

ANEXO IV

Projeto Básico do Sistema de Controle de
Acesso e Circulação em implantação

Projeto Básico
para Instalação de Solução de Segurança Eletrônica
nos Edifícios Sede e Assis Brasil
do TRE-RS



Versão – 3.0
Emissão: 28/08/2019
Projeto baseado nas práticas do PMI
(*Project Management Institute*)

Informações do Documento:

Nome do Projeto:	Projeto Básico (Sistema de Segurança Eletrônica)				
Preparado por:	Eng. Alcides Barbosa	Nº da Versão:	03	Data da Versão:	28/08/2019

Histórico da Versão:

Nº da Versão:	Data Versão:	Preparado por:
1	29/07/2019	Eng. Alcides Barbosa
2	15/08/2019	Eng. Alcides Barbosa
3	28/08/2019	Eng. Alcides Barbosa

Resumo do Projeto:

Gerente do Projeto	Alberto Rafael Moreira Ferreira
Patrocinador do Projeto	Tribunal Regional Eleitoral do Rio Grande do Sul
Metas e Objetivos	Implantação de sistema de CFTV (Circuito Fechado de TV) e controle de acesso, incluindo rede lógica, visando o fornecimento de equipamentos, materiais e acessórios e serviços.
Escopo do Projeto	A implantação do sistema se dará em duas Fases distintas, assim sendo: Fase 1: Edifício Sede, localizado na Rua Duque de Caxias, n. 350; Fase 2: Edifício Assis Brasil, localizado na Rua Sete de Setembro, n. 730.
Prazo Previsto	3 meses (melhor prazo favorável)
Marcos do Projeto	Fase 1: entrega da obra em 60 dias após assinatura do contrato. Fase 2: entrega da obra em 90 dias após a assinatura do contrato.

1 DECLARAÇÃO DO ESCOPO

1.1 Introdução

1.1.1 Através deste projeto básico, o TRE-RS (Tribunal Regional Eleitoral do Rio Grande do Sul), apresenta a necessidade de um investimento tecnológico com especificações mínimas para Implantação de Sistema de CFTV (CIRCUITO FECHADO DE TV) e Controle de Acesso, incluindo a estruturação de rede lógica, o fornecimento de equipamentos, materiais e acessórios e serviços de instalação, configuração e garantia.

1.2 Benefícios

1.2.1 Ampliar a vigilância eletrônica remotamente de vários locais ao mesmo tempo e com número reduzido de vigilantes.

1.2.2 Monitorar o fluxo de veículos e pessoas em áreas comuns.

1.2.3 Dimensionar a gravidade de uma ocorrência para então acionar o atendimento adequado, promovendo assim, uma gestão mais eficaz dos recursos disponíveis para atendimento de emergências, onde as ações de pronto atendimento serão enviadas somente após comprovada a necessidade.

1.2.4 Possibilitar o armazenamento e fornecer um histórico das imagens por tempo determinado (mínimo 45 dias).

1.2.5 Coibir possíveis atos de violência, vandalismo ou ações de má índole e aumentar a qualidade das provas em caso de ocorrências.

1.2.6 Centralizar os sistemas de câmeras IP existentes, visando padronização e operação em uma única plataforma.

1.2.7 Proporcionar maior segurança, cadastrando todos os usuários e atribuindo regras específicas de acesso individual.

1.2.8 Permitir a restrição ou liberação de acessos de colaboradores e visitantes a determinados setores e monitorar sua circulação, evitando assim, uma circulação desordenada e diminuindo rupturas na segurança.

1.2.9 Agilizar o gerenciamento dos acessos de colaboradores e visitantes, principalmente quando há um grande número destes.

1.2.10 Emitir relatórios com dados de acesso como entrada e saída de ambientes ou passagem em pontos de controle, permitindo apurar ocorrências que envolvam ativos do TRE-RS.

1.3 Premissas

1.3.1 Prever a instalação de cabeamento estruturado com reaproveitamento de infraestrutura existente, quando possível.

1.3.2 Aproveitamento de doze câmeras IP's existentes no prédio Sede.

1.3.3 Prever a substituição do cabeamento não funcional, devendo ser substituído no edifício Sede o cabeamento que interliga as câmeras dos elevadores (a partir do switch do 4º andar), que interliga as câmeras externas instaladas na esquina e no poste do pátio em frente ao prédio e, no Assis Brasil, a instalação do cabeamento a partir dos switches disponíveis em cada andar, exceto para os equipamentos instalados no 16 e 17 pavimentos, que devem ser ligados no switch do 15º pavimento.

1.3.4 Prever a estruturação da Central de Monitoramento que ficará alocada no Edifício Assis Brasil, localizado na Rua Sete de Setembro, n. 730.

1.3.5 O processamento e armazenamento das imagens/informações serão realizados em equipamentos (Servidores/Storages) a serem instalados no datacenter alocado no Edifício Sede, localizado na Rua Duque de Caxias n. 350.

1.3.6 O cabeamento a ser aproveitado deve ser revisado e certificado. Havendo necessidade de substituição, deverão ser substituídos pela contratada sem ônus adicional ao contratante.

1.3.7 As câmeras a serem aproveitadas devem ser revisadas e instaladas nos pontos indicados.

1.3.8 A solução deve permitir a configuração de plantas para que os operadores das estações de cadastramento tenham acesso às informações do respectivo edifício em que estão atuando.

1.3.9 A solução deve permitir o estabelecimento de rotas para liberação de acesso de visitantes ao respectivo setor de destino.

1.3.10 A solução deverá possibilitar gerenciamento de controle de acesso por interface web.

1.3.11 A solução deve permitir escalabilidade (suportar ampliação) para que possam ser agregados mais pontos de controle de barreira física (porta com fecho eletromagnético, catracas) e sem barreira física (antena RFID, sensores de passagem), desde que devidamente licenciadas.

1.3.12 A solução deve operar isoladamente (sem acesso à internet), baseada em protocolo TCP/IP, e ter os acessos protegidos por usuário e senha.

1.3.13 A solução deve permitir configurar no mínimo 5 níveis de acesso, cada um com permissões específicas.

1.3.14 A solução deve ter configurada a sua estrutura de armazenamento de modo a garantir a guarda e pesquisa dos dados de registro de acesso (logs) por, no mínimo, 60 (sessenta) meses e imagens de CFTV por, no mínimo 45 (quarenta e cinco) dias.

1.3.15 A solução deve operar com atualizações em tempo real, permitindo verificar registro de logs de todos os eventos assim que registrados.

1.3.16 O suporte à LAN, quando aplicável, deve utilizar Interface Ethernet RJ-45 (100BaseT ou 1000BaseTX).

1.3.17 Em caso de queda da rede (comunicação) ou do computador servidor, cada conjunto controlador de passagem em porta deverá continuar funcionando autonomamente com todas as últimas instruções, validando e registrando os acessos.

1.3.18 Os equipamentos da solução devem detectar automaticamente o retorno da disponibilidade da rede e sincronizar-se com a base de dados centralizada.

1.3.19 A solução deve estar conectada ao sistema de proteção contra incêndio da respectiva planta e liberar as barreiras físicas do controle de acesso (rotas de fuga) em caso de acionamento do alarme de incêndio para evacuação do prédio. Não devem ser liberadas as barreiras físicas do Datacenter e salas de lógica.

1.3.20 Cada conjunto controlador de passagem deverá ter a placa instalada em um gabinete, com grau de proteção adequado ao local de instalação, e possuir fonte alternativa de alimentação que garanta autonomia mínima de 4 (quatro) horas em caso de interrupção do fornecimento de energia.

1.3.21 Prever Suporte Técnico para atendimento de incidentes, esclarecimento de dúvidas, manutenção preventiva e corretiva dos equipamentos em garantia e a manutenção corretiva e evolutiva do software da solução.

1.3.22 O conjunto de controle de acesso ao Datacenter deve manter as funcionalidades do sistema atualmente instalado.

1.3.23 No Edifício Assis Brasil deve ser aproveitada a estrutura de TI na instalação dos equipamentos prevendo a conexão lógica a partir da infraestrutura disponível (rack lógico do respectivo pavimento).

1.3.24 A necessidade de pontos de elétrica ficará sob responsabilidade do TRE-RS.

1.3.25 O sistema pode operar com o banco de dados Oracle fornecido pelo contratante ou, em caso de banco diverso, o mesmo deve ser licenciado para a capacidade máxima prevista do sistema.

1.3.26 A solução deve ser configurada para que o controle de acesso seja gerenciado por edifício de modo que o incidente em um edifício não interfira nas funcionalidades do outro.

1.3.27 Considerando a natureza do TRE, os produtos e/ou serviços descritos neste projeto será objeto de um processo de aquisição através de processo licitatório.

1.4 Restrições

1.4.1 Não está prevista a conexão lógica entre os prédios Sede e Assis Brasil via fibra óptica.

1.4.2 O cronograma de instalação fica sujeito a alterações dependendo das autorizações de acesso, uma vez o trabalho será realizado precipuamente em ambientes internos.

1.5 Exclusões

1.5.1 Comunicação por fibra óptica entre os prédios Sede e Assis Brasil.

1.5.2 Estrutura (rack, switch, etc.) com ponto de lógica PoE disponível a partir da infraestrutura de TI do subsolo ao 15º pavimento do Edifício Assis Brasil.

1.5.3 Os pontos de elétrica, nos locais indicados, serão disponibilizados pelo TRE-RS.

1.5.4 Infraestrutura vertical de lógica entre andares no edifício Assis Brasil, exceto a instalação dos controles no acesso às salas de serviço e terraço acima do 15º pavimento.

1.5.5 Eventuais obras civis que se mostrem necessárias à instalação de quaisquer equipamentos, exceto as descritas neste projeto.

1.5.6 O projeto não contempla sistema de detecção de incêndios, incluindo centrais detectoras, dispositivos, botoeiras e acionadores manuais.

2 DESCRIÇÃO DA SOLUÇÃO

2.1 Condições gerais

2.1.1 Este projeto tem o objetivo de definir de forma detalhada as necessidades do TRE-RS para a implantação de sistema de CFTV e controle de acesso, incluindo a estruturação de rede lógica, o fornecimento de equipamentos, materiais e acessórios e serviços de instalação, configuração e garantia.

2.1.2 A solução a ser implantada dará suporte à equipe de segurança do TRE-RS no controle de acesso e circulação dos edifícios Sede e Assis Brasil localizados nas Rua Duque de Caxias, n. 350, e Rua Sete de Setembro, n. 730, em Porto Alegre.

2.1.3 O Sistema deve ser integrado em uma plataforma TCP/IP nativo (“TCP/IP puro”), com interface de usuário principal via navegador Web, sem auxílio de redes ou sub-redes seriais.

2.1.4 O Sistema deve permitir o gerenciamento centralizado e completo de múltiplos locais (multi-site).

2.1.5 O sistema deve possuir hardware e software modulares e expansíveis de acordo com as necessidades presentes e futuras do contratante.

2.1.6 Os equipamentos de gerenciamento e armazenamento (servidores) de imagens serão alocados no Datacenter existente no prédio Sede, que por sua vez, se conectará com o prédio Assis Brasil via fibra óptica existente, onde serão alocadas duas estações de monitoramento para realizar a administração e controle, aplicação de políticas de acesso e outras funcionalidades relacionadas ao conteúdo local da solução proposta.

2.1.7 A Figura 1 mostra a distribuição da rede e seus pontos de monitoramento e controle de acesso (Estrutura física da Rede a ser construída).



Figura 1: Topologia Física da Rede

2.1.8 O projeto será executado em duas fases distintas, conforme segue:

2.1.9 Fase 1: Edifício Sede, localizado na Rua Duque de Caxias, n. 350;

2.1.10 Fase 2: Edifício Assis Brasil, localizado na Rua Sete de Setembro, n. 730.

2.1.11 A Central de Monitoramento inicialmente será instalada no edifício Sede e na Fase 2, remanejada para o edifício Assis Brasil, onde será estruturado ambiente para a centralização do monitoramento de toda a solução. Nos postos de vigilância instalados na sala do 2º andar do edifício Sede e na portaria e garagem do edifício Assis Brasil serão disponibilizados pontos de monitoramento com permissões específicas definidas pelo administrador do sistema.

2.1.12 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 no momento da instalação.

2.1.13 Será de total responsabilidade da contratada o fornecimento dos equipamentos necessários ao funcionamento completo da solução.

2.1.14 A contratação envolve ainda o treinamento dos usuários para a operação do sistema, bem como a garantia com suporte técnico (manutenção preventiva, corretiva dos equipamentos) de modo a manter a funcionalidade do sistema pelo período da garantia (quarenta e oito meses).

2.1.15 As chaves criptográficas necessárias para acesso e gravação de dados armazenados na memória do servidor do sistema deverão ficar disponíveis para o contratante, para permitir continuidade e evolução da solução em caso de interrupção do suporte técnico contratado.

2.1.16 Cabe salientar que por medidas de segurança estabelecidas pelo TRE-RS, a conexão através de ambiente externo não é permitida. Todo o acesso ao sistema de segurança se dará através da rede interna e de propriedade do TRE-RS.

2.1.17 O sistema deverá permitir a distribuição de suas funções, tais como supervisão e controle e a interface gráfica com o usuário, entre outras, em toda a extensão da rede, de forma a obter a maior flexibilidade e rendimento.

2.1.18 A base de dados do software deverá receber e fornecer informações em padrão aberto, compatível com futuros sistemas da área, incluindo a possibilidade de expansão posterior ou instalação em outros servidores de propriedade do Tribunal.

2.1.19 O sistema terá, em conformidade com as necessidades do Tribunal, funções automáticas de backup e funções de recuperação dos arquivos.

2.1.20 O funcionamento padrão dos equipamentos da solução deve ser *online*. O modo *offline* deverá ser utilizado somente em situações de contingência, isto é, os equipamentos da solução devem prosseguir sua operação normal, com apoio de memória local, durante eventuais indisponibilidades da rede de dados.

2.1.21 A solução deve migrar entre as condições *online* e *offline* sem necessidade de intervenção de operador.

2.1.22 O sistema de gerenciamento deve ser robusto, flexível e atender, no mínimo, os sistemas de: controle de acesso, gestão de alarmes (“I/Os”) e de circuito fechado de TV – CFTV.

2.1.23 O sistema deve compreender recursos avançados, totalmente integrados com Controle de Acesso de Pedestres, Circuito Fechado de Vídeo Digital, Monitoramento de Alarmes, e ainda deve possibilitar a futura integração, se necessária, de Controle de Elevadores, Controle de frequência gerencial e Controle de Veículos.

2.2 Sistema de CFTV

2.2.1 Principais itens

2.2.1.1 Dentre os principais itens a serem instalados no prédio Sede, destacam-se: 28 câmeras de monitoramento (12 existentes e 16 novas), 2 estações de monitoramento e 2 switches. E no prédio Assis Brasil, destacam-se: 56 câmeras e 3 estações de monitoramento. Os locais específicos de instalação estão indicados nos anexos V a VIII deste projeto.

2.2.2 Descrição Geral

2.2.3 Solução de Circuito Fechado de Televisão (CFTV) baseado na tecnologia IP, compreendendo o fornecimento de equipamentos, licenças, serviços de instalação e configuração e suporte técnico, padrão de mercado de segurança eletrônica, tipo profissional, para operação 24 horas, com todas as funcionalidades usualmente requeridas para segurança patrimonial. Compreende ainda elaboração de acervo de documentos referente a instalação.

2.2.4 A solução de CFTV deve fornecer os seguintes resultados:

2.2.5 Capturar imagens de todos os movimentos nos principais pontos de acesso internos e externos (adjacências) dos edifícios Sede e Assis Brasil;

2.2.6 Gravar as imagens geradas em servidores de dados instalados no edifício Sede;

2.2.7 Gerenciar as imagens geradas em tempo real nas estações de monitoramento, permitindo tanto o acesso local às imagens, quanto à distância, do edifício Sede, mediante consulta e busca por dia, horário, ponto de acesso, evento de interesse, etc.

2.2.8 Disparar alarmes nos casos em que forem identificados movimentos em áreas e horários com trânsito impedido previamente configurados no software, e realizar o seguinte:

2.2.9 Enviar e-mails e avisos (popups em telas específicas) ao Serviço de Segurança do TRE-RS, e aos demais responsáveis, a critério da contratante;

2.2.10 Gravar as imagens referentes ao ponto de disparo do alarme e outros determinados pela contratante, com envio instantâneo dessas imagens para o Serviço de Segurança do TRE-RS, ou para outros destinatários definidos pela contratante.

2.2.11 A solução deverá supervisionar todos os equipamentos de coleta e de gravação de imagens a serem instalados e ativados em cada edifício. Todas as funcionalidades do sistema deverão ser compatíveis e integradas à rede de comunicação de dados corporativa predial (baseada na tecnologia Ethernet Local Área Network - LAN), sendo que o subsistema deverá operar sem causar qualquer tipo de interferência à rede supracitada.

2.2.12 A solução completa deverá ser instalada e configurada nos edifícios Sede e Assis Brasil, com o respectivo módulo de estação de monitoramento gerenciadora no edifício Assis Brasil. Até a implementação da segunda fase o monitoramento será realizado no edifício Sede, prédio com os controles da primeira fase da contratação.

2.2.13 A contratada deverá realizar a instalação completa da solução, sem que o Tribunal necessite adquirir/implantar qualquer infraestrutura ou softwares complementares. Tampouco deve ser necessária a aquisição de licenças de sistemas operacionais ou bases de dados proprietárias por parte do Tribunal em caso de expansão do sistema.

2.2.14 O CFTV deverá ser formado por câmeras IP interligadas a comutador (switch) e a servidores de gerenciamento e de dados, de forma que possibilite a filmagem inteligente de movimentos em pontos de acesso pré-definidos pelo contratante, registre essas imagens em servidor de dados, e permita o acesso remoto de qualquer computador interligado à rede da contratante a essas imagens, desde que o usuário requisitante possua perfil de acesso compatível e que o computador utilizado possua a versão cliente do software instalada.

2.2.15 A solução deve contemplar sistema de alarme integrado nas câmeras. Os processos realizados na ocorrência dos eventos de alarme (disparar campainha, e-mails de alerta, avisos ao Serviço de Segurança, entre outros) deverão ser gerenciados pelo software.

2.2.16 Os arquivos de imagens serão armazenados no servidor local, com um histórico mínimo de 45 (quarenta e cinco) dias, promovendo sempre a sobregravação das imagens mais antigas quando atingida a capacidade máxima de armazenamento.

2.2.17 Os cabos a serem fornecidos e instalados devem ser de categoria “6” ou posterior. Caberá à contratada a revisão da estrutura existente, a instalação dos cabos novos, a conexão (com crimpagem de todos os pontos de conexão, inclusive na rede de CFTV a ser aproveitada no prédio Sede) e certificação de todos os cabos do sistema.

2.2.18 A relação de equipamentos previstos encontram-se no item 5. Além dos equipamentos relacionados, a contratada proverá outros elementos acessórios que se mostrem fundamentais ao pleno funcionamento da solução, assim como executar toda a infraestrutura necessária.

2.2.19 Arquitetura

2.2.19.1 Trata-se de uma arquitetura de localidade única com controle centralizado, isto é, o sistema deve ser composto de uma plataforma de controle em um nível.

2.2.19.2 O servidor do sistema controlará todos os hardwares instalados nos dois edifícios, permitindo configurações (administração) a partir das estações de monitoramento.

2.2.19.3 O sistema de CFTV deve ser totalmente modular, permitindo integração com sistemas de controle de acesso, além de permitir o controle multi-site de maneira centralizada via LAN. Os módulos deverão possuir ativação realizada de maneira simplificada.

2.2.19.4 As câmeras não deverão depender do servidor para executar as regras pré-cadastradas, ou seja, em caso de perda de conexão com o servidor a câmera deve continuar executando as regras pré-cadastradas, não aceitando qualquer tipo de lista branca / lista negra.

2.2.19.5 O sistema deve permitir arquitetura conforme diagrama abaixo:



Figura 2: Diagrama básico do sistema de CFTV

2.2.19.6 O diagrama completo do sistema está nos Anexos V a VIII deste projeto.

2.2.20 Funcionalidades do Hardware

2.2.20.1 As câmeras devem estar habilitadas a funcionamento offline, com capacidade de armazenamento local suficiente para preservar todos os registros até o restabelecimento da comunicação com o computador servidor, por no mínimo 4 horas.

2.2.20.2 Todas as câmeras devem conectar-se à Rede TRE-RS por meio de cabo par trançado, fazendo uso do protocolo TCP/IP.

2.2.20.3 As câmeras da solução deverão possuir recursos de gravação por evento e detecção de movimento com pelo menos 5 segundos de gravação em buffer, máscara de privacidade, compensação de luz de fundo e day-night.

2.2.20.4 As câmeras fisheye deverão possibilitar o monitoramento de no mínimo 4 áreas de interesse distintas.

2.2.20.5 As especificações técnicas dos equipamentos

2.2.20.6 Os requisitos mínimos dos equipamentos estão elencados no Caderno de Especificações e Encargos constante no Anexo IX deste projeto.

2.3 Sistema de Controle de Acesso

2.3.1 Principais itens

2.3.1.1 Dentre os principais itens a serem instalados no edifício Sede, destacam-se: 2 controladoras de portas, 4 estações de cadastramento, 1 impressora de cartões, 2 urnas coletoras de cartões e 3 antenas RFID. No prédio Assis Brasil, destacam-se: 51 controladoras de portas, 5 estações de cadastramento, 4 catracas, 2 antenas RFID, 2 urnas coletoras de cartões e 3 sensores de movimento. Os locais específicos de instalação estão indicados nos Anexos V a VIII deste projeto.

2.3.2 Descrição Geral

2.3.2.1 O sistema deve possuir ferramenta gráfica para gerenciamento de cartões em lote, utilizando-se métodos de busca e seleção eficientes.

2.3.2.2 O sistema de gerenciamento de controle de acesso deve ser compatível com Sistema Operacional da solução de modo que, em caso de “logoff” do Sistema Operacional, a aplicação não pare de funcionar ou receber os eventos das câmeras.

2.3.2.3 As controladoras de acesso deverão ser instaladas dentro das áreas seguras (nunca nas áreas externas às portas controladas), impedindo a violação dos seus relés, usando-se magnetos ou outros dispositivos.

2.3.2.4 O sistema de controle de acesso deve ser totalmente modular, permitindo integração com o sistema de CFTV, além de permitir o controle multi-site de maneira centralizada via LAN. Os módulos deverão possuir ativação realizada de maneira simplificada.

2.3.2.5 O sistema de gerenciamento deve ser desenvolvido em plataforma que permita a integração com sistema de terceiros, integração esta, no mínimo, através de Banco de Dados.

2.3.2.6 A solução deverá garantir os desbloqueios de portas e catracas no caso de um dos edifícios precise ser evacuado, incluindo exceção para o Datacenter e salas de TI.

2.3.2.7 O sistema deve permitir inserir plantas dos edifícios controlados para acompanhamento e tratamento de eventos a partir das estações de monitoramento.

2.3.3 Arquitetura

2.3.3.1 Trata-se de uma arquitetura de localidade única com controle centralizado, isto é, o sistema deve ser composto de uma plataforma de controle em um nível.

2.3.3.2 O servidor do sistema, controlará todos os hardwares de ambos os prédios. A estação de monitoramento do Edifício Sede fará o controle na primeira fase do projeto. Na segunda fase a central de monitoramento será alocada para o edifício Assis Brasil.

2.3.3.3 As controladoras não deverão depender do servidor para executar as regras pré-cadastradas, ou seja, em caso de perda de conexão com o servidor a controladora deve continuar executando as regras pré-cadastradas, não aceitando qualquer tipo de lista branca / lista negra.

2.3.3.4 Cada conjunto controlador deverá possuir a interconexão de seus componentes conforme as normas técnicas aplicáveis, devendo a controladora e o sistema de alimentação alternativa ser protegido por gabinete.

2.3.3.5 O sistema deve permitir arquitetura conforme diagrama abaixo:



Figura 3: Diagrama básico do sistema de controle de acesso

2.3.3.6 O diagrama completo do sistema está no Anexo V a VIII deste projeto.

2.3.4 Funcionalidades do Hardware

2.3.5 O hardware controlador de acesso utilizado deve ser sempre capaz, tanto em modo on-line quanto em modo off-line, de realizar a autenticação dos usuários sem a necessidade de consulta ao servidor de controle de acesso, ou seja, a consulta de usuários cadastrados deve ser realizada pela controladora em sua memória interna, sem depender do software instalado no servidor, sendo que todas as credenciais e regras de negócios devem estar armazenadas nesta memória interna, não volátil.

2.3.6 O hardware deve possuir no mínimo 4 entradas físicas de leitores configuráveis por softwares e 2 saídas de relés com tempo configurável em software.

2.3.7 Não serão aceitos sistemas com arquitetura que compreenda redes ou sub-redes seriais como RS-232, RS-422, RS-485 ou outras, ou concentradores TCP/IP e redes seriais entre estes e módulos, de forma a não prejudicarem a performance e velocidade de transmissão de dados no sistema, bem como prejudicarem sua escalabilidade, flexibilidade e manutenção.

2.3.8 O sistema deve possuir comunicação TCP/IP em alta velocidade para reduzir a utilização da banda de transmissão de dados transmitidos em pacotes, otimizando a velocidade de transmissão entre as controladoras e o servidor, provendo transações em tempo real até para o usuário.

2.3.9 O sistema deve permitir a reunião de controladoras em grupos de duas ou mais unidades, para atuação das funcionalidades de antipassback global ou de integração com sistema de incêndio, sendo que a comunicação entre as controladoras do mesmo grupo deve ser feita de forma ponto-a-ponto (peer-to-peer), sem a necessidade de comunicação com o servidor de controle de acesso, a fim de aumentar a confiabilidade do sistema.

2.3.10 O antipassback global deve funcionar sem a necessidade do PC servidor de controle de acesso estar on-line, eliminando falhas do sistema ou interrupções de fluxo, mesmo com os servidores de controle de acesso fora do ar. Portas e demais barreiras e áreas de acesso podem ser agrupadas em um grupo previamente programável, mesmo em locais remotos.

2.3.11 O hardware deve ser capaz de realizar a baixa automática (exclusão de cartão da memória interna da controladora) de cartões de visitante sem a necessidade de comunicação com o servidor de controle de acesso no momento da baixa, eliminando falhas do sistema ou interrupções de fluxo, mesmo com o servidor de controle de acesso fora do ar. Controladoras de acesso podem ser agrupadas em um grupo previamente programável, onde a baixa de cartões será executada somente nestas, sendo que para este fim as mesmas se comunicarão entre si de forma ponto-a-ponto (peer-to-peer).

2.3.12 O sistema deve possuir função de integração com sistemas de incêndio através de uma entrada digital na controladora. A controladora, ao receber, nesta entrada digital, sinal proveniente de um módulo da rede da central de incêndio de terceiros, comunica-se peer-to-peer (ponto a ponto) com outras controladoras de seu grupo, através da rede Ethernet, liberando todas as fechaduras das rotas de fuga até que o operador as rearme novamente, pelo sistema.

2.3.13 O sistema deve permitir a utilização de redes sem fio, reduzindo custos com passagem de cabos, ou viabilizando áreas onde a passagem dos mesmos é muito difícil.

2.3.14 O Sistema deve permitir dispositivos de detecção com contatos normalmente aberto (NA) ou normalmente fechados (NF), a serem conectados às entradas das zonas de alarme, do mesmo modo. Um modo de programação deve ser fornecido para definir cada uma das entradas, e se o dispositivo utiliza saídas NA ou NF.

2.3.15 Deve ser permitido a supervisão dos sensores tipo NA, através de resistores de fim de linha.

2.3.16 Se incorporado futuramente teclado e credencial para acesso as portas, a controladora deve suportar dupla autenticação (cartão & senha) configurável por zona horária diferenciada na entrada e saída. Também deverá permitir até 10 senhas pré-configuradas por zona horária para acesso à porta, a fim de liberar o acesso em caso de emergência.

2.3.17 As urnas coletoras deverão possuir sistema para baixa automática do cartão (registro de saída de visitante) quando este for nela depositado.

2.3.18 As controladoras de acesso deverão possuir carregador flutuante de bateria integrado. Todas estas controladoras deverão funcionar na mesma rede TCP/IP, simultaneamente, conforme a alternativa de solução mais rápida e prática para ampliação do sistema.

2.3.19 Todas as controladoras de campo deverão possuir conexão dedicada para bateria a fim de prover energia de reserva (backup) e segurança em caso de falha de suprimento de corrente alternada ou alimentação PoE. O equipamento deve ser equipado com circuito de carregamento flutuante das baterias durante a operação normal.

2.3.20 A alimentação alternativa das controladoras deve permitir gerenciamento de funcionalidade via software do sistema.

2.3.21 Cada controladora PoE deve fornecer energia para pelo menos quatro leitoras de cartão (duas leitoras de entrada e duas leitoras de saída) e duas fechaduras do tipo eletroímã (de baixo consumo de corrente), podendo então realizar o controle de duas portas.

2.3.22 As controladoras a serem instaladas na sala do shaft de lógica de cada andar no edifício Assis Brasil deverão possuir dispositivo de liberação do tipo eletromecânico.

2.3.23 Cada dispositivo de detecção e alarme deve estar conectado a uma zona em separado, para monitoramento individual e reporte.

2.3.24 O hardware deve ser capaz de controlar ao menos 4 leitores em cada controladora, simplificando a instalação e configuração do sistema.

2.3.25 O hardware deve ter suporte a diferentes tecnologias de leitores, dentre eles:

2.3.26 Leitores Mifare;

2.3.27 Leitores Biométricos;

2.3.28 Leitores de Cartão RFID;

2.3.29 Leitores de código de barra.

2.3.30 O hardware padrão, sem customizações, deve suportar, em sua memória residente, no mínimo 4 protocolos de comunicação (com os leitores) diferentes.

2.3.31 Comunicação

2.3.32 A comunicação entre software e controladora deve ser executada via rede ethernet nativa (10/100Mbps), permitindo escalabilidade de uma até centenas de portas, em incremento de controladoras, uma a uma.

2.3.33 O sistema deve possuir comunicação peer-to-peer (ponto-a-ponto), possibilitando a comunicação entre as controladoras a qualquer momento, sem a necessidade do servidor estar on-line, assim garantindo a qualquer momento a liberação de rota de incêndio, antipassback global ou baixa automática de cartões de visitante.

2.3.34 Cada barreira deve ser assistida por controladora individual em TCP/IP nativo (10/100 Mbps) para reduzir a utilização da banda de transmissão de dados.

2.3.35 O sistema deve permitir a utilização da infraestrutura de rede Ethernet já existente, bem como a adição de uma nova rede de dados, para monitorar e controlar o acesso local ou o acesso remoto de filiais (outras localidades), de uma mesma central de segurança, via VPN em LAN ou WAN.

2.3.36 O sistema deve permitir que uma controladora não afete o funcionamento de outra, como no caso de redes em “daisy-chain” ou “looping”, a fim de aumentar a confiabilidade do sistema, assim como garantir a rápida e simples manutenção do mesmo.

2.3.37 A instalação das controladoras na rede Ethernet deve ser simples e rápida, sem que seja necessária a configuração de jumpers de endereçamento nas mesmas. O sistema deve ser inteligente o suficiente para auto detectar o endereço IP padrão (“default”) de cada controladora, e automaticamente, adicioná-la no banco de dados do sistema, permitindo a mudança manual de endereço IP, via software, para adequação dos dispositivos à rede existente.

2.3.38 Quantitativos, características dos equipamentos e instalação

2.3.39 Os requisitos mínimos dos equipamentos estão elencados no Caderno de Especificações e Encargos constante no Anexo IX deste projeto.

2.3.40 Softwares

2.3.41 A solução em software deve proporcionar a operação integrada de equipamentos, cartões, sensores, leitores de cartões e estações de cadastramento agregando as funcionalidades descritas neste termo de referência para o controle de acesso e circulação nas instalações do contratante.

2.3.42 A solução deverá possuir um software de gerenciamento de controle de acesso operado por interface web e com as funcionalidades discriminadas neste projeto básico.

2.3.43 A solução deve permitir escalabilidade (suportar ampliação) para que possam ser agregadas mais pontos de controle de barreira física (porta com fecho eletromagnético ou eletromecânico, catracas) e sem barreira física (antena RFID, sensores de passagem), desde que devidamente licenciadas.

3 CRONOGRAMA

3.1 O cronograma de implantação do sistema, em cada fase, deverá ser apresentado no plano de execução pela empresa vencedora do certame na reunião inicial a ser realizada no TRE em até 5 dias após assinatura do contrato.

3.2 Deverão constar no cronograma de implantação as etapas principais e secundárias com prazos e marcos do projeto pré-estabelecidos para análise e aprovação da comissão de gestão do contratante.

3.3 O cronograma deve prever a sequência de atividades necessárias para implantação no prazo estabelecido para a respectiva fase.

3.4 Devem ser discriminados os dias e horários de atividades nas dependências do contratante.

3.5 As atividades da contratada poderão ter o cronograma alterado conforme necessidades do contratante.

3.6 A duração das atividades é baseada em dados históricos e assume que as equipes envolvidas têm dedicação exclusiva ao projeto. Portanto, os prazos do projeto e das suas etapas podem variar conforme a quantidade de recursos alocados e das condições imprevistas enfrentadas. O prazo máximo de execução é de 60 dias para a fase 1 (edifício Sede) e 90 dias para a fase 2 (edifício Assis Brasil).

4 CUSTOS

4.1 O orçamento total deste projeto é composto por equipamentos, softwares, materiais, serviços e garantia.

4.2 A planilha analítica está disponível no Anexo II.

4.3 Abaixo, estão elencados os valores de implementação em planilha sintetizada:

Colocar a planilha sintética conforme informado

5 ESTRUTURA A SER INSTALADA

5.1 Edifício Sede

Nr. O.	DESCRIÇÃO	UN.	QUANT.
ETAPA 1 – EQUIPAMENTOS A SEREM INSTALADOS NO EDIFÍCIO SEDE			
1.1	SERVIDORES		
1.1.1	Servidores do sistema		
1.1.1.1	Servidor de gerenciamento do sistema de CFTV	unid	1,00
1.1.1.2	Servidor de controle de acesso	unid	1,00
1.1.1.3	Servidor de banco de dados para controle de acesso	unid	1,00
1.2	OUTROS EQUIPAMENTOS		
1.2.1	Equipamentos de Estrutura lógica		
1.2.1.1	Switches PoE 24P	unid	2,00
1.2.1.2	Patch cord	unid	42,00
1.2.1.3	Gbic	unid	6,00
1.2.1.4	Cabo UTP cat6	m	680,00
1.2.1.5	Cabo UTP cat6 Geleado	m	280,00
1.2.2	Equipamentos de CFTV		
1.2.2.1	Câmeras Fisheye	unid	2,00
1.2.2.2	Câmera Dome	unid	14,00
1.2.2.3	Conjunto estação de monitoramento	unid	2,00
1.2.2.4	Suporte de parede para câmera Fisheye	unid	1,00
1.2.2.5	Suporte de poste para câmera Fisheye	unid	1,00
1.2.3	Equipamentos de Controle de acesso		
1.2.3.1	Conjunto controladora de porta do datacenter	unid	1,00
1.2.3.2	Conjunto controladora de porta para porta corta-fogo	unid	1,00
1.2.3.3	Conjunto urna coletora de cartões	unid	2,00
1.2.3.4	Conjunto antena RFID	unid	3,00
1.2.3.5	Conjunto estações de cadastramento	unid	4,00
1.2.3.6	Impressora de cartões	unid	1,00
1.3	SOFTWARE		
1.3.1	Licenças de software		
1.3.4.1	Licença de software servidor – CFTV	unid	1,00
1.3.4.2	Licença de software servidor – controle de acesso	unid	1,00
1.3.4.3	Licença de software para cliente – CFTV	unid	3,00
1.3.4.4	Licença de software para cliente – Controle de acesso	unid	6,00
1.3.4.5	Licença de software – equipamento CFTV	unid	28,00
1.3.4.6	Licença de software – equipamento de controle de acesso	unid	7,00
ETAPA 2 – SERVIÇOS DE INSTALAÇÃO DA SOLUÇÃO NO EDIFÍCIO SEDE			
2.1	DESPESAS INICIAIS E TAXAS DIVERSAS		
2.1.1	Taxas diversas		

2.1.1.1	Emissão de ART específico	gb	1,00
2.2	INSTALAÇÃO DO SISTEMA		
2.2.1	Serviços preliminares		
2.2.1.1	Revisão do atual sistema de CFTV e retirada dos componentes que não serão aproveitados	unid	1,00
2.2.2	Instalação de eletrodutos e acessórios		
2.2.2.1	Eletroduto	m	35,00
2.2.2.2	Eletrocalha	m	12,00
2.2.3	Instalação de equipamentos		
2.2.3.1	Interconexão óptica com módulo Gbic entre servidores e rede do Tribunal	unid	6,00
2.2.3.2	Interconexão entre os switches e câmeras, estações de cadastramento, estações de monitoramento, urnas coletoras de cartões, controladoras de portas e antenas RFID com cabo UTP cat6	m	680,00
2.2.3.3	Interconexão dos três elevadores e duas câmeras externas com Cabo UTP cat6 Geleado	m	280,00
2.2.3.4	Instalação e configuração de câmera dome nova	unid.	14,00
2.2.3.5	Instalação de câmera externa	cj.	2,00
2.2.3.6	Revisão, instalação e configuração de câmera do sistema atual	unid.	12,00
2.2.3.7	Instalação e configuração de servidor do sistema	unid.	3,00
2.2.3.8	Instalação e configuração de switch e patch panel	unid.	2,00
2.2.3.9	Instalação e configuração do conjunto de controladora de porta no datacenter	unid.	1,00
2.2.4.10	Instalação e configuração do conjunto de controladora de porta em porta corta-fogo	unid.	1,00
2.2.4.11	Instalação e configuração de urna coletora de cartões	unid.	2,00
2.2.4.12	Instalação e configuração de antena RFID	unid.	3,00
2.2.4.13	Instalação e configuração de estação de monitoramento	unid.	2,00
2.2.4.14	Instalação e configuração de estação de cadastramento	unid.	4,00
2.2.4.15	Instalação e configuração de impressora de cartões	unid.	1,00
2.2.4.16	Certificação de pontos de lógica	unid.	43,00
2.2.4.17	Instalação de conexão com o sistema de alarme de incêndio	unid.	1,00
2.2.4	Outros Materiais		
2.2.4.1.	Cartões PVC	unid	1.000,00
2.2.4.2	Cordão personalizado com clip roller	unid	800,00
2.2.4.3	Porta cartão	unid	1.000,00
2.2.4.4	Presilha plástica e prendedor tipo jacaré para porta cartão	unid	200,00
2.2.4.5	Ribbon para impressora de cartões	cj.	3,00
2.2.4.6	Cartão adesivo de limpeza para impressora de cartões	unid	10,00
2.2.5	Configurações		
2.2.5.1	Configuração do sistema de CFTV	unid.	1,00
2.2.5.2	Configuração do sistema de controle de acesso	unid.	1,00
2.2.5.3	Licença de software e configuração de leiaute de cartões	unid	1,00

2.3	TREINAMENTO		
2.3.1	Treinamento		
2.3.1.1	Treinamento	hora	12,00
2.4	GARANTIA		
2.4.1	Garantia e suporte técnico		
2.4.1.1	Garantia e suporte técnico	mês	48,00
2.5	SERVIÇOS DIVERSOS		
2.5.1	Serviços diversos		
2.5.1.1	Projetos "AS BUILT"	gb	1,00
2.5.1.2	Serviços diversos	gb	1,00
2.5.1.3	Manuais	cj.	1,00

5.1.1 As especificações constam no Anexo IX deste projeto.

5.2 Edifício Assis Brasil

Nr. O.	DESCRIÇÃO	UN.	QUANT.
ETAPA 1 – EQUIPAMENTOS A SEREM INSTALADOS NO EDIFÍCIO ASSIS BRASIL			
3.2	EQUIPAMENTOS		
3.2.1	Equipamentos de CFTV		
3.2.2.1	Câmeras Fisheye	unid	4,00
3.2.2.2	Câmera Dome	unid	52,00
3.2.2.3	Sensor de movimento	unid	3,00
3.2.2.4	Conjunto estação de monitoramento – Tipo 1	unid	2,00
3.2.2.5	Conjunto estação de monitoramento – Tipo 2	unid	1,00
3.2.2.6	Monitor 42"	unid	4,00
3.2.2.7	Suporte articulado para monitor	unid	4,00
3.2.2.8	Cabo HDMI 10 m	unid	4,00
3.2.2.9	Monitor 21"	unid	1,00
3.2.3	Equipamentos de Controle de acesso		
3.2.3.1	Conjunto Catraca Pivotante	unid	3,00
3.2.3.2	Conjunto Catraca PNE	unid	1,00
3.2.3.3	Conjunto controladora de porta de madeira – fecho eletromagnético	unid	1,00
3.2.3.4	Conjunto controladora de porta para porta corta-fogo	unid	3,00
3.2.3.5	Conjunto controladora de porta madeira – fecho eletromecânico	unid	14,00
3.2.3.6	Conjunto controladora de porta de vidro	unid	33,00
3.2.3.7	Conjunto urna coletora de cartões	unid	2,00
3.2.3.8	Conjunto antena RFID com suporte e kit de fixação	unid	2,00
3.2.3.9	Conjunto estação de cadastramento	unid	5,00
3.2.3.10	Leitor de cartão de mesa USB	unid	5,00
3.2.3.11	Webcam USB	unid	5,00

3.3	SOFTWARE		
3.3.1	Licenças de software		
3.3.1.1	Licença de software para cliente – CFTV	unid	3,00
3.3.1.2	Licença de software para cliente – Controle de acesso	unid	5,00
3.3.1.3	Licença de software – equipamento CFTV	unid	56,00
3.3.1.4	Licença de software – equipamento de controle de acesso	unid	59,00
3.4	Outros materiais		
3.4.1	Cabo UTP cat6	m	2.320,00
3.4.2	Cabo UTP cat6 Geleado	m	300,00

ETAPA 2 – SERVIÇOS DE INSTALAÇÃO DA SOLUÇÃO NO EDIFÍCIO ASSIS BRASIL

4.1	DESPESAS INICIAIS E TAXAS DIVERSAS		
4.1.1	Taxas diversas		
4.1.1.1	Emissão de ART específico	gb	1,00
4.2	INSTALAÇÃO DO SISTEMA		
4.2.1	Serviços preliminares		
4.2.1.1	Revisão do atual sistema de CFTV e retirada dos componentes que não serão aproveitados	unid	1,00
4.2.2	Instalação de eletrodutos e acessórios		
4.2.2.1	Eletroduto	m	200,00
4.2.3	Instalação de equipamentos		
4.2.3.1	Interconexão entre os switches e câmeras, estações de cadastramento, estações de monitoramento, urnas coletoras de cartões, controladoras de portas e antenas RFID com cabo UTP cat6 Seco	m	2.320,00
4.2.3.2	Interconexão dos três elevadores com Cabo UTP cat6 Geleado	m	300,00
4.2.3.3	Instalação e configuração de câmera Fisheye externa	unid.	2,00
4.2.3.4	Instalação e configuração de câmera Fisheye interna	unid.	4,00
4.2.3.5	Instalação e configuração de câmera dome externa	unid.	4,00
4.2.3.6	Instalação e configuração de câmera dome interna	unid.	46,00
4.2.3.7	Instalação e configuração do conjunto controladora de porta de madeira	unid.	1,00
4.2.3.8	Instalação e configuração do conjunto controladora de porta para porta corta-fogo	unid.	3,00
4.2.3.9	Instalação e configuração do conjunto controladora de porta madeira – fecho eletromecânico	unid.	12,00
4.2.3.10	Instalação e configuração do conjunto controladora de porta de vidro	unid.	33,00
4.2.3.11	Instalação e configuração de urna coletora de cartões	unid.	2,00
4.2.3.12	Instalação e configuração de antena RFID	unid.	2,00
4.2.3.13	Instalação e configuração de estação de monitoramento	unid.	3,00
4.2.3.14	Instalação e configuração de estação de cadastramento	unid.	5,00
4.2.3.15	Certificações de pontos de lógica	unid.	126,00
4.2.3.16	Instalação de conexão com o sistema de alarme de incêndio	unid.	1,00

4.2.4	Configurações		
4.2.4.1	Configuração do sistema de CFTV	unid.	1,00
4.2.4.2	Configuração do sistema de controle de acesso	unid.	1,00
4.3	GARANTIA		
4.3.1	Garantia e suporte técnico		
4.3.1.1	Garantia e suporte técnico	mês	48,00
4.4	SERVIÇOS DIVERSOS		
4.4.1	Serviços diversos		
4.4.1.1	Projetos "AS BUILT"	gb	1,00
4.4.1.2	Serviços diversos	gb	1,00
4.4.1.3	Manuais	cj.	1,00

5.2.1 As especificações constam no Anexo IX deste projeto.

6 DA QUALIFICAÇÃO TÉCNICA

6.1 Para fins de qualificação técnica, a empresa proponente deverá no momento da apresentação da proposta apresentar os seguintes documentos:

6.1.1 Registro de certidão de pessoa jurídica no CREA/RS ou CAU/RS ou no estado sede da empresa.

6.1.2 Declaração da proponente de que possui suporte técnico/administrativo, aparelhamento, instalações e condições adequadas, bem como pessoal qualificado e treinado, disponíveis para a execução dos serviços objeto desta licitação e indicação do Responsável Técnico pela execução do serviço.

6.1.3 Por se tratar de um trabalho multidisciplinar é exigido que a proponente tenha em seu quadro funcional, na data prevista para a entrega da proposta, por uma das seguintes formas: no caso de sócio ou diretor da empresa, através de contrato social ou estatuto social em vigor, acompanhado de prova da diretoria em exercício; no caso de empregado, mediante cópia da Carteira de Trabalho e Previdência Social (CTPS) ou de contrato de prestação de serviços, celebrado de acordo com a legislação civil comum, podendo este ter sua eficácia condicionada a adjudicação do objeto à proponente, pelo menos os seguintes profissionais:

6.1.4 Pelo menos um profissional (engenheiro e arquiteto) com registro do seu respectivo conselho. A necessidade deste profissional destina-se à etapa de execução das instalações, uma vez que faz parte do escopo a análise de desenhos técnicos em planta baixa, esquemas de ligação, diagramas elétricos, eletrônicos, mecânicos e detalhes típicos de instalações.

6.1.5 Pelo menos um profissional na área de informática, como formação superior em análise de sistemas, ciência da computação, engenharia de computação e/ou elétrica. Esta exigência se faz necessária uma vez que é necessário a análise de software existentes bem como a proposta de novos sistemas e softwares. Outro fator de relevância é que todas as aplicações atuais de segurança utilizam protocolos IP e necessitam de redes de dados.

6.1.6 Para atendimento à qualificação técnico-profissional, comprovação da proponente de possuir em seu corpo técnico, ou com contrato de prestação de serviços ou na qualidade de sócio, profissional(is) de nível superior, reconhecido(s) pelo CREA, detentor(es) de atestado(s) de responsabilidade técnica, devidamente registrado(s) no CREA da região onde os serviços foram executados, acompanhado(s) da(s) respectiva(s) Certidão(ões) de Acervo Técnico - CAT, expedidas pelos respectivos Conselhos, que comprove ter o(s) profissional(is), executado para órgão ou entidade da administração pública direta ou indireta, federal, estadual, municipal ou Distrito Federal, ou ainda, para empresa(s) brasileira(s) de direito privado, pelos menos os seguintes atestados:

6.1.7 Certidão de Acervo Técnico (CAT), expedido por conselho que comprove que o responsável técnico é detentor de responsabilidade técnica de, pelo menos, uma implantação de sistema de CFTV com câmeras IP em rede de cabeamento estruturado e de controle de acesso com controladores compatíveis com o escopo do projeto, condizentes com seu grau de complexabilidade.

7 CONSIDERAÇÕES FINAIS

7.1 Considerações técnicas sugeridas para o processo de aquisição do TRE-RS:

7.1.1 Período mínimo de garantia integral para todos os produtos: 48 (quarenta e oito) meses contados da data de emissão do termo de aceite definitivo da respectiva fase.

7.1.2 A substituição de peça/equipamentos e atualizações de softwares e eventuais reconfigurações na vigência do contrato não gera quaisquer ônus adicionais para a contratante. Toda e qualquer peça ou componente consertado ou substituído, fica automaticamente garantido até o final da garantia.

7.1.3 Indicar na proposta a marca e modelo do objeto e apresentar documentação que comprove todas as características técnicas (serão aceitas cópias das especificações obtidas no site do fabricante na Internet, juntamente do endereço do site onde foram obtidas).

7.1.4 Apresentar declaração do proponente informando que o objeto não está fora de linha de fabricação e que todos seus componentes são novos (sem uso, reforma ou recondicionamento).

7.1.5 Apresentar declaração do proponente indicando a razão social e o endereço da empresa responsável pela assistência técnica.

8 ANEXOS

ANEXO I – ART (Anotação de Responsabilidade Técnica)

ANEXO II – Planilha Estimativa de Custos

ANEXO III – Cálculo do BDI

ANEXO IV – Cálculo dos Encargos Sociais

ANEXO V – Plantas de Localização de Equipamentos e Elétrica no Edifício Sede

ANEXO VI – Plantas de Localização de Equipamentos e Elétrica no Edifício Assis Brasil

ANEXO VII – Projeto de Distribuição e Conexão dos Componentes no Edifício Sede

ANEXO VIII – Projeto de Distribuição e Conexão dos Componentes no Edifício Assis Brasil

ANEXO IX – Caderno de Especificações e Encargos

Porto Alegre, RS, 30 de agosto de 2019.

ALCIDES P. BARBOSA

Engenheiro Eletricista

CREA: RS 064481