

ANEXO II - ESPECIFICAÇÕES TÉCNICAS

1. DISPOSIÇÕES GERAIS

1.1. Os significados dos termos utilizados na presente especificação são os seguintes:

- a) CONTRATANTE: União, por intermédio do Tribunal de Contas da União - TCU;
- b) CONTRATADA: Licitante vencedora do certame licitatório, a quem será adjudicado o objeto desta licitação, após a assinatura do contrato;
- c) FISCALIZAÇÃO: Servidor(es) designado(s) formalmente para representar a CONTRATANTE, responsável(eis) pela fiscalização dos serviços.
- d) CFTV: Sistema de monitoramento por Circuito Fechado de Televisão;
- e) EQUIPAMENTOS: Todos os dispositivos eletromecânicos e eletrônicos necessários à completa operação da solução a ser fornecida;
- f) IP: Internet Protocol (Protocolo de Internet);
- g) ISC: Instituto Serzedello Corrêa, Escola Superior do TCU;
- h) SCA: Sistema de Controle de Acesso;
- i) SCES ESTADUAIS: Secretarias do TCU nos Estados;
- j) SOLUÇÃO DE CONTROLE DE ACESSO: O conjunto de softwares e hardwares e demais itens que compõem o objeto da contratação;

2. PREPOSTO

2.1. A CONTRATADA deverá indicar, mediante declaração, um preposto, aceito pela fiscalização, durante o período de vigência do contrato, para representá-la administrativamente, sempre que for necessário. Na declaração deverá constar o nome completo, número do CPF e do documento de identidade, além dos dados relacionados à sua qualificação profissional.

2.2. A qualquer tempo a CONTRATANTE poderá solicitar à CONTRATADA a substituição do preposto indicado que não atenda satisfatoriamente às necessidades da execução contratual.

2.3. O preposto deverá se apresentar à respectiva unidade fiscalizadora no prazo definido no Anexo I – Termo de Referência, para firmar, juntamente com os servidores designados para esse fim, o Termo de Abertura do Livro de Ocorrências, destinado a tratar dos assuntos pertinentes à execução do contrato.

2.4. O preposto deverá estar apto a esclarecer as questões relacionadas às faturas dos serviços prestados.

2.5. A CONTRATADA orientará o seu preposto quanto à necessidade de acatar as orientações da Administração, inclusive quanto ao cumprimento das Normas Internas e de Segurança e Medicina do Trabalho.

2.6. A empresa deverá cuidar para que o preposto mantenha permanente contato com a unidade responsável pela fiscalização do contrato, adotando as providências requeridas relativas à execução dos serviços e comunicando qualquer irregularidade verificada na execução dos serviços.

3. OBJETO

3.1. Definição

3.1.1. Contratação de empresa especializada para fornecer e implantar sistema de controle de acesso de pessoas e veículos, bem como controle de ponto eletrônico, incluindo software, equipamentos, instalação, configuração e manutenção, sob o regime de fornecimento e prestação de serviço associado, para atender às unidades do Tribunal de Contas da União – TCU, Instituto Serzedello Corrêa – ISC e Secretarias do TCU nos Estados.

3.2. Descrição da composição do objeto

3.2.1. O objeto será executado mediante o modelo associado de fornecimento de equipamentos e softwares e a prestação de serviços por escopo, necessários à completa instalação, configuração e funcionamento da solução, bem como, da prestação de serviços de natureza continuada de manutenção e suporte técnico de toda a solução ofertada.

3.3. Cronograma

3.3.1. A execução do objeto deverá observar rigorosamente os prazos estabelecidos no cronograma especificado no Anexo VII do Edital.

3.3.2. Excepcionalmente, após a assinatura do contrato, a Contratada poderá solicitar a alteração deste cronograma, desde que apresentadas as respectivas justificativas, que serão avaliadas pela Contratante.

3.3.3. A implantação da solução poderá ser escalonada e dividida em partes, conforme necessidade e aprovação da Contratada.

3.3.4. Serão considerados injustificados os atrasos não comunicados tempestivamente e indevidamente fundamentados, e a aceitação da justificativa ficará a critério do Contratante.

3.3.5. Havendo pedido de prorrogação do prazo de entrega, este somente será concedido, em caráter excepcional, nas hipóteses previstas Lei nº 14.1333/2021.

3.3.6. Os pedidos de prorrogação deverão ser encaminhados por escrito, com antecedência mínima de 1 (um) dia do seu vencimento, anexando-se documento comprobatório do alegado pela Contratada.

3.4. Do término da execução do objeto

3.4.1. A CONTRATADA deverá continuar prestando o serviço regularmente, até o término efetivo da OS, atendendo às demandas restantes e efetuando a transferência de conhecimento para a equipe da CONTRATANTE.

3.4.2. Toda e qualquer informação produzida no âmbito da execução do objeto do contrato pela empresa fornecedora dos bens e prestadora dos serviços será de propriedade da CONTRATANTE e fica a CONTRATADA obrigada a documentar e registrar os produtos, serviços e eventos observando as metodologias e ferramentas utilizadas na CONTRATANTE.

3.5. Requisitos gerais da solução

3.5.1. A solução a ser contratada deve englobar:

- 3.5.1.1. Acesso de pessoas ao complexo do TCU e ao ISC, em Brasília-DF, com utilização de catracas com barreiras físicas e reconhecimento facial;
- 3.5.1.2. Acesso de pessoas às salas seguras na sede do TCU, em Brasília-DF; e
- 3.5.1.3. Acesso de veículos às garagens do complexo do TCU e do ISC, em Brasília-DF.
- 3.5.1.4. Registro de ponto eletrônico dos servidores e colaboradores na Sede do TCU, em Brasília-DF, no ISC e nas Secretarias de Controle Externo nos estados.
- 3.5.1.5. Serviços por escopo e serviços contínuos necessários à implantação, operação e manutenção de toda a solução.
- 3.5.2. Todos os equipamentos de borda, de um mesmo grupo, devem ser de um único fabricante, garantindo a compatibilidade funcional e estética
- 3.5.3. A solução de controle de acesso de pessoas e veículos será composta, no mínimo, pelos seguintes itens, independente da tecnologia a ser apresentada:
 - 3.5.3.1. **Software de controle de acesso;**
 - 3.5.3.2. **Catracas;**
 - 3.5.3.3. **Leitores com reconhecimento facial;**
 - 3.5.3.4. **Cancela de acesso de veículos;**
 - 3.5.3.5. **Câmeras para reconhecimento de placas dos veículos (LPR);**
 - 3.5.3.6. **Servidor de gerenciamento do controle de acesso;**
 - 3.5.3.7. **Gerenciadoras e Controladoras de controle de acesso;**
 - 3.5.3.8. **Estação de cadastramento;**
 - 3.5.3.9. **Kits controle de acesso para portas;**
 - 3.5.3.10. **Terminal de comunicação bidirecional;**
 - 3.5.3.11. **Fechadura eletroímã para portões;**
 - 3.5.3.12. **Portal detector de metais;**
 - 3.5.3.13. **Registrador de Ponto Eletrônico;**
 - 3.5.3.14. **Serviços por escopo de elaboração de projetos, desmobilização da solução atual, infraestrutura, instalação, configuração e integração dos hardwares e softwares, fechamento com guarda corpo, treinamento e operação assistida; e**
 - 3.5.3.15. **Serviços contínuos de manutenção e suporte técnico de todos os componentes da solução, incluindo a garantia total dos equipamentos e sistemas, reposição de peças, inclusive mediante mão de obra com dedicação exclusiva.**
- 3.5.4. A solução a ser contratada deve possuir as seguintes licenças de uso de softwares:
 - 3.5.4.1. Todos os softwares necessários para o funcionamento da solução deverão ser licenciados em nome do Tribunal de Contas da União - TCU.

- 3.5.4.2. Todas as licenças de aplicação de todos os dispositivos fornecidos para implantação e pleno funcionamento da solução, como por exemplo, licenças de analíticos de LPR;
- 3.5.4.3. Todas as licenças de uso dos softwares e dos sistemas fornecidos para a implantação e pleno funcionamento da solução deve ser do tipo perpétua, em nome do TCU, e seus respectivos termos de licenciamento de uso devem ser entregues ao Tribunal, quando passarão a compor o patrimônio do órgão;
- 3.5.4.4. Em todos os softwares entregues ao TCU devem estar especificadas as características da licença, contendo informações inequívocas sobre: perpetuidade da licença, inexistência de restrição de licenciamento, para uso do software pelo TCU, de qualquer natureza, como número de documentos, número de usuários, quantidade de recursos computacionais (CPU, memória etc.) dos equipamentos onde o software será instalado;
- 3.5.4.5. A quantidade de licenças deve ser suficiente para uso concorrente das estações de trabalho previstas nessa contratação, além das licenças necessárias para administração do sistema.
- 3.5.5. O SCA é destinado ao controle físico da entrada de pessoas nos diversos ambientes do órgão, por meio de catracas ou outros dispositivos.
- 3.5.6. Além dos equipamentos previstos neste edital, o Sistema deverá oferecer a possibilidade de integração com hardware, soluções de videomonitoramento e analíticos de diferentes fabricantes, como por exemplo, mas não limitado a, leitores de proximidade, câmeras de LPR, terminais de biometria por impressão digital, terminais de reconhecimento facial, analíticos de LPR, analíticos de reconhecimento facial, sistemas VMS, etc., de forma a flexibilizar a solução para atender necessidades futuras que possam surgir durante a utilização do sistema.
- 3.5.7. Durante a fase de operação assistida, a contratada será responsável por realizar o cadastramento de todos os servidores, terceirizados e visitantes que necessitem acessar as dependências do órgão contratante. A autenticação biométrica dessas pessoas deverá ocorrer por meio de integração direta com a base de dados da Identificação Civil Nacional (ICN), garantindo que a validação da identidade seja feita de forma segura e padronizada em âmbito nacional. Ou seja, quando alguém for cadastrado no sistema do órgão, os dados biométricos (ex.: reconhecimento facial) não serão validados apenas pelo banco de dados interno do órgão, mas sim comparados/validados com a base da ICN.
- 3.5.8. A solução de controle de acesso tem por função identificar, permitir ou negar o acesso de pessoas e veículos, utilizando critérios pré-configurados, registrando todos os eventos relativos a esta atividade.
- 3.5.8.1. Esta função visa prevenir os riscos que possam afetar as pessoas e as instalações inseridas no sistema.
- 3.5.9. O objetivo da utilização do sistema de controle de acesso é permitir somente que pessoas autorizadas, acessem e/ou transitem pelas áreas distintas inseridas na edificação.
- 3.5.10. A solução deverá operar com atualizações em tempo real, exibindo e armazenando os eventos conforme eles vão ocorrendo. Deve possuir inteligência

distribuída em gerenciadoras de sistema, de tal forma que dispensem a necessidade da conexão permanente com o servidor de banco de dados, já que as gerenciadoras de sistema armazenam localmente as regras de acesso para cada usuário cadastrado e os eventos autorizados ou negados conforme ocorrem. Estas gerenciadoras deverão continuamente ser monitoradas pelo servidor, que informará se a comunicação for interrompida.

- 3.5.11. A solução deverá permitir o cadastramento prévio de visitantes via acesso web e mobile. O cadastramento e controle de entrada de visitantes deverão ser ativados nas recepções dos edifícios do complexo do TCU e do ISC, em Brasília/DF.
- 3.5.12. O sistema deve ter uma arquitetura aberta, suportando integração com aplicações nativas de terceiros.
- 3.5.13. A solução de controle de acesso deve ser fornecida com todos os demais acessórios necessários para o seu pleno funcionamento, ainda que não tenham sido listados exaustivamente neste documento.
- 3.5.14. Todos os custos direta e indiretamente envolvidos e necessários ao fornecimento (incluindo transporte, entrega e impostos), instalação, configuração e manutenção de toda a solução contratada devem ser integralmente considerados pelas licitantes, dentro do valor unitário de cada item (equipamento, software ou serviço), independentemente da localização geográfica da unidade onde a solução será implantada, conforme modelo de proposta de preços constante do Anexo IV do Edital.

4. SISTEMA DE CONTROLE DE ACESSO – SCA

Unidade: Sistema.

Marcas/modelos de referência: Tyco: C CURE 9000, Genetec: Synergis, Lenel: OnGuard ou outro tecnicamente equivalente.

Critério de Medição: A medição e aceitação do fornecimento do sistema de controle de acesso ocorrerá em duas etapas: sendo 50% após a verificação da instalação completa do software nos servidores designados, da parametrização conforme requisitos operacionais do TCU, e da confirmação documental da entrega do software e licenças perpétuas. E a outra parcela (50%) será paga após verificação da configuração dos perfis de acesso e regras de controle de acesso conforme matriz de permissões definida pelo TCU, da integração com os dispositivos de controle de acesso (catracas, cancelas, leitores biométricos, câmeras LPR etc.) e com os sistemas internos do TCU, e da realização de testes de funcionalidades conforme plano aprovado pelo TCU, garantindo que o sistema esteja em pleno funcionamento e atenda a todas as exigências contratuais.

Requisitos gerais:

4.1. O fabricante do Sistema de Controle de Acesso a ser fornecido deverá possuir representante no Brasil, sendo vedado o fornecimento de soluções estrangeiras sem representante em solo nacional.

4.2. O SCA deverá ser acessado via web, compatível com ao menos dois dos três navegadores mais populares (Microsoft Edge, Mozilla Firefox e Google Chrome), sendo o acesso pelo computador cliente através de browser, sem limite de usuários cadastrados.

4.2.1. Caso o Sistema de Controle de Acesso não possua 100% das funcionalidades via WEB, serão aceitas funcionalidades compatíveis com o sistema operacional Windows 10. Não deverá haver limite de usuários cadastrados com o software instalado.

4.3. O SCA deve trabalhar com certificado HTTPS para conexão confiável da estação de trabalho (cliente).

4.4. O SCA deve ser de design modular e fornecer a flexibilidade para permitir ao usuário adicionar ou remover quaisquer componentes e/ou funções controladas, ou em caso de alteração dos requisitos operacionais, bem como nas situações de expansão do sistema.

4.5. O SCA deve prover um gerenciamento da informação e deve operar numa configuração Cliente-Servidor em computadores rodando com a plataforma Windows. Sua arquitetura cliente-servidor deve ser capaz de suportar no mínimo 10 usuários utilizando a versão completa do software (sem contar os operadores de recepção, que irão utilizar o módulo de cadastro de visitantes) e múltiplos tipos de controladoras.

4.6. O SCA deve ser construído para ser independente do banco de dados e deve suportar, no mínimo, o Oracle 12c standard ou SGBD (sistema de gerenciamento de banco de dados) equivalente, para proteção de dados, redundância e gerenciamento.

4.7. O SCA deve ser flexível o suficiente de modo a permitir que a aplicação e banco de dados rodem no mesmo servidor e deve permitir que a aplicação opere em servidor separado do servidor de banco de dados, ficando a critério da Contratante a definição de qual modo mais conveniente será adotado.

4.8. Deverá ser compatível com infraestrutura virtualizada com o uso de ferramentas VMWare ou Hyper-V.

4.9. O SCA deve ter capacidade mínima para 5.000 leitoras por cada servidor e escalabilidade para comportar, pelo menos, 28 servidores de aplicação.

- 4.10. O SCA deverá ser capaz de utilizar protocolo Wiegand e OSDP entre leitores de Cartão/Biometria e os controladores de acesso. A comunicação entre os controladores de acesso, servidores e gerenciadores de rede devem ser através de protocolo TCP/IP.
- 4.11. O SCA deverá possuir Web Client, ou software que poderá ser instalado em um micro cliente, podendo gerenciar, mostrar exibições dinâmicas, monitorar as atividades do sistema, cadastrar e modificar dados dos portadores dos cartões.
- 4.12. O SCA deve ter uma ferramenta de geração de acessos para criar e gerenciar os usuários usando uma interface gráfica e capacidade de consultas para facilitar o gerenciamento de um número grande de acessos.
- 4.13. O SCA também deve conter um componente de monitoramento via web, ou através de software instalado no micro cliente. Com esta característica, o operador poderá gerenciar pessoas, mostrar exibições dinâmicas e monitorar as atividades do sistema diretamente de qualquer PC.
- 4.14. O SCA deverá permitir controlar o acesso de veículos nas cancelas, através de câmeras com captura de placas (LPR). Estas enviarão as informações das placas para o sistema de controle de acesso que irá autorizar a abertura ou não das cancelas.
- 4.15. O SCA deverá ser capaz de utilizar informações como leitura de placas veiculares e de rostos combinadas com leitores de acesso, para permitir ou negar o acesso através de catracas, cancelas e portas, e gerar alarmes.
- 4.16. O sistema deverá permitir que o operador bloqueie ou libere de forma manual a abertura da cancela através de um botão físico, controle remoto ou, preferencialmente, via terminal de comunicação bidirecional.

Requisitos de Arquitetura:

- 4.17. O Sistema de Controle de Acesso (SCA) deverá possuir arquitetura compatível para integração com soluções de CFTV, LPR (Leitura de Placas Veiculares), reconhecimento facial e outros sistemas correlatos, seja de forma nativa ou por meio de APIs/SDKs oficiais disponibilizados pelo fabricante, assegurando interoperabilidade e gestão centralizada de eventos.

- 4.17.1. Nesta contratação não será necessário o fornecimento dos módulos de CFTV, devendo, contudo, a solução ofertada permitir expansões futuras sem necessidade de substituição do sistema existente, a visualização integrada e a

correlação dos eventos em ambiente de gestão centralizada, de forma a garantir rastreabilidade e eficiência operacional.

4.17.2. A solução ofertada deve garantir que, quando da futura integração de CFTV e outros sistemas congêneres, os eventos, por exemplo, provenientes de vídeo, leitura de placas, reconhecimento facial e de controle de acesso possam ser correlacionados em interface única, assegurando a rastreabilidade e a eficiência operacional.

4.18. O SCA deve ser capaz de operar com equipamentos (leitoras, gerenciadoras, bloqueios etc.) de diversos fabricantes, não podendo limitar o seu uso a hardwares de um fabricante específico.

4.19. O sistema deve controlar o acesso a uma área designada.

4.20. O sistema deve validar as credenciais do portador, através dos dados pessoais, formatos de cartão, senhas, reconhecimento facial, cadastramento biométrico e múltiplos cartões ativos, e comparar a tentativa de entrada com as informações contidas na memória.

4.21. As controladoras de acesso devem ser capazes de operar de forma independente em caso de perda de comunicação, através de registros em memória dos dados de logs de acesso de no mínimo 50.000 usuários.

4.21.1. Para essa funcionalidade, a solução poderá utilizar placas gerenciadoras, quando necessário.

4.22. O acesso a uma área designada será validado somente quando a credencial tiver um número válido para essa localidade e o número é válido para a data e hora corrente que a leitora for usada.

4.23. O sistema deve acessar o equipamento que valida o usuário a acessar determinado local e, conseqüentemente, monitorar a segurança da localidade pelo uso de controladoras, portas, leitoras, elevadores, entradas e saídas. Quando o acesso é validado, um sinal é enviado para a leitora para permitir a entrada na localização.

4.24. O sistema deve ser configurado pelo uso da aplicação de Administração e deve prover modelos de configuração.

4.25. O sistema deve permitir a configuração de lógica de acesso, intertravamentos e alarmes, possibilitando efetuar múltiplas configurações lógicas para acionamento de dispositivos de saídas.

- 4.26. O sistema deve monitorar as atividades de controle de acesso pelo uso da estação de monitoramento.
- 4.27. O sistema deve restringir o uso administrativo e a estação de monitoramento pelo uso de privilégios e autenticação (senha de usuário) usando a funcionalidade de senha do sistema operacional Microsoft Windows (autenticação por Windows) e através de autenticação pelo sistema (autenticação básica).
- 4.28. O sistema deverá possuir integração com o sistema de diretório do órgão para gestão de usuários e operadores do sistema.
- 4.29. O sistema deverá suportar Single Sign-On (SSO) por meio de integração com sistemas externos de autenticação.
- 4.30. O sistema deverá ser capaz de se conectar ao serviço de diretório através do Lightweight Directory Application Protocol (LDAP).
- 4.31. A conexão ao LDAP deverá ser configurável pelo usuário diretamente do SCA e não deverá requerer nenhum código customizado.
- 4.32. A interface LDAP deve suportar designação automática de acessos SCA baseada nos dados contidos no registro LDAP.
- 4.33. A funcionalidade LDAP deverá suportar as seguintes funções:
- 4.33.1. Nome do servidor LDAP e número da porta definida pelo usuário;
 - 4.33.2. Um nome único da base para a raiz de pesquisas;
 - 4.33.3. Um filtro de pesquisa LDAP para refinar as pesquisas de objetos;
 - 4.33.4. Mapeamento de atributos para os campos de pessoas;
 - 4.33.5. O uso de nome único para autenticação no LDAP;
 - 4.33.6. Opção de pesquisa em todos os sub-níveis do diretório desde a base;
 - 4.33.7. Prever dados de exemplo baseados nos parâmetros de importação LDAP do SCA;
 - 4.33.8. Acessos automáticos no SCA baseados em funções de campos de dados;
 - 4.33.9. Importação automática das entradas do diretório do LDAP para gestão de usuários e operadores do sistema;
 - 4.33.10. Autenticação via conta de usuário LDAP e SSL;
 - 4.33.11. Designação automática de acessos ao SCA por meio de grupos ou diretamente nos usuários.

- 4.34. O sistema deve ter a capacidade de reportar condições anormais de segurança de forma audível e visual.
- 4.35. O sistema deve controlar os equipamentos a partir da estação de monitoramento pelo uso de ações manuais, eventos e listas de causas.
- 4.36. O sistema deve prover registro e gerenciamento de dados pelo uso do arquivo histórico (arquivamento e visualização), trilha de auditoria e procedimentos de importação e exportação manual ou automática (dados e imagens).
- 4.37. O sistema deve ter compatibilidade com o Protocolo de Dispositivo Aberto Supervisionado (OSDP) para comunicação das leitoras com a central.
- 4.38. A proteção de dados será considerada como prioridade máxima. Para tanto, o fabricante deverá atender a Lei Geral de Proteção de Dados, promulgada pela Lei nº 13.709, de 14/08/2018, respondendo as determinações da ANPD (Autoridade Nacional de Proteção de Dados).
- 4.39. A arquitetura padrão de rede de dados deve ser baseada em topologia TCP/IP entre os elementos de controle e comando.
- 4.40. Deve ser composto pelos elementos finais de controle de acesso, controladoras e módulos de entrada/saída.
- 4.41. Todos os controladores de acesso são considerados controladoras de portas inteligentes, capazes de operar de forma independente em caso de perda de conexão, se comunicar diretamente aos servidores sem necessidade de equipamentos intermediários, devem utilizar protocolo de comunicação TCP/IP entre os controladores de acesso e o servidor de aplicação Principal.
- 4.42. O sistema poderá conter elementos adicionais para interoperabilidade com o Servidor de Aplicação Principal.
- 4.43. Os dispositivos de acesso podem ser dedicados a uma única função ou recurso, ou possuir capacidade de múltiplos recursos ou funções acopladas em um único dispositivo, tais como leitores de cartão, reconhecimento facial, biometria, voz, vídeo, teclado.

Módulos:

- 4.44. O software de Controle de Acesso deverá ofertar, minimamente, os seguintes módulos:

- 4.44.1. Cadastro e gestão de servidores ativos, servidores aposentados, estagiários e colaboradores;

- 4.44.2. Cadastro e gestão de visitantes;
 - 4.44.3. Cadastro e gestão de acesso de veículos;
 - 4.44.4. Cadastro e gestão de empresas;
 - 4.44.5. Gestão de permissão de portas controladas (salas técnicas);
 - 4.44.6. Módulo de administração do sistema;
 - 4.44.7. Módulo do operador do sistema; e
 - 4.44.8. Módulo de integração com sistema de CFTV.
- 4.45. O SCA deverá possibilitar agregação de, pelo menos, 10 novos campos adicionais livres com definição de rótulo nas respectivas interfaces.
- 4.46. Os campos adicionais poderão ser adicionados, eliminados ou editados por um administrador.
- 4.47. Campos adicionais podem ser editados para diferentes tipos de dados, como texto, número, data, hora, check box e caixa de combinação.
- 4.48. O SCA deverá permitir a configuração de campos obrigatórios que devem estar devidamente preenchidos para a liberação de cadastros de usuários, veículos e visitas.
- 4.49. O SCA deverá permitir a validação de digitação de CPF e placas de veículos por meio de máscara de entrada de dados ou equivalente de forma que não sejam incluídos dados de identificação inválidos nos cadastros de usuários e veículos.
- 4.50. Suportar a captura de fotos de usuários e documentos por meio de webcam, scanner, importação de arquivo de imagem ou câmera interligada ao sistema de CFTV.
- 4.51. O SCA deverá permitir que o administrador da Contratante gerencie perfis, permitindo a atribuição de privilégios a cada operador para visualizar, operar, alterar ou excluir, dentre outras funcionalidades.
- 4.52. O SCA deverá contar com particionamento lógico do banco de dados, de modo que cada departamento possa configurar controladores, leitores, níveis de acesso e cartões de maneira independente, porém mantendo a centralização do banco de dados. Com a segmentação do banco de dados deverá ser possível limitar a visualização dos usuários, eventos, cadastros, equipamentos etc., aos quais os operadores têm acesso, ou seja, cada operador só irá visualizar os itens da sua respectiva unidade.
- 4.53. O SCA deve ter botões disponíveis para os operadores monitorarem o estado de funcionamento das portas controladas, incluindo: desativar; bloquear; desbloquear; permitir.

- 4.54. Permitir comunicação com os sistemas de prevenção e detecção de incêndio conforme detalhamento dos serviços de integração.
- 4.55. O SCA deve permitir, em tempo real, o cadastro de colaboradores em grupos de acessos para as portas controladas onde o grupo de acesso será criado pelo administrador do sistema e gerenciado por titular da unidade (controle de privilégio, concessão e exclusão de acesso).
- 4.56. O software deve possibilitar o cadastramento de data de início e término de validade de acesso por usuário e veículo; controlar os dias e horários de acesso de cada usuário e veículo.
- 4.57. O sistema para registro de pessoas deve ser acessível em um navegador da web padrão (Edge, internet explorer, chrome etc.).
- 4.58. Para cadastro de servidores, estagiários e colaboradores deve-se ter, no mínimo, os seguintes dados obrigatórios:
- 4.58.1. Nome completo;
 - 4.58.2. CPF ou outro documento oficial;
 - 4.58.3. Foto para biometria facial com resolução mínima de 150 x 150;
 - 4.58.4. Cargo/função;
 - 4.58.5. Endereço (edifício, andar, sala);
 - 4.58.6. Unidade de lotação;
 - 4.58.7. E-mail; e
 - 4.58.8. Telefone.
- 4.59. O sistema deverá permitir buscar o usuário a partir do nome, documento ou qualquer outro campo customizado presente no cadastro do usuário.
- 4.60. O sistema, em tempo real, deve permitir o acompanhamento de visitantes de forma integrada ao CFTV para controlar a intrusão a áreas não liberadas.
- 4.61. As portas controladas estarão vinculadas aos locais indicados pela Contratante (por meio de grupo de acesso) e a gestão será realizada pelo ponto focal de cada unidade demandante, pesquisando os dados do colaborador, visando conceder ou retirar a permissão de acesso à determinada porta. Além disso, deverá permitir o acesso por dia e horário (exemplos: não permitir o acesso após as 20h; não permitir o acesso aos finais de semana).

Funcionalidades:

4.62. O Sistema de Controle de Acesso deve fornecer 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.

4.63. O Sistema de Controle de Acesso deve permitir:

4.63.1. A composição de níveis de acessos, agilizando o gerenciamento de múltiplos pontos de controle de uma mesma sala;

4.63.2. A composição de níveis de acessos ilimitados;

4.63.3. O controle do número máximo de elementos simultâneos em uma determinada área;

4.63.4. A contagem de pessoas.

4.63.5. A configuração de intertravamento entre as portas controladas; e

4.63.6. Desativar a regra de intertravamento para determinado usuário, quando necessário.

Exigência de dupla autenticação

4.64. Deve possuir funcionalidade que permita exigir do usuário dupla autenticação (biometria e cartão de aproximação, por exemplo) para liberação dos dispositivos de controle de acesso (catracas, cancelas, etc).

4.65. Assim, o gestor do sistema deve poder configurá-lo para que os dispositivos de controle de acesso exijam a autenticação biométrica seguida da autenticação via cartão de proximidade (ou vice-versa) para, só então, liberar a passagem do usuário.

Verificação de acesso em sequência:

4.66. Deve ser fornecida uma verificação de sequência de acesso, permitindo que usuários entrem em uma área somente quando eles tiverem passado seu acesso na área vizinha.

Dupla entrada:

4.67. Possuir controle de anti dupla entrada (APB).

4.68. Permitir a configuração de tempo independente, de entrada e de saída, quando a funcionalidade APB for ativada.

4.69. Permitir desativar para determinado usuário a funcionalidade APB, quando ativada de modo geral.

Codificação QR-Code:

4.70. O sistema deverá fornecer uma aplicação com interface online para geração personalizada de QR-Code.

- 4.71. A solução deverá gerar QRCode com a possibilidade de impressão de etiquetas personalizadas sem a necessidade de qualquer aplicação externa.
- 4.72. A solução deverá permitir ainda a criação de múltiplos layouts de impressão de etiquetas QRCode, selecionáveis no momento da impressão, e cada um destes layouts poderá ser personalizado com a inclusão de quaisquer campos de cadastro dos usuários, visitante ou do visitado, foto do visitante, além de instruções customizáveis para visitante.
- 4.73. O código poderá ser gerado tanto na versão física a ser impressa, quanto na versão digital que poderá ser acessada e utilizada em smartphones.
- 4.74. A solução possibilitará o uso do recurso de impressão do ingresso/voucher ou por meio de aplicativo para celular, ambos contendo código QR-CODE para leitura nos equipamentos de permissão de acesso.
- 4.75. Os códigos gerados devem ser habilitados a operarem como recurso de autenticação de acesso dos leitores biométricos a serem ofertados nesta solução.
- 4.76. Deve possibilitar, por interface online, a geração de QR-Code de acesso aos usuários cadastrados no sistema, de modo que esse recurso de autenticação de acesso seja embutido em aplicações das Contratantes, por meio de API a ser disponibilizada pela Contratada (ex: envio automático do QR Code para participantes cadastrados em determinado evento).
- 4.77. A aplicação deverá possuir a configuração de vincular cada código a um determinado período de uso ou para uso permanente, conforme o caso.
- 4.78. Deverá possibilitar a inabilitação temporária e automática dos QR-Codes gerados.
- 4.79. A aplicação possibilitará a funcionalidade de um pré-cadastro a ser disponibilizada aos usuários que pretendam acessar às dependências da Contratante, a ser utilizada em casos de eventos ou de situações que gerem uma grande quantidade de usuários para ingresso aos prédios do TCU.
- 4.79.1. No pré-cadastro, o visitante deverá inserir os seus dados pessoais e tirar uma foto para cadastro biométrico usando o seu próprio dispositivo eletrônico (computador, smartphone, etc).
- 4.79.2. A aplicação deve permitir que, após o usuário já ter concluído seu pré-cadastro, o operador do sistema de controle de acesso possa visualizar a respectiva solicitação de acesso, inclusive podendo previamente autorizá-la ou negá-la.
- 4.79.3. Essa funcionalidade deve permitir que o pré-cadastro fique bloqueado até autorização do operador do sistema de controle de acesso da Contratante.



4.80. A solução deve ser exclusiva de uso da Contratante, devendo possuir design personalizado com Logotipo do TCU.

4.81. Os dados constantes do sistema de controle de acesso em operação no TCU deverão ser migrados para a aplicação para geração de QRCode.

Gestão de visitantes:

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

4.83. Permitir a captura de fotos de visitantes, com uso de câmeras nas portarias.

4.84. 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.

4.85. Permitir a baixa automática do cartão (ou do QR Code) do visitante após a passagem pela saída de visitantes, quando for utilizada urna associada à catraca.

4.86. Permitir número ilimitado (na ordem de milhões) de visitantes cadastrados ao sistema.

4.87. Permitir a configuração de alarmes para visitas expiradas.

4.88. Permitir o agendamento de visitas, a fim de agilizar a operação da recepção.

4.89. Permitir registrar o motivo da visita e a pessoa que autorizou a entrada do visitante.

4.90. O sistema deve permitir consultar ou sinalizar se o visitado está presente no momento da visita.

4.91. Permitir inserir mensagens de orientação na portaria para visitantes pré-cadastrados que precisem de acompanhamento ou avisar por telefone a um funcionário.

4.92. Permitir limitar o número de visitantes por lotação ou faixa horária a uma área controlada.

4.93. 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.

4.94. A solução deverá permitir a gestão do envio de convites para visitantes e eventos, via interface web responsiva e mobile.

4.95. O aplicativo deverá ter versões disponíveis pelo menos nas lojas App Store, para dispositivos com sistema operacional iOS, e Play Store, para dispositivos com sistema operacional Android.

4.96. A solução deverá permitir a criação de múltiplos tipos de convites personalizados:

4.96.1. Cada tipo de convite deve suportar a inclusão de campos customizados, incluindo campos de controle de veículos.

- 4.96.2. Os convites podem ser configurados para permitir a liberação automática ou exigir uma autorização prévia, dos visitantes e veículos.
- 4.97. A solução deverá gerar para o visitado, notificações via aplicativo, browser e e-mail, relacionadas a todas as etapas da gestão da visita.
- 4.97.1. O e-mail de notificação deverá exibir os dados do visitante e do veículo.
- 4.98. Após ser notificado do registro do visitante, o visitado ou organizador do evento poderá autorizar ou negar um cadastro.
- 4.99. Após ser notificado da chegada do visitante, o visitado ou organizados do evento poderá autorizar, adiar ou negar a visita.
- 4.100. A solução deverá permitir o envio de convites personalizados em lote por meio de upload de arquivo de dados para a autorização em massa de entrada de visitantes e veículos.
- 4.101. O visitado poderá enviar convites de forma automática por meio de sistemas de controle de agenda com suporte a arquivos .ics.
- 4.102. A solução deverá permitir, no processo de autocadastro, que o visitante capture a própria foto e essa seja utilizada como credencial de acesso nos equipamentos de reconhecimento facial.
- 4.103. A solução, deverá possuir soluções alternativas de credencial, como: QRCode dinâmico, credencial mobile, leitura de placa para o acesso de veículos etc.
- 4.104. A solução deverá permitir o uso de leitores móveis de credencial para a liberação de acesso aos eventos realizados em locais não controlados.

Agrupamento das pessoas cadastradas:

- 4.105. O sistema deve permitir o agrupamento das pessoas cadastradas em várias categorias, com funcionalidades distintas, tais como: autoridades, servidores, prestadores de serviço, estagiários, visitantes, por empresa ou novas categorias criadas pela Contratante.
- 4.106. Permitir o bloqueio ou liberação de um grupo.
- 4.107. Permitir editar um campo de todos os elementos de um grupo (edição em lote).

Gerenciamento de Estacionamento:

- 4.108. Permitir configuração para controle de limite de vagas para veículos nos estacionamentos.
- 4.109. Permitir o acesso de veículos através da leitura da placa do veículo (LPR).
- 4.110. O sistema deve permitir a liberação prévia a visitantes por meio de cadastramento de placa.

4.111. Permitir o cadastro de veículos e a associação com os respectivos proprietários.

4.112. Os veículos que podem acessar os estacionamentos do TCU são registrados em sistema próprio do TCU chamado SEG. O SCA deve ser capaz de receber as informações desses veículos e fazer a liberação de acesso dos veículos cadastrados.

4.113. Emergência:

4.114. 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).

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

4.116. Deve ser capaz, inclusive, de acionar os elevadores de forma integrada e automatizada que possibilite os equipamentos descenderem para o térreo e abrirem as portas.

4.117. Deve ser capaz de interagir com o Sistema de Detecção de Alarme e Incêndio para que abra as catracas e cancelas quando houver algum sinistro.

Monitoração:

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

4.119. Permitir que, ao tratar um evento de alarme, o operador registre anotações.

4.120. Permitir monitorar em tempo real o acesso dos usuários, mostrando os dados como: nome do usuário, foto do usuário, número do identificador (se houver), nome da controladora/ponto de acesso, data e hora do acesso, e método de identificação.

4.121. Permitir o rastreamento de usuários.

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

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

4.124. 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, , iniciação de programas e sobreposição de tela nos eventos com maior prioridade.

Relatórios do Sistema:

4.125. Possuir ferramenta de relatórios com layout e consulta totalmente customizáveis pelo usuário, com rotina de impressão em formato A4 e com exportação para diversos formatos de arquivo, como: doc, csv, xls e pdf.

4.126. A ferramenta deverá permitir customizar relatórios por ampla variedade de tipos de campos, como: o órgão de lotação, nomes, CPF, cartão ou intervalo de cartões, por ponto de controle de acesso, cartões provisórios pendentes, empregados, por período e horário.

4.127. A ferramenta deverá permitir a emissão de relatórios com aplicação de filtros a fim de contabilizar o número de acessos baseado em critérios diversos, tais como: tipo, empresa, data, tipo de bloqueio.

4.128. A ferramenta deverá permitir o download e o envio automático de relatórios por e-mail.

4.129. A ferramenta deverá permitir agrupar os relatórios por categoria, a fim de criar maior gestão e organização.

4.130. A ferramenta de criação de relatórios deve utilizar os dados diretamente das tabelas do sistema sem a necessidade de criação de uma estrutura de informação complementar, ou seja, uma base de dados paralela.

4.131. Os relatórios deverão conter elementos gráficos (imagens, logotipo) na definição dos relatórios, que serão disponibilizados pela Contratante.

4.132. Devem ser gerados relatórios de visitantes, cartões provisórios, controle de acesso, aferição de temperatura, controle de itens e guarda volumes, cadastro de veículos e entrada e saída de veículos.

Administração:

4.133. O sistema deve ser capaz de cadastrar os administradores com diversos níveis de permissão e com limitação do horário em que dado administrador tem acesso.

4.134. Deverá 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.

4.135. Deverá ser possível o envio de e-mails automáticos em caso de eventos de alertas.

4.136. Deverá utilizar criptografia na comunicação de todos os dados trafegados.

4.137. Deverá prover auditoria de ações dos usuários, inclusive dos administradores, com possibilidade de filtro de pesquisa.

4.138. Deverá possibilitar a customização dos perfis dos usuários, permitindo a criação de perfis de forma ilimitada.

4.139. Deverá ser possível inserir 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.

4.140. Deverá possuir administração completa e integrada de operadores senhas, com validade e complexidade.

4.141. Deverá possuir controle de credenciamento e operação no sistema por estação de trabalho e horários.

4.142. Deverá possuir auditoria completa de qualquer alteração realizada pelo operador do sistema para, no mínimo: data e horário da operação, usuário que fez a alteração, e o que foi alterado.

Gestão de dispositivos:

4.143. O SCA deve possibilitar o cadastro, consultas, alteração e exclusão dos equipamentos controladores, suas respectivas leitoras e demais dispositivos utilizados na solução de controle de acesso pelo TCU.

4.144. Além das informações básicas tais como: nome, descrição e endereço IP, o sistema deverá possibilitar vincular uma ou mais câmeras ao equipamento.

4.145. Deverá possibilitar a verificação de status e controle do funcionamento em tempo real dos equipamentos.

4.146. A supervisão e controle desses dispositivos deverá ser realizada por meio de telas gráficas.

4.147. Deverá possibilitar o envio de comandos para os equipamentos cadastrados.

4.148. Os comandos devem possibilitar o bloqueio, o desbloqueio e a normalização dos equipamentos.

4.149. Permitir enviar e-mail de alerta sobre falha e retorno de comunicação com a controladora, para análise de manutenção preventiva.

4.150. Permitir o agendamento de abertura e/ou travamento do ponto de controle de acesso sem intervenção de operador.

4.151. Permitir gerar alerta na falta de alimentação elétrica.

4.152. Permitir gerar alerta quando a bateria da fonte estiver com baixa tensão.

4.153. Permitir gerar alerta quando a bateria da fonte não estiver mais carregando.

Customizações:

4.154. Caso não haja funcionalidades nativas para cumprimento integral dos itens definidos nas sessões “gestão de visitantes” e “relatórios”, a Contratada deverá realizar customizações

e parametrizações de forma integrada ao Sistema de Controle de Acesso, e que atenda as funcionalidades supracitadas.

4.155. A comprovação da qualidade e segurança da integração das funcionalidades terá validação que deverá abranger todas as etapas, que compreende planejamento, programação, teste, documentação e operação.

4.156. A Contratada assumirá todos os custos referentes à integração das funcionalidades, que deverão constar na apresentação de suas propostas, não sendo a Contratante responsável por custos adicionais.

Outros requisitos:

4.157. O sistema deve suportar diversos acessos simultâneos nas catracas e cancelas a fim de evitar filas nas catracas.

4.158. O sistema não deve permitir dupla entrada ou dupla saída, ou seja, quem entrou deve sair para entrar novamente.

4.159. Deve suportar a adição de novos pontos de controle de acesso (portas, cancelas e catracas).

4.160. O sistema deve possuir cadastro de blacklist (lista de pessoas não autorizadas a acessarem a edificação).

4.161. Garantir o acesso às informações do banco de dados ao final do contrato, com disponibilização e integração entre banco de dados.

4.162. O sistema deve fornecer o registro de data, horário de entrada e horário de saída de servidores, colaboradores, estagiários e visitantes, bem como de veículos que acessaram as dependências do TCU.

4.163. O SCA deve manter um log com histórico de eventos de auditoria de todas as ações executadas, contendo data e hora, usuário responsável por qualquer inclusão, alteração e exclusão de dados e possibilidade de consulta e pesquisa do conteúdo.

4.164. O sistema de controle de acesso também deve permitir:

4.164.1. O bloqueio por controle de documentos do usuário;

4.164.2. O alerta para o operador quando o usuário tiver alguma restrição ao acesso;

4.164.3. O cadastramento de identificadores (QR Code, por exemplo) individualmente ou em lotes;

4.164.4. A configuração de servidor NTP;

- 4.164.5. A criação de status de usuários com a opção de bloqueio de acesso;
 - 4.164.6. A captura de foto do momento do acesso;
 - 4.164.7. Que o operador crie atalhos de funcionalidades para agilizar a operação.
- 4.165. O software deve suportar a funcionalidade de acesso assistido, em que, após o usuário se identificar, o operador receberá em tela a solicitação de acesso e, após conferência, o operador poderá ou não liberar remotamente o acesso ao ambiente.
- 4.166. O sistema deverá possuir perfeita integração com os dispositivos de reconhecimento facial.
- 4.166.1. A integração deverá permitir o cadastro de foto por usuário por meio da própria interface web, dispensando o uso de softwares de terceiros.
- 4.167. O Sistema de Controle de Acesso deve fornecer fusos horários configuráveis para gerenciar períodos de acesso restrito e irrestrito. Estes fusos horários podem restringir o acesso a diferentes grupos de acesso.
- 4.168. Os fusos horários estarão sujeitos a um calendário configurável, que rastreia feriados definidos pelo utilizador. Todos os fusos horários serão definidos por dia, horas e minutos.
- 4.169. O Sistema de Controle de Acesso deve ser concebido de tal forma que falhas locais não venham implicar falha de todo o 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.
- 4.170. O Sistema de Controle de Acesso deve suportar, no mínimo, 20 estações de trabalho operando nas recepções ao mesmo tempo.
- 4.171. Prever diversas situações para controle de usuários, tais como ativos, inativos, férias, desligados.
- 4.172. O cadastramento para reconhecimento facial deve ser feito uma única vez e propagado para os demais equipamentos.
- 4.173. O cadastramento facial deve poder ser feito nas estações de cadastro ou pelo próprio usuário por meio de seu smartphone, utilizando link exclusivo para cadastro a ser enviado para o usuário por e-mail.
- 4.174. Deve ser possível importação e exportação de cadastro de usuários do sistema de controle de acesso.

4.175. O sistema deve permitir a comunicação com bancos de dados de segurança pública e do sistema judiciário a fim de buscar informações relacionadas aos cadastros de pessoas e veículos.

4.176. O sistema deverá suportar a conferência em tempo real de dados de pessoas e veículos em bases de dados externas, no momento do cadastro ou liberação, de forma que usuários ou veículos com restrições sejam impedidos de ter o seu acesso liberado de forma direta.

4.177. O sistema deverá permitir integração ao sistema de gestão de ponto e frequência existente, tanto para importar os cadastros e faixas horárias dos servidores quanto para exportar as marcações de ponto feitas por meio de terminais dedicados ao controle de ponto ou por meio dos periféricos utilizados para controle de acesso físico.

4.178. O sistema deverá permitir integração futura com sistemas de videomonitoramento com, no mínimo, as seguintes funções:

4.178.1. Associação de câmeras à equipamentos do controle de acesso, permitindo a visualização de imagens associadas aos eventos desses equipamentos. O operador poderá visualizar imagens armazenadas no sistema de VMS nos horários da ocorrência de eventos através da interface do sistema de Controle de Acesso.

4.178.2. Utilização de câmeras ou webcams configuradas no sistema de VMS para registro de fotos e/ou documentos. Armazenando as fotos no servidor, de forma que seja possível visualizá-las a partir de qualquer estação de cadastramento.

4.178.3. Consulta de imagens armazenadas, com opção de busca por data e hora.

4.178.4. Envio de todos os alarmes e eventos gerados no sistema de controle de acesso sejam enviados em tempo real para o sistema de VMS.

4.178.5. Envio de informações de usuários, como face, regras de acesso, e horários de acesso sem a necessidade de interface ou aplicação terceira para sincronização dos dados. A plataforma de acesso deverá estar atualizada com todos os pacotes de atualizações disponibilizados pelo fabricante;

4.178.6. Monitoramento do status da câmera;

4.178.7. API nativa para o carregamento de usuários, seus respectivos dados cadastrais e fotos, de forma individual ou em lote.

4.179. Compartilhar informações e gerar alarmes em tempo real.

- 4.180. Visualizar imagens armazenadas no VMS, nos horários da ocorrência de eventos por meio da interface do sistema de Controle de Acesso, com opção de busca por data e hora.
- 4.181. Visualizar imagens ao-vivo, utilizando telas com layouts customizados.
- 4.182. Selecionar eventos que podem gerar alarmes dentro do VMS. Como exemplo, quando ocorrer o reconhecimento de uma pessoa em área não autorizada.
- 4.183. Gerar alertar em formato de pop-up, dentro do sistema operacional Windows.
- 4.184. No momento dos registros de fotos dos usuários via câmeras ou API o SCA deverá ser capaz de recortar automaticamente a foto de forma que o rosto da pessoa cadastrada fique enquadrado de forma centralizada na imagem.
- 4.185. Adicionalmente o SCA deverá verificar de forma automática e parametrizável se a foto capturada atende aos requisitos mínimos de formato e qualidade para ser usada em um sistema de reconhecimento facial.

5. CATRACAS

Requisitos comuns a todos os tipos de catracas

- 5.1. Devem ser montadas em gabinetes balcão de forma a criar passagens/corredores por onde os usuários poderão acessar.
- 5.2. As barreiras devem ser transparentes.
- 5.3. Estar em conformidade com os regulamentos de evacuação, legislação e determinações do Corpo de Bombeiros do local.
- 5.4. Serem do tipo barreira de vidro de segurança temperado, policarbonato ou acrílico, possibilitando vão de acesso de mínimo 50 cm, ou 90 cm na versão para acesso PcD – pessoa com deficiência.
- 5.5. Deverão possuir sensores na extensão do gabinete para monitorar o fluxo de acesso dos usuários e inibir acesso de “caronas”.
- 5.6. Deverão possuir mecanismo motorizado automático para abertura das barreiras e sistema de amortecimento de impacto.
- 5.7. Sistema de abertura anti-pânico, em que, em caso de emergência ou falta de energia, as barreiras de bloqueio se abrem automaticamente. Para isso, as catracas devem ser capazes de receber sinais externos de sistemas de detecção de alarme e incêndio e outros sistemas.
- 5.8. Deverão possuir pictograma operacional ou luz indicando o modo Stand By, acesso liberado ou bloqueado, bem como luzes ou pictogramas para sinalizar ao usuário a operação do equipamento e o sentido de fluxo.
- 5.9. Deverão possuir alimentação elétrica de 220V e ter dispositivos de proteção contra surtos e curto-circuito.
- 5.10. As catracas devem possuir bateria interna, em caso de falta de energia para abertura imediata das folhas.

- 5.11. Deve possuir abertura e capacidade de passagem para usuários pedestres e para usuários de cadeira de rodas de acordo com a ABNT NBR 9050, mantendo conforto e acessibilidade para todos os usuários.
- 5.12. Deve permitir o funcionamento de todos os corredores de passagens de forma simultânea (acessos multipassagens de rápido fluxo), ou seja, a passagem de um usuário em um corredor não deve bloquear os demais corredores.
- 5.13. Em síntese, dever possuir, no mínimo os seguintes modos de operação:
- 5.13.1. Passagem simples na direção configurada.
 - 5.13.2. Passagem bidirecional.
 - 5.13.3. Passagem livre na direção configurada (opcional).
 - 5.13.4. Sempre liberada ou sempre travada.
- 5.14. Deverão permitir a leitura ótica, por imagem, sem nenhum contato físico da pele com o sensor possibilitando uma leitura rápida e higiênica.
- 5.15. Deverá possuir MCBF mínimo de 5.000.000 (cinco milhões) de ciclos de acionamentos, sendo um ciclo considerado uma abertura e um fechamento completo;
- 5.16. Deverá funcionar de forma suave e sem ruídos, garantindo que o mecanismo não esteja atuando de forma rústica para assim aumentar sua longevidade e garantir conforto e segurança aos usuários;
- 5.17. Possuir sistema de travamento, que controlam o fluxo de usuários de forma independente (entrada e saída).
- 5.18. Possibilitar integração com os sistemas de CFTV, de detecção e alarme de incêndio (SDAI) e outros sistemas internos do TCU, conforme detalhado nos serviços de integração.
- 5.19. Tempo de destrave máximo: 0,7 s.
- 5.20. Taxa de passagem: 20 pessoas / min.
- 5.21. Acionamento via contato seco, com acionamento independente para cada direção;
- 5.22. Ser fabricada com componentes industriais de alta durabilidade.
- 5.23. Todo o corpo do gabinete deve possuir estrutura totalmente lisa, ou seja, sem quaisquer parafusos de fixação para fora de sua carcaça.
- 5.24. Deverá possuir sistema de amortecimento de impacto no sistema de transmissão do motor, reduzindo assim o ruído do conjunto.
- 5.25. A fixação das catracas deverá ser realizada diretamente ao chão através da base do gabinete;
- 5.26. A estrutura das catracas deverá ser resistente de modo a garantir a segurança em caso de vandalismo e/ou má utilização por parte dos usuários;
- 5.27. Seu gabinete deverá comportar a adição de componentes de acesso, como fontes, placas, e módulos controladores bem como leitoras e validadores de acesso diversos, respeitando seu espaço interno;

- 5.28. Deverá permitir passagens unidirecionais e bidirecionais, funcionando de acordo com a configuração do ambiente, com os pictogramas atuando de forma ao controle conforme a configuração definida;
- 5.29. No ato de acesso, o bloqueio deverá possuir capacidade de emissão de feedbacks sonoros como acesso liberado e negado;
- 5.30. O controle de pictogramas e demais facilidades da catraca devem ser realizados pela controladora interna da catraca, sem adição de quaisquer elementos;
- 5.31. Deverá ser entregue com espaço montado com suporte para leitoras, pictogramas, monitores de acesso, entre outros dispositivos de integração e controle. A tampa do display deverá permitir a comunicação de proximidade para casos de leitoras de proximidade, garantindo que não tenha interferência entre a leitora e o crachá;
- 5.32. Deve possuir pictogramas indicativos em ambos os lados de acesso, permitindo facilmente a identificação das passagens disponíveis para o usuário na direção em que ele irá acessar o bloqueio;
- 5.33. A identificação deverá ser feita por pictograma de duplo display ou superior possuindo, no mínimo, cores verde e vermelha. Quando um usuário for validado em uma das direções, deverá possuir recurso onde o pictograma do lado oposto automaticamente se torna vermelho para orientar os usuários em casos de acessos bidirecionais, reduzindo a incidência de dupla validação e tentativa de acessos contrários;
- 5.34. Os pictogramas devem ser confeccionados em LED de alto brilho, com uma proteção acrílica fumê ou vidro de diversas tonalidades, e um dispositivo de feedback sonoro (Buser).
- 5.35. Todos os tipos de catracas a serem fornecidos nesta solução devem possibilitar que o recurso de autenticação de acesso seja, no mínimo, via Smart Card, Biometria Facial e QR-Code para liberação de acesso na entrada e saída.
- 5.36. Todos os tipos de catracas a serem fornecidas nesta solução devem conter mediante serviço de manutenção e suporte a garantia de no mínimo 24 meses para motorização e placa eletrônica.

CATRACA TIPO 1

Unidade: Conjunto

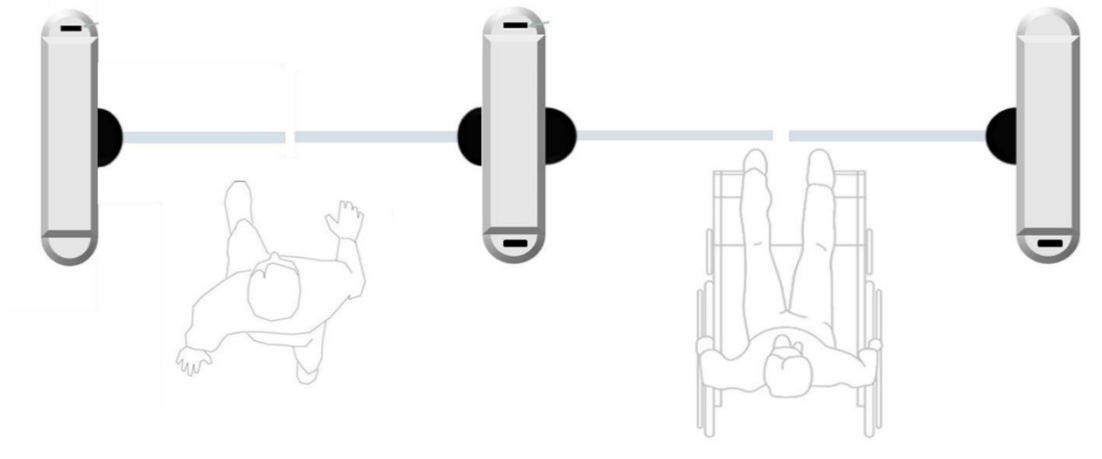
Quantidade: 23

Marcas/modelos de referência: Assa Abloy: VAAFL07; Wolpac: – Wolflap III; e Digicon: dGate AW ou tecnicamente equivalente.

- 5.37. **Critério de Medição:** 50% do valor será pago quando a Contratada fornecer o item e 50% do valor será pago quando ele for instalado, configurado e estiver em pleno funcionamento.
- 5.38. Gabinetes/Balcões do tipo slim.
- 5.39. Tipo de abertura do bloqueio: Flap.
- 5.40. Deverá possuir 2 (dois) corredores de acessos, sendo um de no mínimo 50 cm e outro de no mínimo 90 cm na versão para acesso PcD – pessoa com deficiência.
- 5.41. O corpo do gabinete externo deverá ser confeccionado em aço inoxidável 304 ou superior com chapa de no mínimo 1,2 mm, resistente a choques e vibrações e estrutura

interna em aço de acabamento escovado com baixa rugosidade, garantindo um aspecto visual e mantendo a superfície do material lisa.

5.42. A modelagem desse conjunto deverá obedecer a ilustração a seguir:



5.43. Deverá conter os seguintes módulos/balcões/portões:

5.44. 1 (um) módulo central de duplo mecanismo;

5.45. 1 (um) módulo lateral direito;

5.46. 1 (um) módulo lateral esquerdo;

5.47. 4 (quatro) portões em vidro temperado, policarbonato ou acrílico, de no mínimo 10mm de espessura, sendo 2 (dois) para a versão PcD;

5.48. A Contratada deverá realizar a instalação física e lógica de todos os componentes da catraca, bem com a sua configuração.

5.48.1. Todos os materiais, mão de obra, ferramentas e equipamentos necessários ao fornecimento da infraestrutura de encaminhamento, o cabeamento de dados, o cabeamento elétrico e a conectividade de dados serão fornecidos pela Contratada. O único pagamento a ser feito quanto à infraestrutura será a do item "SERVIÇO DE INSTALAÇÃO DE INFRAESTRUTURA".

5.49. A instalação dos equipamentos e sistemas e a execução dos serviços deverão obedecer ao projeto executivo, que deverá detalhar a infraestrutura necessária.

5.50. O prazo de instalação deverá obedecer ao cronograma elaborado pela contratada e aprovado pela fiscalização.

5.51. Todos os serviços e acessórios necessários às instalações de quaisquer equipamentos previstos na solução são de responsabilidade da Contratada.

CATRACA TIPO 2

Unidade: Conjunto

Quantidade: 1

Marcas/modelos de referência: Assa Abloy: VAAFL07 e VAAFLxxPcD; Wolpac: Wolvision – Wolflap III; e Digicon: dGate AW ou tecnicamente equivalente.

5.52. **Critério de Medição:** 50% do valor será pago quando a Contratada fornecer o item e 50% do valor será pago quando ele for instalado, configurado e estiver em pleno funcionamento.

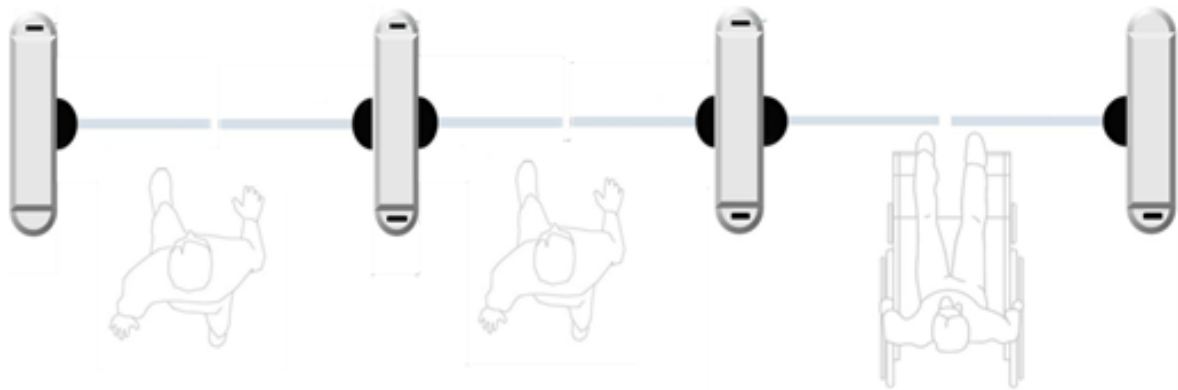
5.53. Gabinetes/Balcões do tipo slim.

5.54. Tipo de abertura do bloqueio: Flap.

5.55. Deverá possuir 3 (três) corredores de acessos, sendo 2 (dois) de no mínimo 50 cm e outro de no mínimo 90 cm na versão para acesso PcD – pessoa com deficiência.

5.56. O corpo do gabinete externo deverá ser confeccionado em aço inoxidável 304 ou superior com chapa de no mínimo 1,2 mm, resistente a choques e vibrações e estrutura interna em aço de acabamento escovado com baixa rugosidade, garantindo um aspecto visual e mantendo a superfície do material lisa.

5.57. A modelagem desse conjunto deverá obedecer a ilustração a seguir:



5.58. Deverá conter os seguintes módulos/balcões/portões:

5.59. 2 (dois) módulos centrais de duplo mecanismo;

5.60. 1 (um) módulo lateral direito;

5.61. 1 (um) módulo lateral esquerdo;

5.62. 6 (seis) portões em vidro temperado, policarbonato ou acrílico, de no mínimo 10mm de espessura, sendo 2 (dois) para versão PcD;

5.63. A Contratada deverá realizar a instalação física e lógica de todos os componentes da catraca, bem com a sua configuração.

5.63.1. Todos os materiais, mão de obra, ferramentas e equipamentos necessários ao fornecimento da infraestrutura de encaminhamento, o cabeamento de dados, o cabeamento elétrico e a conectividade de dados serão fornecidos pela Contratada. O único pagamento a ser feito quanto à infraestrutura será a do item "SERVIÇO DE INSTALAÇÃO DE INFRAESTRUTURA".

5.64. A instalação dos equipamentos e sistemas e a execução dos serviços deverão obedecer ao projeto executivo, que deverá detalhar a infraestrutura necessária.

5.65. O prazo de instalação deverá obedecer ao cronograma elaborado pela contratada e aprovado pela fiscalização.

5.66. Todos os serviços e acessórios necessários às instalações de quaisquer equipamentos previstos na solução são de responsabilidade da Contratada.

CATRACA TIPO 3

Unidade: Conjunto

Quantidade: 6

Marcas/modelos de referência: Assa Abloy: VAA-MSG04; Wolpac: Wolgate III e Digicon: dTower ou tecnicamente equivalente.

5.67. **Critério de Medição:** 50% do valor será pago quando a Contratada fornecer o item e 50% do valor será pago quando ele for instalado, configurado e estiver em pleno funcionamento.

5.68. Modelo adequado para ambientes que possuem pouco espaço.

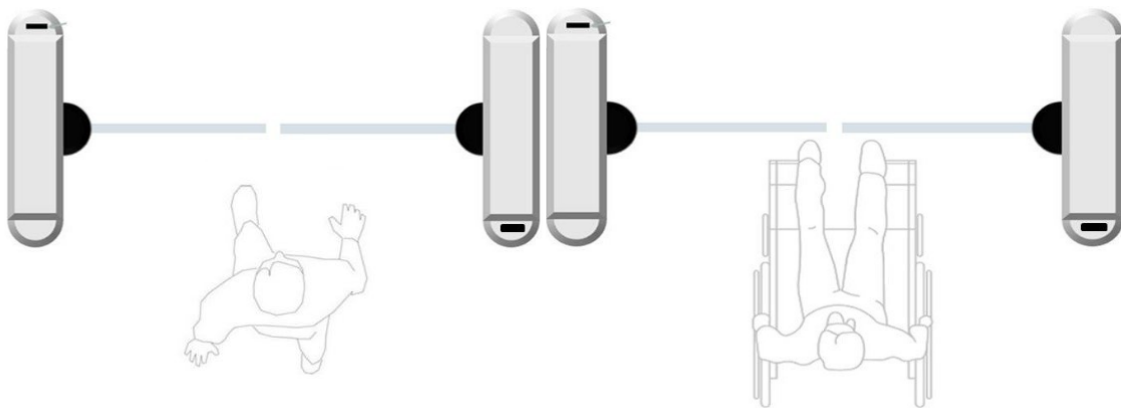
5.69. Gabinetes/Balcões do tipo slim.

5.70. Tipo de abertura do bloqueio: Pivotante ou Flap.

5.71. Deverá possuir 2 (dois) corredores de acessos, sendo um de no mínimo 50 cm e outro de no mínimo 90 cm na versão para acesso PcD.

5.72. O corpo do gabinete externo deverá ser confeccionado em aço inoxidável 304 ou superior.

5.73. A modelagem desse conjunto deverá obedecer a ilustração a seguir:



5.74. Deverá conter os seguintes módulos/balcões/portões:

5.75. 2 (dois) módulos laterais direito;

5.76. 2 (dois) módulos laterais esquerdo;

5.77. 4 (quatro) portões em vidro temperado, policarbonato ou acrílico, de no mínimo 10mm de espessura, sendo 2 (dois) para versão PcD;

5.78. Em função da restrição de espaço nos locais nos quais as catracas serão instaladas, deve possuir um corpo compacto com dimensões máximas de 1100mm de altura, 1000mm de largura e 600mm de profundidade.

5.79. A Contratada deverá realizar a instalação física e lógica de todos os componentes da catraca, bem com a sua configuração.

5.79.1. Todos os materiais, mão de obra, ferramentas e equipamentos necessários ao fornecimento da infraestrutura de encaminhamento, o cabeamento de dados, o cabeamento elétrico e a conectividade de dados serão fornecidos pela

Contratada. O único pagamento a ser feito quanto à infraestrutura será a do item “SERVIÇO DE INSTALAÇÃO DE INFRAESTRUTURA”.

5.80. A instalação dos equipamentos e sistemas e a execução dos serviços deverão obedecer ao projeto executivo, que deverá detalhar a infraestrutura necessária.

5.81. O prazo de instalação deverá obedecer ao cronograma elaborado pela contratada e aprovado pela fiscalização.

5.82. Todos os serviços e acessórios necessários às instalações de quaisquer equipamentos previstos na solução são de responsabilidade da Contratada.

6. CANCELAS DE ACESSO DE VEÍCULOS

Unidade: Unidade

Marcas/modelos de referência: PPA: Barrier Jetflex Brushless; Copiges: CP302 ou tecnicamente equivalente.

Critério de Medição: 50% do valor será pago quando a Contratada fornecer o item e 50% do valor será pago quando ele for instalado, configurado e estiver em pleno funcionamento.

6.1. Cancelas para veículos com haste articulada, ideal para estacionamentos privados com possibilidade de instalação no lado direito ou esquerdo da via, com possibilidade de alteração em campo a mudança da respectiva posição.

6.2. O gabinete da cancela deve ser autossustentável, confeccionado em aço carbono, galvanizado, zincado ou inoxidável com acabamento em pintura eletrostática ou esmalte, tratamento anticorrosivo e preparado para a instalação de acessórios adicionais. O equipamento deve possuir proteção mínima IP54, adequado para operação em ambiente externo, garantindo durabilidade, resistência mecânica e proteção contra poeira e respingos de água.

6.3. As hastes devem ser de alumínio ou liga de alumínio;

6.4. O equipamento deverá possuir os seguintes requisitos de sinalização e iluminação:

6.4.1. Faixas adesivas refletivas ao longo da haste, para aumentar a visibilidade da cancela e chamar atenção do motorista.

6.4.2. Iluminação em LED bicolor (verde/vermelho) para indicar claramente o status do acesso: liberado ou bloqueado. Esta iluminação deverá ser alimentada exclusivamente pela central da cancela, sem utilização de fontes externas, podendo ser disposta ao longo da haste ou na parte superior (coroa luminosa/topo), desde que garanta visibilidade, identificação do equipamento e segurança equivalentes, inclusive em ambientes de baixa luminosidade.

6.4.3. A solução de iluminação deverá possuir baixo consumo de energia, ser compatível com a instalação de acessórios adicionais e atender aos requisitos de durabilidade e operação em ambiente externo.

6.5. Deve utilizar rolamentos ou barra roscada no mecanismo da articulação;

6.6. Deve possibilitar a sua fixação pela direita ou pela esquerda da cancela;

6.7. Deve possuir mecanismo de movimentação com torque motor, através de motor elétrico de consumo máximo de 250W e alimentação 220V, 50/60Hz;

6.8. Deve possuir um tempo de abertura de, no máximo, 3 segundos;

- 6.9. Deve possuir um tempo de fechamento de, no máximo, 4 segundos;
- 6.10. Deve ser projetada para alto fluxo e possuir um desempenho mínimo de 150 ciclos/hora;
- 6.11. Deve possuir elementos mecânicos ou elétricos que permitam o ajuste de balanceamento da haste, de forma que a haste tenha um movimento macio e sem vibrações;
- 6.12. Deve possuir mecanismo ou dispositivo para abertura manual em caso de falta de energia elétrica;
- 6.13. Em caso de ausência de energia, a cancela deve permitir a operação de forma manual de maneira fácil, sem a necessidade do uso de ferramentas e/ou manivelas, opcional utilização de Baterias Internamente nas Cancelas (Placa Gerenciadora , suporte para baterias e 2 baterias 12v 7ah.
- 6.14. As hastes devem ser confeccionadas em alumínio esmaltado branco, com perfil semielíptico ou elíptico (oval), incluindo perfil cobre-vão e perfil anticollisões com borracha de proteção.
- 6.15. Deve ser compatível com o acionamento por meio de reconhecimento da placa dos veículos (LPR)
- 6.16. Deve possuir interface para integração com controladores externos, a exemplo de sistemas SDAI;
- 6.17. Na falta de energia a cancela deverá permitir a operação de forma manual, de maneira fácil e sem a necessidade do uso de ferramentas e/ou manivelas.
- 6.18. Braço haste articulado (retrátil) com dimensão, mínima, compatível com pé-direito de 2,50 m, sendo que o comprimento mínimo das hastes deverá ser de 4 metros.
 - 6.18.1. Demais ajustes acerca do pé direito e do cumprimento exato das hastes serão definidos no projeto executivo, conforme os respectivos espaços físicos onde as cancelas serão instaladas.
- 6.19. A Contratada deverá realizar a instalação física e lógica de todos os componentes das cancelas, bem com a sua configuração.
 - 6.19.1. Todos os materiais, mão de obra, ferramentas e equipamentos necessários ao fornecimento da infraestrutura de encaminhamento, o cabeamento de dados, o cabeamento elétrico e a conectividade de dados serão fornecidos pela Contratada. O único pagamento a ser feito quanto à infraestrutura será a do item "SERVIÇO DE INSTALAÇÃO DE INFRAESTRUTURA".
- 6.20. A instalação dos equipamentos e sistemas e a execução dos serviços deverão obedecer ao projeto executivo, que deverá detalhar a infraestrutura necessária.
- 6.21. O prazo de instalação deverá obedecer ao cronograma elaborado pela contratada e aprovado pela fiscalização.
- 6.22. Todos os serviços e acessórios necessários às instalações de quaisquer equipamentos previstos na solução são de responsabilidade da Contratada.
- 6.23. As cancelas fornecidas nesta solução devem conter mediante serviço de manutenção e suporte a garantia de no mínimo 24 meses para motorização e placa eletrônica.

7. LEITOR FACIAL E DE PROXIMIDADE



Unidade: Unidade

Marcas/modelos de referência: Idemia: VisionPass; Assa Abloy: VF-10K2; HID: Amico 7" | VL70LF; ou tecnicamente equivalente.

Critério de Medição: 50% do valor será pago quando a Contratada fornecer o item e 50% do valor será pago quando ele for instalado, configurado e estiver em pleno funcionamento.

7.1. Devem ser instalados em qualquer dispositivo de controle de acesso (catracas, cancelas etc.).

7.1.1. No caso das cancelas, serão instalados em totens.

7.2. Dever ser instalados e compatíveis com todos os tipos de catracas a serem fornecidos nesta solução, devendo possibilitar que o recurso de autenticação de acesso seja, no mínimo, via Biometria Facial, Smart Card QR-Code para liberação de acesso na entrada e saída.

7.3. Deve ser compatível com o software de controle de acesso ofertado.

7.4. Deve ser capaz de atuar autonomamente (standalone) em caso de desconexão e para fins de controle da catraca em que se encontra.

7.5. Formas de Identificação: Duas câmeras com no mínimo Full HD (1920x1080) operando com luz visível e luz infravermelha.

7.6. Reconhecimento facial com detecção de rosto vivo.

7.7. Distância para leitura de no mínimo 0,70cm a 1,8 metros.

7.8. Velocidade de reconhecimento inferior a 1 segundo.

7.9. Capacidade de identificação de no mínimo 30 pessoas por minuto no modo 1:N.

7.10. Leitor de QR-Code estático e dinâmico (ISO/IEC 18004:2015).

7.11. Cartões de Proximidade e credenciais móveis (NFC e/ou Bluetooth).

7.12. Capacidade para no mínimo 100.000 usuários.

7.13. Capacidade para no mínimo 50.000 faces.

7.14. Streaming de vídeo via Onvif e/ou RTSP.

7.15. O dispositivo deve estar em conformidade com a GDPR/LGPD.

7.16. O dispositivo deve armazenar dados biométricos em formato de templates, ou seja, uma representação matemática da imagem.

7.17. Nenhuma imagem bruta deve ser armazenada no dispositivo, quando assim configurado.

7.18. Os templates armazenados no dispositivo devem ser criptografados por AES 128.

7.19. Protocolo de comunicação OSDP.

7.20. 1 x Entrada ou saída Wiegand nativa.

7.21. Possuir sensores de porta aberta, arrombamento de porta e de violação de equipamento.

7.22. 1 x relé interno ao módulo de acionamento.

7.23. 1 x porta Ethernet 10/100Mbps nativa.

7.24. 1 x porta USB Host 2.0, 1 x RS-485.

- 7.25. Possuir no mínimo, Tela LCD Touchscreen colorido de 7" (1024x600) com tela resistiva sensível ao toque.
- 7.26. Deve possuir certificação Anatel.
- 7.27. Os leitores de reconhecimento facial deverão ter suporte de idioma integrado para interação com o usuário no mínimo, nos seguintes idiomas: Inglês, Português (Brasileiro), Francês e Espanhol.
- 7.28. Nível de proteção mínimo: IP65.
- 7.29. Os leitores faciais deverão ser fornecidos com todos os acessórios e licenças de uso necessários ao seu pleno funcionamento, incluindo softwares, desenvolvimentos e customizações, hardwares, cabos, conectores elétricos e de dados e outros.
- 7.30. A Contratada deverá realizar a instalação física e lógica de todos os componentes dos leitores, bem com a sua configuração.
- 7.30.1. Todos os materiais, mão de obra, ferramentas e equipamentos necessários ao fornecimento da infraestrutura de encaminhamento, o cabeamento de dados, o cabeamento elétrico e a conectividade de dados serão fornecidos pela Contratada. O único pagamento a ser feito quanto à infraestrutura será a do item "SERVIÇO DE INSTALAÇÃO DE INFRAESTRUTURA".
- 7.31. A instalação dos equipamentos e sistemas e a execução dos serviços deverão obedecer ao projeto executivo, que deverá detalhar a infraestrutura necessária.
- 7.32. O prazo de instalação deverá obedecer ao cronograma elaborado pela contratada e aprovado pela fiscalização.
- 7.33. Todos os serviços e acessórios necessários às instalações de quaisquer equipamentos previstos na solução são de responsabilidade da Contratada.

8. SERVIDOR DE GERENCIAMENTO DO CONTROLE DE ACESSO

Unidade: Unidade

Marcas/modelos de referência: Dell: PowerEdge R740; Lenovo: ThinkSystem SR650; HP: ProLiant DL380 Gen10 ou tecnicamente equivalente.

Critério de Medição: 50% do valor será pago quando a Contratada fornecer o item e 50% do valor será pago quando ele for instalado, configurado e estiver em pleno funcionamento.

- 8.1. Deverá ser um equipamento desenvolvido especificamente para a função de servidor, com recursos de processamento adequado para a operação 24x7 em alta carga de processamento.
- 8.2. Vir acompanhado de sistema operacional Windows Server 2019, Windows 10 ou superior instalado de fábrica.
- 8.3. Possuir pelo menos 4Tb de armazenamento em disco (bruto);
- 8.4. Possuir altura de 1U a 2U;
- 8.5. Deve ser compatível de forma nativa com rack padrão 19", não sendo aceitos equipamentos que necessitem de bandejas;
- 8.6. Deve possuir:

- 8.6.1. Memória de 16GB DDR4 ou superior;
- 8.6.2. Pelo menos duas portas de rede gigabit RJ45;
- 8.6.3. Disco SSD 480 GB ou superior para instalação exclusiva do sistema operacional e dos softwares;
- 8.6.4. Placa de Rede Gigabit (10/100/1000).
- 8.6.5. Placa de vídeo dedicada de, no mínimo, 8GB GDDR5, 1683 MHz, com velocidade de 8 Gbps.
- 8.7. Além disso deve vir acompanhado de:
 - 8.7.1. 1 (um) teclado multimídia padrão ABNT-2 em português, na cor preta;
 - 8.7.2. 1 (um) mouse óptico ou laser com fio na cor preta; e
 - 8.7.3. 2 (dois) cabos de alimentação do sistema (português – Brasil).
- 8.8. Deverá possuir sistema de redundância de fontes de alimentação, do tipo Hot-plug, ou superior, já devendo ser fornecido com a fonte principal e a de redundância.
- 8.9. Possuir processamento Intel Xeon escalável da 3ª geração (Ice Lake) ou superior, com pontuação de CPU no benchmark PassMark igual ou superior a 21.000 pontos de multithread.

9. GERENCIADORAS E CONTROLADORAS DE CONTROLE DE ACESSO

Unidade: Conjunto

Critério de Medição: 50% do valor será pago quando a Contratada fornecer o item e 50% do valor será pago quando ele for instalado, configurado e estiver em pleno funcionamento.

- 9.1. A Contratada deverá fornecer e instalar todas as placas gerenciadoras e controladoras necessárias para o pleno funcionamento da solução ofertada.
- 9.2. Como a quantidade de placas depende das particularidades de cada fabricante, este item será pago de forma global para todas as placas necessárias, independentemente da quantidade requerida pela solução de cada fabricante.
- 9.3. Portanto, é dever da Contratada definir a quantidade necessária, que deverá estar abarcada pelo valor global deste item.
- 9.4. As características técnicas das placas deverão ser aquelas necessárias para o funcionamento pleno da solução, sendo compatível com todos os outros equipamentos e componentes incluídos nesta contratação.
- 9.5. A gerenciadora de controle de acesso deverá possuir, no mínimo:
 - 9.5.1. Capacidade de operar de forma autônoma, com processador embarcado.
 - 9.5.2. Armazenamento local de pelo menos 64 mil credenciais e 500 mil eventos.
 - 9.5.3. Suporte a OSDP com criptografia AES-128.
 - 9.5.4. Firmware assinado digitalmente e secure boot.
 - 9.5.5. Capacidade de integrar, ao menos, 8 módulos para expansão.
 - 9.5.6. Suportar no mínimo 32 níveis de acesso por controladora.
 - 9.5.7. Ter opção para alimentação via PoE e 12VDC.

- 9.5.8. Compatibilidade com leitores Wiegand e OSDP.
- 9.5.9. Execução de regras locais, como escolta, antipassback, entre outros, sem necessidade do servidor.
- 9.5.10. Backup de memória e relógio de tempo real: deverá ser respaldado por um supercapacitor ou uma bateria de lítio opcional.
- 9.5.11. Todos os outros dados deverão ser armazenados em memória flash não volátil.
- 9.5.12. Deve possuir suporte para cartão microSD ou micro SDHC com capacidade mínima de 2GB, sendo desejável que chegue a 8GB.
- 9.5.13. Deve possuir suporte nativo a IPv4 e IPv6.
- 9.5.14. Deve suportar criptografia TLS 1.2/1.3.
- 9.5.15. Deve dispor ao menos das entradas: 2 não supervisionadas /supervisionadas, EOL padrão: 1k/1k ohm, 1%, ¼ watt, uma dedicada não supervisionadas para tampo do gabinete.
- 9.5.16. Deve dispor ao menos das Saídas: 2 relés, Forma-C com contatos secos.
- 9.5.17. Deve suportar condições ambientais de 0 a 70°C; 5 a 95% Umidade Relativa (não condensante).
- 9.5.18. Deve possuir certificação de conformidade com os seguintes padrões: CE, RoHS, UL, FIPS 140-3 ou FIPS 140-2.
- 9.6. A contratada deverá fornecer a Controladora com todos os acessórios necessários, tais como: Conectores, fios, fonte de alimentação, e caixa de proteção.
- 9.7. Deve dispor de Alimentação: 12 Vdc $\pm$ 10% regulado, máximo de 300 mA cada leitor.
- 9.8. As entradas de dados devem ser compatíveis com TTL, F/2F ou RS-485 de 2 fios.
- 9.9. Deve dispor de conexão protegida por TLS 1.2/1.1 ou AES-256/128.
- 9.10. A contratada deverá fornecer a Controladora com todos os acessórios necessários, tais como: Conectores, fios, fonte de alimentação, e caixa de proteção.

10. ESTAÇÃO DE CADASTRAMENTO

Unidade: Unidade

Modelos de referência:

- 10.1.1. Unidade de Processamento (CPU com SSD e 8GB RAM): Dell OptiPlex 3000 SFF; HP ProDesk 400 G9 SFF; Lenovo ThinkCentre M70s; ou outro tecnicamente equivalente, sendo todos com Processador Intel® Core™ i5-12500H ou superior;
- 10.1.2. Monitores: AOC 22B2HM; Samsung S22F350FHL; LG 22MP410-B; ou outro tecnicamente equivalente;
- 10.1.3. Teclado e Mouse USB: Logitech MK120; Dell KB216-B + MS116-B; Multilaser TC193 + MO212; ou outro tecnicamente equivalente;

10.1.4. Webcam: Logitech C920s Pro HD; Microsoft Modern Webcam; Redragon Hitman GW800; ou outro tecnicamente equivalente;

10.1.5. Impressora térmica: Zebra ZD500R; TSC TE310; Brother QL-820NWB; ou outro tecnicamente equivalente.

10.2. **Critério de Medição:** 50% do valor será pago quando a Contratada fornecer o item e 50% do valor será pago quando ele for instalado, configurado e estiver em pleno funcionamento.

10.3. Deverá ser um equipamento desenvolvido especificamente para a função de estação tipo cliente (estação de trabalho) que permita operação 24x7 (não serão aceitos equipamentos adaptados ou desenvolvidos para outras finalidades);

10.4. O equipamento cotado deverá ser novo, estar em linha de produção no momento da licitação, sendo possível consultar o site do fabricante para verificação das especificações técnicas;

10.5. Estas especificações devem ser consideradas (quantitativamente e qualitativamente) como exigências mínimas, cabendo a cada proponente analisar as necessidades e compatibilidades com o restante das tecnologias fornecidas, a aplicação descrita e especificada neste certame.

10.6. Nas estações de cadastro de visitantes deverá ser instalado o software de gerenciamento de visitantes totalmente integrado ao servidor de controle de acesso através de API ou SDK com objetivo de interface simples, intuitiva e rápida que permite a identificação e liberação dos visitantes em segundos, eliminando filas na recepção e mantendo os padrões de segurança corporativa.

10.7. Deve possuir processador com arquitetura x86 e x64, com no mínimo 04 (quatro) núcleos, frequência de 2.9 GHz ou superior;

10.8. Possuir, pelo menos, memória instalada de 8GB DDR4 SDRAM;

10.9. Deve possuir 1 (uma) unidade de armazenamento de estado sólido (SSD) com interface SATA III ou NVMe M.2, com capacidade mínima de 256 GB, sendo vedado a utilização de disco rígido (HDD) convencional como armazenamento principal;

10.10. Deve possuir placa de vídeo compartilhada ou dedicada com, no mínimo, 2 (duas) saídas de vídeo;

10.11. Deve possuir interface de rede gigabit RJ-45;

10.12. Deve possuir, no mínimo, 4 (quatro) interfaces USB, vedado o uso de qualquer tipo de adaptador;

10.13. A fonte de alimentação deve ser compatível com o equipamento ofertado e instalada internamente no gabinete;

10.14. Deverão ser fornecidos todos os cabos de alimentação para ativação do equipamento;

10.15. Deve aceitar tensões de 110 a 240 Volts 50-60 Hz;

10.16. Suportar, no mínimo, dois monitores, através das conexões Display Port, DVI ou HDMI.

10.17. Cada equipamento deverá vir com o sistema operacional Microsoft Windows 10 Professional Original 64 bits (OEM), atualizado, em português (Brasil) ou superior,

previamente instalado, licenciado e configurado de modo a reconhecer os elementos de hardware que compõem o sistema, além da etiqueta fixada no gabinete, indicando que o software instalado é original;

10.17.1. A licença fornecida deverá garantir atualizações de segurança gratuitas durante todo o prazo de garantia estabelecida pelo fornecedor do hardware.

10.18. Cada Estação de Cadastro deverá ser fornecida com os seguintes itens/acessórios:

10.18.1. 2 (dois) monitores de LED, tamanho mínimo de 21 polegadas, e resolução mínima de 1920 X 1080 pixels;

10.18.2. 1 (um) Teclado padrão ABNT-2 USB na cor preta;

10.18.3. 1 (um) Mouse óptico USB ou laser na cor preta;

10.18.4. 1 (uma) Webcam com resolução mínima de 1920x1080 pixels e conexão USB; e

10.18.5. 1 (uma) Impressora térmica para impressão de QR CODE para acesso de visitantes, com resolução mínima de 300 dpi.

10.19. A Contratada deverá realizar a instalação física e lógica de todos os componentes das estações, bem com a sua configuração.

10.19.1. Todos os materiais, mão de obra, ferramentas e equipamentos necessários ao fornecimento da infraestrutura de encaminhamento, o cabeamento de dados, o cabeamento elétrico e a conectividade de dados serão fornecidos pela Contratada. O único pagamento a ser feito quanto à infraestrutura será a do item "SERVIÇO DE INSTALAÇÃO DE INFRAESTRUTURA".

10.20. A instalação dos equipamentos e sistemas e a execução dos serviços deverão obedecer ao projeto executivo, que deverá detalhar a infraestrutura necessária.

10.21. O prazo de instalação deverá obedecer ao cronograma elaborado pela contratada e aprovado pela fiscalização.

10.22. Todos os serviços e acessórios necessários às instalações de quaisquer equipamentos previstos na solução são de responsabilidade da Contratada.

11. KIT CONTROLE DE ACESSO PARA PORTAS

Unidade: Unidade.

Critério de Medição: 50% do valor será pago quando a Contratada fornecer o item e 50% do valor será pago quando ele for instalado, configurado e estiver em pleno funcionamento.

11.1. **Tipo:** Porta de acesso – entrada: leitor facial; saída: botoeira.

11.2. Modelo de referência:

11.2.1. Mola Hidráulica: Intelbras Mh 104 A; Papaiz Ud77z; PPA F4; ou outro tecnicamente equivalente;

11.2.2. Fechadura Eletromagnética: Intelbras FE 150 KT 740; AGL AL 150; Ipec A2300/CZ; ou outro tecnicamente equivalente;

11.2.3. Fonte de Alimentação: Intelbras FA 1220S; PPA 2A – FC2A; Ipec A2070; ou outro tecnicamente equivalente;

11.2.4. Bateria 12v: Intelbras XB 1270; Yuasa NP7-12; Unipower UP1270; ou outro tecnicamente equivalente;

11.2.5. Sensor de intrusão: Intelbras XAS CONNECT com fio; Stilus MPIE; Metaltex SM2325; ou outro tecnicamente equivalente;

11.2.6. Leitor facial: ZKTeco SpeedFace V5L; HID Amico VL35LF; Assabloy VF-10K2FP; ou outro tecnicamente equivalente;

11.2.7. Botoeira: AGL 1203036; Intelbras BT 4001; ZKTeco TLEB102; ou outro tecnicamente equivalente.

11.3. A Contratada deverá realizar a instalação física e lógica de todos os componentes do kit, bem com a sua configuração.

11.3.1. Todos os materiais, mão de obra, ferramentas e equipamentos necessários ao fornecimento da infraestrutura de encaminhamento, o cabeamento de dados, o cabeamento elétrico e a conectividade de dados serão fornecidos pela Contratada. O único pagamento a ser feito quanto à infraestrutura será a do item "SERVIÇO DE INSTALAÇÃO DE INFRAESTRUTURA".

11.4. A instalação dos equipamentos e sistemas e a execução dos serviços deverão obedecer ao projeto executivo, que deverá detalhar a infraestrutura necessária.

11.5. O prazo de instalação deverá obedecer ao cronograma elaborado pela contratada e aprovado pela fiscalização.

11.6. Todos os serviços e acessórios necessários às instalações de quaisquer equipamentos previstos na solução são de responsabilidade da Contratada.

11.7. Os kits serão utilizados para acesso às portas de salas técnicas e deverão conter, no mínimo, os itens a seguir.

11.8. **1 (uma) Mola hidráulica:**

11.8.1. Do tipo universal, permitindo a instalação em qualquer tipo de material (madeira, vidro, metal).

11.8.2. Possuir proteção contra corrosão.

11.8.3. Deve suportar portas de até 80kg.

11.9. **1 (uma) Fechadura eletromagnética:**

11.9.1. Possuir acabamento em Aço inoxidável.

11.9.2. Fazer a abertura e o fechamento de forma silenciosa.

11.9.3. Deverá ser acionada por qualquer controle de acesso do mercado.

11.9.4. Temperatura de operação: -5 a 50°C.

11.9.5. Dimensões máximas: 173 x 47 x 28 (A x L x P) mm (margem aceitável de 5cm de variação).

11.9.6. Força de Tração: 150kgf.

11.9.7. Possuir sensor para sinalização do estado de abertura da porta.

11.9.8. As fechaduras devem ser acompanhadas por suportes adequados para facilitar sua instalação em portas e portões, garantindo um encaixe seguro e eficiente.

11.10. 1 (uma) Fonte:

- 11.10.1. Deve possuir entrada bivolt 110/220V a 60Hz;
- 11.10.2. Deve possuir carregador de bateria estacionária integrada;
- 11.10.3. Deve possuir Led's de operação na parte frontal da caixa;
- 11.10.4. Deve possuir tensão de saída estabilizada;
- 11.10.5. Deve vir acompanhada de caixa de proteção fabricada em aço;

11.11. 1 (uma) Bateria 12V:

- 11.11.1. A bateria deve ser de chumbo-ácido regulada por válvula selada VRLA recarregável, livre de manutenção e protegida contra vazamento.
- 11.11.2. Tensão: 12 Vdc.
- 11.11.3. Capacidade: 7 Ah (C20).
- 11.11.4. A bateria deve possuir vida útil de até 5 anos.

11.12. 1 (um) Sensor de intrusão para portas:

- 11.12.1. Dever ser do tipo universal, permitindo a instalação em qualquer tipo de material (madeira, vidro, metal);
- 11.12.2. A comunicação com a controladora deve ser cabeada, não serão aceitos sensores sem fio;
- 11.12.3. Deve detectar a abertura da porta por campo magnético;
- 11.12.4. Deve ser fabricado em ABS branco ou metal.

11.13. 1 (um) Leitores facial:

- 11.13.1. O terminal leitor de reconhecimento facial deve ser integrado ao software de controle de acesso ofertado, podendo também atuar autonomamente (stand alone) em caso de desconexão e para fins de controle da porta de acesso;
- 11.13.2. Formas de identificação:
 - 11.13.2.1. Reconhecimento facial com detecção de rosto vivo;
 - 11.13.2.2. Leitor de QR Code; e
 - 11.13.2.3. Cartões de proximidade;
- 11.13.3. Capacidade para no mínimo 50.000 usuários;
- 11.13.4. Capacidade para no mínimo 10.000 faces;
- 11.13.5. Capacidade para até 200.000 registros de acesso;
- 11.13.6. Capacidade de identificação de no mínimo 30 pessoas por minuto no modo 1:N;
- 11.13.7. Streaming de vídeo via Onvif e RTSP;

11.13.8. Deve possibilitar a leitura de faces dos usuários, de no mínimo, entre 1.2 e 2 metros de altura;

11.13.9. Deve possibilitar que a velocidade de leitura seja de, no mínimo, 1 (um) segundo para reconhecimento facial;

11.13.10. Deve possuir índice de precisão $\geq 99\%$ para reconhecimento facial;

11.13.11. O dispositivo deve estar em conformidade com a GDPR/LGPD.

11.13.12. O terminal de reconhecimento facial deverá possuir a opção de alimentação PoE (IEEE 802.3af ou at).

11.13.13. Possuir ao menos 1 porta de integração para cada uma das seguintes tecnologias/serviços:

11.13.13.1. RS-485;

11.13.13.2. Wiegand e OSPD;

11.13.13.3. Ethernet – 10/100 mbps;

11.13.13.4. Botão de requisição de saída;

11.13.13.5. Relé interno ao módulo de acionamento;

11.13.13.6. Entrada de alarme;

11.13.13.7. Deve possuir interface de configuração via rede;

11.13.14. Ser equipado com tela LED com dimensão mínima de 5", com resolução mínima de 272 x 480 pixels, equipada com função touch screen para acesso ao menu de funções e interação com a interface do equipamento;

11.13.15. O equipamento deverá ser fornecido com sua respectiva fonte de alimentação compatível com as características elétricas da região de instalação;

11.13.16. Deve acompanhar suportes e/ou acessórios para fixação na parede. O suporte deverá possuir acomodação para que os cabos não fiquem expostos.

11.13.17. Deve possuir certificação Anatel.

11.13.18. Os leitores de reconhecimento facial deverão ter suporte de idioma integrado para interação com o usuário no mínimo, nos seguintes idiomas: Inglês, Português (Brasileiro), Francês e Espanhol.

11.14. 1 (uma) Botoeira:

11.14.1. Botoeira de acionamento interno com tecnologia infravermelho para acionamento sem contato;

11.14.2. Deve vir fixado em espelho para instalação em caixa interna ou externa 4 x 2";

11.14.3. Deve possuir moldura em aço inoxidável escovado;

11.14.4. Deve vir acompanhado de todos os acessórios para fixação, como parafusos e demais itens necessários para fixação e adequação às instalações;

11.14.5. Deve possuir LED luminoso para indicação de estado de porta (aberto e fechado).

12. TERMINAL DE COMUNICAÇÃO BIDIRECIONAL

Unidade: Unidade.

Modelos de referência: Intelbrás: XPE 3101 IP, Dahua: DHI-VTO2111D-P-S2, Hikvision: DS-KV8113-WME1 ou tecnicamente equivalente.

Critério de Medição: 50% do valor será pago quando a Contratada fornecer o item e 50% do valor será pago quando ele for instalado, configurado e estiver em pleno funcionamento.

- 12.1. Intercomunicador com câmera e 1 botão, chamada de áudio bidirecional;
- 12.2. Câmera com dispositivo de captura mínima de 1/8", sensor de captura de 2Mp ou superior e sistema de varredura progressiva;
- 12.3. Iluminação mínima de 0 Lux em modo Preto & Branco;
- 12.4. Possuir saída de áudio de 85dB ou superior;
- 12.5. Deverá possuir suporte ao protocolo SIP;
- 12.6. Possuir lente embutida fixa entre 1,5 e 1,95mm;
- 12.7. Possuir as compressões de vídeo MJPEG, H.264;
- 12.8. Possuir tecnologia de controle dinâmico do comprimento de GOV (Group of vídeo), em função da movimentação dos objetos na cena;
- 12.9. Deverá possuir resolução mínima de: 1920x1080;
- 12.10. A câmera deve estar em conformidade com o padrão ONVIF profile S;
- 12.11. O fabricante deve ser membro participante no fórum ONVIF, sem nenhum tipo de restrição ou suspensão;
- 12.12. Possuir servidor web incorporado, permitindo acesso remoto para visualização e configuração;
- 12.13. Suporte aos sistemas operacionais: Windows;
- 12.14. Possuir compensação de luz de fundo (BLC);
- 12.15. Possuir tecnologia de redução digital de ruído;
- 12.16. A câmera deve permitir a criação de mascaramento privativo na área de imagem;
- 12.17. Permitir a gravação de imagens em cartão de memória SD/SDHC/SDXC;
- 12.18. 1 (uma) entrada de alarme para conexão de sensor externo;
- 12.19. 1 (uma) saída de controle para acionamento de dispositivos externos;
- 12.20. Suportar os métodos de endereçamento Ipv4 e Ipv6;
- 12.21. Deverá suportar os seguintes protocolos de rede: TCP/IP, UDP/IP, RTP(UDP), RTP(TCP), RTCP, RTSP, NTP, HTTP, HTTPS, DHCP, ICMP, IGMP, SNMP, ARP, DNS;
- 12.22. Permitir a implementação de segurança em HTTPS (SSL) e autenticação 802.1x;
- 12.23. Temperatura de operação de -10°C ~ +50°C;
- 12.24. Deve possuir certificações IP65 ou superior, IK08 ou superior;
- 12.25. Alimentação PoE (IEEE 802.3af ou at);

12.26. As atualizações de firmware devem ser disponibilizadas gratuitamente no site do fabricante;

12.27. A central de comunicação desses dispositivos devem ser o próprio software de controle de acesso previsto nesta contratação, portanto, os equipamentos devem ser homologados com o respectivo SCA ofertado.

12.28. O fabricante deverá fornecer a API do equipamento para futuras integrações;

12.29. A Contratada deverá realizar a instalação física e lógica de todos os componentes do terminal de comunicação, bem com a sua configuração.

12.29.1. Todos os materiais, mão de obra, ferramentas e equipamentos necessários ao fornecimento da infraestrutura de encaminhamento, o cabeamento de dados, o cabeamento elétrico e a conectividade de dados serão fornecidos pela Contratada. O único pagamento a ser feito quanto à infraestrutura será a do item "SERVIÇO DE INSTALAÇÃO DE INFRAESTRUTURA".

12.30. A instalação dos equipamentos e sistemas e a execução dos serviços deverão obedecer ao projeto executivo, que deverá detalhar a infraestrutura necessária.

12.31. O prazo de instalação deverá obedecer ao cronograma elaborado pela contratada e aprovado pela fiscalização.

12.32. Todos os serviços e acessórios necessários às instalações de quaisquer equipamentos previstos na solução são de responsabilidade da Contratada.

13. FECHADURA ELETROÍMÃ PARA PORTÕES

Unidade: Unidade.

Marcas de referência: Intelbras: FE 20150, IPEC: M150, Vault: 10006S ou tecnicamente equivalente.

Critério de Medição: 50% do valor será pago quando a Contratada fornecer o item e 50% do valor será pago quando ele for instalado, configurado e estiver em pleno funcionamento.

13.1. Possuir acabamento em Aço inoxidável;

13.2. Fazer a abertura e o fechamento de forma silenciosa;

13.3. Deverá ser acionada por qualquer controle de acesso do mercado;

13.4. Temperatura de operação: -5 a 50°C;

13.5. Dimensões máximas: 173 x 47 x 28 (A x L x P) mm;

13.6. Força de Tração: 150kgf;

13.7. Possuir sensor para sinalização do estado de abertura da porta.;

13.8. A Contratada deverá realizar a instalação física e lógica de todos os componentes da fechadura, bem com a sua configuração.

13.8.1. Todos os materiais, mão de obra, ferramentas e equipamentos necessários ao fornecimento da infraestrutura de encaminhamento, o cabeamento de dados, o cabeamento elétrico e a conectividade de dados serão fornecidos pela Contratada. O único pagamento a ser feito quanto à infraestrutura será a do item "SERVIÇO DE INSTALAÇÃO DE INFRAESTRUTURA".

13.9. A instalação dos equipamentos e sistemas e a execução dos serviços deverão obedecer ao projeto executivo, que deverá detalhar a infraestrutura necessária.

13.10. O prazo de instalação deverá obedecer ao cronograma elaborado pela contratada e aprovado pela fiscalização.

13.11. Todos os serviços e acessórios necessários às instalações de quaisquer equipamentos previstos na solução são de responsabilidade da Contratada.

14. PORTAL DETECTOR DE METAIS

Unidade: Unidade.

Marcas de referência: Dahua: DHI-ISC-D718-S2, Garrett: PD 6500i; Rapiscan Systems: Metor 6S ou tecnicamente equivalente.

Critério de Medição: 50% do valor será pago quando a Contratada fornecer o item e 50% do valor será pago quando ele for instalado, configurado e estiver em pleno funcionamento.

14.1. Deverá ser do tipo portal, permitindo que pessoas de diversas estaturas cruzem a área de detecção;

14.2. Apresentar múltiplos indicadores visuais quando em funcionamento;

14.3. Apresentar ao menos 200 níveis ajustáveis de sensibilidade;

14.4. Deve permitir a seleção da frequência operacional.

14.5. Dispor de mecanismo que isole possíveis interferências;

14.6. Dispor de ao menos 18 zonas independentes de detecção;

14.7. O portal detector de metais deverá possuir sistema de detecção multizonal com indicação visual da localização aproximada do objeto metálico detectado no corpo da pessoa, por meio de sinalização luminosa disposta ao longo das laterais ou da parte central do equipamento, ou por interface local com display LCD ou tela sensível ao toque;

14.8. O equipamento deverá estar em conformidade com a ISO 9001.

14.9. A irradiação dissipada pelo campo magnético do detector deverá ser totalmente inofensiva às pessoas;

14.10. Deverá possuir, na parte superior do detector, painel indicativo que apresente informações funcionais;

14.11. Possuir recurso que possibilite a contagem de passagens realizadas pelo equipamento;

14.12. O vão de passagem do detector deve apresentar minimamente as seguintes dimensões: 2000 x 700 mm (A-L);

14.13. Deverá apresentar peso total inferior a 70 kg considerando todos os elementos da instalação;

14.14. Ser alimentado eletricamente em rede 100 ~ 240 Vac ou ser fornecido com sua respectiva fonte de alimentação compatível com a tensão alternada indicada;

14.15. Ser capaz de operar em ambientes cuja temperatura varie entre 0 ~ 55°C com umidade relativa do ar entre 0 ~ 95%;

14.16. Todos os acessórios necessários ao perfeito funcionamento do equipamento deverão acompanhá-lo no momento do fornecimento.

14.17. A Contratada deverá realizar a instalação física e lógica de todos os componentes do portal, bem com a sua configuração.

14.17.1. Todos os materiais, mão de obra, ferramentas e equipamentos necessários ao fornecimento da infraestrutura de encaminhamento, o cabeamento de dados, o cabeamento elétrico e a conectividade de dados serão fornecidos pela Contratada. O único pagamento a ser feito quanto à infraestrutura será a do item "SERVIÇO DE INSTALAÇÃO DE INFRAESTRUTURA".

14.18. A instalação dos equipamentos e sistemas e a execução dos serviços deverão obedecer ao projeto executivo, que deverá detalhar a infraestrutura necessária.

14.19. O prazo de instalação deverá obedecer ao cronograma elaborado pela contratada e aprovado pela fiscalização.

14.20. Todos os serviços e acessórios necessários às instalações de quaisquer equipamentos previstos na solução são de responsabilidade da Contratada.

15. CÂMERA PARA LEITURA DE PLACA DE VEÍCULOS (LPR)

Unidade: Unidade.

Marcas de referência: Axis: P1467-LE-3, Pelco: Sarix Pro 4 SRXP4-5V29-EBT-IR, Bosch: NBE-5703-AL, VivoTek: IB9387-LPR-V2 ou tecnicamente equivalente.

Critério de Medição: 50% do valor será pago quando a Contratada fornecer o item e 50% do valor será pago quando ele for instalado, configurado e estiver em pleno funcionamento.

15.1. A Contratada deverá realizar a instalação física e lógica de todos os componentes da câmera, bem com a sua configuração.

15.1.1. Todos os materiais, mão de obra, ferramentas e equipamentos necessários ao fornecimento da infraestrutura de encaminhamento, o cabeamento de dados, o cabeamento elétrico e a conectividade de dados serão fornecidos pela Contratada. O único pagamento a ser feito quanto à infraestrutura será a do item "SERVIÇO DE INSTALAÇÃO DE INFRAESTRUTURA"

15.2. A instalação dos equipamentos e sistemas e a execução dos serviços deverão obedecer ao projeto executivo, que deverá detalhar a infraestrutura necessária.

15.3. O prazo de instalação deverá obedecer ao cronograma elaborado pela contratada e aprovado pela fiscalização.

15.4. Todos os serviços e acessórios necessários às instalações de quaisquer equipamentos previstos na solução são de responsabilidade da Contratada.

15.5. Tipo e formato da câmera: Bullet lente varifocal para reconhecimento de placas veiculares – License Plate Recognition (LPR).

15.6. Deve ser equipamento com IP nativo, sem adaptação de analógico para IP;

15.7. Deve suportar modo stand alone;

15.8. Deve suportar integrações com softwares e plataformas fornecidos nesta contratação;

15.9. Deverá ser câmera IP com resolução de no mínimo 5MP;

- 15.10. Câmera com dispositivo de captura de 1/2.8" ou maior, com varredura progressiva;
- 15.11. Iluminação mínima de 0.15Lux (F1.6, 1/30seg), 0,03Lux (F1.6. 1;30seg) e 0 Lux em modo Preto & Branco (iluminação IR ativada);
- 15.12. Possuir lente embutida varifocal, auto-iris, motorizada de 4.5 a 10mm - ou valor equivalente que permita cobertura da área e distância especificadas para LPR;
- 15.13. Ângulo de visão horizontal: H: 90º(Wide) ou maior ~45º (Tele) ou menor;
- 15.14. Ângulo de visão vertical: V: 53.6º(Wide) ou maior~25.5º (Tele) ou menor;
- 15.15. Possuir recurso P-iris;
- 15.16. Possuir ajuste de foco automático;
- 15.17. Alcance mínimo da iluminação IR de 30 metros;
- 15.18. Possuir as compressões de vídeo MJPEG, H.264 e H.265;
- 15.19. Possuir tecnologia de controle dinâmico do comprimento de GOV (Group of Video), em função da movimentação dos objetos na cena, de forma a não comprometer a capacidade ou outros recursos presentes no equipamento;
- 15.20. Possuir tecnologia de controle dinâmico das fotos por segundo (FPS), em função da movimentação dos objetos na cena, de forma a não comprometer a capacidade ou outros recursos presentes no equipamento;
- 15.21. Taxa de atualização de 30fps na máxima resolução;
- 15.22. Permitir a criação e configuração de 3 (três) perfis independentes de fluxos de vídeo;
- 15.23. Deve ser compatível com os métodos de transmissão Unicast e Multicast;
- 15.24. Deverá ser compatível com padrão ONVIF profiles, G, S e T;
- 15.25. A linguagem da interface de usuário deve estar no idioma português;
- 15.26. Possuir servidor web incorporado, permitindo acesso remoto para visualização e configuração;
- 15.27. Função Day/Night com remoção de filtro infravermelho;
- 15.28. A câmera deve possuir função de aprimoramento de contraste;
- 15.29. A câmera deve possuir WDR de no mínimo 120dB;
- 15.30. Deverá possuir tecnologia de estabilização digital de imagem;
- 15.31. Possuir recurso de detecção de movimento;
- 15.32. A câmera deve permitir a criação de mascaramento em 6 zonas privativas na área de imagem;
- 15.33. A câmera deve possuir análise de vídeo inteligente embarcada ou através da simples adição de licença, composta de detecção de desfoque, detecção de movimento, adulteração, Detecção de áudio, classificação de som, detecção de choque;
- 15.34. A câmera deve possuir reconhecimento de placas e de veículos embarcada ou através de licença adicional ou opcionalmente em servidor, devidamente licenciada com as seguintes especificações mínimas:
 - 15.34.1. Cobertura de 1 Faixa em 3,6 metros com iluminação IR Ativada;

- 15.34.2. Detecção, leitura e registros de placas de veículos com velocidade de, no mínimo, até 30 km/h;
- 15.34.3. Distância mínima de avanço de 12 metros;
- 15.34.4. Distância máxima de avanço 12 metros com iluminação IR ativada;
- 15.34.5. Possuir armazenamento mínimo para 10.000 de imagens de LPR e Veículos.
- 15.35. Deverá ser capaz de reconhecer placas padrão Mercosul e brasileiro de todos os veículos atuais circulantes em território nacional;
- 15.36. Identificar a direção dos veículos em uma área pré-determinada, entrando ou saindo.
- 15.37. Permitir a gravação de imagens em cartão de memória SD/SDHC/SDXC;
- 15.38. Deverá vir com cartão de 32GB instalado;
- 15.39. 01 (uma) entrada de áudio para conexão de microfone externo;
- 15.40. 01 (uma) saída de áudio para conexão de falantes externos;
- 15.41. Compressão de áudio G.711 e/ou G.726 e/ou AAC-LC;
- 15.42. Possuir obturador eletrônico com opções de seleção entre 1/5 e 1/8.500seg;
- 15.43. Possuir função de espelhamento de imagem;
- 15.44. 01 (uma) entrada de alarme para conexão de sensor externo;
- 15.45. 01 (uma) saída de controle para acionamento de dispositivos externos;
- 15.46. Possuir interface de rede 10/100;
- 15.47. Suportar os métodos de endereçamento Ipv4 e Ipv6;
- 15.48. Deverá suportar os seguintes protocolos de rede: TCP/IP, UDP/IP, RTP, RTCP, RTSP, NTP, HTTP, HTTPS, DHCP, ICMP, IGMP, SNMP e DNS;
- 15.49. Permitir a implementação de segurança em HTTPS (SSL), autenticação de login, filtro de endereços IP, Autenticação Digest, registro de logs de acesso e autenticação 802.1x (EAP-TLS) e inicialização segura;
- 15.50. Deve possuir certificações IP66 e IK10;
- 15.51. Alimentação PoE+ (IEEE 802.3at e/ou IEEE 802.3af);
- 15.52. As atualizações de firmware devem ser disponibilizadas gratuitamente no site do fabricante;
- 15.53. O fabricante deverá fornecer a API do equipamento para futuras integrações;
- 15.54. Os equipamentos deverão ser compatíveis com a plataforma de gestão de acesso ofertado.
- 15.55. Os equipamentos devem ser ofertados com os respectivos protetores de surto, visando evitar com que os dispositivos queimem com descargas elétricas. Os protetores devem ser de fácil instalação além de serem utilizados como supressor de ruído, eliminando possíveis interferências nas câmeras.
- 15.56. As câmeras deverão ser entregues instaladas e em pleno funcionamento, inclusive o recurso de reconhecimento e leitura de placa de veículos. O processamento da leitura de placa deve ser feito na borda do dispositivo ou mediante licença no sistema de controle de acesso, conforme a disponibilidade de cada fornecedor.

16. REGISTRADOR DE PONTO ELETRÔNICO

Unidade: Unidade.

Modelo de referência: Control ID: iDFace; Anviz: FacePass 7; ZKTeco: FaceDepot 7 ou tecnicamente equivalente.

Critério de Medição: 50% do valor será pago quando a Contratada fornecer o item e 50% do valor será pago quando ele for instalado, configurado e estiver em pleno funcionamento.

16.1. A Contratada deverá realizar a instalação física e lógica de todos os componentes do registrador de ponto, bem com a sua configuração.

16.1.1. Todos os materiais, mão de obra, ferramentas e equipamentos necessários ao fornecimento da infraestrutura de encaminhamento, o cabeamento de dados, o cabeamento elétrico e a conectividade de dados serão fornecidos pela Contratada. O único pagamento a ser feito quanto à infraestrutura será a do item "SERVIÇO DE INSTALAÇÃO DE INFRAESTRUTURA".

16.2. A instalação dos equipamentos e sistemas e a execução dos serviços deverão obedecer ao projeto executivo, que deverá detalhar a infraestrutura necessária.

16.3. O prazo de instalação deverá obedecer ao cronograma elaborado pela contratada e aprovado pela fiscalização.

16.4. Todos os serviços e acessórios necessários às instalações de quaisquer equipamentos previstos na solução são de responsabilidade da Contratada.

16.5. Métodos de Autenticação: Reconhecimento facial como método primário de autenticação e via PIN (senha numérica) e/ou cartão RFID (crachá), como recursos opcionais de identificação.

16.6. O reconhecimento facial deve:

- 16.6.1. Ser mediante duas câmeras HD 1080p (luz visível e luz infravermelha);
- 16.6.2. Possuir capacidade de identificação de no mínimo, 10.000 faces com detecção de rosto vivo;
- 16.6.3. Ser coletado em menos de 1 segundo;
- 16.6.4. Suportar reconhecimento de rostos com máscara;

16.7. O dispositivo de ponto eletrônico deve:

- 16.7.1. Possibilitar o cadastro e armazenamento de, no mínimo, 100.000 usuários;
- 16.7.2. Possuir beep sonoro para confirmação ou não do registro do ponto;
- 16.7.3. Informar se o ponto foi registrado ou não, informando a data e hora registrada;
- 16.7.4. Conter grau de Proteção IP65;
- 16.7.5. Possuir comunicação criptografada em ambos os sentidos;
- 16.7.6. Possuir calendário perpétuo, com tratamento de horário de verão;
- 16.7.7. Possibilitar o registro de ponto on-line e off-line;

16.8. O registrador de ponto eletrônico deverá possuir a seguinte configuração de comunicação e conectividade:

- 16.8.1. TCP/IP;
- 16.8.2. Ethernet: sendo, no mínimo, 1 porta Ethernet 10/100Mbps nativa;
- 16.8.3. USB: sendo, no mínimo, 1 porta USB Host 2.0;
- 16.8.4. Wi-Fi 802.11b/g/n
- 16.8.5. Wireless 2.4GHz;
- 16.8.6. RS-485: sendo, no mínimo, 1 porta RS-485.

16.9. O dispositivo deverá possuir a seguinte configuração de interface:

- 16.9.1. Tela LCD colorida;
- 16.9.2. Display touchscreen de 5" ou superior; e
- 16.9.3. Áudio via alto-falante e microfone embutidos.

16.10. Protocolos de Integração: O dispositivo deve ser homologado com o software ofertado na solução de controle de acesso.

- 16.10.1. Deve ser capaz de utilizar os dados dos usuários já validados no sistema de controle de acesso para fins cadastramento.

16.11. O equipamento deve ser inviolável, de forma a bloquear o acesso às memórias do equipamento.

16.12. As marcações devem ser registradas permanentemente na memória, permitindo que seja recuperada em caso de perda de dados.

16.13. Deve ser ofertado juntamente com o dispositivo, o respectivo software de gestão da comunicação e configuração dos equipamentos.

- 16.13.1. O software deve ser operar na versão Web via browser, sendo compatível com os principais navegadores do mercado (Internet Explorer, Google Chrome, Mozilla Firefox);

- 16.13.2. Deverá ser integrado com o sistema de gerenciamento de controle de acesso ofertado na solução e ao sistema de GRH do TCU. A integração com o sistema de controle de acesso limitar-se-á ao envio automatizado dos cadastros de usuários, de forma a evitar duplicidade de registros. Com isso, os usuários cadastrados no controle de acesso serão automaticamente habilitados para registrar a frequência nos equipamentos de ponto eletrônico. Em seguida, o sistema de controle de acesso deverá, de forma automática, coletar os arquivos de registro eletrônico de ponto (AFD) e encaminhar as marcações de frequência diretamente ao sistema de controle de frequência do TCU (GRH).

16.14. Deverá possuir integração nativa entre todos os módulos funcionais inclusive entre as ferramentas de tecnologia, sem necessidade de execução de rotinas (automáticas ou não) para compatibilização de dados e sem necessidade de redundância de processos.

16.15. A solução de software deve ser homologada pelo fabricante do registrador de ponto eletrônico.

- 16.16. O sistema de gerenciamento deverá realizar a coleta de dados dos equipamentos e sincronização com o servidor central de forma automática e periódica, sem necessidade de intervenção humana.
- 16.17. Quando a rede ou acesso à internet não estiver operacional, os equipamentos deverão permanecer registrando as ocorrências e armazenando internamente os dados, sincronizando automaticamente quando a conexão for restabelecida.
- 16.18. O sistema deve ser capaz de armazenar dados de maneira segura, com criptografia dos dados biométricos.
- 16.19. Garantia de privacidade, de acordo com a Lei Geral de Proteção de Dados (LGPD), para o tratamento de dados pessoais.

17. ELABORAÇÃO DE PROJETOS

Unidade: Serviço.

Critério de medição: Será medido e pago conforme a respectiva entrega, ou seja, quando a Contratada enviar cada um dos projetos exigidos no contrato e este for aprovado pela Fiscalização.

- 17.1. Durante a execução contratual, a Contratada deverá elaborar 2 projetos: **projeto executivo e projeto as-built**.
- 17.2. O projeto executivo deverá ser elaborado assim que o contrato for assinado para nortear os trabalhos que serão executados pela Contratada e deverá detalhar todos os aspectos das instalações a serem feitas, incluindo, mas não se limitando a cabeamento, eletrodutos, pontos de elétrica, pontos de rede etc.
- 17.3. Caso haja solicitação da Contratada, poderá ser admitido o reaproveitamento de parte da infraestrutura já existente no Tribunal, como cabeamentos, eletrodutos etc.
- 17.4. O projeto executivo deverá detalhar a infraestrutura que a Contratada pretende reaproveitar para que o reaproveitamento seja submetido à aprovação da Fiscalização.
- 17.5. Faz parte do Projeto Executivo a apresentação, pela Contratada, de memorial ou plano de ação contendo a estratégia detalhada de integração do Sistema de Controle de Acesso (SCA) com os sistemas corporativos (GRH, Contrata, Correio Eletrônico, SEG, Indicador Eletrônico, CFTV, SDAI, ICN e Gestão de Patrimônio). O documento deverá descrever, de forma clara e objetiva:
 - 17.5.1. A arquitetura e os fluxos de dados previstos;
 - 17.5.2. Os mecanismos de autenticação, protocolos e formatos de integração a serem adotados;
 - 17.5.3. As medidas de segurança da informação aplicáveis (autenticação, confidencialidade, integridade e rastreabilidade);
 - 17.5.4. O plano de execução, incluindo riscos relevantes e cronograma estimado.
- 17.6. Também faz parte do projeto executivo a entrega do cronograma dos serviços a serem executados, que deverá detalhar, pelo menos, as etapas de fornecimento, instalação, testes, implementação das integrações, projeto as-built, treinamentos, operação assistida, manutenção e suporte técnico.
- 17.7. O projeto executivo deverá ser desenvolvido dentro das dependências do TCU, em sala ser disponibilizada para esse fim.

17.8. O projeto as-built deverá ser elaborado após o recebimento definitivo de todas as instalações e deverá refletir exatamente o que foi executado pela Contratada. Faz parte do as-built os memoriais descritivos de funcionamento do sistema instalado, cadernos de operação do sistema, tabelas de localização de todos os equipamentos instalados, entre outros.

17.9. Na elaboração do projeto executivo a Contratada deverá considerar as informações constantes do Anexo X – Projetos e Lista de Pontos, sem prejuízo das adaptações e ajustes necessários solicitados pela Contratante na execução dos serviços.

18. ADEQUAÇÃO, RETIRADA E/OU DESMOBILIZAÇÃO ATUAL

Unidade: Serviço.

Critério de medição: Os serviços serão medidos e pagos pela efetiva e completa adequação, retirada e desmobilização da solução atual que será demandada mediante ordem de serviço.

18.1. A Contratada será responsável pela desinstalação e retirada de toda infraestrutura e equipamentos existentes da atual solução como por exemplo: cancelas, catracas, estrutura de fechamento e outros que não serão aproveitados ou remanejados;

18.2. Todos os serviços necessários para a remoção de quaisquer equipamentos são de responsabilidade da Contratada.

18.3. Todos os equipamentos retirados serão catalogados e deverão ser desinstalados e embalados pela empresa Contratada e entregues à unidade técnica do Tribunal de Contas da União, encarregada de seu desfazimento.

18.4. Os tipos e quantidades estimadas dos equipamentos e da estrutura atual da Contratante estão relacionados no Anexo IV que trata da INFRAESTRUTURA TECNOLÓGICA ATUAL - LEGADO DE EQUIPAMENTOS E SISTEMAS.

18.5. Toda a área compreendida pelos serviços deverá ser totalmente limpa e recomposta, incluindo piso, forro e paredes no mesmo padrão existente.

19. INSTALAÇÃO, PARAMETRIZAÇÃO, CONFIGURAÇÃO E INTEGRAÇÃO DE SOFTWARE

Unidade: Serviço.

Critério de medição: Os serviços serão medidos e pagos pela efetiva e completa instalação, parametrização, configuração, de cada item previsto nesse projeto para fins de integração com o software de gestão de acesso a ser fornecido, sendo demandada mediante ordem de serviço.

19.1. A Instalação do software compreende a preparação e instalação de todos os módulos de software, inclusive, aqueles que forem requisitos do software da contratada, como servidores de banco de dados e servidores de aplicação.

19.2. A Parametrização do software compreende a configuração necessária para o software funcionar nas redes de computadores do TCU.

19.3. A Configuração do software compreende a configuração das regras de negócio do TCU no software de Controle de Acesso.

19.4. A Integração compreende toda aplicação do software de Controle de Acesso com os itens de hardware contratados ou já existentes no TCU, bem como a integração entre o

software de Controle de Acesso e outros softwares do TCU, visando promover a interoperabilidade da solução contratada.

19.5. A sincronização online entre a base de dados do sistema fornecido e a base de dados corporativa do TCU deve fazer uso da tecnologia “Web Service”, protocolos Rest ou Soap, ou da funcionalidade de banco de dados “view”.

19.6. Providenciar sincronização offline entre a base de dados do sistema fornecido e a base de dados corporativa do TCU por meio do desenvolvimento de rotinas ou programas que façam verificação e restabelecimento da consistência entre as bases citadas.

19.7. Possibilitar exportação da base de dados do sistema fornecido, por tabela ou toda a base, por meio da geração de arquivo de texto ou em formato XML.

19.8. O sistema de integração compreende todos os componentes desenvolvidos e/ou configurados para promover a integração bidirecional, incremental e contínua dos dados entre a solução contratada e soluções em uso e softwares de apoio da CONTRATANTE.

19.9. A CONTRATADA deverá promover a integração das soluções instaladas com a base de dados de autenticação de usuários da CONTRATANTE, de forma que a autenticação nos novos sistemas se dê por meio do diretório de usuários atualmente utilizado.

19.10. A CONTRATADA deverá promover a carga da base de dados de acesso da CONTRATANTE, de forma a importar o banco de dados atual de usuários no novo sistema de controle de acesso, sem que haja necessidade de recadastramento manual de usuários.

19.11. Todas as adaptações e integrações realizadas pela CONTRATADA deverão ser formalmente documentadas.

19.12. Os códigos produzidos serão de propriedade da CONTRATANTE e deverão ser a ela entregues junto com toda a documentação.

19.13. Todos os módulos e funcionalidades a serem integradas conforme detalhado nos itens em sequência devem observar as seguintes configurações e possibilidades detalhadas a seguir.

19.14. Os serviços de integração devem possuir os seguintes requisitos de integração com o CFTV e possibilitar os seguintes resultados e ações automatizadas:

19.14.1. Direcionamento de câmera mais próxima e respectiva filmagem ou fotografia de todos eventos e registros de acesso (entrada/saída) ou apenas daqueles definidos pela CONTRATANTE, como por exemplo:

- 19.14.1.1. Alerta de intrusão;
- 19.14.1.2. Alerta de porta forçada;
- 19.14.1.3. Alerta de acesso negado de pessoas;
- 19.14.1.4. Alerta de acesso negado de veículos;
- 19.14.1.5. Alerta de elevador preso;
- 19.14.1.6. Alerta de ocorrência/emergência nos elevadores;
- 19.14.1.7. Alerta de tentativa de burla à catraca;
- 19.14.1.8. Alerta de uso de credencial de acesso inválida/baixada;

19.14.1.9. Alerta de número anormal de acessos por usuário no mesmo dia; e

19.14.1.10. Alerta de duplas ou consecutivas entradas.

19.14.2. Esses registros, acompanhados das imagens, devem estar disponíveis para acesso, por meio de busca por data, horário, matrícula do servidor, nome ou documento de identificação de servidor ou visitante;

19.14.3. As imagens serão salvas nos mesmos padrões das atualmente arquivadas pelo software do sistema de CFTV - IP, podendo ser visualizadas a partir de busca nesse mesmo software por ponto de acesso, data e horário;

19.14.4. Além disso, as imagens poderão ser acessadas mediante busca por nome do servidor, matrícula, data, horário, ponto de acesso, realizada a partir do software da solução contratada.

19.14.5. No momento da passagem do colaborador ou visitante pelo ponto de acesso, tanto na entrada quanto na saída, deve gerar, ao mesmo tempo, na estação cliente, a foto de cadastro do indivíduo e a imagem instantânea, a fim de serem comparadas.

19.15. Os serviços de integração devem possuir os seguintes requisitos de integração com o SDAI e possibilitar os seguintes resultados e ações automatizadas:

19.15.1. As soluções de monitoramento e de controle de acesso deverão permitir a integração com o Sistema de Detecção e Alarme de Incêndios (SDAI) que opera atualmente no TCU. A integração deverá ser realizada de forma unidirecional, onde os outros sistemas recebam informações provenientes do SDAI do TCU e priorizem o tratamento dos respectivos eventos de alta criticidade.

19.15.2. A integração do SDAI com o controle de acesso deve ser totalmente via contato seco direto, para liberação das portas e catracas, por ambiente atendido;

19.15.3. Os sistemas devem integrar-se à central de alarme contra incêndio via Ethernet, de modo que: a partir do acionamento da central em qualquer ponto do edifício, ou mesmo do acionamento remoto, as catracas e cancelas de controle de acesso sejam liberadas automaticamente, e que o software fornecido seja capaz de mapear os acionadores do alarme de incêndio.

19.15.4. A integração deve possibilitar que os pontos de acesso sejam destravados quando um alarme do SDAI acionar.

19.15.5. Evacuação Controlada: Em caso de incêndio, o sistema de alarme de incêndio pode acionar os alarmes sonoros e visuais, e o sistema de controle de acesso libera as portas, catracas e cancelas, e aciona comando para os elevadores descerem para o térreo.

19.16. Os serviços de integração devem possuir os seguintes requisitos de integração com o Sistema de Gestão de Patrimônio (Gestão de Ativos) da Contratante e possibilitar os seguintes resultados e ações automatizadas:

19.16.1. As soluções de monitoramento e de controle de acesso deverão permitir a integração com o Sistema de Gestão de Ativos do TCU de forma unidirecional, onde os outros sistemas recebam informações provenientes do

Sistema de Gestão de Ativos do TCU e priorizem o tratamento dos respectivos eventos de alta criticidade, como por exemplo: envio de alerta à central de monitoramento em casos de etiqueta de RFID violada, movimentação de item para uma área sem autorização e movimentação de bens rastreados por RFID para fora das dependências da Contratante.

19.16.2. Deverá possibilitar que sistemas de bloqueio automatizados sejam ativados se ativos específicos estiverem sendo movidos ou acessados sem autorização.

19.17. Os serviços de integração devem possuir os seguintes requisitos com os sistemas internos da Contratante e possibilitar os seguintes resultados e ações automatizadas:

19.17.1. **Integração com o GRH** – Sistema programado em linguagem Java para gerência de recursos humanos:

19.17.1.1. Permitir a integração com a base de dados do sistema de gerência de recursos humanos do TCU - GRH, de modo que, ocorrido o evento de registro da passagem da pessoa (entrada ou saída) em qualquer leitor de ponto para frequência, o GRH deverá exibir esse registro em até 5 minutos depois, em condições normais de operação; e

19.17.1.2. Providenciar integração com a base de dados do GRH do TCU para receber os dados cadastrais dos servidores no mesmo dia em que forem atualizados, contendo dados pessoais, lotação, cargo, status e foto.

19.17.2. **Integração com o Contrata** – Sistema programado em linguagem Java para gestão de contratos do TCU:

19.17.2.1. Permitir a integração com a base de dados do sistema de gestão de contratos do TCU, de modo que, quando houver expiração de vigência de contratos, as permissões de acesso dos colaboradores vinculados ao contrato sejam automaticamente suspensas; e

19.17.2.2. Providenciar integração com a base de dados do Contrata do TCU para receber os dados cadastrais dos colaboradores no mesmo dia em que forem atualizados, contendo dados pessoais, lotação, cargo, status e foto.

19.17.3. **Integração com o Correio Eletrônico – Plataforma do Outlook Microsoft 365** para comunicação via e-mail do TCU:

19.17.3.1. Providenciar integração com o servidor de correio eletrônico do TCU para possibilitar que o sistema de controle de acesso de pessoas envie e-mails de modo automático a determinadas pessoas, em relação a eventos pré-determinados.

19.17.4. **Integração com o SEG** – Sistema programado em linguagem Java para gerenciamento e controle de veículos, vagas, placas, RFID no estacionamento do TCU:

19.17.4.1. Providenciar integração da base de dados do SEG do TCU para alimentar o SCA a ser fornecido pela Contratada.

19.17.4.2. O banco de dados do SEG possui o cadastro de todos os veículos dos servidores e colaboradores do Tribunal. O SCA deve ser capaz de ler esses

registros e, automaticamente, liberar o acesso dos veículos cadastrados às garagens do TCU por meio da leitura das placas, conforme autorizações de acesso constantes no SEG.

19.17.5. **Integração com o Indicador Eletrônico** – Sistema programado para consulta a informações inerentes a servidores, autoridades e unidades do TCU, como nome, lotação, telefone, foto, matrícula etc.:

19.17.5.1. Providenciar integração da base de dados do Indicador Eletrônico do TCU para alimentar o SCA a ser fornecido pela Contratada. Inclusive, podendo utilizar na operação da solução de controle de acesso informações e arquivos provenientes desse sistema do TCU, como uso da foto de servidores cadastrados para fins de autenticação de acesso via reconhecimento facial.

19.17.6. **Integração com o ICN** - O sistema de controle de acesso deverá possuir integração com o registro de identificação integrados pela API de validação biométrica Facial e Digital da ICN (Identificação Civil Nacional), base essa que atende também ao “Gov.br”, inclusive para acesso de visitantes.

19.17.6.1. Essa funcionalidade dependerá de gestão da Contratante junto ao Tribunal Superior Eleitoral (TSE) - órgão responsável por gerir e armazenar a base de dados da ICN, e ao Serviço Federal de Processamento de Dados (Serpro) – empresa pública responsável por operacionalizar a Identificação Civil Nacional.

19.17.6.2. A viabilização dessa integração deverá seguir as disposições constantes da Lei nº 13.444, de 11 de maio de 2017 e da Resolução nº 23.656, de 7 de outubro de 2021 do Tribunal Superior Eleitoral.

19.18. As soluções ofertadas neste projeto devem importar a base de dados do sistema de controle de acesso em operação atualmente no TCU.

19.19. O software de controle de acesso deve suportar integração bidirecional com o software de videomonitoramento em uso pelo TCU atualmente.

19.20. O software de controle de acesso deve ser integrado aos leitores faciais ofertados, de forma que o cadastro de usuários e faces seja de feito de forma unificada em uma única interface.

19.21. O terminal leitor de reconhecimento facial deve ser integrado ao software de controle de acesso ofertado, podendo também atuar autonomamente (stand alone) em caso de desconexão e para fins de controle da catraca em que se encontra.

19.22. A integração deve possibilitar o cadastramento de faces em uma interface unificada, não sendo permitido o uso de um software distinto para cadastramento de faces e outro para cadastramento de visitantes.

19.23. A Contratada elaborará plano e casos de testes para as integrações definidas neste projeto.

19.24. Os sistemas de integração de dados produzidos pela Contratada serão de propriedade do Contratante e deverão estar documentados pela Contratada.

19.25. Caberá unicamente à Contratada, durante o período de vistoria, coletar dados suficientes do parque computacional do Tribunal de Contas da União para que possa estimar, corretamente, o esforço necessário à integração.

19.25.1. Passado o período de vistoria, os detalhes técnicos específicos sobre APIs, schemas de dados, mecanismos de autenticação, volumes de transação e eventuais padrões adicionais de segurança só serão disponibilizados à futura Contratada, em momento oportuno - após a assinatura do Contrato, em conformidade com as políticas internas de governança de tecnologia da informação do TCU.

20. INSTALAÇÃO DE INFRAESTRUTURA

Unidade: Serviço.

Critério de medição: Os serviços serão medidos e pagos pela efetiva e completa instalação da infraestrutura necessária à integral operação de toda a solução que será demandada mediante ordem de serviço.

20.1. Todos os custos inerentes aos serviços de obras civis necessários à implantação da solução contratada deverão compor a proposta da Contratada. Para estimar esses custos, a Contratada poderá utilizar a vistoria para fazer os levantamentos que julgar necessários.

20.1.1. Caso as licitantes optem pela substituição da vistoria nos termos do § 3º do art. 63 da Lei nº 14.133/2021, poderão utilizar as informações constantes do Anexo X – Projetos e Lista de Pontos, para mensurar os respectivos custos desses serviços na elaboração de suas propostas.

21. Será pago um valor único para todo o serviço de instalação de infraestrutura necessário. A Contratada deverá apresentar, em sua proposta, o valor global para esse item, sem necessidade de detalhar as minúcias da infraestrutura a ser instalada.

22. Não haverá nenhum pagamento extra para o caso de a Contratada alegar ter gastado mais do que o valor registrado para o item. A Contratada é a única responsável por apresentar a sua proposta e deverá considerar isso quando da elaboração da proposta.

22.1. Da mesma forma, não será descontado nenhum valor caso a Contratada gaste menos do que o valor previsto.

22.2. Todos os serviços necessários às instalações de quaisquer equipamentos previstos na solução são de responsabilidade da CONTRATADA. Dentre os serviços, constam de maneira exemplificativa, os seguintes:

22.2.1. Recorte de pisos e paredes para a passagem de eletrodutos e instalação/chumbamento dos equipamentos;

22.2.2. Fixação dos equipamentos e instalações elétricas/lógicas nos pisos e paredes;

22.2.3. Instalação da infraestrutura necessária para o perfeito funcionamento da solução, incluindo todos os eletrodutos, cabos, tomadas, quadros, caixas de passagem, tomadas, disjuntores, conectores, suportes etc.

22.2.4. Reposição dos revestimentos de pisos e paredes nos locais em que houver recorte, de modo que o acabamento, ou aparência exterior, retorne à condição inicial;



- 22.3. Todo o cabeamento necessário para as instalações elétricas e lógicas da solução deverá ser acondicionado em eletrodutos embutidos nas paredes e pisos, exceto quando indicado de outra forma pela fiscalização;
- 22.4. Nas garagens do TCU, excepcionalmente, quando for impossível instalar os cabos nas paredes e pisos, estes poderão ser acondicionados em eletrodutos aparentes;
- 22.5. O sistema de cabeamento deverá obedecer ao seguinte padrão:
- 22.5.1. O CONTRATANTE designará os pontos de energia e lógica mais próximos de cada ponto de instalação dos equipamentos do sistema;
 - 22.5.2. Sempre que possível, os eletrodutos serão embutidos nos forros removíveis; seguindo para as paredes e, depois para os pisos; e
 - 22.5.3. Deverão ser minimizados os recortes em pisos.

23. INSTALAÇÃO DE REGISTRADORES DE PONTOS ELETRONICOS NAS SECs ESTADUAIS

Unidade: Unidade

Critério de medição: Será medido e pago uma vez para cada Secretaria Estadual em que os registradores de ponto forem instalados e configurados, sendo pago uma única vez por SEC, independentemente da quantidade de dispositivos instalados.

- 23.1. A contratada deverá incluir nesse item todos os insumos e acessórios necessários para a instalação e configuração dos registradores de ponto nas SECs estaduais.
- 23.2. A Contratada deverá não apenas fazer a instalação física dos equipamentos, mas entregá-los funcionando e conectados ao GRH do TCU.

24. FECHAMENTO E GUARDA-CORPO

Unidade: Metro linear.

Critério de medição: Os serviços serão medidos e pagos por metro de fechamento efetivamente fornecido e instalado por completo. A quantidade definida é meramente estimativa, devendo a prestação dos respectivos serviços ser realizada conforme necessidade detalhada no projeto executivo.

- 24.1. Os fechamentos serão instalados em locais que possuem equipamentos de controle de acesso, atuando como uma barreira física que separa o ambiente controlado do ambiente não controlado.
- 24.2. Os materiais devem obedecer ao padrão já existente no TCU e deverão ser utilizados para realizar o fechamento de espaços e pontos onde serão instalados bloqueios de acesso, catracas e demais equipamentos.
- 24.3. Os serviços devem ser compostos de guarda corpo em inox com fechamento em vidro com as seguintes especificações:
- 24.3.1. Vidro temperado incolor com espessura de 8mm;
 - 24.3.2. O fechamento em vidro deverá possuir no mínimo uma altura de 75 cm;
 - 24.3.3. Estrutura em aço inox AISI 201 ou 202 composto por perfil tubular de 50 mm x 1" com acabamento fosco;

24.4. Estrutura de fixação do vidro será em perfil em “U” de aço inox, de 25 x 12 mm, com 0,8 mm de espessura, que deverá ser soldado à estrutura principal e à base.

24.5. O detalhamento dos fechamentos deve ser feito no projeto executivo e será submetido à equipe de engenharia e arquitetura do TCU para aprovação.

25. TREINAMENTO E CAPACITAÇÃO

Unidade: Turma.

Critério de medição: Os serviços serão medidos e pagos por turma efetivamente treinada pela Contratada.

25.1. Para a execução do serviço de treinamento e capacitação, a Contratante disponibilizará ambiente físico adequado em suas dependências na localidade de Brasília/DF.

25.2. A Contratada deverá realizar a instrução técnica e operacional, com treinamento sobre todas as funcionalidades inerentes à instalação, à administração e ao uso da solução, com o objetivo de prover aos profissionais da Contratante os conhecimentos e habilidades necessários para o bom uso e funcionamento da solução adquirida.

25.3. A Contratada deverá providenciar o treinamento para o pessoal indicado pelo Contratante, que será realizado presencialmente nas dependências da Contratante na localidade de Brasília/DF conforme as seguintes turmas:

25.3.1. Grupo de no mínimo 5 (cinco) servidores e/ou colaboradores do TCU, enfocando aspectos de arquitetura, instalação, configuração do sistema, e perfil de gestor do sistema; e

25.3.2. Grupo de no mínimo 10 (dez) servidores e/ou colaboradores do TCU, enfocando aspectos do perfil operacional dos sistemas, e atendimento de suporte técnico, remoto e presencial.

25.4. Devem ser fornecidas apostilas impressas a todos os participantes.

25.5. Assim que for concluído o treinamento de cada turma, a empresa Contratada deve submeter a cada colaborador capacitado formulário de avaliação do treinamento, planejado para respostas objetivas, sendo que a consolidação das respostas deve estar inclusa no relatório de ocorrências da respectiva fase, de modo a subsidiar o recebimento por parte da CONTRATANTE.

25.6. O treinamento deverá ser realizado nas dependências do Tribunal de Contas da União em Brasília-DF, devendo utilizar o ambiente de produção da Contratante, de forma a viabilizar as aulas práticas.

25.7. O conteúdo do treinamento deverá abordar, no mínimo, os seguintes tópicos:

25.7.1. Configuração - melhores práticas;

25.7.2. Configuração e operação básica - comandos básicos; e

25.7.3. Conceitos básicos e avançados como: cadastramento, operação, supervisão e administração.

25.8. A data de início do repasse de conhecimento será definida pela Contratante de acordo com suas necessidades, observando cronograma de implementação da solução.

25.9. O treinamento deverá ser ministrado por profissional certificado e/ou autorizado pelo fabricante da solução de controle de acesso ofertada, com a devida comprovação, constando nome completo e CPF de cada profissional que ministrará.

25.10. A Contratada deverá prover toda a logística e todo o material didático necessário à execução do treinamento teórico e prático, como manuais e apostilas, entre outros. Deverá disponibilizar o material didático impresso, elaborado com o conteúdo a ser aplicado, em número compatível com o de participantes e fornecer cópia em formato digital. Todos os materiais deverão estar em língua portuguesa.

25.11. O treinamento deverá ser realizado utilizando conteúdo teórico e prático, disponibilizando a ferramenta/solução ofertada, onde estarão disponíveis as mesmas funcionalidades das especificações técnicas.

25.12. Todas as despesas com material, equipamentos, instrutores (deslocamento, despesas com traslado, hospedagem e alimentação), e demais itens necessários serão de responsabilidade da Contratada.

25.13. No âmbito da execução do contrato, respeitado o período de vigência, caso surja atualização de algum componente que integra a solução contida neste projeto, a Contratante poderá solicitar novo treinamento específico.

26. OPERAÇÃO ASSISTIDA

Unidade de medida: Serviço.

Critério de medição: Será medido e pago após a conclusão do período total da operação assistida, desde que tenham sido satisfeitas todas as exigências descritas abaixo.

26.1. A Operação Assistida se dará após o treinamento e visa assimilar na prática as informações repassadas no item treinamento.

26.2. A operação assistida terá duração de 2 meses.

26.3. Durante o período de operação assistida, a Contratada deverá manter equipe técnica especializada nas dependências do TCU por 8h diárias para prestar todo o suporte necessário para a operacionalização da solução contratada, especialmente para a realização de testes, análises, medidas e ajustes.

26.4. A equipe técnica deverá estar apta a agir rapidamente para corrigir eventuais falhas ou comportamentos inesperados da solução.

26.5. Os profissionais desta equipe técnica deverão possuir certificação na solução de controle de acesso instalada, comprovados por certificação ou outro documento idôneo que comprove de forma inequívoca a capacidade do profissional na solução implantada

26.6. Este serviço inclui, mas não se limita à seguinte atividade:

26.6.1. Disponibilização de formulário web, com possibilidade de acesso mobile, para cadastramento do quadro de pessoal da Contratante no Distrito Federal visando acesso aos edifícios, contemplando, no mínimo, as informações: biometria facial/impressão digital, nome completo, CPF, cargo, função, endereço comercial (bloco, andar, sala), lotação, e-mail, telefone.

- 26.6.2. Execução de atividade de autorização de acesso à porta controlada pelo ponto focal da unidade demandante onde será pesquisado o nome, CPF e concedido acesso à determinada porta.
 - 26.6.3. Elaboração de procedimentos especiais ou detalhamento dos procedimentos padrão, caso seja necessário.
 - 26.6.4. Elaboração de relatórios de atividades detalhando os procedimentos realizados e eventuais ajustes, se necessário.
- 26.7. A operação assistida iniciará imediatamente após a implementação de todos os equipamentos e a finalização do treinamento.
- 26.8. Devem ser fornecidos, no mínimo, os seguintes entregáveis da operação assistida:
- 26.8.1. Procedimentos customizados, possibilitando que o cliente assuma as atividades com sua própria equipe no menor tempo possível;
 - 26.8.2. Relatório ao final do período de operação contendo informações sobre atividades executadas e recomendações sobre como executar as atividades com efetividade e eficácia;
 - 26.8.3. A Contratada deve propor e tomar as ações necessárias para a prevenção da repetição das falhas que ocorrerem;
- 26.9. A operação assistida deve abranger todos os componentes da Solução de Controle de Acesso de Pessoas e Veículos, incluindo os equipamentos e softwares principais e de apoio necessários ao funcionamento da solução. A operação assistida abrange todos os componentes da Solução de Controle de Acesso de Pessoas e Veículos e de Registro de Frequência, incluindo os equipamentos e softwares principais e de apoio necessários ao funcionamento da solução.

27. MANUTENÇÃO E SUPORTE TÉCNICO

Unidade: mês.

Critério de medição: Estes serviços serão medidos e pagos por mês mediante valor fixo, composto pelos custos do posto de Técnico em Manutenção em Eletrônica e pelos custos dos demais componentes relativos aos serviços como garantia de toda a solução (equipamentos e sistemas), reposição de peças e equipamentos, atualização de softwares, suporte remoto etc., que poderá ser ajustado pelo instrumento de medição de resultados.

27.1. Os serviços de manutenção e suporte técnico terão duração inicial de 24 meses, a contar da data do recebimento definitivo do fornecimento de equipamentos e dos serviços de instalação, implementação, treinamento e operação assistida, podendo ser prorrogado nas hipóteses legais.

27.1.1. Finalizada a fase por escopo do contrato, iniciam-se os serviços de manutenção e suporte técnico, caracterizando o início da fase de prestação de serviço associado do contrato, considerando o regime de execução de fornecimento e prestação de serviço associado previsto no art. 6º, XXXIV, da Lei 14.133/2021

27.2. A prestação do serviço de manutenção e suporte técnico deverá ser realizada mediante a alocação de mão de obra com dedicação exclusiva de profissional qualificado. Ou seja, o profissional técnico deverá prestar, de forma presencial e com dedicação exclusiva, os serviços de manutenção preventiva, corretiva e de suporte técnico relativos à solução de

controle de acesso do TCU, que compreende, entre outros componentes, catracas, cancelas, portas com controle eletrônico, leitores biométricos/faciais, controladoras, sensores, botoeiras, fontes, baterias, software de controle de acesso e demais periféricos associados.

27.2.1. O posto de serviço de técnico em manutenção de solução de controle de acesso deverá funcionar de segunda a sexta-feira, das 8h às 18h, obedecendo todos os aspectos relativos à legislação trabalhista correlata, como limites mensais de horas trabalhadas e intervalos de intrajornadas para alimentação etc.

27.2.2. Atribuições do posto:

27.2.2.1. Realizar manutenções corretivas e preventivas nos equipamentos de controle de acesso;

27.2.2.2. Atuar no suporte técnico aos usuários e às equipes da contratante na operação dos sistemas;

27.2.2.3. Realizar inspeções periódicas e testes de funcionamento dos equipamentos e do sistema;

27.2.2.4. Registrar, relatar e acompanhar ocorrências e chamados técnicos;

27.2.2.5. Substituir ou reparar componentes danificados, quando necessário;

27.2.2.6. Acompanhar e apoiar atualizações e configurações do software de controle de acesso;

27.2.2.7. Auxiliar na integração de novos dispositivos ao sistema existente;

27.2.2.8. Emitir relatórios técnicos de manutenção e intervenções realizadas;

27.2.2.9. Atuar em conformidade com as normas de segurança, boas práticas e padrões definidos pelo TCU;

27.2.2.10. Apoiar atividades correlatas sempre que demandado pela fiscalização do contrato; e

27.2.2.11. Executar outras atividades inerentes aos serviços de manutenção e suporte técnico da solução de controle de acesso.

27.2.3. Requisitos mínimos de qualificação:

27.2.3.1. Ensino médio completo;

27.2.3.2. Curso técnico completo (mínimo de 120 horas) em eletrônica, eletrotécnica, mecatrônica, automação, informática ou áreas correlatas; e

27.2.3.3. Experiência comprovada de, no mínimo, **2 (dois) anos** na manutenção de sistemas e equipamentos de controle de acesso eletrônico, tais como catracas, cancelas, controladoras, leitores biométricos/faciais e softwares correlatos.

27.2.4. O profissional deve possuir certificados que atestem a sua qualificação para operar e dar manutenção nos sistemas instalados pela Contratada.

27.2.5. Este profissional será responsável por realizar atividades de manutenção e suporte técnico que não exijam mão de obra mais especializada e que possam ser realizadas in loco nas próprias dependências do Tribunal.

- 27.2.6. Caso haja a criação de chamados mais complexos que não possam ser resolvidos por esse profissional dedicado, a Contratada deverá mobilizar a equipe necessária, sem custos extras para o Tribunal e respeitando os prazos definidos no Instrumento de Medição de Resultados (IMR) para atendimento dos chamados.
- 27.3. O pagamento destes serviços será em parcelas mensais, devendo ser considerado na parcela mensal o valor do posto de técnico em manutenção de controle de acesso, bem como o custo com as manutenções preventivas e corretivas, inclusive com eventuais reposições de peças e equipamentos.
- 27.4. A Contratada deverá prover durante a vigência contratual, inclusive após o prazo final da garantia do fabricante, considerando os termos do art. 24 do CDC, a garantia contratual estendida contra vícios ou defeitos dos equipamentos e sistemas fornecidos, ou seja, a garantia de todos os itens que compõe a solução durante toda a vigência contratual será associada à prestação dos serviços de manutenção e suporte.
- 27.5. Os serviços de suporte técnico têm por finalidade garantir a sustentação e a plena utilização da solução durante a vigência do contrato. Inclui o atendimento para sanar dúvidas relacionadas com a instalação, a configuração e o uso do software e dos equipamentos ou para a correção de problemas desses, em especial na configuração de parâmetros e no tratamento de falhas, erros, defeitos ou vícios identificados no funcionamento da solução. Deve contemplar, quando for o caso, atendimento a eventual problema de instalação ou configuração de softwares básicos e de infraestrutura de TI (sistemas operacionais, servidores de banco de dados, servidores de aplicação etc.) necessários ao funcionamento da solução.
- 27.6. Deve compreender a manutenção técnica preventiva, preditiva, corretiva e evolutiva dos componentes da solução, bem como a reposição de peças e equipamentos.
- 27.7. Deve contemplar a atualização de versões dos softwares aplicativos, as quais incorporam correções de erros ou problemas registrados e melhorias implementadas pela empresa Contratada, num empacotamento estável do sistema.
- 27.8. Todos os materiais, peças e equipamentos a serem empregados nos serviços deverão ser novos, comprovadamente de primeira qualidade, e estar de acordo com as especificações, devendo ser submetidos à prévia aprovação da Fiscalização.
- 27.9. Durante o período dos serviços continuados de suporte técnico e manutenções, os valores de eventuais reposições de equipamentos e peças devem ser absorvidos no custo da mensalidade fixa precificada para este item.
- 27.10. Os equipamentos, peças e componentes para reposição/substituição deverão apresentar padrões de qualidade e desempenho iguais ou superiores aos das peças contidas na proposta da Contratada.
- 27.11. Os novos equipamentos e peças devem ser entregues no prazo máximo de 20 (vinte) dias, contados da comunicação da Fiscalização à Contratada, solicitando ou concordando com a reposição do respectivo item.
- 27.12. Para cada solicitação de reposição de item (equipamentos ou peças) deverá ser aberto um chamado para tratar do respectivo fornecimento, devendo ser objeto do respectivo IMR.

27.13. As atualizações de versão do software deverão preservar as características personalizadas para o TCU. A personalização efetuada não poderá servir de obstáculo para que o TCU receba novas versões lançadas no mercado.

27.14. Os tempos de resposta aos chamados de suporte técnico serão definidos no IMR.

27.15. Os chamados de suporte técnico poderão ser abertos 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana. No caso de sanar dúvidas quanto ao uso e outros aspectos da solução, deverão ser atendidos em horário comercial, ou seja, das 08h às 18h, de segunda-feira a sexta-feira, horário de Brasília, exceto feriados nacionais, onde:

27.15.1. **MANUTENÇÃO PREVENTIVA (MP):** é toda a ação periódica de controle e monitoramento, com o objetivo de reduzir ou impedir falhas no desempenho de um equipamento/instalação, aumentando a confiabilidade e levando o equipamento a operar sempre próximo das condições em que saiu de fábrica. Qualquer manutenção preventiva a ser realizada pela Contratada deverá ser previamente comunicada ao Contratante e por ele autorizada. Em caso de necessidade de paradas dos sistemas, os horários para as intervenções devem ser previamente combinados.

27.15.2. **MANUTENÇÃO PREDITIVA (MPD):** é uma preventiva com base na análise dos dados coletados no monitoramento (instrumentalizado ou sensitivo), prediz o tempo de vida útil de componentes de um equipamento/instalação e as condições necessárias para que este tempo seja aproveitado, definindo o melhor momento para realizar uma preventiva específica.

27.15.3. **MANUTENÇÃO CORRETIVA (MC):** é aquela realizada após a ocorrência de uma falha, visando restaurar a capacidade produtiva de um equipamento/instalação que esteja com a capacidade de exercer suas funções reduzida ou cessada. Esta manutenção inclui os procedimentos destinados a recolocar em perfeito estado de operação os serviços e produtos ofertados, tais como:

27.15.3.1. Do hardware: desinstalação, reconfiguração ou reinstalação decorrente de falhas de fabricação no hardware, atualização da versão de drivers e firmwares, correção de defeitos de fabricação, ajustes e reparos necessários, de acordo com os manuais e as normas técnicas específicas para os recursos utilizados;

27.15.3.2. Do software: desinstalação, reconfiguração ou reinstalação decorrente de falhas de desenvolvimento do software, correção de defeitos de desenvolvimento do software, de acordo com os manuais e as normas técnicas específicas do fabricante para os recursos utilizados.

27.15.4. **MANUTENÇÃO EVOLUTIVA (ME):** é o conjunto de ações destinadas à melhoria contínua dos softwares que compõem a solução de controle de acesso, visando aprimorar seu desempenho, segurança, usabilidade e compatibilidade com novas tecnologias.

27.15.4.1. Diferente da manutenção corretiva, que trata falhas já ocorridas, ou da manutenção preventiva e preditiva, que visam evitar problemas, a manutenção evolutiva busca adaptar e expandir funcionalidades,

otimizando a eficiência operacional e garantindo a adequação do sistema às novas demandas organizacionais e normativas.

27.15.4.2. Esse tipo de manutenção pode envolver atualizações de software, implementação de novos módulos, ajustes para integração com outros sistemas e aprimoramento da interface do usuário. Todas as alterações devem ser previamente avaliadas e comunicadas ao Contratante, garantindo a continuidade operacional e minimizando impactos no funcionamento do sistema.

27.16. A manutenção da solução deverá contemplar a atualização de versões do software aplicativo, as quais incorporam correções de erros ou problemas registrados e melhorias implementadas pela Contratada, num empacotamento estável do sistema. O serviço de atualização de versão tem por finalidade assegurar a devida atualização da solução durante o período de vigência do contrato. Refere-se ao fornecimento de novas versões, releases e patches de correção da solução lançados no período. A cada nova liberação de versão, release e patch de correção, a Contratada deverá fornecer juntamente as atualizações de manuais e demais documentos técnicos, bem como nota informativa das funcionalidades implementadas.

27.17. Em todos os casos, a Contratada deverá comunicar o fato ao Contratante e indicar os defeitos que serão corrigidos pelo patch e/ou alterados. A comunicação deve ser feita no prazo de até 30 (trinta) dias, a contar do lançamento de nova versão, release e/ou solução de correção.

27.18. A Contratada poderá solicitar a prorrogação de qualquer dos prazos para conclusão de atendimentos de chamados, desde que o faça antes do seu vencimento com as justificativas necessárias e que seja aprovado pela fiscalização.

27.19. A Contratada deverá prover a garantia dos novos componentes/sistemas da solução durante toda a vigência contratual, corrigindo qualquer vício ou problema encontrado, sem qualquer ônus adicionais para o Contratante.

27.20. Caso a vigência do contrato finalize e não haja renovação, a Contratada será obrigada a finalizar, em até 30 dias, os chamados abertos antes do término da vigência contratual, contados do dia posterior ao último dia do contrato.

27.20.1. A Contratante poderá reter o valor necessário para fazer frente às pendências que não forem finalizadas antes do término do contrato.

27.21. Na ocorrência de falhas que resultem perda das funções básicas, a Contratada deverá obrigatoriamente providenciar, de imediato, o restabelecimento do sistema, inclusive em horários noturnos e aos sábados, domingos e feriados.

27.22. A Contratada deverá prestar suporte técnico de forma a assegurar a disponibilidade 24h x 7 dias dos ambientes e, para isso, manter a solução em perfeitas condições de uso.

27.23. A Contratada deverá comunicar ao gestor do contrato todas as ocorrências nos equipamentos instalados que possam comprometer os serviços.

27.24. As peças, componentes e outros materiais eventualmente substituídos devem ser originais, novos e sem uso.

27.25. Toda e qualquer substituição de peças e componentes deverá ser autorizada e acompanhada pela equipe de fiscalização.

27.26. Os prazos para resolução dos chamados começarão a correr imediatamente a partir do momento em que a Contratada tome ciência do problema, seja por verificação do técnico residente, seja por meio de comunicação da Fiscalização.

27.27. A Contratada deverá prover rapidez e tempestividade na execução do suporte técnico, devendo ser observados os prazos definidos no Instrumento de Medição de Resultados (IMR).

27.28. A Contratada deverá manter atualizada a documentação da base de conhecimento e manuais de operações da solução.

27.29. Sobre os chamados técnicos:

27.29.1. Os chamados poderão ser abertos tanto pela Contratante quanto pela Contratada, quando forem identificados problemas que precisem de correção

27.29.2. Os chamados técnicos deverão ser registrados pela Contratada em plataforma específica para gerenciamento de chamados a ser disponibilizada pela Contratada sem custos extras para a Contratante.

27.29.3. De 8h às 18h dos dias úteis, os chamados serão considerados abertos imediatamente a partir do momento em que a Contratada tomar ciência do problema, seja por verificação do técnico residente, seja por meio de comunicação da Fiscalização.

27.29.3.1. Caso a ciência ocorra fora do período citado, será considerado aberto no início do dia útil subsequente.

27.29.3.2. A comunicação da Fiscalização citada acima poderá ser feita via email, telefone ou diretamente na plataforma de gerenciamento de chamados.

27.29.3.3. Feita a comunicação, a Contratada é quem deverá registrar o chamado na plataforma de gerenciamento.

27.29.3.4. A data e hora de abertura considerada deve ser a da comunicação, e não a do registro na plataforma.

27.29.4. Antes do fechamento de cada chamado, a Contratada consultará a Contratante para aprovar a solução dada. Um chamado só poderá ser encerrado quando houver a aprovação da fiscalização.

27.29.4.1. Um chamado fechado sem anuência da Contratante ou sem que o problema tenha sido de fato resolvido será reaberto e os prazos serão contados a partir da abertura original do chamado, inclusive para efeito de incidência do IMR e de aplicação das sanções previstas.

27.29.5. Para cada chamado registrado, a empresa CONTRATADA deverá associar identificador único que permita acompanhar o ciclo de vida do chamado e enviar e-mail ao Fiscal do Contrato com os dados do chamado.

27.29.6. Quando houver essa necessidade, correrá por conta exclusiva da Contratada a responsabilidade pelo deslocamento, alimentação e estadia do seu técnico ao local da disponibilização da solução, bem como pela retirada e entrega das peças e dos componentes de reposição, assim como de todas as despesas de

transporte, frete e seguro correspondentes, ou quaisquer outros custos envolvidos nos atendimentos dos chamados técnicos.

27.29.7. A Contratada ficará responsável pelo devido recolhimento dos resíduos dos processos de manutenção e limpeza dos equipamentos, que deverão ser tratados de forma ambientalmente adequada, respeitando a legislação ambiental vigente.

27.29.8. A Contratada deverá solucionar os chamados nos prazos definidos no quadro abaixo, de acordo com a criticidade do chamado. Solucionar o problema implica retornar à condição normal todos os serviços impactados pelo problema.

27.29.9. Os chamados serão divididos em dois tipos de criticidade (normal ou urgente), com prazos de resolução conforme quadro a seguir.

Criticidade do chamado	Prazo para resolução do chamado
NORMAL	20 horas
URGENTE	10 horas

27.29.10. Chamados urgentes são aqueles em que um equipamento, componente ou sistema fica inoperante, provocando a interrupção do seu funcionamento.

27.29.11. Chamados normais são aqueles que limitam, mas não interrompem o funcionamento do equipamento, componente ou sistema.

27.29.12. Caso seja comprovadamente necessária a aquisição de itens de reposição, o prazo será suspenso pelo mesmo período necessário para o fornecimento do item.

27.29.12.1. O tempo decorrido entre a abertura do chamado e o diagnóstico de necessidade de substituição não será excluído da contagem.

27.30. Relatórios.

27.30.1. A cada mês, a Contratada deverá emitir Relatório Técnico Mensal das intervenções realizadas no período ressaltando os fatos importantes ocorridos, de forma a manter registros significativos das ocorrências e intervenções nos equipamentos/sistemas, constando no mínimo os seguintes itens:

27.30.1.1. Listagem das intervenções registradas de Manutenção (MP/MPD e MC) por equipamento/instalação, categorizando entre chamados em andamento ou chamados encerrados;

27.30.1.2. Registros fotográficos dos equipamentos envolvidos antes e depois da solução dos problemas.

27.30.1.3. Total de horas gastas por tipo de intervenção (MP/MPD e MC) e tipo de equipamento/instalação;



- 27.30.1.4. Informar data do registro de acesso mais antigo armazenado nos sistemas, bem como o espaço disponível em disco;
 - 27.30.1.5. Nome do solicitante, a data de início e de fim da resolução do incidente, bem como outras informações pertinentes à gestão dos níveis de serviço solicitados; e
 - 27.30.1.6. Assinatura do Responsável Técnico da Contratada.
- 27.30.2. A Contratada deverá, ainda, fornecer Relatório Técnico específico para cada manutenção corretiva (MC), que acarretar indisponibilidade em qualquer sistema, contendo, no mínimo:
- 27.30.2.1. Descrição detalhada, com registros da ocorrência;
 - 27.30.2.2. Causa da ocorrência, com laudo técnico do fabricante/credenciado (se necessário);
 - 27.30.2.3. Histórico das rotinas de MP/MPD realizadas pertinentes à MC em questão;
 - 27.30.2.4. Solução definitiva aplicada;
 - 27.30.2.5. Nome do solicitante, a data de início e fim da resolução do incidente, bem como outras informações pertinentes à gestão dos níveis de serviço solicitados; e
 - 27.30.2.6. Assinatura do Responsável Técnico da Contratada.
 - 27.30.2.7. Este relatório (Relatório Técnico específico para cada MC), citado no item anterior, deve ser entregue até o 5º (quinto) dia útil após o encerramento do respectivo chamado.