



Consulta Pública Sistema Integrado de Controle de Acesso e CFTV para Regionais BSA e SPO

| | |
|---|-----------|
| Objeto | 4 |
| Especificação do Objeto a ser Contratado | 4 |
| Descrição da Solução | 4 |
| Locais da Execução do Serviço | 4 |
| Requisitos Gerais da Solução | 5 |
| Requisitos da Solução de Controle de Acesso | 6 |
| Especificação Técnica dos Equipamentos de Controle de Acesso | 15 |
| Requisitos da Solução de CFTV | 24 |
| Especificação Técnica dos Equipamentos de CFTV | 33 |
| Arquitetura e Integrações | 37 |
| Infraestrutura | 39 |
| Implantação da Solução | 42 |
| Cronograma | 47 |
| Qualidade e Resultados Esperados | 48 |
| Níveis de serviço e Sancionamentos | 51 |
| Especificação de Valores e Forma de Pagamento | 57 |
| Da Vistoria | 59 |
| Da Seleção do Fornecedor | 60 |

As empresas interessadas devem responder à consulta pública com as seguintes informações:

1. Contato

1.1. Nome completo do responsável pelas respostas desta Consulta Pública.

1.2. Cargo, telefones e endereço de e-mail.

2. Identificação da Empresa

2.1. Nome completo e fantasia.

2.2. CNPJ.

2.3. Endereço completo.

2.4. Site WEB (www).

3. Solução

3.1. Nome da solução, objeto desta consulta pública.

3.2. Site WEB do fabricante da solução (www).

3.3. Descrição detalhada da solução e seus componentes (Documentos/datasheet, etc).

4. Base de Clientes

4.1. Quantidade de clientes no Brasil.

4.2. Nomes dos entes públicos que já adquiriram a solução.

5. Experiência e Suporte

5.1. Possui equipe de suporte técnico para atendimento fora do horário comercial e em dia não úteis.

5.2. O suporte é prestado pelo fabricante ou parceiro?

5.3. Quais os níveis de serviços ofertados para a solução (Tempo de atendimento, tempo de resposta)

6. Proposta comercial

6.1. A proposta comercial, deve conter, no mínimo:

6.1.1. descrição do objeto, valor unitário e total;

6.1.2. Cadastro Nacional de Pessoa Jurídica - CNPJ;

6.1.3. endereço e telefone de contato; e

6.1.4. data de emissão.

7. Anexo "A" - Planilha de requisitos preenchidos.

8. Observações

8.1. Ressaltamos que o Serpro não concede ou autoriza nenhum tipo de registro de oportunidade em seus processos de contratação.

8.2. Para este processo foi observada a política de integridade de acordo com art. 32, inc. V, da Lei no 13.303/2016, Programa Corporativo de Integridade do SERPRO - PCINT (TR-082/2021) e a Cartilha de Integridade do Processo de Aquisições e Contratações.

8.3. Para conhecimento das regras de conduta no relacionamento entre fornecedores e empregados do SERPRO, acesse a Cartilha de Integridade do Processo de Aquisições e Contratações, disponível no link: https://www.transparencia.serpro.gov.br/acesso-a-informacao/licitacoes-e-contratos/documentos/Cartilha_paq_verso_final_diagramada.pdf "

1. Objeto

Contratação de serviço de controle de acesso e CFTV para as Regionais Brasília e São Paulo do SERPRO.

2. Especificação do Objeto a ser Contratado

2.1. Descrição da Solução

- 2.1.1. A contratada deverá implantar e manter uma solução integrada de Controle de Acesso e CFTV, nas instalações das Regionais Brasília e São Paulo do Serpro, pelo prazo inicial de 48 meses, conforme requisitos e especificações deste documento.
- 2.1.2. Compõe o Sistema Integrado de Segurança:
 - a. Sistema de Controle de Acesso.
 - b. Sistema de Monitoramento por Circuito Fechado IP (CFTV IP).
 - c. Infraestrutura de cabeamento estruturado em par metálico e rede elétrica.
- 2.1.3. O Sistema de Controle de Acesso a ser fornecido será composto de equipamentos de controle de acesso para portas e catracas, equipadas com leitoras de reconhecimento biométrico facial, leitoras de proximidade RFID com biometria e leitoras de proximidade RFID sem biometria. Nas cancelas a autenticação será por reconhecimento de placas veiculares. É incluso todos os elementos necessários ao funcionamento do sistema, como controladores, leitores, estações de cadastramento, switches, infraestrutura completa, serviços de instalação, configuração e capacitação técnica.
- 2.1.4. O Monitoramento por Circuito Fechado IP (CFTV IP) será composto por câmeras IP, servidor de gerenciamento, servidores de armazenamento, estações de monitoramento, switches, infraestrutura completa, serviços de instalação, configuração e capacitação técnica, tudo integrado ao Sistema de Controle de Acesso.

2.2. Locais da Execução do Serviço

- 2.2.1. Os serviços deverão ser prestados nas regionais do Serpro em Brasília e São Paulo, conforme endereços abaixo:
 - a. Regional Brasília: Módulo G Via L2 Norte SGAN 601 - Asa Norte, DF, CEP: 70836-900

- b. Regional Socorro: Rua Olívia Guedes Penteado, 941, Bairro Capela do Socorro, São Paulo, SP, CEP: 04766-900

2.3. Requisitos Gerais da Solução

- 2.3.1. A solução de Segurança deverá incluir todos os elementos necessários para seu pleno funcionamento, tais como: equipamentos, acessórios, cabeamento lógico horizontal, softwares, entre outros.
- 2.3.2. A solução deverá ser capaz de controlar a passagem de elementos diversos, tais como: controle de veículos, funcionários, prestadores de serviço, fornecedores e visitantes, além de registrar seus pertences, como notebooks e malas.
- 2.3.2.1. A identificação acontecerá em pontos de controle/bloqueio físico.
- 2.3.3. O sistema de acesso deverá estar integrado ao sistema de cftv permitindo a associação de câmeras de forma a tratar eventos gerados nos equipamentos desejados.
- 2.3.3.1. A integração deve permitir que eventos de trânsito sejam refletidos no sistema de CFTV.
- 2.3.3.2. O sistema de CFTV deve permitir integração com os eventos gerados pelo sistema de controle de acesso, tais como: acesso permitido, acesso bloqueado, porta aberta e porta forçada.
- 2.3.4. Cada um dos eventos citados no item anterior, deve permitir a adição de marcadores a trechos do vídeo correspondente ao evento ocorrido, permitindo a visualização do vídeo da(s) câmera(s) associadas à área controlada.
- 2.3.5. Todos os equipamentos, produtos, peças ou softwares necessários à contratação deverão ser novos e de primeiro uso e não constar, no momento da apresentação da proposta, em listas de end of sale, end of support ou end of life do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante.
- 2.3.6. Os relatórios gerados devem ser plenamente compatíveis com o servidor de impressão do SERPRO.
- 2.3.7. A solução deve estar em conformidade com a Lei Geral de Proteção de Dados Pessoais - LGPD, Lei nº 13.709/2018.

- 2.3.8. Todos os elementos de controle de acessos devem estar em conformidade com os regulamentos de evacuação, legislação e determinações do Corpo de Bombeiros do local.
- 2.3.9. Deverá ser permitida a inserção, em ambos sistemas de controle de acesso e CFTV, de Avisos de Privacidade e Termos de Uso, para conformidade com a LGPD. Os referidos Avisos de Privacidade e Termos de Uso serão elaborados pelo Serpro.

2.4. Requisitos da Solução de Controle de Acesso

- 2.4.1. Todos os equipamentos de borda, de um mesmo grupo, devem ser de um único fabricante, garantindo a compatibilidade funcional e estética.
- 2.4.2. O Sistema de Controle de Acesso deverá ser compatível com ao menos dois dos três navegadores mais populares (Microsoft Edge, Mozilla Firefox e Google Chrome), ser 100% WEB, sendo o acesso pelo computador cliente exclusivamente através de browser sem limite de estações de trabalho.
- 2.4.3. O sistema de controle de acesso deve trabalhar com certificado HTTPS para conexão confiável da estação de trabalho (cliente).
- 2.4.4. O Sistema de Controle de Acesso 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.
- 2.4.5. O software deve desvincular o cartão provisório automaticamente quando o usuário colocar o cartão na urna.
- 2.4.6. O software deve ativar automaticamente o cartão principal quando o cartão provisório for desvinculado manualmente ou automaticamente.
- 2.4.7. O software deve permitir a configuração para que seja obrigatório o depósito do cartão provisório na urna ao sair
- 2.4.8. Deve possuir lista de acesso de pessoas proibidas (blacklist)
- 2.4.9. O sistema deve disponibilizar manuais de acesso via Interface, a fim de agilizar o autoconhecimento do operador.
- 2.4.10. O sistema deve permitir:
 - a. o bloqueio por controle de documentos do usuário;
 - b. o alerta para o operador quando o usuário tiver alguma restrição ao acesso;
 - c. o bloqueio de usuário por inatividade de acesso por período configurável;
 - d. que um usuário tenha mais de um crachá vinculado ao seu cadastro;

- e. o cadastramento de identificadores (cartões de proximidade) individualmente ou em lotes;
- f. a configuração de servidor NTP;
- g. a criação de status de usuários com a opção de bloqueio de acesso;
- h. o registro de acesso manualmente, conforme permissão do operador;
- i. capturar foto do momento do acesso;
- j. que o operador crie atalhos de funcionalidades para agilizar a operação.

- 2.4.11. O software deve suportar a funcionalidade de acesso assistido, onde 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.
- 2.4.12. O sistema deverá possuir perfeita integração com os dispositivos de reconhecimento facial.
- 2.4.13. 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.
- 2.4.14. 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.
- 2.4.15. O Sistema de Controle de Acesso deve ser concebido de tal forma que falhas locais não venham implicar falha de todo sistema. Controladores de acesso locais continuam a funcionar, mantendo a integridade dos níveis de acesso dos usuários, mesmo se a conexão de rede com o software de gerenciamento falhar.
- 2.4.16. O sistema deve permitir a administração de crachás, criando tipos/ layout de crachás como Funcionário, Prestador de Serviço, Visitante, Provisório, e/ou algum tipo Especial (personalizado pelo administrador) salvando o modelo para uso futuro.
- 2.4.16.1. Uma vez elaborado o crachá, o sistema deve permitir o controle sobre o status de impressão.
- 2.4.17. O Sistema de Controle de Acesso deve gerenciar datas de validade de usuários e cartões, e permitir que a ativação de cartões provisórios invalide o cartão original temporariamente.
- 2.4.18. O Sistema de Controle de Acesso pode ser compartilhado com, no mínimo, 50 divisões. Cada divisão tem acesso apenas a seus próprios dados.

- 2.4.19. O servidor do sistema de controle de acesso deve atuar como a fonte que fornece sincronização de horário em todos os subsistemas.
- 2.4.20. O Sistema de Controle de Acesso deve ser concebido de tal forma que uma falha de qualquer subsistema não afete todos os outros subsistemas.
- 2.4.21. O Sistema de Controle de Acesso deverá ter uma estrutura modular que permita a sua expansão ou redução futura, com interrupção mínima para o sistema operacional existente.
- 2.4.22. O Sistema de Controle de Acesso deve suportar, no mínimo, 10 estações de trabalho operando nas recepções ao mesmo tempo.
- 2.4.23. O Sistema de Controle de Acesso deve fornecer uma maneira fácil de cadastrar cartões de acesso no banco de dados. Além dos dados básicos, como nome, sobrenome, número de crachá, foto 3x4 e autorizações, as seguintes informações devem ser possíveis, mas não limitadas a:
- a. 3 códigos PIN (ID, acesso, identificação)
 - b. Período de validade
 - c. Filiação
 - d. Campos de status, como empregado, visitante, guarda
 - e. Campos de endereço
 - f. Matrícula e lotação
 - g. Dados pessoais
- 2.4.23.1. Campos individuais podem ser adicionados, eliminados ou editados por administrador.
- 2.4.23.2. Campos individuais podem ser editados para diferentes tipos de dados, como texto, número, data, hora, check box e caixa de combinação.
- 2.4.23.3. Prever diversas situações para controle de usuários, tais como ativos, inativos, férias, desligados.
- 2.4.24. O cadastramento de cartões deverá ser possível através de um leitor de controle de acesso ligado ao sistema de controle de acesso.
- 2.4.25. O cadastramento biométrico (como impressões digitais, palma, veia e imagens) deve ser totalmente integrado no Sistema de Controle de Acesso, sem a necessidade de software de terceiros.

- 2.4.26. O cadastramento de biometria da falange e reconhecimento facial deve ser feito uma única vez, e propagado para os demais equipamentos.
- 2.4.27. Deve ser possível importação e exportação de cadastro de usuários do sistema de controle de acesso.
- 2.4.28. O Sistema de Controle de Acesso deve fornecer uma maneira simples, para os administradores configurarem entradas/coletores.
- 2.4.29. O sistema de controle de acesso deve ter, no mínimo, as seguintes funcionalidades:
- a. O Sistema de Controle de Acesso deve fornecer a capacidade de definir e gerenciar áreas lógicas arbitrárias no interior das instalações. Estas poderiam ser salas individuais, grupos de salas, andares inteiros ou áreas de estacionamento.
 - b. O Sistema de Controle de Acesso deve permitir a composição de níveis de acessos, agilizando o gerenciamento de múltiplos pontos de controle de uma mesma sala.
 - c. O sistema deve permitir a composição de níveis de acessos ilimitados.
 - d. O Sistema de Controle de Acesso deve permitir o controle do número máximo de elementos simultâneos em uma determinada área.
 - e. Permitir a configuração de intertravamento entre as portas controladas.
 - f. Permitir desativar a regra de intertravamento para determinado usuário, quando necessário.

Verificação de acesso Sequência

- 2.4.30. Deve ser fornecida uma verificação de sequência de acesso, permitindo que portadores de cartões autorizados entrem em uma área somente quando eles tiverem passado seu cartão na área vizinha.

Acesso autorizado duplo ou múltiplos

- 2.4.31. Possuir recurso de múltipla autenticação para, no mínimo, 2 usuários, aplicável quando 2 ou mais usuários são requeridos para liberação de acesso em dado recinto.

Dupla entrada

- 2.4.32. Possuir controle de anti dupla entrada (APB).
- 2.4.33. Permitir a configuração de tempo independente, de entrada e de saída, quando a funcionalidade APB for ativada.
- 2.4.34. Permitir desativar para determinado usuário a funcionalidade APB, quando ativada de modo geral.

Gestão de visitantes

- 2.4.35. Administração de visitantes deve ser fornecida pelo software de gerenciamento do sistema de controle de acesso no mesmo banco de dados.
- 2.4.36. A gestão de visitantes deve permitir a impressão de um crachá de visitante.
- 2.4.37. A solução deverá conter, ou possibilitar personalização, campos tais como: nome, documento oficial, foto 3x4, empresa de origem, cargo, telefone, e funcionário do SERPRO responsável pelo visitante.
- 2.4.38. Permitir a captura de fotos de visitantes, com uso de câmeras nas portarias.
- 2.4.39. 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.
- 2.4.40. Permitir a baixa automática do cartão do visitante após a passagem pela saída de visitantes, quando for utilizada urna associada à catraca.
- 2.4.41. Permitir número ilimitado (na ordem de milhões) de visitantes cadastrados ao sistema (na condição de inativos – dissociados de cartão RFID).
- 2.4.42. Permitir a configuração de alarmes para visitas expiradas.
- 2.4.43. Permitir o agendamento de visitas, a fim de agilizar a operação da recepção.
- 2.4.44. Permitir identificar o motivo da visita.
- 2.4.45. Sinalizar se o visitado está presente na empresa no momento da visita.
- 2.4.46. Permitir inserir mensagens de orientação na portaria para visitantes pré-cadastrados que precisem de acompanhamento ou avisar por telefone a um funcionário.
- 2.4.47. Permitir o limite de visitantes por lotação ou faixa horária a uma área controlada;
- 2.4.48. 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.

Agrupamento dos elementos controlados

- 2.4.49. O sistema deve permitir agrupamento dos elementos controlados em várias categorias, com funcionalidades distintas, tais como: Prestadores de Serviço, Estagiário, Visitante, Por Empresa ou novas categorias criadas pelo SERPRO.
- 2.4.50. Permitir o bloqueio ou liberação de um grupo.
- 2.4.51. Permitir editar um campo de todos os elementos de um grupo.

Gerenciamento de Estacionamento

- 2.4.52. Permitir configuração para controle de limite de vagas para veículos - estacionamento.
- 2.4.53. Permitir o acesso de veículos através da leitura da placa do veículo (LPR).
- 2.4.54. O espaço pode ser dado a pessoas externas via vouchers para várias entradas.
- 2.4.55. Permitir o cadastro de veículos e a associação com os respectivos proprietários.

Gerenciamento de rondas e patrulhas

- 2.4.56. Deverá ser capaz de realizar o controle de rondas dos vigilantes.

Aplicação de rotas

- 2.4.57. Uma Rota é uma sequência predefinida de leitores que podem ser prescritos para as pessoas a direcionarem seus movimentos no interior das instalações, independentemente de autorização da pessoa.

Rastreamento de pessoas para pesquisa forense

- 2.4.58. Uma pessoa pode ser pesquisada em um banco de dados para todas as ações de entrada, para que os vídeos gravados dessa pessoa sejam mostrados rapidamente. Ex: uma porta pode ser pesquisada para todas as pessoas que passaram por esta para a investigação de vídeo rápido.

Gestão de claviculários

- 2.4.59. O sistema deverá possuir funcionalidade para gerenciamento de chaves, de acordo com permissão do usuário.
- 2.4.60. A funcionalidade de gerenciamento de chaves deve possuir um relatório que permita identificar no mínimo: chave retirada ou devolvida, localidade da chave, responsável por conceder acesso ou devolução da chave, usuário que recebeu e devolveu a chave e data/hora do evento.
- 2.4.61. Essa funcionalidade deverá estar vinculada à gestão de permissões de acesso do sistema.

Controle de Itens e guarda volumes

- 2.4.62. Deverá ser permitido o cadastro de itens diversos que podem ser associados e dissociados dos elementos controlados, sendo itens de sua responsabilidade, tais como: notebooks, malas executivas, smartphones, tablets e equipamentos eletrônicos que podem interferir nos serviços da empresa.

- 2.4.63. Deve ser possível criar tipos de itens para fins de cadastramento, e personalizar seus campos para contemplar critérios como: “notebook contendo campos para nº de série, fabricante, modelo, considerações, características”.
- 2.4.64. Deve ser possível cadastrar guarda volumes e controlar os itens em dois tipos de fluxo: em trânsito ou armazenamento (guarda volumes).
- 2.4.65. Essa funcionalidade deverá estar vinculada à gestão de permissões de acesso do sistema.

Emergência

- 2.4.66. Permitir, em caso de emergência, a liberação e/ou bloqueio de controladoras de modo automático (sem intervenção de operador) ou manual (com intervenção de operador).
- 2.4.67. O Sistema de Controle de Acesso deve ser capaz de realizar o destravamento de todos os pontos através da interface cliente.

Monitoração

- 2.4.68. O software deve possuir tela de monitoramento de alarmes gerados por eventos da controladora e/ou dispositivos I/O's.
- 2.4.69. Permitir que ao tratar um evento de alarme, o operador registre anotações.
- 2.4.70. Permitir monitorar em tempo real o acesso dos usuários, mostrando os dados como:
 - a. Nome do usuário;
 - b. Foto do usuário
 - c. Número do crachá/identificador (se houver);
 - d. Nome da controladora/ponto de acesso;
 - e. Data e hora do acesso;
 - f. Método de identificação;
- 2.4.71. Permitir monitorar um ponto de acesso em tempo real com visualização de câmeras em tempo real.
- 2.4.72. A solução deverá ser capaz de personalizar as configurações de visualização de telas.
- 2.4.73. As configurações devem abranger no mínimo a permissão de emissão de som em caso de alarmes, tempo de atualização de informações na página de eventos e sobreposição de tela nos eventos com maior prioridade.

Relatórios do Sistema

- 2.4.74. 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: csv, xls e pdf.
- 2.4.75. 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.
- 2.4.76. 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.
- 2.4.77. A ferramenta deverá permitir o download e envio de relatórios por e-mail.
- 2.4.78. A ferramenta deverá permitir agrupar os relatórios por categoria, a fim de criar maior gestão e organização.
- 2.4.79. 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.
- 2.4.80. Os relatórios deverão conter elementos gráficos (imagens, logotipo) na definição dos relatórios, que serão disponibilizados pelo SERPRO.
- 2.4.81. A ferramenta deverá permitir a definição e utilização de fórmulas, totalizadores e expressões matemáticas.

Segurança e Administração do sistema

- 2.4.82. O sistema de controle de acesso deve:
 - a. Ser capaz de cadastrar os administradores com diversos níveis de permissão e com limitação do horário em que dado administrador tem acesso.
 - b. Permitir o impedimento de autenticação simultânea em mais de uma estação.
 - c. 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.
 - d. Deverá ser possível o envio de e-mails automáticos em caso de eventos de alertas.
 - e. Deverá utilizar criptografia na comunicação de todos dados trafegados.
 - f. Deverá prover auditoria de ações dos usuários, inclusive os administradores, com possibilidade de filtro de pesquisa.
 - g. Deverá possibilitar a customização dos perfis dos usuários, permitindo a criação de perfis de forma ilimitada.
 - h. 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.

- i. Deverá configurar permissões de acesso por estações permitidas de login.

Ações Automatizadas

- 2.4.83. O sistema deverá possibilitar a configuração de ações iniciadas a partir de eventos ou através de agendamento.
- 2.4.84. As ações deverão abranger a possibilidade de rastrear o trânsito de uma pessoa, notificando todos eventos de cartão gerado pela pessoa em específico.
- 2.4.85. As ações deverão permitir o envio de e-mails nas situações dos eventos de maior prioridade.
- 2.4.86. Quanto ao envio de e-mails, deve ser possível customizá-los utilizando tags HTML.
- 2.4.87. O sistema deve permitir o envio de e-mails para os responsáveis em caso de violação das políticas de horário de acesso às dependências do SERPRO;
- 2.4.88. Possuir registros de ocorrências por categorias, com opção de envio por e-mail.
- 2.4.89. Permitir a criação de alerta caso um usuário permaneça em uma área por tempo superior ao estabelecido previamente.

Gestão de dispositivos

- 2.4.90. Quanto à gestão de dispositivos, o sistema de controle de acesso deverá:
 - a. Possibilitar o cadastro, consultas, alteração e exclusão dos equipamentos controladores e suas respectivas leitoras.
 - b. Além das informações básicas tais como: nome, descrição e endereço IP, o sistema deverá possibilitar vincular uma câmera ao equipamento.
 - c. Deverá possibilitar a verificação de status e controle do funcionamento em tempo real dos equipamentos.
 - d. A supervisão e controle desses dispositivos deverá ser realizada por meio de telas gráficas.
 - e. Deverá possibilitar o envio de comandos para os equipamentos cadastrados.
 - f. Os comandos devem possibilitar o bloqueio, desbloqueio e normalização dos equipamentos.
 - g. Permitir enviar e-mail de alerta sobre falha e retorno de comunicação com a controladora, para análise de manutenção preventiva.
 - h. Permitir o agendamento de abertura e/ou travamento do ponto de controle de acesso sem intervenção de operador.
 - i. Permitir gerar alerta na falta de alimentação AC.

- j. Permitir gerar alerta quando a bateria da fonte estiver com baixa tensão.
- k. Permitir gerar alerta quando a bateria da fonte não estiver mais carregando.

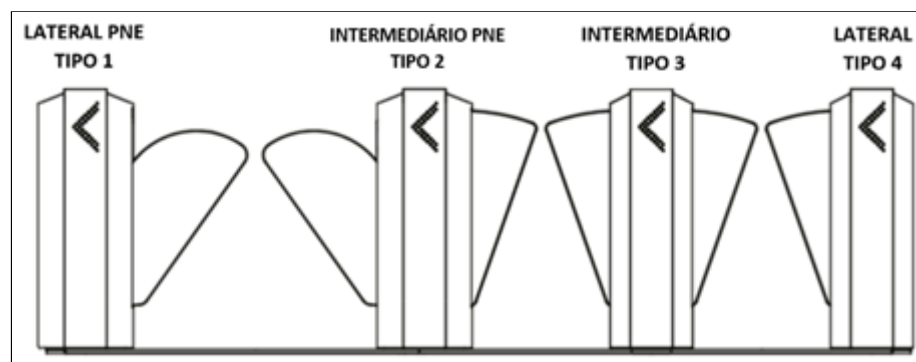
Customizações

- 2.4.91. Caso não hajam funcionalidades nativas para cumprimento integral dos itens definidos nas sessões "gestão de claviculários", "controle de itens e guarda volume", "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.
- 2.4.92. 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.
- 2.4.93. A CONTRATADA assumirá todos os custos referentes à integração das funcionalidades, que deverão constar na apresentação de suas propostas e o SERPRO não será, em nenhum caso, responsável por esses custos.

2.5. Especificação Técnica dos Equipamentos de Controle de Acesso

Catracas Tipo Flap

- 2.5.1. As catracas do tipo "Flap" são categorizadas pelos seguintes módulos: Lateral PNE, Intermediário PNE, Intermediário e Lateral. A utilização desses módulos segue conforme abaixo:



- 2.5.2. As catracas "Flap" deverão atender os seguintes requisitos:
 - a. Estar em conformidade com os regulamentos de evacuação, legislação e determinações do Corpo de Bombeiros do local. Serem do tipo barreira de vidro de segurança

temperado ou policarbonato, possibilitando vão de acesso de mínimo 500 mm, ou 900 mm na versão para acesso PNE. As barreiras poderão ainda ser de vidro de segurança temperado com espessura mínima de 12 mm ou serem policarbonato de segurança com espessura mínima de 15 mm.

- b. Deverão possuir sensores na extensão do gabinete para monitorar o fluxo de acesso dos usuários e inibir acesso de “caronas” com acabamento em aço inox, com 1,5mm de espessura, resistente a choques e vibrações. Deverão ainda possuir estrutura interna em aço e peças mecânicas tratadas contra corrosão.
- c. Deverão permitir controle de acesso bidirecional.
- d. Deverão possuir mecanismo motorizado automático para abertura das barreiras e sistema de amortecimento de impacto.
- e. Sistema de abertura anti-pânico, onde em caso de emergência ou falta de energia as barreiras de bloqueio se abrem automaticamente.
- f. Deverão possuir pictograma operacional indicando Stand by, acesso liberado ou bloqueado, bem como pictogramas intuitivos bicolores ou tricolores para sinalizar ao usuário a operação do equipamento e sentido de fluxo.
- g. Fonte de alimentação chaveada “Full Range” 110 ou 220V com proteção de curto circuito.
- h. Deve possuir no mínimo 5 pares de sensores Fotoelétricos de alta precisão tipo barreira que monitoram a passagem do usuário desde o início até o final do percurso, sendo no mínimo, 1 (um) par para a função de anti-esmagamento (evita que o vidro de segurança temperado ou policarbonato feche no usuário).
- i. As catracas devem possuir cofre coletor no corpo do equipamento e capacidade de armazenamento de no mínimo 120 cartões.
- j. Deverá possuir tempo médio entre falhas (MCBF): mínimo 500.000 de ciclos e suportar temperatura de trabalho entre 0 e 55°C.

Catraca Motorizada PNE

2.5.3. As catracas motorizadas PNE deverão atender os seguintes requisitos:

- a. Estar em conformidade com os regulamentos de evacuação, legislação e determinações do Corpo de Bombeiros do local.
- b. Possibilitar um vão de 90 cm de passagem. Sua porta de bloqueio deve possuir abertura em 180°.
- c. Deverão possuir mecanismo motorizado, garantindo maior precisão, durabilidade e suavidade durante a passagem.
- d. Sistema de liberação automática de passagem em caso de emergências permitindo uma evacuação segura e rápida.
- e. Braço em vidro de segurança temperado de no mínimo 12 mm de espessura ou policarbonato de no mínimo 15mm de espessura;
- f. Deverão possuir sensores de monitoramento de passagem.

- g. Deverão ser construídas por estrutura monobloco com acabamento totalmente em aço inox escovado longitudinalmente, configurada a laser, resistente a choques, vibrações e elementos ácidos e alcalinos.
- h. Deverão suportar temperatura de trabalho entre 0 e 50°C.
- i. Deverão ser fornecidas com totem com urna coletora de cartões.

Catraca Balcão

2.5.4. As catracas “Balcão” deverão atender os seguintes requisitos:

- a. Estar em conformidade com os regulamentos de evacuação, legislação e determinações do Corpo de Bombeiros do local.
- b. Catraca com braço em aço inox.
- c. Acabamento em aço inox, com 1,2mm de espessura, resistente a choques e vibrações;
- d. Terem estrutura interna em aço e peças mecânicas tratadas contra corrosão.
- e. Permite controle de acesso bidirecional.
- f. Deverão possuir mecanismo automático para destrave do braço, do tipo “braço que cai”.
- g. Deverão possuir sistema de amortecimento de impacto.
- h. Sistema de abertura anti-pânico, onde em caso de emergência ou falta de energia as barreiras de bloqueio se abrem automaticamente “braço que cai”;
- i. Deverão possuir pictogramas intuitivos bicolores ou tricolores para sinalizar ao usuário a operação do equipamento e sentido de fluxo;
- j. Fonte de alimentação chaveada “Full Range” 110 ou 220V com proteção de curto circuito;
- k. As catracas deverão possuir cofre coletor no corpo do equipamento e capacidade de armazenamento de no mínimo 120 cartões.
- l. Deverão possuir Tempo médio entre falhas (MTBF): mínimo 500.000 (quinhentos mil) de ciclos e suportar temperatura de trabalho entre 0 e 55°C.

Cancelas

- 2.5.5. Deverá ser do mesmo fabricante das catracas, possuir braço em alumínio e a barreira deverá ser do tamanho 6 metros. A cancela ainda deverá possuir gabinete confeccionado em alumínio e aço inoxidável, livre de corrosão, em junção com a tecnologia de pintura eletrostática a pó em aço carbono, contendo tratamento anticorrosão e pintura eletrostática.
- 2.5.6. A cancela deverá operar totalmente à seco, não necessitando de lubrificação ou substituição de batentes de borracha. Deverá ainda possuir sistema que evite que o braço e a cancela sejam danificados no caso de passagem não permitida ou forçada. No caso de um veículo colidir com o braço da cancela, este deve movimentar-se lateralmente.
- 2.5.7. A cancela deverá possuir MTBF: 5.000.000 ciclos, conter sistemas de acionamento manual e antiesmagamento para emergências.

2.5.8. Deverá ainda possuir fonte de alimentação: fase 110V / 220V +/- 10% de variação, possuir índice de proteção IP54 e entradas para sinais de detector tipo laço indutivo e de fotocélula infravermelha.

2.5.9. Deverá ser fornecida com 01 (um) laço indutivo.

Controlador de Acesso

2.5.10. Consiste em uma ou mais placas controladoras, que irão gerenciar os bloqueios de acesso e leitores de cartão e biometria.

2.5.11. As placas deverão ser compatíveis com os Leitores de Cartão de Proximidade, Leitores de Cartão de Proximidade e Biometria e Leitores Biométricos Faciais para Portas e Catracas.

2.5.12. Deverá possuir interface de comunicação ethernet TCP/IP 10/100 Mbps integrada, sem o uso de dispositivo auxiliares.

2.5.13. Deverá possuir tensão de alimentação: 11,5 – 15VDC e suportar alimentação PoE 802.3af ou PoE+ 802.3at, on board sem auxílio de dispositivos externos.

2.5.14. Deverá possuir RTC onboard com alimentação independente por bateria de lítio de longa duração.

2.5.15. Deverá possuir no mínimo as seguintes proteções: contra sobrecorrente na saída de alimentação para as leitoras, e contra inversão de polaridade na alimentação do dispositivo.

2.5.16. Deverá possuir modo de operação configurável via sistema, isto é, opera com portas, catracas (incluindo modelos PNE e balcão), torniquetes e cancelas, sem a necessidade de dispositivo auxiliar.

2.5.17. Deverá possuir capacidade de armazenamento de 100.000 eventos na memória interna em caso de perda de comunicação com o servidor de acesso. Possuir capacidade de armazenamento para: 100.000 usuários nos modos de identificação por cartão, senha, código; 100.000 usuários nos modos de verificação por cartão + biometria e código + biometria (1:1) e 10.000 usuários no modo de identificação por biometria (1:n).

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

- 2.5.19. Deverá permitir atualização de firmware remotamente via servidor ou estação de cadastro e ter opção, por hardware, para reset de configuração default.
- 2.5.20. Deverá possuir interface para conexão de display, que fornecerá ao usuário informações de data/hora e mensagens relativas ao seu acesso.
- 2.5.21. A validação local dos acessos e o relógio interno (RTC) garantem, mesmo em caso de perda de comunicação com o servidor, que o acesso e o registro de eventos dos usuários não sejam prejudicados.
- 2.5.22. Deverá possuir recursos de Anti-Dupla-Entrada (APB), contendo configuração de tempo de entrada e/ou saída de APB independentes, bem como possuir alarme de Porta Aberta por Muito Tempo (PAMT).
- 2.5.23. Deverá possuir controle de faixas horárias de acesso simples e agrupadas. Deverá permitir apontamento para mais de um host/servidor.
- 2.5.24. Deverá ainda possuir memória flash não volátil para armazenamento de informações e comando remoto para captura de biometria de usuário.
- 2.5.25. Deverá possibilitar modos de acesso com lógica e/ou: reconhecimento facial e cartão, biometria de falange e cartão, somente reconhecimento facial, somente biometria falange ou somente cartão. Atendendo o conceito de multi fator de autenticação. Deverá ainda conter sistema operacional ou firmware livre de renovação de licenciamento.

Leitor Biométrico Facial

- 2.5.26. Deverá suportar modo de operação stand-alone com memória para, pelo menos, 6.000 faces. O leitor deverá ainda detectar as faces, capturar, realizar a comparação com banco de dados de imagens interno e realizar o acesso. Deverá possuir interface Ethernet para comunicação via TCP/IP com o repositório do banco de dados de faces.
- 2.5.27. Deverá possuir alertas de voz e ser capaz de permitir a leitura das faces em até 1m de distância. Deverá ainda possuir display de LCD de pelo menos 7", possuir, ao menos, duas câmeras de 2MP para captura de faces, possuir tempo de comparação de faces 1:N menor que 0,5s e Taxa de Acurácia de Reconhecimento de Faces maior que 99%. Deverá permitir distinguir um rosto de uma pessoa viva de uma foto ou imagem de vídeo (liveness).
- 2.5.28. Deverá suportar conexão a controladora externa, temperatura de operação de no mínimo 0 a 50°C e operação com umidade de 10 a 90%, não condensada, no mínimo.
- 2.5.29. Deverá suportar alimentação elétrica de 12VDC, com grau de proteção IP55 ou superior.

- 2.5.30. Deverá ainda ser integrado ao software ofertado, ou seja, os cadastros e envios de fotos devem possuir a mesma interface do software de acesso.
- 2.5.31. Deverá identificar a face independente do uso de máscara.
- 2.5.32. Deverá alertar para uso de máscara facial: se o rosto de reconhecimento não usar máscara, o dispositivo emitirá um lembrete de voz.
 - 2.5.32.1. Deverá permitir o bloqueio do acesso quando não for detectado o uso de máscara.

Características específicas do leitor biométrico facial com termografia

- 2.5.33. Deverá realizar medição de temperatura entre: 30 °C a 45 °C, com precisão de medição: 0,1 °C e desvio de medição: $\pm 0,5$ °C.
- 2.5.34. Os leitores para reconhecimento facial, a serem instalados para controle de portas, deverão ser fornecidos com suporte para instalação em parede.

Leitor de Cartão de Proximidade

- 2.5.35. O leitor fornecido deverá ser compatível com todas as funcionalidades do sistema de controle de acesso e deverão atender os seguintes requisitos:
- 2.5.36. Suportar a leitura de cartões no padrão ISO 14443A. Operar na frequência de 13,56MHz, com interface de comunicação Wiegand. Deverá possuir indicação sonora, com capacidade de emissão de som com diferentes sequências para significar acesso concedido, acesso negado, energização e diagnóstico.
- 2.5.37. Possuir indicação visual, luz de alta intensidade que fornece uma indicação visual clara de estado, permitir distância de leitura de no mínimo 5 cm,, não sendo permitida a alimentação com fontes adicionais.
- 2.5.38. Deverá ser compatível com os cartões utilizados atualmente no SERPRO, cuja tecnologia é denominada Mifare Classic.

Leitor de Cartão de Proximidade e Biometria

- 2.5.39. Deverá ser do mesmo fabricante do Leitor de Cartão de Proximidade.
- 2.5.40. Deverá possuir elemento de sinalização por LED, teclado para autenticação por senha numérica e leitor de cartões 13,56MHz integrado (onboard).

- 2.5.41. O leitor biométrico deverá ainda suportar Taxa de Falsa Rejeição (FRR) e Taxa de Falsa Aceitação (FAR) menores que 0,01%.
- 2.5.42. O leitor biométrico deverá possuir capacidade de analisar, no mínimo, 80 pontos (minúcias) por impressão digital (template), possuir tempo típico de reconhecimento de templates biométricas inferior a 1 segundo e permitir a identificação com variações angulares do dedo de 30 graus (podendo variar de acordo com a qualidade da captura).
- 2.5.43. Deverá ainda possibilitar modos de acesso com lógica e/ou impressão digital e cartão, somente impressão digital ou somente cartão.
- 2.5.44. Deverá ser compatível com os cartões utilizados atualmente no SERPRO.

Kit Fechadura Eletrônica

- 2.5.45. Deverá ser instalado 01 (um) kit composto pelos seguintes acessórios:
- a. 01 (uma) Fechadura Eletromagnética com: acabamento em aço inox ou alumínio escovado, força de ataque mínimo 150 kg. O eletroímã será instalado em portas que abrem para dentro e o suporte deve permitir a instalação no lado de dentro do ambiente.
 - b. 01 (uma) Fonte de Alimentação com bateria
 - c. 01 (um) Botão de acionamento de saída de emergência com: botoeira de emergência rearmável, possuir conexões COM-NA-NF para liberação da porta e acionamento de alarme. Deverá ser fornecido na cor verde ou vermelha e possuir construção em plástico ABS.
 - d. 01 (um) Sensor Magnético com: sensor magnético de abertura de porta e deverá ser instalado sobreposto nas portas controladas.

Câmera para Leitura de Placas

- 2.5.46. Câmera IP do tipo bullet ou box com caixa de proteção, com ajuste de posicionamento em 3 eixos, permitindo a regulação de ângulo de rotação, inclinação vertical e horizontal;
- 2.5.47. Deverá possuir corpo em metal e possuir 1 (uma) saída e 1 (uma) entrada de alarme. Deverá ainda possuir LEDs infravermelhos integrados (ou ser fornecida com iluminador).
- 2.5.48. Deverá ser fornecida com suporte para fixação em parede, poste ou teto, conforme a necessidade e local de instalação. Deverá ser fornecida com caixa de proteção para acomodação de cabos/conexões quando necessário e os acessórios como caixas de proteção e suportes, deverão ser do mesmo fabricante da câmera, ou homologados pela mesma, garantindo a qualidade da solução.

- 2.5.49. Deverá possuir conector Ethernet RJ-45 compatível com padrão 100BaseT integrado à câmera, sem a necessidade de adaptadores externos, além de possuir slot para SD/Micro SD/SDHC/SDXC com suporte para cartões de 64GB;
- 2.5.50. As câmeras deverão vir acompanhadas com o cartão de memória de no mínimo 64GB.
- 2.5.51. Deverá possibilitar operação em temperaturas entre 0°C a +50°C, com até 95% de umidade (sem condensação) e possuir alimentação PoE ou PoE+. Caso o modelo não seja compatível com PoE ou PoE+, deve ser fornecida fonte ou injetor do mesmo fabricante. Deverá ainda possuir certificação IP66 e IK10.
- 2.5.52. Deverá possuir sensor de imagem CMOS de varredura progressiva com resolução HD de 2MP (1920 x 1080).
- 2.5.53. Deverá operar com baixa luminosidade, com sensibilidade mínima igual ou inferior a 0,005 lux no modo colorido, possuir função Dia/Noite com filtro de IR com troca automática, programada ou ativada por alarme, função de Compensação de Luz de Intensa (HLC) e função de Compensação de Luz de Fundo (BLC). Deverá ainda suportar faixa dinâmica ampla (WDR) e possuir função de foco automático.
- 2.5.54. Deverá possuir funcionalidade embarcada para inserir máscaras de privacidade e suportar protocolos, conectividade e segurança. Deverá suportar protocolo de compressão de vídeo superior ao padrão H.264 (H.265, H.264B, Zipstream, H.264+, H.264H, H.265+ ou similares), com alta relação de compressão, permitindo uma economia de tráfego de transmissão e maior capacidade de armazenamento.
- 2.5.55. Deverá possuir servidor web embarcado, permitindo a configuração da câmera e visualização das imagens em navegador web. Deverá possibilitar que os recursos de configuração, gravação e visualização somente sejam acessados através de senha pré-configurada.
- 2.5.56. Deverá possuir criptografia HTTPS, bem como ser compatível com os protocolos: TCP/IP, HTTP, HTTPS, FTP, DNS, RTP, RTSP, RTCP, UPnP, IPv6, UDP. Deverá ainda suportar protocolo NTP (Network Time Protocol) para sincronismo de horário, suportar função de gravação local no caso de falha na rede (ANR) e possuir interface de entrada e saída de áudio.
- 2.5.57. Deverá registrar eventos a partir de: tentativa de obstrução/ violação da câmera (tampering), rede desconectada, conflito de endereço IP e falha no armazenamento de imagens.
- 2.5.58. Deverá possuir análise de vídeo inteligente embarcada e/ou licenciada para funcionamento via software, permitindo a detecção e reconhecimento de placas

veiculares por uma combinação de algoritmos de análise de vídeo. Deve atender aos requisitos:

- a. Detecção e reconhecimento de placas veiculares compatível com o padrão vigente no Brasil; e
- b. Detecção e reconhecimento de placas em motocicletas.

Estação de Cadastro

- 2.5.59. Deverá ser do tipo Desktop.
- 2.5.60. Suportar no mínimo dois monitores, através das conexões Display Port, DVI ou HDMI.
- 2.5.61. Deverá possuir sistema Operacional Microsoft ® Windows 10 ou superior instalado de fábrica e ser compatível com o Software Cliente do Software de Controle de Acesso.
- 2.5.62. Deverá possuir no mínimo: 1 porta de rede Gigabit Ethernet e 1 (um) processador de 6 (seis) núcleos físicos e 6 (seis) "threads" ou superior, com frequência base real a 2.2 GHz e cache de 9 MB ou superior. Deverá ainda possuir no mínimo 8GB DDR4 memória RAM e conter capacidade mínima da unidade de armazenamento de 1 (um) Terabyte de disco, com velocidade mínima de 7200 RPM, interface SATA.
- 2.5.63. Deverá ser fornecida com os seguintes Acessórios:
 - a. 1 (um) Teclado USB;
 - b. 1 (um) Mouse óptico USB; e
 - c. 1 (uma) Câmera USB, resolução HD (720p);

Leitor de Cartão de Proximidade e Biometria para Cadastro

- 2.5.64. Deverão ser fornecidos leitores de proximidade de cartões para estações de cadastro.
- 2.5.65. Deverá possuir conexão USB, operar na frequência de 13,56MHz, com interface de comunicação Wiegand e possuir controle dos sinalizadores luminosos (LED bicolor) e sonoro (buzzer).
- 2.5.66. Deverá permitir distância de leitura de no mínimo 5 cm, conter leitor biométrico integrado, compatível com as especificações MINEX e FIPS201 e utilizar tecnologia óptica de alta resolução (500 Dpi), garantindo alto desempenho e segurança superior. O leitor biométrico deverá ainda possuir Taxa de Falsa Rejeição (FRR) e Taxa de Falsa Aceitação (FAR) menores que 0,01%.

Impressora de Cartões com Ribbon

- 2.5.67. Deverá ser disponibilizada, no mínimo, uma impressora para cartões de proximidade com resolução de 300 dpi (pontos por polegada) ou superior, por regional.
- 2.5.68. Deverá realizar a impressão nos cartões utilizando método de sublimação de tinta (transferência térmica) e ser compatível com fitas de impressão YMCKO e YMCKOK.
- 2.5.69. Deverá ser compatível com cartões de PVC de tamanhos CR-80 (85,6 mm x 54 mm) e CR-79 (84,1 mm x 52,4 mm) com espessuras entre 0,3 mm e 1 mm e conter bandeja de alimentação de 100 cartões.
- 2.5.70. Deverá possuir interface USB e Ethernet e alimentação elétrica bivolt.
- 2.5.71. Deverão ser disponibilizadas fitas ribbon, durante a vigência do contrato, com as seguintes características:
 - a. Não poderão ser recondicionadas, remanufaturadas ou recicladas, parcialmente ou totalmente. Deverão ser inteiramente novas, de primeiro uso, inclusive carcaça e todos os seus componentes. As fitas deverão vir lacradas de forma a proteger o material da luz, poeira e umidade e o prazo de validade (mês/ano) deverá constar no rótulo da fita;
 - b. Deverão ser do padrão YMCKO (Y: Yellow M: Magenta C: Ciano K: Preto O: Overlay) ou superior e possuir rendimento de no mínimo 400 cartões;
- 2.5.72. O equipamento deverá ser entregue com todos os itens acessórios de hardware e de software compatíveis com a impressora e necessários à sua perfeita instalação e funcionamento, incluindo cabos, conectores, interfaces, suportes, drivers de controle e programas de configuração.

2.6. Requisitos da Solução de CFTV

- 2.6.1. Deverá ser fornecida solução de CFTV IP que tem como objetivo a captura, detecção e análise de intrusão, do perímetro externo, do movimento de pessoas e veículos que passam pela portaria e área de estacionamento interno, bem como o monitoramento das áreas internas e externas dos ambientes das instalações do Serpro Regional Brasília e Regional São Paulo, tendo como enfoques principais a segurança patrimonial, pessoal e a operação do centro de dados.
- 2.6.2. A solução de Circuito Fechado de Televisão (CFTV) baseada na tecnologia IP deve compreender o fornecimento, instalação, configuração e suporte técnico das câmeras de videomonitoramento IP, servidores de gerenciamento, servidor de armazenamento, estações de monitoramento, infraestrutura completa, serviços de instalação, configuração e capacitação técnica, softwares cliente e servidor, tudo integrado ao Sistema de Controle

de Acesso, e o licenciamento adicional para o sistema de videomonitoramento, com garantia on-site, conforme especificações e condições estabelecidas neste documento.

- 2.6.3. A solução de CFTV deverá funcionar em operação contínua, 24 horas por dia e sete dias por semana.
- 2.6.4. As imagens da solução de CFTV deverão ser geradas com ausência de distorções geométricas ou linearidade.
- 2.6.5. A solução de CFTV deverá possibilitar a gravação local das imagens das câmeras fixas e móveis.
- 2.6.6. A solução de CFTV deverá possibilitar a disponibilização remota de imagens em tempo real e gravadas, de sinais de alarmes e de áudio bidirecional.
- 2.6.7. A solução de CFTV contratada deve trabalhar com sistema de licenciamento por câmeras, permitindo a expansão do sistema com licenças adicionais.
- 2.6.8. A solução de CFTV deve possuir compatibilidade com Caracteres Unicode.
- 2.6.9. Permitir suporte para armazenamento de borda que possibilita gravar vídeo diretamente em um armazenamento como um cartão microSD / SDHC TM *, criando assim um sistema de vigilância por vídeo flexível e confiável.
- 2.6.10. Deverá permitir a tecnologia de redução de largura de banda e armazenamento.
- 2.6.11. Permitir que detalhes importantes na imagem recebam atenção suficiente no fluxo de vídeo, enquanto dados desnecessários podem ser removidos.
- 2.6.12. A solução de CFTV deverá possuir capacidade de armazenamento de pelo menos 30 dias de gravação contínua, a uma taxa mínima de 30 fps (superior H.264) e resolução 1920x1080.
 - 2.6.12.1. Admite-se taxas de fps e resolução menores que os acima especificados para até 30% das câmeras.
- 2.6.13. A solução de CFTV deverá possibilitar que as câmeras sejam alimentadas pelo sistema PoE – Power over Ethernet.
- 2.6.14. A solução de CFTV deverá suportar gravação por detecção de movimento e eventos, sejam estes eventos manuais, de análise de vídeo ou oriundos da integração com o sistema de acesso.

- 2.6.15. O quantitativo, tipo, modelo e posicionamento dos equipamentos componentes da solução de CFTV, tais como câmeras e demais dispositivos, poderão ser revistos no Layout Técnico da Solução.
- 2.6.16. A monitoração e detecção de intrusão dos perímetros das regionais Brasília e São Paulo deverá ser realizada por intermédio de análise inteligente de vídeo e câmeras, podendo ser associada com o emprego de radares ou outros equipamentos, desde que esses sejam integrados à solução de CFTV.
- 2.6.17. O fornecedor deve, sempre que solicitado, realizar o cálculo do espaço em disco necessário para gravação, baseando-se em dados como resolução, quadros por segundo, tempo desejado para armazenar e estimativa de detecção de movimento.

Software de Videomonitoramento (VMS)

- 2.6.18. Deve ser fornecido 01 (uma) licença individual de Software de Videomonitoramento para cada canal (câmera) que compõem o sistema, suportando um número ilimitado de servidor de gravação e visualização de câmeras IP, codificadores de vídeo IP, utilizando métodos como a Universal Plug and Play, Broadcast, varredura manual e varredura por faixa de IP.
- 2.6.19. O sistema de gerenciamento de vídeo deve ser baseado em solução de vídeo IP, que suporta operação de imagens de vídeo, áudio e dados digitais dentro de uma rede IP.
- 2.6.20. Rede e armazenamento otimizados, por multi-streaming, que otimiza a banda usando novos métodos de compressão, superiores ao padrão H.264 (H.265, H.264B, Zipstream, H.264+, H.264H, H.265+ ou similares).
- 2.6.21. A solução de CFTV deverá gerar uma determinada foto da reprodução de vídeo com um descritivo, data e hora do evento ocorrido.
- 2.6.22. O sistema deve operar em forma de matriz digital assegurando chaveamento e controle das câmeras. O sistema deve possuir topologia cliente-servidor, bem como servidores de gravação e estações clientes para operadores. Imagens de vídeo das localidades remotas devem ser acessíveis por diferentes estações de operação simultaneamente. Câmeras, gravadores e estações de visualização podem ser instalados em qualquer ponto dentro da rede.
- 2.6.23. O sistema deve permitir que o operador realize tarefas de recuperação de imagens dos servidores de gravação.
- 2.6.24. O sistema deve ter suporte em Português em todas as operações.
- 2.6.25. O sistema deve permitir criação de grupos com direitos de acesso para câmeras específicas, prioridade de controle das câmeras, direito de exportação de imagens e

acesso aos arquivos de log de eventos. Acessos de visualização, playback, áudio, controle PTZ e de comandos auxiliares devem ser programáveis baseados em câmeras individuais.

- 2.6.26. O sistema deve suportar autorização de logon dual, com seguintes funções:
- a. Criação de usuários de autorização dual.
 - b. Logon em pares de operadores.
 - c. Lista de privilégios e de prioridades em separado designados para cada grupo de acesso dual.
- 2.6.27. Caso um operador dual acesse individualmente, deve receber os privilégios e prioridades atribuídos apenas ao seu respectivo grupo. Se o segundo operador dual acessar o sistema, os operadores receberão todos os privilégios e prioridades previamente definidas.
- 2.6.28. O sistema deverá possuir log de eventos que deverá registrar todas as atividades dos usuários bem como as atividades do próprio sistema.
- 2.6.29. O sistema deve suportar operação (programação, visualização e recuperação) de funções de análise inteligente de vídeo.
- 2.6.30. O sistema deve permitir que estações de operação suportem até 2(dois) monitores, onde podem ser configurados individualmente para visualização de vídeo ao vivo, vídeo recuperado e alarmes.
- 2.6.31. O servidor de operação deve ser capaz de suportar a apresentação de pelo menos 100 imagens de vídeo ao vivo.
- 2.6.32. O sistema deve exportar dados de vídeo e de áudio para CD/DVD, gravador de rede ou USB. Os dados exportados devem incluir todos os metadados associados que permite recuperação dos mesmos vinculados aos eventos de metadados.
- 2.6.33. O sistema deve possuir função auto-discover para os gravadores e câmeras IPs e respectivos endereços IPs, suportando todos os dispositivos em sub-redes diferentes com varredura manual e por faixa de IP.
- 2.6.34. O sistema deve suportar no mínimo 500 câmeras, distribuídas entre 5 subsistemas, operando em rede, ou em forma independente.
- 2.6.35. O sistema deve suportar operação hot-standby, ou seja, mesmo na ausência (quebra) do servidor de vídeo as estações de operação devem manter a configuração sem interrupção de atividades das estações de operação até o retorno do servidor principal.
- 2.6.36. O sistema deve dispor de SDK, permitindo sua integração com sistemas de outros fabricantes.

- 2.6.37. Deve integrar com sistemas de controle de acesso, de maneira bidirecional.
- 2.6.38. Suportar serviços via aparelhos móveis, assegurando transmissão de imagens com função de transcodificação, permitindo acesso de vídeo mesmo com variação da capacidade de rede, limitando a banda mínima de 500 kbps.
- 2.6.39. Dispor de aplicativo em dispositivos baseados em sistema operacional Android (Google) ou iOS (Apple), sem licença adicional, permitindo, no mínimo:
 - a. Visualização de múltiplas imagens simultaneamente.
 - b. Busca e reprodução vídeos gravados.
 - c. Salvamento ou compartilhamento de uma foto do vídeo exibido ao vivo.
- 2.6.40. Interfaces digitais (entradas e saídas), com conexão IP, devem permitir vincular controles de imagens de vídeo de acordo com a programação.
- 2.6.41. O sistema especificado deve tratar os alarmes gerados a partir de interfaces nos servidores de vídeo que foram integrados a rede com o sistema de gerenciamento de vídeo. Além disso, o sistema de gerenciamento deve ser capaz de combinar os alarmes gerados a partir das interfaces de alarmes dos servidores de vídeo com funções lógicas internas para criar novos gatilhos que permitam ao sistema reagir de acordo com um cenário de alarme pré-programado. Temporizadores internos e com os dias da semana, podem ser programados para determinar com precisão exatamente quando os alarmes podem ser ativados.
- 2.6.42. O sistema deve aceitar entradas de eventos de alarmes e então colocá-los em uma pilha de alarmes para ser reconhecido ou a entrada de alarme pode automaticamente disparar uma série de operações no sistema (cenários).
- 2.6.43. O acionamento de entradas de alarme no sistema pode ser causado por qualquer uma das seguintes condições nos servidores remotos de vídeo:
 - a. Contato de entrada.
 - b. Detecção de movimento.
 - c. Perda de sinal de vídeo.
 - d. Perda de resposta dos servidores
 - e. Diversos eventos gerados pelas câmeras
- 2.6.44. O acionamento de entradas de eventos no sistema deve ser capaz de reconhecer placas de veículos, permitindo:
 - a. Cadastrar placas veiculares.
 - b. Registrar e arquivar no banco de dados a imagem da placa, data, hora, número da placa e número de registro da placa (ID placa).

- c. Registrar quando uma placa não for reconhecida, ou quando um carácter estiver em falta, ou quando o índice de qualidade de captura for abaixo do configurado.
 - d. Extrair relatórios dos veículos capturados contendo informações de data, horário e número de placa.
 - e. Analisar placas autorizadas e permitir passagem de veículo, abrindo cancelas de acesso aos estacionamentos, sem a intervenção de um operador.
- 2.6.45. O sistema deve mostrar os logs de alarme dentro de uma janela específica de alarmes, de forma que o operador não necessite procurar as imagens de ocorrência de alarmes.
- 2.6.46. O sistema deve ser capaz de distribuir e replicar os eventos de alarmes para grupos específicos de operadores ou de operador específico.
- 2.6.47. O sistema deve associar workflows com eventos de alarme, em forma de caixas de diálogo e janelas de planos de ação, bem como caixas de resposta de logs.
- 2.6.48. O sistema deve possuir capacidade de forçar um workflow de um alarme, de modo que o alarme não pode ser eliminado até que o respectivo workflow seja cumprido.
- 2.6.49. O sistema deve ter capacidade de enviar mensagens SMS ou de e-mail em resposta à ocorrência de eventos de alarme.
- 2.6.50. O sistema deve ter capacidade, em caso de evento de alarmes, mostrar imagens de vídeo ao vivo, vídeo recuperado, documentos de texto, sitemaps, arquivos HTML ou web sites (URLs).
- 2.6.51. O sistema deve ser capaz de limpar automaticamente os alarmes, quando as condições que originaram eventos não mais existirem.
- 2.6.52. O sistema deve registrar cada evento e alarme numa base de dados SQL. A entrada de alarme deve conter título da câmera que tenha registrado o evento.
- 2.6.53. O sistema deve permitir a busca dos registros pelo operador. E permitir ainda exportação dos resultados localizados numa lista de valores.
- 2.6.54. O sistema deve possuir uma base de dados SQL pronta para uso. O sistema deve ainda, opcionalmente, permitir utilização de base de dados SQL em separado.
- 2.6.55. O sistema deve suportar monitoramento do desempenho que inclui verificação das câmeras, computadores, software.
- 2.6.56. O sistema deve possuir capacidade de gerenciar equipamentos de terceiros através de protocolo SNMP.

- 2.6.57. O sistema deve possuir interface de script de comandos que permite controle das operações em forma programável.
- 2.6.58. O sistema deve possuir um editor para criação de scripts de comando, de forma que operadores executem scripts criados com duplo clique, sobre os ícones dentro da árvore de diretórios ou em site map.
- 2.6.59. O sistema deve permitir execução automática de scripts em resposta aos eventos de sistema, tanto em forma individual quanto em grupo de operadores.
- 2.6.60. O sistema deve possuir servidor de OPC, permitindo integração, quando necessário, com outras plataformas de automação.
- 2.6.61. A interface OPC deve obedecer padrões de alarme e eventos.
- 2.6.62. O sistema deve suportar função de áudio bidirecional de sistemas de intercomunicação, diretamente da estação de operação com os codificadores remotos.
- 2.6.63. O sistema deve dispor de uma árvore lógica de configuração do administrador, a árvore deve ser livremente configurável com qualquer estrutura, com nós de pastas de mapas, e folhas de dispositivos (câmeras, codificadores, etc.), sequências, documentos, URLs ou scripts de comandos. Cada grupo de usuário poderá visualizar apenas itens permitidos pelo administrador.
- 2.6.64. O sistema deve permitir criação de árvores favoritas para cada usuário, personalizando a estrutura de acordo com o usuário.
- 2.6.65. O sistema deve permitir arranjo de imagens em mosaico, de 1 a 25 imagens simultaneamente, em formatos de 1x1, 2x2, 3x3, 4x4 e 5x5 (em monitor padrão 4:3), para monitores de formato 16:9, deverá suportar exibição do mosaico de 1 a 30 imagens em formatos de 1x1, 3x2, 4x3, 5x4 e 6x5. O sistema deve ainda permitir livre configuração no tamanho de cada imagem do mosaico, permitindo melhor visualização para a operação.
- 2.6.66. O sistema deve suportar sobre mapas ou plantas sinópticas com ícones dos dispositivos (câmeras, dispositivos, etc.), inicialização de script de comandos, inicialização de sequência de câmeras, e links para outros mapas. Suportar ainda capacidade de zoom e cujos ícones deve mostrar opcionalmente nomes com títulos dos links.
- 2.6.67. O sistema deve suportar operação com controles de joystick ou mouse, permitindo livre operação dos comandos em giros horizontal, vertical, zoom óptico, íris, foco e comandos auxiliares das câmeras. Deve ainda suportar zoom digital para qualquer imagem através de um controle gráfico na interface do usuário.

- 2.6.68. O sistema deve suportar função de reprodução (playback) instantâneo para uma ou múltiplas imagens, com funcionalidades de pausa, avanço, avanço reverso, avanço quadro, reverso quadro, avança rápido e reverso rápido.
- 2.6.69. O sistema deve suportar barra de tempo permitindo visualização gráfico do tempo, com escala que variam de 15 minutos a 1 mês por divisão, para todas as imagens gravadas.
- 2.6.70. O sistema deve permitir exportação de vídeo sincronizada de câmeras simultâneas.
- 2.6.71. O sistema deve permitir o processo de exportação e reprodução de vídeo simultaneamente.
- 2.6.72. O sistema deve suportar reprodução sincronizada de pelo menos 16 câmeras, com todas as funções de controle simultâneos.
- 2.6.73. O sistema deve suportar função de busca de eventos com pelo menos os seguintes critérios: tamanho do objeto, cor do objeto, bem como eventos de entrar ou sair de áreas designadas.
- 2.6.74. O sistema deve, opcionalmente, mostrar as informações referentes a análise de vídeo, tais como detecção de movimentos, máscaras de objetos e trajetória dos objetos ao vivo e em reprodução.
- 2.6.75. O sistema deve suportar buscas de imagens baseados em qualquer combinação de: tempo, data, tipo de evento, prioridade de alarme, estado de alarme e tipo de dispositivo. Possibilitando ainda salvar e recuperar os parâmetros de busca.
- 2.6.76. O sistema deve permitir mostrar estado dos dispositivos, tanto na estrutura da árvore como nos ícones gráficos, para caso das câmeras devem ser: perda de sinal de vídeo, perda da conexão de rede, gravação de vídeo, sinal de vídeo muito ruidoso, sinal de vídeo com excesso de brilho, sinal de vídeo muito escuro, vídeo desajustado, vídeo associado a áudio e indicação dos estados dos comandos remotos.
- 2.6.77. O sistema deve manter gravado perfil dos usuários para as configurações individuais, as configurações devem incluir pelo menos as seguintes informações: tempo de acesso, tempo com recuperação de imagens, configuração dos monitores (16:9 ou 4:3), servidor em uso, etc.
- 2.6.78. Ajuste automático do tamanho dos arquivos de gravação.
- 2.6.79. O sistema deverá suportar as seguintes opções de segurança:
 - a. Certificados digitais instalados em câmeras para verificação de dispositivos confiáveis.

- b. Conexão segura (criptografada e verificação de origem) entre a câmera e o servidor de vídeo. O controle da câmera, incluindo sinais de PTZ, vídeo, áudio e comandos I/O, devem ser transferidos e criptografados (por meio de encapsulamento HTTPS).
- c. Estabelecer sessões por HTTPS (autorização segura (por SSL / TLS) com certificado confiável instalado na câmera) para proteger os dados do usuário.
- d. Conexões HTTPS seguras entre os servidores de vídeo e as instâncias do *thin client* (web e móvel).
- e. Encapsulamento HTTPS ao recuperar vídeo do armazenamento de borda da câmera.
- f. Assinatura digital do vídeo exportado para comprovar a autenticidade do vídeo. A assinatura digital deve ser feita pelo VMS e deverá possuir formas de validar o vídeo exportado.

Gravação de Vídeo

- 2.6.80. O sistema tem como objetivo gerenciar grupo de gravadores de imagens em rede, permitindo distribuição e alocação dos pacotes de vídeo.
- 2.6.81. O sistema deve suportar ainda operação de gravação e recuperação de metadados vinculados ao vídeo através de banco de dados, cujo aplicativo de análise de vídeo suporte as seguintes características:
 - a. Função de análise inteligente de vídeo integrada às câmeras ~~ou codificadores~~, eliminando a necessidade de PCs dedicados e a manutenção do software associado.
 - b. Deve ser capaz de detectar um objeto estático/removido, a permanência prolongada num determinado local e o cruzamento de linha virtual, previamente programada.
 - c. Deve exibir/detectar trajetórias do objeto, a velocidade, a direção e a cor do mesmo.
 - d. Deve criar metadados para a pesquisa futura nas imagens de vídeos gravados.
 - e. Deve dispor de um assistente de configuração e função de recolhimento de objeto para uma configuração rápida.
 - f. Deve suportar pelo menos 8 critérios de análise por cenário.
 - g. Detectar a entrada, saída ou a simples permanência dos objetos numa determinada área (campo de detector).
 - h. Detectar a permanência prolongada num determinado local, relacionada ao raio e tempo.
 - i. Detectar objetos estáticos num espaço de tempo configurável.
 - j. Detectar objetos removidos num espaço de tempo configurável.
 - k. Detectar trajetórias/percursos dos objetos que circulam na cena, exibidos com linhas de seguimento.
 - l. Detectar o cruzamento múltiplo de linha, de uma até três linhas combinadas numa sequência lógica.
 - m. Detectar propriedades de mudança de condição tais como tamanho, velocidade, direção e a mudança de formato de imagem num espaço de tempo especificado (por exemplo, um objeto em queda).
 - n. Detectar movimentação suspeita de pessoas.

- o. Detectar presença humana.
- p. Detectar formação de multidão.
- q. Contagem de número de pessoas.
- r. Suportar estabilização eletrônica de imagens.
- s. Gestor de script de tarefas de alarme no modo avançado para combinar tarefas de forma lógica.
- t. Distribuir a gravação de vídeo.
- u. Fácil expansão da capacidade de gravação.
- v. Endereçamento inteligente, assegurando o balanceamento dos dados gravados dentro do dispositivo.
- w. Proporcionar a recuperação de dados com a pesquisa de dados e metadados.
- x. Capacidade de auto recuperação dos dados perdidos.
- y. Suportar operação de gravação redundante.
- z. Proteção de falha do grupo de discos, com função de gerenciamento centralizado.

Operar em modo stand-alone.

- 2.6.82. Gerenciar todas as unidades de disco dentro do sistema como uma única massa de gravação.
- 2.6.83. O sistema deve operar em modo automático, neste formato o sistema utiliza automaticamente os recursos de banda e de gravação para melhor distribuir a carga de memória dentro do sistema. Este modo de operação pode ser configurado tanto para gravação redundante quanto para otimização de memória (sem redundância).
- 2.6.84. O sistema deve conter criptografia e opção de senha de proteção para as gravações e arquivos exportados. Não deve ser possibilitada a exportação de vídeo sem criptografia.

2.7. Especificação Técnica dos Equipamentos de CFTV

2.7.1. Características gerais a todas as câmeras:

- a. Deverão possuir alimentação Power over Ethernet.
- b. Deve suportar no mínimo os seguintes protocolos: IPv4, IPv6, UDP, TCP, HTTP, HTTPS, RTP/RTCP, IGMP, ICMP, RTSP, FTP, ARP, DHCP, SNTP, SNMP, 802.1x, DNS, DDNS, SMTP, UPnP (SSDP), DiffServ (QoS).
- c. Deve suportar seguintes criptografias: TLS 1.2, SSL, AES.
- d. Suportar operação com áudio bidirecional.
- e. Suportar envio de alarmes e imagens via rede endereçado ao servidor FTP, deve ainda permitir exportação de vídeo clips ou imagens JPEG.
- f. Os vídeos exportados deverão conter marca d'água com nome da câmera, data e hora.

- g. A câmera deve permitir criptografia para as gravações em armazenamento local (SD/MicroSD card, compact Flash ou USB memory card).
- h. Combinar tarefas usando scripts.
- i. Suportar envio de alarmes de vídeo via e-mail.
- j. Deve possuir proteção por senha.
- k. Deve possuir função de alarme de áudio ambiente.
- l. As câmeras deverão ser fornecidas com as lentes e possuirão as seguintes características técnicas mínimas:
 - o Deverão ter um conjunto de algoritmos avançados que reduzam níveis de ruídos e aumentem o sinal da imagem para exibir cada detalhe na cena da melhor maneira possível.
 - o Prover qualidade de imagem em resolução HDTV 1080p. Sob iluminação fraca, com adaptação automática a exposição da câmera para produzir vídeos de alta qualidade com baixo nível de ruído.
 - o Deverá ter recurso de Exposição Inteligente, permitindo qualidade de vídeo perfeitamente balanceada em cenas com fortes variações de luz.
 - o Deverá permitir a tecnologia WDR, permitindo excelente usabilidade de imagem com pouca luz, podendo transitar facilmente entre o manuseio de WDR e condições de baixa luminosidade.

2.7.2. Características das Câmeras PTZ

- a. Câmera dome externo na forma de uma unidade PTZ.
- b. A caixa de proteção deverá ser de material resistente às intempéries, com índice de proteção IP66.
- c. Deve possuir iluminador infravermelho integrado de no mínimo 150m.
- d. A câmera deverá dispor de, no mínimo, 265 pré-posições, 1 tour definido pelas pré-posições e 2 tours de ronda programada com duração total de 30 minutos.
- e. Configurações e programações da câmera são através de funções (OSD) direto na tela, através de árvore de menu.
- f. Resoluções: 1080p / 720p / d1 / SD.
- g. Possibilitar 60fps para todas as resoluções.
- h. WDR, de pelo menos, 92dB.
- i. Ganho, AGC on/off (30dB max).
- j. Velocidade do obturador, de pelo menos, 1/30s a 1/15.000s.
- k. Lente motorizada de 4,8 a 132mm.
- l. Foco automático com controle manual.
- m. Íris automática com controle manual.
- n. Zoom óptico, de pelo menos, 30x e digital, de pelo menos, 15x.
- o. Campo de visão horizontal de 4° a 55°.
- p. Sensibilidade típica de 0,05 lux (dia) e 0,01 lux (noite) a 30 IRE.

- q. Possuir filtro mecânico para operação dia e noite.
- r. Possuir, pelo menos, três programações para operação em ambientes interno, externo e com reforço para ambientes de grande contraste luminoso.
- s. Possuir pelo menos, 24 máscaras de privacidade com configuração individual e 16 setores independentes com identificação.
- t. Possuir função de equalização de neblina, reforçando visualização do cenário em condições de saturação.
- u. Suportar operação com compressão H.265 em todas as resoluções disponíveis a velocidade de 60 quadros por segundo.
- v. Pan alcance de 0 – 360° contínuo.
- w. Tilt ângulo de 0 – 90°.
- x. Suportar velocidade em Pan de 160°/s.
- y. Suportar velocidade em Tilt de 120°/s.
- z. Possuir 2x entradas de alarme e 1x saída de comando.
- aa. Temperatura de Operação de 0°C a 60°C.

2.7.3. Características das Câmeras Fixas para ambientes externos

- a. Possuir sensor CMOS tipo 1/2.7".
- b. Possuir filtro mecânico de infravermelho, para operação dia e noite.
- c. Deve suportar múltiplos fluxos, com velocidade de 30 quadros por segundo na resolução máxima da câmera.
- d. Deve possuir sensibilidade igual ou inferior no modo colorido a 0,008 lux, no modo monocromático a 0,0009 lux
- e. Deve possuir obturador eletrônico com operação manual e automática de 1/25s a 1/15.000s.
- f. Distância focal de 12-50mm (com filtro de Infravermelho)
- g. Formato 1/1.8".
- h. Campo de visão (sensor de 1/1.8"), aberto: 33 x 19°, fechado: 8,3 x 4,7°.
- i. Temperatura de operação de -10°C a 50°C com 90% de umidade sem condensação.
- j. Ajuste de foco e de zoom.
- k. Deve possuir função de compensação de luz de fundo (BLC).
- l. Deve suportar pelo menos 4 máscaras de privacidade.
- m. Deve suportar áudio bidirecional com padrão G.711, 8 kHz.
- n. Deve suportar a faixa dinâmica (WDR) superior a 110dB.
- o. Deve possuir relação sinal ruído superior a 50dB.
- p. Suporte para cartão de memória SD/SDHC (SDXC) com capacidade mínima de 256GB, assegurando gravação contínua de imagens, mesmo com perda de conexão na rede.
- q. Suportar operação de regiões de interesse dentro da mesma imagem, permitindo gravação de mais detalhes para futura análise.
- r. Pára-sol (sunshield).

- s. Resistente a abertura forçada.
- t. Índice de proteção IP67.

2.7.4. Características das Câmeras Interna Tipo 1

- a. Ser do tipo Dome, possuir sensor CMOS 1/2.8"
- b. Possuir filtro mecânico de infravermelho, para operação dia e noite.
- c. Deve suportar alcance mínimo de 15m com LED (850nm) infravermelho.
- d. Deve suportar múltiplos fluxos em H.265, com velocidade de 30 quadros por segundo na resolução máxima da câmera.
- e. Deve suportar operação com resoluções: 1080p e 720p, ambos com possibilidade de resolução de aspecto 16:9.
- f. Deve possuir lente varifocal automática entre 3,3 mm e 9 mm com foco automático, possibilitando ajustes do ângulo de visualização horizontal entre 34° e 102°.
- g. Deve possuir sensibilidade igual ou inferior no modo colorido a 0,07 lux, no modo monocromático a 0,03 lux e 0,0 lux com IR ligado
- h. Deve possuir obturador eletrônico com operação manual e automática de 1/30s a 1/15.000s.
- i. Deve possuir função de compensação de luz de fundo (BLC).
- j. Deve suportar pelo menos 4 máscaras de privacidade.
- k. Deve suportar áudio bidirecional com padrão G.711, 8 kHz
- l. Deve suportar a faixa dinâmica (WDR) superior a 85dB.
- m. Deve possuir relação sinal ruído superior a 50dB.

2.7.5. Características das Câmeras Internas do Tipo 2

- a. Ser do tipo Dome, possuir sensor CMOS tipo 1/2.8"
- b. Possuir filtro mecânico de infravermelho, para operação dia e noite.
- c. Deve suportar múltiplos fluxos, com velocidade de 30 quadros por segundo na resolução máxima da câmera.
- d. Deve suportar operação com resoluções: 1080p e 720p, ambos com possibilidade de resolução de aspecto 16:9.
- e. Deve possuir lente fixa de 2.8mm, possibilitando ângulo de visualização de pelo menos 105° na Horizontal e 58° na Vertical.
- f. Sensibilidade em modo colorido 0,1 lux, modo monocromático 0,06 lux.
- g. Deve possuir obturador eletrônico com operação manual e automática de 1/30s a 1/15.000s.
- h. Deve possuir função de compensação de luz de fundo (BLC).
- i. Deve suportar pelo menos 4 máscaras de privacidade.
- j. Deve suportar áudio bidirecional com padrão G.711, 8 kHz

- k. Deve suportar a faixa dinâmica (WDR) superior a 85dB.
- l. Deve possuir relação sinal ruído superior a 50dB.
- m. Deve possuir classificação IP66 e IK10.

2.8. Arquitetura e Integrações

Arquitetura Básica

- 2.8.1. A solução deverá funcionar em perfeita integração à Rede Local.
- 2.8.2. A solução deverá suportar comunicação entre os equipamentos de borda (elementos controladores porta, catracas, cancelas) e servidores através de IPv4 e/ou IPv6.
- 2.8.3. Os dados irão transitar pela rede local associados a uma VLAN.
- 2.8.4. A solução deverá permitir que equipamentos de borda se comuniquem com os servidores também através da rede WAN do SERPRO.
- 2.8.5. Quando houver indisponibilidade em um dos sistemas de controle de acesso físico, deverá ser possível realizar toda gestão do acesso físico das regionais a partir do sistema de controle de acesso físico que encontra-se disponível.
- 2.8.6. Todo empregado lotado em uma das unidades, deverá ter seu acesso de primeiro nível automaticamente liberado nas demais unidades.
- 2.8.7. A solução deverá ser dotada de servidores de gerenciamento de controle de acesso, servidores de gerenciamento de CFTV e de gravação de imagens.
- 2.8.8. Os registros das imagens do sistema de CFTV deverão ser armazenadas em storages específicos para este fim, e devem atender uma disponibilidade de 100% para imagens de até 30 dias.
- 2.8.9. Os servidores deverão atender aos requisitos mínimos:
 - a. Ser adequado para instalação em rack padrão 19", com altura máxima de 2U.
 - b. Deve possuir fonte de alimentação redundante e com capacidade de substituição no modo Hot Swap.
 - c. Suportar a substituição de discos rígidos em Hot Swap.
 - d. Deve vir acompanhado de console para monitoração/manutenção.

Integrações

- 2.8.10. Integração com Login Único do SERPRO com autenticação através de SSO (Single Sign-On) compatível com OpenID Connect 1.0 ou SAML 2.0, implementando as recomendações do protocolo OAuth, disponibilizando plenos direitos aos recursos do sistema aos usuários logados via SSO e com possibilidade de uso de SDK/API para adição, remoção, bloqueio e gestão de usuários
- 2.8.11. A solução deverá possibilitar a integração a sistemas terceiros por meio de API Rest e protocolo SNMPv2.
- 2.8.12. A solução deverá oferecer a possibilidade de integração com software de diferentes fabricantes, de forma a flexibilizar o atendimento de necessidades futuras que possam surgir durante a utilização.
- 2.8.13. O sistema de acesso deverá estar integrado ao sistema de cftv permitindo a associação de câmeras de forma a tratar eventos gerados nos equipamentos desejados. Os sistemas devem ser compatíveis para mútua troca de informações.
- 2.8.14. A solução de acesso deverá permitir a integração com os Sistemas de Detecção e Alarme de Incêndios (SDAIs), Notifier e Edwards EST3, hoje instalados no prédio da Regional Brasília, localizado no CPD.
- 2.8.15. A solução deverá priorizar o tratamento de eventos de alta criticidade, tais como eventos de intrusão e/ou alarmes de incêndio.
- 2.8.16. A solução deverá ter um completo gerenciamento de alarmes e eventos, devendo reconhecer alarme de qualquer dispositivo com contato seco ou através de integração.
- 2.8.17. A integração com os referidos sistemas de detecção e alarme de incêndios deve garantir que as portas do ambiente de centro de dados sejam destravadas quando um alarme desses sistemas ocorrer.
- 2.8.18. A solução deve permitir a importação/sincronização dos dados de usuários à medida que forem cadastrados/atualizados na Solução de Gestão de Identidade e Acesso do SERPRO (GIA):
 - a. Deverão ser importados dados do cadastro, no mínimo: nome, foto, matrícula, identidade e lotação.
 - b. O conector entre o GIA será de responsabilidade do fornecedor da solução.
 - c. A solução deverá adicionar automaticamente permissão para passagem pelas catracas das portarias.

2.9. Infraestrutura

- 2.9.1. Por padrão, as câmeras deverão ser alimentadas por meio do recurso de POE. Somente será admitida alimentação de câmeras via fontes individuais, em casos específicos, mediante apresentação de justificativa técnica da Contratada.
- 2.9.2. Toda a infraestrutura predial necessária para perfeita implementação da solução, bem como integrações a outros sistemas, deverão ser realizadas pela contratada, e estarem contemplados nos custos da proposta.
- 2.9.3. A infraestrutura de instalações elétricas e lógicas deverão seguir estritamente as recomendações das normas técnicas vigentes.
- 2.9.4. Os trechos contínuos de tubulação, sem interposição de caixas ou equipamentos, não devem exceder 15 metros para as linhas internas às edificações, se os trechos forem retilíneos. Se os trechos incluírem curvas, o limite de 15 metros deve ser reduzido em 3 metros para cada curva de 90°, portanto faz-se necessário o fornecimento e instalação de caixas de passagem.
- 2.9.5. Deverão ser instaladas as caixas de passagem em todos os pontos da tubulação onde houver entrada ou saída de condutores, exceto nos pontos de transição de uma linha aberta para a linha em eletrodutos e ainda nos pontos de emenda ou de derivação de condutores ou sempre que for necessário segmentar a tubulação.
- 2.9.6. Cabeamento lógico e elétrico deverão ser instalados em infraestruturas distintas.
- 2.9.7. As instalações que forem aparentes ou instaladas em entreforro ou entrepiso deverão ser metálicas e seguir o padrão existente.
 - 2.9.7.1. Para instalações embutidas admite-se tubulações de PVC rígido.

Ponto de Rede Estruturado Categoria 6

- 2.9.8. O cabeamento deverá atender os seguintes requisitos:
 - a. Possuir certificado de performance elétrica (VERIFIED) pela UL ou ETL, conforme especificações da norma ANSI/TIA-568-C.2 CATEGORIA 6.;
 - b. O cabo utilizado deverá possuir certificação Anatel;
 - c. Possuir certificação de canal para 6 conexões por laboratório de 3a. Parte;
 - d. Possuir impresso na capa externa nome do fabricante, marca do produto, e sistema de rastreabilidade que permita identificar a data de fabricação dos cabos;

- e. Capa externa em composto retardante à chama, com baixo nível de emissão de fumaça (LSZH) em conformidade com a norma 60332-3;
- f. Possuir preferencialmente o Selo Verde de Qualidade Ambiental aplicado para cabos de telemática;
- g. Deverá ser apresentado através de catálogos ou proposta técnica de produto do fabricante, testes das principais características elétricas em transmissões de altas velocidades (valores típicos) de ATENUAÇÃO (dB/100m), NEXT (dB), PSNEXT(dB), RL(dB), ACRF(dB), para frequências de 100, 200, 350 e 550Mhz.

2.9.9. Os conectores RJ-45 fêmea devem atender os seguintes requisitos:

- a. Ter corpo em material termoplástico de alto impacto não propagante à chama;
- b. Possuir vias de contato produzidas em bronze fosforoso com camadas de níquel e ouro;
- c. O keystone deve ser compatível para as terminações T568A e T568B, segundo a ANSI/TIA/EIA-568-C.2;
- d. Certificação ETL VERIFIED;
- e. Certificação ETL LISTED ou UL
- f. Suportar ciclos de inserção, na parte frontal, igual ou superior a 750 (setecentas e cinquenta) vezes com conectores RJ-45, 200 inserções com RJ11 e 200 (duzentas) vezes com terminações 110 IDC;
- g. Identificação da Categoria gravado na parte frontal do conector;
- h. Exceder as características elétricas contidas na norma ANSI/TIA/EIA-568-C.2 Categoria 6;
- i. O produto deve cumprir com os requisitos quanto a taxa máxima de compostos que não agredam ao meio ambiente conforme a diretiva RoHS.

2.9.10. Os cordões de conexão utilizados devem possuir os seguintes requisitos:

- a. Possuir no mínimo 1,5 metros;
- b. Certificação Anatel do cabo flexível conforme classe de flamabilidade e do cordão de manobra;
- c. Certificação ETL VERIFIED;
- d. Certificação ETL LISTED ou UL
- e. Deve cumprir com os requisitos quanto à taxa máxima de compostos que não agredam ao meio ambiente conforme a diretiva RoHS;
- f. Deverão ser montados e testados em fábrica, com garantia de performance;
- g. O acessório deve ser confeccionado em cabo par trançado, U/UTP Categoria 6 (Unshielded Twisted Pair), 24 AWG x 4 pares, composto por condutores de cobre flexível, multifilar, isolamento em poliolefina e capa externa em material não propagante a chama tipo LSZH, conectorizados à RJ-45 macho Categoria 6 nas duas extremidades, estes conectores (RJ-45 macho), ter corpo em material termoplástico de alto impacto não

propagante a chama que atenda a norma UL 94 V-0 (flamabilidade), possuir vias de contato produzidas em bronze fosforoso com camadas de níquel e ouro;

2.9.11. Os Patch Panel utilizados deverão possuir os seguintes requisitos:

- a. Ser do tipo descarregado;
- b. Apresenta largura de 19", conforme requisitos da norma ANSI/TIA/EIA-310E;
- c. Deve apresentar uma capacidade de 24 portas numeradas e altura de ½ (meio) U;
- d. Fabricado em aço;
- e. Acabamento em pintura epóxi de alta resistência a riscos na cor preta resistente e protegido contra corrosão;
- f. Compatível com Conectores RJ-45 (Fêmea) Categorias 5e e/ou 6 e/ou 6A UTP;
- g. Deve possuir identificação do fabricante no corpo do produto;
- h. Deve possuir identificação dos conectores na parte frontal do Patch Panel;
- i. O ponto de rede categoria 6 deverá ser fornecido completo, incluindo todos os materiais necessários além de miscelâneas e materiais de identificação;
- j. Para perfeito funcionamento cada ponto de rede categoria 6 deverá ser composto por: até 90 (noventa) metros de cabo U/UTP, 02 (dois) conectores RJ-45 fêmea, 02 (dois) cordões de conexão e por 01 (uma) porta de patch panel, miscelâneas e material para identificação.

Ponto de Energia Elétrica

2.9.12. O cabeamento elétrico deverá atender os seguintes requisitos::

- a. Possuir 03 condutores (fios) de cobre eletrolítico nu, têmpera mole, flexível classe 5, conforme NBR NM 280;
- b. Condutores preferencialmente nas cores do padrão existente;
- c. Isolação: Composto termofixo (HEPR) – 90°C. Capa Interna: Composto termoplástico (PVC) antichama – 90°C
- d. Temperatura de operação em regime permanente de 90° C em sobrecarga 100°C;
- e. Normas de Referência: NBR 7288, ABNT NBR NM 280;
- f. Seção mínima de 2,5 mm².

2.9.13. O ponto de rede elétrica deverá ser fornecido completo, incluindo todos os materiais necessários além de miscelâneas e materiais de identificação;

2.9.14. O ponto de rede elétrica deverá derivar de um quadro elétrico ou ponto elétrico já existente no ambiente de instalação, indicado pelo Serpro. Caso o quadro elétrico disponibilizado não possua disjuntor reserva o mesmo deverá ser fornecido pela

contratada. A contratada deverá analisar a possibilidade da derivação do ponto elétrico de modo a evitar sobrecarga das instalações existentes;

- 2.9.15. Toda rede elétrica deverá ser proveniente de rede ininterrupta de energia, por meio de nobreaks do Serpro.
- 2.9.16. A tensão elétrica disponibilizada deverá ser adequada ao local de instalação indicado pelo Serpro.

2.10. Implantação da Solução

- 2.10.1. A vistoria é facultativa nas dependências da Regional Brasília e de São Paulo para dirimir dúvidas, caso haja, em relação à solução a ser fornecida. Esta visita tem por objetivo promover o perfeito entendimento e dimensionamento da solução, onde a empresa poderá proceder ao levantamento dos quantitativos a serem orçados, e que serão de sua exclusiva responsabilidade.
- 2.10.2. Os serviços de implantação se dividirão em quatro etapas:
 - A. Layout Técnico da Solução.
 - B. Instalação/Configuração de equipamentos, softwares e materiais.
 - C. Testes e Homologação
 - D. Treinamento da Solução.

Layout Técnico

- 2.10.3. A primeira etapa da fase de implantação é o desenvolvimento do layout técnico da solução.
- 2.10.4. A instalação dos equipamentos, softwares e materiais está vinculada à aprovação do Layout Técnico, que compreende o desenvolvimento de projeto técnico de alocação dos equipamentos. O layout técnico deverá ser entregue em mídia impressa e digital e deverá ser desenvolvido em formato CAD (computer aided design). O projeto deverá contemplar o projeto de cabeamento estruturado, Videomonitoramento e Controle de Acesso.

Instalação e Configuração dos Equipamentos

- 2.10.5. Após a etapa de layout técnico, mediante aprovação da contratante, a contratada deverá iniciar toda a infraestrutura necessária para implantação, tais como passagem de circuitos elétricos e lógicos, rasgos em alvenarias, instalação de bases para tótems, e etc.
- 2.10.6. Todas as intervenções civis necessárias são por conta da contratada, que deverá recompor todas as áreas afetadas ao seu estado original.

- 2.10.7. A fase de implantação da infraestrutura física, abrange, entre outros, os seguintes serviços:
- a. Instalação de Infraestruturas físicas internas e externas.
 - b. Serviço de instalação do ponto de rede:
 - c. Lançamento de cabo UTP Cat.6 do ponto de concentração (rack principal) até o ponto de instalação do equipamento remoto.
 - d. Conectorização de cabos de rede.
 - e. Instalação física de Patch Panel seguindo padrões previamente definidos.
 - f. Testes e certificações de cabeamento de acordo com as normas internacionais EIA/TIA 568-B e normas complementares.
 - g. Identificação dos componentes do cabeamento (cabo, espelhos e painéis) com etiqueta adesiva.
 - h. Todos os pontos fornecidos com todos os acessórios para fixação e identificação, tais como: velcro para amarração, etiquetas, etc.
- 2.10.8. Ficará sob responsabilidade da empresa instaladora, a limpeza do local de trabalho, bem como todo e qualquer acabamento necessário.
- 2.10.9. Todos os enlaces devem ser certificados e o relatório desta certificação deve constar da documentação da implantação.
- 2.10.10. É dever da Contratada toda recomposição civil de intervenções realizadas durante a instalação de infraestruturas internas ou externas. Deverá prever ainda a recomposição de fachadas, paredes, pinturas, gesso, grama, calçadas, pisos e outros.
- 2.10.11. Findada a implantação da infraestrutura física, inicia-se a etapa de instalação e configuração dos equipamentos e sistemas, que compreende:
- a. Instalação física do equipamento e de materiais em ambiente designado em projeto técnico.
 - b. Configuração de todos os softwares, conforme melhores práticas adotadas pelos fabricantes.
 - c. Integração dos Sistemas de Videomonitoramento e Controle de Acesso IP, conforme requisitos exigidos.
- 2.10.12. A implantação da solução engloba ainda a execução de todas as integrações necessárias para o perfeito funcionamento dos sistemas, bem como o cadastro dos dados dos usuários no sistema de controle de acesso (biometria, facial, etc.), configuração de zonas de detecção e de analíticos de vídeo do CFTV, dentre outros.
- 2.10.13. Deverá prever a identificação física dos equipamentos/instalações e documentação técnica em língua portuguesa, conforme layout projetado da solução.

- 2.10.14. Inclusão dos dados de configuração de todos os sistemas/equipamentos na documentação AS-Built depois de instalados.
- 2.10.15. Os serviços serão considerados terminados somente após a entrega, pela CONTRATADA, da documentação "As Built", da lista completa dos equipamentos instalados, dos catálogos e manuais de instalação, manutenção e operação dos fabricantes de todos equipamentos, dispositivos, acessórios, e componentes instalados.
- 2.10.16. Todos os serviços deverão seguir e estar em completo acordo com as normas e recomendações competentes, ainda que não especificados neste termo, nas versões vigentes quando da apresentação das propostas.

Testes e Homologação

- 2.10.17. Será considerada implantada a solução somente após a etapa de testes e homologação.
- 2.10.18. Nesta etapa a Contratada deverá demonstrar o atendimento a todos os requisitos deste documento, devendo estes estarem disponibilizados e operacionais.

Repassé de Conhecimento

- 2.10.19. A CONTRATADA deverá realizar repasse de conhecimento, inerente à instalação, administração e ao uso da solução, conforme descrito a seguir:
 - 2.10.19.1. A CONTRATADA deverá providenciar os repasses de conhecimentos durante a vigência do contrato, sem ônus para o SERPRO, que serão realizados na localidade de Brasília/DF e São Paulo/SP na modalidade presencial ou na modalidade remota com carga horária 40h, 2 turmas com até 15 empregados cada, considerando:
 - 2.10.19.1.1. Sustentação e administração da solução, que deverá abordar, pelo menos, os seguintes tópicos:
 - a. Configuração – melhores práticas.
 - b. Configuração e operação básica – comandos básicos.
 - c. Conceitos básicos e avançados como: busca forense, cadastramento, operação, PTZ.
 - 2.10.19.2. O repasse de conhecimento na modalidade presencial deve seguir as orientações do Ministério da Saúde e da Organização Mundial da Saúde – OMS quanto às medidas de prevenção e redução dos riscos de contágio pelo Coronavírus – Covid-19.
 - 2.10.19.3. A data de início do repasse de conhecimento será definida pelo SERPRO de acordo com suas necessidades observando o cronograma e requisitos do plano de implantação da ferramenta.

- 2.10.19.3.1. O SERPRO deverá comunicar formalmente à CONTRATADA a data de início do repasse de conhecimento com uma antecedência mínima de 10 (dez) dias corridos.
- 2.10.19.4. A CONTRATADA deverá entregar ao SERPRO em até 30 (trinta) dias corridos após o início da vigência do Contrato, a ementa, no idioma português do Brasil, contendo: Nome do repasse de conhecimento, carga horária, objetivo, pré-requisitos, conteúdo programático bem como o material do repasse.
- 2.10.19.5. O repasse deverá ser ministrado por profissional(ais) certificado(s) e/ou autorizado(s) pelo fabricante da Ferramenta de Desempenho Profissional ofertada, com a devida comprovação, constando nome completo e CPF de cada profissional que ministrará.
- 2.10.19.6. A CONTRATADA deverá apresentar em até 5 (cinco) dias após o início da vigência do contrato, o(s) certificado(s) solicitado(s) bem como declaração de que a empresa está autorizada pelo fabricante a prestar o repasse.
- 2.10.19.7. A CONTRATADA deverá prover toda a logística e todo o material didático necessário à execução do repasse de conhecimento teórico e prático, com manuais e apostilas, entre outros.
- 2.10.19.8. O repasse de conhecimento deverá ser realizado utilizando conteúdo teórico e prático, disponibilizando a ferramenta ofertada, onde estarão disponíveis as mesmas funcionalidades das especificações técnicas.
- 2.10.19.9. Todas as despesas com material, equipamentos, instrutores, deslocamento de instrutores e demais itens serão de responsabilidade da CONTRATADA.
- 2.10.19.10. Após o repasse de conhecimento a CONTRATADA deverá emitir certificado para cada participante, obedecendo ao critério de frequência de 80% (oitenta por cento) para os repasses de conhecimentos com carga horária de 20hs e com carga horária de 40hs.
- 2.10.19.11. O certificado deverá conter as seguintes informações: Nome completo do participante, Nome responsável do repasse de conhecimento, Período de Realização, Carga Horária e Conteúdo Programático.
- 2.10.19.12. O (s) certificado (s) deverá (ão) ser encaminhado (s) ao responsável pela área do SERPRO na localidade onde ocorreu do repasse de conhecimento em até 10 (dez) dias corridos após o término.

- 2.10.19.13. Ao final do repasse de conhecimento, o SERPRO, por meio de formulário específico fará a avaliação do repasse ministrado, para emissão de termo de aceite, a qual a Contratada deverá obter a média de 70% de conceitos "bom e/ou ótimo".
- 2.10.19.14. Caso não atinja o conceito mencionado no subitem acima, o SERPRO encaminhará um relatório à Contratada informando o que deverá ser adequado para a realização de um novo repasse.
- 2.10.19.14.1. A CONTRATADA deverá encaminhar ao SERPRO as alterações para análise e aprovação.
- 2.10.19.14.2. Se aprovado, o prazo do novo repasse de conhecimento deverá estar de acordado com a equipe do SERPRO.
- 2.10.19.15. A CONTRATADA deverá disponibilizar ao SERPRO o conteúdo para repasse em formato web HTML5, que seja compatível com o ambiente virtual de aprendizagem Moodle (versão 3.10 ou superior) e que contenha todos os objetos multimídias utilizados como vídeos, áudios e imagens.
- 2.10.19.16. A Contratada deverá providenciar a assinatura dos termos de cessão de imagem e voz, nos modelos fornecidos pelo SERPRO, a fim de resguardar tanto o SERPRO quanto a própria contratada quanto a quaisquer riscos jurídicos quanto à essa matéria.
- 2.10.19.17. A Contratada deverá se responsabilizar por todos os ativos digitais utilizados na produção do conteúdo do repasse, garantindo o cumprimento da legislação vigente no que diz respeito a direitos autorais e de cessão de imagem.
- 2.10.19.18. Ao final o SERPRO emitirá a Declaração de Aceite se a CONTRATADA atender todos os requisitos.

2.11. Cronograma

2.11.1 A Contratada deverá observar os prazos estabelecidos para implantação conforme quadro abaixo:

| Etapas | Objeto | Prazos |
|--|---|--|
| 1 | Layout Técnico da Solução | Até 15 (quinze) dias após a assinatura do contrato. |
| 2 | Elaboração de Cronograma/Planejamento de entrega e execução | Até 05 (cinco) dias após a aprovação do layout pelo Serpro. |
| 3 | Execução do Serviço de Infraestrutura | Até 45 (quarenta e cinco dias) após a aprovação do cronograma. |
| 4 | Entrega e Instalação dos Equipamentos | Até 45 (quarenta e cinco dias) após a aprovação do layout técnico. |
| 5 | Teste de Aceite e Homologação da Solução | Até 20 (vinte) dias após a execução do serviço de instalação. |
| 6 | Repasse de conhecimento | Até 20 (vinte) dias após a execução dos testes e homologação |
| Prazo total estimado para a Implantação da solução em cada localidade | | 120 (cento e vinte) dias |

2.11.2 O Serpro terá 5 (cinco) dias úteis para aprovar cada etapa.

2.12. Qualidade e Resultados Esperados

SUPORTE TÉCNICO E MANUTENÇÃO

2.12.1. A Contratada deverá disponibilizar os seguintes tipos de atendimento:

- a. Nível I - Atendimento Telefônico e por sistema de abertura de chamado via internet (Help Desk): chamados abertos através de ligação telefônica ou sistema de abertura de chamado via Internet. Esse serviço deve atender demandas dos usuários referentes ao funcionamento da solução, que decorram de problemas de funcionamento.
- b. Nível II - Atendimento Remoto: atendimento remoto de chamados de suporte técnico através de tecnologia disponibilizada pela CONTRATANTE, mediante prévia autorização e seguindo os padrões de segurança da CONTRATANTE, objetivando análise e solução remota dos problemas apresentados.
- c. Nível III - Atendimento Presencial (On-Site): atendimentos técnicos realizados nas dependências do CONTRATANTE, através de visita de técnico especializado, com a finalidade de resolver demandas abertas no Help Desk e não solucionadas pelo Atendimento Telefônico e/ou Remoto.

2.12.2. O suporte técnico deverá prestar manutenções preventivas e corretivas.

2.12.3. A manutenção corretiva possui causas em falhas e erros no Software/Hardware e trata da correção dos problemas atuais e não iminentes de fabricação dos mesmos. Esta manutenção inclui os procedimentos destinados a recolocar em perfeito estado de operação os serviços e produtos ofertados, tais como:

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

2.12.3.1. Quanto às atualizações pertinentes aos softwares: entende-se como “atualização” o provimento de toda e qualquer evolução de software, incluindo correções, “patches”, “fixes”, “updates”, “service packs”, novas “releases”, “versions”, “builds”, “upgrades”, englobando inclusive versões não sucessivas.

2.12.3.2. Quando das alterações corretivas que forem necessárias ao perfeito funcionamento dos softwares (bug, fixing e patches), entrarem em módulo de manutenção, deverão

ser efetuados todos os procedimentos para estabilização das licenças instaladas até a total normalização da produção.

2.12.3.3. A CONTRATADA fornecerá e aplicará pacotes de correção, em data e horário a serem definidos pela CONTRATANTE, sempre que forem encontradas falhas de laboratório (bugs) ou falhas comprovadas de segurança em software ou firmware dos aparelhos que integrem o objeto do contrato.

2.12.3.3.1. O atendimento deste requisito está condicionado à liberação pelo fabricante dos pacotes de correção e/ou novas versões de software.

2.12.4. A Manutenção preventiva destina-se a manter os softwares e os hardwares em sua plena condição de funcionamento e desempenho, prevenindo a ocorrência de quebras e defeitos.

2.12.5. Qualquer manutenção preventiva realizada pela contratada deverá ser previamente comunicada à contratante. Em caso de paradas dos sistemas, os horários para as intervenções devem ser previamente combinados.

RELATÓRIOS

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

- a. Listagem das intervenções registradas (MP/MPD, MC e OP) por equipamento/instalação;
- b. Total de horas gastas por tipo de intervenção (MP/MPD, MC e OP) e tipo de equipamento/instalação;
- c. Informar data do registro de acesso e de vídeo mais antigo armazenado no sistemas, bem como o espaço disponível em disco;

2.12.6.1. O relatório deverá ser entregue juntamente à Nota Fiscal e é condição para a emissão do recebimento definitivo, e respectivo pagamento.

2.12.7. A CONTRATADA deverá, ainda, fornecer Relatório Técnico específico para cada MC, de severidade Crítica, que acarretar indisponibilidade em qualquer sistema, contendo, no mínimo:

- a. Descrição detalhada, com registros da ocorrência;
- b. Causa da ocorrência, com laudo técnico do fabricante/credenciado (se necessário);
- c. Histórico das rotinas de MP/MPD realizadas pertinentes à MC em questão;
- d. Solução definitiva aplicada;
- e. Assinatura(s) do(s) Responsável(is) Técnico(s) da CONTRATADA.

2.12.7.1. Este relatório deve ser entregue até o 5º (quinto) dia útil após o registro do incidente que gerou a manutenção corretiva.

3. Níveis de serviço e Sancionamentos

3.1. Possuir suporte técnico para todos os itens contratados e descritos (MP, MPD, MC E OP), bem como para os demais acessórios integrantes da proposta, 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana, à exceção dos chamados de Severidade 5, que 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:

- **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.
- **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.
- **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.
- **OPERAÇÃO (OP):** é toda a operacionalização de equipamentos e instalações (periódicas ou não) com o intuito de mantê-los em funcionamento ou simplesmente o acompanhamento durante a operação/manutenção destes.

3.2. O atendimento aos chamados deverá obedecer à seguinte classificação quanto ao nível de severidade:

| SEVERIDADE | DESCRIÇÃO | IMPACTO | TEMPO DE ATENDIMENTO IN LOCO (minutos) | TEMPO DE RESOLUÇÃO PARA SOLUÇÃO DEFINITIVA OU PALIATIVA (horas) | PENALIDADE |
|-------------|--|-----------|--|---|--|
| 1 - Crítica | Chamados referentes a situações de emergência ou problema crítico, caracterizado | Altíssimo | No máximo 2 (duas) horas após a abertura do chamado. | No máximo 04 (duas) horas após o início do atendimento. | Aplicação de multa à CONTRATADA de 5% do valor mensal do sistema impactado (CFTV ou Controle de Acesso), por |

| | | | | | |
|----------------|--|------------|---|---|--|
| | pela existência de ambiente paralisado (indisponibilidade na solução de acesso ou CFTV). | | | | evento de parada do serviço, independente do prazo de solução, e 1% (um por cento) do valor mensal contratado do sistema impactado (CFTV ou Controle de Acesso), por hora ou fração de hora de atraso em relação aos prazos estabelecidos. |
| 2 – Muito Alta | Chamados associados a situações de alto impacto com indisponibilidade de equipamentos ou funcionalidade da solução que afete o DATACENTER, incluindo os casos de degradação severa de desempenho | Muito Alto | No máximo 04 (quatro) horas após a abertura do chamado. | No máximo 08 (oito) horas após o início do atendimento. | O não atendimento dentro dos prazos estabelecidos para o chamado ensejará aplicação de multa à CONTRATADA de 3% (três por cento) do valor mensal contratado do sistema impactado (CFTV ou Controle de Acesso), por hora ou fração de hora de atraso em relação aos prazos estabelecidos. |
| 3 - Alta | Chamados associados a situações de alto impacto com indisponibilidade de equipamentos ou funcionalidade | Alto | No máximo 06 (seis) horas após a abertura do chamado. | No máximo 12 (doze) horas após o início do atendimento. | O não atendimento dentro dos prazos estabelecidos para o chamado ensejará aplicação de multa à CONTRATADA de 2% (dois por cento) do valor mensal |

| | | | | | |
|-----------|---|-------|---|---|--|
| | <p>e da solução que NÃO afete o DATACENTER, incluindo os casos de degradação severa de desempenho.</p> <p>Ou</p> <p>Casos de intermitência ou baixo desempenho de equipamentos que afete o DATACENTER</p> | | | | contratado do sistema impactado (CFTV ou Controle de Acesso), por hora ou fração de hora de atraso em relação aos prazos estabelecidos. |
| 4 - Média | Chamados referentes a situações de baixo impacto com baixo desempenho, ou para aqueles problemas que se apresentem de forma intermitente | Médio | No máximo 06 (seis) horas após a abertura do chamado. | No máximo 24 (vinte e quatro) horas após o início do atendimento. | O não atendimento dentro dos prazos estabelecidos para o chamado ensejará aplicação de multa à CONTRATADA de 1% (um por cento) do valor mensal contratado do sistema impactado (CFTV ou Controle de Acesso), por hora ou fração de hora de atraso em relação aos prazos estabelecidos. |
| 5 - Baixa | Chamados com objetivo de sanar dúvidas | Baixo | Não se aplica. | No máximo 96 (noventa e seis) horas após a | O não atendimento dentro dos prazos estabelecidos para |

| | | | | | |
|--|--|--|--|----------------------|---|
| | quanto ao uso, monitoração e outros aspectos da solução, instalação de novas versões ou atualizações e patches | | | abertura do chamado. | o chamado ensejará aplicação de multa à CONTRATADA de 0,5% (cinco décimos por cento) do valor mensal contratado do sistema impactado (CFTV ou Controle de Acesso), por hora ou fração de hora de atraso em relação aos prazos estabelecidos. |
|--|--|--|--|----------------------|---|

3.2.1 As penalidades decorrentes do não atendimento dos prazos supramencionados limitar-se-ão a **15%** do valor mensal contratado, sem prejuízo de outras iniciativas do Serpro para aplicação de sanções previstas no instrumento contratual.

3.3. Caso a solução aplicada seja paliativa e acatada pelo Serpro, a CONTRATADA deverá entregar em até 2 (dois) dias úteis um cronograma para execução da solução definitiva.

3.3.1. Caso esse cronograma não seja aceito pelo Serpro, o fornecedor terá 1 (um) dia útil para apresentar um novo cronograma.

3.3.2. Terminado o prazo da resolução paliativa, e não implementada a solução definitiva, inicia-se a contagem do tempo de atraso para fins de penalidade, de acordo com o nível de severidade.

3.3.3. Caso ocorra um novo incidente decorrente da solução paliativa, será aberto um novo chamado, para o qual os prazos devem ser adequados à sua severidade, não sendo mais aceita nenhuma outra solução paliativa neste caso.

3.3.4 A severidade do chamado poderá ser reavaliada quando verificado, pela fiscalização do Serpro, que a mesma foi erroneamente aplicada, passando a contar no momento da reavaliação dos novos prazos de atendimento e solução.

3.3.5 Sempre que ficar provado que a causa de determinada falha ou inoperância seja fruto de falha de elemento de hardware e/ou software não fornecido pela CONTRATADA, ficam suspensos todos os prazos de atendimento até que a CONTRATANTE resolva os problemas externos que provocam a inoperância da solução. Após a CONTRATANTE disponibilizar o ambiente de forma estável para a reativação da solução, a CONTRATADA

realizará avaliação da extensão do dano e da solução, e as partes definirão em comum acordo o prazo para a reativação da solução.

3.3.6 A CONTRATADA poderá solicitar a prorrogação de qualquer dos prazos para conclusão de atendimentos de chamados, desde que o faça antes do seu vencimento e devidamente justificado.

3.4. Canais de atendimento:

3.4.1. O atendimento e os chamados técnicos deverão ser realizados por meio de canal telefônico gratuito 0800 e/ou tarifação reversa, e/ou site na Internet, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana;

3.4.2. Os chamados técnicos poderão ser realizados e registrados por meio de software de gestão de manutenção, a ser disponibilizado pelo Serpro;

3.5. Correrá por conta exclusiva da CONTRATADA a responsabilidade pelo deslocamento, alimentação e estadia do seu técnico ao/no 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.

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

3.5.2. 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.

3.6. Monitoramento do atendimento dos chamados:

3.6.1. Os chamados poderão ser controlados pelo sistema de informação da CONTRATADA ou por sistema de gestão disponibilizado pelo Serpro, à critério da fiscalização técnica do Contratante.

3.6.2. O fechamento do chamado poderá se dar tanto pela aplicação de correção ao produto quanto pela aplicação de solução paliativa que possibilite a operação do sistema.

3.6.3 Antes do fechamento de cada chamado, a CONTRATADA consultará o SERPRO para validar o fechamento do chamado.

3.6.4. Um chamado fechado, sem anuência do SERPRO 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 aplicação das sanções previstas.

3.6.5. A CONTRATADA manterá cadastro das pessoas indicadas pelo SERPRO que poderão efetuar abertura e autorizar fechamento de chamados.

3.7. Instrumento de Medição de Resultados (IMR)

3.7.1. O IMR é o mecanismo que define os níveis esperados de qualidade da prestação dos serviços rotineiros e respectivas adequações de pagamento para os casos de descumprimento. O anexo denominado ANEXO 2 ("IMR Acesso e CFTV")

3.7.2. O desempenho da CONTRATADA na execução dos serviços rotineiros será medido através do Indicador de Resultado de Serviço (IRS), conforme detalhado no Anexo 3("Formulário de Inspeção IMR")

3.7.3. O IMR apura níveis de serviços diferentes dos casos descritos no item relativo às manutenções corretivas.

4. Especificação de Valores e Forma de Pagamento

4.1 O valor global estimado para a contratação da solução integrada de controle de acesso e CFTV (IP) para as Regionais Brasília e São Paulo do SERPRO, na modalidade serviço, conforme descrito a seguir:

| Grupo | Itens | Descrição | Localidade | Métrica | Qtd. | Valor Mensal (R\$) | Valor Anual (R\$) | Valor 48 Meses (R\$) |
|-------------|-------|----------------------------|------------|---------|------|--------------------|-------------------|----------------------|
| 1 | 1 | Solução Controle de Acesso | Brasília | Serviço | 1 | R\$ 0,00 | R\$ 0,00 | R\$ 0,00 |
| | | | São Paulo | | | R\$ 0,00 | R\$ 0,00 | R\$ 0,00 |
| | 2 | Solução CFTV IP | Brasília | Serviço | 1 | R\$ 0,00 | R\$ 0,00 | R\$ 0,00 |
| | | | São Paulo | | | R\$ 0,00 | R\$ 0,00 | R\$ 0,00 |
| Total Geral | | | | | | R\$ 0,00 | R\$ 0,00 | R\$ 0,00 |

4.2. Forma e condições de pagamento.

4.2.1 O pagamento pelos serviços prestados só serão iniciados após a implantação e o funcionamento dos sistemas, podendo este ser proporcional aos sistemas já implantados e em funcionamento.

4.2.2. Os pagamentos serão efetuados mensalmente, no 1º (primeiro) dia útil, após o 30º (trigésimo) dia corrido, a contar da data de emissão do Recebimento Definitivo, nos locais indicados nas respectivas notas fiscais entregues no Protocolo Geral do SERPRO ou através do endereço eletrônico a ser informado pelo Gestor do Contrato.

4.2.2.1. No primeiro mês de faturamento, o valor deverá ser rateado à base de 1/30 (um trinta avos) do valor da contraprestação mensal, por dia, considerando-se o mês de 30 dias.

4.2.2.2. Nos meses subsequentes, os serviços serão cobrados mensalmente, considerando-se o mês de 30 (trinta) dias.

4.2.3. O prazo para emissão do recebimento definitivo por parte do SERPRO é de 10 (dez) dias corridos a partir do recebimento da nota fiscal e/ou fatura.

5. Da Vistoria

5.1 O fornecedor interessado tenha necessidade de realizar visita in loco, o agendamento deverá ser realizado das 9h00 às 17h00, de segunda a sexta feira.

5.1.1 A visita in loco não é condição obrigatória, sendo opcional a apresentação de Termo de Vistoria. Esta visita tem por objetivo promover o perfeito entendimento e dimensionamento da solução, onde a LICITANTE poderá proceder ao levantamento dos quantitativos a serem orçados, e que serão de sua exclusiva responsabilidade.

5.1.2 A visita poderá ser realizada pelo representante legal, a seu critério ou conveniência, comprovado por meio de documentação.

5.1.3 A vistoria e os elementos técnicos fornecidos são suficientes para os levantamentos necessários à elaboração da proposta, bem como o desenvolvimento dos trabalhos a serem realizados, de modo a não incorrer em omissões. Não serão aceitas reclamações posteriores, sob alegação de desconhecimento das condições locais, aumento no escopo da presente contratação.

5.1.4 Será disponibilizado aos fornecedores interessados os layouts e as plantas das edificações da Regional Brasília e São Paulo somente mediante assinatura eletrônica do Termo de Confidencialidade e Sigilo.

6. Da Seleção do Fornecedor

6.1 A HABILITAÇÃO, em complemento às condições já estabelecidas na Seção Da Habilitação do edital padrão, deverá(ão) ser exigida(s) dos licitantes, a(s) seguinte(s) informação(ões):

a) Registro ou prova de inscrição válido(a) da pessoa jurídica licitante e dos Responsáveis Técnicos no CREA (Conselho Regional de Engenharia e Agronomia);

a.1) Caso a certidão ou registro da pessoa jurídica e dos Responsáveis Técnicos seja emitida em CREA diferente do Estado de execução, em sendo vencedora do certame, deverá providenciar o visto no conselho local, até 30 dias após a assinatura do contrato.

b) Atestado(s) de Capacidade Técnica – ACT, fornecido por pessoa jurídica de direito público ou privado, que comprove ter a empresa licitante, desempenhado de forma satisfatória atividade compatível em características e quantidades de acordo com o objeto da contratação;

b.1) O(s) atestado(s) deverá(ão) ser emitido(s) em papel timbrado, contendo razão social, endereço, CNPJ, e-mail e telefone da pessoa jurídica que o emitiu, além da identificação (nome e função) do declarante. Caso estes requisitos não sejam atendidos, impossibilitando ao SERPRO efetuar diligência que julgar necessária, os atestados não serão considerados;

b.2) O(s) atestado(s) deverá(ão) referir-se a serviços prestados no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente;

b.3) Para fins de compatibilidade será(ão) considerado(s) o(s) atestado(s) / certidão(ões) / declaração(ões) que comprove(m) a prestação de serviços de Controle de Acesso e CFTV., com a(s) seguinte(s) característica(s) mínimas:

- Mínimo de XX pontos de câmeras de CFTV
- Mínimo de YY pontos de controle de acesso

b.4) A licitante poderá apresentar mais de um ACT, desde que os períodos informados demonstrem concomitância de execução dos serviços por sistema.

c) Certidão de Acervo Técnico – CAT, emitida pelo CREA, que comprove ter o(s) Responsável(is) Técnico(s), desempenhado de forma satisfatória atividade compatível em características e quantidades de acordo com o objeto desta licitação.

c.1) O(s) Responsável(is) Técnico(s) deverá(ão) possuir o(s) seguinte(s) título(s) profissional(is): Engenheiro Eletricista, Eletrônica e/ou afins.

c.2) A(s) CAT(s) deverá(ão) apresentar a mesma compatibilidade definida na alínea “b.3”.

c.3) A licitante poderá apresentar mais de uma CAT, desde que os períodos informados demonstrem concomitância de execução dos serviços por grupo.

d) Comprovante de que o(s) Responsável(is) Técnico(s) integra(m) o quadro permanente da LICITANTE. A comprovação será feita mediante a apresentação dos seguintes documentos, conforme o caso:

I. Apresentação de Carteira de Trabalho (CTPS) e/ou GFIP (Guia de Recolhimento do FGTS e Informações à Previdência Social), comprovando o vínculo empregatício do profissional, na empresa licitante na data da licitação, ou;

II. Apresentação do contrato social ou outro documento legal, devidamente registrado na Junta Comercial, no caso de ser sócio proprietário da empresa licitante, ou;

III. Apresentação de Registro do Profissional junto ao CREA da Empresa, ou;

IV. Declaração de contratação futura do profissional, com a anuência deste, ou;

V. Contrato de prestação de serviços, sem vínculo trabalhista e regido pela legislação civil comum.