



Descritivo Funcional

Versão 3.0.0
2024

Índice

1. Visão Geral.....	3
1.1. Resumo.....	3
2. Características.....	3
2.1. Produto SURICATO.....	4
2.2. Estrutura do Sistema SURICATO.....	4
2.3. Instalador SURICATO.....	4
2.4. Módulo do Sistema SURICATO.....	4
2.4.1. Módulo de Monitoramento Gráfico On-line.....	4
2.4.2. Módulo Gerador de Relatórios.....	5
2.4.3. Módulo Active Directory (do Windows).....	5
2.5. Ajuda ao Usuário.....	5
2.6. Periféricos do Sistema SURICATO.....	6
2.6.1. Webcam.....	6
2.6.2. Torre de Captura.....	6
2.6.3. Scanner.....	6
2.6.4. Leitora de mesa Smartcard.....	6
2.6.5. Leitora de mesa Biométrico.....	6
2.6.6. Leitora de mesa da Palma da Mão.....	6
3. Funcionalidades.....	7
3.1. Cadastros.....	7
3.1.1. Colaboradores.....	7
3.1.2. Grupo de Acesso.....	8
3.1.3. Visitantes, Candidatos e Pessoas Não Gratas.....	8
3.1.4. Crachás.....	8
3.1.5. Recursos de Sistema.....	9
3.1.6. Regras de Negócio no Sistema SURICATO.....	10
3.1.7. CODINs.....	11
3.1.8. CODINs ReP.....	11
3.1.9. CFTV.....	11
3.1.10. Processos Automático.....	11
3.1.11. Relatórios.....	12
3.1.12. Login e Usuários.....	12
3.1.13. Reação de Eventos.....	12
3.1.14. Colaboradores.....	NN
4. Anexos.....	12
4.1. Anexo I - Matriz de Funcionalidades.....	13
5. Pré-Requisitos.....	16
5.1. Servidor de Banco de Dados.....	17
5.2. Servidor Aplicação SURICATO.....	17
5.3. Servidor Conex.....	17
6. Modelo de Arquitetura.....	17
6.1. Arquitetura - A.....	18
6.2. Arquitetura - B.....	19
6.3. Arquitetura - C.....	19
6.4. Arquitetura - D.....	20

1. Visão Geral

1.1. Resumo

- O SURICATO é um sistema de segurança e controle de acesso com recursos avançados que garantem o amparo a todo e qualquer tipo de negócio, porte ou segmento em áreas internas e externas, supervisionadas em tempo real.
 - Atua em diferentes frentes de segurança, como monitoramento de alarmes, incêndio, violação e intrusão, bem como no tratamento desses alarmes no modo manual e automático.
 - O monitoramento é uma das interfaces de integração ao sistema de CFTV (Circuito Fechado de TV) Digital TELEMÁTICA, que permite a visualização de imagens em tempo real das zonas controladas e a obtenção de gravações dos momentos de disparo de ocorrências. Os ajustes das câmeras podem ser controlados de acordo com a necessidade de visualização da imagem: zoom e direção.
 - Toda imagem é gravada com data, hora e local de origem. As imagens podem ser localizadas através de uma busca com parâmetros de data, hora ou local e encaminhadas por e-mail para um destinatário cadastrado.
 - O SURICATO integra-se com diversos sistemas de identificação de acesso, como cartões de proximidade, Smartcard, RFid, biometria digital ou facial.
 - A partir da versão 2.10.0, lançada no final de 2018, o SURICATO passou a integrar-se com os seguintes ERPs da TOTVS: PROTHEUS, DATASUL e RM. Desta forma, a manutenção dos dados dos colaboradores, tais como: dados pessoais, departamentos, escalas, etc., uma vez alterados em um destes ERPs, serão automaticamente atualizados no SURICATO.
 - Permite a importação de dados de sistemas legados com processos automáticos configurados na aplicação através de arquivos com interfaces definidas. O formato padrão de exportação e importação é arquivo texto.
 - Além de dados pessoais, disponibiliza informações de ponto para colaboradores, controla escalas de trabalho, permite a configuração de tolerância para os limites de horários (jornada de trabalho), afastamento e crédito de refeitório.
 - Também exporta marcações de ponto dos colaboradores, no formato AFD, conforme layout da portaria 671 e da portaria 1510 do MTE
 - Como gestor de inteligência de segurança, o SURICATO mantém históricos de todas as informações de colaboradores, mantendo um registro desde a admissão até o desligamento do colaborador. Da mesma maneira, mantém registros de todas as ações efetuadas no sistema em áreas de controle que impactam no processo de configuração corporativa (regras de negócio).
 - Ele se utiliza da tecnologia dos CODINs Telemática para controlar pessoas, objetos e veículos em áreas supervisionadas e restritas ao acesso comum.
 - Além de controlador, o CODIN é utilizado para obter informações sobre o ponto, controle de acesso e de créditos de refeitório, abertura de cancelas em estacionamentos, alarmes e sensores. Existem vários tipos de equipamentos controlados pelo CODIN, como catracas (as fornecidas pela Telemática já incluem um CODIN), cancelas e torniquetes que utilizam a tecnologia do CODIN para controlar acesso.
 - Em casos de falta de comunicação, os CODINs off-line possuem inteligência local para trabalhar com listas de liberação ou bloqueio, listas de veículos e lista com templates de biometria, garantindo o acesso seguro de pessoas autorizadas. As listas formam uma composição que é gerada a partir de: grupo de acesso, situação, do crachá, validade do crachá, área restrita e situação trabalhista. Após isto, são enviadas por comandos executados no SURICATO.
 - A segurança interna do sistema (dados e informações) é mantida através de perfil de acesso e senhas, configuradas na instalação do produto.
 - O sistema conta com uma interface intuitiva e amigável, com ótima navegabilidade e apresentação.
- O SURICATO é um produto eficaz para controle e monitoramento de segurança física, inovador no mercado brasileiro de segurança e controle de acesso

2. Características

- Neste tópico, descreveremos as principais características do sistema SURICATO

2.1. Produto SURICATO

- Garante o amparo a todo e qualquer tipo de negócio, porte ou segmento, em áreas internas e externas, supervisionadas em tempo real.
- O SURICATO apresenta um instalador simples, mas ao mesmo tempo intuitivo e amigável.

2.2. Estrutura do Sistema SURICATO

- Desenvolvido em um ambiente 100% Web, em linguagens PHP, JavaScript, Ajax e componentes JAVA.
- Utiliza Certificado Digital (HTTPS) para proteção dos dados do cliente e proteção à instalação e licença, validando o hardware físico do servidor, o número de equipamentos Telemática adquiridos e os módulos do Sistema SURICATO.
- Segurança do produto com criptografia/ofuscamento das aplicações. Como servidor WEB, o SURICATO oferece as opções: APACHE ou IIS.
- Os Bancos de Dados homologados são:
 - a. Oracle 19C e 21C – (padrão Inglês)
 - b. Microsoft SQL Server 2016, 2017, 2019 e 2022 – (padrão Inglês).
- Os tópicos 5 e 6 descrevem respectivamente os requisitos da máquina e modelos de arquitetura recomendados para o funcionamento do sistema SURICATO.

2.3. Instalador SURICATO

- O instalador do SURICATO apresenta uma série de benefícios para o produto no momento da instalação. De modo prático, é possível instalar o produto em etapas e acompanhar todo o processo passo a passo.
- É modular, ou seja, o cliente instala somente os módulos de acordo com a licença adquirida do produto. A validação da licença ocorre da seguinte maneira: Modo on-line: o servidor deve ter acesso à internet para validar a licença no servidor de licenças da Telemática.
- A instalação segue as seguintes etapas:
 - a. **Local de Instalação:** permite que o cliente defina o local de instalação do produto no servidor.
 - b. **Banco de Dados:** permite a seleção do Banco Oracle ou MSSQL (ambos homologados para o Sistema SURICATO).
 - c. **Copiar Arquivos:** comando para iniciar a cópia dos arquivos de aplicação para dentro do servidor.
 - d. **Servidores WEB:** APACHE ou IIS: instalação do servidor definido.
 - e. **Ambiente de Produção:** configuração do ambiente de produção do Sistema SURICATO.

2.4. Módulo do Sistema SURICATO

2.4.1. Módulo de Monitoramento Gráfico On-line

- Desenvolvido em Java, permite a visualização de alarmes na planta do cliente e a tomada de ações (tratamento e encerramento de alarmes) on-line.
- Oferece visualização do dispositivo (em seu local na planta) no momento da ocorrência do alarme ou evento.

- É integrado ao CFTV e permite visualizar vídeos e imagens no momento da ocorrência dos alarmes e/ou em tempo real das instalações controladas com câmeras de segurança.
- Por conta dessa integração, na ocasião de uma ocorrência, o monitoramento prioriza a apresentação de modo visual na tela e o operador pode acionar o vídeo do local no momento da ocorrência do alarme e tomar as devidas providências seguindo ou não um procedimento previamente planejado.
- Todo evento pode ser Reconhecido ou Tratado.
 - a. Reconhecer é uma maneira de informar que já se tomou conhecimento sobre a ocorrência e que o tratamento será enviado posteriormente.
 - b. Tratar o alarme significa enviar o comando (bloqueio, liberação, etc.) para que algo seja feito em relação à ocorrência, ou seja, solucioná-la.
- O Monitoramento Gráfico on-line SURICATO permite várias outras maneiras de tratamento de um alarme, de acordo com o tipo de evento: bloqueio de acesso, arrombamento, invasão, dedo do pânico, acesso por coação.
- A interface é amigável para que o operador não tenha dificuldades na operação.
- Para a visualização das plantas da empresa, sugere-se a utilização de plantas baixas, em formato SVG (Scalable Vector Graphics).
- Possui uma barra de ferramentas com botões dinâmicos e indicativos das funcionalidades. Permite zoom das áreas na navegação e alteração de planta de maneira rápida e amigável, com controle na tela.

2.4.2. Módulo Gerador de Relatórios

- Permite gerar relatórios desenhados de acordo com a necessidade do cliente.
- O Gerador de Relatórios é uma ferramenta amigável e robusta, disponível na barra de menu do produto¹.
- Com o Gerador de Relatórios é possível criar relatórios com filtros de pesquisas, quebras, totalizações, gráficos, ordenação, paginação e impressão em PDF e XLS, além de inúmeros outros recursos.

¹ Desde que adquirido pelo cliente.

2.4.3. Módulo Active Directory (do Windows)

- O sistema de integração com o AD integra as permissões de rede dos colaboradores ao sistema de controle de acesso SURICATO, controlando o acesso lógico dos mesmos ao parque de máquinas da empresa.
- É necessária a disponibilização de ambiente: Windows independente da versão, Advanced Server com protocolo LDAP. O controle é feito, basicamente, com o seguinte fluxo:
 1. O colaborador receberá uma conta de acesso no AD com os respectivos direitos de acesso que sua função permite (isso será feito pelo administrador do AD). É nessa conta de acesso, no AD, que deverão ser identificadas quais máquinas (ou faixa de IPs) as quais esse usuário poderá acessar.
 2. A integração será responsável por liberar ou bloquear a conta do colaborador. Isso será feito levando em conta os registros de acesso do colaborador aos CODINs, validando o acesso e em que nível o mesmo foi realizado, de forma a liberar ou bloquear o acesso lógico do colaborador.

2.5. Ajuda ao Usuário

- O SURICATO utiliza ferramentas de última geração para o desenvolvimento do Help.
- Desenvolvida em HTML, possui todo o conteúdo do sistema e de suas operações de modo detalhado. Conta com pesquisa por índice (palavras chaves) ou por funcionalidades (busca). Além disto, possui Glossário para os termos técnicos do sistema de controle de segurança e controle de acesso.
- Essa ajuda está disponível na barra de Menu do SURICATO, no submenu Conteúdo da Ajuda.

2.6. Periféricos do Sistema SURICATO

- O Sistema SURICATO é composto por periféricos que auxiliam na agilidade de informações para a empresa de maneira a garantir a segurança de acesso.
- Por isso são capturadas as fotos de todos os colaboradores, terceiros, visitantes, candidatos e pessoas não gratas.

2.6.1. Webcam

- Para a captura da foto, o sistema SURICATO utiliza um equipamento Webcam que, conectado a uma porta USB, interage com a aplicação através do Suricato Client.
- A foto é capturada e armazenada em uma tabela no formato imagem, atribuída ao colaborador.
- O sistema tem a opção de procurar um arquivo em disco, dessa maneira, sem utilização da câmera.
- Com a opção de importação coletiva de foto, é possível, a partir de um banco de fotos, importar essas fotos de forma automática, sem a necessidade de captura individual.

2.6.2. Torre de Captura

- É um sistema desenvolvido para realizar a captura da foto do visitante e do documento frente e verso em uma única execução na aplicação do SURICATO utilizando o Suricato Client na opção 3 em 1, na barra de menu existe a opção de entrada de visitante com captura de foto.

2.6.3. Scanner

- O sistema solicita a imagem do documento do visitante no momento da entrada (cadastro) e liberação do crachá.
- O scanner homologado para uso pelo Sistema possui a funcionalidade de “duplicar” o documento do visitante frente e verso e envia-lo a uma tabela no formato imagem.
- Para seu funcionamento, esse dispositivo utiliza o Suricato Client e uma Scanner.

2.6.4. Leitora de mesa Smartcard

- Dispositivo leitor de crachás que é utilizado como periférico para gravar e ler cartões Smartcard no sistema SURICATO.
- Utiliza Suricato Client para executar a ação. Todas as aplicações que utilizam gravação de crachás têm uma integração com a Leitora.

2.6.5. Leitora de mesa Biométrico

- Dispositivo de leitura de biometria dos dedos para realizar o cadastro dos colaboradores na base de dados do SURICATO.
- Após efetuado o cadastro da biometria, é enviado para os equipamentos a biometria referente ao equipamento no qual o colaborador tem acesso.

2.6.6. Leitora de mesa da Palma da Mão

- A leitora de mesa da palma da mão é utilizada para o cadastro do colaborador e envio do registro da palma para o devido equipamento de acesso. O sistema utiliza o Suricato Client especifica para esse tipo de leitora.

3. Funcionalidades

- O SURICATO foi desenvolvido para garantir segurança e amparo aos clientes de maneira efetiva e integral.
- As funcionalidades descritas a seguir demonstram o quanto o sistema foi planejado para ser uma solução definitiva neste aspecto.

3.1. Cadastros

- Possui registros no sistema para controlar a informação absoluta do negócio.
- Empresa, Empresa Terceira e Filial especificam a origem do colaborador
- Planta e Portaria especificam a área da empresa que será controlada e identifica a entrada principal para a empresa, respectivamente.
- CODINs, Modelos de CODINs, Gateway, Alarmes e CFTV especificam a estrutura física da instalação do SURICATO. Esses dispositivos controladores serão responsáveis por capturar e controlar as informações pertinentes ao acesso às áreas da empresa.

3.1.1. Colaboradores

- Colaboradores são pessoas identificadas no sistema SURICATO de três maneiras: Empregados, Terceiros e Parceiros. Dos colaboradores, o sistema registra e mantém as seguintes informações:
- **Cadastro completo do Colaborador:** Registra os dados individuais de cada pessoa no sistema incluindo desde data de admissão até número de documentos como CPF e Carteira de Habilitação.
- **Perfil:** Configura as regras de acesso de cada pessoa. As regras são partes fundamentais das validações de acesso que o sistema deve tomar como parâmetro para garantir a integridade das informações. Entre as validações principais estão controles como verificações de grupo de acesso, anti-dupla, faixa horária, validade do ASO (Atestado de Saúde Ocupacional) e validade do treinamento. Existe um grupo de acesso para cada situação: Dias Normais (úteis), Sábados, Domingos e Feriados.
- **Históricos:** (Crachá, Afastamento, Escala, Baixa de Crachá, Cargo, Local, Filial, Centro de Custo e Contrato) – Mantém e controla alterações nos registros de colaboradores. Permite consultas e alterações, possibilitando manutenções dos dados sobre os colaboradores e ajustes de cargos, escala, situação, etc.
- **Crachás:** Informa o número do cartão atribuído para o colaborador. Por meio dessa função, atribui-se um número para o crachá e também a sua data de validade, além de gerenciar todos os crachás já disponibilizados às pessoas.
- **Baixa de Crachá:** É utilizada quando o crachá não será mais utilizado e será atribuído outro crachá para o colaborador, no caso de perda.
- **Afastamento:** Especifica a situação do colaborador na empresa. Em caso de afastamento, temporário ou definitivo, deve ser registrado um histórico de afastamento, com a devida situação trabalhista. A situação trabalhista do colaborador é cadastrada no sistema, conforme regra da empresa. Se a situação estiver definida para bloqueio de acesso, o crachá dessa pessoa será bloqueado automaticamente durante o período determinado de afastamento.
- **Escala:** Especifica a escala de trabalho do colaborador. Cadastrar a escala significa estabelecer horários de acesso à empresa e de marcação de ponto permitidos para o colaborador. A escala pode ser programada conforme os dias da semana e também pode ser adaptada para até 7 faixas horárias por dia. No histórico de escalas, ocorre a atribuição da escala definida pelo sistema ao colaborador.
- **Cargo:** Determina qual o cargo ocupado pelo colaborador na empresa. No cadastro de empresa existe o recurso de inserir todos os cargos de uma empresa e no histórico de cargos, atribui-los a um colaborador.
- **Local:** Especifica a posição do Organograma da empresa que é ocupada pelo colaborador. No cadastro de empresa deve ser informado o Organograma de maneira a definir os locais para cada empresa. No histórico de Locais, é mantido um registro de acordo com a condição do colaborador.

- **Filial:** Especifica a Filial à qual o colaborador pertence. O Cadastro de Filial registra as filiais existentes na empresa, além de informar diferenças de fuso horário, para o controle de pontos e acessos.
- **Centro de Custo:** Especifica a qual centro de custo da empresa o colaborador pertence.
- **Contrato:** Utilizado para Terceiros, o Histórico de Contratos define o tipo e a validade do contrato do terceiro na empresa. Os contratos devem ser cadastrados no sistema e depois atribuídos a um terceiro.

3.1.2. Grupo de Acesso

- Todo colaborador deve pertencer a um grupo de acesso no sistema para que suas permissões de acesso sejam estabelecidas.
- Um grupo de Acesso corresponde a um grupo de CODINs ao qual o colaborador terá permissão de acesso. Esse grupo de CODINs corresponderá às áreas da empresa às quais o colaborador terá acesso.
- No SURICATO, o grupo de acesso pode ser atribuído ou alterado individual ou coletivamente.

3.1.3. Visitantes, Candidatos e Pessoas Não Gratas

- Visitantes são pessoas que não pertencem à empresa e têm acesso definido por meio de autorização prévia de um responsável, com início e fim de permanência. No SURICATO, as funções disponíveis para controle de visitantes são:
- **Cadastro de Visitante e Grupo de Visitante:** Registra e mantém os dados dos visitantes e grupos de visitantes.
- **Tipo de Visita:** Especifica a regras de acesso que serão aplicadas ao visitante, como por exemplo, o tempo mínimo de visita, horário limite de visita, geração de créditos automáticos, entre outros. O SURICATO permite a criação de vários tipos de visitas, determinando assim diversas categorias que podem ser aplicadas de acordo com a definição do usuário.
- **Agendamento de Visitante e Agendamento de Grupo:** Realiza um pré-cadastro do visitante da empresa. O agendamento do visitante ou de um grupo de visitantes facilita o trabalho da portaria da empresa. Todos os dados relativos à visita já estarão pré-cadastrados, restando apenas atribuir o crachá e a data de validade. Agiliza-se assim o processo de credenciamento.
- **Candidatos:** Pessoas que não pertencem à empresa e terão acesso restrito, definido por autorização prévia e limite de permanência. Para a autorização do candidato, é necessário informar o motivo de acesso.
- **Pessoas Não Gratas:** São pessoas que, de acordo com a configuração individual no sistema, só poderão entrar na empresa com autorização concedida na hora da entrada. O sistema torna obrigatório o preenchimento do Motivo da Pessoa Não Grata e qual o procedimento padrão para cada caso.

3.1.4. Crachás

- No sistema SURICATO, o crachá constitui-se como cartão identificador de uma pessoa ou de um objeto.
- Todo crachá é configurado antes de ser atribuído a uma pessoa ou a um objeto. Essa configuração é denominada pré-cadastro do crachá. A principal função do pré-cadastro é inserir no sistema a tecnologia do crachá, seu número e o número físico para garantir que o crachá que está sendo utilizado no SURICATO é realmente o que está sendo gerenciado pelo por ele.
- O SURICATO oferece um recurso de cadastro de crachás por faixa. O conceito dessa funcionalidade é o de inserir um grupo sequencial de faixas (números) de crachá que especifiquem um tipo de colaborador (empregado, terceiro, parceiro), candidato, crachás provisórios, etc.
- Para crachás provisórios, o SURICATO permite que seja informado um número igual à quantidade de crachás que serão disponibilizados mensalmente por pessoa, gerando um alarme caso esse número ultrapasse o previamente definido. As outras validações da configuração do crachá se restringem a estabelecer regras de uso que melhor se adequem às necessidades da empresa.

• **Crachá Mestre e Acesso Geral:** esse crachá é utilizado no sistema para configurar os dispositivos de controle de acesso (CODINs). O crachá mestre tem permissão para configurar todos os CODINs da empresa cadastrados no SURICATO. O crachá mestre é atribuído a um colaborador que será o responsável por esse crachá na empresa.

3.1.5. Recursos de Sistema

- A partir do momento em que os colaboradores foram registrados no SURICATO, o sistema apresenta recursos funcionais para o controle de acesso e manutenção individual ou coletiva.
- São recursos que estão relacionados aos acessos às áreas controladas e também às funcionalidades operacionais do dia a dia da empresa.
- A seguir, é apresentada uma relação desses recursos e as funcionalidades de cada um deles.
- **Programação:** Agendamentos de alterações (trocas) no sistema SURICATO com utilização do Processo Automático (Serviço SURICATO que compõe o produto). As trocas podem ocorrer em Troca de Escala, Troca de Grupo de Acesso, Troca de Horário e Troca de Pontes.
- **Área Restrita:** Possibilita que um determinado colaborador tenha acesso a um local que lhe é restrito (fora do seu grupo de acesso) por um tempo determinado. O acesso restrito complementa o grupo original da pessoa.
- **Benefício** – Se a empresa utilizar distribuição de benefícios aos colaboradores (cestas básicas, prêmios, brindes e etc.), o SURICATO apresenta uma funcionalidade que controla e registra essa ação. Para isto basta configurar um CODIN como “benefícios”. Após isto, basta utilizar o recurso de controle de benefícios para que seja realizado um controle sobre distribuição, produtos, quantidades, históricos e relatórios.
- **Crédito de Acesso:** Controla e distribui créditos aos colaboradores na empresa.
- **Controle de Materiais:** Cadastra materiais que terão a saída permitida da empresa junto a um determinado colaborador. Todo material deve ter um colaborador como responsável. Permite realizar autorização de entrada e saída, solicitação de saída e movimentação do material.
- **Liberação de Faixa Horária:** Permite prolongar o horário de um determinado colaborador de acordo com a necessidade. Essa liberação só é permitida para o dia corrente, ou seja, não se trata de uma programação de troca de horário, mas sim de uma liberação ocasional. A liberação de Faixa Horária não altera a escala do colaborador.
- **Autorização de Entrada:** Permite ao colaborador acesso à empresa fora de seu perfil, ou seja, se o colaborador precisar entrar na empresa num dia em que não esteja escalado para tal, pode-se utilizar esse recurso para autorizar a entrada somente na data específica. Nesse momento, um outro crachá será disponibilizado para o colaborador e este perderá a validade tão logo acabe o prazo previamente estabelecido. O sistema SURICATO permite que ocorra um agendamento para a autorização da entrada.
- **Crachá Provisório:** Utilizado em caso de perda, roubo ou esquecimento do crachá titular. No momento da atribuição do crachá provisório, o crachá titular é bloqueado (por motivo de segurança). Essa ação é automática. O crachá provisório possui uma data e horário de validade. Se ocorrer a expiração da data e hora, ambos os crachás permanecerão bloqueados. O crachá titular é liberado somente após a baixa do crachá provisório.
- **Bloqueio e Desbloqueio de Crachás e Colaboradores:** O crachá permanece bloqueado até ocorrer o seu desbloqueio (somente neste caso). Em caso de data e hora de validade expirada, o crachá permanece bloqueado. A função de bloqueio de colaboradores tem uma funcionalidade dupla: bloqueia o colaborador e também o crachá titular (por segurança).
- **Envio de Mensagem Individual ou Coletiva:** O sistema SURICATO permite que sejam enviadas mensagens aos colaboradores através dos dispositivos CODINs de maneira individual ou coletiva. A mensagem é disponibilizada no momento do acesso do colaborador através do dispositivo. É configurada pelo número de vezes que será mostrada no visor dos CODINs e pela data de início e término da mensagem. Será vista em todos os CODINs do grupo de acesso do colaborador.

- **Afastamento:** O SURICATO permite efetuar o afastamento de pessoas bloqueando o crachá por um período pré-definido.
- **Filtro de abrangência:** O filtro de abrangência serve para separar a visibilidade do usuário no sistema, sendo possível dividir por empresa, filial, tipo de colaborador, empresa terceira, contrato, centro de custo, situação trabalhista, organograma, local, colaborador responsável, planta, CODIN, grupo de acesso e portaria.
- **Log:** Todas as aplicações registram as ações executadas em arquivos tipo Log. O sistema armazena numa tabela o usuário logado no sistema no momento da ação e permite que esse registro seja consultado posteriormente. Esse recurso permite segurança para a instalação, uma vez que é possível reconhecer quem acessou tal aplicação, em que momento e o que fez (inclusão, alteração ou exclusão).
- **Idioma:** O SURICATO possui 3 idiomas português, inglês e espanhol.

3.1.6. Regras de Negócio no Sistema SURICATO

- No Sistema SURICATO, as regras de validação estão contidas no Banco de Dados e serão executadas ao longo de todo processo.
- As validações compreendem as configurações cadastradas para os colaboradores e também para os CODINs.
- A seguir, são demonstradas algumas validações do Sistema SURICATO para tratamento de situações comuns:
- **Bloqueio de Acesso de Colaboradores** :Um colaborador pode ser bloqueado pelos seguintes motivos:
 - a. Validade do crachá;
 - b. Validade do Atestado de Saúde Ocupacional;
 - c. Validade do Treinamento de Segurança;
 - d. Situação;
 - e. Validade do Contrato de Serviço;
 - f. Validade de CNH (Carteira Nacional de Habilitação);
 - g. Validade equipamento de proteção individual (EPI);
 - h. Validade histórico de integração;
 - i. Validade da carteira de trabalho da previdência social (CTPS).
- Situações que poderão ocasionar bloqueio nos CODINs (colaboradores e visitantes):
 - a. **Escala:** Colaborador fora da escala horária tentando acessar o CODIN;
 - b. **Faixa Horária:** A faixa horária do CODIN determina a sua utilização;
 - c. **Permanência:** Permanência do visitante ou candidato expirada enquanto está dentro da empresa;
 - d. **Acesso restrito:** Expirada a liberação ao acesso restrito;
 - e. **Autorização de Entrada:** Expirada a Autorização de entrada do colaborador;
 - f. **Faixa Horária de Almoço:** Determina o horário de almoço que deve ser cumprido;
 - g. **Intervalo de tempo:** Determina o intervalo que o colaborador poderá sair/entrar da empresa;
 - h. **Tolerância de entrada/saída:** Tolerância no horário do colaborador, para entrar ou sair da empresa;
 - i. **Local inválido:** Colaborador não ter acesso a uma determinada área (CODIN) para acesso;
 - j. **Anti-dupla:** CODIN configurado para não aceitar anti-dupla, ou seja, dois acessos com o mesmo crachá e no mesmo sentido;
 - k. **Controle de nível:** CODIN configurado, para efetuar controle de nível (rota), dessa forma, caso a pessoa tente um acesso pelo nível 2 sem passar pelo nível 1, seu acesso é bloqueado;
 - l. **Validade do Crachá Provisório:** Expirado o crachá provisório do colaborador;
 - m. **Crédito de acesso ao refeitório:** Controle por faixa horário e por quantidade.

3.1.7. CODINs

- Os dispositivos de controle de acesso no Sistema SURICATO são cadastrados de forma individual, cada um com um endereço IP (para redes TCP/IP).
- Para cadastrar um CODIN, é necessário que seja informada a localização e o modelo do CODIN, a planta de localização, o tipo de leitora (tecnologia), entre outras informações.
- Ainda no cadastro do CODIN, deve-se determinar as configurações das portas de entrada e saída, ou seja, o CODIN comporta outros equipamentos conectados a ele, como integração com o CFTV, por exemplo.
- O Sistema SURICATO possui o cadastro de CFTV e de alarmes. Todas essas funcionalidades são agregadas na configuração do CODIN.
- Se o ambiente de instalação possuir alarmes nas portas que poderão disparar eventos para os CODINs, então essa informação deve ser registrada.
- Da mesma forma, as câmeras de CFTV deverão estar relacionadas às portas dos CODINs, de modo que a aplicação consiga interpretá-las e enviar o comando corretamente na integração com o monitoramento on-line.

3.1.8. CODINs ReP

- Os dispositivos de controle de ponto no Sistema SURICATO são cadastrados de forma individual, cada um com um endereço IP (para redes TCP/IP).
- Para cadastrar um CODIN de Ponto, o processo é o mesmo do CODIN de acesso. O que diferencia é o modelo selecionado, que deverá ser cadastrado com as características de um CODIN de ponto

3.1.9. CFTV

- A integração do CFTV no sistema SURICATO ocorre no monitoramento on-line.
- As câmeras de CFTV (Circuito Fechado de TV) são instaladas em pontos estratégicos da empresa e são capazes de detectar movimentos suspeitos, acessos indevidos, coação, arrombamentos, pânico e outras situações que estabeleçam falta de segurança para o ambiente.
- No monitoramento on-line, as imagens são exibidas no momento que antecede o alarme (3 segundos antes) para que o operador visualize o exato momento da ocorrência. Na mesma tela, o operador tem a opção de visualizar o vídeo em tempo real, possibilitando assim a tomada de ação imediata após o evento.

3.1.10. Processos Automático

- O Sistema SURICATO utiliza um serviço chamado Processos Automáticos desenvolvido na linguagem de programação JAVA.
- Esse serviço é responsável por executar todas as programações e agendamentos do sistema em modo automático.
- Entre as funcionalidades principais, os Processos Automáticos são responsáveis por executar a importação e exportação de dados, disponibilizando um arquivo.txt em cada exportação e recebendo para importação um arquivo.txt com layout pré-definido. Além de enviar comandos aos CODINs, enviam relatórios automaticamente e outros recursos.
- O Processo Automático disponibiliza uma tela de configuração do leiaute das tabelas do sistema. O mesmo se faz para os arquivos de importação.
- Após a definição do leiaute, o comando de importação ou exportação pode ser executado.
- Essa rotina pode ser repetida de acordo com a necessidade. Na configuração do processo, existe opção para que este seja repetido em cada x minutos, em cada x horas, em cada x dias, etc

3.1.11. Relatórios

- O SURICATO disponibiliza uma série de relatórios padronizados que podem ser impressos ou apenas consultados na tela.
- Esses relatórios podem ser gerados pelo processo automático e enviados por e-mail, impressos, ou até mesmo exportados para os formatos pdf, xls, etc.
- O SURICATO oferece o recurso do módulo Gerador de Relatórios.
- Através desse Módulo, é possível criar relatórios específicos, desenhados pelo próprio usuário, e enviá-los para que os Processos Automáticos os executem conforme seja necessário.
- Ou seja, o SURICATO apresenta opções em termos de relatórios para que qualquer que seja a necessidade do usuário, o produto o atenda com sucesso.

3.1.12. Login e Usuários

- O Sistema SURICATO é instalado com um Login e senha padrão de acesso irrestrito a todas as aplicações e permissões.
- Na configuração do sistema, o cliente deve configurar os usuários que terão acesso e determinar as permissões de cada um.
- É possível estabelecer a que cada usuário terá acesso ou permissão, restringindo permissões a menus que não sejam convenientes ao seu tipo de trabalho.
- As permissões são distribuídas conforme os menus do sistema SURICATO.
- Cada usuário cadastrado tem controle sobre suas ações na tela de configuração. Todas as alterações, inclusões e exclusões são registradas em arquivos e podem ser consultadas sempre que necessário.
- Outro recurso disponibilizado é a substituição de usuários provisórios para o acesso ao sistema SURICATO.
- Quando um usuário estiver ausente ou de férias e uma outra pessoa o substituir em sua função, ao invés de criar um outro usuário com permissões idênticas, utiliza-se o usuário provisório.
- Dessa maneira, o sistema garante integridade das ações, pois, o provisório passará a utilizar uma permissão que fora atribuída ao titular por um período de tempo determinado no sistema e o titular dessa permissão ficará bloqueado até retornar à sua função.
- Esse é mais um benefício de garantia de segurança SURICATO

3.1.13. Reação de Eventos

- O SURICATO possui um recurso de reações de eventos, disparados automaticamente como resposta a um evento de acesso ou alarme, de acordo com as definições programadas pelo usuário.
- As reações, por exemplo, podem ser um envio de e-mail; acionamento de sirene de um CODIN, liberação condicional dos CODINs (emergência), etc.

4. Anexos

- Neste tópico exibiremos no formato de planilha a matriz de funcionalidades do sistema SURICATO .

4.1. Anexo I - Matriz de Funcionalidades

- Matriz de Funcionalidades do Sistema de Controle de Acesso e Segurança SURICATO

Estrutura do Sistema

Desenvolvido em plataforma WEB nas Linguagens PHP, Java Script, Java e Ajax.

Utilização de Certificado Digital.

Comunicação segura utilizando https.

Segurança do produto com a criptografia/ofuscamento das aplicações

Suporte aos idiomas Português (Brasil), Espanhol (Espanha) e Inglês (Americano).

Servidor Web Apache ou IIS.

Banco de dados Oracle 19C e 21C – (padrão Inglês) e/ou Microsoft SQL Server 2016, 2017, 2019 e 2022 – (padrão Inglês)

Sistema Operacional - Servidor: Microsoft Windows Server® 2019 ou Microsoft Windows Server® 2022

Sistema Operacional - Estação: Microsoft Windows 10 ou Microsoft Windows 11

Navegadores: Google Chrome, Microsoft Edge e Mozilla Firefox

Funcionalidades

Controle de funções dos CODINs	Acesso
Comunicação com os CODINs via TCP-IP	Acesso
Tecnologia de Crachás barras, proximidades, Smart Card, RFID Biometria 1:1 e 1:N.	Acesso
Listas de Liberação, bloqueio, senhas e veículos quando o sistema estiver offline (exceto Smartcard).	Acesso
Restrição de acesso ao CODIN por faixas horárias independente do perfil da pessoa.	Acesso
Gerenciamento de Grupo de acesso aos CODINs, individual ou coletivamente e multiplanta.	Acesso
Gerenciamento de faixas horárias dos CODINs pertencentes aos grupos de acesso.	Acesso
Reconhecimento de eventos de acesso enviando e-mail.	Acesso
Reconhecimento de eventos de acesso com interação aos CODINs, podendo tocar sirene, abrir portas, etc	Acesso
Controle de anti-dupla ou anti-passback.	Acesso
Bloqueio automático por falta.	Acesso
Controle de Afastamento	Acesso
Controle de faixa horária de acesso.	Acesso
Controle de faixa horária de ponto.	Acesso
Controle de faixa horária de ponto e acesso.	Acesso
Controle de crédito de acesso por cotas ou por faixas.	Acesso
Controle de biometria 1:1.	Acesso
Controle de biometria 1:N - CODIN.	Acesso

<i>Controle de Biometria 1:N - Servidor.</i>	<i>Acesso</i>
<i>Controle de intervalo de almoço.</i>	<i>Acesso</i>
<i>Controle de permanência.</i>	<i>Acesso</i>
<i>Controle de validade da ASO (Atestado de Saúde Ocupacional).</i>	<i>Acesso</i>
<i>Controle de validade de treinamentos.</i>	<i>Acesso</i>
<i>Liberação de acesso por grupos pré-definidos para dias úteis (segunda a sexta), sábado, domingo e feriados.</i>	<i>Acesso</i>
<i>Controle de nível de acesso.</i>	<i>Acesso</i>
<i>Programações futuras de troca temporária de horário, escala, ponto e grupo de acesso.</i>	<i>Acesso</i>
<i>Trocas efetivas de grupos de acesso coletivamente ou individualmente.</i>	<i>Acesso</i>
<i>Cadastro de senha para utilização de controle de acesso nos CODINs.</i>	<i>Acesso</i>
<i>Crachá mestre, que dá direito ao acesso total à empresa.</i>	<i>Acesso</i>
<i>Controle de crachás extraviados.</i>	<i>Acesso</i>
<i>Pré-cadastro de crachás, garantindo que os crachás distribuídos são realmente os cadastrados.</i>	<i>Acesso</i>
<i>Leitura de crachás Smartcard, possibilitando visualizar o conteúdo dos crachás.</i>	<i>Acesso</i>
<i>Bloqueio e desbloqueio de pessoas, possibilitando que a pessoa utilize um outro crachá.</i>	<i>Acesso</i>
<i>Bloqueio e desbloqueio de crachás, não permitindo que a pessoa utilize nenhum outro tipo de crachá.</i>	<i>Acesso</i>
<i>Liberação de faixas horárias quando uma pessoa estiver bloqueada pelo horário.</i>	<i>Acesso</i>
<i>Envio de mensagens aos CODINs.</i>	<i>Acesso</i>
<i>Distribuição e controle de benefícios.</i>	<i>Acesso</i>
<i>Gerenciamento de áreas restritas. Liberando o acesso de uma pessoa por um determinado período.</i>	<i>Acesso</i>
<i>Consulta de acesso as áreas restritas.</i>	<i>Acesso</i>
<i>Sistema Multi-empresa (permite o gerenciamento de várias empresas).</i>	<i>Administração</i>
<i>Controle de Organogramas por empresa.</i>	<i>Administração</i>
<i>Controle de Cargos por empresa.</i>	<i>Administração</i>
<i>Controle de Escalas/Jornadas Horárias.</i>	<i>Administração</i>
<i>Controle de Centro de Custo.</i>	<i>Administração</i>
<i>Gerenciamento de Filiais.</i>	<i>Administração</i>
<i>Administração de Empresas terceiras (pessoal terceirizado e visitantes).</i>	<i>Administração</i>
<i>Administração de Contratos de terceiros.</i>	<i>Administração</i>
<i>Sistema Multiplanta (permite o gerenciamento de várias plantas individualmente ou coletivamente).</i>	<i>Administração</i>
<i>Controle descentralizado de portarias e recepções.</i>	<i>Administração</i>
<i>Manual on-line do SURICATO com todas as funcionalidades.</i>	<i>Ajuda</i>
<i>Gerenciamento de alarmes.</i>	<i>Alarmes</i>
<i>Exibição dos alarmes por prioridades.</i>	<i>Alarmes</i>
<i>Possibilidade de configurações de cores para exibição dos alarmes (* exceto monitoramento com planta).</i>	<i>Alarmes</i>
<i>Tocar arquivo de som (* somente no monitoramento com plantas).</i>	<i>Alarmes</i>
<i>Reconhecimento de alarmes.</i>	<i>Alarmes</i>
<i>Tratamento de alarmes.</i>	<i>Alarmes</i>
<i>Cadastro de procedimentos que o operador deve tomar quando acontecer um alarme.</i>	<i>Alarmes</i>
<i>Envio de e-mail quando ao ocorrer um alarme.</i>	<i>Alarmes</i>

<i>Interação com outros dispositivos CODINs ao ocorrer um alarme podendo tocar sirene, abrir portas, etc.</i>	<i>Alarmes</i>
<i>Cadastro de candidatos para controle de acesso.</i>	<i>CFTV</i>
<i>Agendamento da entrada de um candidato.</i>	<i>CFTV</i>
<i>Autorização de acesso de um candidato.</i>	<i>CFTV</i>
<i>Integração com CFTV Telemática.</i>	<i>CFTV</i>
<i>Pesquisa de imagem automaticamente no momento da geração de um evento de acesso ou alarme.</i>	<i>CFTV</i>
<i>Tela cheia dos vídeos.</i>	<i>CFTV</i>
<i>Vídeos no modo Playback e no modo ao vivo.</i>	<i>CFTV</i>
<i>Visualização de vídeos do CFTV com apenas um clique nas câmeras do monitoramento.</i>	<i>CFTV</i>
<i>Relacionamento de vídeos com CODINs.</i>	<i>CFTV</i>
<i>Relacionamento de vídeos com sensores.</i>	<i>CFTV</i>
<i>Integração com o sistema de OCR de placa quando integrado ao CFTV Telemática.</i>	<i>CFTV</i>
<i>Integração com o sistema de Reconhecimento de face quando integrado ao CFTV Telemática.</i>	<i>CFTV</i>
<i>10 opções de consulta, como presença e acessos das pessoas, visitantes, alarmes etc.</i>	<i>Consultas</i>
<i>Impressão de crachás.</i>	<i>Dispositivos</i>
<i>Integração com leitoras de mesa Smartcard Telemática.</i>	<i>Dispositivos</i>
<i>Integração com leitoras de mesa RFid Telemática.</i>	<i>Dispositivos</i>
<i>Captura de fotos dos documentos frente e verso através de scanner.</i>	<i>Dispositivos</i>
<i>Gerador de relatórios, possibilitando a criação de relatórios customizados.</i>	<i>Módulos Adicionais</i>
<i>Monitoramento de eventos de alarmes e acesso através de plantas gráficas.</i>	<i>Monitoramento</i>
<i>Navegação nas plantas, zoom, troca de plantas, som e pop-up de telas no momento do alarme.</i>	<i>Monitoramento</i>
<i>Monitoramento de eventos de alarmes e acesso através das tabelas no navegador.</i>	<i>Monitoramento</i>
<i>Ponto de Encontro</i>	<i>Monitoramento</i>
<i>Cadastro de colaboradores, com seus dados básicos.</i>	<i>Pessoas</i>
<i>Cadastro de terceiros, com seus dados básicos.</i>	<i>Pessoas</i>
<i>Cadastro de parceiros, com seus dados básicos.</i>	<i>Pessoas</i>
<i>Controle de liberação de crachás por validade.</i>	<i>Pessoas</i>
<i>Captura de fotos através de uma webcam.</i>	<i>Pessoas</i>
<i>Dados complementares, como andar, ramal, e-mail.</i>	<i>Pessoas</i>
<i>Integração com a base de dados CEP.</i>	<i>Pessoas</i>
<i>Controle do histórico de contratos dos terceiros, permitindo um mesmo terceiro migrar para outra empresa.</i>	<i>Pessoas</i>
<i>Históricos de filial.</i>	<i>Pessoas</i>
<i>Históricos de local</i>	<i>Pessoas</i>
<i>Históricos de cargo.</i>	<i>Pessoas</i>
<i>Históricos de escala.</i>	<i>Pessoas</i>
<i>Históricos de afastamento.</i>	<i>Pessoas</i>
<i>Históricos de crachá.</i>	<i>Pessoas</i>
<i>Históricos de centro de custo.</i>	<i>Pessoas</i>
<i>Perfil de acesso completo da pessoa através de uma única tela.</i>	<i>Pessoas</i>
<i>Notificação de Vencimento de Documentos</i>	<i>Pessoas</i>

<i>Registro de ocorrências, podendo enviar e-mail aos responsáveis.</i>	<i>Portaria</i>
<i>Gerenciamento remoto dos CODINs de todas as plantas, possibilitando bloquear, acertar data e hora, carregar listas e etc.</i>	<i>Processos</i>
<i>Ativação de modo emergência dos coletores, desbloqueando os acessos fisicamente.</i>	<i>Processos</i>
<i>Envio de comandos em lote.</i>	<i>Processos</i>
<i>Geração de listas automaticamente.</i>	<i>Processos</i>
<i>Módulo para criação de modelos de layout para importação de dados.</i>	<i>Processos</i>
<i>Importação automática e agendada de dados.</i>	<i>Processos</i>
<i>Exportação automática e agendada de dados.</i>	<i>Processos</i>
<i>Envio automático e agendado de relatórios.</i>	<i>Processos</i>
<i>Envio automático e agendado de e-mails.</i>	<i>Processos</i>
<i>Importação e exportação de fotos de pessoas.</i>	<i>Processos</i>
<i>Configuração e criação de usuários da aplicação SURICATO</i>	<i>Processos</i>
<i>Liberação de acesso aos menus de acordo com o perfil de cada usuário ou grupo de usuário.</i>	<i>Processos</i>
<i>Atualização automática das informações dos CODINs quando retornar ao modo on-line.</i>	<i>Processos</i>
<i>31 opções de relatórios de acessos, alarmes, visitantes e cadastro do SURICATO.</i>	<i>Relatórios</i>
<i>Liberação de visitas somente para pessoas autorizadas</i>	<i>Visitantes</i>
<i>Cadastro de visitantes utilizando RG, CPF e outros.</i>	<i>Visitantes</i>
<i>Cadastro de grupos de visitantes.</i>	<i>Visitantes</i>
<i>Perfil de acesso individual ou coletivo para as visitas, designando tipo de visitas.</i>	<i>Visitantes</i>
<i>Agendamento de visita.</i>	<i>Visitantes</i>
<i>Agendamento de grupo de visita.</i>	<i>Visitantes</i>
<i>Controle de vídeo de segurança (briefing)</i>	<i>Visitantes</i>
<i>Controle de pessoas não gratas (visitantes ou funcionários), apresentando mensagem durante cadastramento de um visitante.</i>	<i>Visitantes</i>
<i>Procedimento para pessoa não grata.</i>	<i>Visitantes</i>
<i>Credenciamento de visitantes.</i>	<i>Visitantes</i>
<i>Bloqueio manual de crachá de visitantes.</i>	<i>Visitantes</i>
<i>Baixa manual de crachá de visitantes.</i>	<i>Visitantes</i>
<i>Bloqueio automático de crachá de visitantes.</i>	<i>Visitantes</i>
<i>Baixa automática de crachá de visitantes.</i>	<i>Visitantes</i>
<i>Cadastro de visitantes a partir da última visita, mantendo as principais informações.</i>	<i>Visitantes</i>
<i>Distribuição e baixa de crachás provisórios, mantendo o titular bloqueado enquanto não efetivar a baixa.</i>	<i>Visitantes</i>
<i>Cadastro de autorização de entrada, permitindo o acesso de uma pessoa em local não utilizando seu crachá e perfil original.</i>	<i>Visitantes</i>
<i>Controle de carga e descarga de materiais dos veículos, com cadastro dos veículos e motoristas.</i>	<i>Visitantes</i>
<i>Controle de entrada e saída de materiais relacionados a pessoas.</i>	<i>Visitantes</i>
<i>Rastreamento de pessoas quando utilizado RFid.</i>	<i>Visitantes</i>

5. Pré-Requisitos

- Neste tópico descreveremos os requisitos de sistema para o funcionamento do sistema SURICATO.

5.1. Servidor de Banco de Dados

- **Processador:** Intel® Xeon® Quad Core ou superior
- **Memória:** 16GB
- **Espaço em Disco para Instalação:** 3GB

5.2. Servidor Aplicação SURICATO

- **Processador** Intel® Xeon® Quad Core ou superior
- **Memória** 8GB
- **Espaço em Disco para Instalação:** 8GB

5.3. Servidor Conex

- **Processador** Intel® Xeon® Quad Core ou superior
- **Memória** 16GB (500 CODINs) / Memória 32GB (1000 CODINs)
Acima de 1000 CODINs, adicionar um novo servidor
- **Espaço em Disco para Instalação:** 1GB

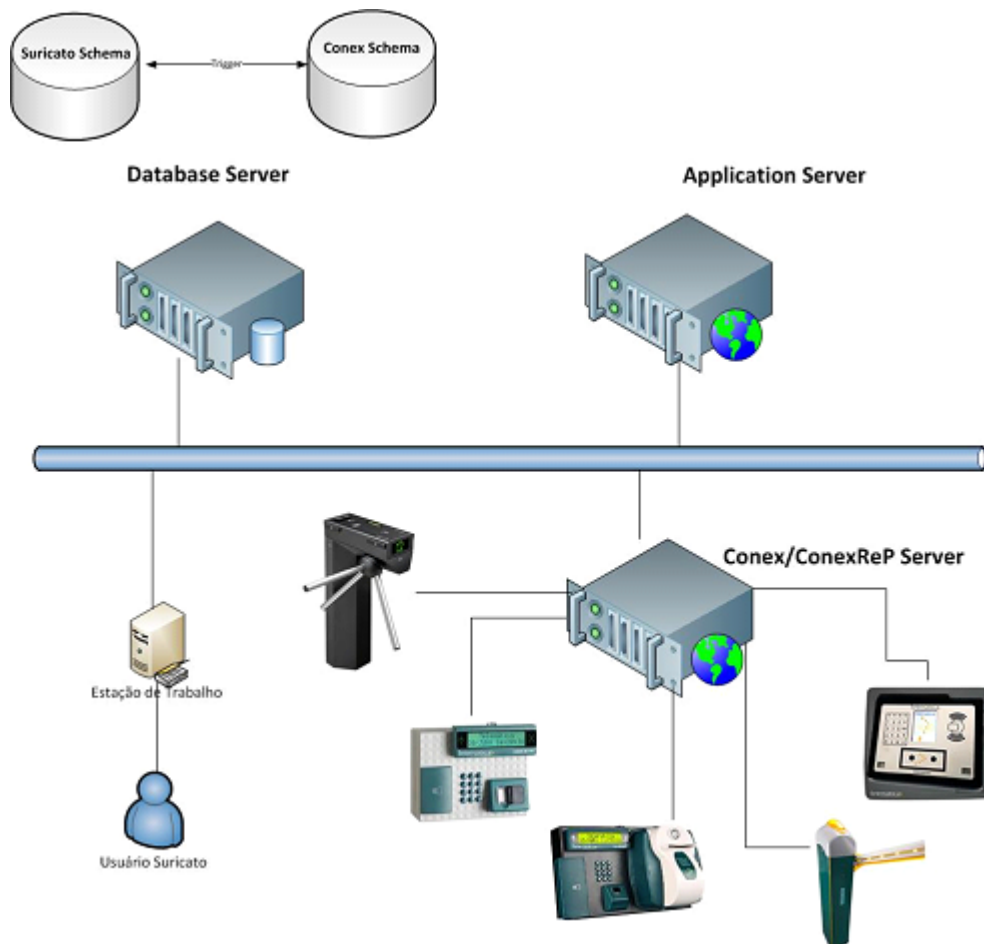
6. Modelo de Arquitetura

- Neste tópico exemplificaremos os modelos de arquitetura suportados pelo sistema SURICATO.

6.1. Arquitetura - A

- Modelo de Arquitetura recomendado para redes com grande quantidade de CODINs. Neste modelo de arquitetura será necessário:

- a. servidor de aplicação para a aplicação SURICATO.
- b. servidor de aplicação para a aplicação Conex/ConexReP.
- c. servidor de banco de dados para o SGDB do sistema Suricato

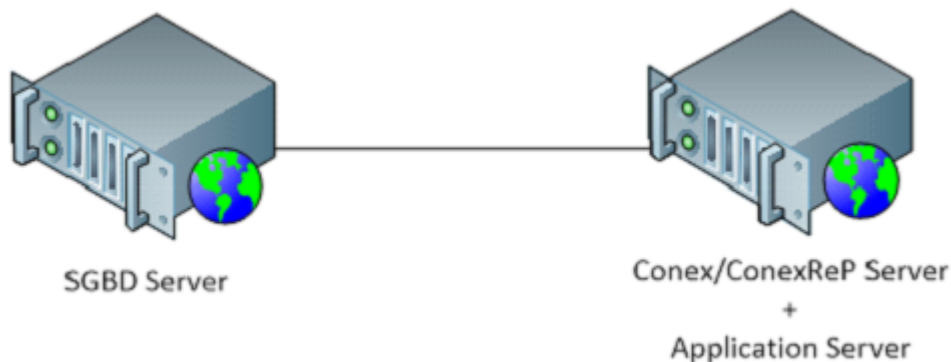


Exemplo - Arquitetura A

6.2. Arquitetura - B

• Modelo de Arquitetura recomendado para redes com no máximo 50 CODINs. Neste modelo de arquitetura será necessário:

- servidor de aplicação, para a aplicação SURICATO e Serviço Conex/ConexReP.
- servidor de banco de dados para o SGDB do sistema SURICATO.

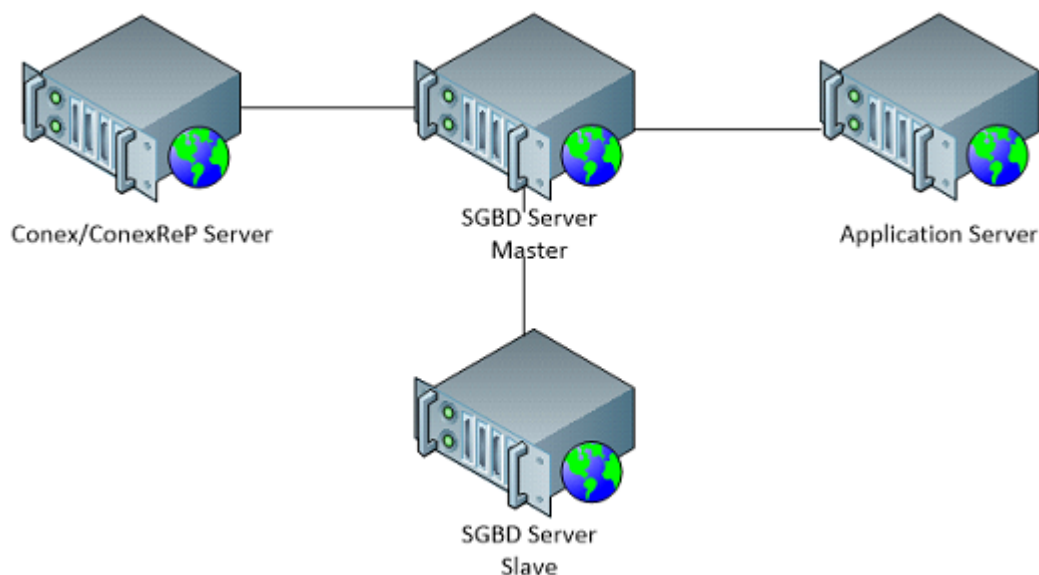


Exemplo - Arquitetura B

6.3. Arquitetura - C

• Modelo de Arquitetura onde se faz necessário contingência de banco de dados, e prevê um segundo servidor. Neste modelo de arquitetura será necessário:

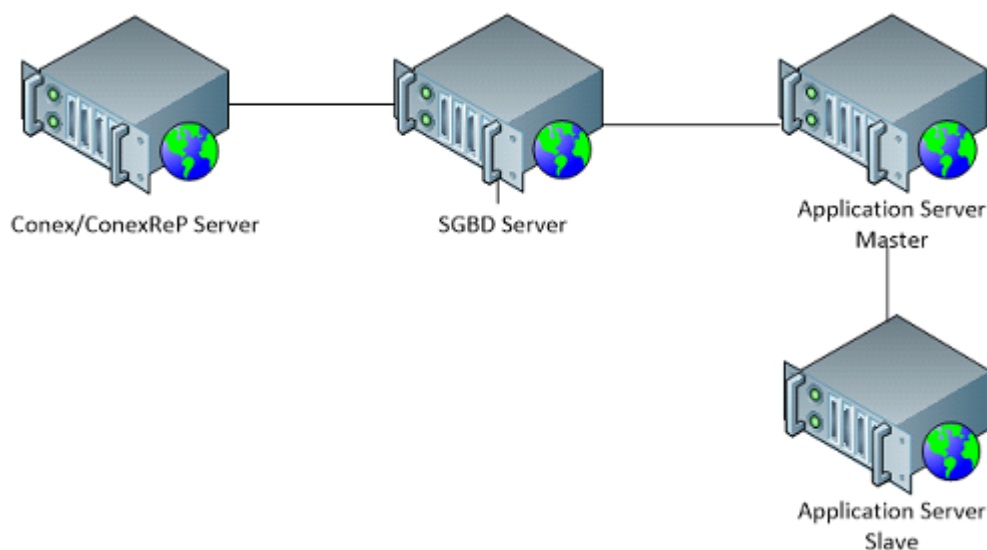
- servidor de aplicação para a aplicação SURICATO.
- servidor de aplicação para a aplicação Conex/ConexReP.
- servidor de banco de dados para o SGDB do sistema SURICATO. (Master)
- servidor de banco de dados para o SGDB do sistema SURICATO. (Slave)



Exemplo - Arquitetura C

6.4. Arquitetura - D

- Modelo de Arquitetura onde se faz necessário contingência do servidor de aplicação e prevê um segundo servidor. Neste modelo de arquitetura será necessário:
 - a. servidor de aplicação para a aplicação SURICATO. (Master)
 - b. servidor de aplicação para a aplicação SURICATO. (Slave)
 - c. servidor de aplicação para a aplicação Conex/ConexReP.
 - d. servidor de banco de dados para o SGDB do sistema SURICATO.
- Nesse modelo, há contingência do servidor de aplicação (Cluster) e prevê um segundo servidor. No caso de problema com o servidor Master, o servidor Slave entra em execução, garantindo a operação.



Exemplo - Arquitetura D