

SESC
SERVIÇO SOCIAL DO COMÉRCIO

CONCORRÊNCIA N.º 01/2020

ANEXO IV

CFTV E CONTROLE ACESSO

PROJETO EXECUTIVO

MEMORIAL DESCRITIVO

JANEIRO DE 2019

SUMÁRIO

1	INTRODUÇÃO	3
1.1	OBJETIVO.....	3
1.2	NORMAS TÉCNICAS.....	4
1.3	LOCALIZAÇÃO DA OBRA.....	4
1.4	CARACTERIZAÇÃO DO EDIFÍCIO.....	ERRO! INDICADOR NÃO DEFINIDO.
2	SISTEMA DE CFTV	5
2.1	CONFIGURAÇÃO	5
2.2	INFRAESTRUTURA E EQUIPAMENTOS.....	5
2.2.1	INFRAESTRUTURA.....	5
2.2.2	EQUIPAMENTOS.....	5
2.3	OBJETIVOS	6
2.3.1	ARQUITETURA DA PLATAFORMA	6
2.3.2	MÓDULOS DO SISTEMA	7
2.3.3	VISUALIZAÇÃO E MONITORAMENTO.....	10
2.3.4	SERVIDOR DE CFTV	10
2.4	ALIMENTAÇÃO ELÉTRICA.....	10
3	SISTEMA DE CONTROLE DE ACESSO (SCA).....	11
3.1	CONFIGURAÇÃO	11
3.2	INFRAESTRUTURA E EQUIPAMENTOS.....	11
3.2.1	INFRAESTRUTURA.....	11
3.2.2	EQUIPAMENTOS.....	11
3.3	OBJETIVOS	12
3.3.1	ARQUITETURA DA PLATAFORMA	13
3.3.2	DESCRIÇÃO DA SOLUÇÃO	13
3.4	ALIMENTAÇÃO ELÉTRICA.....	15

1 INTRODUÇÃO

1.1 OBJETIVO

O presente Memorial tem como objetivo apresentar o Projeto Executivo de Eletrônica a ser implementado no edifício da **Sede do SESC/DF**.

Neste Memorial estão descritos os requisitos técnicos e funcionais empregados no projeto que será utilizado como base para a implantação da obra no que tange às instalações de circuito fechado de TV (CFTV) e controle de acesso (SCA) da nova edificação a ser construída.

Na definição e no desenvolvimento das soluções foram devidamente ponderados os aspectos relativos às limitações físicas do espaço em análise, à funcionalidade, às condições de manutenção, à fiabilidade das instalações e naturalmente à sua viabilidade econômica.

Os equipamentos, materiais e serviços abrangidos por este documento correspondem, sem se limitar, aos seguintes:

CFTV:

- Câmeras internas e externas;
- Estação de operação e monitoramento;
- Sistema de visualização;
- Servidor;
- Infraestrutura: eletrodutos, eletrocalhas, caixas de passagem e tomadas RJ-45.

SCA:

- Controladores de acesso;
- Kits para controle de acesso;
- Bloqueios;
- Cancelas;
- Estação de operação;
- Servidor;
- Infraestrutura: eletrodutos, eletrocalhas, caixas de passagem e tomadas RJ-45.

Este documento, juntamente com a Especificação Técnica Específica (ETE), Planilha de Serviços e Quantidades (PSQ) e o conjunto de desenhos do Projeto Executivo comporão os documentos para a contratação do fornecimento de equipamentos, materiais e serviços do sistema.

No caso de se verificar qualquer dúvida ou incompatibilidade em obra envolvendo o presente projeto, deverão os projetistas ser contatados antes da sua execução.

Todas as soluções propostas no projeto respeitarão a regulamentação vigente nas normas técnicas aplicáveis.

1.2 NORMAS TÉCNICAS

Todos os equipamentos, sistemas e materiais deverão ser projetados, fabricados, montados e testados de acordo com as normas ABNT. Na ausência destas, demais normas poderão ser utilizadas, desde que expressamente indicadas pelo Fornecedor e aprovado pelo Contratante.

Deverá ser adotada como referência a versão mais atual das seguintes normas:

- NBR-14565 - Procedimento Básico para Elaboração de Projetos de Cabeamento de Telecomunicações para Rede Interna Estruturada;
- NBR 5410 – Instalações elétricas de baixa tensão;
- Norma NBR 5419 – Proteção de Estruturas Contra Descargas Atmosféricas.

1.3 LOCALIZAÇÃO DA OBRA

O edifício da Sede do SESC/DF será construído no endereço SIA trecho 4, lotes 80-90-100-110, Setor de Indústria e Abastecimento, na cidade de Brasília/DF, conforme mostrado abaixo:



2 SISTEMA DE CFTV

2.1 CONFIGURAÇÃO

A configuração do Sistema CFTV é o que se apresenta nas Peças Desenhadas de projeto.

2.2 INFRAESTRUTURA E EQUIPAMENTOS

2.2.1 Infraestrutura

A infraestrutura necessária ao sistema de CFTV será compartilhada com Telecomunicações e Controle de Acesso e será composta, no mínimo, pelos seguintes itens:

- Rede de dutos, eletrocalhas e caixas de passagens;
- Gabinetes (caixas e rack's) para equipamentos;
- Acessórios;
- Cabos, sinal, controle e dados (UTP, Cat.6);
- Aterramentos.

2.2 Equipamentos

2.2.2.1 Câmeras

- Câmera tipo 1 - fixa dome (instalação interna);
- Câmera tipo 2 - fixa mini dome (instalação em elevador);
- Câmera tipo 3 – fisheye 360° (instalação interna);
- Câmera tipo 4 – multisensor (instalação interna);
- Câmera tipo 5 – bullet (instalação externa);
- Câmera tipo 6 – bullet (instalação externa);
- Câmera tipo 7 – video comunicador.

2.2.2.2 Estações de Operação

- Computador;
- Monitor, Teclado de operação e Mouse.

2.2.2.3 Sistema de visualização

- Conjunto de monitores 55" formando videowall.

2.2.2.4 Servidor de Vídeo

- Unidade de monitoramento do CFTV e armazenamento de dados.

2.2.2.5 Proteção e alimentação elétrica

- Filtros protetores contra surtos;
- Alimentação elétrica através de No Break.

2.2.2.6 Softwares

- Sistemas Operacionais;
- Aplicativos.

2.3 OBJETIVOS

Pretende-se com este projeto a implementação de um sistema de segurança unificado que seja um complemento das funções de segurança e proteção, aumentando a assertividade nas tomadas de decisões utilizando um sistema altamente moderno.

O projeto é composto por plataformas tecnológicas que garantem os seguintes princípios de funcionamento:

- Alta disponibilidade;
- Fácil expansibilidade;
- Flexibilidade, garantida pelo uso de tecnologias e protocolos abertos;
- Integração com outros sistemas.

O projeto foi desenvolvido de forma integrada, garantindo soluções técnicas eficientes, de fácil utilização e com provas dadas no mercado.

A solução proposta deverá garantir a integração de módulos adicionais: o SDAI (Sistema de Detecção e Alarme de Incêndio) e SCA (Sistema de Controle de Acesso). A solução deverá assentar numa plataforma aberta que permita a gestão de equipamentos de diversos fabricantes, comunicando entre si através do protocolo TCP/IP sobre uma rede com suporte Multicast.

Todos os componentes deverão ser geridos através de um único software, permitindo aos utilizadores gerir e interagir com os diferentes módulos utilizando a mesma interface gráfica, levando a uma uniformização das operações de segurança.

A solução a apresentar deverá ser tecnologicamente avançada e ter uma presença sólida no mercado Brasileiro, devendo ser indicadas pelo menos duas referências de grandes clientes institucionais com instalações de dimensão considerável.

Todo o sistema deverá apresentar, obrigatoriamente, características “future-proof”, ou seja, deverá garantir a continuidade de operação com as tecnologias disponíveis atualmente e também no futuro.

2.3.1 Arquitetura da Plataforma

O sistema a implementar deve assentar numa arquitetura cliente-servidor, permitindo que todas as configurações e registros de eventos e alarmes sejam guardados em bancos de dados relacionais

SQL nos servidores. Desta forma, para além de centralizar o processamento, fica também assegurada a segurança do próprio sistema. A aplicação cliente servirá apenas de interface para o utilizador final.

Dependendo da dimensão final do sistema, os vários serviços poderão ser instalados numa única máquina ou em diferentes servidores de forma a distribuir o processamento e assegurar a continuidade do sistema em funcionamento.

2.3.2 Módulos do Sistema

O sistema CFTV deverá suportar câmeras IP de diversos fabricantes, sendo indicado como referência: Bosch, Axis, Pelco, Sony, Verint, Panasonic ou equivalente técnico.

A solução deverá ser o mais flexível possível no que diz respeito à expansibilidade, de forma a acompanhar o natural crescimento das instalações. Deverão ser apresentadas referências nacionais ou internacionais de sistemas instalados com esta dimensão.

O software de gestão de vídeo deverá suportar tráfego multicast. No entanto deverá ter a capacidade de gerir múltiplos métodos de transmissão (unicast e multicast) dentro do mesmo sistema. No caso das fontes serem provenientes de redes exteriores ou que não suportem multicast, deverá o sistema oferecer um serviço de proxy que transforme tráfego unicast em multicast para que seja distribuído dentro da rede interna, bem como o contrário para fornecer vídeo ao exterior.

O sistema deverá ter a capacidade de autodeteção das capacidades de ligação à rede para, autonomamente, escolher a melhor forma de ligação. Caso as fontes de vídeo o permitam, o sistema deverá conseguir gerir os diferentes streams de vídeo disponíveis, de acordo com as necessidades do utilizador. Assim será possível que um utilizador interno receba vídeo em tempo real com grande resolução e um utilizador conectado através da Internet receba vídeo de menor qualidade, devido às limitações de largura de banda.

No que diz respeito à gestão de streams, o software deverá ainda alternar entre os diversos streams de uma mesma fonte de vídeo, sempre que o utilizador altere o número de fontes simultâneas visualizadas na sua aplicação cliente. Desta forma será garantida uma eficiente gestão de largura de banda.

As câmeras deverão poder ser agrupadas e organizadas em pastas representativas da sua localização física, para facilitar o acesso às suas imagens.

Adicionalmente deverão poder ser carregadas as plantas do edifício em autocad, com o posicionamento das diversas câmeras, servindo como hiperligação para a abertura da imagem das mesmas.

Deverá ser possível definir alarmes diversos como detecção de sabotagem ou de movimento, independentemente das funcionalidades das próprias câmeras. O software de gestão deverá ter a capacidade de detectar movimento numa determinada área (definida pelo operador) das imagens.

Sempre que um alarme for acionado, deverá a câmara correspondente ser assinalada em modo gráfico nos monitores dos operadores. Paralelamente poderão ser emitidos sons, enviados e-mails, abertas janelas com imagem da câmara, fechados contatos por relé, etc.

Os alarmes disparados, tal como outros eventos de sistema, serão registrados na base de dados correspondente, e serão associados ao vídeo, permitindo posteriormente pesquisar por alarme e visualizar as imagens correspondentes ao momento do alarme. Sempre que ocorrer um alarme, este deve ser aceite pelo vigilante ou enviado para um superior para que seja aceite.

Também ao nível do suporte de gravação a plataforma deverá ser aberta, suportando uma grande diversidade de armazenamentos, independentemente do seu fabricante. O vídeo poderá ser visualizado e gravado nos formatos de compressão MJPEG e H.264, dependendo das câmeras e codificadores instalados. No entanto, o sistema deverá poder suportar todos eles.

As gravações deverão poder ser agendadas recorrendo a diversos critérios no que diz respeito a horários e qualidade de imagem. Assim, deverá ser possível que uma câmara grave com a mesma qualidade 24 horas por dia, grave apenas durante um determinado horário, grave com uma qualidade durante um intervalo e com outra qualidade em outro intervalo, grave apenas quando ocorre um alarme ou uma detecção de movimento, ou qualquer conjugação destes fatores, permitindo otimizar o espaço em disco necessário para o armazenamento das imagens.

Deverá ser possível definir um limite máximo de dias de retenção das imagens gravadas, no caso vertente prevê-se nesta fase 30 dias. Ao fim desse período, todas as imagens mais antigas serão eliminadas ou marcadas como não necessárias, com a exceção das imagens que tenham sido protegidas pelos utilizadores. Neste caso as imagens ficarão eternamente no sistema até que sejam desprotegidas.

Deverá ser possível gerar uma chave de encriptação no vídeo gravado para posterior verificação da autenticidade das imagens gravadas (em caso de uso como prova em tribunal).

As sequências de vídeo gravadas poderão ser exportadas em diferentes formatos de vídeo, podendo inclusive conter informação relativa aos alarmes ocorridos nesse período. A exportação deverá poder ser feita em formatos de vídeo padrão como AVI, ou em formato proprietário,

oferecendo a possibilidade de incluir um leitor auto executável com a maior parte das funcionalidades do leitor instalável.

O software de visualização de imagens gravadas deve permitir a pesquisa das mesmas através de vários critérios como data, hora, alarmes, bookmarks e outros eventos do sistema, ou mesmo pesquisando por movimento numa determinada área do campo de visão da câmera em questão (área definida pelo operador no momento da busca).

No que diz respeito ao vídeo, poderão ser definidos layouts de visualização contendo desde uma imagem (1x1) até 16 imagens (4x4). Estes layouts e as câmeras neles visualizadas num determinado momento poderão ser gravadas e carregadas mais tarde.

O software deverá suportar teclados com joystick para controle de câmeras.

O software deverá apresentar uma representação gráfica das janelas de vídeo dos monitores com screenshots das imagens apresentadas em cada momento. O utilizador deverá poder arrastar (drag&drop) câmeras da árvore de dispositivos para qualquer quadrante do monitor. Deverá ser ainda possível criar, gravar e chamar layouts de fontes de vídeo, através do posicionamento e dimensionamento livre das diversas janelas de vídeo pela área útil do monitor.

O software deverá disponibilizar ainda plugins para interligação do sistema de análise de vídeo inteligente. Assim, o sistema será obrigatoriamente dotado das funções que se referem:

- Proteção de periferia, detectando sempre que alguém transpõe uma linha imaginária definida no software;
- Contagem de pessoas que passem numa determinada área para contabilizar o número de passagens em cada um dos sentidos;
- Detecção e seguimento de pessoas, ou outros objetos;
- Detecção de intrusão numa área protegida definida anteriormente;
- Detecção de objetos abandonados numa cena, através da aprendizagem inteligente da mesma;
- Proteção de objetos disparando um alarme em caso de remoção do mesmo do local inicial;
- Pesquisa de imagens de forma inteligente, filtradas não só por data e hora mas também por detecção de movimento em determinadas áreas, tamanho de objetos, cor, velocidade e direção do movimento;
- Detecção inteligente de movimento, analisando o vídeo em tempo real, que elimine eventuais falsos alarmes que normalmente ocorrem nos sistemas de detecção inseridos nas próprias câmeras;
- Detecção de sabotagem da câmera;
- Reconhecimento Facial.

2.3.3 Visualização e monitoramento

As imagens captadas pelas diversas câmeras serão visualizadas na estação de operação e através 06 monitores de 55" (vídeo wall) instalados na Sala de Monitoramento do CFTV localizada no 2º pavimento do edifício. Adicionalmente, o sistema deverá possibilitar ainda a visualização de imagens na guarita do prédio, através de estação de monitoramento.

2.3.4 Servidor de CFTV

O gerenciamento e armazenamento de dados do CFTV será realizado por 01 gravador Apliance LPR, que será responsável pela gestão do sistema e dois gravadores de vídeo, que serão responsáveis pelo gerenciamento de gravação.

Com o intuito de proporcionar maior segurança ao sistema, todos os servidores serão instalados no data center localizado no edifício do Bloco de Apoio.

2.4 ALIMENTAÇÃO ELÉTRICA

O sistema elétrico para alimentação do servidor/gravador e estações de monitoramento do CFTV será em 220 (FN) / 60Hz. Já a alimentação das câmeras deverá ser realizada através do cabeamento de rede, pela tecnologia PoE (Power Over Ethernet) proveniente dos switches.

A alimentação elétrica dos sistemas e equipamentos da rede de CFTV será efetuada através de energia estabilizada ininterrupta ("no-break"), devendo apresentar uma arquitetura com os seguintes princípios básicos:

- Fonte de energia estabilizada;
- Energia imune a microcortes;
- Reserva Estratégica.

3 SISTEMA DE CONTROLE DE ACESSO (SCA)

3.1 CONFIGURAÇÃO

A configuração do Sistema de Controle de Acessos é o que se apresenta nas Peças Desenhadas do projeto.

3.2 INFRAESTRUTURA E EQUIPAMENTOS

3.2.1 Infraestrutura

A infraestrutura será compartilhada com Telecomunicações e CFTV e será composta, no mínimo, pelos seguintes itens:

- Rede de dutos, eletrocalhas e caixas de passagens;
- Gabinetes (caixas e rack's) para equipamentos;
- Acessórios;
- Cabos, sinal, controle e dados;
- Aterramentos.

3.2.2 Equipamentos

3.2.2.1 Controladores

- Unidade de Controle de Acesso (UCA);
- Controladora para bloqueios, portas e cancela.

3.2.2.2 Fechadura

- Fechadura eletromagnética;
- Bloqueador de porta.

3.2.2.3 Leitor de acesso

- Leitor de proximidade;

3.2.2.4 Cartão de proximidade

- Cartões.

3.2.2.5 Botoeira

- Botoeira de abertura para saída;
- Botoeira de emergência.

3.2.2.6 Contato eletromagnético

- Sensor eletromagnético.

3.2.2.7 Servidor

- Servidor de controle de acesso.

3.2.2.8 Estações de Trabalho para credenciamento

- Computador;
- Monitor;
- Teclado;
- Mouse;
- Webcam;

3.2.2.9 Catraca

- Catraca comum – para acesso de pedestre;
- Catraca especial – para acesso de portadores de necessidades especiais.

3.2.2.10 Cancela

- Cancela para controle de veículos.

3.2.2.11 Proteção e alimentação elétrica

- Filtros protetores contra surtos;
- Alimentação elétrica através No Break.

3.3 OBJETIVOS

Pretende-se com este projeto a implementação de um sistema de segurança unificado que seja um complemento das funções de segurança e proteção, e um fator de incremento da operacionalidade dos serviços, designadamente pela informatização e automação.

O controle de acesso é composto dos processos de autenticação, autorização e auditoria (accounting). A autenticação identifica quem acessa o sistema, a autorização determina o que um usuário autenticado pode fazer e a auditoria diz o que o usuário fez.

O projeto foi desenvolvido de forma integrada, garantindo soluções técnicas eficientes, de fácil utilização e com provas dadas no mercado.

O sistema de controle de acesso proposto visa o controle de entradas e saídas nas diversas dependências do edifício cujo acesso deve ser limitado a pessoas autorizadas. Estes locais são os indicados nas peças desenhadas do projeto.

Embora este projeto trate do SCA, a solução proposta deverá garantir a integração de módulos adicionais, a saber: SDAI e CFTV. A solução deverá assentar numa plataforma aberta que permita a gestão de equipamentos de diversos fabricantes, comunicando entre si através do protocolo TCP/IP sobre uma rede convencional.

Todos os componentes deverão ser geridos através de um único software, permitindo aos utilizadores gerir e interagir com os diferentes módulos utilizando a mesma interface gráfica, levando a uma uniformização das operações de segurança.

A solução a apresentar deverá ser tecnologicamente avançada e ter uma presença sólida no mercado Brasileiro, devendo ser indicadas pelo menos duas referências de grandes clientes institucionais com instalações de dimensão considerável.

Todo o sistema deverá apresentar, obrigatoriamente, características “future-proof”, ou seja, deverá garantir a continuidade de operação com as tecnologias disponíveis atualmente e também no futuro.

3.3.1 Arquitetura da Plataforma

O sistema a implementar deve assentar numa arquitetura cliente-servidor, permitindo que todas as configurações e registros de eventos e alarmes sejam guardados em bancos de dados relacionais SQL nos servidores. Desta forma, para além de centralizar o processamento, fica também assegurada a segurança do próprio sistema. A aplicação cliente servirá apenas de interface para o utilizador final.

Dependendo da dimensão final do sistema, os vários serviços poderão ser instalados numa única máquina ou em diferentes servidores de forma a distribuir o processamento e assegurar a continuidade do sistema em funcionamento.

No que tange ao armazenamento de dados, deverá ser possível definir um limite máximo de dias de retenção dos registros efetuados pelos leitores de controle de acessos, no caso vertente prevê-se nesta fase 30 dias. Ao fim desse período, todos os registros mais antigos serão eliminados ou marcados como não necessários, com a exceção dos registros que tenham sido protegidas pelos utilizadores. Neste caso os registros ficarão eternamente no sistema até que sejam desprotegidas.

O software de registros gravados deve permitir a pesquisa dos mesmos através de vários critérios como data, hora, alarmes, bookmarks e outros eventos do sistema.

Para facilitar o gerenciamento do sistema, deverão poder ser carregadas as plantas do edifício com o posicionamento dos diversos pontos monitorados e controlados (portas).

3.3.2 Descrição da Solução

O sistema é do tipo semi-descentralizado, permitindo assim ser alterado e/ou ampliado de forma fácil em função de alterações ou solicitações novas que venham a existir. A sua composição é a que se apresenta abaixo:

3.3.2.1 Controladores

As Unidades de Controle de Acesso destinam-se ao processamento de informações relativas ao cadastro de funcionários e visitantes, supervisão das Unidades de Controle Local e interligação ao servidor de controle de acesso.

São previstos dois tipos de controladores distintos, sendo um para controle das portas e outro para as catracas/cancelas.

3.3.2.2 Fechaduras eletromagnéticas

As fechaduras eletromagnéticas serão constituídas em aço inox e serão instaladas nas portas das salas controladas. As fechaduras serão acionadas externamente pelos leitores de cartão ou manualmente a partir do interior das salas, por meio de botões de pressão ou botoeiras de emergência.

3.3.2.3 Leitores

Os leitores serão responsáveis por acionar as fechaduras eletromagnéticas e liberar o acesso às salas controladas.

Os leitores serão do tipo biométrico e ficarão instalados na parte externa das salas. Serão constituídos por caixa de material termoplástico, próprios para montagem de sobrepor ou embutida na parede, não existindo qualquer tubulação aparente.

Os leitores para as catracas e cancelas deverão possibilitar a leitura de cartões ou biometria.

3.3.2.4 Botoeiras

As botoeiras de acionamento deverão ser instaladas na parte interna das salas controladas. Ao ser acionado, o botão enviará um comando à unidade de controle e esta acionará a fechadura eletromagnética para liberação da porta.

Em todas as portas com controle de acesso será prevista uma botoeira de emergência na cor verde, instalada no sentido de evacuação, que será responsável por realizar o corte da alimentação à fechadura / bloqueador magnético. A botoeira deverá contar com os dizeres: “Quebrar apenas em caso de emergência”.

3.3.2.5 Contato eletromagnético (sensor de abertura de porta)

Os contatos de abertura de porta são basicamente compostos por um micro-interruptor eletromagnético, enclausurados num invólucro metálico de construção hermética, o qual se destina a sinalizar o estado da porta (aberto/fechado).

3.3.2.6 Estações de Trabalho

A arquitetura de gestão de segurança que se preconiza para o sistema SCA prevê a instalação de duas Estações de Operação localizadas na recepção, permitindo o monitoramento do sistema de controle de acesso. As estações farão também o papel de Estação de Credenciamento, permitindo para efetuar o credenciamento de funcionários e visitantes.

3.3.2.7 Catracas e Cancelas

As catracas serão instaladas na recepção do edifício e serão destinadas ao controle de entrada de funcionários e visitantes. Serão de dois tipos:

- Comum - composta por três conjuntos;
- Especial composta por dois conjuntos, própria para acesso de portador de necessidades especiais.

As cancelas serão instaladas na entrada da rampa de acesso ao 1º subsolo.

3.3.2.8 Hardware e Software

O sistema que se propõe será composto de hardware, software e demais dispositivos necessários para o gerenciamento do sistema, garantindo todos os recursos associados a um sistema desta natureza, para implantação no edifício, como sendo:

- Cadastramento de usuários;
- Definição de níveis de acesso;
- Horários de acesso;
- Captação e consulta de dados, de fotos digitais, e de relatórios;
- Integração com os dispositivos de campo (leitoras, controladoras, fechaduras, etc.).

3.4 ALIMENTAÇÃO ELÉTRICA

O sistema elétrico para alimentação dos equipamentos será em 220 (FN) / 60Hz.

A alimentação elétrica da rede de controle de acesso será efetuada através de energia estabilizada ininterrupta (“no-break”), devendo apresentar uma arquitetura com os seguintes princípios básicos:

- Fonte de energia estabilizada;
- Energia imune a microcortes;
- Reserva Estratégica.