



**ESTADO DO RIO GRANDE DO SUL  
POLÍCIA CIVIL  
DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO POLICIAL  
DIVISÃO DE ACESSORAMENTO ESPECIAL**

**ANEXO A - FERRAMENTAS DE GERENCIAMENTO  
E MONITORAMENTO DO AMBIENTE DE TI**

**1. CONCEITO**

1.1. Entende-se como ferramenta de gerenciamento toda aquela ferramenta ou recurso de software que busca auxiliar a gestão dos processos referentes aos serviços contratados e aos processos de gestão e controle do ambiente de TI da CONTRATANTE.

**2. FERRAMENTAS DA CONTRATADA**

2.1. Todas as ferramentas e *softwares* de apoio utilizados pela CONTRATADA deverão ser conhecidos e aprovados previamente pela CONTRATANTE, de forma a manter a compatibilidade e total aderência aos produtos utilizados por ela.

2.2. A utilização das ferramentas será de responsabilidade exclusiva da CONTRATADA, que deverá tomar todas as providências relativas ao licenciamento do *software*, assumindo os custos correspondentes.

2.3. Em caso de encerramento do contrato, a propriedade das licenças de software adquiridas continuará sendo da CONTRATADA.

2.4. A CONTRATADA disponibilizará acesso a essas ferramentas a empregados da CONTRATANTE e colaboradores previamente cadastrados, conforme identificado pelos administradores do contrato.

2.5. Os empregados e colaboradores a terem acesso às ferramentas serão cadastrados pela CONTRATADA por solicitação formal do Administrador do Contrato pela CONTRATANTE. A solicitação de cadastro deverá conter a identificação do empregado e colaborador bem como o perfil de acesso desejado.

2.6. Os custos de gerenciamento e manutenção dessas ferramentas serão de responsabilidade da CONTRATADA.



**Av. João Pessoa, nº 2050, 3º andar, sala 480, Bairro Azenha, Porto Alegre/RS  
CEP: 90040-001 - Fone: 51 3288-2116  
E-mail: dtip-dae@pc.rs.gov.br**

1



**ESTADO DO RIO GRANDE DO SUL**  
**POLÍCIA CIVIL**  
**DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO POLICIAL**  
**DIVISÃO DE ACESSORAMENTO ESPECIAL**

2.7. A CONTRATADA deverá disponibilizar as licenças das ferramentas para a CONTRATANTE durante a vigência do contrato no caso de não ser Licença Pública Geral (GPL). Após o encerramento do contrato, as licenças permanecerão sob propriedade da CONTRATADA.

**2.8. Ferramentas para Solução de Monitoração**

2.8.1. A CONTRATADA deverá disponibilizar uma solução completa, igual a utilizada em seu NOC, composta de *software*, com características de multiplataforma, para monitoramento e gerenciamento de servidores, redes e sistemas da CONTRATANTE. As ferramentas deverão possibilitar o acompanhamento *on-line* e a consulta de dados históricos em relação à disponibilidade e desempenho relativos a todos os serviços e equipamentos que venham a compor o Ambiente de Tecnologia da Informação da CONTRATANTE.

**2.9. Ferramenta de Gerenciamento de Infraestrutura de TI**

2.9.1. Constitui-se de gerenciamento de TI composta por funcionalidades que estão relacionadas às disciplinas de Gerenciamento de Serviços e Configurações (Service Asset & Configuration Management), Gerenciamento de Mudanças (Change Management, Gerenciamento de Eventos (Event Management), Gerenciamento de Disponibilidade (Availability Management) e Gerenciamento de Capacidade (Capacity Management), conforme definido dentro das práticas ITIL. Todas essas funcionalidades deverão também ser embasadas por uma Base de Dados de Gerenciamento de Configuração (CMDB) integrada que armazena as informações sobre a Infraestrutura de TI. Nas seções abaixo são fornecidas as características e funcionalidades exigidas neste processo de aquisição.

**2.9.1.1. Base de Dados de Gerenciamento de Configurações (CMDB)** – A CMDB é a base de dados que armazena as informações dos itens que compõe a infraestrutura de TI de uma organização, os Itens de Configuração (IC). A CMDB deverá guardar, além dos itens de configuração, os Atributos destes elementos, as relações que eles mantêm com outros Itens de Configuração do Ambiente e todas as informações de apoio para suportar as necessidades de cada funcionalidade do software que está relacionada às disciplinas de gestão de TI relacionadas acima.

**Av. João Pessoa, nº 2050, 3º andar, sala 480, Bairro Azenha, Porto Alegre/RS**  
**CEP: 90040-001 - Fone: 51 3288-2116**  
**E-mail: dtip-dae@pc.rs.gov.br**

2



**ESTADO DO RIO GRANDE DO SUL**  
**POLÍCIA CIVIL**  
**DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO POLICIAL**  
**DIVISÃO DE ACESSORAMENTO ESPECIAL**

2.9.1.1.1. A CMDB deverá ser capaz de armazenar:

2.9.1.1.1.1. Itens de Configuração:

2.9.1.1.1.1.1. Os itens de Configuração são as unidades de armazenamento mais importantes das CMDB, todos os outros elementos de uma CMDB são subelementos de um IC. Um IC pode ser entendido como qualquer elemento configurável de um ambiente de TI, devendo ser tipificado de acordo com sua natureza. Um IC pode ser um Hardware, Software ou quaisquer subcomponentes (hardware ou software) usado para manipular uma configuração qualquer ou armazenar de forma organizada informações sobre tais elementos. É importante que a ferramenta armazene cada Item de Configuração de forma isolada na CMDB, evitando que se agregue configurações ou atributos de mais de Item de Configuração em um elemento único. Assim sendo a ferramenta deve ser capaz de armazenar cada item de configuração isoladamente, cada qual com seus atributos e configurações para fins de possibilitar análises de impactos e dependências com a granularidade desejada. Não serão aceitas ferramentas que interpretem os conceitos de Item de Configuração como um sinônimo de host, dispositivo ou qualquer simplificação do conceito de Item de Configuração.

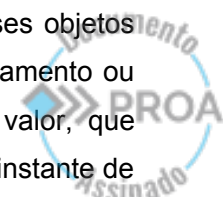
2.9.1.1.1.1.2. Os itens de Configuração deverão ser tipificados de acordo com uma lista de tipos pré-definidas (ver Modelos de Itens de Configuração). Um Item de Configuração sempre deverá ser de um tipo específico. Os tipos de itens de configuração deverão definir de quais grupos eles participam (em decorrência de sua classificação), quais atributos podem ser associados ao IC e quais os possíveis valores que poderão assumir, quais são os atributos obrigatórios e quais relações poderão manter com outros tipos de IC.

2.9.1.1.1.2. Atributos de Itens de Configuração:

2.9.1.1.1.2.1. Os atributos dos itens de configuração são informações relacionadas aos IC que podem representar uma simples característica de um desses objetos ou armazenar configurações que afetam o modo seu modo de funcionamento ou operação. Devem ser sempre armazenados como um par nome e valor, que identifique o atributo e seu respectivo valor que está assumindo em um instante de

**Av. João Pessoa, nº 2050, 3º andar, sala 480, Bairro Azenha, Porto Alegre/RS**  
**CEP: 90040-001 - Fone: 51 3288-2116**  
**E-mail: dtip-dae@pc.rs.gov.br**

3





**ESTADO DO RIO GRANDE DO SUL**  
**POLÍCIA CIVIL**  
**DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO POLICIAL**  
**DIVISÃO DE ACESSORAMENTO ESPECIAL**

tempo. O tipo do IC e seu conjunto de atributos e valores identificam um exemplar do IC no ambiente de TI.

2.9.1.1.1.2.2. A ferramenta deverá ter a capacidade de definir o conjunto de atributos possíveis e obrigatórios para um IC específico em função do seu tipo. Deverá ter a capacidade de definir valores padrão para um atributo para que, no evento de sua criação, o IC tenha valores pré-definidos para determinados atributos. É importante também que se possa utilizar fórmulas para os valores de atributos, podendo compor o valor de um atributo com o valor de outros atributos do item de configuração.

2.9.1.1.1.3. Relação:

2.9.1.1.1.3.1. A ferramenta deverá ter a capacidade de armazenar na CMDB as relações diretas entre os Itens de Configuração. Tais relações deverão ser tipificadas quanto ao seu tipo, para que se possa posteriormente pesquisar as relações entre os IC de maneira padronizada. Deverá então a ferramenta possuir a capacidade de cadastro de tipos de relação. Cada tipo de IC deverá então ser configurado para possuir relações de determinado tipo com outros tipos de IC. Em tempo de criação dos itens de configuração, baseado em seu tipo, deverá ser possível criar as relações com outros itens de configuração, baseados nas relações possíveis para o seu tipo de IC.

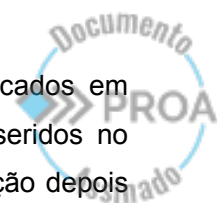
2.9.1.1.1.3.2. As relações deverão ser usadas nas análises de dependências e impactos realizadas pela ferramenta e posteriormente descritas neste documento. Deverão também ser usadas para identificar em tempo real os IC afetados pela falha de um outro determinado IC, isolando a causa raiz de uma falha detectada no ambiente. As relações deverão ser utilizadas também para simular os impactos que uma determinada mudança detectada pela ferramenta pode causar em outros elementos da infraestrutura de TI.

2.9.1.1.1.4. Grupos de Itens de Configuração:

2.9.1.1.1.4.1. Os tipos de Itens de Configuração deverão ser classificados em grupos que representam classes maiores em que tais tipos estão inseridos no universo de tipos itens de configuração possíveis. O item de configuração depois

**Av. João Pessoa, nº 2050, 3º andar, sala 480, Bairro Azenha, Porto Alegre/RS**  
**CEP: 90040-001 - Fone: 51 3288-2116**  
**E-mail: dtip-dae@pc.rs.gov.br**

4





**ESTADO DO RIO GRANDE DO SUL**  
**POLÍCIA CIVIL**  
**DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO POLICIAL**  
**DIVISÃO DE ACESSORAMENTO ESPECIAL**

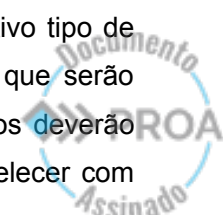
de criado deverá então ser inserido nos grupos cujo seu tipo participa. Tais grupos deverão ser usados para pesquisa, classificação, relatórios e filtros entre outras funcionalidades de extração de dados e listagem presentes no sistema.

2.9.1.1.2. Modelos de Itens de Configuração:

2.9.1.1.2.1. Todos os Itens de Configuração em uma CMDDB devem ser tipificados de acordo com sua classe, aqui tratado como Tipo de IC. Um tipo de Item de Configuração irá definir quais são seus atributos e seus relacionamentos válidos. A ferramenta deverá ter a capacidade de tipificar e padronizar os tipos de Itens de Configuração definindo modelos que deverão ser seguidos sempre que um IC de um determinado tipo for criado, regravando seus atributos quanto à obrigatoriedade de existir um valor associado ou não, do tipo de dado que será aceito como valor de um atributo específico e se o atributo terá um valor padrão ou não. Quanto às relações os modelos deverão definir quais tipos de relações um IC poderá ter com outros IC, baseados em seus tipos. Deverá também impor limites quanto ao número de relacionamentos que um IC de um determinado tipo pode ter com IC de outro determinado tipo. Quanto às relações de composição, quando um IC compõe outro ser significando que é um subcomponente do IC "Pai" a ferramenta deve regravar onde (dentro de quais outros tipos de IC) um determinado tipo de IC pode ser instanciado. A ferramenta deve impedir que Itens de Configuração sejam instanciados dentro (relação pai e filho) de outros IC de tipos que não podem ser compostos por aquele determinado tipo de IC, evitando assim erros de operação por parte do usuário.

2.9.1.1.2.1.1. Modelos nativos

2.9.1.1.2.1.1.1. A ferramenta deverá oferecer modelos nativos que contemplem o ambiente atual e previsto que irá gerenciar. Os modelos deverão possuir o nome do tipo de IC, os grupos de tipos de IC dos quais participarão os IC daquele tipo que forem instanciados na CMDDB, o conjunto de atributos e o respectivo tipo de dado que será aceito como valor para o atributo, os valores padrão que serão assumidos para cada atributo quando o IC for instanciado. Os modelos deverão também definir quais tipos de relação o IC daquele tipo poderá estabelecer com





**ESTADO DO RIO GRANDE DO SUL  
POLÍCIA CIVIL  
DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO POLICIAL  
DIVISÃO DE ACESSORAMENTO ESPECIAL**

outros IC além de definir os IC que poderão ser compostos por e que poderão compor o IC daquele tipo (relação pai e filho).

2.9.1.1.2.1.1.1.1.1. Modelos que deverão ser fornecidos nativamente junto com a ferramenta.

2.9.1.1.2.1.1.1.1.1.1. A ferramenta deverá fornecer os modelos de IC necessários, além de ser capaz de descobrir automaticamente, para o cadastro de todos os elementos das tecnologias utilizadas atualmente (e em um futuro breve) pela Companhia, sendo que cada elemento que compõe a Tecnologia deverá ser um Item de Configuração isolado com seus respectivos atributos e relações. As tecnologias utilizadas atualmente pela Companhia são:

**2.9.1.1.2.1.1.1.1.1.1. Hardwares:**

2.9.1.1.2.1.1.1.1.1.1.1. Servidores.

2.9.1.1.2.1.1.1.1.1.1.2. Storages.

2.9.1.1.2.1.1.1.1.1.1.3. Robôs de Backup.

2.9.1.1.2.1.1.1.1.1.1.4. Switches e Access Points.

2.9.1.1.2.1.1.1.1.1.1.5. Roteadores.

2.9.1.1.2.1.1.1.1.1.1.6. Impressoras

**2.9.1.1.2.1.1.1.1.1.2. Sistemas operacionais e seus subcomponentes:**

2.9.1.1.2.1.1.1.1.1.2.1. Linux.

2.9.1.1.2.1.1.1.1.1.2.2. Microsoft.

2.9.1.1.2.1.1.1.1.1.2.3. Unix.

**2.9.1.1.2.1.1.1.1.1.3. Banco de dados e suas databases:**

2.9.1.1.2.1.1.1.1.1.3.1. Microsoft SQL Server.

2.9.1.1.2.1.1.1.1.1.3.2. Oracle.

2.9.1.1.2.1.1.1.1.1.3.3. MySQL.

2.9.1.1.2.1.1.1.1.1.3.4. PostgreSQL.

**Av. João Pessoa, nº 2050, 3º andar, sala 480, Bairro Azenha, Porto Alegre/RS  
CEP: 90040-001 - Fone: 51 3288-2116  
E-mail: dtip-dae@pc.rs.gov.br**





**ESTADO DO RIO GRANDE DO SUL  
POLÍCIA CIVIL  
DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO POLICIAL  
DIVISÃO DE ACESSORAMENTO ESPECIAL**

**2.9.1.1.2.1.1.1.1.1.4. Servidores de aplicação:**

2.9.1.1.2.1.1.1.1.1.4.1. Java.

2.9.1.1.2.1.1.1.1.1.4.2. .NET.

2.9.1.1.2.1.1.1.1.1.4.3. PHP.

2.9.1.1.2.1.1.1.1.1.4.4. Outros.

**2.9.1.1.2.1.1.1.1.1.5. Aplicações antivírus.**

**2.9.1.1.2.1.1.1.1.1.6. Sistemas de backup.**

**2.9.1.1.2.1.1.1.1.1.7. Servidores de e-mail e colaboração.**

**2.9.1.1.2.1.1.1.1.1.8. Containers e orquestração:**

2.9.1.1.2.1.1.1.1.1.8.1. Docker

2.9.1.1.2.1.1.1.1.1.8.2. Docker Swarm

2.9.1.1.2.1.1.1.1.1.8.3. Kubernetes

2.9.1.1.2.1.2. Modelos customizados

2.9.1.1.2.1.2.1. Além dos modelos nativos, os usuários da ferramenta deverão ser capazes de definir seus próprios modelos, com as mesmas características dos modelos nativos. Deverá ser possível utilizar tais modelos customizados para padronizar a criação de IC de mesmo tipo.

2.9.1.1.2.1.3. Integrações

2.9.1.1.2.1.3.1. Deverão ser oferecidos webservices para interação com a CMDB bem como um Pacote de Desenvolvimento de Software (SDK) de integração com os devidos manuais para que qualquer interessado possa integrar suas ferramentas com a CMDB.

2.9.1.1.2.1.3.2. Deverão ser fornecidos os seguintes serviços mínimos para interação com a CMDB:

2.9.1.1.2.1.3.2.1. Criação de IC.

2.9.1.1.2.1.3.2.2. Remoção de IC.

**Av. João Pessoa, nº 2050, 3º andar, sala 480, Bairro Azenha, Porto Alegre/RS  
CEP: 90040-001 - Fone: 51 3288-2116  
E-mail: dtip-dae@pc.rs.gov.br**







**ESTADO DO RIO GRANDE DO SUL**  
**POLÍCIA CIVIL**  
**DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO POLICIAL**  
**DIVISÃO DE ACESSORAMENTO ESPECIAL**

2.9.1.1.2.1.3.2.3. Alteração de Valores de Atributo de IC.

2.9.1.1.2.1.3.2.4. Listagem de IC:

2.9.1.1.2.1.3.2.4.1. Por tipo.

2.9.1.1.2.1.3.2.4.2. Filtrando valor de atributo.

2.9.1.1.2.1.3.2.4.3. Por relações com outros IC.

2.9.1.1.2.1.3.2.4.4. Por composição.

2.9.1.1.2.1.4. Discovery

2.9.1.1.2.1.4.1. A ferramenta deverá ter a capacidade de descobrir Itens de Configuração automaticamente através de processos de varredura que irão automaticamente cadastrar devidamente classificados e com os atributos essenciais os IC na CMDB. O processo de Discovery deverá ser capaz de detectar e de cadastrar na CMDB no mínimo os seguintes tipos de Itens de Configuração:

2.9.1.1.2.1.4.1.1. Discovery de Hosts

2.9.1.1.2.1.4.1.1.1. Hosts são quaisquer dispositivos físicos ou virtuais que se comunicam na rede por protocolo IP. Tais elementos deverão ser detectados e seu modelo de Hardware e de Sistema operacional deverão ser identificados pela ferramenta e vinculados a um tipo de IC válido da CMDB. Deverão também ser identificados de IP e nome DNS (Domain Name System) pelo qual se comunica na rede.

2.9.1.1.2.1.4.1.1.2. A ferramenta deverá reconhecer hosts de duas estruturas diferentes quanto ao número de Itens de Configuração que o compõe: podem ser simples tendo Sistema Operacional embarcado no dispositivo, sendo indivisível para fins de funcionamento (por exemplo: Storages, Switches e Roteadores) ou podem ser compostos, recebendo um sistema operacional de diferente fabricante (por exemplo Servidores físicos e Virtuais). Hosts simples poderão ser identificados apenas com um Item de Configuração enquanto Hosts compostos deverão resultar em dois Itens de Configuração distintos na CMDB e suas configurações (Atributos) deverão ser identificados no Dispositivo (hardware ou virtual) ou no Sistema Operacional de forma adequada, conforme de fato o item é.

**Av. João Pessoa, nº 2050, 3º andar, sala 480, Bairro Azenha, Porto Alegre/RS**  
**CEP: 90040-001 - Fone: 51 3288-2116**  
**E-mail: dtip-dae@pc.rs.gov.br**

8





**ESTADO DO RIO GRANDE DO SUL**  
**POLÍCIA CIVIL**  
**DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO POLICIAL**  
**DIVISÃO DE ACESSORAMENTO ESPECIAL**

O Discovery deverá ser capaz de identificar tanto os Dispositivos quanto os Sistemas Operacionais dos hosts descobertos e sugerir aos usuários da ferramenta que o aceitem na CMDB. Apenas os hosts aceitos por ao menos um usuário da ferramenta deverá de fato ser cadastrado na CMDB.

2.9.1.1.2.1.4.1.1.3. Os hosts deverão ser descobertos no mínimo pelos seguintes métodos:

2.9.1.1.2.1.4.1.1.3.1. Baseados no Microsoft Active Directory: A ferramenta deve detectar os hosts que estão cadastrados no Active Directory e realizar checagens para confirmar sua existência e atividade na rede. Quando confirmada a existência de tal Host deverá enviá-lo para a confirmação do usuário antes da importação.

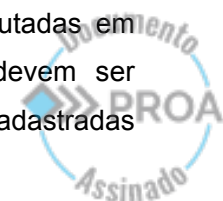
2.9.1.1.2.1.4.1.1.3.2. Baseados em protocolo SNMP: A ferramenta deverá ser capaz de varrer redes (segmentos de rede IP) informadas pelos usuários da ferramenta a fim de encontrar hosts via protocolo SNMP. Os usuários deverão por informar, para cada rede ip, quais são as possíveis comunidades SNMP usadas para a varredura. Após encontrar e confirmar a atividade do Host ele deve ser enviado para aprovação de um usuário da ferramenta antes de ser cadastrado na CMDB.

2.9.1.1.2.1.4.1.1.3.3. Por varredura de Rede: Deverão ser realizadas varreduras de rede que consistem em identificar por protocolos ICMP, TCP e UDP se há respostas em algum dos IP das subredes definidas pelos usuários da ferramenta. A ferramenta deverá checar cada IP e cada porta TCP e UDP para identificar hosts ativos, deverá resolver seu nome DNS e identificar modelo de Hardware e de Sistema Operacional sempre que possível para então enviar aos usuários da ferramenta para aprovação e cadastro na CMDB.

2.9.1.1.2.1.4.1.1.4. Através de APIs fornecidas pelo fabricante do Hypervisor: Deverá haver a possibilidade de realizar Discovery via API disponibilizadas por Microsoft e VMware para listagem de máquinas virtuais sendo executadas em seus Hipervisors (Hyper-V e VMware). As máquinas detectadas devem ser sugeridas aos usuários da ferramenta e quando aceitas deverão ser cadastradas na CMDB.

**Av. João Pessoa, nº 2050, 3º andar, sala 480, Bairro Azenha, Porto Alegre/RS**  
**CEP: 90040-001 - Fone: 51 3288-2116**  
**E-mail: dtip-dae@pc.rs.gov.br**

9





**ESTADO DO RIO GRANDE DO SUL**  
**POLÍCIA CIVIL**  
**DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO POLICIAL**  
**DIVISÃO DE ACESSORAMENTO ESPECIAL**

2.9.1.1.2.1.4.1.1.4.1. Quando um host for reportado por um dos mecanismos de Discovery, a ferramenta deverá realizar as checagens necessárias para garantir que já não foi reportado por um dos outros mecanismos. Quando um host for importado, ele também deverá ser ignorado caso seja reportado novamente pelo mesmo ou por outro mecanismo.

2.9.1.1.2.1.4.1.2.2. Para Servidores:

2.9.1.1.2.1.4.1.2.2.1. Dispositivos de Hardware:

2.9.1.1.2.1.4.1.2.2.1.1. Discos: Unidades de disco físico e virtuais montados os gerenciados pelo sistema operacional.

2.9.1.1.2.1.4.1.2.2.1.2. Unidades de Armazenamento de dados: Identificadas por letras em sistemas operacionais Windows e pontos de montagem em Sistemas operacionais Unix/Linux.

2.9.1.1.2.1.4.1.2.2.1.3. Placas de Rede: Qualquer tipo de interface de comunicação em rede instalada no servidor.

2.9.1.1.2.1.4.1.2.2.1.4. Impressoras: Dispositivos de impressão configurados no servidor.

2.9.1.1.2.1.4.1.2.2.2. Funcionalidades Nativas do Sistema Operacional e seus subcomponentes:

2.9.1.1.2.1.4.1.2.2.2.1. As funcionalidades nativas do sistema operacional consistem em serviços que são partes da distribuição oficial (por parte do fabricante ou mantenedor oficial do sistema) do sistema operacional e que podem ser habilitadas ou desabilitadas conforme necessidade do usuário. Tais serviços podem ainda ser compostos por elementos filhos que podem ser instanciados uma vez ou múltiplas vezes a fim de criar configurar o serviço, uma instância do serviço ou ainda uma instância de algum elemento que o serviço mantém o funcionamento. Assim sendo cada elemento, serviços e subcomponentes devem ser tratados como Itens de Configuração individuais pois são de fato elementos relacionados, mas independentes um do outro.

2.9.1.1.2.1.4.1.2.2.3. Softwares Instalados e seus subcomponentes:

**Av. João Pessoa, nº 2050, 3º andar, sala 480, Bairro Azenha, Porto Alegre/RS**  
**CEP: 90040-001 - Fone: 51 3288-2116**  
**E-mail: dtip-dae@pc.rs.gov.br**

10





**ESTADO DO RIO GRANDE DO SUL**  
**POLÍCIA CIVIL**  
**DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO POLICIAL**  
**DIVISÃO DE ACESSORAMENTO ESPECIAL**

2.9.1.1.2.1.4.1.2.2.3.1. Softwares instalados podem ser quaisquer softwares que o usuário decida instalar sobre o sistema operacional. Assim como as Funcionalidades Nativas do SO os softwares podem ter subcomponentes que podem ser instanciados e que são mantidos pelo software instalado. Tais elementos deverão ser tratados como Itens de Configuração separados do Software em si para fins de manter a estrutura correta de IC e permitir a correta relação de dependência no nível de granularidade desejado.

2.9.1.1.2.1.4.1.2.2.4. Serviços:

2.9.1.1.2.1.4.1.2.2.4.1. São processos mantidos pelo sistema operacional de forma padronizada para que sejam inicializados, finalizados e gerenciados pelo sistema operacional de uma forma homogênea. Os serviços deverão ser detectados pelo Discovery e inseridos na CMDB.

2.9.1.1.2.1.4.1.2.2.4.2. Para Storages:

2.9.1.1.2.1.4.1.2.2.4.2.1. Discos.

2.9.1.1.2.1.4.1.2.2.4.2.2. Qualquer elemento de hardware ou software usado para organizar discos.

2.9.1.1.2.1.4.1.2.2.4.2.3. Grupos de Disco, seja como for a nomenclatura usada pelo fabricante.

2.9.1.1.2.1.4.1.2.2.4.2.4. LUN.

2.9.1.1.2.1.4.1.2.2.4.3. Para Switches:

2.9.1.1.2.1.4.1.2.2.4.3.1. Portas de Rede de qualquer tipo.

2.9.1.1.2.1.4.1.2.2.4.3.2. VLAN.

2.9.1.1.2.1.4.1.2.2.4.4. Para Roteadores

2.9.1.1.2.1.4.1.2.2.4.4.1. Interface de rede de qualquer tipo.

2.9.1.1.2.1.4.1.2.3. Cada Item de Configuração encontrado poderá possuir ou não outros Itens de configuração que o compõe. Um serviço de DNS por exemplo pode ser composto por Zonas DNS. O Processo de Discovery deverá ser capaz de descobrir a árvore de IC do Host e apresentar os resultados do processo nível a

**Av. João Pessoa, nº 2050, 3º andar, sala 480, Bairro Azenha, Porto Alegre/RS**  
**CEP: 90040-001 - Fone: 51 3288-2116**  
**E-mail: dtip-dae@pc.rs.gov.br**

11



**ESTADO DO RIO GRANDE DO SUL**  
**POLÍCIA CIVIL**  
**DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO POLICIAL**  
**DIVISÃO DE ACESSORAMENTO ESPECIAL**

nível. Quando um IC pai for aceito e importado pelo usuário, deverão então ser apresentados os resultados da busca dos filhos o IC importado. Tais descobertas deverão estar de acordo com os modelos de IC nativos ou customizados cadastrados na ferramenta conforme as especificações definidas anteriormente neste documento.

2.9.1.1.2.1.4.1.2.3.1. Tratamento das Descobertas de IC

2.9.1.1.2.1.4.1.2.3.1.1. Os Itens de Configuração descobertos deverão cadastrados na ferramenta e o usuário deverá poder optar, em tempo de configuração da ferramenta, por dois modos de inserção na CMDB: Manual e Automático.

2.9.1.1.2.1.4.1.2.3.1.1.1. O modo de inserção manual deverá oferecer ao usuário a opção de decidir IC por IC se ele deve ou não ser inserido na CMDB.

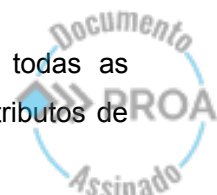
2.9.1.1.2.1.4.1.2.4. Discovery de Relações entre os Itens de Configuração

2.9.1.1.2.1.4.1.2.4.1. A ferramenta deverá ser capaz de descobrir e cadastrar na CMDB automaticamente as relações entre os Itens de Configuração tais quais são apresentadas no ambiente de TI. Desta forma, se um IC depender de ou se relacionar com outro IC do ambiente, uma relação do tipo adequado deverá ser criada entre os dois IC na CMDB. Se tal relação deixar de ser verdadeira, a ferramenta deve então apagar tal relação. A detecção de relações deve ser realizada sempre que as configurações dos IC permitirem, ou seja, se tal relação pode ser detectada pelas configurações do IC no ambiente, então tal relação deve ser detectada.

2.9.1.1.2.1.4.1.2.4.2. A detecção de relações deve ser realizada sempre que as configurações dos IC permitirem, ou seja, se tal relação pode ser detectada pelas configurações do IC no ambiente, então tal relação deve ser detectada.

2.9.1.1.2.1.4.1.2.4.2.1. Operação da CMDB

2.9.1.1.2.1.4.1.2.4.2.1.1. Por Operação da CMDB deve-se entender todas as ações que visam criar, editar, excluir ou manipular as relações e os atributos de





**ESTADO DO RIO GRANDE DO SUL**  
**POLÍCIA CIVIL**  
**DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO POLICIAL**  
**DIVISÃO DE ACESSORAMENTO ESPECIAL**

um IC manualmente, sem o auxílio do Discovery ou de auditoria de configuração, visto mais adiante neste documento.

#### 2.9.1.1.2.1.4.1.2.5. Criação de Itens de Configuração

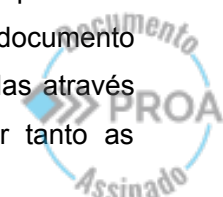
2.9.1.1.2.1.4.1.2.5.1. A ferramenta deverá oferecer ao usuário uma interface simples para criação de Itens de Configuração de forma manual, quando o Discovery não for capaz de detectar um elemento no ambiente de TI. Deverá ser possível criar Itens de Configuração de tipos nativos, que possuem modelo nativo cadastrado na ferramenta, ou IC de tipo customizado, que são tipos criados pelos próprios usuários da ferramenta.

2.9.1.1.2.1.4.1.2.5.2. A ferramenta deverá ter a capacidade de controlar onde um Item de Configuração pode ser criado de acordo com as relações que pode possuir, realizando assim um controle lógico que impede o usuário de criar um Item de Configuração dentro de outro que não pode, na prática, ser composto pelo tipo de IC que se está desejando criar. As relações possíveis de um determinado IC deve ser baseado no modelo nativo que define seu tipo. Itens de Configuração customizados podem possuir relações customizadas de acordo com as necessidades do usuário.

2.9.1.1.2.1.4.1.2.5.3. Ao criar um Item de Configuração, novamente baseado no modelo do tipo a ser criado, a ferramenta deve exigir o preenchimento de Atributos obrigatórios cuja obrigatoriedade fora definida em seu modelo (tipo de IC). Deverá também apresentar os atributos opcionais para que o usuário preencha os valores desses atributos em tempo de criação do IC.

#### 2.9.1.1.2.1.4.1.2.6. Edição de Itens de Configuração

2.9.1.1.2.1.4.1.2.6.1. A ferramenta deverá permitir a edição dos atributos dos itens de configuração conforme desejo do usuário. Sempre que um atributo for alterado, a ferramenta deverá criar um registro (log) para que se possa acompanhar a evolução das mudanças e como elas ocorreram. Posteriormente neste documento será definido como as mudanças nos atributos poderão ser manipuladas através da auditoria de configurações. O log de mudanças deverá registrar tanto as





**ESTADO DO RIO GRANDE DO SUL**  
**POLÍCIA CIVIL**  
**DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO POLICIAL**  
**DIVISÃO DE ACESSORAMENTO ESPECIAL**

mudanças detectadas no ambiente através da auditoria como as mudanças realizadas por um usuário, manualmente.

2.9.1.1.2.1.4.1.2.7. Exclusão de Itens de Configuração

2.9.1.1.2.1.4.1.2.7.1. A ferramenta deverá permitir que o usuário exclua Itens de Configuração da CMDB, porém gerando registros em Log para que fique registrada a sua deleção. Quando um Being pai (relação de composição) for excluído a ferramenta deverá excluir seus Itens de Configuração filhos registrando os logs para futura consulta.

2.9.1.1.2.1.4.1.2.8. Criação de relações entre os itens de configuração

2.9.1.1.2.1.4.1.2.8.1. A ferramenta deverá permitir a criação manual, além da criação por Discovery conforme já definido anteriormente, de relações entre os Itens de Configuração, respeitando o que foi definido no Tipo do Item de Configuração que se está desejando criar.

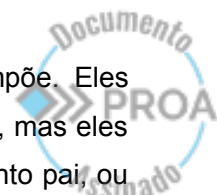
2.9.1.1.2.1.4.1.2.9. Apresentação dos Dados da CMDB

2.9.1.1.2.1.4.1.2.9.1. Os dados da CMDB deverão ser apresentados aos usuários através de uma interface que sirva como uma documentação do ambiente de TI. Esta interface deve permitir a exibição dos Itens de Configuração, seus atributos e relações a fim de servir de fonte de informação aos interessados em entender, administrar e planejar o ambiente.

2.9.1.1.2.1.4.1.2.10. Itens de Configuração e sua composição

2.9.1.1.2.1.4.1.2.10.1. Os usuários que tiverem acesso à ferramenta deverão poder compreender quais são os dispositivos e quais elementos (IC) estão em funcionamento e dependem de cada dispositivo. A exibição dos IC deverá ser apresentada de forma que o cada Item de Configuração seja exibido dentro do Item de Configuração que ele compõe, sendo que Itens de Configuração que nada compõe serão tratados nesse documento como IC Raiz.

2.9.1.1.2.1.4.1.2.10.2. Os IC raízes são os elementos que nada compõe. Eles podem depender ou até ser montados em outros Itens de Configuração, mas eles representam unidades autônomas que podem funcionar sem um elemento pai, ou





**ESTADO DO RIO GRANDE DO SUL**  
**POLÍCIA CIVIL**  
**DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO POLICIAL**  
**DIVISÃO DE ACESSORAMENTO ESPECIAL**

um elemento que devem compor. Para melhor entendimento podemos citar um servidor de rede (hardware). Ele é um item de configuração que funciona independentemente de um outro elemento. Ele precisa ser montado em um Rack e precisa de energia elétrica para funcionar, mas ele não compõe o Rack e tão pouco o Nobreak nos quais estar ligado apesar de depender de ambos para funcionar. Por sua vez o Nobreak e o Rack são outros Itens de Configuração raiz. Eles estão dentro de uma sala, porém podem ser movidos a outra sala, criando uma dependência deste objeto, mas são autônomos em relação a sala. Este conceito define o que é uma relação de composição. Serviço que roda em um servidor compõe um sistema operacional que por sua vez compõe um servidor (hardware) que por sua vez é o Item de Configuração raiz, que não compõe outro IC.

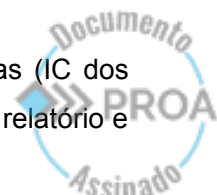
2.9.1.1.2.1.4.1.2.10.3. Definidos estes conceitos, a ferramenta deverá então apresentar o conteúdo da CMDB de forma que se compreenda facilmente através da interface de usuários quais são os Itens de Configuração Raiz e quais outros elementos o compõe. Internamente um elemento raiz possui também estruturas de composição que formam uma árvore de composição. A interface deve permitir a compreensão dessas estruturas de composição de uma forma intuitiva.

2.9.1.1.2.1.4.1.2.11. Itens de Configuração e suas relações

2.9.1.1.2.1.4.1.2.11.1. Além das relações de composição os Itens de Configuração podem ter entre si diversos tipos de relações. Podem estar ligados física ou logicamente por relações de diversos tipos.

2.9.1.1.2.1.4.1.2.11.2. A ferramenta deverá possibilitar a exibição das relações de um Item de Configuração e se a relação representa uma dependência de funcionamento entre os IC. Deverá também apresentar graficamente as relações de um IC, em tela navegável onde o usuário possa expandir as relações de dependência do IC e dos IC com os quais está relacionado.

2.9.1.1.2.1.4.1.2.11.3. A ferramenta deverá apresentar as Dependências (IC dos quais depende) e os Impactos (IC que podem ser afetados), em formato relatório e







**ESTADO DO RIO GRANDE DO SUL**  
**POLÍCIA CIVIL**  
**DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO POLICIAL**  
**DIVISÃO DE ACESSORAMENTO ESPECIAL**

em gráfico interativo onde o usuário pode expandir a árvore de dependências e impactos de um determinado Item de Configuração.

2.9.1.1.2.1.4.1.2.11.4. Os usuários da ferramenta devem ter a possibilidade de simular impactos para cada item de configuração do ambiente. A ferramenta deve apresentar uma lista e um desenho contendo os IC impactados. Essas conclusões deverão ser baseadas nas relações de dependência criadas durante o processo de Discovery ou da criação manual de relações de dependência.

2.9.1.1.2.1.4.1.2.11.5. Além da simulação de impactos deve ser possível também a simulação de dependências de um determinado IC. A ferramenta deve apresentar uma lista e um desenho contendo os IC e quais IC do ambiente dependem seu funcionamento. Essas conclusões deverão ser baseadas nas relações de dependência criadas durante o processo de documentação.

2.9.1.1.2.1.4.1.2.11.6. Deve ser possível identificar em qual horário um elemento do ambiente deve estar ativo e quando ele pode ser desativado, baseado no cronograma das relações que representam uma dependência. Para isso, a ferramenta deve realizar uma análise de impactos e identificar os cronogramas atribuídos aos processos de negócio suportados em qualquer nível pelo elemento em questão, montando um cronograma de uso do elemento baseado nas relações.

2.9.1.1.2.1.4.1.2.12. Relatórios

2.9.1.1.2.1.4.1.2.12.1. A ferramenta deverá permitir que os usuários extraiam dados da CMDB por meio de relatórios. Deverá ser possível extrair relatórios no mínimo nos formatos: PDF, Microsoft Word, TXT e HTML.

2.9.1.1.2.1.4.1.2.12.2. A ferramenta deverá possibilitar a confecção de relatórios customizados, oferecendo um método padrão de desenvolvimento e publicação que permita a personalização de acordo com as necessidades da Companhia.

2.9.1.1.2.1.4.1.2.12.3. Deverá também oferecer relatórios prontos, acessíveis através da interface da ferramenta em cada Item de Configuração, de acordo com o seu tipo e que apresentem as informações relevantes para cada tipo de IC.

**Av. João Pessoa, nº 2050, 3º andar, sala 480, Bairro Azenha, Porto Alegre/RS**  
**CEP: 90040-001 - Fone: 51 3288-2116**  
**E-mail: dtip-dae@pc.rs.gov.br**

16





**ESTADO DO RIO GRANDE DO SUL**  
**POLÍCIA CIVIL**  
**DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO POLICIAL**  
**DIVISÃO DE ACESSORAMENTO ESPECIAL**

2.9.1.1.2.1.4.1.2.13. Procedimentos de Manutenção dos Itens de Configuração

2.9.1.1.2.1.4.1.2.13.1. A solução deverá permitir a documentação de procedimentos de manutenção de cada Item de Configuração, armazenando o passo-a-passo para cada procedimento necessário.

2.9.1.1.2.1.4.1.2.13.2. Deve ser possível atribuir uma agenda para cada um dos procedimentos caso o procedimento seja algo a ser executado como uma rotina.

2.9.1.1.2.1.4.1.2.13.3. A agenda de cada IC deverá alimentar uma agenda centralizada de manutenção, onde os usuários da ferramenta poderão ver a agenda de manutenção de todo o ambiente, podendo os usuários ter uma visão mensal, semanal e diária de suas tarefas.

2.9.1.1.2.1.4.1.2.13.4. O usuário deverá poder, a partir da agenda de manutenção, marcar cada um dos procedimentos como executado, para que tenha uma visão precisa das atividades que ainda não foram executadas.

2.10. Gerenciamento de Serviços, Configurações e de Mudanças.

2.10.1. A ferramenta deverá ter a capacidade de descobrir e armazenar as informações a respeito dos serviços mantidos e oferecidos aos usuários e suas configurações, e a capacidade de identificar as mudanças ocorridas nos serviços ou em toda a cadeia de dependência (Itens de Configuração) que mantém o serviço em funcionamento.

2.10.2. Os serviços nada mais são que recursos de TI consumidos por qualquer usuário interno ou externo e que deve ser mantido em funcionamento, podendo ser um hardware ou software. As dependências dos serviços são os Itens de Configuração que sustentam o funcionamento do serviço.

2.10.3. Uma configuração por sua vez é qualquer atributo de um Item de Configuração que influencia em seu funcionamento. Os atributos de um IC podem também ser meramente descritivos.

2.10.3.1. Quanto à Gerência de Serviços e Configurações a ferramenta deve seguir as seguintes definições:



**Av. João Pessoa, nº 2050, 3º andar, sala 480, Bairro Azenha, Porto Alegre/RS**  
**CEP: 90040-001 - Fone: 51 3288-2116**  
**E-mail: dtip-dae@pc.rs.gov.br**

17



**ESTADO DO RIO GRANDE DO SUL**  
**POLÍCIA CIVIL**  
**DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO POLICIAL**  
**DIVISÃO DE ACESSORAMENTO ESPECIAL**

2.10.3.1.1. Cada Item de Configuração possui diferentes configurações, dependendo do seu tipo. Cada tipo de IC deve ser modelado antes de ser instanciado na CMDB, conforme descrito anteriormente neste documento, podendo ser um modelo Nativo ou modelo Personalizado pelos usuários das ferramentas. Quando um IC é instanciado na CMDB, a ferramenta deverá manter a documentação de suas configurações.

2.10.3.1.2. A ferramenta deverá ser capaz de coletar o valor de cada configuração dos IC no ambiente de TI e manter o valor para cada configuração sincronizada com a CMDB.

2.10.3.1.3. Deverá ser mantido o histórico de mudanças das configurações e possibilitar a consulta deste histórico por IC em suas composições ou suas dependências, apresentando as mudanças encontradas em ordem de tempo.

#### 2.10.3.2. Gerencia de Mudanças

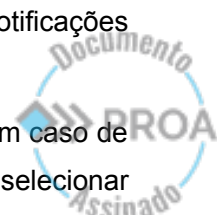
2.10.3.2.1. A ferramenta deve detectar mudanças nas configurações do ambiente de TI e oferecer aos usuários a opção de gerar alertas às equipes adequadas quando ocorrer eventos dessa natureza considerando as seguintes definições:

2.10.3.2.1.1. A ferramenta deverá gerar alertas na interface, aos usuários responsáveis apresentando o Item de Configuração alterado, a configuração alterada, o horário em que a alteração foi detectada, os valores antigo e o novo da configuração.

2.10.3.2.1.2. O alerta deverá ser tratado como um ticket, organizado por Item de Configuração e deverá possibilitar que os usuários alertados aprovelem a mudança ou a selecionem para execução de Rollback, realizando o controle da configuração até sua reversão e aprovação por parte do usuário.

2.10.3.2.1.3. O alerta deverá ser enviado aos responsáveis pelos seguintes canais de comunicação: tela da aplicação, e-mail e aplicativo de celular via notificações para as plataformas IOS e Android.

2.10.3.2.1.4. A seleção de equipe que receberá o alerta de notificação em caso de mudança deverá ser feita por item de configuração, sendo possível selecionar





**ESTADO DO RIO GRANDE DO SUL**  
**POLÍCIA CIVIL**  
**DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO POLICIAL**  
**DIVISÃO DE ACESSORAMENTO ESPECIAL**

diferentes equipes para cada item de configuração especificamente ou usando uma das formas abaixo:

2.10.3.2.1.4.1. Tipo do Item de Configuração: Caso não tenha sido definido uma equipe responsável por receber a notificação especificamente para um Item de Configuração deverá ser possível selecionar e enviar a notificação para equipes responsável pelo tipo do item em questão.

2.10.3.2.1.4.2. Tipo dos Itens de Configuração pai: Caso não tenha sido definido um responsável pelo IC especificamente e tão pouco para seu tipo a aplicação deve verificar se há disponível um responsável pelo IC pai ou pelo tipo do IC pai, verificando todos os IC até encontrar o IC raiz até encontrar uma equipe para enviar a notificação.

2.10.3.2.1.4.3. Quando não for possível encontrar uma equipe para envio da notificação pelos métodos anteriores a ferramenta deverá enviar a uma equipe padrão, responsável em último caso a tratar o alerta de mudança.

2.10.3.2.1.4.4. Para cada um dos métodos acima, deve ser ainda possível selecionar uma equipe para cada Site da companhia, definindo assim equipes específicas responsáveis por reagir aos eventos de mudança para cada localidade.

## 2.11. Gerenciamento de Eventos

2.11.1. A ferramenta deverá ser capaz de gerenciar eventos relacionados aos aspectos de capacidade e de disponibilidade ocorridos no ambiente, configurando as ferramentas que irão coletar os eventos no ambiente com os devidos KPI, recebendo os eventos do ambiente e realizando a sua classificação e direcionando para a equipe responsável pelo tratamento do evento.

2.11.1.1. Configuração da Ferramenta de Gestão de Capacidade e Disponibilidade.

2.11.1.1.1. A ferramenta deverá manter, associado aos modelos (Tipos de Itens de Configuração), uma lista de Indicadores Chave de Performance (KPI) que definem





**ESTADO DO RIO GRANDE DO SUL**  
**POLÍCIA CIVIL**  
**DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO POLICIAL**  
**DIVISÃO DE ACESSORAMENTO ESPECIAL**

quais são os contadores relevantes para cada tipo de IC em relação às matérias de Gerenciamento de Disponibilidade e de Capacidade.

2.11.1.1.2. Quando instanciado um Item de Configuração na CMDDB, seja por processo de Discovery como por cadastro manual, a ferramenta deverá ser capaz de criar o Item de Configuração e os KPI relacionados na ferramenta de monitoramento Sistema de Monitoramento (atualmente utilizada pela Companhia), configurando-a automaticamente e eliminando a necessidade de configuração manual desta ferramenta. Após criados os IC e os KPI, a ferramenta deverá manter sincronizada a configuração refletindo as alterações realizadas na CMDDB e realizando a remoção quando necessário.

2.11.1.1.3. Caso a ferramenta não possua essa integração nativamente, será concedido um prazo de 60 dias para a integração via webservices do fabricante da ferramenta.

2.11.1.2. Webservices de Integração com ferramentas de Gestão de Capacidade e Disponibilidade.

2.12. Com a finalidade de garantir a liberdade de troca da atual ferramenta de Gestão de Capacidade e Disponibilidade e garantir futuras integrações e a continuidade dos trabalhos independentemente do software que venha ser adotado futuramente pela Companhia, a ferramenta deverá oferecer Webservices com todas as funcionalidades que garantam a sincronização com tais ferramentas permitindo a criação de IC, seus KPI e a total configuração das ferramentas mantendo todas as funcionalidades descritas anteriormente neste documento caso o software de monitoramento seja substituído. O serviço de desenvolvimento dos artefatos de software que realizarão tal integração não fazem parte do escopo deste edital, no entanto todas as funcionalidades descritas aqui deverão ser mantidas viáveis após a substituição, caso ela ocorra.

### 3. SISTEMA DE MONITORAMENTO

3.1. O Sistema de Monitoramento deve atender os seguintes requisitos:

**Av. João Pessoa, nº 2050, 3º andar, sala 480, Bairro Azenha, Porto Alegre/RS**  
**CEP: 90040-001 - Fone: 51 3288-2116**  
**E-mail: dtip-dae@pc.rs.gov.br**



20



**ESTADO DO RIO GRANDE DO SUL**  
**POLÍCIA CIVIL**  
**DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO POLICIAL**  
**DIVISÃO DE ACESSORAMENTO ESPECIAL**

- 3.1.1. Permitir ser instalada em ambientes de alta disponibilidade.
- 3.1.2. Capacidade de monitorar sistemas sem utilizar agente.
- 3.1.3. Monitorar serviços de rede tais como: SMTP, POP3, HTTP, SNMP, NNTP, PING, etc.
- 3.1.4. Mostrar de forma gráfica os mapas das redes WAN.
- 3.1.5. Gerar notificações para a lista de contatos, quando ocorrerem problemas em serviços ou servidores e sua resolução.
- 3.1.6. Possuir interface WEB para visualização do 'status' atual da rede, notificações, histórico de problemas, relatórios, arquivos de log, etc.
- 3.1.7. Coletar e enviar alarmes críticos para contas de e-mail e números de celulares pré-definidos.
- 3.1.8. Coletar indicadores de disponibilidade: MTTF, (Mean Time to Failure - Média de tempo estimada para ocorrer à próxima falha ou perda do serviço), MTTR (Mean Time to Repair - Média do tempo requerida para resolver os problemas relacionados à falha), MTBR (Mean Time Between Failures - Tempo médio entre falhas), Total (Tempo total de indisponibilidade de todos os servidores).
- 3.1.9. Gerar Gráficos de Capacity Planning dos Servidores, com curvas de carga máxima e mínima, processos em fila esperando processamento, consumo máximo e mínimo de memória por servidor, número máximo e mínimo de usuários conectados ao servidor.
- 3.2. A CONTRATANTE poderá solicitar que seja apresentado/monitorado qualquer serviço/equipamento relativo ao serviço de monitoramento.
- 3.3. A solução de monitoração deve incluir o fornecimento de *softwares* de monitoração e sistemas de distribuição de sinal de vídeo para dispositivos de TVs/Painéis a serem fornecidos pela CONTRATANTE, com especificações definidas em comum acordo com a CONTRATANTE.
- 3.4. O *software* de monitoramento deverá atender, no mínimo, as seguintes funcionalidades:

**Av. João Pessoa, nº 2050, 3º andar, sala 480, Bairro Azenha, Porto Alegre/RS**  
**CEP: 90040-001 - Fone: 51 3288-2116**  
**E-mail: dtip-dae@pc.rs.gov.br**

21





**ESTADO DO RIO GRANDE DO SUL**  
**POLÍCIA CIVIL**  
**DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO POLICIAL**  
**DIVISÃO DE ACESSORAMENTO ESPECIAL**

**3.4.1. Alertas e Escalação:**

3.4.1.1. A solução deverá permitir notificações, eventos e alertas configurados a partir das regras da operação pelos seguintes meios: e-mail (correio eletrônico), SMS (através de modem GSM ou via *gateway*), interface com sistemas de *Help Desk/Service Desk* e mensagens instantâneas.

3.4.1.2. Prover a capacidade de utilizar diferentes níveis de severidade ou urgência dos alarmes (ex. Crítico, Informação, etc.).

3.4.1.3. A solução deve ter eventos com severidades previamente configurados para diversos tipos de monitoração.

3.4.1.4. A solução deve permitir alterar a severidade de texto dos eventos já existentes na monitoração.

3.4.1.5. A solução deve permitir criar eventos definindo o texto e severidade.

3.4.1.6. A solução deve permitir que eventos e/ou alarmes sejam escalados, reiniciados, e/ou suprimidos baseado em critérios múltiplos como fonte, conteúdo, horário ou outros itens que sejam obtidos pela monitoração.

3.4.1.7. A solução deve suportar *baseline* de métricas de desempenho coletadas, permitindo alertas inteligentes com os indicadores críticos de sistemas e aplicações.

3.4.1.8. A solução deve permitir criar regra de correlação de eventos para a geração de alarmes.

3.4.1.9. A solução deve ter portal web com informações gráficas contendo o status, alarmes e métricas dos sistemas monitorados.

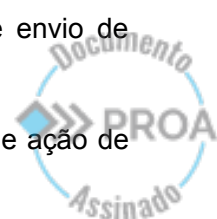
3.4.1.10. O portal da solução deve ser acessado via web browsers de mercado tais como Microsoft Internet Explorer, Google Chrome e Mozilla Firefox.

3.4.1.11. A solução deve suportar múltiplos métodos de notificação e envio de alertas, incluindo e-mail, SMS e SNMP Traps.

3.4.1.12. A solução deve ter sistema de agendamento para a tomada de ação de escalação/notificação de alertas.

**Av. João Pessoa, nº 2050, 3º andar, sala 480, Bairro Azenha, Porto Alegre/RS**  
**CEP: 90040-001 - Fone: 51 3288-2116**  
**E-mail: dtip-dae@pc.rs.gov.br**

22







**ESTADO DO RIO GRANDE DO SUL**  
**POLÍCIA CIVIL**  
**DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO POLICIAL**  
**DIVISÃO DE ACESSORAMENTO ESPECIAL**

3.4.1.13. A solução deve ter acesso por meio de sistemas móveis com suporte a Android e IOS.

**3.4.2. Painéis e Relatórios:**

3.4.2.1. A solução deve guardar dados históricos em banco de dados relacional compatível ao ambiente da CONTRATANTE.

3.4.2.1.1. Deve ser mantido um período mínimo de 05 (cinco) anos de dados históricos.

3.4.2.2. A solução deve ter sistema de geração de relatórios baseado nos dados contidos no banco de dados relacional da solução.

3.4.2.3. O sistema de relatórios deve conter relatórios prontos para uso com temas sobre utilização, capacidade e disponibilidade.

3.4.2.4. Os relatórios devem conter gráficos, tabelas ou objetos gráficos (como imagens, URL links) contendo dados de desempenho.

3.4.2.5. O sistema deve permitir o agendamento de relatórios.

3.4.2.6. A solução deve ter portal web com informações gráficas contendo o status, alarmes e métricas dos sistemas monitorados e a ferramenta de relatórios.

3.4.2.7. A solução deve possuir cadastro de usuários de forma a permitir que empregados e colaboradores possam consultar as informações, conforme itens e

3.4.2.8. O portal da solução deve permitir a criação de visões (*Dashboards*) conforme o perfil do usuário.

3.4.2.9. Gerar relatórios de acompanhamento periódicos *web* através de gráficos, tabelas e dados estatísticos. Analisar o tempo de atividade / inatividade e o desempenho de seus sites a qualquer momento.

3.4.2.10. Permitir exportar os relatórios para, no mínimo, os formatos Microsoft Excel, HTML e PDF.

3.4.2.11. Relatórios informando e apresentando, no mínimo, dados estatísticos sobre:

**Av. João Pessoa, nº 2050, 3º andar, sala 480, Bairro Azenha, Porto Alegre/RS**  
**CEP: 90040-001 - Fone: 51 3288-2116**  
**E-mail: dtip-dae@pc.rs.gov.br**

23





**ESTADO DO RIO GRANDE DO SUL**  
**POLÍCIA CIVIL**  
**DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO POLICIAL**  
**DIVISÃO DE ACESSORAMENTO ESPECIAL**

3.4.2.11.1. Tempos de resposta.

3.4.2.11.2. Percentual de disponibilidade dos serviços (*uptime*).

3.4.2.11.3. Períodos de manutenção programada.

**3.4.3. Monitoração de Itens de Configuração:**

3.4.3.1. Em linhas gerais a solução deverá atender às seguintes necessidades quanto à monitoração de Itens de Configuração relevantes da CONTRATANTE:

**3.4.3.1.1. SERVIDORES:**

3.4.3.1.1.1. Deve ter capacidade de monitorar o desempenho e disponibilidade de servidores.

3.4.3.1.1.2. Prover suporte para os principais ambientes de mercado, sendo virtuais ou físicos.

3.4.3.1.1.3. Deve permitir o gerenciamento com ou sem uso de agente.

3.4.3.1.1.4. Deve ter capacidade de monitorar os recursos de Sistema Operacional (SO) tais como CPU, Memória e Partição/File System.

3.4.3.1.1.5. Deve monitorar recursos dos servidores (carga do processador, utilização de disco e memória, processos em execução, arquivos de log).

3.4.3.1.1.6. Deve ter capacidade de monitorar os arquivos (logfiles) e diretórios.

3.4.3.1.1.7. Para a monitoração de arquivos (logfiles) deve permitir uso de expressões regulares.

3.4.3.1.1.8. Deve permitir a monitoração de log de eventos.

3.4.3.1.1.9. Deve permitir a monitoração de contadores de desempenho do Sistema Operacional.

3.4.3.1.1.10. Deve permitir a monitoração de serviços nos Sistemas Operacionais da CONTRATANTE.

3.4.3.1.1.11. Deve permitir a monitoração de processos.





**ESTADO DO RIO GRANDE DO SUL**  
**POLÍCIA CIVIL**  
**DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO POLICIAL**  
**DIVISÃO DE ACESSORAMENTO ESPECIAL**

3.4.3.1.1.11.1. Na monitoração de processos deve permitir identificar processos individuais por meio de argumentos, ou conter processos que devem existir em quantidades específicas.

3.4.3.1.1.11.2. Caso a monitoração seja sem agente deve suportar coletas via WMI, Telnet ou SSH.

3.4.3.1.1.11.3. Monitorar e gerenciar além dos equipamentos atualmente disponíveis na CONTRATANTE, descritos **no ANEXO II, item 6**, outras plataformas de servidores que a CONTRATANTE porventura venha a possuir, incluindo os sistemas operacionais AIX, LINUX e Windows.

**3.4.3.1.2. BANCO DE DADOS:**

3.4.3.1.2.1. Deve suportar a monitoração de SGBD compatíveis com o ambiente da CONTRATANTE.

3.4.3.1.2.2. A monitoração deve coletar métricas de desempenho do uso de recursos dos bancos de dados, tais como espaço de tabelas, *buffer cache hit ratios*, usuários ativos, *locks*, entre outros.

3.4.3.1.2.3. A solução deve permitir a criação de *queries* customizadas, sendo que estas *queries* são *statements* SQL executados com o intuito de gerar alarmes, coletar métricas de desempenho, tempo de resposta ou valor que deva ser armazenado e reportado pela solução.

3.4.3.1.2.4. A solução deve permitir a descoberta de instancias de banco de dados.

3.4.3.1.2.5. A solução deve permitir a definição de coleta de métricas e *thresholds* para cada instancia ou de forma global.

3.4.3.1.2.6. A solução deve permitir a monitoração baseada em calendário, determinando quando certa monitoração em banco de dados deve iniciar e terminar.

3.4.3.1.2.7. Permitir a monitoração do SGBD Oracle, com o detalhamento das seguintes funções:

**Av. João Pessoa, nº 2050, 3º andar, sala 480, Bairro Azenha, Porto Alegre/RS**  
**CEP: 90040-001 - Fone: 51 3288-2116**  
**E-mail: dtip-dae@pc.rs.gov.br**

25





**ESTADO DO RIO GRANDE DO SUL**  
**POLÍCIA CIVIL**  
**DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO POLICIAL**  
**DIVISÃO DE ACESSORAMENTO ESPECIAL**

- 3.4.3.1.2.7.1. Número de transações.
- 3.4.3.1.2.7.2. Funcionamento do listener.
- 3.4.3.1.2.7.3. Oracle cache.
- 3.4.3.1.2.7.4. Table space system.
- 3.4.3.1.2.7.5. Sessões ativas.
- 3.4.3.1.2.7.6. Shared pool.
- 3.4.3.1.2.7.7. Sessões em lock.
- 3.4.3.1.2.7.8. Controle do volume de redo logs por períodos.
- 3.4.3.1.2.7.9. Schema lists.
- 3.4.3.1.2.7.10. Informações sobre sessões.
- 3.4.3.1.2.7.11. Tablespaces.
- 3.4.3.1.2.7.12. Datafiles.
- 3.4.3.1.2.7.13. Segmentos de rollback.
- 3.4.3.1.2.7.14. Performance/memória.
- 3.4.3.1.2.7.15. Control files.
- 3.4.3.1.2.7.16. Oracle RAC.
- 3.4.3.1.2.7.17. Eventos recentes.

**3.4.3.1.3. SISTEMAS/APLICATIVOS/PORTAIS:**

- 3.4.3.1.3.1. Deve ter capacidade de monitorar aplicações residentes nos sistemas operacionais gerenciados pela solução.
- 3.4.3.1.3.2. Deve ter a capacidade de monitorar desempenho e disponibilidade de servidores de aplicação, tais como IIS, Apache Tomcat, entre outros.
- 3.4.3.1.3.3. Para gerenciamento de IIS deve ser capaz de monitorar checkpoints individuais como *System*, *Web Services*, IIS e ASP.
- 3.4.3.1.3.4. Deve executar testes sintéticos em URL para coleta de tempo de resposta e disponibilidade.

**Av. João Pessoa, nº 2050, 3º andar, sala 480, Bairro Azenha, Porto Alegre/RS**  
**CEP: 90040-001 - Fone: 51 3288-2116**  
**E-mail: dtip-dae@pc.rs.gov.br**

26





**ESTADO DO RIO GRANDE DO SUL**  
**POLÍCIA CIVIL**  
**DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO POLICIAL**  
**DIVISÃO DE ACESSORAMENTO ESPECIAL**

3.4.3.1.3.5. Os testes sintéticos de URL devem monitorar o tempo de download da página e comparar conteúdo da página com valores definidos.

**3.4.3.1.4. REDE DE DADOS:**

3.4.3.1.4.1. Deve permitir o monitoramento nos servidores o tráfego das interfaces de rede do ponto de vista de desempenho.

3.4.3.1.4.2. Deve ser capaz de monitorar para todas as interfaces ethernet nos servidores todo o tráfego TCP/IP com contadores relacionados ao volume trafegado.

3.4.3.1.4.3. Para o tráfego nas interfaces deve analisar por protocolos tais como IP, ARP, RARP e IPX e comparar ao dado coletado.

3.4.3.1.4.4. Deve permitir criar thresholds para monitorar a banda de rede via coleta da interface de rede dos servidores.

3.4.3.1.4.5. A solução deve permitir o monitoramento do tempo de resposta para LDAP, DHCP e DNS por meio de testes sintéticos.

3.4.3.1.4.6. Para DNS deve ser capaz de monitorar tempo de resposta de resolução, monitorar diretórios sem resposta para um ou mais servidores DNS. O DNS pode ser questionado por hostname, mail server ou name server.

3.4.3.1.4.7. Para DHCP deve ser capaz de monitorar o tempo de resposta de assinalar um IP para um ou mais servidores DHCP.

3.4.3.1.4.8. Para LDAP deve ser capaz de monitorar o tempo de resposta e número de itens encontrados nas queries LDAP.

3.4.3.1.4.9. Ter capacidade de fazer testes de Ping e conexão em portas definidas pelo usuário, para identificar a disponibilidade do host e serviços.

3.4.3.1.4.10. Ter capacidade de fazer queries SNMP em dispositivos que o suportem a fim de coletar métricas de disponibilidade e desempenho.

3.4.3.1.4.11. Receber traps SNMP de outros dispositivos ou EMS para tratamento e geração de alarmes.

3.4.3.1.4.12. Suportar coletas via SNMP v1, v2 e v3.

**Av. João Pessoa, nº 2050, 3º andar, sala 480, Bairro Azenha, Porto Alegre/RS**  
**CEP: 90040-001 - Fone: 51 3288-2116**  
**E-mail: dtip-dae@pc.rs.gov.br**

27





**ESTADO DO RIO GRANDE DO SUL**  
**POLÍCIA CIVIL**  
**DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO POLICIAL**  
**DIVISÃO DE ACESSORAMENTO ESPECIAL**

**3.4.3.1.5. VIRTUALIZAÇÃO:**

3.4.3.1.5.1. A solução deve monitorar sistemas de virtualização compatíveis com o ambiente da CONTRATANTE.

3.4.3.1.5.2. A monitoração de sistemas virtuais deve ser realizada sem agente (*agentless*).

3.4.3.1.5.3. Para a monitoração de sistemas virtuais a solução deve identificar recursos, máquinas virtuais, e coletar métricas de consumos relacionados a estes recursos e máquinas.

3.4.3.1.5.4. Para a monitoração de sistemas virtuais a solução deve identificar o consumo de recursos físicos e virtuais.

3.4.3.1.5.5. Deve ser possível identificar visualmente se um dado servidor é físico ou virtual.

3.4.3.1.5.6. Deve ser possível identificar qual o servidor que hospeda uma dada máquina virtual.

3.4.3.1.5.7. Deve organizar a hierarquia de forma que as máquinas virtuais sejam separadas de acordo com os servidores físicos que as hospedam.

**3.4.3.1.6. INTEGRAÇÕES:**

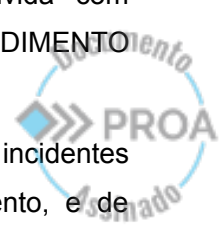
3.4.3.1.6.1. A solução deve suportar recebimento de SNMP traps para integrações com outros sistemas da CONTRATANTE.

3.4.3.1.6.2. A solução deve suportar o envio de traps SNMP para outros sistemas da CONTRATANTE.

3.4.3.1.6.3. A solução deve ter capacidade de exportar configurações em formato XML para integração com sistema de BDGC.

3.4.3.1.6.4. A solução deverá ser capaz de integração, desenvolvida com tecnologia *webservices*, com o SISTEMA DE GESTÃO DE ATENDIMENTO (*software* de Service Desk) a ser ofertado descrito no ANEXO B.

3.4.3.1.6.5. A solução deverá ser capaz de abrir, de forma automática, incidentes no *Service Desk*, a partir de eventos da plataforma de monitoramento, e de





**ESTADO DO RIO GRANDE DO SUL**  
**POLÍCIA CIVIL**  
**DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO POLICIAL**  
**DIVISÃO DE ACESSORAMENTO ESPECIAL**

realizar a associação de um IC ao chamado de incidente no momento do seu registro.

3.4.3.1.6.6. A solução deverá ser capaz de registrar de forma automática comentários/ações na plataforma de monitoramento com o número do chamado.

3.4.3.1.6.7. A solução deverá ser capaz de criar *dashboards* e relatórios customizáveis de indicadores do OTRS.

**3.4.3.1.7. RECURSOS DE VISUALIZAÇÃO DE DADOS ATRAVÉS DE DASHBOARDS:**

3.4.3.1.7.1. A solução deverá prover recursos para a construção, edição e visualização de *dashboards* (painéis visuais) para a centralização de informações importantes através de combinação de um ou mais indicadores ou gráficos.

3.4.3.1.7.2. A solução deverá prover recurso de visualização de dados de capacidade dos elementos nos gráficos.

3.4.3.1.7.3. A solução deverá ter a capacidade prover recurso de visualização em tempo real do status ou de acordo com o tempo de checagem configurado, de cada um dos itens monitorados.

3.4.3.1.7.4. A solução deverá prover recurso que permita alterações de recursos dos gráficos como eixos, grades, cores, fontes, tamanhos, intervalos e métricas.

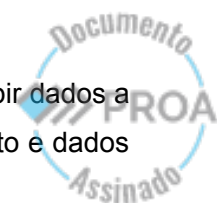
3.4.3.1.7.5. A solução deverá prover recurso que permita a alteração de métricas dos gráficos como nomes, cores, linhas, marcas, legendas e limites de alarmes.

3.4.3.1.7.6. A solução deverá prover recurso para editar os seguintes componentes: gráficos do tipo linha, área, barra e disco; containers (podendo representar estados agrupados de um conjunto de IC da infraestrutura); área de texto, permitindo customizar, escolher e representar em tempo real os últimos valores coletados dos itens monitorados; grade de dados; mostradores (relógio e similares) e elementos do tipo gauges.

3.4.3.1.7.7. Os componentes da construção de *dashboards* deverão exibir dados a partir da associação com itens gerenciados na solução de monitoramento e dados de fontes externas através de integração com *webservices*.

**Av. João Pessoa, nº 2050, 3º andar, sala 480, Bairro Azenha, Porto Alegre/RS**  
**CEP: 90040-001 - Fone: 51 3288-2116**  
**E-mail: dtip-dae@pc.rs.gov.br**

29







**ESTADO DO RIO GRANDE DO SUL**  
**POLÍCIA CIVIL**  
**DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO POLICIAL**  
**DIVISÃO DE ACESSORAMENTO ESPECIAL**

3.4.3.1.7.8. A solução deverá prover recurso para apresentação de dados agrupados de um ou mais itens gerenciados nos componentes a partir da ferramenta de monitoramento ou de fontes de dados externos.

3.4.3.1.7.9. A solução deverá prover recurso para criação de *links* de compartilhamento para visualização de *dashboards* em diversos navegadores sem a necessidade de realizar o *Login* dentro da plataforma.

3.4.3.1.7.10. A solução deverá prover recurso para selecionar os níveis de usuários que visualizarão o *dashboard*.

3.4.3.1.7.11. A solução deverá prover recurso para importação de imagens para utilização delas como componentes dos *dashboards*.

3.4.3.1.7.12. A solução deverá prover recurso para importação de imagens para utilização como plano de fundo dos *dashboards*.

3.4.3.1.7.13. A solução deverá prover recurso para *slide-show* com seleção de telas, seleção de efeitos e tempo de transição automática entre as telas selecionadas para apresentação.

**3.4.3.1.8. MONITORAMENTO CONFORME DESVIO DO COMPORTAMENTO PADRÃO:**

3.4.3.1.8.1. A solução deverá ser capaz realizar a criação automática de linhas de base ou "*baselines*", a partir da análise dos dados coletados e padrões de comportamento, de modo a estabelecer uma linha de base que represente o comportamento normal e esperado, ao longo do período de amostragem, do ambiente de TI, a fim de permitir a identificação automática e em tempo real de mudanças no comportamento de um componente em relação ao valor basal (linha de base).

3.4.3.1.8.2. A solução deverá prover recurso para realizar previsão dinâmica de limites máximo e mínimo esperados para métricas, com base no comportamento histórico e com os seguintes filtros de comparação:

3.4.3.1.8.2.1. Dia: comparação da amostra atual com os dias anteriores.

**Av. João Pessoa, nº 2050, 3º andar, sala 480, Bairro Azenha, Porto Alegre/RS**  
**CEP: 90040-001 - Fone: 51 3288-2116**  
**E-mail: dtip-dae@pc.rs.gov.br**

30





**ESTADO DO RIO GRANDE DO SUL**  
**POLÍCIA CIVIL**  
**DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO POLICIAL**  
**DIVISÃO DE ACESSORAMENTO ESPECIAL**

3.4.3.1.8.2.2. Semana: comparação da amostra atual com as amostras de semanas anteriores.

3.4.3.1.8.2.3. Mês: comparação da amostra atual com as amostras dos meses anteriores.

3.4.3.1.8.2.4. Calendário: comparação da amostra atual com as amostras de meses anteriores levando em consideração o número de dias úteis ou não úteis de cada mês.

3.4.3.1.8.3. A solução deverá permitir que o período de amostragem das linhas de base seja configurável por IC (semana, mês, ano), podendo ser aferida a sazonalidade de um serviço sendo monitorado.

3.4.3.1.8.4. A solução deverá permitir que a frequência de amostragem das linhas de base configurável por IC (a partir de 5 minutos).

3.4.3.1.8.5. A solução deverá prover recursos para notificações automáticas aos responsáveis para detecção de comportamentos anômalos mesmo que não tenha se configurado *thresholds*.

**3.4.3.1.9. MONITORAMENTO DA PERCEPÇÃO DO USUÁRIO:**

3.4.3.1.9.1. A solução deverá prover ferramenta para a criação e edição de robôs que simulam a experiência de usuários através da execução de rotinas análogas às dos usuários, a fim de medir seu tempo de resposta, a taxa de sucesso/falha das rotinas, identificação de erros e *bugs* em aplicações, dentre outras a serem customizadas dentro do módulo.

3.4.3.1.9.2. A solução deverá realizar a verificação/simulação dos seguintes itens: velocidade, correção de cada etapa, disponibilidade de *links* e serviços, situações em que erros ocorrem, real dimensão do problema, impacto, identificação de causa raiz de um problema de desempenho.

3.4.3.1.9.3. A solução deverá permitir a criação de robôs de três tipos:

3.4.3.1.9.3.1. *Web* puros (GET/POST).

3.4.3.1.9.3.2. *Web* híbridos.

**Av. João Pessoa, nº 2050, 3º andar, sala 480, Bairro Azenha, Porto Alegre/RS**  
**CEP: 90040-001 - Fone: 51 3288-2116**  
**E-mail: dtip-dae@pc.rs.gov.br**



31



**ESTADO DO RIO GRANDE DO SUL**  
**POLÍCIA CIVIL**  
**DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO POLICIAL**  
**DIVISÃO DE ACESSORAMENTO ESPECIAL**

3.4.3.1.9.3.3. *Pixel a pixel (Terminal Services).*

3.4.3.1.9.4. A solução deverá realizar a execução de robôs de forma local, remota (dentro da rede do cliente) ou externamente (servidores *web*).

3.4.3.1.9.5. A solução deverá possibilitar a executar simulações com tempo de resposta e taxa de falha/sucesso: transações *web*, acessos a áreas restritas, caminho de um usuário para executar rotinas, testes de *software*, emissão de nota fiscal eletrônica, emissão de segundas-vias de boletos, entre outras.

3.4.3.1.9.6. A solução deverá realizar rotinas de simulação a partir de: reconhecimento de clique, inserção de texto e execução de atalhos de teclado.

3.4.3.1.9.7. A solução deverá permitir a criação de ciclos de repetições de rotinas, onde uma rotina é testada após a execução da anterior.

3.4.3.1.9.8. A solução deverá permitir a clonagem de rotinas para reaproveitamento através de pequenas alterações.

#### **4. DA COMPROVAÇÃO DE REQUISITOS E TESTE DE CONFORMIDADE**

4.1. A licitante no momento da apresentação da proposta deverá enviar documentação garantindo a comprovação detalhada da aderência do sistema ofertado aos requisitos técnicos do edital.

4.2. O licitante classificado em primeiro lugar será convocado para realizar Teste de Conformidade do sistema ofertado, para avaliação técnica de compatibilidade com o solicitado no Termo de Referência, conforme os prazos abaixo:

4.2.1. Prazo para iniciar o Teste de Conformidade e apresentar a pertinente documentação técnica: no máximo **2 (dois) dias úteis**, a contar da suspensão da sessão pública do certame.

4.2.2. Prazo para concluir o Teste de Conformidade: no máximo **5 (cinco) dias úteis**, a contar do início do teste.





**ESTADO DO RIO GRANDE DO SUL**  
**POLÍCIA CIVIL**  
**DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO POLICIAL**  
**DIVISÃO DE ACESSORAMENTO ESPECIAL**

4.3. O Teste de Conformidade servirá para resguardar a segurança da futura contratação e para indicar preliminarmente que o sistema tem condições básicas para atendimento aos requisitos técnicos.

4.4. A condução do Teste de Conformidade se dará conforme descrito no subitem 4.8 deste anexo.

4.5. O sistema a ser utilizado no Teste de Conformidade não poderá ser diferente do apresentado na proposta de preço.

4.6. A fim de garantir que a(s) ferramenta(s) ofertadas tenha condições de suportar plenamente os processos modelados pela CONTRATANTE, o sistema deverá comprovar todas as funcionalidades e especificações descritas neste Anexo do Termo de Referência.

4.7. Caso o Teste de Conformidade da autora da melhor proposta seja reprovado, a proposta será recusada e será convocada a autora da segunda melhor proposta para realizar o teste, e assim sucessivamente.

4.8. Roteiro do Teste de Conformidade.

4.8.1. O licitante classificado em primeiro lugar será convocado a realizar Teste de Conformidade do sistema de gerenciamento de chamados ofertado, para avaliação técnica de compatibilidade com o Termo de Referência, observadas as condições abaixo:

4.8.1.1. Disposições gerais:

4.8.1.1.1. A CONTRATANTE designará uma comissão técnica que acompanhará o licitante em todas as etapas do teste.

4.8.1.1.2. O licitante deverá prover o ambiente de hardware, software e demais recursos necessários à realização do teste, em quantidade e especificação suficientes para a execução de todos os passos.

4.8.1.1.3. O Roteiro de teste deverá ser proposto pela licitante e deverá comprovar todas as especificações técnicas constantes no Termo de Referência.



**Av. João Pessoa, nº 2050, 3º andar, sala 480, Bairro Azenha, Porto Alegre/RS**  
**CEP: 90040-001 - Fone: 51 3288-2116**  
**E-mail: dtip-dae@pc.rs.gov.br**

33



**ESTADO DO RIO GRANDE DO SUL**  
**POLÍCIA CIVIL**  
**DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO POLICIAL**  
**DIVISÃO DE ACESSORAMENTO ESPECIAL**

4.8.1.1.4. Poderá ser solicitada, durante a execução do Roteiro Proposto, a demonstração de qualquer funcionalidade listada nas especificações técnicas constantes no Termo de Referência.

4.8.1.2. Locais, horários e prazos:

4.8.1.2.1. O teste será realizado, em sessão aberta, nas dependências da CONTRATANTE de maneira presencial.

4.8.1.2.2. O licitante terá um prazo de até **2 (dois) dias úteis** após o encerramento da fase de lances para iniciar o Teste de Conformidade, sob pena de recusa de sua proposta pelo não cumprimento do prazo.

4.8.1.2.3. Após o início do teste, o licitante terá um prazo de até **5 (cinco) dias úteis** para concluí-lo, sob pena de recusa de sua proposta pelo não cumprimento do prazo.



**Av. João Pessoa, nº 2050, 3º andar, sala 480, Bairro Azenha, Porto Alegre/RS**  
**CEP: 90040-001 - Fone: 51 3288-2116**  
**E-mail: dtip-dae@pc.rs.gov.br**

34



23120400058592

**Nome do documento:** ANEXO\_A\_Ferramentas\_de\_Gerenciamento\_e\_Monitoramento\_do\_ambiente\_TI\_Rev4\_Final.docx

<b>Documento assinado por</b>	<b>Órgão/Grupo/Matrícula</b>	<b>Data</b>
HENRIQUE SMIDT SEEWALD	PC / 400705 / 322135002	25/03/2024 15:09:39

