação da placa do veículo, que por sua vez é capturada por meio de câmeras LPR.

3.4.4. A cada captura, devem ser consultados na API, no mínimo, os dados abaixo:

a. Nome do proprietário do veículo
b. Cor, marca e modelo do veículo
c. Se há comunicação de roubo ou furto

3.4.5. Caso haja comunicação de roubo ou furto, deverá ser enviado um alerta aos operadores do sistema, que comunicarão ao gestor de segurança do Serpro.

3.5. Demais integrações

3.5.1. A solução deverá possibilitar a integração a sistemas terceiros por meio de API Rest e protocolo SNMPv2.

3.5.2. A solução deverá oferecer a possibilidade de integração com software de diferentes fabricantes, de forma a flexibilizar o atendimento de necessidades futuras que possam surgir durante a utilização.

3.5.3. A solução deverá ter um completo gerenciamento de alarmes e eventos, devendo reconhecer alarme de qualquer dispositivo com contato seco ou através de integração.

3.5.4. Todas as aplicações, sistemas e equipamentos devem ter seus horários sincronizados com o servidor de tempo do Serpro (NTP).

4. Sistema Integrado de Gestão

4.1. Todas as aplicações devem estar integradas, possibilitando a montagem e disponibilização de painéis e dashboards para monitoramento em tempo real.

4.2. Disponibilizar relatórios consolidados dos sistemas e aplicações, tanto por demanda quanto relatórios agendados.

4.3. Deverá enviar alarmes e alertas com base em parâmetros pré-configurados de qualquer uma das aplicações.

5.Métricas de Avaliação

5.1. O sucesso da POC será avaliado com base nas seguintes métricas principais:

a) **Taxa de reconhecimento facial bem-sucedido:** Percentual de tentativas de acesso autenticadas corretamente.
b) **Taxa de integração bem-sucedida:** Percentual de sistemas e dispositivos integrados com sucesso.
c) **Tempo de resposta do sistema de controle de acesso:** Tempo médio para processar e conceder ou negar acesso de uma pessoa.
d) **Número de alertas gerados:** Quantidade de alertas e notificações geradas pela plataforma.

e) **Painéis e dashboards:** Número de painéis e dashboards desenvolvidos

6.Resultados Esperados

6.1. Taxa de Reconhecimento Facial Bem-Sucedido

Resultado Esperado: Atingir uma taxa de reconhecimento facial bem-sucedido de pelo menos 95%, garantindo que a maioria das tentativas de acesso sejam autenticadas corretamente e minimizando falsos positivos e negativos.

6.2. Taxa de Integração Bem-Sucedida

Resultado Esperado: Integrar com sucesso 100% dos sistemas e dispositivos planejados, assegurando que todos os componentes funcionem de maneira coesa e integrada, permitindo uma gestão centralizada e eficiente.

6.3. Tempo de Resposta do Sistema de Controle de Acesso

Resultado Esperado: Reduzir o tempo médio de resposta do sistema de controle de acesso para menos de 2 segundos, garantindo que os usuários não enfrentem atrasos significativos ao tentar acessar o prédio.

6.4. Número de Alertas Gerados

Resultado Esperado: Gerar pelo menos 90% dos alertas abaixo:

a) Temperatura Fora do Intervalo Ideal: Alerta gerado quando a temperatura em uma área monitorada está fora do intervalo predefinido.
b) Umidade Fora do Intervalo Ideal: Alerta gerado quando a umidade em uma área monitorada está fora do intervalo predefinido.
c) Nível de CO2 Elevado: Alerta gerado quando os níveis de CO2 ultrapassam os limites aceitáveis, indicando possível problema de ventilação.
d) Acesso indevido a ambiente: Alerta gerado quando uma linha virtual for cruzada em um local não previsto
e) Nível de tensão fora do padrão: Alerta gerado quando o nível de tensão de uma instalação monitorada está fora do intervalo predefinido.
f) Detecção de Movimento em Área Restrita: Alerta gerado quando há movimento detectado em uma área que deveria estar vazia.

g) Perda de Sinal de Vídeo: Alerta gerado quando uma câmera perde o sinal ou fica offline.
h) Estacionamento Lotado: Alerta gerado quando todas as vagas de estacionamento estão ocupadas.
i) Falha na Estação de Carregamento: Alerta gerado quando uma estação de carregamento de veículos elétricos apresenta falha ou está fora de serviço.

6.5. Painéis e Dashboards Desenvolvidos

Resultado Esperado: Desenvolver e implementar pelo menos 3 painéis e dashboards personalizados, que permitam a visualização e análise de dados em tempo real, facilitando a tomada de decisões informadas e a gestão eficiente do prédio.

6.6. Resultados Gerais Esperados

a) Melhoria na Segurança: Aumento da segurança predial através de um sistema de controle de acesso eficiente e videomonitoramento integrado.
b) Eficiência Operacional: Otimização das operações prediais com a integração de sistemas IoT e gestão centralizada.
c) Sustentabilidade: Redução do consumo de energia e melhoria na gestão de recursos, promovendo um uso mais sustentável dos recursos prediais.
d) Satisfação dos Usuários: Aumento da satisfação dos usuários e administradores com a facilidade de uso e eficiência dos sistemas implementados.
e) Validação Tecnológica: Validação da viabilidade e benefícios das tecnologias avançadas utilizadas na POC, demonstrando seu potencial para implementação em larga escala.

7.Local de Execução

7.1. A Prova de Conceito deverá ser realizadas nas instalações do Serpro, relacionadas abaixo:

I. **Regional Brasília**, localizada na SGAN Av. L-2 Norte Quadra 601 – Módulo G - Brasília/Distrito Federal, CEP: 70.836-900
II. **Regional Belo Horizonte**, localizada na Av. José Cândido da Silveira, 1200 - Horto Florestal, Belo Horizonte - MG, CEP 31035-536.
III. **Regional Curitiba**, localizada na R. Carlos Pioli, 133 - Bom Retiro, Curitiba - PR, CEP 80520-170.

8.Etapas e Prazos

8.1. A Prova de Conceito deverá seguir as etapas e prazos estabelecidos abaixo:

i. Etapa 1: Elaboração do layout técnico, topologia dos sistemas e preenchimento dos Anexos 2 e 3;
ii. Etapa 2: Instalação da infraestrutura física, equipamentos e softwares
iii. Etapa 3: Configuração e parametrização dos sistemas e equipamentos, e implementação das integrações
iv. Etapa 4: Período de testes e validações
v. Etapa 5: Apresentação dos resultados

8.2. Os prazos de cada etapa estão representados abaixo, em dias corridos:

i. Etapa 1: até 5 dias após notificação de início da POC
ii. Etapa 2: até 25 dias após a etapa anterior
iii. Etapa 3: até 10 dias após a etapa anterior
iv. Etapa 4: até 40 dias após a etapa anterior
v. Etapa 5: até 10 dias após a etapa anterior

8.3. O prazo máximo da Prova de Conceito, incluindo sua avaliação, será de até 150 dias.

ANEXO 2

Neste Comodato, serão disponibilizados os produtos (hardwares e softwares) especificados abaixo:

Nome do Produto	Quant.	Tipo*	Observações**

***Tipo:** H para hardware ou S para software.

****Observações:** Incluir descrição, número de série e demais informações necessárias a identificação do produto.

ANEXO 3

Requisitos a serem disponibilizados pela COMODATÁRIA para execução da POC:

Nº *	Descrição*

*Deve ser preenchido pelo fornecedor.