NOTA TÉCNICA GESEC - COSEB Nº 018/2025 Data: 31/10/2025.

ASSUNTO: ANÁLISE TECNICA DA EMPRESA FG – LICITAÇÃO 90019/2025

De acordo

03/11/2025

X 

Eduardo da Costa Dias Junior
Gerente Exec. Int.º da GESEC
Assinado por: 7177

Senhor Pregoeiro,

I – INTRODUÇÃO

O Objetivo da presente Nota Técnica é Levarmos ao seu conhecimento nossos esclarecimentos acerca da licitação PE 90019/2025, em relação a emprega FG Serviços e Comércio de Equipamentos de Segurança e Informática Ltda, inscrita no CNPJ nº 47.957.488/0001-03, e sua documentação analisada, bem como os demais documentos enviados pela referida.

II – ANÁLISE DA GESEC COSEB

O processo em contratação exige grande capacidade técnica e econômica, são poucas empresas efetivamente que possuem tal conjunto de capacitação, adicionalmente o contrato atual já se encontra em regime de contratação emergencial, a substituição dele pode levar no mínimo 120 dias e implica em todo sistema de segurança das agências do BASA mais dos edifícios administrativos.

O uso da POC é para comprovação efetiva de funcionamento integrado de diversas tecnologias de alta complexidade, este conjunto de funções está em outras instituições, assim como na atual estrutura do BASA, o software e todos equipamentos necessitam atender os mais altos níveis de segurança de rede para não expor a instituição a vulnerabilidades, portanto é mandatório seguirmos os cuidados definidos como premissas de contratação na mesma medida da importância dos riscos envolvidos que podem representar riscos em valores de extrema monta, falta de atendimento aos requisitos de atendimento de licenças de funcionamento junto a Polícia Federal, o sistema em contratação visa efetuar todo monitoramento de alarmes, CFTV, defesas ativas de áreas internas e externas, vídeo analíticos, controle de abertura dos cofres, controles de aberturas e fechamentos das agências, de suas tesourarias, monitoração dos edifícios administrativos entre outros.

O tempo estimado para uma comprovação em POC pode levar por volta de 20 a 30 dias por empresa.

O objeto software de integração é de suma e absoluta importância insubstituível, apesar de ser possível desenvolver, o tempo de desenvolvimento caso não esteja pronto pode ser de 6 a 12 meses, portanto a busca por soluções comprovadamente em funcionamento em outros clientes semelhantes foi fundamentada no edital.

A capacidade econômica e técnica para um projeto da magnitude desta contratação igualmente não pode ser mitigada, o tempo de implantação necessário, as dificuldades geográficas são de grande porte, com relação a questão econômica a empresa precisa ter condições de efetuar grandes investimentos para recuperar em

cobranças mensais ao longo de 60 meses, desta maneira foi fundamentado que o atestado deve ser proporcional a 50% do que se está em contratação seguindo modelos de outras contratações públicas e privadas por nós consultadas para dar base as especificações do edital.

Com base nas premissas acima fundamentamos a necessidade de identificarmos empresas sem devida condição de atendimento inicialmente pelos atestados de qualificações técnicas, proposta com marca e modelo para adequada pré análise evitando desperdício de tempo em processo de POC já tendo claro o não atendimento já na fase documental.

Com relação aos atestados segue abaixo a tabela comparativa do que foi solicitado x o que foi entregue pela empresa:

ITEM 23.2.2 - Numeração do Edital

HABILITAÇÃO TÉCNICA ITENS A SEREM COMPROVADOS POR ATESTADOS			
EQUIPAMENTOS	QUANTIDADE TOTAL	50%	Somatório Atestados FG
Central de Alarme	130	60	48
Teclado para Central de Alarme	130	60	0
Sensores de Alarme	4.467	2.234	330
Sirene Convencional 12 VDC	488	244	0
Sirene Alta Potência	80	40	0
Câmera Tipo IP	2.488	1.244	183
Gravador Digital NVR/HVR de 16 Canais	142	71	1
No Break 3200 KVA	142	71	6

Switch Poe / PoE+	146	73	5
Gerador de Neblina	318	159	0
Controlador de Acesso por leitor biometria Facial	227	114	0
Controle Automatizado de Porta de Enrolar	10	5	0
Analíticos de Vídeo	200	100	0
Software de Monitoramento e Controle integrando sistemas de Alarmes, CFTV, Gerador de Neblina, Controle de Fechaduras de Cofres e Controle de Acesso	1	1	0
Monitoramento de Unidades	122	61	0

EMISSOR DO ATESTADO	OBJETO	DESCRIÇÃO	OBSERVAÇÕES
Peritoplast Ind. E Com LTDA	Serviços de Instalação e Manutenção	30 Câmeras ,01 DVR, 5 Switch, 6 Nobreaks, Sistema de Alarme	
Prefeitura de Rodeio	Fornecimento	Notebooks, Mochilas. Mouses e Mouse PAD	Não atende

Prefeitura Municipal de Sangão	Serviços de Instalação e Manutenção	30 Centrais,100 Câmeras	
W.W.E	Serviços de Instalação	Equipamentos de Informática	Não atende
Velho Paletes	Serviços de Instalação	Equipamentos de Informática	Não atende
Prefeitura de Mondaí	Serviços de Instalação e Fornecimento	4 Câmeras Automotivas	Não atende
Prefeitura de Cocal do Sul	Serviços de Instalação e Fornecimento	53 Câmeras IP, 18 Centrais de Alarme, 330 Sensores	
Prefeitura de Porto Alegre	Fornecimento	160 Câmeras Corporais	Não atende

OBS: Item 23.5 não comprovado pois não há nenhum atestado que contemple software

A Qualificação Técnica apresentada pela Empresa FG Serviços e Comercio de Equipamentos de Segurança e Informática LTDA, não atendem o item 23 e seus subitens do Edital nas quantidades mínimas obrigatórias para comprovação discriminados em cada um conforme tabelas acima.

Pelo demonstrado fica evidente a falta de atendimento de maneira extensa e em desacordo com o edital. Mudar agora implica em todos os riscos da introdução e eminente pedido de Recurso Administrativo do certame por outras empresas participantes e em especial as que corretamente não se cadastraram cientes de não serem capazes de atender ao objeto especificado.

No que diz respeito aos catálogos técnicos, entendemos que o fato mencionado já configura motivo suficiente para desclassificação. Contudo, o que se verifica de forma incontestável é que o processo se torna insanável, diante do evidente desconhecimento de itens críticos — como, por exemplo, o uso do spray neutralizador, conforme especificado na página 113, item 2.4."

PAINEL DE CONTROLE LÓGICO PROGRAMÁVEL PARA PROTEÇÕES EXTERNAS DAS AGÊNCIAS COM SPRAY NEUTRALIZADOR, SIRENE CONVENCIONAL, SIRENE DE ALTA POTÊNCIA, HOLOFOTES E CERCA ELÉTRICA.

Páginas 115 a 117

Spray Neutralizador

• Este equipamento complementa segurança adicional para solução de restrição de visibilidade em áreas protegidas, assim como poderá ser utilizado isoladamente, de acordo com escolhas da Contratante e severidade do ataque.

• Deve ser atóxico e capaz de causar desconforto respiratório, como tosse, irritação de olhos e mucosas tornando impraticável a permanência no local de forma prolongada.

• O agente neutralizador será fornecido em embalagem com capacidade de 90g e protegido por gabinete metálico, com bateria para funcionamento em caso de falta de energia. Página 116 de 260

• Disparo deve ser controlado de forma precisa pelo Painel de Controle Lógico Programável e pelo Software de Gerenciamento conforme opção de escolha da Contratante, sempre mandatoriamente priorizando lógicas de proteção contra disparos indevidos e seguindo programações horárias de livre escolha do Contratante.

• O software de supervisão deve informar a quantidade de disparos total e remanescentes após seu uso;

• A troca e instalação do mesmo deve ser segura prevendo refil de teste e sequência controlada pelo software para evitar uso equivocado de refil, ou seja, garantir que testes somente possam ser realizados com refil de água e ativação somente com refil de neutralizador efetivo de forma controlada, ainda deve ser garantida a rastreabilidade de cada neutralizador não permitindo reaproveitamento do mesmo, identificando data de

validade e local de instalação;

• Neutralizador deve ter documentação que comprove ser atóxico e conformidade FISPQ, ABNT 14725:201.

IDENTIFICAÇÃO DE RISCOS

• Classificação de perigo do produto químico: Aerosol não inflamável Gás dissolvido

• Perigo por aspiração – Categoria 1 Lesões oculares graves/irritação ocular

• Categoria 2B Toxicidade para órgãos-alvo específicos - exposição única

• Categoria 3 Sistema de classificação utilizado: Norma ABNT-NBR 14725-2:2009 – versão corrigida 2:2010.

• Sistema Globalmente Harmonizado para a Classificação e Rotulagem de produtos químicos, ONU.Página 117 de 260

FISPQ em conformidade com ABNT 14725:201

• Deverá permitir total controle por programações horarias os acionamentos das entradas e saídas, sendo aceito no mínimo os seguintes formatos:

A) Modo Manual

B) Modo Semiautomático

C) Modo Automático

A descrição técnica acima não permite desvios, o produto claramente deve possuir características aprovadas e já em uso em outras instituições.

O produto ofertado por esta licitante é um Gás de Pimenta, este produto em território nacional é controlado pelo Exército e absolutamente proibido para uso comercial, caracteriza porte ilegal pois ele é considerado um produto de uso restrito e controlado, fabricação, comercialização e uso dependem de autorização do Exército brasileiro. O porte não autorizado pode levar à responsabilização criminal.

Quanto a demais itens é possível fazer uma lista extensa de não atendimentos que ferem o especificado como por exemplo:

TERMO DE REFERÊNCIA TÉCNICA EDITAL	ATENDE	NÃO ATENDE	COMENTÁRIOS
· 2.1 SISTEMA DE ALARME a) CENTRAL DE ALARME COM NO MÍNIMO 64 ZONAS SUPERVISIONADASCentral de alarme, responsável por gerenciar todos os recursos que compõem o sistema de alarme monitorado instalado na Unidade.		X	Central utilizada => marca Honeywell possui apenas 48 Zonas e os Módulos/Placas apresentados de expansão B308, Interface de Barramento B810, GPRS B443 são de outro fabricante portanto não ha compatibilidade dos equipamentos apresentados
· Todas as características elétricas do painel, inclusive a tensão de alimentação, tensão de consumo, etc, devem ser compatíveis entre si, de modo a manter a solução funcional e com a possibilidade de uso de todas as funcionalidades, por tempo integral e sem ônus adicionais ao BASA.			Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere
· Ser instalada e protegida por gabinete de aço com pintura eletrostática, com proteção contra violação por impacto físico, proteção contra			Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere

infiltração de água ou umidade, danos físicos.			
· Possuir, no mínimo, 08 (oito) partições e 08 (oito) setores fixos.			Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere
· Central de Transmissão deve ter seu horário sincronizado e ajustado automaticamente com o horário da rede IP (NTP) do BASA ou sincronizar via rede de dados móvel.			Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere
· Possibilitar a expansão para até 99 (noventa e nove) setores (zonas), conforme a quantidade de sensores dispostas neste documento.			Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere
· Cada setor (zona) poderá receber no máximo 01 (um) sensor que seja devidamente identificado no sistema de gerenciamento remoto da Central de Monitoramento remoto, de forma que se identifique o tipo de sensor ou dispositivo e o local exato onde foi instalado.			Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere
· Possuir sistema alternativo de energia elétrica para o caso de falta de suprimento pela rede pública.			Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere
· O sistema alternativo deve contemplar bateria selada estacionária, específica para centrais de alarme, não sendo admitido o uso de baterias veiculares adaptadas.			Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere
· A capacidade do sistema alternativo de suprimento deve manter as condições de funcionamento e operação da solução por, no mínimo, 24 (vinte e quatro) horas consecutivas, ainda que não esteja no modo stand by.			Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere

· Quando do retorno do fornecimento de energia elétrica pela rede pública, o sistema deverá ser capaz de recarregar todas as baterias em até 24 (vinte e quatro) horas consecutivas.			Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere
· A capacidade do sistema alternativo deve ser supervisionada e reportada ao sistema de monitoramento de alarme, para o operador da Central de Monitoramento Principal e de Contingência.			Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere
· A Central de Transmissão deverá ser interligada à Central de Monitoramento pelas vias de comunicação, conforme descritas neste documento.			Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere
· Deve possuir sistema de manutenção de memória permanente para manter a programação do sistema.			Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere
· Deve possuir sistema de autodiagnóstico/varredura do perfeito funcionamento dos sensores, sirene (SI), bateria, alimentação elétrica da rede pública, acionadores, vias de comunicação, módulos de comunicação e expansão de setores, e emitir notificação instantânea à Central de Monitoramento.			Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere
· Supervisionar os contatos de entradas e saídas e transmitir instantaneamente eventos			Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere
· Supervisionar os contatos de entradas e saídas e transmitir instantaneamente eventos à Central de Monitoramento Principal e de Contingência, em caso de falhas. A Central de Monitoramento Principal e de Contingência receberão os eventos dos sistemas de alarme monitorados e comandarão procedimentos de forma remota nos sistemas de alarme monitorados através das vias de comunicação.			Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere

· A central de transmissão deve ser capaz de promover supervisão das vias de comunicação, inclusive com teste periódico – keep alive – além de identificar e comunicar defeitos e falhas na capacidade de comunicação das vias, individualmente.			Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere
· No caso de defeito ou falha na capacidade de comunicação de uma via ou mais vias, a via que estiver funcionamento normalmente deverá ser capaz de identificar instantaneamente e reportar imediatamente à Central de Monitoramento Principal e de Contingência o defeito das vias problemáticas, além de manter o sistema de alarme monitorado funcionando normalmente.			Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere
· Permitir a interligação de, no mínimo, 03 (três) teclados de alarme para operação em um mesmo sistema de alarme monitorado.			Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere
· Permitir programação de agendamento de horário para ativação e desativação de partições, acionamento de intertravamento de dispositivos (por exemplo, portas de acesso a ambientes) automaticamente, mediante a programação, independente em cada uma das partições, em horários previamente definidos pelo usuário do sistema de alarme na Unidade do BASA, que será implementada quando da instalação do equipamento.			Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere
· Possibilitar o cadastro de senhas distintas, pessoais e intransferíveis para cada usuário local, sendo que cada usuário deverá possuir uma senha de uso rotineiro e uma senha de uso em modo coação também distintas uma da outra.			Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere
· Devem ser considerados, no mínimo, 20 (vinte) usuários distintos localmente em cada Unidade.			Informação não disponível e/ou não considerada visto não atendimento do

			equipamento a que se refere
· A Central de Monitoramento deve receber eventos distintos para quando forem utilizadas senhas de rotina e senhas em modo coação pelos usuários lotados nas Unidades, de forma que no caso desta última possa perceber risco iminente e adotar as medidas emergenciais de reação.			Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere
· Permitir a auditoria pela Central de Monitoramento remoto de uma operação de arme e desarme das partições, registrando o usuário que a executou, o tipo da operação, o que foi alterado, além do dia, mês, ano, hora, minuto e segundo em que a operação foi realizada.			Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere
· Quando um dispositivo, zona ou partição apresentar problema que impossibilite o arme do sistema de alarme adequadamente, deve ser possível ao usuário local ou remoto realizar a anulação daquele dispositivo, zona ou partição, armando os demais normalmente.			Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere
· A solução deve permitir que as partições sejam programadas para armar automaticamente em um determinado horário pré-definido pelo usuário.			Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere
· Possibilitar a supervisão de bateria, interferência de rádio frequência e supervisão de tamper dos equipamentos que possuam esta funcionalidade.			Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere
· Deve ser capaz de transmitir, no mínimo, todos os eventos e comandos remotos constantes neste documento.			Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere
· A CONTRATADA fornecerá e manterá atualizada a lista de comandos que podem ser transmitidos às centrais, sendo que o protocolo ou a forma de acionamento adotado deve, obrigatoriamente, possuir:	ATENDE	NÃO ATENDE	COMENTÁRIOS

· Criptografia nas comunicações, utilizando métodos simétricos ou assimétricos;			Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere
· Autenticação da origem das conexões, utilizando chaves/senhas de autenticação;			Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere
origem dos comandos à central;			Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere

· Sinal de acknowledge da recepção do comando;			Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere
· Código de erro no caso de falha do comando.			Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere
· Possibilitar a expansão de zonas e do quantitativo de sensores e acionadores que compõem a solução de sistema de alarme monitorado.			Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere
· Permitir a supervisão, pela Central de Monitoramento Principal e de Contingência, do funcionamento das vias de comunicação, configurável para períodos diferentes, como, por exemplo, para comunicar de 01 (um) em 01 (um) minuto, até a cada a cada 24 horas.			Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere
· Suportar a integração com VMS (Video Monitoring System), BMS (Business Management System) e PSIM (Physical Security Information Management) de terceiros, via SDK (Software Development Kit) e protocolos abertos ou de mercado, através de adaptador Ethernet integrado ou placa de interface de ethernet instalada no barramento de comunicação do painel.			Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere
· A integração deve ocorrer de forma que, o painel de alarme ou o servidor sejam integrados diretamente ao V M S , BMS, PSIM ou outro sistema de integração, sem a utilização de hardwares			Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere

intermediários e estranhos a ambos os sistemas.			
· Suportar atualizações locais e remotas de firmware do painel de controle e periféricos permitindo novas atualizações sempre que necessário.			Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere
· A supervisão deve ocorrer para estado de bateria (baixa), nível e perda de sinal e eventuais interferências.			Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere
a.a) Das vias de Comunicação	ATENDE	NÃO ATENDE	COMENTÁRIOS
· As vias de comunicação devem ser compatíveis com a central de transmissão contratada e funcionar de forma independente, ou seja, cada via de comunicação deve ser capaz de receber e transmitir eventos integralmente e de forma individualizada, bem como de receber e transmitir comandos remotos integralmente.			Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere
· Devem, a qualquer momento e conforme definido pela Área de Segurança, testar e enviar o status (condição de funcionamento), além de testar, detectar e reportar o status (condição de funcionamento) das demais vias de comunicação.			Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere
· Identificar e reportar para o sistema de monitoramento remoto os problemas nas demais vias de comunicação			Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere
· Devem realizar a comunicação integral de eventos e comandos remotos entre a Central de			Informação não disponível e/ou não considerada visto não atendimento do

Monitoramento Principal e de Contingência e os sistemas de alarme monitorados.			equipamento a que se refere
· Ser capazes de transmitir simultaneamente e concomitantemente para e a partir da Central de Monitoramento Principal e de Contingência, todos os eventos ou comandos remotos.			Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere
· Quaisquer módulos de comunicação independentes (separados) da central de alarme deverão possuir fonte de alimentação e bateria exclusiva com autonomia mínima igual à bateria auxiliar da solução, além de proteção contra violação, proteção da interligação entre o módulo e o painel de alarme, e ser monitorados ininterruptamente.			Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere
· As vias de comunicação devem ser, no mínimo, as seguintes:	ATENDE	NÃO ATENDE	COMENTÁRIOS
· Rede ethernet (TCP/IP) corporativa do Banco: principal;			Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere
· Possuir protocolo 802.1X (padrão IEEE para controle de acesso à rede baseado em porta PNAC)			Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere
· Telefonia móvel (GPRS/GSM): contingência com chip quadriband. O chip deve funcionar em todas as frequências do âmbito nacional (850/900/1800/1900MHz), possibilitando a comunicação mesmo em locais mais afastados das grandes capitais. O contrato do serviço de dados do chip, deverá ser de responsabilidade da contratada.			Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere
· A via de comunicação prioritária será a rede IP			Informação não disponível e/ou não

(TCP/IP – UDP/IP).			considerada visto não atendimento do equipamento a que se refere
· Quando instalada esta via de comunicação, a empresa CONTRATADA deverá obedecer às indicações informadas pela Área de TI do BASA.			Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere
· A via de comunicação IP deverá funcionar conforme as políticas de segurança de TI do BASA, tanto lógicas quanto físicas, de forma a impedir a exposição da rede de dados interna contra acessos externos desautorizados, cabendo às empresas licitantes consultar mais informações durante a licitação – se assim o desejarem – bem como à CONTRATADA providenciar as adequações necessárias, sem custo adicional ao BASA, para que o funcionamento desta via de comunicação seja ativada.			Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere
· Transmitir eventos e receber comandos remotos através da rede TCP/IP do BASA, respectivamente, para e a partir da Central de Monitoramento Principal e de Contingência.			Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere
· A via de comunicação deverá ser estabelecida e configurada de forma que a comunicação de dados ocorra exclusivamente entre os sistemas de alarme monitorados e a Central de Monitoramento Principal e de Contingência de dados ocorra exclusivamente entre os sistemas de alarme monitorados e a Central de Monitoramento Principal e de Contingência.			Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere
· Os eventos transmitidos pela via principal de comunicação deverão ser direcionados para a Central de Monitoramento do BANCO, os quais serão replicados, por canal seguro via internet (VPN), para a Central de Monitoramento do CONTRATADO;			Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere

· Em caso de transmissão de eventos pela via contingencial, os mesmos deverão ser enviados em duplicidade, sendo uma das vias, para a Central de Monitoramento do BANCO e para a Central de Monitoramento do CONTRATADO;			Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere
· A Contratada será responsável por todo o fornecimento dos hardwares de comunicação;	ATENDE	NÃO ATENDE	COMENTÁRIOS
· Todas as vias deverão ter recurso de supervisão de disponibilidade, reportando à:	ATENDE	NÃO ATENDE	COMENTÁRIOS
Central de Monitoramento com as seguintes periodicidades:			Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere
Rede ethernet (TCP/IP) corporativa do Banco: 1 (um) minuto;			Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere
Telefonia móvel (GPRS/GSM): 05 (cinco) minutos.			Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere
b) TECLADO DE ALARME	ATENDE	NÃO ATENDE	COMENTÁRIOS
Interface de comunicação Ethernet (10/100Mbps) e ou RS485;	X		Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere
Aviso sonoro (buzzer)	X		Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere

Teclado de alarme numérico, deve possuir mensagens em texto, menu, personalização de funções, bloqueio/desbloqueio manual de setores com mensagens em português e visor de cristal líquido (LCD), para bloqueio/desbloqueio manual de setores e ativação/desativação da proteção noturna do sistema de alarme do local vigiado, somente através de senhas individuais e pessoais;	X		Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere
Possibilitar o cadastro de senhas comuns e de "coação" para no mínimo 40 posições de usuários, com capacidade de gerenciamento distinto entre um tipo e outro de senha;	X		Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere
Aviso sonoro Buzzer;	X		Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere
Teclado deve possuir teclas para acessos rápidos que permitam acionamento de dispositivo	X		Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere

Indicar as mensagens de texto em português.	X		Informação não disponível e/ou não considerada visto não atendimento do equipamento a que se refere
c) SENSOR DE IMPACTO E VIBRAÇÃO	ATENDE	NÃO ATENDE	COMENTÁRIOS
· Sensor para detectar tanto vibração quanto impacto na superfície onde for instalado;	X		
· Deve ter capacidade para identificar tentativa de rompimento da superfície onde estiver fixado, realizada por instrumento de perfuração ou impacto;	X		
· Detecção inteligente de vibração de 3 eixos;		X	
· Possuir led indicativo para teste de funcionamento;	X		
· Sensor deve possuir raio de operação de 1,5m quando instalado em concreto e de 3m quando instalado em chapa de aço;			
· Possuir recurso de autoaprendizagem para auxílio do ajuste do nível de sensibilidade durante a instalação; durante a instalação;	X		
· Chave de anti-violação da tampa;	X		
· Definições de sensibilidade através de interruptores (DIP, Trimmer, Trimpot, Jumper,	X		

etc) ou por software;			
· Temperatura de operação de 0 a 55º C.	X		
d) SENSOR DETECTOR DE FUMAÇA	ATENDE	NÃO ATENDE	COMENTÁRIOS
· Sensores que possuam tecnologia para avaliar e identificar fumaça oriunda de incêndio e do uso de equipamentos ou ferramentas que produzam ou utilizem chama ou calor e, consequentemente, produzam fumaça;	X		
· Capacidade de limpeza da câmara ótica sem a necessidade de desmontar o sensor;	X		
· Temperatura de operação de 0˚ a 38˚C.	X		
e) DETECTOR DE QUEBRA DE VIDRO	ATENDE	NÃO ATENDE	COMENTÁRIOS
· Deve ser do tipo com fio;		X	
· Sensor para identificação de quebra de, no mínimo, vidros dos tipos planos, laminados e temperados, tanto por impacto quanto por estilhaçamento;		X	
· Possuir microprocessador para análise dos sinais recebidos, distinguindo o som de quebra real de vidro e ignorando outros sons ao redor, evitando, assim, falsos alarmes;		X	
· Possuir detecção com dupla frequência;		X	

· Possuir ajuste automático de sensibilidade;		X	
· Possuir raio de detecção mínimo de 7 (sete) metros e com ajuste automático para adequar a capacidade de detecção ao local onde for instalado;		X	
· Operar em temperatura entre 0ºC e 49ºC;		X	
· O detector de quebra de vidro deve ser instalado no teto ou nas paredes perpendiculares ou opostas a área envidraçada. Caberá à empresa contratada verificar o funcionamento do sensor com o uso de ferramenta apropriada de simulação do som da quebra da vidraça e ajustando a posição do detector, se for o caso, antes de dar a instalação por concluída;		X	
· Com identificação de abertura (tamper) para a Central de Monitoramento;		X	
· Possuir led indicativo para teste de funcionamento.		X	
f) TRANSMISSOR REMOTO	ATENDE	NÃO ATENDE	COMENTÁRIOS
· Acionador portátil de alarme tipo chaveiro remoto sem fio;	X		
· Bateria de lítio com duração mínima de 24 meses a partir da sua instalação de fácil substituição e sem necessidade de recarga;	X		
· Possuir mecanismos para que cada acionador e seus respectivos acionamentos sejam identificados	X		

individualmente pela Central de Monitoramento;			
· Receptores de Sinal que comuniquem as informações com o painel de monitoramento;	X		
· Não deve ocupar nenhuma das 64 zonas da central de transmissão;	X		
· Permitir o acionamento da Central de Transmissão do sistema de alarme de maneira silenciosa e discreta, de qualquer local no interior da Unidade onde estiver o respectivo painel de alarme;	X		
· Deve ser supervisionado automaticamente pelo painel de alarme, não dependendo do usuário para verificar o nível baixo de carga das baterias, havendo transmissão de um aviso para a central de transmissão e consequentemente para a Central de Monitoramento;	X		
· Deve possuir dimensões reduzidas para ser portado de maneira discreta pelo usuário;	X		
· A cobertura do sinal do acionador deve ser garantida em toda a parte interna da	X		
unidade, de maneira que o evento seja recepcionado independente do ponto de acionamento.	X		
g) SIRENE PIEZOELÉTRICA BLINDADA E AUTO-ALIMENTADA	ATENDE	NÃO ATENDE	COMENTÁRIOS
· Sirene tipo piezoelétrica, respeitando os limites da legislação de 110 dB a 1 (um) metro de distância do equipamento, com programação para funcionamento de 01 até 20 minutos quando da ocorrência de		X	Tempo de 20 minutos quando ocorrência de corte de energia não informado

corte de energia;			
· Deve ser instalada em caixa blindada, resistente a intempéries, em local de difícil acesso, possuir chave com fechadura para desativação em caso de corte ou manutenção e possuir fonte de alimentação com bateria, roteção contra-abertura e contra retirada da parede (tamper de abertura e de parede), e não deve ocupar nenhuma das zonas (setores) da central de transmissão destinada a detectores diversos;		X	
· As sirenes internas e externas deverão ser instaladas em local a ser indicado pela Área de Segurança do BASA, com fiação não visível. Fiação das sirenes deve ser protegida por laço de sirene, em caso de sabotagem ou corte acionar disparo de alarme e comunicar a Central de Monitoração;		X	ABS com UV
· Deve possibilitar a detecção e posterior envio de evento para a Central de Monitoramento, quando ocorrer as seguintes condições:	X		
· Detectar a abertura da caixa de proteção;	X		
· Detectar a remoção da sirene do seu local de fixação.	X		
h) SENSOR DETECÇÃO MAGNÉTICO	ATENDE	NÃO ATENDE	COMENTÁRIOS
· Deve ser do tipo com fio;	X		
· Adequado para fixação em portas e janelas;	X		
· Contato do tipo NF;	X		

· GAP de abertura a partir de 2 (dois) e até 6 (seis) cm;	X		
· Deve ser instalado e fixado com parafusos.	X		
i) ACIONADOR FIXO DE ALARME – COM FIO	ATENDE	NÃO ATENDE	COMENTÁRIOS
· Acionador de alarme do tipo fixo, com fio, a ser instalado ou fixado em paredes de concreto, drywall ou superfícies metálicas, em local de fácil acesso e visualização;			Documentação não enviada
· Deverá possuir um único botão com cor ou sinalização que o diferencie visualmente do resto do corpo do equipamento;			Documentação não enviada
· Conformidade com a certificação de segurança EN50131 ou UL 636.			Documentação não enviada
j) SENSOR DE DETECÇÃO DE PRESENÇA DUPLA TECNOLOGIA (Infravermelho e Microondas) – COM TECNOLOGIA ANTIMASCARAMENTO, COM FIO	ATENDE	NÃO ATENDE	COMENTÁRIOS
· Possuir a detecção conjunta e combinada dos sensores Microondas e PIR, para evitar disparos falso- positivos;			Catalogo não se refere ao produtudo ofertado na planilha
· Possuir proteção contra disparos falsos causados por luz branca;			Catalogo não se refere ao produtudo ofertado na planilha
· Possibilitar ajuste de alcance da detecção do			Catalogo não se refere ao produtudo

canal microondas;			ofertado na planilha
· Possuir tecnologia de detecção de anti mascaramento com utilização de produto líquido, viscoso ou em pó de forma borrifada ou espalhada por pincel, isopor, papelão, manta térmica, guarda-chuva, madeira, acrílico ou outros materiais;			Catalogo não se refere ao produtudo ofertado na planilha
· Possuir tecnologia anti camuflagem de corpo humano;			Catalogo não se refere ao produtudo ofertado na planilha
· Alcance mínimo do sensor de 15m x 15m (metros);			Catalogo não se refere ao produtudo ofertado na planilha

· Deve possuir tecnologia de ajuste automático de temperatura de forma que a sensibilidade do sensor aumente quando a temperatura do ambiente se aproximar da temperatura do corpo humano e reduza quando a temperatura do ambiente se afastar da temperatura do corpo humano;			Catalogo não se refere ao produtudo ofertado na planilha
· Chave antiviolação (tamper) de tampa e parede;			Catalogo não se refere ao produtudo ofertado na planilha
· LED de teste de passagem remoto;			Catalogo não se refere ao produtudo ofertado na planilha
· Imunidade a correntes de ar, insetos e animais;			Catalogo não se refere ao produtudo ofertado na planilha
· Programação local por interruptor (DIP, Trimmer, Trimpot, Jumper, etc);			Catalogo não se refere ao produtudo ofertado na planilha
· Ângulo de abertura mínimo de 90º;			Catalogo não se refere ao produtudo ofertado na planilha
· Sensor com tecnologia look down zone ou equivalente;			Catalogo não se refere ao produtudo ofertado na planilha
· Altura de instalação de a partir de 2m (metros) sem a necessidade de ajustes adicionais;			Catalogo não se refere ao produtudo ofertado na planilha
· Temperatura de operação: 0ºC a 55ºC, com umidade relativa do ar a cerca de 93% sem condensação;			Catalogo não se refere ao produtudo ofertado na planilha
· Processamento de sinal de interferência antifluorescentes;			Catalogo não se refere ao produtudo ofertado na planilha

· Deverá possuir resistores fim de linha integrados ao sensor ou tecnologia de barramento;			Catalogo não se refere ao produtudo ofertado na planilha
· Conformidade com a certificação de segurança EN50131 Grade 3.			Catalogo não se refere ao produtudo ofertado na planilha
2.2 CFTV. A) SISTEMA DE GRAVAÇÃO E GERENCIAMENTO DE CFTV GRAVADOR DIGITAL –	ATENDE	NÃO ATENDE	COMENTÁRIOS
Possuir 16 ou 32 canais de vídeo de câmeras IP.	X		
Operação do gravador local em interface gráfica utilizando saída HDMI de alta resolução (1920x1080) ou superior	X		
Sincronização de tempo entre os gravadores da rede através de Servidor NTP.	X		
Reprodução de imagens gravadas, de 4 ou 8 ou 16 câmeras simultâneas.	X		
Compressão de vídeo em H.265 ou superior.	X		
Gravação e transmissão de vídeo com opção diferenciada de resolução e taxa de frames para possibilitar o arquivamento local em alta resolução e o acesso remoto com consumo de banda inferior conforme necessidade de cada local.	X		
Possuir controle de usuário e senha diferenciados para configuração e visualização;	X		

Possibilitar o acesso simultâneo de 10 conexões ou superior.	X			
Possibilidade de criação de diversos usuários ou perfis de usuários com detalhamento de permissões.	X			
Possuir interface USB, frontal e traseira para gravação de vídeo e utilização de mouse/teclado.	X			
Possibilitar backup através de interface USB.	X			
Possibilidade de recuperação das gravações de vídeo e utilização das imagens nas unidades onde as câmeras estão instaladas.	X			
Garantir obrigatoriamente o armazenamento de todas as imagens gravadas nas unidades onde o sistema for instalado por tempo não inferior a 60 dias. Havendo qualquer alteração de normativa regulamentadora deverá a proponente se adequar prontamente em acordo com prazos determinados pela normativa imposta, os equipamentos devem ser fornecidos com no mínimo 2x HDS de 6TB provendo total de 12 TB onde tiver 16 canais e no mínimo 2x HDS de 10TB provendo total de 20TB onde tiver 32 canais e garantir o tempo mínimo acima estabelecido em configurações de boa qualidade de gravação, ou seja se necessário o fornecedor deverá incluir capacidade adicional além da mínima solicitada, em não necessitando da capacidade mínima solicitada ainda assim o sistema deve ser fornecido atendendo o mínimo exigido.	X			
Possuir os protocolos de rede: TCP/IP IPv4/IPv6, RTSP, UDP, PPPoE, DHCP, DNS, DDNS, NTP, DHCP, Filtro IP, FTP, SFTP, SMTP, SNMP, Multicast, 802.1x,		X	Catalogo não contem informações sobre os protocolos: UDP, PPPoE, Filtro IP, FTP, SFTP, Multicast, 802.1x, RTMP, UPnP e ONVIF.	

RTMP, UPnP, HTTP, HTTPS e ONVIF.			
Possuir alimentação elétrica 100 ~ 240 VAC (Full Range)	X		
Temperatura de operação 0°C à 55°C	X		
Conexão com canais IP através de padrão ONVIF e RTSP.		X	
Possuir ou permitir sistema detecção de face interno ou externo para garantir que a imagem detectada pela câmera seja realmente de uma pessoa.		X	
Permitir integração com câmeras que possuam recurso de vídeo analítico embarcado.	X		
Possuir recurso de vídeo analítico embarcado pelo menos para as seguintes analises: movimento, Perda de vídeo, Mascaramento e Mudança de Cena e ser compatível com sistemas de geradores de analíticos VMS.	X		
Gravador deve ser de padrão de 1U para instalação em rack 19”, aceitando acondicionamento em bandeja, o equipado deve possuir no mínimo de duas (2) baias internas para instalação dos discos de gravação.		X	
Suportar resolução de 3MP em 5 canais e 2MP (1080p) em todos os canais,	X		
Configuração de resolução inferior na transmissão remota.	X		

Controlar individualmente a qualidade de imagem de todos os canais.	X		
Permitir o acesso remoto via principais navegadores (browser) com opção de seleção de fluxo de vídeo (alta resolução ou resolução inferior).	X		
Possuir protocolo 802.1X (padrão IEEE para controle de acesso à rede baseado em porta PNAC)		X	
B) CÂMERA TIPO DOME IP - HIKVISION DS-2CD2147G2-L	ATENDE	NÃO ATENDE	COMENTÁRIOS
O corpo do conjunto deverá ser construído em alumínio para maior durabilidade do produto.	X		
Possuir tecnologias de transmissão TCP/IP com protocolo Onvif (versão 2.4 ou superior), contar com os profile S, T, G e M;		X	Catalogo não consta profile M no item Network
Compressão H.265+ ou tecnologia H.265 e recurso adicional de compactação como (HDSM, SmartCompression, ZipStream);	X		
Resolução de 1920x1080, com ao menos 3 níveis de resolução inferior e com pelo menos dois fluxos (stream) de vídeo;	X		
Possuir capacidade de imagem colorida mesmo em condições de baixíssima iluminação, 0.06lux em modo color	X		

Possuir lente varifocal de 2.8 a 13mm com zoom e foco remote;	X		
Ângulo de visão horizontal de pelo menos 110 graus;	X		
Possuir iluminador infravermelho (IR) embutido na câmera para alcance máximo de no mínimo 30 metros;	X		
Possuir iluminador por luz branca de pelo menos 25m;	X		
Possuir barra de controle de intensidade do IR;	X		
A câmera deverá contar com grau de proteção IP67 e IK10.Câmera e o suporte devem ser de alumínio para maior resistência e durabilidade;	X		
Alimentação da câmera com 12VDC com conector P4 ou através do cabo de rede (PoE IEEE802.3af);	X		
Possuir relação sinal/ruído > 50dB;	X		
Possuir ajuste de compensação de iluminação WDR, BLC;	X		
Contar com detecção de movimento e máscara de vídeo, compatível com o padrão Onvif;	X		
Possuir máscara de privacidade para seleção de áreas que não devem ser monitoradas;	X		
Temperatura de operação entre -10 e +60 graus Celsius;	X		

Possuir os seguintes protocolos: IPv4; IPv6; HTTP; TCP; UDP; ARP; RTP; RTSP; RTCP; FTP; SFTP; DHCP; DNS; DDNS; QoS; UPnP; NTP; Multicast; ICMP; IGMP e SNMP;	X		

Possuir protocolo 802.1X (padrão IEEE para controle de acesso à rede baseado em porta PNAC;	X		
Possuir protocolos de segurança tais como Encriptação SSL, Autenticação Digest e Secure Boot;		X	Catalogo enviado não contem informações sobre Secure Boot
A câmera deverá possuir os seguintes analíticos embarcados: Detecção de Movimento, Sabotagem e Movimento Adaptativo, sendo a câmera ainda capaz de a partir de um evento, automatizar um processo como uma gravação no cartão SD, envio de imagem para FTP, acionamento da luz branca, envio de e- mail, texto e http genérico;	X		
CÂMERA TIPO BULLET IP - HIKVISION DS-2CD2T47G2-L	ATENDE	NÃO ATENDE	COMENTÁRIOS
Câmera tipo bullet sendo que o conjunto deverá ser construído em alumínio para maior durabilidade do produto	X		
Possuir tecnologias de transmissão TCP/IP com protocolo Onvif (versão 2.4 ou superior), contar com os profile S, T, G e M;		X	Catalogo não consta profile M no item Network
Compressão H.265+ ou tecnologia H.265 e recurso adicional de compactação como (HDSM, Smart Compression, ZipStream);	X		
Resolução de 1920x1080, com ao menos 3 níveis	X		

de resolução inferior e com pelo menos dois fluxos (stream) de vídeo;			
Possuir capacidade de imagem colorida mesmo em condições de baixíssima iluminação, 0.06lux em modo color	X		
Possuir lente varifocal de 2.8 a 13mm com zoom e foco remote;	X		
Ângulo de visão horizontal de pelo menos 110 graus;	X		
Possuir iluminador infravermelho (IR) embutido na câmera para alcance máximo de no mínimo 30 metros;	X		
Possuir iluminador por luz branca de pelo menos 25m;	X		
Possuir barra de controle de intensidade do IR;	X		
A câmera deverá contar com grau de proteção IP67;	X		
Câmera e o suporte devem ser de alumínio para maior resistência e durabilidade;	X		
Alimentação da câmera com 12VDC com conector P4 e através do cabo de rede (PoE IEEE802.3af);	X		
Possuir relação sinal/ruído > 50dB;	X		
Possuir ajuste de compensação de iluminação	X		

WDR, BLC;			
Contar com detecção de movimento e máscara de vídeo, compatível com o padrão Onvif;	X		
Possuir máscara de privacidade para seleção de áreas que não devem ser monitoradas;	X		
Temperatura de operação entre -10 e +60 graus Celsius;	X		
Possuir os seguintes protocolos: IPv4; IPv6; HTTP; TCP; UDP; ARP; RTP; RTSP; RTCP; SMTP, FTP; SFTP; DHCP; DNS; DDNS; QoS; UPnP; NTP; Multicast; ICMP; IGMP e SNMP;	X		
Possuir protocolo 802.1X (padrão IEEE para controle de acesso à rede baseado em porta PNAC);	X		
Possuir protocolos de segurança tais como Encriptação SSL, Autenticação Digest e Secure Boot;		X	Catalogo enviado não contem informações sobre Secure Boot
A câmera deverá possuir os seguintes analíticos embarcados: Detecção de Movimento, Sabotagem e Movimento Adaptativo, sendo a câmera ainda capaz de a partir de um evento, automatizar um processo como uma gravação no cartão SD, envio de imagem para FTP, acionamento da luz branca, envio de e- mail, texto e http genérico;	X		
C) CÂMERA TIPO FISHEYE - HIKVISION DS-2CD2955FWD-I	ATENDE	NÃO ATENDE	COMENTÁRIOS
O corpo do conjunto deverá ser construído em	X		

alumínio para maior durabilidade do produto;			
Possuir tecnologias de transmissão TCP/IP com protocolo Onvif (versão 2.4 ou superior), contar com os profile S, T, G e M;		X	Catalogo não constam profiles T e M, por ser um modelo de camera descontinuado pelo fabricante https://www.hikvision.com/pt-br/products/IP-Products/Network-Cameras/Pro-Series-EasyIP-/DS-2CD2955FWD-I2/?q=ds-2cd2955fwd-i&pageNum=1&position=1&hiksearch=true&subName=DS-2CD2955FWD-IS
Compressão H.265+ ou tecnologia H.265 e recurso adicional de compactação como (HDSM, Smart Compression, ZipStream);	X		
Resolução de 2048 x 2048, com ao menos 3 níveis de resolução inferior e com pelo menos dois fluxos (stream) de vídeo;		X	Catalogo não informa 3 niveis de resocução inferior
Possuir capacidade de imagem colorida mesmo em condições de baixíssima iluminação, 0.1lux em modo color	X		
Possuir lente tipo fisheye de 1.4mm;	X		
Visão 360 graus com campo de visão horizontal de pelo menos 180 graus;	X		
Possuir iluminador infravermelho (IR) embutido na câmera para alcance máximo de no mínimo 17 metros;		X	Catalogo informa alcance do IR até 8 metros
A câmera deverá contar com grau de proteção		X	Catalogo não contem as proteções

IP66, IP67 e IK10;			solicitadas
Alimentação da câmera do tipo PoE 802.af ou 802.3at;	X		
Possuir Firmware assinado e criptografado;		X	Catalogo não contem qualquer informação do item
Microfone embutido com capacidade de ativar e desativar através de chave seletora;		X	Catalogo não contem qualquer informação do item
Possuir ajuste de compensação de iluminação WDR e BLC;	X		
Contar com detecção de movimento e máscara de vídeo, compatível com o padrão Onvif;	X		
Possuir máscara de privacidade para seleção de áreas que não devem ser monitoradas;	X		
Temperatura de operação entre -40 e +60 graus Celsius;		X	Catalogo informa temperatura de -10º até 50º C
Possuir os seguintes protocolos: IPv6, IPv4, HTTP, HTTPS, SOAP, DNS, NTP, RTSP, RTCP, RTP, TCP, UDP, IGMPv3, ICMP, DHCP, Zeroconf, DSCP, multicast, HTTP, SRTP, SNMP v2c e SNMP v3.		X	Não possui todos os protocolos solicitados
Possuir protocolo 802.1X (padrão IEEE para controle de acesso à rede baseado em porta PNAC);	X		
A câmera deverá estar em conformidade com os padrões de segurança cibernética, como por exemplo NDAA		X	Catalogo não contem qualquer informação do item

Vídeo Analítico embarcado para classificação e pessoas e veículos, tendo a capacidade de analisar comportamentos desses objetos tais como: Objeto na área, Loitering, Cruzamento de feixes, Objeto deixando o local, Objeto parado no local e detecção de aglomerações.		X	Não possui todos os analiticos solicitados
A) MONITOR DE 21,5 POLEGADAS	ATENDE	NÃO ATENDE	COMENTÁRIOS
Tamanho da tela mínima (Polegadas): 21”	X		
Contraste mínimo: 30.000:1 DFC		X	
Tempo de Resposta: 5ms	X		
Brilho: 250 cd/m²	X		
Resolução: 1920 x 1080 @ 60Hz	X		
Conector de entrada: VGA / HDMI INRGB IN (PC) / HDMI IN	X		
Sinal de Vídeo: Analógico / Digital	X		
B) MINI RACK 16U 19” EM PAREDE.	ATENDE	NÃO ATENDE	COMENTÁRIOS
Estrutura montável para fixação em parede;		X	
Base com entrada de cabos;	X		
Porta frontal em aço/acrílico reversível + fecho Yale	X		
Fechamento traseiro aço/liso	X		

Fechamentos laterais aço/aletado + fecho rápido em poliamida	X		
Planos de Montagem	X		
Ventilação natural ou forçada	X		

Com no mínimo 570mm de profundidade	X		
C) CALHA COM 8 TOMADAS HORIZONTAL PADRÃO 19”	ATENDE	NÃO ATENDE	COMENTÁRIOS
· Régua/calha elétrica de 8 tomadas para rack (PDU);			Informação não disponível na documentação apresentada
· Padrão tomada fêmea NBR 14136, 20 Amperes;			Informação não disponível na documentação apresentada
· Suporta até 750Watts;			Informação não disponível na documentação apresentada
· Número de tomadas 8;			Informação não disponível na documentação apresentada
D) KIT PORCA GAIOLA PARA RACK 19”	ATENDE	NÃO ATENDE	COMENTÁRIOS
Com Parafusos Philips rosca M5;			Informação não disponível na documentação apresentada
Com garra de fixação para padrão em Rack 19”;			Informação não disponível na documentação apresentada
Comprimento do parafuso: 12mm;			Informação não disponível na documentação apresentada
Tipo de cabeça: redonda tipa panela com base chat;			Informação não disponível na documentação apresentada
Tipo de porca: M5 com encaixe Gaiola.			Informação não disponível na documentação apresentada

BANDEJA FIXA PARA RACK 19” X 570mm			Informação não disponível na documentação apresentada
Fabricada em chapas de aço carbono;			Informação não disponível na documentação apresentada
Fixação nos 4 perfis do Rack 19”;			Informação não disponível na documentação apresentada
I) DISCO RÍGIDO SATA com capacidade mínima de 10TB.	ATENDE	NÃO ATENDE	COMENTÁRIOS
Interface: sata de 6 gb/s;	X		
HD Interno, conexão SATA;	X		
Velocidade de rotação: 7.200 RPM ou superior	X		
Tamanho do buffer: 256 mb;	X		
Ciclos de carga/descarga: 300.000 mínimos;	X		
Tamanho físico: 3,5 pol;	X		
J) DISCO RÍGIDO SATA com capacidade mínima de 06TB.	ATENDE	NÃO ATENDE	COMENTÁRIOS
· Interface: sata de 6 gb/s;	X		
· HD Interno, conexão SATA;	X		
· Velocidade de rotação: 5.400 RPM ou superior	X		
Tamanho do buffer: 64 mb;	X		

Ciclos de carga/descarga: 300.000 mínimos; Tamanho físico: 3,5 pol.	X		
K) TECLADO USB PARA COMPUTADOR	ATENDE	NÃO ATENDE	COMENTÁRIOS
Layout: ABNT 2;			Informação não disponível na documentação apresentada
Compatível com: Linux, Windows 9x, 2000, ME, XP, NT ou superiores;			Informação não disponível na documentação apresentada
Conexão: USB.			Informação não disponível na documentação apresentada
L) MOUSE USB PARA COMPUTADOR	ATENDE	NÃO ATENDE	COMENTÁRIOS
Com sensor óptico;			Informação não disponível na documentação apresentada
Conexão USB;			Informação não disponível na documentação apresentada
Resolução: 1000dpi;			Informação não disponível na documentação apresentada
Quantidade de botões: 3;			Informação não disponível na documentação apresentada
Função Scroll			Informação não disponível na documentação apresentada
M) SWITCH L3 PoE+ - CISCO C9300L-24P-4X	ATENDE	NÃO ATENDE	COMENTÁRIOS
· Switch Gerenciável de camada 3 (Layer 3).	X		

· Deve suportar os padrões IEEE802.3af (PoE) e IEEE802.3at (PoE+).	X		
· Mínimo de 24 portas 10/100/1000 BASE-T com autonegociação de velocidade e Power Over Ethernet (PoE).	X		
· Deverá possuir no mínimo a potência PoE de 370W. Deverá possuir até 30W por porta no PoE.	X		
· Deverá possuir 4 portas SFP+ (10 Gbps).	X		
· Deverá possuir LED's indicativos do estado de funcionamento do equipamento.	X		
· Deverá possibilitar a obtenção de estatísticas de tráfego e falhas das portas para todas as portas. Deverá possuir LED's indicativos do estado de funcionamento do equipamento.	X		
· Deverá implementar ajuste de clock utilizando NTP (Network Time Protocol).	X		
· Deverá permitir a atualização de versões de código utilizando os protocolos Secure File Transfer Protocol (SFTP), Trivial File Transfer Protocol (TFTP) ou através da interface web.	X		
· Deverá estar equipado com recursos que implementem funcionalidades de gerenciamento relativas ao padrão de gerenciamento SNMP (Simple Network Management Protocol), com suporte ao SNMP v3.	X		
· Deverá implementar mecanismos de monitoramento e análise local e remota de			

tráfego em portas de switches pertencentes a uma mesma VLAN, através de configuração de espelhamento de portas.	X		
· Deverá suportar o Link Layer Discovery Protocol (LLDP).	X		
· Deverá estar equipado com 1 (uma) porta de comunicação out-of-band para gerenciamento de configuração, podendo essa ser uma porta serial, ou isolar uma porta de comunicação do switch através de uma VLAN, tornando a porta totalmente isolada do ambiente de acesso.	X		
· Deve possuir as seguintes Características: Static Routing; DHCP Relay DHCP Server IGMP Snooping 802.3ad LACP; Spanning Tree STP/RSTP/MSTP BPDU Filtering/Guard Root Guard Loopback detection; MAC static, dynamic, Link aggregation and vlan. IP ACL GVRP; ARP Inspection Port Security	X		
· Deverá estar equipado com recursos que permitam o gerenciamento através de Command Line Interface (CLI).	X		
· Deverá estar equipado com o gerenciamento através de web browser com suporte a SSL (Secure Socket Layer) versão 3 ou SSH (Secure Shell) versão 2 (RFC 4252).	X		
· Deverá possuir estrutura apropriada para acondicionamento em armário de fiação (rack) de 19 polegadas, ocupando uma unidade (1U), sendo incluso o fornecimento dessas peças para prender no rack, conhecidas como “orelhas” por exemplo, ou trilhos, mantendo 1U.	X		

· Deverá possuir memória DRAM (ou SDRAM) de, no mínimo, 512 (quinhentos e doze) megabytes. Deverá possuir memória flash de, no minimo 256, com dual boot.	X		
· Deverá implementar ACLs baseadas em Portas (Ethernet) Físicas do switch;	X		
· Deverá implementar autenticação de login/senha ou certificado para a liberação de tráfego na porta através do protocolo IEEE 802.1x com as seguintes funcionalidades:	X		
· atribuição de VLAN conforme a autenticação do usuário; reautenticação forçada de porta;	X		
· reautenticação periódica.	X		
· Devem possuir capacidade de limitação de endereços MAC por porta, acessíveis em uma dada interface de LAN do switch.	X		
· Deverá suportar a visualização de endereços MAC aprendidos pelo switch.	X		
· Deverá possibilitar a obtenção de estatísticas de tráfego e falhas das portas para todas as portas.	X		
· Empilhamento de no mínimo switches. Virtual Switching Technology	X		
· Deverá suportar VLAN baseado em Tag 802.1Q, VLAN UNTAG e VLAN Híbrida.	X		

· Deverá suportar Gerenciamento Multicast Fast Leave, Multicast VLAN e Controle Multicast	X		
· Deverá suportar QoS baseado em portas, 802.1p, Algoritmos de fila: SP, RR, WDRR e Controle de banda por porta.	X		
· Deverá suportar Segurança das portas, Isolamento das portas, Filtro de endereço MAC, RBAC, Radius, detecção Anti-attack , ARP Poison e TACACS+.	X		
· Deverá suportar OSPF OSPFv3, IP-SLA Based On ICMP, VRRP e Roteamento IPv4/IPv6 estático e dinâmico com suporte a políticas, policy-based routing (PBR).	X		

· Deverá suportar Habilitar/Desabilitar Porta PoE e Prioridade de Porta PoE. Alimentação de entrada entre 100~240V.	X		
· Temperatura de operação entre 0º e 40°C ou melhor. Trabalhar com humidade relativa do ar de até 90% ou melkhor	X		
N) NOBREAK - SINUS TRIAD 3KVA / SINUS TRIAD NG 6 E 10 KVA	ATENDE	NÃO ATENDE	COMENTÁRIOS
Potência nominal de 3200 [VA]		X	
Fator de potência 0,70	X		
Tecnologia interativo convencional	X		
Faixa de operação de entrada de 91 volts até 272 volts em CA	X		
Rendimento deverá ser maior que 95% com Rede maior 85% com inversor	X		
Regulação de Saída do inversor +/-6% com carga linear		X	
Tempo de acionamento do inversor 1 ms			Informação não disponível na documentação apresentada
Forma de onda do inversor deverá ser senoidal pura	X		

Frequência de saída do inversor 60 Hz	X		
Proteção eletrônica contra sobrecarga	X		
Números de tomadas 10 T		X	
Devera possuir modulo de bateria externo com bateria de 12v/40 A	X		
2.3 GERADOR DE NEBLINA E SISTEMAS DE DEFESAS ATIVAS	ATENDE	NÃO ATENDE	COMENTÁRIOS
O equipamento deve ser composto por Gerador de Neblina e acessórios (recipiente com fluído, bateria interna, suporte/insumos para fixação em teto ou parede). O Gerador de Neblina (GN) é um equipamento eletroeletrônico, destinado a restringir a visibilidade de ambientes, através da liberação de uma névoa espessa, atóxica, inodora e que não gera resíduos após a sua dispersão. Pode ser instalado nas posições vertical ou horizontal. É utilizado para inibir intrusões e ataques em ambientes, através de diminuição de visibilidade, onde os equipamentos estiverem instalados;	X		
O equipamento deverá restringir a visibilidade à no máximo 20 cm em todas as direções num intervalo de tempo de no máximo 30 segundos preenchendo por completo um ambiente de no mínimo 100 m³, sendo aceitável variação nestas condições de 5% para mais ou para menos;		X	Informação não disponível na documentação apresentada
O equipamento deve possuir capacidade de conexão direta com sensores necessários para lógica de sua ativação sendo no Hall 01 sensor de presença, 01 sensor sísmico, 01 sensor de porta, 01 sensor quebra vidro e na tesouraria capacidade de conexão direta com 01 sensor sísmico, 01 sensor de porta e 01 sensor de presença. O gerador mesmo sem rede e energia			

deve possuir capacidade de pronta resposta em caso de ataques conforme programação a ser definida junto a segurança BASA. As condições de defesa devem permitir configurações por disparo simples de um único sensor e também por combinação de múltiplos sensores simultaneamente.		X	
A persistência da neblina em ambiente sem ventilação forçada deverá ser de, no mínimo, 20 minutos, nas mesmas condições de visibilidade do item acima;			Informação não disponível na documentação apresentada
Deverá ser capaz de gerar neblina com disparos programáveis em intervalo de até 1 minuto;	X		
Deverá ser capaz de efetuar no mínimo 20 disparos de 30 segundos por carga de líquido, conforme itens acima;		X	
Tempo de pré-aquecimento inferior a 20 minutos;	X		
O sistema deve oferecer opções de condições de disparos 100% automáticos e disparos semiautomáticos solicitando confirmação da Central de Monitoramento e acionamentos manuais via Central de Monitoramento;		X	
O gerador de neblina deverá ser capaz de funcionar por um tempo não inferior a 120 minutos durante a falta de energia elétrica, independente se o equipamento estiver instalado em ponto proveniente de no- break/estabilizador ou ponto proveniente da ligação direta da concessionária de energia elétrica;	X		

A neblina gerada pelo equipamento deverá ser seca e atóxica, não podendo, após sua dissipação, deixar resíduos, umidade, ou quaisquer tipos de elementos sólidos ou líquidos nas superfícies em que ela entrou em contato;			Informação não disponível na documentação apresentada
O Gerador de Neblina deverá ser capaz de apresentar tempos de disparo programáveis de 1 a 60 segundos, de forma a configurar os intervalos de acionamento e adequar a quantidade de neblina gerada ao volume do ambiente protegido. Concomitantemente, deverá possuir opção de teste de disparo com configuração do tempo entre 1(um) e 3 (três) segundos para realização de testes com neblina;		X	
O Gerador de Neblina deverá pesar no máximo 25 Kg, com carga total de fluído e bateria;	X		
Em caso de abertura e violação do Gerador de neblina deverá ser gerado sinal de alarme (tamper) para que possa ser identificado pelo serviço de monitoramento.			Informação não disponível na documentação apresentada
O Gerador de Neblina deverá possuir sistema de medição precisa de supervisão do nível do fluido, informando o nível vazio, baixo, médio e completo para o módulo de supervisão local e remoto, ativando o relé de sinalização de fluído baixo;		X	
No recipiente do fluido deverá existir identificação do fabricante, data de fabricação, data de validade e permitir a impostação da data de instalação do gerador de neblina no ambiente. Além, disso, a data de validade não poderá ser inferior a dois anos da data de instalação do equipamento. O acesso ao fluído deve ser, preferencialmente, por abertura independente			Informação não disponível na documentação apresentada

com controle de violação permitindo rápida troca em especial quando equipamento estiver em locais de difícil acesso;			
O Gerador de Neblina deverá funcionar perfeitamente em ambientes com temperaturas no mínimo entre 5°C e +50°C.;	X		
O Gerador de Neblina deve dispor de módulo de comunicação com a rede IP afim de permitir tanto seu monitoramento, como seu acionamento remoto pela Central de Operações de Segurança;		X	
O Gerador de Neblina deverá ter um sistema de autodiagnóstico, capaz de informar por meio de alarmes técnicos locais e para o painel de alarme, se há algum tipo de problema que impossibilite seu disparo, como falhas em bateria, temperatura, nível de fluido, falta de alimentação AC etc.;			Informação não disponível na documentação apresentada
O Gerador de Neblina deverá possuir bloco de conexões para ligação dos cabos de supervisão, sinalização, acionamento e diagnóstico com compatibilidade de integração com painéis de alarme e intrusão de mercado e, no mínimo, as seguintes possibilidades:			Informação não disponível na documentação apresentada
Conexão serial, USB ou similar com painel de supervisão local;		X	
Deverá ser capaz de sinalizar reposição de fluido;			Informação não disponível na documentação apresentada
Deverá ser capaz de sinalizar falha do equipamento;	X		

Deverá ser capaz de sinalizar Ativação do Gerador de Neblina;			Informação não disponível na documentação apresentada
Deverá ser capaz de sinalizar abertura do Gerador de Neblina (tamper);		X	
Deverá ter Entrada para Inibir o Gerador de Neblina;			Informação não disponível na documentação apresentada
Deverá ter 18 Entrada de alarme;		X	5 IMPUTS
Deverá ter 6 Saídas de rele;		X	3 OUTPUTS
Deverá possuir capacidade permitindo parametrizar regras de negócio para ativação do gerador de neblina por conexão direta com sensores do tipo, sísmico, presença, quebra vidro, magnético e outros;		X	
Os sensores contemplados na LPU item 2.3 Sistema de Gerador de Neblina e defesas Ativas devem seguir respectivas especificações técnicas descritas no item 2.1 ALARME	ATENDE	NÃO ATENDE	COMENTÁRIOS
Para condição de disparos 100% (cem por centos) automáticos, deverão ser observadas, no mínimo, as seguintes combinações:			

Detecção no Sensor de Presença combinado com detecção no Sensor Quebra Vidro aciona a Liberação de Névoa.		X	
Detecção no Sensor de Presença combinado com detecção no Sensor Sísmico aciona a Liberação de Névoa.		X	
Detecção no Sensor de Presença combinado com detecção no Sensor Sísmico e combinado com detecção no Sensor Quebra Vidro aciona a Liberação de Névoa.		X	
A solução deverá permitir ativação e/ou desativação local e remota do gerador de neblina e a ação deve ser registrada nos logs do servidor.			Informação não disponível na documentação apresentada
Deverá possuir entrada para integração com Central de Incêndio;			Informação não disponível na documentação apresentada
O Gerador deverá armazenar log de auditoria dos registros de falha, sinalizações, comando e funcionamento do gerador, tais como: sinais de falha, funcionamento, sinalizações com data e hora de cada evento, e prover estas informações para o módulo ou aplicativo de supervisão/diagnóstico local e remotamente quando utilizado acesso via comunicação IP;			Informação não disponível na documentação apresentada
O gerador de neblina deverá ser capaz de operar de forma automática com tensões de entrada de 110/127V AC – 60hz e 220/240V AC - 60hz e corrente máxima de 10 ampères, de acordo com		X	

a tensão adotada na unidade do local de instalação. Não sendo permitida a utilização de transformadores externos ao gerador de neblina;			
O gerador de neblina deve possuir meios de detecção de tentativa de obstrução de saída de fluído, com sinalização de alarme para o painel de monitoramento;		X	
O Gerador de Neblina deverá possuir mecanismo simples para substituição do recipiente do fluido e das baterias, de modo que não seja necessária a retirada, desinstalação ou a desmontagem completa do equipamento, provendo através de tampas o acesso aos itens consumíveis;		X	
O fluído do Gerador de Neblina deverá ser armazenado em reservatório rígido.	X		
O recipiente do fluído deverá possuir: nome e marca do fluído, volume total de fluído, identificação do fabricante, data de fabricação, data de validade e permitir a impostação da data de instalação pelo técnico instalador;			Informação não disponível na documentação apresentada
A data de validade do fluido não poderá ser inferior a dois anos da data de entrega do kit reposição de fluido;			Informação não disponível na documentação apresentada
Deverão ser fornecidas informações sobre condições de armazenagem segura e eventuais incompatibilidades de armazenamento e			Informação não disponível na

orientações sobre o método correto para manuseio seguro do fluído;			documentação apresentada
Deverá ser fornecido os acessórios de conexões, alimentação e fixação para o perfeito funcionamento do sistema;			Informação não disponível na documentação apresentada
O gerador de neblina deverá ser construído de forma a permitir sua instalação tanto de modo vertical quanto horizontal, a fim de poder ser fixado no piso, paredes, tetos ou embutido em forros - de acordo com a necessidade requerida pelo ambiente sem que para tanto sejam necessários opcionais não inclusos no fornecimento original do equipamento;	X		
Quando fixados diretamente na parede ou teto, os elementos de fixação não deverão ser acessíveis externamente e em caso de violação deverá ser gerado sinal de alarme que possa ser identificado pela monitoração;	X		
Para evitar risco de incêndio, o gerador de neblina deverá ser dotado de meios capazes de desarmar automaticamente seus elementos geradores de calor, de forma independente de seus circuitos eletroeletrónicos (“disjuntor térmico”).	X		
Protocolo 802.1X (padrão IEEE para controle de acesso à rede baseado em porta PNAC).		X	
2.4 PAINEL DE CONTROLE LÓGICO PROGRAMÁVEL PARA PROTEÇÕES EXTERNAS DAS AGÊNCIAS COM SPRAY NEUTRALIZADOR, SIRENE CONVENCIONAL,	ATENDE	NÃO	COMENTÁRIOS

SIRENE DE ALTA POTÊNCIA, HOLOFOTES E CERCA ELÉTRICA .		ATENDE	
Gabinete metálico tipo caixa, para área externa com no máximo as medidas 40cm de altura, 36cm de largura e 15cm de profundidade.		X	
Placa de automação com controle Lógico Programável, projetada para aplicação industrial, conexão ethernet nativa com protocolo 802.1X (padrão IEEE para controle de acesso à rede baseado em porta PNAC).		X	
Deverá disponibilizar, no mínimo 18 entradas do tipo supervisionada	X		
Deverá disponibilizar, no mínimo 06 saídas do tipo isoladas, que controlem através de relés, para acionamento de dispositivos externos.	X		
Deverá permitir configurar as entradas e saídas de modo personalizado em interface gráfica.			Informação não disponível na documentação apresentada
Deverá possuir sistema para supervisionamento remoto ou ser integrado a ferramenta contratada pelo banco.			Informação não disponível na documentação apresentada
Deverá ser capaz de operar de forma automática com tensões de entrada de 110/127V e 220/240V.	X		

Deverá ser capaz de realizar as operações em modo stand-alone, em caso de falhas de rede de dados.			Informação não disponível na documentação apresentada
Deve disponibilizar armazenamento de logs, em caso de falhar da rede de dados TCP/IP, de modo que seja transmitido para software de integração na restauração de comunicação.			Informação não disponível na documentação apresentada
Deverá permitir controle de acionamentos automatizado das entradas e saídas permitindo controles de Sirenes convencionais, Sirenes de Alta Potência, holofotes, cercas perimetrais, sprays tipo neutralizador e outros equipamentos comandados por saídas digitais. Os acionamentos serão realizados pela central de monitoramento de forma manual e/ou configurados para pronta resposta automática, com base de recebimento de sensores externos de movimento, detecções de movimentos de câmeras, monitoramento de cercas e em especial por combinação com analíticos de inteligência integrado ao sistema atuando de forma integrada com software de monitoramento.			Informação não disponível na documentação apresentada
As áreas a serem protegidas incluem estacionamentos, fachada, fundos, laterais e calçadas adjuntas a agência onde os analíticos devem ser capazes de detectar qualquer tipo de comportamento anormal por autoaprendizagem do gerador de analíticos previsto neste edital, com base em invasões de linhas de cruzamento, aglomerações de 02 (duas) ou mais pessoas de forma a mesmo durante o dia poder detectar abordagens de assalto a transeuntes e veículos, assim como outras possibilidades de programações por cruzamento de linhas,			Informação não disponível na documentação apresentada

vadiagens e outras condições futuras com uso dos analíticos previstos.			
Holofotes tipo led 150-200W área externa IP67 Prova d'água, Branco Frio 6000k, carcaça em alumínio preto.		X	Modelo apresentado IP 66 não resistente a agua
Sirene Convencional. A sirene deverá ser do tipo piezoelétrica, operando em tensão de 12V, 120dB com condições de operação e funcionamento inclusive durante a falta de energia elétrica.	X		
A sirene deverá ser compatível com o painel de comando e diagnóstico fornecido e poderá, através do painel citado, ser acionada remotamente, bem como ser programada para funcionamento de 1 (um) até 20 (vinte) minutos, quando da ocorrência de corte de energia.			Informação não disponível na documentação apresentada
Sirene de Alta Potência	ATENDE	NÃO ATENDE	COMENTÁRIOS
Sirene eletromecânica unidirecional montada em alumínio, pintado em epóxipreto.	X		
Possuir flange, hélice, tampa frontal e base de fixação em chapa	X		
Alimentação 127VAC OU 220VAC 50/60HZ	X		
220VAC – 15% - 50/60Hz | 114,0dB@1 m		X	

Cerca Elétrica	ATENDE	NÃO ATENDE	COMENTÁRIOS
Tipo monitorada com capacidade de interligação com painel de controle lógico programável, com bateria, módulo de tensão incorporado, intervalo de pulsos de 1 segundo saída para aviso de central armada e desarmada, proteção IPX4, carregador de bateria interno, ajustável entre 8.000 e 12.000 volts			Documentação não enviada
Spray Neutralizador	**ATENDE**	**NÃO ATENDE**	**COMENTÁRIOS**
Este equipamento complementa segurança adicional para solução de restrição de visibilidade em áreas protegidas, assim como poderá ser utilizado isoladamente, de acordo com escolhas da Contratante e severidade do ataque.		X	
Deve ser atóxico e capaz de causar desconforto respiratório, como tosse, irritação de olhos e mucosas tornando impraticável a permanência no local de forma prolongada.		X	Gas tipo Pimenta Importado (Proibida a utilização no Brasil) SUJEITO A AÇÃO CRIMINAL
O agente neutralizador será fornecido em embalagem com capacidade de 90g e protegido por gabinete metálico, com bateria para funcionamento em caso de falta de energia.		X	
Disparo deve ser controlado de forma precisa pelo Painel de Controle Lógico Programável e pelo Software de Gerenciamento conforme opção de escolha da Contratante, sempre mandatoriamente priorizando lógicas de proteção contra disparos indevidos e seguindo		X	

programações horárias de livre escolha do Contratante.			
O software de supervisão deve informar a quantidade de disparos total e remanescentes após seu uso;		X	
A troca e instalação do mesmo deve ser segura prevendo refil de teste e sequência controlada pelo software para evitar uso equivocado de refil, ou seja, garantir que testes somente possam ser realizados com refil de água e ativação somente com refil de neutralizador efetivo de forma controlada, ainda deve ser garantida a rastreabilidade de cada neutralizador não permitindo reaproveitamento do mesmo, identificando data de validade e local de instalação;		X	
Neutralizador deve ter documentação que comprove ser atóxico e conformidade FISPQ, ABNT 14725:201. IDENTIFICAÇÃO DE RISCOS		X	
Classificação de perigo do produto químico: Aerosol não inflamável Gás dissolvido		X	
Perigo por aspiração – Categoria 1 Lesões oculares graves/irritação ocular		X	
Categoria 2B Toxicidade para órgãos-alvo específicos - exposição única		X	
Categoria 3 Sistema de classificação utilizado: Norma ABNT-NBR 14725- 2:2009 – versão corrigida 2:2010.		X	

Sistema Globalmente Harmonizado para a Classificação e Rotulagem de produtos químicos, ONU. FISPQ em conformidade com ABNT 14725:201		X	
Deverá permitir total controle por programações horarias os acionamentos das entradas e saídas, sendo aceito no mínimo os seguintes formatos:		X	
A) Modo Manual		X	
B) Modo Semiautomático		X	
C) Modo Automático		X	
2.5 CONTROLE DE ACESSO INTEGRADO	ATENDE	NÃO ATENDE	COMENTÁRIOS
· Todos os acionamentos deverão ser registrados e associados com os respectivos operadores permitindo a identificação inequívoca para cada evento.	X		
· A configuração local de parâmetros de operação do equipamento deve ser feita sem a necessidade de recursos externos ou acessórios. A solução deve possuir teclado interno ou outros recursos próprios que permitam fácil configuração inicial para se comunicar com o Software gerenciador instalado na Central de Monitoramento;			Informação não disponível na documentação apresentada
· Deve permitir que a solução seja configurada parA operar com controle de custódia externa (dupla- custódia).			Informação não disponível na documentação apresentada

· Todas as ocorrências devem ser registradas na memória de eventos da controladora;			Informação não disponível na documentação apresentada
· Cada controladora biométrica estará cadastrada no sistema da Central de Monitoramento com identificação do local controlado;			Informação não disponível na documentação apresentada
· A controladora biométrica deve utilizar chave de encriptação, devendo ser configuráveis para cada controladora de acordo com o padrão de segurança do BASA;	X		
· A controladora biométrica deve permitir que a carga de dados e informações dos usuários seja feita pelo Servidor do Sistema através da rede de comunicação de forma totalmente transparente aos usuários sem interrupção do seu funcionamento normal;			Informação não disponível na documentação apresentada
· Deve permitir a comunicação com o Servidor do Sistema mesmo que este esteja instalado em sub- rede distinta do local onde está instalada a controladora.	X		
· Todos os eventos devem ser registrados, tais como: acessos solicitados, acessos realizados, tentativas frustradas de acesso, biometrias inválidas, horários proibidos, porta forçadas, etc;			Informação não disponível na documentação apresentada
· Realização de atualização remotamente pela rede TCP/IP, de forma que quando houver correções, implantações de novas funções, novos recursos ou melhorias;			Informação não disponível na documentação apresentada
· Permitir a comunicação via protocolo SNMP por meio de aplicativo do BASA para verificação do status de funcionamento;			Informação não disponível na documentação apresentada

2.6 TECLADO OU DISPLAY COM SENHA E LEITOR POR RECONHECIMENTO FACIAL INTEGRADO	ATENDE	NÃO ATENDE	COMENTÁRIOS
· Display LCD touch com função de teclado com backlight ;	X		
· 06 inputs configuráveis;		X	
· Interface de comunicação Ethernet (10/100Mbps);	X		
· Aviso sonoro (buzzer);			Informação não disponível na documentação apresentada
· Capacidade mínima de usuários: 1.000;	X		
· Tempo máximo para leitura facial: 3 segundos;	X		
· Tempo máximo para verificação facial: 2 segundos;	X		
· Templates protegidos por criptografia;	X		
· Taxa de Falsa Rejeição (FRR) e Aceitação (FAR) menores que 0,01%;			Informação não disponível na documentação apresentada
· Operação: 0°C a 50°C;	X		
· Controle de Eletroímã até 2 portas;		X	
· Entrada para Botão de Saída;	X		
· Entrada para Botão de Emergência;	X		
· Operação em Dupla Custódia, abertura conjunta assistida sendo uma pessoa no local e a sala de monitoramento validando on-line e off-line em			

caso de perda de rede por senha criptografada exclusiva e restrita ao local, dia e hora com margem de 1 minuto, garantindo dados da confirmação de autorização local registrada e validada;			Informação não disponível na documentação apresentada
· Operação por duas liberações locais ao mesmo tempo, opção de abertura em dupla custódia local por dois autorizados para a operação de abertura;			Informação não disponível na documentação apresentada
·Capacidade de abertura simples por um usuário;	X		
· Abertura por senha e reconhecimento facial;	X		

·Logs completos de todas atividades;	X		
·Bloqueio por férias ou desativação de permissão;	X		
·Cadastro de senha pelo usuário;		X	
·Pré cadastro pela central de monitoramento com registro prévio de senha conforme matrícula e facial por foto sendo a senha e foto atualizados localmente pelo usuário ao efetuar primeiro cadastramento.			Informação não disponível na documentação apresentada
·Reconhecimento de tentativas de burla por fotos ou vídeos;	X		
·Sistema de troca de senha assistido pela Central por exclusão da anterior voltando a etapa de cadastro, porém registrando a ocorrência;			Informação não disponível na documentação apresentada
· Programação de horários e dias de acesso;			Informação não disponível na documentação apresentada
·Programação de feriados;			Informação não disponível na documentação apresentada
· Opções de abertura em contingência local segura;			Informação não disponível na documentação apresentada
·Proteção contra quedas de energia permitindo aberturas por capacidade de se manter ativa em sistema duplo de back-up de energia de emergência, ou seja sendo o primeiro estágio de forma automática para ciclos de falta de energia de até 6 horas e em caso de falta de energia			

superior a 6 horas ter mecanismo local de acionamento de um segundo sistema de back up com igual capacidade de 6 horas adicionais, também serão aceitas soluções com um único sistema de back- up por falta de energia desde que o mesmo possua capacidade mínima de 18 horas ininterruptas.			Informação não disponível na documentação apresentada
·Proteção em caso de falta continua de energia manter travado eletroímã com solenóide de atraque.		X	Documentação enviada da fechadura, não é tipo solenoite
· Em caso de furto do controlador de acesso e vandalismos o sistema deve manter porta fechada;		X	Documentação enviada da fechadura, não é tipo solenoite
·Fechadura Solenoide do Tipo Fail Secure para Porta de Vidro;		X	Documentação enviada da fechadura, não é tipo solenoite
·Estas fechaduras deverão funcionar alimentadas em 12 VCC, sendo que quando desenergizadas mantém as portas travadas, destravando-se somente quando energizadas;		X	Documentação enviada da fechadura, não é tipo solenoite
· Dever possuir sistema de detecção de vandalismo "Tamper, de tampa e de parede, detectando tanto a abertura do mesmo quanto seu afastamento da parede;	X		
· Deve ser do tipo solenóide próprio para instalação em portas de vidro com ou sem batente, devendo conseguir aliar características de fácil instalação, design moderno e construção robusta;		X	Documentação enviada da fechadura, não é tipo solenoite
·Controle para até 04 portas, com possibilidade de intertravamento.			Informação não disponível na documentação apresentada

o Relatório de data/hora do acesso;	X		
o Alerta PAMT (porta aberta muito tempo);			Informação não disponível na documentação apresentada
o Delay de entrada/saída;	X		
o Auto-arme (particionamento);			Informação não disponível na documentação apresentada
o Liberação remota de acesso;			Informação não disponível na documentação apresentada
o Contingência (portas destravadas);			Informação não disponível na documentação apresentada
o Opção de controle de aberturas intertravadas;			Informação não disponível na documentação apresentada
o O acesso será concedido remotamente com a abertura e fechamento das portas nas unidades do BASA onde a solução estiver instalada;	X		
· Todos os acionamentos deverão ser registrados e associados com os respectivos operadores permitindo a identificação inequívoca para cada evento;	X		
· Deve verificar a autenticidade dos usuários pelo reconhecimento facial independentemente da quantidade de arquivos existentes em sua memória local;	X		
· Deve permitir que os usuários se identifiquem			Informação não disponível na

em modo normal ou sob coação;			documentação apresentada
· Em ambos os casos o equipamento deve apresentar comportamento idêntico não emitindo sinais que possam alertar os presentes para o modo de identificação que o usuário utiliza naquele momento. Caso a identificação tenha sido realizada sob coação a controladora deve enviar uma mensagem ao Software gerenciador do sistema alertando para o fato;			Informação não disponível na documentação apresentada
· A configuração local de parâmetros de operação do equipamento deve ser feita sem necessidade de recursos externos ou acessórios. A solução deve possuir display touch que permita fácil configuração inicial para se comunicar com o Software gerenciador instalado na Central de Monitoramento;	X		
· Deve permitir que a solução seja configurada par operar com controle de custódia externa (dupla- custódia);			Informação não disponível na documentação apresentada
· Todas as ocorrências devem ser registradas na memória de eventos da controladora;	X		
· Quando a operação estiver ativada a controladora de biometria facial deve estar em modo online e a autorização de acesso deve obedecer a seguinte sequência:			
1º. O usuário digita seu código de identificação numérica no teclado;			Informação não disponível na documentação apresentada
2.º O equipamento solicita ao usuário que apresente sua identificação de Biometria facial; 3º. O equipamento captura a a imagem digital do			Informação não disponível na

usuário e a compara com a imagem digital cadastrada;			documentação apresentada
4º. Caso o usuário seja reconhecido e possa acessar o local a controladora biométrica envia uma mensagem ao operador e a solicitação é avaliada por ele, caso contrário a solicitação é negada;			Informação não disponível na documentação apresentada
5º Se o operador do sistema autorizar a entrada a controladora deve liberar a fechadura a qual ela controla, caso contrário a solicitação é negada; Todas as ocorrências devem ser registradas na memória de eventos da controladora;			Informação não disponível na documentação apresentada
· A controladora deve permitir que o tempo máximo de ingresso de dados seja configurado;			
· Os Cadastros dos usuários devem possuir no mínimo os seguintes campos: nome completo, nome da mãe, CPF, Carteira Identidade/Carteira Nacional de Vigilante – CNV, data de nascimento, celular e foto;			Informação não disponível na documentação apresentada
· Deve disponibilizar campos de dados extras personalizáveis, com conteúdo e nome a critério do BASA;			Informação não disponível na documentação apresentada
· A controladora deve permitir a programação horária de acionamento (janela de abertura e de fechamento), liberando a validação do usuário unicamente durante os horários permitidos;			Informação não disponível na documentação apresentada
· Será informada no visor da controladora a informação de tentativa de abertura ou de fechamento fora			Informação não disponível na documentação apresentada

do horário programado;			
· Fora da janela só será alertada a Central de Monitoramento em caso de senha de coação, não exibindo a mensagem anterior.			Informação não disponível na documentação apresentada
· A controladora deve identificar o acionamento para fechamento da agência mediante um caractere ou código especial inserido após a verificação do usuário;			Informação não disponível na documentação apresentada
· Cada controladora de reconhecimento facial estará cadastrada no sistema da Central de Monitoramento com identificação do local controlado;			Informação não disponível na documentação apresentada
· A controladora de reconhecimento facial deve utilizar chave de encriptação, devendo ser configuráveis para cada controladora de acordo com o padrão de segurança do BASA;	X		
· A controladora de reconhecimento facial deve permitir que a carga de dados e informações dos usuários seja feita pelo Servidor do Sistema através da rede de comunicação de forma totalmente transparente aos usuários sem interrupção do seu funcionamento normal;	X		
· Deve permitir a comunicação com o Servidor do Sistema mesmo que este esteja instalado em sub-rede distinta do local onde está instalada a controladora;	X		

· Deverá funcionar através de verificação de firewall, sem perda de comunicação, por meio de porta disponibilizada pela área de tecnologia do BASA;	X			
· Deve permitir que a captura da face digital de um usuário seja feita no próprio equipamento sob comando remoto do Sistema Central de Monitoramento dispensando a necessidade de equipamentos adicionais para o cadastramento de usuários ou ainda que estes se desloquem de seu local de trabalho;	X			
· A memória do equipamento deve manter todos os registros de ocorrências até que a coleta e armazenamento no Servidor de banco de dados do sistema;	X			
· A controladora de reconhecimento facial deve ter capacidade de armazenar localmente pelo menos 1.000 (mil) registros de ocorrências;	X			
· Monitorar o estado de uma porta controlada (aberta/fechada), bem como detectar as aberturas autorizadas, forçadas ou situações de porta por tempo excessivo (time-out de porta aberta).				Informação não disponível na documentação apresentada
· Todas as ocorrências de aberturas e fechamento de porta devem ser registradas;	X			
· Todos os eventos devem ser registrados, tais como: acessos solicitados, acessos realizados, tentativas frustradas de acesso, biometrias inválidas, horários proibidos, porta forçadas, etc;	X			

Realização de atualização remotamente pela rede TCP/IP, de forma que quando houver correções, implantações de novas funções, novos recursos ou melhorias a atualização seja possível remotamente; correções, implantações de novas funções, novos recursos ou melhorias a atualização seja possível remotamente;	X		
O visor de cristal líquido deve possuir no mínimo 2 (duas) linhas de 16 (dezesseis) caracteres cada com retro-iluminação (backlight);	X		
Permitir comunicação via protocolo SNMP por meio de aplicativo do BASA para verificação do status de funcionamento;			Informação não disponível na documentação apresentada
Deverá possibilitar a instalação nas posições horizontal ou vertical e garantir que o mecanismo de travamento e fios fiquem posicionados no lado interno da unidade;	X		
Protocolo 802.1X (padrão IEEE para controle de acesso à rede baseado em porta PNAC).			Informação não disponível na documentação apresentada
2.7 CONTROLE DE PORTA DE ENROLAR	ATENDE	NÃO ATENDE	COMENTÁRIOS
· Deverá prover capacidade de abertura e fechamento remoto com opção de ativação manual pelo operador do software de monitoramento e por programação automática de horário e dias de abertura e fechamento através do acionamento do(s) motor(es) de abertura, parada (se o motor permitir) e			Documentação não enviada

fechamento da(s) porta(s) de aço de enrolar.			
· Deverá ser sistema integrado com a central de alarme e/ou ter sensor independente de forma a identificar presença no ambiente de pessoas e neste caso não efetuar o fechamento e enviar alarme para Central de Monitoramento, postergando o procedimento de fechamento em 05 (cinco) minutos, em caso de manter a situação na segunda tentativa de fechamento o sistema deverá enviar novo alerta de impossibilidade passando a operação para ser realizada manualmente com intervenção e sob responsabilidade visual da sala de monitoramento.			Documentação não enviada
· Sistema deve prever sensor de confirmação de fechamento e de abertura.			Documentação não enviada
· Deve permitir registro completo de logs de alarmes, atividades executadas, registros de ações manuais com identificação no software de monitoramento e controle integrado.			Documentação não enviada
· Sistema deve possuir bateria com capacidade de manter placas de controle por 12 horas.			Documentação não enviada
2.7.1 Porta de enrolar automática é fabricada com perfis em aço galvanizado, podendo usar na folha, chapa #22 ou chapa 20#, automatizadas com botoeira, corrente para acionamento manual. A definição da potência do motor dependerá das dimensões e principalmente do peso da porta a ser instalada. O posicionamento da porta, da botoeira e do motor será pela Área de Arquitetura do Banco.	ATENDE	NÃO ATENDE	COMENTÁRIOS
2.7.2 Automatizador de Portas de Enrolar: são componentes que realizará a movimentação da porta de enrolar automática para abertura e fechamento. O Conjunto é composto			

fundamentalmente por: AUTOMATIZADOR: de utilização exclusiva para portas de enrolar. Contém várias capacidades e tamanhos. Deve ser definido pelo peso, tamanho e ciclo de funcionamento da Porta de Enrolar			Documentação não enviada
2.8 VIDEO WALL E SALA DE MONITORAMENTO	ATENDE	NÃO ATENDE	COMENTÁRIOS
· Deve ser fornecimento um vídeo wall, que contenha 4 monitores profissionais de 55”, borda ultrafina, no formato 2x2, com monitores individuais, que pode apresentar um conteúdo com alto nível de detalhes gráficos, ou uma imagem única em todas as telas, semelhante a aplicação de projetos de comunicação visual digital.	X		
· A solução de vídeo wall deve permitir ser instalada em parede de alvenaria ou dry-wall reforçado, teto ou viga, ou mesmo em um sistema autoportante, com suportes de fixação.	X		
· Tela IPS (ângulo de visão 178/178),			Informação não disponível na documentação apresentada
· Resolução 1920x1080.	X		
· Brilho máx 500 nits.	X		
· Conexões: 2xHDMI/1xDP/1xDVI.	X		
· Largura de Borda: 2,25 mm (U/L), 1,25 mm (R/B).		X	
· Dimensão: 1.213,5 x 684,3 x 73,1 mm.		X	

· Suportes de fixação em parede de alvenaria ou dry-wall reforçado e cabeamento.			Informação não disponível na documentação apresentada
· A configuração de montagem, será em conjunto de 4 telas na montagem de 2 colunas por 2 linhas, gabaritados com ajuste fino para o perfeito alinhamento entre os módulos.			Informação não disponível na documentação apresentada
· Deve estar incluso todos os cabos, os cabos de vídeo HDMI deve ser blindados.			Informação não disponível na documentação apresentada
· Fechamentos laterais e inferior (molduras), na cor preto fosco.			Informação não disponível na documentação apresentada
· Instalação, alinhamento dos monitores, configuração;			Informação não disponível na documentação apresentada
2.8.1Gerenciador Gráfico Vídeo Wall	ATENDE	NÃO ATENDE	COMENTÁRIOS
· Processador compatível com a solução proposta de vídeo wall,			Documentação não enviada
· Memória RAM instalada 16GB RAM,			Documentação não enviada
· Memória não volátil de 480GB tipo SSD em raid1,			Documentação não enviada
· Sistema Operacional Windows 11 Pro,			Documentação não enviada
· 4 saídas de vídeo digitais independentes.			Documentação não enviada
2.8.2Ferramenta de colaboração	ATENDE	NÃO ATENDE	COMENTÁRIOS

· Gerenciar Identidade, acesso e usuário, com suporte para mais 200 funcionários			Documentação não enviada
· A ferramenta de colaboração deve utilizar e-mail empresarial (nome@suaempresa.com.br), não será aceito ferramentas de nivel doméstico.			Documentação não enviada
· Versões web e móvel dos aplicativos, bem como plataforma de e-mail.			Documentação não enviada
· A ferramenta deve disponibilizar em nuvem, 1 TB de armazenamento por funcionário e que possua recursos de compartilhamento com o BASA e colaboradores.			Documentação não enviada
· Deve possuir filtragem automática e bloqueio de malware e spam			Documentação não enviada
· Suporte por telefone ou pela web, com suporte 24x7x365, com SLA máximo de 4 horas.			Documentação não enviada
· Licenças para os 5 anos de contrato.			Documentação não enviada
· Deve possuir recursos de reunião online, com áudio e vídeo, para no mínimo 20 colaboradores ao mesmo tempo, sem um limite de tempo preestabelecido.			Documentação não enviada
2.8.3Mobiliário da sala de monitoramento a cargo da Contratada	ATENDE	NÃO ATENDE	COMENTÁRIOS
· A Sala de Monitoramento, deverá abrigar, confortavelmente, os operadores que ali estão de plantão no videomonitoramento, bem como os equipamentos destinados a esse fim. O Layout da			

sala de operações deverá possuir toda a infraestrutura no mínimo duas estações de monitoramento e 1 estação para o Supervisor, incluindo todos os equipamentos necessários para atividades dos colaboradores da Contratada que estarão locados nesta sala, cabendo a Contratante somente ceder o espaço necessário para as instalações da sala de monitoramento.			Documentação não enviada
· O supervisor deve estar alocado em mesa separada dos operadores.			Documentação não enviada
· O painel de visualização de imagens, tipo vídeo wall, ficará em frente as estações de operação			Documentação não enviada
· As estações de operação mesas individuais ou móvel planejado para dois operadores considerando 2 monitores de 21 polegadas para cada operador, 2 estações de computador e demais mobiliários que sejam demandados pela contratada para executar suas atividades devem ser de madeira, de boa qualidade em cor preta, deverão estar adequados para melhor visualização dos monitores dos colaboradores, bem como o vídeo wall.			Documentação não enviada
· As cadeiras, disponibilizadas para os operadores e supervisores, deverão ser do tipo Gamer e na cor preta.			Documentação não enviada
· Projeto da sala de monitoramento com descrição de mobiliário deverá ser apresentado junto com cronograma de instalações para que seja aprovado pela Contratante.			Documentação não enviada
· A Contratada deve zelar por manter durante toda permanência do contrato o mobiliário, equipamentos e todos os itens pertinentes da sala de monitoramento em perfeito estado e deverá atender qualquer demanda da Contratante apontando inconformidades com projeto			Documentação não enviada

aprovado e ou necessidades adicionais que surjam no decorrer do contrato.			
2.8.4 MONITOR DE 21,5 POLEGADAS	ATENDE	NÃO ATENDE	COMENTÁRIOS
Tamanho da tela mínima (Polegadas): 21”	X		
Contraste mínimo: 30.000:1 DFC		X	
Tempo de Resposta: 5ms	X		
Brilho: 300 cd/m²		X	
Resolução: 1920 x 1080 @ 60Hz	X		
Conector de entrada: RGB IN (PC) / HDMI IN	X		
Sinal de Vídeo: Analógico / Digital		X	
Conexões: RGB IN (PC) / HDMI IN / Componente IN	X		
2.9 SOFTWARE DE MONITORAMENTO. A) ARQUITETURA DO SOFTWARE	ATENDE	NÃO ATENDE	COMENTÁRIOS
O Software de Monitoramento e Controle deve integrar em ferramenta única para os operadores permitindo total monitoramento, controle, programações de horários, cadastros, registros de observações, relatórios, e todas funções previstas para os itens 2.1 Alarme, 2.2 CFTV, 2.3 Geradores de Neblina e Sistemas de Defesas Ativas, 2.4 Controles de Acesso,			Documentação enviada não informa atendimento
2.5 Controles de Portas de Aço de enrolar, 2.6 Sistema de Vídeo Wall, assim como integração e controle do sistema de cofres existente, provendo			

todas as funcionalidades descritas ao longo deste item em uma solução única, composta por uma única interface de utilização completando todas funções com sistema gerador de analíticos também integrado como ferramenta única;			Documentação enviada não informa atendimento
A solução deverá ser composta por funcionalidades que possibilitem a verificação do estado de segurança de todas unidades monitoradas remotamente, deve prover capacidade de acionamento remoto de todos dispositivos integrados com vistas à mitigação de ocorrências/ações criminosas, assim como garantindo suportes aos clientes e funcionários para aberturas assistidas, recebimentos de acionamentos de botão de pânico e funções de controles geradas pelos analíticos disponíveis como por exemplo, detecções de cruzamento de linhas, permanências em locais monitorados, objetos deixados ou removidos, anomalias de qualquer tipo, contagem de pessoas, identificação de mais de uma pessoa parada em local monitorado com riscos de ser um ato anormal, etc.			Documentação enviada não informa atendimento
Possuir capacidade de receber modificações e melhorias para adaptar-se as necessidades identificadas pelo BASA, o que inclui demandas futuras para se integrar com outros equipamentos que se façam necessários/desejados pela área de segurança BASA.			Documentação enviada não informa atendimento
Possibilitar o desenvolvimento dos serviços de monitoramento de eventos envolvendo os ambientes monitorados como origem ou destino, além da gestão de ações e respostas no tratamento de diversas situações identificadas nestes ambientes e municiando a ativação dos dispositivos de monitoramento.			Documentação enviada não informa atendimento
Funcionar em ambas as Centrais de			

Monitoramento do BASA (local e remota como back up) como uma única solução, de modo que, quando necessário, uma Central de Monitoramento possa realizar a gestão remota ao mesmo tempo.			Documentação enviada não informa atendimento
As integrações deverão prover todas as interligações físicas e lógicas necessárias para conexão e comunicação entre a solução e os sistemas, equipamentos ou dispositivos de monitoramento ativos.			Documentação enviada não informa atendimento
Possuir e disponibilizar biblioteca de APIs, SDK, DLL para fornecer aos desenvolvedores os recursos que esses necessitam para integrar sensores de terceiros, sistemas e dispositivos.			Documentação enviada não informa atendimento
Possuir uma arquitetura que permita integrações de forma a não afetar a funcionalidade principal do produto/sensor e sua estabilidade.			Documentação enviada não informa atendimento
Todas as interfaces do sistema são 100% web, acessíveis através dos navegadores Google Chrome 115 (ou superior) ou Mozilla Firefox 110 (ou superior);			Documentação enviada não informa atendimento
O software deve realizar funções/rotinas relacionadas ao monitoramento e tratamento de eventos, configuração, atuação nos equipamentos, emissão de relatórios de texto e gráficos sem a instalação de programas cliente na estação de trabalho.			Documentação enviada não informa atendimento

Trabalhar com Centrais IP simultaneamente conectadas ao servidor de comunicação.			Documentação enviada não informa atendimento
O sistema deve ser baseado na arquitetura “cliente/servidor” permitindo que o servidor realize as tarefas de comunicação, gerenciamento, operação e monitoramento simultaneamente, além de diversas outras tarefas (geração de relatórios, configuração, etc.);			Documentação enviada não informa atendimento
A execução de uma tarefa não deve interfere na execução de outra, sem limite de clientes conectados (de acordo com a capacidade do servidor).			Documentação enviada não informa atendimento
Suportar o monitoramento de imagens via servidor de imagens (VMS) ou via conexão direta com os NVRS e as câmeras.			Documentação enviada não informa atendimento
Poder trabalhar com dois ou mais processadores, dividindo as tarefas do software nos processadores disponíveis a fim de aumentar o desempenho do sistema.			Documentação enviada não informa atendimento
Deve ser instalado em Sistemas Operacionais de 64 bits, Windows Server 2019 ou superior, Linux em versões Enterprise (com subscrição ativa de suporte).			Documentação enviada não informa atendimento
Permitir rodar o sistema em Banco de Dados SQL Server 2016 ou superior, bem como PostgreSQL 12 ou superior.			Documentação enviada não informa atendimento

Permitir que a operação possa ser executada em um Cluster de Banco de Dados.			Documentação enviada não informa atendimento
Permitir instalação e operação com balanceamento de carga e failover.			Documentação enviada não informa atendimento

Trabalhar com sistema de licenciamento por Centrais de Alarme IP cadastradas, permitindo a expansão livremente do sistema com licenças adicionais.			Documentação enviada não informa atendimento
Permitir a separação das centrais de alarme em regiões, para serem monitoradas por diferentes grupos de usuários, se assim necessário.			Documentação enviada não informa atendimento
Suportar a gestão de "inúmeras" centrais por servidor, sendo que o limite máximo de centrais deve ser de acordo com a capacidade de disco e de processamento do servidor. O software não possui limitação do número de centrais por servidor.			Documentação enviada não informa atendimento
a. O software cliente de monitoramento e controle será acessado via web pelas estações de monitoramento da Central de Monitoramento e deverá comandar todos os componentes deste edital, assim como ser capaz de assumir todas demais UCM constituindo uma central única para gerenciar todos os equipamentos instalados em caso de contingência.			Documentação enviada não informa atendimento
O software cliente deverá se conectar ao servidor de aplicação para efetuar a monitoramento e o gerenciamento de todos os ativos deste contrato.			Documentação enviada não informa atendimento
O software cliente deve ser de uso livre, não exigindo uso de licença e deverá ser instalado em quantos computadores forem indicados pelo BASA.		X	Depende de Licenças

3- ESPECIFICAÇÃO DOS SERVIÇOS DE MONITORAMENTO POR IMAGENS E SINAIS DE ALARME. 3.1 REQUISITOS TÉCNICOS GERAIS DA SOLUÇÃO INTEGRADORA 3.1.1 DESCRIÇÃO DA SOLUÇÃO	ATENDE	NÃO ATENDE	COMENTÁRIOS
3.1.1.2 Fornecimento de solução integradora dos equipamentos de segurança com a gestão, acionamento e tratamento de informações de segurança e realização da integração nas unidades BASA, incluindo a cessão de direito de uso dos softwares, hardwares (quando instalado em modo on premises para o funcionamento da solução) e soluções de middleware (integradores), em caso de uso de infraestrutura de nuvem pública.			Documentação enviada não informa atendimento
O objeto de contratação deve contemplar ainda a disponibilização segregada dos ambientes			Documentação enviada não informa atendimento
tecnológicos de produção e de homologação (on premises ou nuvem), serviços de parametrização e configuração inicial da ferramenta, incluindo as integrações com os equipamentos a serem fornecidos.			Documentação enviada não informa atendimento
A solução deverá ser composta por funcionalidades que possibilitem a verificação do estado de segurança on line das unidades monitoradas remotamente, e o acionamento remoto de dispositivos com vistas à mitigação de ocorrências/ações criminosas.			Documentação enviada não informa atendimento
A solução deve interligar eventos de alarmes com pop-up de respectiva câmera do local e em caso de haver dispositivos de defesa incluindo no mesmo			Documentação enviada não informa atendimento

pop-up as opções de defesas do ambiente em alarme.			
Possuir capacidade de receber modificações e melhorias para adaptar-se as necessidades identificadas pelo BASA.			Documentação enviada não informa atendimento
Ser integrável com dispositivos de segurança que realizam o monitoramento e gerenciamento dos componentes no atual parque do BASA, ou futuro no caso de novas integrações, respeitando a limitação das funcionalidades disponíveis na API dos fabricantes.			Documentação enviada não informa atendimento
Possibilitar o desenvolvimento dos serviços de monitoramento de eventos envolvendo os ambientes monitorados como origem ou destino, além da gestão de ações e respostas no tratamento de diversas situações identificadas nestes ambientes e municiando a ativação dos dispositivos de monitoramento.			Documentação enviada não informa atendimento
Funcionar como uma única solução incluindo recepção dos analíticos de vídeos.			Documentação enviada não informa atendimento
As integrações deverão prover todas as interligações físicas e lógicas necessárias para conexão e comunicação entre a solução e os sistemas, equipamentos ou dispositivos de monitoramento ativos.			Documentação enviada não informa atendimento
A solução deverá realizar a troca de informações com sistemas de monitoramento e gerenciamento legados.			Documentação enviada não informa atendimento
O objetivo primordial é reduzir a quantidade de interfaces sistêmicas adotados nas Centrais de Monitoramento, unificando a visão de múltiplos sistemas em uma única interface,			

possibilitando,através da solução integradora, o gerenciamento de disponibilidade dos ativos, bem como que as diversas tarefas realizadas por diferentes monitoradores passem a ser realizadas por um mesmo operador.			Documentação enviada não informa atendimento
A CONTRATADA é responsável por disponibilizar todos os softwares intermediários e respectivos acessórios, como plugins e licenças, necessários para ativação dos serviços e funcionalidades requeridos pelo BASA, não podendo se eximir de quaisquer responsabilidades e ações junto aos fabricantes e fornecedores para atender as necessidades do BASA.			Documentação enviada não informa atendimento
Fornecer interface amigável para elaborar a modelagem de processos de monitoramento e fluxos operacionais, não exigindo dos usuários conhecimento especializado de tecnologias de informação.			Documentação enviada não informa atendimento
Permitir através desta interface a criação de fluxos operacionais com tarefas automáticas ou manuais vinculados aos processos de monitoramento do BASA.			Documentação enviada não informa atendimento
Permitir a customização e adaptação dos fluxos operacionais e processos de monitoramento já existentes ou que venham a ser estabelecidos.			Documentação enviada não informa atendimento
Possuir arquitetura projetada e construída com capacidade de integração com sistemas de segurança física a serem implantados no BASA de forma a permitir receber eventos e enviar comandos dos dispositivos de detecção de intrusão, sistemas de vídeo/áudio, controladores de acesso e geradores de			Documentação enviada não informa atendimento

neblina.			
Possuir e disponibilizar biblioteca de APIs, SDK, DLL para fornecer aos desenvolvedores			Documentação enviada não informa atendimento
os recursos que esses necessitam para integrar sensores de terceiros, sistemas e dispositivos.			Documentação enviada não informa atendimento
Essas bibliotecas fazem parte dos sistemas e licença que serão fornecidas ao BASA, concomitantemente, com autorização expressa para fornecimentos destas para terceiros desenvolverem dispositivos e recursos para integração com as funcionalidades da solução.			Documentação enviada não informa atendimento
Possuir uma arquitetura que permita integrações de forma a não afetar a funcionalidade principal do produto/sensor e sua estabilidade.			Documentação enviada não informa atendimento
Possuir a capacidade de informar ao usuário quando jobs, scripts, rotinas e serviços estiverem apresentando erro ou falha de operação.			Documentação enviada não informa atendimento
Possuir uma documentação completa em língua portuguesa (português brasileiro), com cópia eletrônica, dos produtos, contemplando guias de instalação, administração do sistema e personalização.			Documentação enviada não informa atendimento
Atuar como um gestor para as funções de segurança e operações, unificando o comando operacional e facilitando seu controle via interface gráfica do usuário.			Documentação enviada não informa atendimento
Disponibilizar a informação a ser consultada em tempo real pelos intervenientes envolvidos, bem			

como a localização dos eventos e dispositivos relacionados à ocorrência em análise, permitindo uma melhor gestão das atividades e planejamento do trabalho.			Documentação enviada não informa atendimento

Possuir funcionalidade para fazer a gestão dos ativos interligados na solução e apresentar em visão gerencial, de forma que seja possível ao usuário visualizar todos os equipamentos, por Unidade, por Município, por UF, de forma que sejam apresentados os tipos de equipamentos, ambientes onde estão instalados, se estão disponíveis (online ou offline), percentual de disponibilidade, número de IP correspondente a cada um, com os respectivos filtros correspondentes.			Documentação enviada não informa atendimento
Realizar a gestão, gerenciamento, supervisão, operação e auditoria dos processos de tratamento de eventos originários dos canais de monitoramento do BASA, de acordo com as limitações da API do fornecedor.			Documentação enviada não informa atendimento
IDIOMA	ATENDE	NÃO ATENDE	COMENTÁRIOS
A Solução ofertada deverá fornecer todas as interfaces de acesso dos usuários finais ao sistema no idioma português do Brasil.			Documentação enviada não informa atendimento
Todos os relatórios disponibilizados pela Solução ofertada deverão estar no idioma português do Brasil.			Documentação enviada não informa atendimento
Todos os artefatos gerados pela CONTRATADA deverão estar no idioma português do Brasil.			Documentação enviada não informa atendimento
DESEMPENHO	ATENDE	NÃO ATENDE	COMENTÁRIOS
A Solução deverá estar disponível para			Documentação enviada não informa

funcionamento ininterrupto (24X7).			atendimento
A Solução deverá garantir disponibilidade de 99,99% no período de segunda a sexta-feira, das 08h às 20h.			Documentação enviada não informa atendimento
Solução deverá garantir disponibilidade de 98% nos demais períodos.			Documentação enviada não informa atendimento
As interações com os clientes deverão possuir limite de latência de forma que seja possível, através da solução integradora, identificar uma situação, acionar um mecanismo de resposta e a execução efetiva da resposta no equipamento de segurança, em tempo máximo de 5 (cinco) segundos, contados a partir do momento da identificação do evento e o acionamento do mecanismo de resposta na solução integradora, desconsiderando as variações naturais na REDE BASA			Documentação enviada não informa atendimento
Garantir o acesso simultâneo da quantidade de usuários definida sem comprometimento de desempenho e/ou estabilidade, incluindo balanceamento de distribuição de eventos de forma automática com base nos operadores que estejam logados no momento dos eventos.			Documentação enviada não informa atendimento
LEGAIS	ATENDE	NÃO ATENDE	COMENTÁRIOS
Estar aderente à Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n 13.709/2018 e demais legislações vigentes.			Documentação enviada não informa atendimento
Em caso de soluções providas em Nuvem, devem estar aderentes à norma 05/2021/GSI/PR, que dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de			Documentação enviada não informa

computação em nuvem pelos órgãos e pelas entidades da administração pública federal.			atendimento
Estar aderente à resolução CMN n°4893/2021 nos pontos complementares à supracitada. Neste caso, os dados, meta dados e informações produzidos devem estar hospedados em território brasileiro.			Documentação enviada não informa atendimento
Estar aderente à legislação e normas vigentes que possuam relação com o objeto do contrato.			Documentação enviada não informa atendimento
ACESSIBILIDADE	ATENDE	NÃO ATENDE	COMENTÁRIOS
A Solução deverá seguir os padrões W3C no que se refere a acessibilidade e compatibilidade com os navegadores.			Documentação enviada não informa atendimento
A Solução deverá possuir aderência às Diretrizes de Acessibilidade para Conteúdo Web (WCAG)			Documentação enviada não informa atendimento
DOCUMENTAÇÃO	ATENDE	NÃO ATENDE	COMENTÁRIOS
Deverá fornecer a documentação de todos os serviços disponibilizados pela Solução, bem como os respectivos contextos de uso e formas de acesso – manual operacional – no formato on-line/digital.			Documentação enviada não informa atendimento
Realizar a transferência de conhecimento para que multiplicadores BASA possuam os conhecimentos necessários para utilização das soluções criadas ou já constantes nativamente na plataforma.			Documentação enviada não informa atendimento

Disponibilizar materiais que serão utilizados na transferência de conhecimento em idioma português do Brasil.			Documentação enviada não informa atendimento
ARQUITETURA	ATENDE	NÃO ATENDE	COMENTÁRIOS
Os componentes cliente da solução devem:			Documentação enviada não informa atendimento
Suportar os seguintes softwares de apoio: Microsoft Office versão 2016, Adobe Acrobat Reader DC, e respectivas versões superiores lançadas até a data de assinatura do contrato.			Documentação enviada não informa atendimento
A arquitetura deve evitar a duplicidade de dados, de forma que todos os eventos, comandos, registros e informações tratadas por uma Central de Monitoramento não sejam apagados ou sobrepostos pelo tratamento de eventos, comandos, registros ou informações oriundas das outras Centrais de Monitoramento.			Documentação enviada não informa atendimento
Em caso de uso de sistema em nuvem ou portabilidade futura do sistema para nuvem, retirando o sistema on primese, a CONTRATADA, deve instalar servidores de middleware, para que todos os serviços de nuvem, não tenham qualquer conexão com a rede do BASA. Não será aceito nenhuma conexão externa para a rede LAN.			Documentação enviada não informa atendimento
BANCO DE DADOS	ATENDE	NÃO ATENDE	COMENTÁRIOS

A solução deve garantir a integridade das informações, ou seja, ter a capacidade de desfazer transações incompletas e manter a consistência das informações na base de dados, ou auditar todos os incidentes e ações relacionadas executadas, concluídas ou incompletas.			Documentação enviada não informa atendimento
Suportar mecanismos para permitir o expurgo de dados conforme regras a serem definidas pelo BASA.			Documentação enviada não informa atendimento
A ferramenta deverá atender as regras descritas na lei nº 13.709 (LGPD) para expurgo dos dados.			Documentação enviada não informa atendimento
A critério do BASA e prévio comunicado a CONTRATADA, as regras de expurgo e murchação poderão ser redefinidas ao longo da vigência do contrato.			Documentação enviada não informa atendimento
O BASA poderá ter acesso irrestrito aos dados através da aplicação do serviço de monitoração.			Documentação enviada não informa atendimento
A CONTRATADA deverá, a pedido do BASA, disponibilizar cópias dos dados persistidos (imagens, áudio, comandos para dispositivos, informações sobre procedimentos tomados quanto às ocorrências diversas) mediante acordo e agenda acordada entre as partes.			Documentação enviada não informa atendimento
A solução deve implementar o acesso simultâneo e concorrente de múltiplos usuários ao sistema, para pesquisa e edição, preservando a integridade dos dados.			Documentação enviada não informa atendimento
Dispor de um banco de dados escalável para suportar muitos usuários simultâneos e taxas de			Documentação enviada não informa atendimento

transações de medio e grande porte.			
Permitir o armazenamento e a consulta dos dados administrativos, operacionais e históricos em um banco de dados.			Documentação enviada não informa atendimento
Os servidores da camada de banco de dados deverão ser segregados dos demais servidores da solução.			Documentação enviada não informa atendimento
REDE	ATENDE	NÃO ATENDE	COMENTÁRIOS
Possuir compatibilidade com os protocolos IP (Intenet Protocol) versão 4 e versão 6.			Documentação enviada não informa atendimento

Possuir compatibilidade com os serviços DNS (Domain Name Server), de forma transparente para resolução de nomes de registros tipo A ou AAAA.			Documentação enviada não informa atendimento
Possuir compatibilidade com os protocolos: TCP/IP, HTTP, HTTPS, FTP, DNS, RTCP, UPnP, UDP.			Documentação enviada não informa atendimento
Deverá ainda prever para o servidor suporte ao protocolo NTP (Network Time Protocol) para sincronismo de horário.			Documentação enviada não informa atendimento
Havendo necessidade de conexão externa, a solução deverá permitir que equipamentos de borda se comuniquem com os servidores através da rede WAN do BASA (firewall).			Documentação enviada não informa atendimento
Suportar a configuração do número da porta TCP/UDP dos componentes da solução.			Documentação enviada não informa atendimento
A solução deve permitir o balanceamento de carga.			Documentação enviada não informa atendimento
Incluir rotinas de recuperação dos serviços, como por exemplo, reiniciar um serviço, notificações por e-mail, LAN, quando um número de tentativa de reinicialização predefinido seja ultrapassado.			Documentação enviada não informa atendimento
SEGURANÇA	ATENDE	NÃO ATENDE	COMENTÁRIOS
A CONTRATADA deve adotar mecanismos que garantam a segurança da informação conforme os			Documentação enviada não informa

conceitos de confidencialidade, disponibilidade, integridade e pertinência da informação, conforme descritos abaixo.			atendimento
Confidencialidade é entendida como o princípio de segurança da informação pelo qual é garantido o acesso à informação a usuários autorizados e vedado o acesso a usuários não autorizados.			Documentação enviada não informa atendimento
Entende-se por disponibilidade o princípio de segurança da informação pelo qual é garantido o acesso a usuários autorizados sempre que necessário.			Documentação enviada não informa atendimento
Entende-se por integridade o princípio de segurança da informação que garanta a inviolabilidade do conteúdo da informação.			Documentação enviada não informa atendimento
Pertinência é o princípio de segurança da informação pelo qual se restringe o acesso apenas aos usuários que necessitem da informação.			Documentação enviada não informa atendimento
A Solução deve permitir a autenticação utilizando padrão de federação de identidade OpenID Connect/OAuth 2.0 com o fluxo Authorization Code e também SAML 2.0 permitindo a associação de políticas/perfis às estruturas de grupos e subgrupos			Documentação enviada não informa atendimento
A Solução deverá permitir a definição de segurança por usuário ou por grupo (perfil), levando também em consideração a estrutura organizacional da empresa.			Documentação enviada não informa atendimento

A Solução deve permitir listar as permissões dos usuários, onde seja possível classificá-los de acordo com variados perfis e permissões de acesso.			Documentação enviada não informa atendimento
Caberá ao BASA, após conhecimento da Solução adquirida definir qual das formas de controle de acesso lógico listadas será adotada.			Documentação enviada não informa atendimento
A Solução deverá possuir relatórios e registros de auditoria detalhados, que identifiquem o histórico completo de acessos (logins) e ações, por cada usuário ou grupo de usuários, incluindo as contas administrativas e com privilégios. Estes registros devem ser protegidos contra adulteração.			Documentação enviada não informa atendimento
O acesso a trilha de auditoria será efetuado por usuário autorizado.			Documentação enviada não informa atendimento
Os registros de trilha de auditoria devem ser protegidos contra adulteração.			Documentação enviada não informa atendimento
A trilha de auditoria deverá ficar disponível mesmo nos casos de cancelamento ou estorno de operações, pelo período determinado pela BASA e conforme legislação vigente.			Documentação enviada não informa atendimento
Qualquer alteração dos parâmetros deve ser registrada em trilha de auditoria.			Documentação enviada não informa atendimento
O procedimento para entrada no sistema deve ser configurado para proibir acessos não autorizados.			Documentação enviada não informa atendimento
A Solução não deve mostrar a senha que está sendo informada.			Documentação enviada não informa atendimento
A Solução não deve transmitir senhas em texto			Documentação enviada não informa

claro pela rede.			atendimento
Solução deverá encerrar sessões inativas após período de inatividade configurado pelo BASA.			Documentação enviada não informa atendimento
O tempo limite para sessões e log-off em caso de inatividade poderá ser alterado conforme interesse do BASA.			Documentação enviada não informa atendimento
A Solução deve suportar criptografia TLS 1.2 ou superior.			Documentação enviada não informa atendimento
O tráfego das informações entre os servidores da solução e os navegadores e browsers instalados nas estações do BASA deverá ser feito de forma criptografada, com utilização do protocolo SSL/https.			Documentação enviada não informa atendimento
A Solução deverá possuir mecanismo de monitoração com geração de logs, evento para armazenamento de dados históricos de desempenho, falhas e disponibilidade da solução como um todo e de suas principais funcionalidades e componentes, contemplando integração com a solução de monitoração definida pelo BASA.			Documentação enviada não informa atendimento
A Solução deverá prover a criptografia de arquivos em repouso, caso não sejam armazenados criptografados no SGDB, utilizando chave simétrica usando, no mínimo, algoritmo AES com 128 bits ou 3DES com 168 bits.			Documentação enviada não informa atendimento
A Solução deverá possuir capacidade de autenticação mútua através da troca de			Documentação enviada não informa atendimento

certificados digitais.			
A Solução deverá permitir a execução de processos de gestão de vulnerabilidades e de aplicação de patches para identificar e corrigir vulnerabilidades no ambiente.			Documentação enviada não informa atendimento
A Solução fornecida deverá garantir que o desenvolvimento possua políticas e procedimentos estabelecidos para o desenvolvimento seguro, controle de mudança dos sistemas, segregação do ambiente de desenvolvimento e produção, testes de segurança, aceitação, e proteção dos dados em ambiente de produção.			Documentação enviada não informa atendimento
A CONTRATADA deverá dispor de mecanismos para realizar regularmente testes de segurança da informação (incluindo análise e tratamento de riscos, verificação de vulnerabilidades, avaliação de segurança da Solução e testes de penetração) podendo o BASA realizar auditorias, inclusive com apoio de terceira parte, para comprovar que a solução mantém esse requisito.			Documentação enviada não informa atendimento
A CONTRATADA deverá fornecer ao BASA, sempre que solicitado, informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de dados do BASA.			Documentação enviada não informa atendimento
A CONTRATADA deverá manter a confidencialidade de toda a informação a respeito dos negócios, ideias, produtos, clientes ou serviços da outra parte, que podem ser consideradas como “informação confidencial”.			Documentação enviada não informa atendimento
A CONTRATADA não deverá veicular publicidade acerca do fornecimento de materiais,			

equipamentos ou serviços objeto deste contrato, que envolva o nome do BASAA, salvo se houver autorização expressa desta.			Documentação enviada não informa atendimento
A CONTRATADA deverá identificar e corrigir qualquer problema de segurança na solução, sem qualquer custo adicional para o BASA.			Documentação enviada não informa atendimento
Toda a solução deverá ser capaz de funcionar integralmente em ambientes protegidos por sistemas de segurança do tipo appliance Multifunção (Firewall e IPS) com aplicação de inspeção statefull de tráfego de rede e capacidade de identificação e bloqueio de ataques, incluindo ataques direcionados ao equipamento.			Documentação enviada não informa atendimento
SUPORTE TÉCNICO	ATENDE	NÃO ATENDE	COMENTÁRIOS
A CONTRATADA deverá prestar o serviço de suporte para assegurar a disponibilidade do sistema, em horário integral – 7 dias x 24 horas x 365 dias no ano, a fim de oferecer suporte à utilização e funcionamento das funcionalidades oferecidas pela solução integradora.			Documentação enviada não informa atendimento

O suporte técnico deverá ser realizado por telefone, e-mail, site na internet, ferramenta de comunicação instantânea via internet e outros meios sugeridos pela CONTRATADA e autorizados pelo BASA.			Documentação enviada não informa atendimento
A CONTRATADA deverá prestar o serviço de suporte técnico presencial nas unidades do BASA sempre que se deparar com uma das seguintes situações:			Documentação enviada não informa atendimento
Receber uma mensagem de erro e não conseguir solucionar a ocorrência remotamente com			Documentação enviada não informa atendimento
base nas instruções contidas em documentação fornecida;			Documentação enviada não informa atendimento
Irregularidades no comportamento da solução e não conseguir solucioná-las remotamente com base nas instruções contidas em documentação fornecida;			Documentação enviada não informa atendimento
Surgimento de dúvidas sobre a infraestrutura de rede e a conectividade da solução com o BASA que não possam ser esclarecidas remotamente através das informações contidas na documentação fornecida;			Documentação enviada não informa atendimento
OUTROS	ATENDE	NÃO ATENDE	COMENTÁRIOS
A Solução deverá ter o tempo sincronizado com a hora legal brasileira ou de acordo com fuso horário definido pelo BASA.			Documentação enviada não informa atendimento

A Solução fornecida deverá garantir que qualquer implementação ou parametrização realizada na plataforma NÃO seja impeditivo de evolução de versão dela.			Documentação enviada não informa atendimento
Todos os componentes da Solução deverão ser completamente integrados e interoperáveis entre si.			Documentação enviada não informa atendimento
Todos os componentes da Solução tecnológica devem estar em linha de produção do fabricante, não sendo aceito soluções e/ou componentes com previsão de descontinuidade, end- of-support ou end-of- life.			Documentação enviada não informa atendimento
A solução deve ser interoperável compatível para se desejável pelo BASA também poder operar em diferentes fornecedores de nuvem, sem que haja qualquer dependência aos ambientes de nuvem providos (lock-in).			Documentação enviada não informa atendimento
Na ocasião dos eventos para treinamento, a CONTRATADA deverá apresentar ao BASA.			Documentação enviada não informa atendimento
Manual de operação, em português brasileiro, contendo todos os procedimentos operacionais necessários para o gerenciamento eficaz da solução ofertada, incluindo as instruções operacionais para cada tópico abordado.			Documentação enviada não informa atendimento
Deverão ser fornecidos certificados ou declaração de participação em treinamento para			Documentação enviada não informa atendimento
os empregados e prestadores participantes, nas condições e formatos definidos pelo BASA.			Documentação enviada não informa atendimento

SEGURANÇA DE REDES	ATENDE	NÃO ATENDE	COMENTÁRIOS
Todo o tráfego de rede associado ao objeto do contrato deve ser mediado por uma solução de controle de tráfego de borda do tipo firewall (norte-sul, leste/oeste, e de aplicações).			Documentação enviada não informa atendimento
O tráfego de rede associado, entre as unidades e os servidores, bem como todo o tráfego da contratada por rede privada virtual (vpn) para acesso aos recursos do BASA ou controle da aplicação em nuvem, deve ocorrer por meio de firewall que suporte camada 7 (layer 7).			Documentação enviada não informa atendimento
O conjunto de regras da firewall deve se basear na negação de todos os serviços, exceto aqueles especificamente permitidos.			Documentação enviada não informa atendimento
O processo para instalação e adaptação de regras de firewall deve ser feito com duplo controle.			Documentação enviada não informa atendimento
A Contratada deve revisar as regras de firewall pelo menos semestralmente, guardando evidências dessas revisões e dos ajustes eventualmente realizados, comunicando ao BASA sobre a realização desta revisão.			Documentação enviada não informa atendimento
Todos os componentes de gateway de perímetro e sistemas de computadores devem ser monitorados contra tentativas de intrusão, por meio de solução de prevenção e detecção de intrusão (IPS).			Documentação enviada não informa atendimento
O monitoramento de segurança deve ser configurado para rastrear e registrar tentativas de			Documentação enviada não informa atendimento

intrusão suspeitas ou reais.			
A Contratada deve informar imediatamente a equipe de tecnologia do banco em caso de tentativa de intrusão real, e informar em relatório mensal sobre as tentativas de intrusão suspeitas.			Documentação enviada não informa atendimento
A Contratada deve implementar solução anti-DDoS, capaz de prevenir ataques de negação de serviço (Denial of Service).			Documentação enviada não informa atendimento
As soluções de firewall, CASB, IPS e anti-DDoS utilizadas pela Contratada serão validadas pela equipe de tecnologia a partir de documentações do fabricante ou certificações.			Documentação enviada não informa atendimento
A Contratada deve impedir em sua rede local (Lan) o uso do protocolo Bluetooth para transferência de dados, bem como dispositivos usb (pendrive e hd externo).			Documentação enviada não informa atendimento
Todas as comunicações e trocas de informações entre a Contratada e o Banco da Amazônia devem ser realizadas por meio de conexão protegida, com TLS 1.2 ou superior.			Documentação enviada não informa atendimento
Para os casos aplicáveis, os acessos diretos de diferentes equipamentos ao serviço da			Documentação enviada não informa atendimento
Contratada devem ser gerenciados por ferramentas de gerenciamento de dispositivos			Documentação enviada não informa

e/ou aplicativos (MDM/MAM) ou controle de acesso à rede (NAC).			atendimento
CICLO DE VIDA DE DESENVOLVIMENTO SEGURO	ATENDE	NÃO ATENDE	COMENTÁRIOS
A Contratada deve adotar o princípio de security by design para garantir que as aplicações de TI por ela desenvolvidas sejam seguras desde a concepção.			Documentação enviada não informa atendimento
A Contratada deve fazer análise de código automatizada com base nas melhores práticas de mercado, utilizando como referência os padrões do OWASP.			Documentação enviada não informa atendimento
A Contratada deve estabelecer critérios de escala e prazo para correção das vulnerabilidades e deve definir as alçadas para aceitação de riscos. Adicionalmente, devem ser estabelecidas responsabilidades por perdas causadas por incidentes decorrentes de vulnerabilidades identificadas nos testes de segurança, que não foram tratadas ou corrigidas em tempo hábil.			Documentação enviada não informa atendimento
A Contratada deve fazer análise de código estática (SAST) e dinâmica (DAST) periodicamente e de forma integrada ao ciclo de desenvolvimento como um todo para a solução Contratada. Essas análises precisam ser executadas pelo menos uma vez por ano ou quando houver uma mudança considerada significativa nas funcionalidades do sistema/aplicação (como a inclusão de uma nova funcionalidade crítica ou manutenção em módulos que tratem informações sensíveis e confidenciais). A bateria de testes deve incluir testes de resistência, injeções de falhas, teste de penetração e teste de vulnerabilidades onde aplicável.			Documentação enviada não informa atendimento

A Contratada deve incluir a análise e a remediação das vulnerabilidades detectadas como parte do ciclo de vida de desenvolvimento de software padrão, sem custo adicional para o BASA, dentro de um período razoável e de acordo com a criticidade da falha encontrada.			Documentação enviada não informa atendimento
A Contratada deve estabelecer critérios de escala e prazo para correção das vulnerabilidades			Documentação enviada não informa atendimento

e deve definir as alçadas para aceitação de riscos. Adicionalmente, devem ser estabelecidas responsabilidades por perdas causadas por incidentes decorrentes de vulnerabilidades identificadas nos testes de segurança, que não foram tratadas ou corrigidas em tempo hábil.			Documentação enviada não informa atendimento
Os relatórios dos testes realizados e o planejamento das correções a serem feitas devem ser disponibilizados ao Banco da Amazônia sempre que solicitado.			Documentação enviada não informa atendimento
GESTÃO DE SERVIÇOS E MUDANÇAS	ATENDE	NÃO ATENDE	COMENTÁRIOS
A Contratada deve ter um processo de Gestão de Mudanças para garantir a proteção contínua dos ativos de informação e dados, em particular aqueles que fazem parte do escopo do objeto do contrato.			Documentação enviada não informa atendimento
Contratada deve revisar periodicamente as atividades de gestão de mudanças, incluindo a acurácia da Base de Dados de Gerenciamento de Configuração (Configuration Management Database – CMDB).			Documentação enviada não informa atendimento
A Contratada deve cumprir com os procedimentos de registros de informações relacionadas ao processo de gestão de mudanças, no contexto do contrato, incluindo:	ATENDE	NÃO ATENDE	COMENTÁRIOS
Referência da mudança;			Documentação enviada não informa atendimento

Data de implementação;			Documentação enviada não informa atendimento
Avaliação de impactos;			Documentação enviada não informa atendimento
Resultados do teste;			Documentação enviada não informa atendimento
Procedimentos de rollback;			Documentação enviada não informa atendimento
Alterações de emergência;			Documentação enviada não informa atendimento
Atualizações relacionadas ao inventário de ativos de informação;			Documentação enviada não informa atendimento
Armazenamento Seguro de mídia de backup produzidos durante a atualização;			Documentação enviada não informa atendimento
Atualização dos procedimentos de Documentação e de trabalho;			Documentação enviada não informa atendimento
Atualizações aos documentos de Plano de Continuidade dos Negócios / Recuperação			Documentação enviada não informa atendimento
de Desastres se for o caso;			Documentação enviada não informa atendimento
Categorização, priorização e procedimentos de emergência;			Documentação enviada não informa atendimento
Autorização de mudança;			Documentação enviada não informa atendimento
Gerenciamento de liberação;			Documentação enviada não informa

			atendimento
Link para incidentes / problemas (conforme apropriado).			Documentação enviada não informa atendimento
A Contratada só deve promover os aplicativos e sistemas relacionados ao escopo do objeto do contrato para o ambiente de Produção após a realização com sucesso dos testes predefinidos baseados em caso de uso.			Documentação enviada não informa atendimento
A Contratada deve conduzir uma avaliação de risco e ameaças, contemplando inclusive os testes baseados em casos de uso, quando da implantação de uma mudança.			Documentação enviada não informa atendimento
A Contratada deve realizar uma avaliação de risco:	N/A	N/A	N/A
Quando o escopo do sistema é expandido para incluir novos ativos de informação com novas funcionalidades;			Documentação enviada não informa atendimento
Quando uma nova comunidade de usuários é introduzida; ou			Documentação enviada não informa atendimento
Anualmente, por se tratar de risco cibernético, nos termos do art. 8º da Resolução BACEN 4.893/2021.			Documentação enviada não informa atendimento
GESTÃO DE INCIDENTES DE SEGURANÇA	ATENDE	NÃO ATENDE	COMENTÁRIOS
A Contratada deve obedecer a este item, assim como os requisitos apresentados ou, caso os dados			Documentação enviada não informa atendimento

estejam sendo armazenados ou processados no ambiente do Provedor de Serviço em Nuvem, pelo Provedor.			
Se os dados estiverem exclusivamente no Provedor, a Contratada deverá comprovar por relatório de auditoria (Due Dilligence Remoto) que o armazenamento ocorre somente em ambiente de nuvem.			Documentação enviada não informa atendimento
A Contratada deve possuir um processo de Gestão de Incidentes que registre os incidentes de segurança cibernética ocorridos e que guarde informações como: a descrição dos incidentes ou eventos, as informações e sistemas envolvidos, as medidas técnicas e de segurança utilizadas para a proteção das informações, os riscos relacionados ao incidente e às medidas tomadas para mitigá-los e evitar reincidências.			Documentação enviada não informa atendimento
O processo de Gestão de Incidentes também deve implementar e manter controles e procedimentos específicos para detecção, tratamento, coleta/preservação de evidências e resposta a incidentes de segurança da informação, de forma a reduzir o nível de risco ao qual o objeto do contrato ou o BASA estão expostos, considerando os critérios de aceitabilidade de riscos definidos pelo BASA.			Documentação enviada não informa atendimento
A Contratada deve realizar testes independentes de penetração pelo menos uma vez por ano. Os testes devem ser executados por terceiros, sem ônus adicional para o BASA. O escopo dos testes deve ser previamente combinado e aprovado pelo BASA, dentro dos limites do contrato.			Documentação enviada não informa atendimento
A Contratada deve implementar um processo de gestão de vulnerabilidades que inclua sua			Documentação enviada não informa atendimento

infraestrutura de servidores e redes.			
Todos os relatórios com os resultados dos testes de penetração e varredura de vulnerabilidades, bem como o planejamento das correções a serem feitas, devem ser fornecidos ao Banco da Amazônia sempre que solicitado.			Documentação enviada não informa atendimento
A Contratada deve comunicar os incidentes detectados ao BASA dentro do prazo acordado, conforme termos do SLA definido em contrato.			Documentação enviada não informa atendimento
A Contratada deve ter um processo de notificação de incidentes 24x7.			Documentação enviada não informa atendimento
No caminho inverso, se o BASA detectar um incidente de segurança, a Contratada será notificada e deverá cooperar totalmente para resolver o incidente de segurança, fornecendo todas as informações relacionadas que possam levar a solução do incidente em questão (também 24x7).			Documentação enviada não informa atendimento
Vale ressaltar que em se tratando de contratos para tratamento de dados pessoais, nos termos da LGPD, a Contratada deve provar que tem capacidade de fornecer uma resposta organizada e eficaz a um incidente de privacidade. Neste sentido, o BASA desenvolverá e implementará juntamente com o fornecedor do serviço um plano de resposta a incidentes de privacidade, que inclua por exemplo, definição de incidente de privacidade e o escopo da resposta ao incidente, estabelecimento de equipes multifuncionais de resposta a incidente de privacidade, entre outros aspectos relevantes.			Documentação enviada não informa atendimento

A Contratada deve ter um processo de lições aprendidas para incidentes de segurança implementado e comunicado aos seus funcionários e parceiros, com objetivo de agilizar a atuação caso surjam incidentes semelhantes.			Documentação enviada não informa atendimento
A integração da gestão de incidentes da Contratada com o Centro de Operações de Segurança do Banco da Amazônia deve ser considerada, observada a regulamentação em vigor, conforme art 3º, §4º da Res. BACEN 4.893/2021.			Documentação enviada não informa atendimento
Se a Contratada precisar envolver outras partes externas para investigar e/ou resolver incidentes que afetem o escopo do objeto contratado, ela deve obter a anuência do Banco da Amazônia por escrito antes de iniciar o contato com tais partes, observada a política de segurança cibernética do Banco da Amazônia.			Documentação enviada não informa atendimento
CONTINUIDADE DE NEGÓCIOS E RECUPERAÇÃO DE DESASTRES	ATENDE	NÃO ATENDE	COMENTÁRIOS
A Contratada deve possuir, plano de continuidade, recuperação de desastres e contingência de negócio, que possa ser testado regularmente, objetivando a disponibilidade dos dados e serviços em caso de interrupção, bem como desenvolver e colocar em prática procedimentos de respostas a incidentes relacionados com os serviços.			Documentação enviada não informa atendimento

Caso a Contratada utilize um Provedor de Serviços em Nuvem para todos os serviços, as apresentações das certificações por parte do provedor já serão consideradas suficientes para garantir os processos deste item.			Documentação enviada não informa atendimento
A Contratada deve possuir, plano de continuidade, recuperação de desastres e contingência de negócio, que possa ser testado regularmente, objetivando a disponibilidade dos dados e serviços em caso de interrupção, bem como desenvolver e colocar em prática procedimentos de respostas a incidentes relacionados com os serviços.			Documentação enviada não informa atendimento
O referido plano de continuidade deverá ser informado para o BASA como parte das ações de acompanhamento do contrato, e deverá ser atualizado e testado anualmente, ou em qualquer mudança significativa do ambiente de hospedagem (data center do banco ou em nuvem).			Documentação enviada não informa atendimento
A atuação, em caráter de contingência, causada por uma eventual indisponibilidade do serviço prestado, considera as seguintes premissas:	ATENDE	NÃO ATENDE	COMENTÁRIOS
a) Interrupção total ou parcial dos serviços			Documentação enviada não informa atendimento
b) Ter infraestrutura alternativa: física e lógica nos dois ambientes de data center do Banco da Amazônia ou em nuvem, com o objetivo de minimizar o risco de perda de ambas as instâncias;			Documentação enviada não informa atendimento
c) Manter os serviços essenciais suportados pelo			Documentação enviada não informa

contrato			atendimento
d) Manter a lista de integrantes das equipes e o Plano de Recuperação de Desastres atualizados;			Documentação enviada não informa atendimento
e) Ter local seguro para guarda de backups fora do local atingido;			Documentação enviada não informa atendimento
f) Assegurar a disponibilidade dos serviços essenciais dentro do tempo previsto para recuperação do serviço, de acordo com o contrato;			Documentação enviada não informa atendimento
g) Procedimento documentado e evidenciado de testes das mídias armazenadas offsite;			Documentação enviada não informa atendimento
h) Cópias de todos os procedimentos abordando backup, restauração e reconstituição de armazenamento de dados.			Documentação enviada não informa atendimento
A obrigatoriedade do plano de continuidade se estende para empresas que sejam			Documentação enviada não informa atendimento
A Contratada, visando a continuidade dos negócios, deve implantar uma política de backup.			Documentação enviada não informa atendimento
A Contratada deve fornecer os subsídios necessários para que o BASA implemente os indicadores de desempenho de segurança que vierem a ser definidos durante a vigência do contrato.			Documentação enviada não informa atendimento
A Contratada em caso de utilização de Serviços em Nuvem deverá apresentar as seguintes certificações e processos de auditoria disponíveis, apresentados periodicamente, conforme coluna			Documentação enviada não informa atendimento

Vigência:			
AUDITORIA	ATENDE	NÃO ATENDE	COMENTÁRIOS
O sistema deverá registrar e armazenar os logs de auditoria permitindo, consultas, exportação, emissão de relatórios, com parâmetros de no mínimo:			Documentação enviada não informa atendimento
- Acessos de usuários (Nome, Matrícula, Data (dd:mm:aa), Horário(hh:mm:ss));			Documentação enviada não informa atendimento
- Registro individualizado de todas as ações e eventos ocorridos no sistema;			Documentação enviada não informa atendimento
- Permitir ordenação e filtro conforme os seguintes parâmetros: Usuário, Palavras-chaves, Período, Data, Horário, Tipo de ação, Tipo de usuário, Cod. Agência, Nome da Agência, Evento, Ambiente.			Documentação enviada não informa atendimento
Configurações aplicadas nos equipamentos das agências;			Documentação enviada não informa atendimento
Consulta e relatório de todas as ações dos operadores, incluindo as operações realizadas no tratamento de eventos de alarme;			Documentação enviada não informa atendimento
Consulta e relatório com as alterações de permissões e configurações dos operadores do sistema;			Documentação enviada não informa atendimento
Consulta e relatório dos acessos (logons e logouts) dos usuários do sistema, registrando os horários de entrada e saída no sistema e todos os acessos às funcionalidades realizados;			Documentação enviada não informa atendimento

Consulta e relatório de todos os eventos gerados pelo sistema, identificando individualmente e todos os registros com os horários das ocorrências			Documentação enviada não informa atendimento Documentação enviada não informa atendimento
GESTÃO DO EQUIPAMENTO	ATENDE	NÃO ATENDE	COMENTÁRIOS
Possibilita o registro e a exclusão de pessoas para o arme e desarme na central de alarme de forma remota, sem necessidade de presença de técnico no local. Caso o equipamento esteja desligado ou sem acesso à rede, o software mantém o registro e atualiza a lista de pessoas na central de alarme assim que o equipamento estiver ligado e comunicando com o software.			Documentação enviada não informa atendimento
Possui a função de cadastramento de horário com pelo menos dois agendamentos diários, para abertura e fechamento (arme e desarme);			Documentação enviada não informa atendimento
Permite pelo menos 3 status de ativação do equipamento, sendo um deles “ativo”, “em manutenção” (os eventos devem ser mostrados em segundo plano na tela de monitoramento) e “inativo” (os eventos não devem ser salvos			Documentação enviada não informa atendimento
OPERAÇÃO GERAL DO SISTEMA	ATENDE	NÃO ATENDE	COMENTÁRIOS
Monitoramento de eventos de alarme dividido em pelo menos 3 filas de atendimento, onde os alarmes poderão ser movidos pelos operadores do sistema e Todos os novos eventos são direcionados para a primeira fila de atendimento			Documentação enviada não informa atendimento

Possuir configuração de “Tipos de Alarme”, que define o motivo dos eventos de Alarmes			Documentação enviada não informa atendimento
Possuir função” Cadastramento de Operadores”. Cada registro de operador no sistema tem permissões configuradas individualmente, não afetando assim a operação dos demais operadores cadastrados no sistema.			Documentação enviada não informa atendimento
Permitir, a qualquer momento, a extração de relatórios referente a:			Documentação enviada não informa atendimento
o Eventos de alarme por unidade, por data, por tipo de evento;			Documentação enviada não informa atendimento
o Configurações de inputs;			Documentação enviada não informa atendimento
o Logs do sistema;			Documentação enviada não informa atendimento
o Auditoria;			Documentação enviada não informa atendimento
o Permissões dos operadores;			Documentação enviada não informa atendimento
o Ocorrências por unidade, por tipo, por data;			Documentação enviada não informa atendimento
o Equipamentos por status de comunicação, por status de arme/desarme;			Documentação enviada não informa atendimento
o Alterações de status do equipamento e justificativa.			Documentação enviada não informa atendimento

o Possuir módulo de Liberação de Acesso Monitorado a unidade:			Documentação enviada não informa atendimento
o Permitir o agendamento prévio de visita de prestadores de serviços a uma unidade para finalidade que se faça necessária;			Documentação enviada não informa atendimento
o Registro do autorizador;			Documentação enviada não informa atendimento
o Registro do usuário com CPF/RG;			Documentação enviada não informa atendimento
o Cadastro de empresas contratadas;			Documentação enviada não informa atendimento
o Cadastro de vigilantes;			Documentação enviada não informa atendimento
MONITORAMENTO DE ALARMES	ATENDE	NÃO ATENDE	COMENTÁRIOS
Deve possuir interface de telas no sistema para o atendimento dos eventos de alarme;			Documentação enviada não informa atendimento
Deve permitir o acesso por operadores com permissões especificadas, podendo ser determinando a quais equipamentos os operadores terão acesso para atendimento dos eventos;			Documentação enviada não informa atendimento
Deve monitorar todos os eventos gerados pelos equipamentos de Alarme;			Documentação enviada não informa atendimento

Deve fornecener logs de todas as ligações realizadas nos possíveis eventos, disponibilizar inclusive gravação das mesmas se for necessário.			Documentação enviada não informa atendimento
Deve reportar através de recurso sonoro o momento em que um novo equipamento dispara eventos de intrusão, violação ou falha de comunicação;			Documentação enviada não informa atendimento
Deve possuir mecanismo para tratamento/justificativa e classificação dos eventos em um campo livre para justificativa contendo pelo menos 10 respostas padrões pré-cadastradas no sistema e um campo de seleção que classifique o evento. Estes tipos são gerenciáveis através do sistema mediante permissão especifica			Documentação enviada não informa atendimento
Deve possui 3 (ou mais) filas de atendimentos, com nomes configuráveis, para a gerência das centrais de alarme com eventos não-tratados;			Documentação enviada não informa atendimento
Deve permite o arme e o desarme remoto dos equipamentos, sendo estas ações obrigatoriamente justificadas pelo operador;			Documentação enviada não informa atendimento
Deve possuir a visualização da configuração de todos os inputs (sensores) presentes no equipamento de alarme;			Documentação enviada não informa atendimento

Deve possuir a visualização de todos os eventos já ocorridos em cada uma das centrais de alarme;			Documentação enviada não informa atendimento
Deve possuir a visualização de informações do local (endereço, telefones e contatos) aonde a central de alarme está instalada;			Documentação enviada não informa atendimento
Deve possuir a visualização das informações de rede da central de alarme IP;			Documentação enviada não informa atendimento
Deve possuir a visualização dos usuários com permissão para arme/desarme local no equipamento de alarme;			Documentação enviada não informa atendimento
Deve possuir mecanismo para testar o funcionamento dos sensores instalados no equipamento de alarme, permitindo geração de relatório após término do teste contendo minimamente a quantidade de eventos gerados e os horários de início e fim dos testes, bem como os horários do primeiro e último evento gerado em cada um dos sensores;			Documentação enviada não informa atendimento
Deve permitir o cadastramento de ocorrências (assalto, furto, arrombamento, incêndio, etc.).			Documentação enviada não informa atendimento
CONTROLE DE CHAMADOS	ATENDE	NÃO ATENDE	COMENTÁRIOS
Deve possuir interface de telas para o gerenciamento e controle de chamados realizados.			Documentação enviada não informa atendimento
Deve dispor das seguintes informações:			Documentação enviada não informa

			atendimento
Devem ser Abertos e “Fechados Com Pendência” e ou “Definitivamente” pelos Gestores ou Responsáveis pelas Unidades do BANCO;			Documentação enviada não informa atendimento
Unidade a ser atendida;			Documentação enviada não informa atendimento
Chamado de origem;			Documentação enviada não informa atendimento
Nível de emergência (pelo menos 3 níveis);			Documentação enviada não informa atendimento
Título;			Documentação enviada não informa atendimento
Descrição;			Documentação enviada não informa atendimento
Empresa prestadora;			Documentação enviada não informa atendimento
Nome dos técnicos;			Documentação enviada não informa atendimento
Deve possuir um cadastro de tipos de chamados, sendo que cada tipo de chamado deve ter um tempo de atendimento (em dias) máximo estipulado;			Documentação enviada não informa atendimento
Deve permitir que para cada empresa prestadora de serviços seja possível determinar um tempo de atendimento diferenciado do padrão para cada			Documentação enviada não informa atendimento

um			
dos tipos de chamados;			Documentação enviada não informa atendimento
Deve controlar o tempo de atendimento considerando apenas dias úteis, sendo que o sistema identifica automaticamente os sábados e domingos como não-úteis e possui ferramenta para cadastro de feriados nacionais, estaduais e municipais, incluindo a possibilidade de inclusão de feriados móveis;			Documentação enviada não informa atendimento
Deve possuir ferramenta para envio de e-mail diretamente para os prestadores de serviços, contendo as informações do chamado no corpo do e-mail e/ou em anexo, sem a utilização de aplicações externas;			Documentação enviada não informa atendimento
prestadores de serviços, contendo as informações do chamado no corpo do e-mail e/ou em anexo, sem a utilização de aplicações externas;			Documentação enviada não informa atendimento
Deve permitir que sejam anexados qualquer tipo de documento no registro, para posterior consulta;			Documentação enviada não informa atendimento
Toda alteração realizada nos chamados deve ser auditável;			Documentação enviada não informa atendimento
SISTEMA DE ANÁLISE DE VÍDEO POR SERVIDOR GERADOR DE ANALÍTICOS E HUB DE INTEGRAÇÃO DE CFTV.	ATENDE	NÃO ATENDE	COMENTÁRIOS

Faz parte do Software de Monitoramento e Controle o Sistema de Análise de Vídeo por Gerador de Analíticos. O mesmo deve estar em servidor ou appliance devendo ser de padrão para montagem em rack 19” com altura 2U ou 4U equipado com quatro (4) baias internas mínimas para instalação dos discos de gravação.			Documentação enviada não informa atendimento
Deverá contar com 2x GPUs no mínimo, ou quantidade superior necessária para adicionar os recursos analíticos às câmeras associadas a ele.			Documentação enviada não informa atendimento
Deverá receber o vídeo das câmeras através das interfaces de rede minimo 4x 1Gb Base-T ou 10Gb SFP, configuradas de modo atender as demandas aqui solicitadas.			Documentação enviada não informa atendimento
Possuir alimentação elétrica 100 ~ 240 VAC (Full Range) e com dual (duas).			Documentação enviada não informa atendimento
O sistema deve ter memória, processador e licenciamento devidamente dimensionados para prover os serviços de análise de vídeo solicitados em todas as câmeras a ele associadas.			Documentação enviada não informa atendimento
Suportar ao menos 200 canais ou 200 câmeras de vídeo IP por servidor com capacidade de prover ao menos 5 analíticos de livre escolha por canal/câmera;			Documentação enviada não informa atendimento
O cliente poderá a seu exclusivo critério fazer uso das 200 licenças disponíveis sem nenhum custo			

adicional em QUALQUER câmera de seu parque instalado e da mesma forma ter livre escolha dos analíticos desejados que devem possuir capacidade de programação horária por dias de semana, final de semana e feriados.		X	Documentação enviada não informa atendimento
O sistema a ser fornecido de analíticos deve prever atualizações, suporte, up-grades sem qualquer custo adicional ao longo do contrato de forma a up-grades sem qualquer custo adicional ao longo do contrato de forma a garantir que novos analíticos disponibilizados pelo fabricante, sejam liberados ao BASA tão logo estejam disponiíveis nos produtos atualizados do respectivo fabricante.		X	A documentação informa que dentro da mesma versão as atualizações são gratuitas, mas caso a versão seja alterada deve ser contratado nova licença
Os analíticos devem ter inteligência embarcada de autoaprendizagem com motor base de comportamento anormal, desta maneira permitindo analíticos de comprtamento anormal não esperado.	X		
Deverá suportar fluxos de vídeo no padrão h.264 e h.265, através do padrão Onvif, ou através do protocolo RTSP.	X		
Deverá ser capaz enviar e-mail, notificações HTTP ou acionar Webhooks, em função da violação de regras de análise de vídeo ou regras de contagem, para integração com outros sistemas.	X		
Deverá ser capaz de receber notificações de sistemas terceiros ou dispositivos através de estratégia POS - na qual um evento de texto ou valor número é encaminhado fica associado a um trecho ou momento do vídeo.	X		

O fluxo de vídeo de todas as câmeras IP associadas ao servidor devem ser analisadas e toda vez que pessoa ou veículo sejam detectados o vídeo deve ser armazenado no próprio servidor e notificar o sistema de gerenciamento que conta com as imagens armazenadas pelo tempo requerido de todas as câmeras do sistema.	X		

BANCO DA AMAZÔNIA

GESEC – Gerência de Segurança Corporativa
COSEB – Coordenadoria de Gestão da Segurança Patrimonial Bancária

O servidor de análise de vídeo analítico deve estar integrado ao sistema de gravação e gerenciamento de cftv, de modo que: violações detectadas pelo servidor, sejam exibidas no servidor e que o vídeo gravado das câmeras esteja disponível localmente no gravador.	X		
O servidor deve suportar análise de vídeo simultânea em todas as câmeras a ele associadas. Entre elas, o sistema deve suportar no mínimo: Cruzamento de linha por pessoa ou veículo, permitindo excluir objetos fixos;	X		
a) Cruzamento de linha por pessoa portando mochila ou mala;	X		
b) Cruzamento de linha por pessoa com aparência similar à de uma imagem configurada na regra;	X		
c) Cruzamento de linha virtual por veículo que não esteja na lista de placa exclusão;	X		
d) Cruzamento de linha virtual por veículos categorizados (motos, veículos pequenos, médios ou grandes)	X		
e) Contar pessoas presentes na	X		

cena ou em área da cena;			
f) Notificar excessos de pessoas no ambiente;	X		
g) Contar pessoas que cruzarem linha entrando, saindo ou em ambos os sentidos e apresentar a diferença;	X		
h) Permanência prolongada na cena de pessoa ou veículos, suportando os tempos de poucos segundos até hora;	X		
i) Notificar pessoas ou veículos em atitude ou movimento suspeito, hora do dia incomum, local incomum, velocidade incomum e som incomum quando a câmera possuir recurso de áudio.			Documentação enviada não informa atendimento
j) Analisar a cena por meio de IA (Inteligência Artificial), notificando qualquer atitude anormal de pessoas ou veículos.	X		
k) Para as câmeras que tenham recurso de áudio, do mesmo fabricante da solução de servidor de análise de vídeo, deve possibilitar o recebimento eventos de Analíticos de Aviso de:			
1) quebra de vidro;	X		

2) ruído alto;	X		
3) Grito;			Documentação enviada não informa atendimento
4) Disparo de arma de fogo;			Documentação enviada não informa atendimento
Para quaisquer dos eventos de analítico o Sistema de Análise de Vídeo e Hub de Integração deve ser capaz de:			
1) Enviar e-mail caso uma regra seja violada ou que uma contagem alcance, esteja abaixo ou que seja igual a um valor previamente definido;	X		
2) Acionamento de uma URL com envio de parâmetros;	X		
3) Acionamento de um Webhook com passagem de parâmetros;	X		
A parametrização do servidor de análise deve ter interface própria, simples e acessível a partir de qualquer local e poder ser aberta ou executada em ambientes Microsoft, Linux ou MAC. Para sistemas que contêm recurso em nuvem deverá ser informada lista de domínios/IPs acessados pela solução.	X		

O servidor de análise deve contar com ambiente em nuvem/ou serviço similar que permita receber notificações de sensores homologados pelo fabricante da solução, ou permitir a integração de sensores terceiros através de API aberta e disponível, que permitam:			
1) medir temperatura do ambiente;	X		
2) umidade do ambiente;	X		
3) quantidade de CO2;	X		
4) Fumaça;	X		
5) THC;	X		
O servidor de análise deve contar com módulo de busca no vídeo gravado que permita desenhar uma linha sobre a imagem da cena, selecionar sentido ou direção, e filtrar as pessoas que cruzaram a linha desenhada sobre a imagem da cena. A partir da foto das pessoas identificadas, deve ser possível a reprodução do vídeo gravado do momento em que a pessoa passou	X		
O servidor de análise deve contar com módulo de busca no vídeo gravado que permita desenhar área de interesse em uma cena e	X		

realizar pesquisa por pessoas que tenham ficado na cena por um tempo prolongado que pode ser de poucos segundos, minutos ou até horas.			
O servidor de análise quando receber eventos pelo canal de POS, deve permitir a busca no período de vídeo armazenado dos eventos relacionados às transações de POS, inclusive com possibilidade de filtro de texto ou valor numérico (e.g. eventos cujo valor número seja superior, menor ou igual a valor informado na busca);	X		
A operação do servidor de análise de vídeo será através de aplicação instalada em estações clientes ou browser, o que estiver disponível, preferencialmente o que permitir facilidade de atualização, para soluções que contam com conexão em nuvem deverá ser fornecida lista de domínios e IPs utilizados pela solução;	X		
Possuir ISO 27001;			Documentação enviada não informa atendimento
Possuir no mínimo TLS 1.2 por padrão;	X		
Possuir autenticação centralizada (ADFS, Azure AD) usando	X		

integração SAML.			
3) quantidade de CO2;	X		
4) Fumaça;	X		
5) THC;	X		
O servidor de análise deve contar com módulo de busca no vídeo gravado que permita desenhar uma linha sobre a imagem da cena, selecionar sentido ou direção, e filtrar as pessoas que cruzaram a linha desenhada sobre a imagem da cena. A partir da foto das pessoas identificadas, deve ser possível a reprodução do vídeo gravado do momento em que a pessoa passou	X		
O servidor de análise deve contar com módulo de busca no vídeo gravado que permita desenhar área de interesse em uma cena e realizar pesquisa por pessoas que tenham ficado na cena por um tempo prolongado que pode ser de poucos segundos, minutos ou até horas.	X		
O servidor de análise quando receber eventos pelo canal de POS, deve permitir a busca no período de vídeo armazenado dos eventos relacionados às transações de POS, inclusive com possibilidade de filtro de texto ou valor numérico (e.g. eventos cujo valor número seja superior, menor ou igual a	X		

valor informado na busca);			
A operação do servidor de análise de vídeo será através de aplicação instalada em estações clientes ou browser, o que estiver disponível, preferencialmente o que permitir facilidade de atualização, para soluções que contam com conexão em nuvem deverá ser fornecida lista de domínios e IPs utilizados pela solução;	X		
Possuir ISO 27001;			Documentação enviada não informa atendimento
Possuir no mínimo TLS 1.2 por padrão;	X		
Possuir autenticação centralizada (ADFS, Azure AD) usando integração SAML.	X		

III – CONCLUSÃO

Diante do exposto, conclui-se que a documentação e proposta apresentada pela empresa não atende aos requisitos técnicos e comerciais estabelecidos no edital, impossibilitando a sua habilitação. De modo que pedimos sua desclassificação e a convocação da próxima licitante.

03/11/2025

X

Diego Expedito Ferreira Lobo
Coord. Int.º da COSEB
Assinado por: 7887