



---

# Memorial de Especificações de Materiais e Equipamentos – CONTROLE DE ACESSO

Brasília , 14 de agosto de 2008

---

*MPM – Ministério Público Militar*

Setor de Autarquia Sul • Quadra 03 • Bloco J • Brasília-DF • CEP 70.070-925

Tel. (61)3343.3226 • [www.mpm.gov.br](http://www.mpm.gov.br) • [da.sea@mpm.gov.br](mailto:da.sea@mpm.gov.br)



## Índice

<b>1.1 - CONCEITOS</b>	<b>3</b>
1.1.1 - Bloco 01	3
1.1.2 - Bloco 02	3
1.1.3 - Bloco 03	3
1.1.4 - Contratante	3
1.1.5 - Contratada	3
1.1.6 - Fiscalização	3
1.1.7 - Relação de Desenhos	4
1.1.7.1 - Arquitetura	4
1.1.7.2 - Segurança – Controle de Acesso	4
1.1.8 - SISTEMA DE PLATAFORMA INTEGRADA DE SEGURANÇA	5
<b>2 . SISTEMA DE CONTROLE DE ACESSO</b>	<b>6</b>
2.1 - DESCRITIVO	6
2.2 - APROVAÇÕES	6
2.3 - ESPECIFICAÇÃO DO SISTEMA DE CONTROLE DE ACESSO	7
2.4 - CARACTERIZAÇÃO E APLICAÇÃO	8
2.4.1 - SOFTWARE DE GERENCIAMENTO (PLATAFORMA INTEGRADA SEGURANÇA)	9
2.4.1.1 - RELATÓRIOS	10
2.4.1.2 - APRESENTAÇÃO DE ALARMES	11
2.4.1.3 - RASTREAMENTO DE CARTÃO DE ACESSO	12
2.4.2 - LEITORES DE PROXIMIDADE	12
2.4.3 - LEITORES DE PROXIMIDADE COM BIOMETRIA	12
2.4.4 - LEITORES DE PROXIMIDADE COM TECLADO	13
2.4.5 - CARTÕES DE PROXIMIDADE	13
2.4.6 - CONTROLADORAS REMOTAS	13
2.4.7 - FECHADURA ELETROMAGNÉTICA	14
2.4.8 - Cabos blindado com shield trançados par a par para comunicação de dados 20 awg	14
2.4.9 - Condutores elétricos	15
2.4.9.1 - Cabos Singelos com Isolação em PVC	15
2.4.9.2 - Cabos uni e multipolares não-propagantes de chama, livres de halogênios e baixa emissão de fumaça	15
2.4.10 - CATRACA BI-DIRECIONAL	16
2.4.11 - CAPTURA DE IMAGEM	16
2.4.11.1 - Software	16
2.4.11.2 - Hardware	16
2.4.11.3 - Câmera em Pedestal	16
2.4.12 - IMPRESSORA DE CARTÕES EM PVC	17
2.4.13 - SERVIDOR DO CONTROLE DE ACESSO	17
2.4.14 - NOBREAK PARA SERVIDOR	18
2.4.15 - SWITCH DE REDE PARA CONTROLE DE ACESSO	18
2.4.16 - WORKSTATIONS PARA CONTROLE DE ACESSO	18
2.4.17 - CANCELA PARA VEÍCULO	19
<b>3 . CONSIDERAÇÕES GERAIS</b>	<b>20</b>
3.1 - SISTEMA DE AUTOMAÇÃO E SUPERVISÃO PREDIAL	21
3.2 - PRAZO DE EXECUÇÃO	21
3.3 - GARANTIAS	21
3.4 - TREINAMENTOS	21



## INTRODUÇÃO

### 1.1 -CONCEITOS

---

#### 1.1.1 -BLOCO 01

---

- 1) Por bloco 01 entende-se o edifício sede da PJMDF mais à esquerda no croqui abaixo.

#### 1.1.2 -BLOCO 02

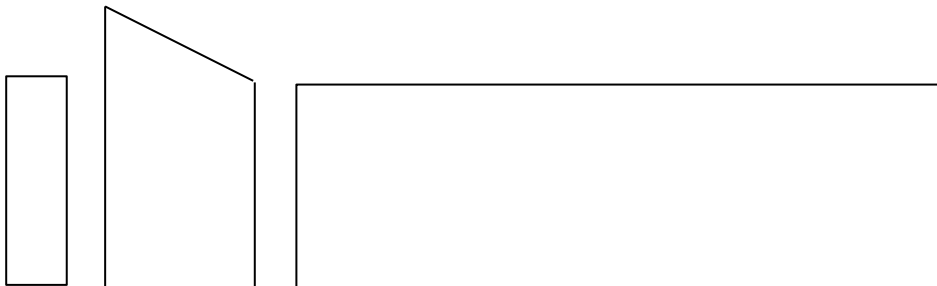
---

- 1) Por bloco 02 entende-se o edifício central onde estão localizados o auditório, restaurante, biblioteca e área médica).

#### 1.1.3 -BLOCO 03

---

- 1) Por bloco 03 entende-se o edifício maior, sede da PGJM, mais à direita no croqui abaixo.



**Bloco 01 Bloco 02**

**Bloco 03**

#### 1.1.4 -CONTRATANTE

---

- 1) Entende-se por Contratante o MINISTÉRIO PÚBLICO MILITAR.

#### 1.1.5 -CONTRATADA

---

- 1) Entende-se por Contratada a empresa executora dos serviços.

#### 1.1.6 -FISCALIZAÇÃO

---



- 1) Entende-se por Fiscalização o agente do Ministério Público Militar responsável pela verificação do cumprimento dos projetos, normas e especificações gerais dos serviços a serem executados.

## 1.1.7 -RELAÇÃO DE DESENHOS

### 1.1.7.1 -Arquitetura

Nº	PRANCHA	DESCRIÇÃO
1	A-01	PLANTA DE SITUAÇÃO
2	A-02	IMPLANTAÇÃO
3	A-03	PLANTA BAIXA – SS – TRECHO A
4	A-04	PLANTA BAIXA– SS – TRECHOS B e C
5	A-05	PLANTA BAIXA– TÉRREO – TRECHO A
6	A-06	PLANTA BAIXA– TÉRREO – TRECHOS B e C
7	A-07	PLANTA BAIXA– 1º PAV – TRECHO A
8	A-08	PLANTA BAIXA– 1º PAV – TRECHOS B e C
9	A-09	PLANTA BAIXA– 2º PAV – TRECHO A
10	A-10	PLANTA BAIXA– 2º PAV – TRECHOS B e C
11	A-11	PLANTA BAIXA– COBERTURA/ÁTICO – TRECHO A
12	A-12	PLANTA BAIXA– COBERTURA/ÁTICOS – TRECHOS B e C
13	A-13	CORTES A, B e C
14	A-14	CORTES D, E e F
15	A-15	CORTES G e H
16	A-16	CORTES I, J e K
17	A-17	ELEVAÇÕES 01 a 08 – COM BRISE
18	A-18	ELEVAÇÕES 01 a 08 – SEM BRISE
19	A - 19	SEÇÃO DO TERRENO
20	B-01	PLANTA DE FORRO – SS – TRECHO A
21	B-02	PLANTA DE FORRO – SS – TRECHOS B e C
22	B-03	PLANTA DE FORRO – TÉRREO – TRECHO A
23	B-04	PLANTA DE FORRO – TÉRREO – TRECHOS B e C
24	B-05	PLANTA DE FORRO – 1º PAV – TRECHO A
25	B-06	PLANTA DE FORRO – 1º PAV – TRECHOS B e C
26	B-07	PLANTA DE FORRO – 2º PAV – TRECHO A
27	B-08	PLANTA DE FORRO – 2º PAV – TRECHOS B e C
28	B-09	DETALHES GERAIS DE FORRO

### 1.1.7.2 -Segurança – Controle de Acesso

Nº	Planta	Descrição	Trecho	Pavimento
29	A-01	Planta baixa	A	Subsolo
30	A-02	Planta baixa	B	Subsolo
31	A-03	Planta baixa	C	Subsolo
32	A-04	Planta baixa	A	Térreo



33	A-05	Planta baixa	B	Térreo
34	A-06	Planta baixa	C	Térreo
35	A-07	Planta baixa	A	1º Pav
36	A-08	Planta baixa	B	1º Pav
37	A-09	Planta baixa	C	1º Pav
38	A-10	Planta baixa	A	2º Pav
39	A-11	Planta baixa	B	2º Pav
40	A-12	Planta baixa	C	2º Pav
41	A-13	Implantação		

### **1.1.8 -SISTEMA DE PLATAFORMA INTEGRADA DE SEGURANÇA**

- 1) Estas especificações referem se ao fornecimento e execução do sistema de controle de acesso.
- 2) O sistema de controle de acesso deverá ser totalmente integrado com o sistema de segurança e vigilância eletrônica, que compreende os sistemas de CFTV, controle de acesso, detecção de incêndio e supervisão predial. Todos os sistemas deverão ser **totalmente integrados** por protocolo Bacnet e Modbus de domínio público aberto, possibilitando, por exemplo, acionamento das câmeras móveis a partir de um alarme gerado pela central de controle de acesso, liberação das catracas dado um alarme da central de detecção de incêndio, etc.
- 3) O sistema de controle de acesso deverá ser integrado ao sistema de automação predial já adquirido para a edificação, conforme descrição constante no item 3.1 deste caderno, através de protocolo Bacnet e Modbus de domínio público aberto.
- 4) **A infra-estrutura necessária para a instalação dos sistemas está em execução. Será de responsabilidade da CONTRATADA, o acompanhamento dessa execução, adequando seu cronograma e o projeto executivo às necessidades reais da obra e para tanto deverá manter engenheiro electricista e encarregado em período integral no canteiro, a partir do 1º dia subsequente à data de expedição da Ordem de Execução.**
- 5) Será de responsabilidade da CONTRATADA a execução de todos os ajustes necessários à integração do sistema de controle de acesso com os outros sistemas de supervisão (CFTV, detecção e alarme de incêndio e automação predial), devendo para tanto, apresentar profissional qualificado a solucionar qualquer problema encontrado.



## 2 .SISTEMA DE CONTROLE DE ACESSO

### 2.1 -Descritivo

- 1) Deverá ser fornecido e instalado sistema de controle de acesso com o objetivo de controlar o acesso de pessoas, identificando-as, verificando autorizações (de local e horário), localizando-as e registrando os eventos para fins de auditoria.
- 2) Não farão parte dessa licitação os eletrodutos, caixas de passagem e eletrocalhas. Porém, a CONTRATADA terá que ajustar a infra-estrutura executada na obra às necessidades das instalações dos seus equipamentos, fazendo inclusive complementos às instalações existentes.
- 3) O banco de dados do sistema de controle de acesso deverá ser compartilhado com o Departamento de Recursos Humanos, a fim de ser trabalhado pelo software Grifô, para fins de ponto eletrônico.
- 4) A CONTRATADA deverá instalar todos os equipamentos, conectores, cabos, fontes etc., destinados ao perfeito funcionamento do sistema proposto.
- 5) A infra-estrutura necessária à instalação do sistema está em execução. Para realizar os trabalhos, a CONTRATADA deverá adequar seu cronograma ao desenvolvimento real da obra.
- 6) O CONTRATANTE poderá participar, mediante solicitação, dos testes/ensaios de operação dos equipamentos.
- 7) As marcas/modelos de equipamentos/sistemas informados neste caderno de encargos são de referência, podendo ser ofertados marcas/modelos similares. Nesse caso, a critério da CONTRATANTE, poderá ser exigida, **após a fase de lances ou na fase de execução contratual**, a comprovação de similaridade. Essa comprovação dar-se-á mediante apresentação, pela licitante detentora do melhor lance ou pela CONTRATADA, conforme o caso, e com ônus para estas últimas, de laudo técnico expedido por laboratório ou instituto idôneo.

### 2.2 -Aprovações

- 1) O sistema **deverá obrigatoriamente** ter certificações apropriadas de pelo menos uma das certificadoras abaixo:
- 2) UL;
- 3) IEEE;
- 4) CE;
- 5) FCC;
- 6) EIA;
- 7) INMETRO.
- 8) A CONTRATADA deverá apresentar documentação pertinente, atestados, certificações acima descritas com vistas a comprovar que o sistema a ser fornecido atende integralmente ao item acima.



## 2.3 -ESPECIFICAÇÃO DO SISTEMA DE CONTROLE DE ACESSO

---

- 1) O sistema de gerenciamento de controle de acesso deverá usar uma arquitetura cliente-servidor baseada em uma rede modular de computadores pessoais (PC), empregando sistemas operativos, redes e protocolos Standard da indústria.
- 2) 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 maior flexibilidade e rendimento.
- 3) O Sistema deve estar baseado em uma solução de software que permita um gerenciamento integrado da segurança, através de rede corporativa LAN/WAN, onde o usuário poderá acessar as mesmas informações a que teria acesso na central de segurança a partir de qualquer estação de trabalho que esteja conectada à rede, sem limite de conexões.
- 4) O Sistema deve permitir aos administradores controlar o acesso a cada função do sistema, atribuindo permissões aos operadores e usuários ou grupos de usuários cadastrados.
- 5) A arquitetura deverá incluir suporte para vários tipos de rede usando o hardware e software Standard para interconectar os nodes, formando um só sistema integrado.
- 6) O protocolo de rede a ser utilizado deverá ser o Standard da industria TCP/IP. O sistema deverá suportar também configurações e operações remotas usando modems convencionais (dial-up).
- 7) O servidor deverá ser capaz de interconectar-se com os seguintes tipos de painéis:
  - a. Painéis Controladores de Acesso;
  - b. Painéis Controladores de sistema de segurança;
  - c. Comutadores de sistema de CFTV;
  - d. Painéis de detecção e alarme de Incêndio;
  - e. Painéis Controladores do sistema de automação predial.
- 8) A comunicação com os painéis controladores de acesso deverá ser feita através de protocolo TCP-IP, via rede LAN/WAN. O sistema deverá integrar com os demais sistemas de Segurança tais como: Sistemas de Alarmes, Central de Monitoramento e Gravação de Imagem Digital. A técnica de interface elétrica para integração a estes painéis deverá estar de acordo com os Standards EIA RS-422 e ou RS-232 e ou RS-485.
- 9) Todas as controladoras do sistema de controle de acesso **deverão obrigatoriamente possuir processadores de 32 bits e ter inteligência distribuída**. As decisões normais de controle de acesso nos painéis localmente deverão ser tomadas automaticamente, sem interferência do servidor.
- 10) Em caso de falha na rede de comunicação entre um painel e o servidor, as controladoras locais de acesso deverão armazenar temporariamente um mínimo de **20.000 cartões de acesso e 5.000 transações** até que a comunicação com o servidor seja restabelecida.
- 11) As mudanças na base de dados do servidor do sistema serão descarregadas nos controladores de acesso apropriados e na base de dados dos sub-sistemas conectados através do mesmo meio físico de comunicação. Tal descarga deve ser realizada em tempo real e não poderá afetar a normal comunicação de dados sobre o mesmo enlace.



- 12) Todas as regras de negócio e os dados funcionais deverão estar armazenados em um servidor de Aplicação e em um servidor de Banco de Dados. A transferência das informações de acesso para as Controladoras deverá ser atualizada periodicamente, de uma única vez, não devendo ser necessária a consulta ao Banco de Dados para liberação ou autorização de acesso, com isso o sistema fica operando mesmo que a comunicação com o servidor seja interrompida.
- 13) A arquitetura de software do Sistema de Acesso deverá ter compatibilidade com todos os principais Browsers. **Utilizar MS SQL2000 como Banco de Dados e Windows como sistema operacional.**
- 14) O bloqueio do sistema de Controle de Acesso deverá ser feito através de fechaduras elétricas, fechaduras eletromagnéticas, catracas, cancelas, torniquetes, baias ópticas, etc., conforme indicado em projeto. Cada usuário receberá um código numérico único que poderá ser uma senha numérica e/ou um cartão. Dessa forma, quando o usuário acessa o ponto de controle (digitando sua senha no teclado ou passando seu cartão pelo leitor ou ainda utilizando sua identificação biométrica), o sistema de controle de acesso verifica se esse usuário está autorizado a entrar naquele local e naquele horário e somente após essa verificação o acesso é liberado.
- 15) O sistema de controle de acesso deverá ser integrado ao sistema de CFTV, de forma que eventos de tentativas de acesso negado em áreas de segurança pré-estabelecidas em projeto, gerem ações imediatas de “Pop UP” de imagem da câmera de vídeo mais próxima ao evento para o monitor principal, inicie um processo de gravação em resolução diferenciada, gere alarme com os procedimentos a serem tomados pelo operador, bem como disponibilize relatório das tentativas de acesso com data e hora para uma posterior auditoria.
- 16) Com a Integração pode-se identificar, por exemplo, um acesso não autorizado em horário não permitido, trazendo a foto do usuário do cartão em conjunto com o vídeo ao vivo diretamente no software, de modo a possibilitar a verificação se a pessoa da foto é a mesma do vídeo.
- 17) Os fechos magnéticos serão do tipo eletroímã de alta resistência, alimentados por corrente contínua a partir de um quadro elétrico (QDEE), que deverá ser instalado na Sala de Controle, com circuitos de distribuição para as portas, conforme indicado em projeto.
- 18) Um conjunto de portas consecutivas que formam uma eclusa será eletricamente intertravado ou via software, através de dispositivos que impeçam a abertura simultânea das duas portas que constituem uma eclusa.
- 19) Foi previsto (onde não houver leitoras de saída) a instalação de botoeiras de pressão retornáveis à posição normalmente fechada, através de mola incorporada possibilitando a abertura da porta pelo lado interno. Esses dispositivos serão alojados em caixa de 4x2 com espelho em aço escovado (um protótipo deverá ser montado para a aprovação da FISCALIZAÇÃO).
- 20) O banco de dados do sistema de controle de acesso deverá ser compartilhado com o Departamento de Recursos Humanos, a fim de ser trabalhado pelo software Grifo, para fins de ponto eletrônico.
- 21) O software Grifo, que fará o controle de ponto dos servidores na nova sede da PGJM, utiliza MS SQL2000 como Banco de Dados e Windows como sistema operacional. A comunicação entre os sistemas será através de rede corporativa TCP/IP.
- 22) O sistema de controle de acesso deverá exportar os dados de acesso à edificação para o servidor rede localizado no DRH.
- 23) O software Grifo não faz parte do escopo desse contrato.

## **2.4 -CARACTERIZAÇÃO E APLICAÇÃO**



- 1) O Sistema de Controle de acesso deverá ser composto pelos seguintes elementos:
  - a. Software de Gerenciamento
  - b. Leitoras de Proximidade
  - c. Leitoras de proximidade com PIN
  - d. Leitoras de Proximidade com Biometria
  - e. Cartão HIBRIDO Smartcard Contactless Mifare, memória de 1Kbits e Proximidade
  - f. Captura de imagem dos visitantes
  - g. Controladoras Remotas
  - h. Catracas
  - i. Fechaduras Eletromagnéticas

#### **2.4.1 -SOFTWARE DE GERENCIAMENTO (PLATAFORMA INTEGRADA SEGURANÇA)**

O software deverá ter as seguintes características, bem como possibilitar as atividades descritas a seguir:

- 1) Interface Gráfica que fará uso de ícones, de maneira que minimize a digitação de comandos.
- 2) Banco de dados compatível com MS SQL2000.
- 3) Compatível com Windows XP/ 2000 Server.
- 4) Possibilidade de operação em rede com até 40 conexões simultâneas.
- 5) Definição de tabelas horárias para restrição e permissão de acessos aos locais controlados.
- 6) Definição de Níveis de acesso específicos para cada cartão programado no sistema.
- 7) Possibilidade de cadastramento de fotos por usuário.
- 8) Cadastramento de cartões para prestadores de serviço com possibilidade de programação da data de expiração e de ativação.
- 9) Restrição de acesso ao software através de senhas e níveis para os operadores.
- 10) Auditoria sobre as atividades dos operadores no software.
- 11) Software disponível em diversos idiomas incluindo: inglês, português e espanhol.
- 12) Visualização da foto e dados do usuário através de um computador com o software no momento da passagem do cartão pelo leitor.
- 13) Permitir ao operador enviar comandos às Unidades Remotas, para a atuação nos dispositivos de controle no campo tais como fechaduras, catracas, relês, etc.
- 14) Emissão de relatórios baseados em diversos tipos de filtros.
- 15) Possibilidade de exportação de dados gerados nos relatórios em diversos formatos tais como: Excel, Texto, Access, etc.
- 16) Monitoramento e operação do sistema através de Telas Sinópticas importadas no padrão \*.wmf (Windows Metafiles).
- 17) Localização Rápida de usuários através do Nome ou número do cartão.
- 18) Aplicativo que permite a elaboração e impressão de crachás personalizados.
- 19) Monitoramento de eventos de acessos, alarmes e imagens de CFTV de qualquer estação cliente do software.
- 20) Cadastro de funcionários e visitantes com nome, sobrenome, foto, foto do documento e ainda 40 campos auxiliares de notas definidos pelo cliente.
- 21) Recuperação do cadastro de um visitante no momento de uma nova visita.
- 22) Levantamento da identificação dos usuários que tiveram solicitações de acesso negadas.



- 23) Programação de horários de acesso permitido ou negado em função do horário, do dia (dias úteis, fins de semana, feriados, etc.), das características do usuário, do usuário em si, etc.
- 24) Programação de categorização do usuário para fins de acesso a um determinado recinto.
- 25) Restrição de acesso ao software através de senhas e níveis de acesso para os operadores.
- 26) Auditoria sobre todas as atividades do operador no software.
- 27) Possibilidade de definição de data de ativação e validade de um cartão de acesso.
- 28) Solicitação de senha de acesso de um cartão no caso de áreas de segurança.
- 29) Alarme e indicação da leitora de cartões em que foi tentado um acesso com cartão cancelado.
- 30) Indicação do motivo pelo qual a solicitação de acesso não foi concedida (local não autorizado, horário não autorizado, senha inválida, site code inválido, etc.).
- 31) Particionamento do Banco de Dados em contas permitindo assim aplicações Multi-Empresas.
- 32) Telas de operação do software em português.
- 33) Indicação de acessos às áreas de segurança, nome do usuário, data e hora e local acessado (sala de equipamento, subestação, etc.).
- 34) Recurso de visualização de foto e dados do usuário de cartão através de qualquer estação do software no momento do acesso em um determinado local.
- 35) Integração com sistemas de CFTV e alarme de intrusão possibilitando o monitoramento e operação destes sistemas pelo software aplicativo.
- 36) Comando e visualização de câmeras de matrizes de CFTV através do software aplicativo, possibilitando o comando de movimentação de câmeras PTZ, chaveamento de câmeras para monitores analógicos, visualização de câmeras ao vivo através da tela de operação do Software Aplicativo, chamada de preset's, etc.
- 37) Comando e visualização de câmeras de gravadores digitais de vídeo (DVRs) via rede Ethernet através do Software Aplicativo, possibilitando a visualização de câmeras ao vivo, visualização de gravações antigas, comando de câmeras PTZ, chamada de preset's.
- 38) Comando automático via RS-232 dos equipamentos de CFTV baseado em eventos do controle de acesso.
- 39) Possibilidade de interfaces com o operador, através de quadros sinópticos dos locais com controle de acesso, em telas gráficas coloridas de múltiplos níveis que permitam o "zoom" de uma determinada área, controle e monitoramento de dispositivos tais como portas, catracas, câmeras, DVR's, Matrizes de CFTV, sensores, relês, etc.
- 40) Integração com painéis de Alarme de Intrusão e Incêndio, possibilitando a operação destes sistemas via Planta Baixa Digitalizada.
- 41) Possibilidade de gerenciamento e controle de um número ilimitado de Unidades Remotas (UR), leitores de acesso, entradas de alarme, câmeras, DVR's e saídas a relês.
- 42) Possibilidade de programação de rondas de guarda baseado e leitores de acesso e pontos de alarme.

#### **2.4.1.1 -RELATÓRIOS**

---

- 1) O sistema deverá possibilitar que, sob comando do operador sejam emitidos, no mínimo, os seguintes relatórios padrões:
  - a. Por pessoas;
  - b. Por cartões;
  - c. Por configuração;



- d. Por status de dispositivos;
  - e. Por informações históricas;
  - f. Por atividades de cartão;
  - g. Por um dos 40 campos de notas definidos pelo cliente;
  - h. Por atividade de alarme;
  - i. Por atividade de operador (capacidade de auditar um operador).
- 2) A geração de relatórios não deverá causar qualquer degradação no desempenho do sistema.
  - 3) O editor de relatórios deverá possibilitar o agrupamento e a seleção de relatórios por qualquer campo dentro dos mesmos e também a possibilidade de "salvar" um relatório como uma "macro" (uma seqüência automática de relatórios), a qual será definida pelo operador com um nome único. O editor de relatórios deverá possibilitar que com o uso de "macros" se elabore relatório complexo de forma simples e rápida.
  - 4) Deverá haver a possibilidade de exportação dos relatórios em diversos formatos, tais como xls, txt, doc, etc.
  - 5) O usuário poderá programar para que os relatórios sejam executados automaticamente, uma vez, diariamente, semanalmente ou mensalmente.
  - 6) O software deverá enviar os relatórios gerados automaticamente para os e-mails previamente cadastrados.

#### **2.4.1.2 - APRESENTAÇÃO DE ALARMES**

O sistema deverá ter as seguintes características, bem como possibilitar as atividades descritas a seguir:

- 1) Uma caixa/janela inicial de apresentação de alarmes deverá identificar de forma automática e inconfundível os novos alarmes e seus graus de prioridade. A apresentação dos alarmes na tela do monitor será acompanhada de uma indicação sonora diferente para cada tipo de alarme, sendo que para sua desativação será necessária a intervenção do operador.
- 2) Cada alarme poderá ser categorizado com prioridade variando de 1 (Prioridade Máxima) até 99 (Prioridade Mínima). Deverá ser possível determinar o nível de prioridade a partir do qual os alarmes necessitarão de reconhecimento e confirmação por parte do operador.
- 3) Deverá ser possível programar mensagens de instruções e procedimentos para o operador em função de cada alarme.
- 4) Para que um alarme seja reconhecido haverá a intervenção do operador. O reconhecimento de alarmes deverá ser permitido a partir da tela de apresentação inicial, ou a partir de qualquer nível de hierarquia de apresentação de alarmes. O reconhecimento de um alarme deverá requerer, para todas as indicações de condição de alarme, que o referido alarme esteja no estado de reconhecimento.
- 5) O sistema deverá permitir que o operador possa editar um parecer relativo à causa do alarme e/ou editar informações adicionais em uma janela de edição de texto da tela de alarmes, as quais deverão ser anexadas obrigatoriamente aos registros de alarmes do sistema.
- 6) A remoção de qualquer alarme de uma lista de alarmes ativos só poderá ocorrer através de ação do operador.
- 7) Na ocorrência de um alarme, o operador poderá selecionar a linha deste evento e visualizar a planta do local ou então a imagem de uma câmera que estiver associada a este alarme. O



- operador poderá escolher se deseja visualizar a imagem ao vivo ou a gravação do evento de alarme acessando as imagens armazenadas nos DVR's via rede Ethernet TCP/IP.
- 8) Todas as informações de alarmes, inclusive data e hora das ocorrências, deverão ser armazenadas no banco de dados do sistema.
  - 9) Qualquer mau funcionamento e anormalidades relacionadas com as UR (Unidades Remotas), linhas de comunicações e demais periféricos/dispositivos do sistema, deverão ser apresentadas ao operador.

#### **2.4.1.3 - RASTREAMENTO DE CARTÃO DE ACESSO**

---

Quanto ao rastreamento, o sistema deverá ter as seguintes características, bem como possibilitar as atividades descritas a seguir:

- 1) O sistema deverá permitir o acompanhamento, em toda a área controlada, de determinados cartões previamente selecionados, registrando, de forma diferenciada (data, hora, local) os seus deslocamentos.
- 2) O sistema deverá possibilitar a procura rápida do último acesso de um determinado usuário de cartão.
- 3) Fabricante de referência: WINPAK PE/LOBWORKS HONEYWELL ou similar.
- 4) Aplicação: Gerenciamento controle acesso

#### **2.4.2 - LEITORES DE PROXIMIDADE**

---

Os leitores de proximidade deverão possuir as seguintes características mínimas:

- 1) Alcance de leitura de até 10 cm.
- 2) Sinalização audio-visual indicando o reconhecimento do cartão.
- 3) Sinalização audio-visual indicando a liberação do acesso.
- 4) Capacidade de identificação da retirada do leitor de seu local de instalação, informando no software situações de vandalismo.
- 5) Possibilidade de escolha da cor do leitor, adequando-o assim às características decorativas existentes no ambiente de instalação.
- 6) Fabricante de referência: PRMINIPROX- Honeywell ou similar.
- 7) Aplicação: Leitora do sistema de controle de acesso

#### **2.4.3 - LEITORES DE PROXIMIDADE COM BIOMETRIA**

---

Os leitores de proximidade com biometria deverão possuir as seguintes características mínimas:

- 1) Alcance de leitura de até 10 cm.
- 2) Sinalização audiovisual indicando o reconhecimento do cartão.
- 3) Sinalização audiovisual indicando a liberação do acesso.
- 4) Capacidade de identificação da retirada do leitor de seu local de instalação. Informando no software situações de vandalismo.
- 5) Algoritmo FVC2002 & 2004
- 6) Capacidade de cadastro de até 4.000 traços biométricos.



- 7) Taxa de Falso Aceite máxima de 1:1.000.000 e Taxa de Falsa Rejeição inferior a 0,5%.
- 8) O tempo de identificação biométrica (busca 1:1) deverá ser de, no máximo, 3 segundos, e o de liberação deverá ser de, no máximo, 2 seg.
- 9) Sensor de leitura biométrica de impressões digitais de captura ótica com resolução mínima de 500 dpi. Área de captura mínima: 13 x 17 mm; detecção automática da presença do dedo sobre o dispositivo. Capacidade de desconsiderar impressões latentes.
- 10) Não deve sofrer interferência causada por incidência de luzes internas e/ou externas.
- 11) Superfície de captura deverá ser resistente a mais de 100 milhões de toques.
- 12) Fabricante de referência: PRMINIPROX-K HONEYWELL ou similar.
- 13) Aplicação: Leitora do sistema de controle de acesso

#### **2.4.4 -LEITORES DE PROXIMIDADE COM TECLADO**

---

Os leitores de proximidade com teclado deverão possuir as seguintes características mínimas:

- 1) Alcance de leitura de até 10 cm.
- 2) Sinalização audiovisual indicando o reconhecimento do cartão.
- 3) Sinalização audiovisual indicando a liberação do acesso.
- 4) Capacidade de identificação da retirada do leitor de seu local de instalação, informando no software situações de vandalismo.
- 5) Possibilidade de escolha da cor do leitor adequando-o assim as características decorativas existentes no ambiente de instalação.
- 6) Fabricante de referência: PRMINIPROX-K HONEYWELL ou similar.
- 7) Aplicação: Leitora do sistema de controle de acesso

#### **2.4.5 -CARTÕES DE PROXIMIDADE**

---

Os cartões de proximidade deverão possuir as seguintes características mínimas:

- 1) Cartão HIBRIDO Smartcard Contactless Mifare, memória de 1Kbits e proximidade combinado em PVC, sem logo.
- 2) Ser resistente e Durável.
- 3) Possibilidade de colagem de PVC auto-adesivo com impressão do crachá do usuário.
- 4) Fabricante de referência: MARTPROX HONEYWELL ou similar.
- 5) Aplicação: Cartão do sistema de controle de acesso.

#### **2.4.6 -CONTROLADORAS REMOTAS**

---

As controladoras remotas deverão possuir as seguintes características mínimas:

- 1) Arquitetura Modular, expansível até 64 leitoras.
- 2) Cada controladora deverá ter capacidade de gerenciar uma combinação de até 32 Módulos de expansão bastando para isso adicionar os módulos que poderão ser: Módulos para 2 leitores, Módulos para 16 entradas Digitais e Módulos para 16 Saídas via Relê.
- 3) Ser compatível com a maioria das tecnologias de leitores, tais como: Proximidade, Magnético, Código de barras, Biométricos, Wiegand, Smart Card e Leitores RF para controle de frota de veículos.



- 4) Cada controladora deverá ter processador de 32 bits e ser dotada de base de dados que permita a operação autônoma.
- 5) Memória para até 100.000 usuários e 35.000 eventos.
- 6) Possibilidade de operação completa em caso de perda de conexão com o Servidor.
- 7) Possibilidade de Comunicação em RS-485, RS-232 ou via rede TCP/IP.
- 8) Possibilidade de programação automática dos relês baseada em Janelas de Tempo dos relês para acionamentos automáticos.
- 9) Possibilidade de monitorar a abertura da caixa do painel (tamper).
- 10) Sistema de backup de alimentação próprio com carregador de bateria interna que possibilita o funcionamento do painel por até 5 horas em caso de queda da alimentação primária.
- 11) Em caso de queda da alimentação primária e da Bateria de Backup, o painel deverá manter em sua memória toda configuração nele armazenada.
- 12) Possibilitar o monitoramento dos sensores das portas com definição de tempo de abertura.
- 13) 9-dígitos (32-bit) identificação de usuário padrão e 15 dígitos máximos.
- 14) Incluir ou excluir os campos da base de dados durante a configuração para maximizar o uso de memória.
- 15) Ativação e desativação de datas por cartão.
- 16) Capacidade de configurar até 32 níveis de acesso por cartão ou individual período de tempo por leitora.
- 17) O formato "anti-pass-back" poderá ser configurado para operar em um dos três modos abaixo conforme necessidade do CLIENTE:
  - a. Modo Leve: Permite ao usuário a dupla entrada/saída, mas informa no software que houve a violação;
  - b. Modo Rígido: Não permite ao usuário a dupla entrada/saída; ou
  - c. Modo Temporizado: Permite ao usuário a dupla entrada/saída depois de um certo tempo programável;
- 18) Capacidade de atribuir até 8 dígitos de senha por usuário.
- 19) Modelo de referência: PW5000 HONEYWELL ou similar.
- 20) Aplicação: Hardware do sistema de controle de acesso

#### **2.4.7 - FECHADURA ELETROMAGNÉTICA**

---

A fechadura eletromagnética deverá possuir as seguintes características mínimas:

- 1) Força de atraque de 200 Kgf.
- 2) Sensor de porta imbutido
- 3) Led indicativo de operação
- 4) Possibilidade de adequar-se ao tipo de porta na qual será instalado.
- 5) Fabricante de referência: SIBRAG ou similar.
- 6) Aplicação: Hardware do sistema de controle de acesso.

#### **2.4.8 - CABOS BLINDADO COM SHIELD TRANÇADOS PAR A PAR PARA COMUNICAÇÃO DE DADOS 20 AWG**

---

Os cabos para transmissão de dados deverão possuir as seguintes características mínimas:



- 1) Condutor interno: Corda de fios de cobre estanhado.
- 2) Isolação: Polietileno 70°
- 3) Blindagem: Coletiva, composta por Fita de Poliéster / Alumínio + Trança de fios de cobre estanhado.
- 4) Cobertura: PVC Classe Térmica 70° C.

## **2.4.9 -CONDUTORES ELÉTRICOS**

---

Os condutores elétricos deverão possuir as seguintes características mínimas:

- 1) Os tipos de condutores deverão sempre obedecer às restrições da NBR 5410/2004 quanto aos condutores permitidos nas diversas linhas elétricas.
- 2) Toda instalação deverá estar em conformidade com os requisitos da NBR 5410 item 6.2.11 para seleção dos cabos de acordo com o tipo de linha elétrica.
- 3) A identificação dos cabos, por meio de anilhas, deverá ser executada a cada 3 metros. Para circuitos terminais a identificação dos cabos deverá ser executada em cada caixa de passagem e em linhas elétricas abertas (eletrocalhas, perfilados, etc) a cada 2 metros.

### **2.4.9.1 -Cabos Singelos com Isolação em PVC**

---

- 1) Para baixa tensão, terão condutores em cobre nu, têmpera mole, encordoamento classe 2, com isolamento em PVC, sem chumbo e livre de halogênios, com características de não propagação e auto-extinção de fogo, tensão de isolamento 450/750V. Deverá operar para as seguintes temperaturas máximas: 70° C em serviço contínuo, 100° C para sobrecarga e 160° C para curto circuito.
- 2) Deverão obedecer às prescrições da NBR NM247 (partes 1, 2 e 3).
- 3) Quando não tiverem capa protetora, deverão obedecer às prescrições da NBR 6148. Nos casos em que tenham capa protetora deverão obedecer às prescrições da NBR 7288.

### **2.4.9.2 -Cabos uni e multipolares não-propagantes de chama, livres de halogênios e baixa emissão de fumaça**

---

- 1) Deverão ter capa protetora e obedecer às prescrições da NBR 13248. Terão condutores em cobre nu, têmpera mole, encordoamento classe 5, com isolamento em composto termofixo em dupla camada de borracha HEPR (EPR/B-alto módulo), enchimento de composto poliolefilico não halogenado, cobertura constituída por composto termoplástico com base poliolefilico não halogenada, com características de não propagação e auto-extinção.
- 2) Tensão de isolamento 0,6/1kV.
- 3) Deverá operar para as seguintes temperaturas máximas: 90° C em serviço contínuo, 130° C para sobrecarga e 250° C para curto circuito.
- 4) Para todos os casos acima devem ser atendidas todas as exigências das normas complementares para cada caso específico.
- 5) Para cabos singelos, a isolamento terá obrigatoriamente cor azul claro para o neutro, verde para condutor de proteção (TERRA).
- 6) Nos casos onde a cobertura do condutor não permitir a sua identificação por cores (inexistência

---

**MPM – Ministério Público Militar**

Setor de Autarquia Sul • Quadra 03 • Bloco J • Brasília-DF • CEP 70.070-925

Tel. (61)3343.3226 • [www.mpm.gov.br](http://www.mpm.gov.br) • [da.sea@mpm.gov.br](mailto:da.sea@mpm.gov.br)



no mercado), para os casos específicos de neutro e terra, a identificação dos mesmos deverá ser executada por meio de instalação de anilhas específicas e apropriadas que garantam a identificação destas funções nos seus respectivos circuitos, conforme prescrito na NBR 5410.

- 7) Em nenhuma hipótese será permitido o emprego de condutores rígidos (fio), devendo ser empregados obrigatoriamente cabos com encordoamento concêntrico.

## **2.4.10 - CATRACA BI-DIRECIONAL**

---

A catraca bi-direcional deverá possuir as seguintes características mínimas:

- 1) Catraca eletrônica, bidirecional, tipo Portal de Bloqueio Autotravado, de operação suave, com display, pictogramas ou LED(s) de operação e orientação, acabamento em aço inox escovado.
- 2) Mecanismo que proporcione uma operação suave, silenciosa.
- 3) Tampo e portinholas providos de fechos tipo Castelo ou chave tipo Yale, para limitar o acesso ao mecanismo.
- 4) Estrutura confeccionada em aço inox escovado.
- 5) Acabamentos frontais, laterais e portal em aço inox escovado.
- 6) Fonte de alimentação – “Full Range” (tensão de 90 a 230 VAC; frequência 50/60Hz).
- 7) Operação integrada com as Controladoras de Acesso.
- 8) Pictogramas ou LED(s) que indicam acesso permitido ou acesso bloqueado em cores diferentes.
- 9) Fabricante de referência: WOLPAC ou similar.
- 10) Aplicação: Bloqueio do sistema de controle de acesso

## **2.4.11 -CAPTURA DE IMAGEM**

---

O software de captura de imagem deverá ser composto pelos seguintes elementos mínimos:

### **2.4.11.1 -Software**

---

- 1) Software de captura com drive para o sistema de controle de acesso;
- 2) Compatível com Windows 2000/XP,
- 3) Formato de gravação das imagens: JPEG com nível de compressão configurável;
- 4) Tamanho do quadro de imagem gravada: 640x480 e 320x240 configuráveis.

### **2.4.11.2 -Hardware**

---

- 1) Placa de captura com barramento PCI; Resolução de 320x240 e 640x480 configuráveis;
- 2) Apresentação de vídeo em 30 fps;
- 3) Dois canais independentes de entrada de vídeo e conexão RCA.

### **2.4.11.3 -Câmera em Pedestal**

---

- 1) Câmera colorida, CCD, padrão NTSC, 12 VDC, BLC;
- 2) Pedestal metálico articulado, cabeamento embutido;



- 3) Dispositivo de alimentação incluso.
- 4) Fabricante de referência: LWVMDOME HONEYWELL ou similar.
- 5) Aplicação: Hardware do sistema de controle de acesso

#### **2.4.12 -IMPRESSORA DE CARTÕES EM PVC**

---

A impressora de cartões em PVC deverá possuir as seguintes características mínimas:

- 1) Impressão monocromática e colorida.
- 2) Impressão automática dos dois lados.
- 3) Modo de Impressão: Sistema de Fitas de impressão integrado.
- 4) Velocidade de Impressão: 140 cartões/hora modo colorido um lado; 110 cartões/hora modo colorido dois lados; 1000 cartões/hora modo monocromático um lado; 350 cartões/hora modo monocromático dois lados. Resolução: 300 dpi.
- 5) Windows NT 4/2000; Driver com Guia de Desenvolvimento para desenvolvedores de Software Próprio. Software para edição e design para cartões PVC.
- 6) Capacidade de armazenamento: 100 cartões (0,76mm).
- 7) Ajuste de espessura variável: 0,25 a 1,00mm. Ref.: Evolis, Tipo Dualys Basic ou similar.
- 8) Fabricante de referência: Dualys Basic ou similar.
- 9) Aplicação: Confecção crachá do sistema de controle de acesso

#### **2.4.13 -SERVIDOR DO CONTROLE DE ACESSO**

---

O servidor de controle de acesso deverá possuir as seguintes características mínimas:

- 1) 2 Processadores Intel Xeon E5410 Quad-Core de 2.33 GHz com 2 x 6 MB de memória Cache (1333 FSB)
- 2) Processador com tecnologia EM64T
- 3) 4 GB de memória Fully Buffered Dimm (FBD), 667 MHz (4 x 1 GB)
- 4) 03 discos rígidos de 73GB SAS 3.5" de 15.000 rpm
- 5) Backplane para 6 discos rígidos de 3,5"
- 6) Controladora de array integrada SAS 3Gb/s para até 6 discos, com 256 MB de memória cache ECC e com bateria (PERC6/i)
- 7) 2 Interfaces de rede 10/100/1000 UTP Onboard
- 8) Adaptador para conversão USB/PS-2
- 9) Software de gerenciamento Dell Open Manage
- 10) Painel Frontal (Bezel)
- 11) Riser com 3 slots PCI-e
- 12) 2 Placas de rede Broadcom NetXtreme 5721 Single Port (PCIe x1)
- 13) Fonte de alimentação redundante com dois cabos de força
- 14) Unidade de 24x CDRW/DVD
- 15) Sem unidade de disco flexível
- 16) Mouse Ótico USB 2 botões com scroll e teclado USB
- 17) Monitor LCD 19"



- 18) Gabinete de 2U com trilhos para rack padrão 19"
- 19) Sistema Operacional Windows 2003 Standard Server 32/64 bits R2 em Português
- 20) 5 CALs para Windows Server 2003 32/64 bits
- 21) MICROSOFT SQL2000 SERVER.**
- 22) Modelo de referência: **PowerEdge 2950 III** DELL ou similar.
- 23) Aplicação: Servidor do sistema de controle de acesso

#### **2.4.14 -NOBREAK PARA SERVIDOR**

---

O nobreak para servidor deverá possuir as seguintes características mínimas:

- 1) No-Break APC Smart de 2.000VA - 220V
- 2) Gabinete de 2U para montagem em Rack
- 3) Modelo de referência: **UPS 2 KVA 220V** DELL ou similar.
- 4) Aplicação: Servidor do sistema de controle de acesso.

#### **2.4.15 -SWITCH DE REDE PARA CONTROLE DE ACESSO**

---

O switch de rede para controle de acesso deverá possuir as seguintes características mínimas:

- 1) Switch de rede 24 portas 10/100/1000 UTP + 2 porta para conexão de fibra óptica.
- 2) Slots combo 1000BaseT / SFP (para conexão com fibra ótica), gerenciável via Web.
- 3) Modelo de referência: **PowerConnect 2724** DELL ou similar.
- 4) Aplicação: Servidor do sistema de controle de acesso.

#### **2.4.16 -WORKSTATIONS PARA CONTROLE DE ACESSO**

---

As workstations para controle de acesso deverão possuir as seguintes características mínimas:

- 1) Workstation com a seguinte configuração mínima:
- 2) Processador: Processador Intel® Xeon®
- 3) Sistema operacional: Windows® XP Professional Original
- 4) Memória: 1024 MB de memória RDRAM dual-channel (capacidade para até 4GB)
- 5) Placa de vídeo: 8X AGP Pro 110, com 256 MB de memória incorporada e sinal de saída de vídeo para TV.(BNC)
- 6) Rede: Interface de Rede 10/100/1000 Gigabit Integrada
- 7) Disco rígido: SCSI Ultra320 até 120GB
- 8) Gravador de DVD-RW
- 9) Fabricante de referência: DELL ou similar.
- 10) Visualização e monitoramento do Sistema de acesso.



## 2.4.17 -CANCELA PARA VEÍCULO

---

A cancela para veículo deverá possuir as seguintes características mínimas:

- 1) Cancela tipo pedestal com “Totem” para instalação da leitora de cartão de proximidade.
- 2) Corpo em aço carbono pintado na cor grafite à prova de intempéries.
- 3) Retorno do braço controlado por amortecedor hidráulico com dispositivo antiesmagamento.
- 4) Abertura vertical articulada, comprimento de 3,5 metros e alimentação 220 VAC, aterrada, 60Hz.
- 5) Fabricante de referência: PPA ou similar
- 6) Aplicação: Cancela do Sistema de acesso.



### 3 .CONSIDERAÇÕES GERAIS

- 1) Foram observadas as Normas e Códigos de Obras aplicáveis e a prescrição das Normas Brasileiras consideradas como elementos base para quaisquer serviços, ou fornecimento de materiais e equipamentos.
- 2) **O sistema contratado deverá ser altamente integrado com os sistemas de automação predial, controle de acesso e detecção e alarme de incêndio, em um software único, em rede corporativa trafegando com protocolos Modbus ou Bacnet de domínio público aberto.**
- 3) Na falta ou no caso de insuficiência de normas específicas da ABNT ou Inmetro, foram adotadas as recomendações da IEEE, CE, FCC, EIA e UL como referência de qualidade dos serviços, fornecimento e testes.
- 4) A instalação dos sistemas de plataforma integrada de segurança deve ser feita pela CONTRATADA, através de profissionais especializados, com experiência comprovada através de exigências de acervo técnico junto ao CREA.
- 5) O sistema de controle de acesso deverá ser integrado com a plataforma integrada de segurança, devendo, para tanto, utilizar apenas o seu software de operação.
- 6) **Para a execução do sistema de controle de acesso, não será aceito sistema híbrido, devendo ser do mesmo fabricante.**
- 7) Os equipamentos deverão ser fornecidos, instalados e integrados sob responsabilidade da CONTRATADA, a qual se responsabiliza também por manter a garantia, efetuar a manutenção e o fornecimento de peças de reposição durante o prazo da garantia contratual.
- 8) A instalação e “start up” do sistema serão feitos pela CONTRATADA, mediante utilização de mão-de-obra qualificada e treinada de acordo com as recomendações do fabricante.
- 9) A CONTRATADA, no final da execução, deve providenciar o projeto “AS BUILT”, com as devidas correções sobre o projeto original, mediante fornecimento de jogo de cópias e de arquivo eletrônico gerado em CAD. Deverão ser entregues ao CONTRATANTE manuais completos, em português, de operação de todos os equipamentos do sistema.
- 10) Todo e qualquer dispositivo do sistema será alimentado por fonte redundante e ininterrupta tipo no-break. Toda distribuição de força deverá ser de seção mínima de 2,5 mm<sup>2</sup> e estar devidamente protegida contra descargas atmosféricas, surtos e picos.
- 11) Será instalado quadro elétrico próprio para cada sistema de segurança. Os condutores de energia deverão seguir o código de cores definido pela FISCALIZAÇÃO.
- 12) As conexões dos condutores aos componentes elétricos devem ser feitas por meio de terminais de compressão apropriados. Nas ligações devem ser empregadas arruelas lisas de pressão ou de segurança (dentadas), além dos parafusos e/ou porcas e contra porcas, onde aplicáveis.
- 13) Será obrigatória a instalação de prensa-cabos em toda passagem de cabos por furos em caixas, evitando o contato com rebarbas metálicas ou quinas vivas.
- 14) Em toda infraestrutura de passagem de cabos, deverá ser considerada o memorial descritivo do projeto de elétrica visando padronizar a instalação.
- 15) Toda distribuição de rede e de elementos de campo deverão ter seus condutores com seção e proteção mecânica adequada, blindados contra interferência eletromagnética e devidamente aterrados e protegidos.
- 16) Todos os componentes do sistema deverão ser integrados ao servidor em protocolos abertos.



### **3.1 -SISTEMA DE AUTOMAÇÃO E SUPERVISÃO PREDIAL**

---

- 1) O sistema de automação e supervisão predial está em execução na obra da Procuradoria-Geral da Justiça Militar.
- 2) As controladoras digitais do sistema de automação e supervisão predial são de fabricação Honeywell.
- 3) O software do servidor do sistema de automação e supervisão predial será o SYMMETRE.

### **3.2 -PRAZO DE EXECUÇÃO**

---

- 1) O prazo de fornecimento e instalação dos bens e serviços objeto deste caderno é de até 180 (cento e oitenta) dias, a contar do 1º dia subsequente à emissão da Ordem de Execução.

### **3.3 -GARANTIAS**

---

- 1) Todos os equipamentos e softwares adquiridos deverão possuir garantia contra defeitos de fabricação e de instalação de, no mínimo, 24 meses, a contar a da assinatura do termo de recebimento definitivo dos bens/serviços. Caso um item específico tenha tempo de garantia maior que na descrição de sua especificação, valerá o maior tempo de garantia.
- 2) O custo total decorrente da necessidade de substituição de materiais, equipamentos e ou reparo de serviços deverão correr por conta da CONTRATADA, para corrigir quaisquer defeitos apresentados no período de garantia.
- 3) A determinação anterior abrange os itens cuja garantia não foi explicitada nessa especificação.

### **3.4 -TREINAMENTOS**

---

- 1) Deverá estar incluso no fornecimento dos sistemas contratados, um treinamento técnico operacional para até cinco funcionários do CONTRATANTE. O conteúdo do curso deverá abranger, no mínimo:
  - a. Introdução aos sistemas instalados no edifício
  - b. Teoria de operação;
  - c. Modos de operação;
  - d. Operação;
  - e. Especificações;
  - f. Manutenções Preventivas e Corretivas;
  - g. Aula prática.
- 2) A contratada deverá prestar assistência técnica/manutenção preventiva dos bens/sistemas, durante o período de garantia, no local de instalação dos mesmos, sendo que a contratada deverá apresentar o plano completo de manutenção dos bens/sistemas, a qual deve ser efetuada por mão-de-obra qualificada e treinada de acordo com as recomendações do fabricante, visando prover a totalidade de serviços preventivos e preditivos de manutenção, testes e reparos. A periodicidade da manutenção e testes deverá ser conforme recomendado pelos fabricantes dos bens/sistemas.