



SERVIÇO PÚBLICO FEDERAL
MJSP - POLÍCIA FEDERAL
NÚCLEO DE TECNOLOGIA DA INFORMAÇÃO - NTI/SR/PF/PE

ATESTADO DE CAPACIDADE TÉCNICA Nº 15508015/2020-NTI/SR/PF/PE

Processo nº 08400.005439/2020-80

Interessado: FERNANDO ANTONIO MACIEL RAMOS, G4F SOLUÇÕES CORPORATIVAS LTDA

ATESTADO DE CAPACIDADE TÉCNICA

Atestamos, para os devidos fins, que a empresa **G4F SOLUÇÕES CORPORATIVAS LTDA**, inscrita no CNPJ nº 07.094.346/0001-45, está executando junto à **SUPERINTENDÊNCIA REGIONAL DE POLÍCIA FEDERAL EM PERNAMBUCO**, CNPJ nº 00.394.494/0033-13, por meio do contrato nº 014/2019, a prestação de serviços técnicos continuados na área de Tecnologia da Informação para suporte técnico à usuários (Service Desk) e sustentação da infraestrutura de Tecnologia da Informação da Polícia Federal de Pernambuco.

Início: 21/10/2019

OBJETO: Contratação, em lote único, de uma empresa especializada para execução de SERVIÇOS TÉCNICOS CONTINUADOS E ESPECIALIZADOS EM INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO (TI) E SUPORTE A USUÁRIOS, para suprir as necessidades das unidades da Superintendência Regional de Polícia Federal no Estado de Pernambuco e em suas Unidades Descentralizadas, abrangendo o atendimento aos usuários finais, a execução dos processos vinculados à Operação de Serviço (Service Operation da ITIL), a assistência técnica ao parque de equipamentos de TI e a operação e manutenção das redes de cabeamento estruturado das instalações prediais, incluindo atendimento presencial (com intervenção direta nos equipamentos, ou via Terminal Service) para Suporte, suporte técnico à infraestrutura de TI – suporte e administração de rede dados local e banco de dados, sustentação de servidores, manutenção da segurança da informação e antivírus, e os processos relacionados com o gerenciamento de incidentes, gerenciamento de eventos, gerenciamento de acesso, gerenciamento de problemas, gerenciamento de configurações e o gerenciamento de mudanças, conforme condições, quantidades e exigências estabelecidas no Termo de Referência e abaixo transcrito.

1. Descrição da Solução:

A descrição da solução como um todo, conforme minudenciado nos Estudos Preliminares, abrange a prestação do serviço de implantação de uma Central de Serviços para atender o Suporte Técnico ao Usuário e Sustentação da Infraestrutura, nos moldes das boas práticas inscritas na ITIL, da circunscrição de todas as Unidades da SR/PF/PE, com vistas à execução continuada das seguintes atividades e processos:

- Gerenciamento e tratamento de incidentes e de solicitações de serviços, através de suporte técnico remoto e presencial a usuários, abrangendo o esclarecimento de dúvidas e o acompanhamento do ciclo de vida dos incidentes – detecção e registro dos incidentes, classificação e suporte inicial,

investigação e diagnóstico, resolução e recuperação, acompanhamento e monitoramento do atendimento de incidente até seu fechamento;

- Gerenciamento de eventos, através da detecção de notificações de anormalidades no comportamento de componentes da infraestrutura de TI e monitoração de alertas, com a adoção tempestiva das medidas proativas ou reativas que visem eliminar a causa que está provocando o desvio detectado;
- Gerenciamento de acesso, provendo aos usuários os privilégios necessários para acesso aos serviços que necessitam e são autorizados e removendo os que não são mais necessários;
- Gerenciamento de problemas, através da identificação das causas dos incidentes, sua eliminação, definição de soluções de contorno para problemas conhecidos e manutenção dos roteiros de atendimento da Central de Serviços;
- Gerenciamento de configuração, através da identificação dos itens de configuração necessários para a entrega dos serviços de TI, fornecendo um modelo lógico da estrutura de TI das unidades e mantendo essas informações atualizadas na base de dados de gerenciamento de configuração;
- Gerenciamento de mudanças, assegurando que as mudanças na infraestrutura de TI das unidades são feitas de forma controlada, sendo avaliadas, priorizadas, planejadas, testadas, implantadas e documentadas, seja para a solução de um problema seja para a implementação de novas funcionalidades ou serviços, mantendo a Central de Serviços informada a respeito da agenda de mudanças e seus impactos previstos;
- Instalação e suporte a sistemas operacionais de baixa plataforma, programas aplicativos e aplicativos corporativos da PF no parque de informática da circunscrição das Unidades da SR/PF/PE;
- Suporte a infraestrutura de TI da Superintendência Regional em Pernambuco e de suas unidades descentralizadas, compreendendo a administração da rede de dados, sustentação de servidores, segurança da informação e suporte e administração de banco de dados; e
- Assistência técnica ao parque de equipamentos de TI atualmente instalado ou que venha a ser instalado, compreendo a manutenção preventiva e corretiva de equipamentos de informática (servidores, microcomputadores, notebooks, netbooks, monitores, impressoras, nobreaks, câmeras de vídeo IP, switches, scanners, estabilizadores e projetores multimídia), bem como instalação e manutenção de cabeamento estruturado, de CFTV, centrais de alarmes e de telefonia em dutos ou calhas existentes, sem o fornecimento de peças e componentes, inclusive telefonia IP.
- No que diz respeito à assistência técnica ao parque de equipamentos de TI e à manutenção das redes de cabeamento estruturado, caberá à PF o fornecimento de materiais, peças e componentes necessários para a realização dos serviços, bem como a preparação da infraestrutura necessária para o lançamento de cabos UTP de par trançado para rede local (LAN) CAT 5e ou CAT 6, destinados a eventuais expansões das redes lógicas
- As obras de infraestrutura para o lançamento dos cabos, tais como a instalação de dutos e calhas, não estão incluídas no escopo dos serviços a serem contratados.

A contratação envolve a prestação de duas modalidades básicas de serviços de Tecnologia da Informação: suporte técnico aos usuários (Equipe Especializada I) e sustentação de infraestrutura (Equipes Especializadas II e III). Ambos devem apoiar a utilização dos recursos computacionais e de telecomunicações da PF, existentes no estado de Pernambuco ou distribuídos aos usuários, a fim de garantir não só a continuidade das operações, mas também sua execução de acordo com a configuração e capacidade planejadas e o desempenho esperado. A seguir apresentamos definições quanto às duas principais categorias de serviço

2. Definições de Categorias de Serviços:

2.1 - O Suporte Técnico ao Usuário:

O Suporte Técnico ao Usuário consiste no atendimento das demandas dos usuários (chamados) de soluções e recursos de Tecnologia da Informação e Comunicação, executados

por meio de supervisão e operação de atividades de orientação, esclarecimento, investigação, definição e solução de incidentes e requisições decorrentes de serviços, hardware, software, aplicativos, sistemas corporativos e outros produtos disponíveis na rede da PF e em seu parque tecnológico, bem como por meio da entrega de serviços constantes no catálogo de serviços aos usuários de TI.

A adoção de um modelo de suporte técnico centralizado em uma central de serviços faz parte

das boas práticas de gestão de serviços de TI recomendadas pelo ITILv3. Esse modelo possibilita a solução de dúvidas e solicitações de todos os usuários com tempestividade, padrões e, conseqüentemente, mais qualidade, tendo em vista um Catálogo de Serviços estabelecido para atendimento pela CONTRATADA.

2.2 - Sustentação da Infraestrutura:

A Sustentação da Infraestrutura consiste na supervisão, análise e operação de recursos de infraestrutura de hardware, software e serviços, tais como redes, bancos de dados, servidores, appliances, aplicações de rede, base de conhecimento, base de gerenciamento de itens de configuração, além de outros serviços constantes no Catálogo de Serviços de

Tecnologia da Informação e Comunicação.

A sustentação da infraestrutura deve garantir a disponibilidade dos recursos e sistemas de informação, a fim de preservar a continuidade da prestação de serviços informatizados por parte da instituição.

Na execução dos serviços deverão ser consideradas as melhores práticas de gestão e qualidade amparadas nos modelos ITIL, COBIT, NBR ISO/IEC 17799, NBR ISO/IEC 27000 e

PMBok - em suas versões atualizadas.

Os colaboradores são divididos em três (03) equipes distintas, de modo a refletir as características das atividades a serem desempenhadas e o perfil profissional dos executores das atividades. Cada uma das equipes especializadas será responsável por atuar em um determinado segmento da cadeia de prestação de serviços, de acordo com a sua especialidade, de modo a garantir a observância dos níveis de serviço e desempenho.

Para cada uma das equipes especializadas está definido um conjunto de atividades a serem executadas, conforme será detalhado nos itens na sequência. Além das atividades próprias de cada equipe, estão definidas as seguintes atividades e atributos comuns às equipes especializadas:

- Deverão atender aos chamados da fila sob sua responsabilidade.
- Deverão reportar a incidência de problemas ou a indisponibilidade de serviços para a chefia do NTI/PF/SRPE.
- Deverão realizar todas as atividades típicas da sua especialidade, mesmo aquelas não explicitamente relacionadas.
- Deverão participar de reuniões com o CONTRATANTE e com as equipes de projeto, desde que previamente agendadas e para tratar de assuntos relativos à sua especialidade de atuação.
- Deverão comunicar qualquer incidente de segurança que coloquem em risco as instalações ou as informações do CONTRATANTE.
- Deverão produzir, sempre que demandado, relatórios de continuidade de negócios com indicadores de capacidade e disponibilidade dos recursos de TI e a projeção da sua utilização.
- Deverão criar, verificar e manter atualizados os scripts de solução de problemas dentro da sua especialidade.
- Deverão monitorar de forma proativa a capacidade e a disponibilidade dos ativos sob sua responsabilidade.

- Deverão executar todas as atividades em concordância com as políticas de segurança da informação e de infraestrutura de TI do CONTRATANTE.
- A Contratada deverá garantir a segurança e autenticação de seus empregados através da identificação individual de técnicos, supervisores e gerentes.
- Em caso de desligamento de qualquer empregado da Contratada, este deverá ter imediatamente todos os seus acessos aos sistemas cancelados.

3. Equipes Especializadas:

As equipes especializadas atuam na prestação de duas categorias básicas de serviços de Tecnologia da Informação: Os serviços aos usuários (equipe I) e os serviços de infraestrutura (equipes II e III). Estas categorias se complementam, uma vez que o atendimento a uma requisição de usuário pode dar origem a uma intervenção na infraestrutura, ou a necessidade de alteração de um item na infraestrutura pode demandar intervenções nas estações de usuário.

3.1 A Equipe Especializada I – Atendimento ao usuário atenderão aos seguintes preceitos:

Atendimento Presencial ao Usuário é responsável pela atuação in loco, solucionando as demandas de usuários não resolvidas via atendimento remoto, e também na instalação, distribuição e/ou redistribuição de equipamentos. O atendimento presencial compreende o recebimento, análise, acompanhamento e a solução dos problemas de hardware, software, produtos, serviços e soluções disponibilizadas aos usuários da rede corporativa e aos seus dispositivos (estações de trabalho, telefonia IP, videoconferência e dispositivos móveis), assim como a instalação, configuração e distribuição de dispositivos, tanto devido a novas aquisições como para atender demandas pontuais. Os serviços da Equipe Especializada I, que estão relacionados ao atendimento de 2º (segundo) Nível na referência ITIL, serão prestados nas dependências da PF, visando o pronto atendimento das demandas e a facilitação dos procedimentos de planejamento, monitoramento, fiscalização e melhoria contínua dos processos de gestão dos serviços com a devida segurança física e lógica.

3.2 Equipe Especializada II – Aplicações, Sistemas Operacionais, Serviço de Banco de Dados e Orquestração de Servidores, atenderão aos seguintes preceitos:

A Equipe Especializada II de Suporte à Infraestrutura - Aplicações, Sistemas Operacionais, Serviço de Banco de Dados e Orquestração de Servidores - é responsável pela operação e manutenção, elaboração e execução de rotinas e scripts nos sistemas operacionais dos servidores de aplicações da SR e descentralizadas e é também responsável pela instalação (deploy), configuração e controle da execução das aplicações corporativas, sejam elas adquiridas ou desenvolvidas internamente pela própria instituição. A Equipe II, que estão relacionados ao atendimento de 3º (terceiro) Nível na referência ITIL, também é responsável pelas atividades de manutenção dos bancos de dados, incluindo a sustentação, suporte e administração dos sistemas de gerenciamento de banco de dados (SGBD) existentes nas diversas plataformas da Polícia Federal e pela orquestração do ambiente virtualizado, sendo a responsável por criar e configurar máquinas virtuais e instâncias IaaS (Infrastructure as a Service) para a execução das aplicações, com a consequente administração dos recursos para o bom funcionamento do ambiente. A Equipe II será responsável pela observância às recomendações e boas práticas ITILv3 de Gestão de Incidentes, Gestão de Problemas, Gestão de Mudanças, Gestão de Liberação, Gestão de Acesso, Gestão de Ativos de Hardware e Software, Gestão de Configuração, Gestão da Base de Conhecimentos, Gestão dos Níveis de Serviço, Gestão da Capacidade, Gestão da Disponibilidade e Gestão da Continuidade dos Serviços de TI.

3.3 Equipe Especializada III – Redes Locais, Metropolitanas e de Longa Distância, a Domínio Microsoft, Apoio a Processos de Segurança da Informação e Monitoramento de Ativos:

A Equipe Especializada III de Suporte à Infraestrutura - Redes Locais, Metropolitanas e de Longa Distância, a Domínio Microsoft, Apoio a Processos de Segurança da Informação e Monitoramento de Ativos - é a responsável pela implantação, configuração e manutenção dos ativos e dos enlaces de redes de dados corporativas locais e de longa distância, baseadas nas tecnologias Ethernet, TCP/IP, ATM e MPLS. A Equipe III, também é responsável pelas atividades de manutenção dos bancos de dados, incluindo a sustentação, suporte e administração dos sistemas de gerenciamento de banco de dados (SGBD) existentes nas diversas plataformas da Polícia Federal e também, concentra os colaboradores responsáveis pela execução das atividades de administração, configuração e otimização dos serviços de rede e de domínio baseados na plataforma Windows Server.

4. Requisitos das Equipes Especializadas:

4.1 Requisitos para a Equipe I:

- O atendimento presencial será prestado a partir do escalamento do chamado pela central de atendimento. A partir dos dados registrados quando da abertura do chamado, os técnicos se deslocarão ao local do incidente, em qualquer um dos sítios relacionados neste Termo de Referência, no Estado de Pernambuco.
- Os chamados previamente classificados pela central de atendimento e escalados para o atendimento presencial serão atendidos de acordo com o seu nível de prioridade, estabelecido em função do impacto e da urgência da solicitação. Usuários definidos como VIP terão preferência na classificação de impacto e urgência, e terão prioridade no atendimento.
- Auxiliar e orientar os usuários na abertura de chamado, bem como abrir diretamente os chamados em casos urgentes na Central de Atendimento ao Usuário da DTI
- Manter os usuários informados do estado dos serviços, incidentes e sobre o andamento de suas solicitações
- Contribuir para a identificação de necessidades de treinamento dos usuários Manter uma base de Respostas a Perguntas Frequentes (FAQ – Frequently Asked Questions) para consulta e autoatendimento dos usuários.
- Executar todos os atendimentos técnicos presenciais aos usuários de TI, envolvendo hardware e software. Eventualmente executar atendimentos remoto.
- Executar a instalação, configuração, monitoramento, manutenção, avaliação e acompanhamento dos sistemas de segurança e Antivírus para estações de trabalho.
- Executar serviços de manutenção preventiva de hardware e software.
- Executar serviços de higienização de hardware
- Executar serviços de reparo microeletrônico de bancada de determinados equipamentos e circuitos, tais como fontes de alimentação, impressoras e também de cabos e outros elementos de interconexão, devendo contar com todas as ferramentas e equipamentos necessários para a execução destas atividades.
- Realizar a configuração e formatação de microcomputadores e notebooks.
- Instalar ou substituir impressoras, scanners, switches de rede, leitores biométricos de ponto e outros periféricos.
- Esclarecer dúvidas sobre o manuseio de equipamentos de informática e sobre a utilização de aplicativos
- Esclarecer as dúvidas dos usuários.
- Acompanhar o registro dos bens de informática do CONTRATANTE
- Realizar a instalação, configuração e habilitação necessárias para que os dispositivos eletrônicos funcionem adequadamente na infraestrutura elétrica e de rede local existente.
- Instalar e configurar softwares utilizados nas estações de trabalho do CONTRATANTE.

- Apoiar a elaboração e manter atualizado o inventário de ativos de Tecnologia da Informação e Comunicação (hardware e software), revisando-o sempre que solicitado pelo NTI/SR/PE.
- Encerrar as requisições de serviço corretamente atendidas, registrando detalhadamente no sistema todas as medidas tomadas e os itens da base de conhecimento utilizados, se for o caso.
- Acompanhar a prestação do serviço de videoconferência nas unidades da PF, incluído testes de conexão, agendamento e suporte presencial aos usuários da videoconferência.
- Orientar os usuários quanto à correta utilização dos recursos da rede corporativa do CONTRATANTE, envolvendo hardware e software, de acordo com os normativos internos da PF.
- Apoiar na recepção, montagem e teste de software e hardware adquiridos ou desenvolvidos pelo CONTRATANTE.
- Reportar as ocorrências à supervisão do suporte presencial, registrando os diagnósticos de falhas em microcomputadores e periféricos.
- Identificar com precisão o serviço ou sistema de origem do incidente.
- Acionar fornecedores de suporte e assistência técnica, quando necessário (por exemplo, em caso de vigência da garantia de produtos de informática).
- Escalar chamados para a equipe especializada de apoio à governança, nos casos em que ficar constatado que o incidente está além da capacidade da intervenção local, e tem como causa alguma questão relativa à infraestrutura de TI. Acompanhar o fluxo e os prazos de atendimento.
- Reportar problemas similares ou recorrentes para a equipe especializada de apoio à governança, a fim de determinar a sua causa raiz.
- Alimentar a base de conhecimento com as soluções adotadas para os chamados, para que possam ser também utilizadas pela equipe de atendimento remoto em ocorrências posteriores.
- Atuar na instalação, na conexão e no reordenamento de cabos e pontos de acesso da rede local (LAN), inclusive organização de patch cords em racks, desde que tal atuação não se estenda a ações ou intervenções na rede de cabeamento lógico estruturado.
- Confeccionar cabos lógicos para interconexão entre equipamentos na rede local (LAN), devendo contar com todas as ferramentas necessárias para a execução desta atividade.
- Gerar imagens de desktops e notebooks para instalação e recuperação rápida do sistema operacional, restaurá-las quando da instalação de novos equipamentos.
- Garantir a padronização e a aplicação das regras de compliance definidas para estações de trabalho e notebooks.
- Registrar no SGSD detalhes dos tratamentos dados aos incidentes de forma a manter um histórico que possa ser útil a outro nível em caso de escalonamento.
- Substituir tóner em impressoras
- Gerar imagens (backup) dos discos rígidos que contém a configuração, sistema operacional e aplicativos homologados pela PF relativos aos modelos de microcomputadores existentes no parque de equipamentos das unidades da circunscrição da Superintendência Regional da PF.
- Organizar o cabeamento nos shafts e armários técnicos.
- Realizar atendimento presencial diferenciado e especializado aos grupos de usuários internos definidos pelo NTI/SR/PE (usuários VIPs), e também dos incidentes e requisições de alta complexidade (atendimento especial), de acordo com os requisitos definidos de impacto e urgência
- As atividades de atendimento presencial ao usuário deverão estar disponíveis para o CONTRATANTE no horário entre as 07:00 horas e 21:00 horas dos dias úteis. Todos os níveis mínimos de serviço especificados neste Termo de Referência deverão ser atendidos.
- Os colaboradores da CONTRATADA diretamente envolvidos nas atividades de atendimento presencial devem possuir ensino médio completo ou curso técnico equivalente, comprovado por certificado expedido por instituição de ensino reconhecida pelo Ministério da Educação.

- Possuir experiência mínima de 24 (vinte e quatro) meses no atendimento a usuários de TI, visando à resolução de eventos referentes à configuração, instalação e manutenção física e lógica de estações de trabalho dos usuários do órgão, e suporte a sistema Windows e aplicativos.
- Possuir experiência de manutenção de hardware de microcomputadores e de microeletrônica.
- Possuir experiência com utilização e gerenciamento em nível avançado dos softwares dos pacotes de escritório e aplicativos comuns.
- Conhecimento de redes locais de computadores e em confecção de cabos e instalação de pontos de rede, e também organização de patch cords em racks.
- Noções de Inglês técnico.

4.2 Requisitos de Supervisão para a Equipe especializada I:

- Acompanhar a execução das atividades visando o cumprimento dos níveis de serviço estabelecidos.
- Dimensionar e alocar os recursos da CONTRATADA, com base na demanda de atendimento, no perfil dos técnicos e na disponibilidade da infraestrutura.
- Otimizar escalas, turnos de trabalho e equipes, atuando no planejamento, buscando ganhos de produtividade
- Criar e compartilhar conhecimento, programas motivacionais e atualizações tecnológicas para os profissionais da CONTRATADA envolvidos na execução das atividades de suporte presencial.
- Garantir que normas internas do CONTRATANTE sejam respeitadas pelos colaboradores da CONTRATADA.
- Participar de reuniões mensais com representantes do CONTRATANTE para a medição de serviços e avaliação de desempenho dos níveis de serviços contratados.
- Planejar, acompanhar e controlar a qualidade e o grau de satisfação de usuários em relação às atividades de suporte presencial, a partir dos chamados finalizados por esta equipe no sistema de requisição de serviço.
- Priorizar os atendimentos mais críticos na escala de prioridades, de acordo com o definido neste Termo de Referência, assim como aqueles que o CONTRATANTE definir como críticos.
- Gerir a atualização da Base de Dados de Gerenciamento de Configuração e da Base de Conhecimentos.
- Relacionar-se com fornecedores externos de suporte e assistência técnica para o CONTRATANTE, quando necessário (por exemplo, nos casos de acionamento de serviço de assistência técnica e/ou garantia de produtos de informática).
- Controlar o prazo de atendimento dos chamados de assistência técnica e de suporte técnico de fornecedores externos, em relação ao suporte de equipamentos de usuários de TI.
- Comunicar à Chefia do NTI/PE o não cumprimento de prazos de atendimento dos chamados de assistência técnica e/ou suporte técnico de fornecedores externos do CONTRATANTE, em relação ao suporte de equipamentos de usuários de TI.
- Cuidar da correta alocação dos recursos humanos disponíveis para as atividades de suporte presencial.
- Gerenciar a implantação das melhorias solicitadas pelo CONTRATANTE.
- Apoiar a gestão do inventário de estações de trabalho, impressoras e outros equipamentos utilizados pelos usuários finais de TI
- Elaborar padrões de configuração a serem adotados pelas estações de trabalho (desktops e notebooks Windows XP, 7, 8 e superiores), de acordo com as orientações e normativos estabelecidos pelo CONTRATANTE, a fim de implementar as políticas de compliance para os desktops/notebooks corporativos.
- Colaborar com a implantação/otimização e operacionalização das seguintes disciplinas de ITILv3 – Gerenciamento de Incidente, Gerenciamento de Requisição, Gerenciamento de Acesso,

Gerenciamento da Configuração e de Ativos de Serviço, Gerenciamento de Mudança, Gerenciamento da Base de Conhecimentos.

- O supervisor das atividades de atendimento presencial deve possuir ensino médio completo ou curso técnico equivalente, comprovado por certificado expedido por instituição de ensino reconhecida pelo Ministério da Educação acompanhado de certificado de conclusão de curso na área de Tecnologia da Informação de, no mínimo, 360 horas/aula.
- Experiência profissional mínima 02 (dois) anos de atuação na área de Tecnologia da Informação.
- Experiência profissional mínima de 01 (um) ano como gerente ou supervisor de equipe de suporte técnico a usuários de Tecnologia da Informação.
- Conhecimentos de boas práticas de gestão e governança de TI baseadas nos frameworks ITIL e COBIT; Sistemas operacionais Windows; configuração e instalação de hardware e software; manutenção em sistemas operacionais; métodos, processos e ferramentas de gestão de sistemas de atendimento.

4.3 Requisitos para a Equipe Especializada II:

- Manter e administrar os recursos dos sistemas operacionais dos servidores de aplicações, bancos de dados e orquestração de servidores.
- Realizar o deploy, a manutenção e o controle da execução das aplicações corporativas.
- Administrar os recursos de orquestração do ambiente virtualizado.
- Realizar atividades de instalação física de servidores de aplicações, appliances e outros equipamentos dedicados ao provimento de serviços de TI.
- Fornecer suporte para os incidentes relacionados a servidores de aplicação Linux ou Windows, incluindo diagnóstico e restauração das aplicações que encontram-se em produção ou homologação.
- Analisar e registrar soluções de ocorrências, mantendo o respectivo histórico bem como as soluções.
- Garantir que não haja negação de serviço para os usuários legítimos de aplicações, reportando os problemas para a equipe técnica responsável.
- Manter atualizada a Base de Dados de Configuração dos ativos de servidores e serviços de TI, inclusive em relação aos relacionamentos entre os itens de configuração (ICs). Garantir a consistência e a segurança das informações.
- Atuar junto à Equipe de Desenvolvimento/Manutenção de Sistemas para assegurar o pleno funcionamento das aplicações
- Instalar e administrar Certificados Digitais de servidores e de aplicações.
- Fornecer informações e relatórios sobre a utilização e situação das aplicações.
- Manter e suportar as interfaces entre a Internet e as aplicações, implementar softwares e mecanismos que garantam o acesso seguro e a consistência das funcionalidades web.
- Monitorar e gerenciar a performance dos servidores de aplicação e de banco de dados.
- Analisar periodicamente os logs das aplicações buscando potenciais falhas existentes
- nos sistemas, tomar medidas contingenciais e alertar as áreas responsáveis pelo
- desenvolvimento e uso da aplicação.
- Desenvolver rotinas e scripts voltados à continuidade das aplicações.
- Aplicar as diretrizes institucionais de segurança da informação no que concerne aos
- servidores e às aplicações.
- Fornecer suporte em operações de instalação, implantação e migração de aplicações que se encontram nos ambientes de produção, homologação e testes.
- Atualização de aplicações sustentadas em ambientes de produção, homologação e

- testes.
- Executar mudanças, migrações, atualizações, implantações e testes de novos produtos na plataforma Linux.
- Executar serviços nos servidores de aplicação Linux/Unix e Windows, tais como gerenciamento de discos, parametrização dos sistemas, atualização de versões dos sistemas operacionais e aplicativos, aplicação de correções, service packs, patches e security fixes.
- Propor a atualização dos recursos de software e hardware à CONTRATANTE.
- Transmitir informações sobre assuntos que afetem os usuários, tais como mudanças de configurações de servidores, novas versões de software, etc.
- Garantir a integridade e confidencialidade das informações sob seu gerenciamento e verificar ocorrências de infrações de segurança.
- Implantar processos automatizados de análise, monitoramento e identificação de falhas.
- Apoiar processos de automação de builds e controle de versionamento de aplicações.
- Exercitar e simular contingências, e informar a necessidade de correções e aperfeiçoamentos.
- Executar as atividades de mudanças programadas, atualizando todas as informações pertinentes.
- Garantir a operacionalidade, acessibilidade, disponibilidade e integridade dos softwares de gerência de servidores e aplicações.
- Elaborar padrões de configuração a serem adotados pelos servidores de rede Linux e Windows, de acordo com as orientações e normativos estabelecidos pelo CONTRATANTE, a fim de implementar as políticas de compliance.
- Instalar, customizar e tornar disponível as novas versões dos sistemas operacionais e softwares básicos no ambiente de médio porte (z/OS, z/VM, TSO, CICS, Unix Solaris e AIX), e no ambiente open (RedHat Linux, Suse Enterprise, Fedora, Debian, MS Windows Server 2003, 2008 e 2012), e também drivers e firmwares, a fim de agregar novas funcionalidades às ferramentas, manter a atualização tecnológica e a conformidade com o suporte do fornecedor.
- Instalar, customizar e tornar disponível as novas versões dos softwares aplicativos e de middleware (CASpool, Queue Managers, HTTP/HTTPS servers, Java Application Servers) a fim de agregar os novos recursos das ferramentas e manter a atualização tecnológica e a conformidade com o suporte do fornecedor.
- Administrar a rede e protocolos de comunicação em ambiente mainframe e plataformas intermediárias efetuando a instalação e configuração de placas de comunicação, drivers, TCP/IP, VTAM, etc.
- Administrar serviços adicionais de rede nas plataformas mainframe e open, tais como SSH, TELNET, FTP/SFTP, NFS, RSYSLOG, dentre outros.
- Instalar, configurar e manter os serviços (webservices) dedicados à comunicação
- máquina-máquina, vinculados às aplicações institucionais.
- Apoiar a Instalação e configuração da solução de Backup utilizada pelo CONTRATANTE nos servidores de aplicações, e garantir o seu correto funcionamento.
- Executar testes de regressão e rollback em sistemas quando houver a necessidade de retornar a uma determinada versão de sistema do CONTRATANTE, caso algum deixe de funcionar após uma mudança no ambiente.
- Utilizar recursos de virtualização de servidores e serviços com o intuito de aumentar o
- desempenho e a disponibilidade dos serviços de TI.
- Gerenciar a ferramenta de orquestração de recursos do ambiente virtualizado Hyper-V, ou outras definidas pelo CONTRATANTE.
- Criar mediante requisição de serviço máquinas virtuais para execução, testes ou implantação de novos sistemas, para os ambientes de produção, homologação, testes e desenvolvimento.

- Alocar no ambiente de orquestração recursos de hardware para as máquinas virtuais, tais como unidades lógicas de armazenamento, interfaces de rede, processamento, memória, etc.
- Monitorar na ferramenta de orquestração a utilização dos recursos de hardware do ambiente virtualizado.
- Verificar os problemas no ambiente virtualizado e promover a realocação imediata de recursos para outro pool ou site, evitando assim que ocorram indisponibilidades.
- Realizar o planejamento dos recursos e da capacidade do ambiente virtualizado.
- Executar trabalhos de consolidação, configuração de cluster e distribuição de carga no ambiente virtualizado.
- Apoiar a instalação e configuração de novos servidores de rede e domínio Microsoft para as unidades descentralizadas que ainda não estejam incorporadas ao domínio nacional.
- Manutenção das políticas de backup e restore dos SGBD e da documentação dos procedimentos de backup e restore, seguindo os padrões estabelecidos pela PF.
- Análise dos backups e restores dos bancos de dados, com a execução de testes periódicos para garantir a recuperação dos backups de acordo com as determinações da PF.
- Gerenciamento e monitoramento dos servidores e SGBD da PF.
- Tratamento dos incidentes e problemas relacionados com SGBD, comunicando as ocorrências à Central de Serviços para orientação aos usuários.
- As atividades relacionadas com aplicações, sistemas operacionais e orquestração de servidores e banco de dados deverão estar disponíveis para o CONTRATANTE, local ou remotamente, no regime 24/7/365 (todos os dias do ano em horário integral, de forma ininterrupta). Todos os níveis mínimos de serviço especificados neste Termo de Referência deverão ser atendidos, independentemente do momento de abertura do chamado.
- Experiência Os colaboradores da CONTRATADA diretamente envolvidos na execução das atividades da Equipe II devem possuir diploma de conclusão de curso de graduação em nível superior em qualquer área de Tecnologia da Informação (ou área correlata), fornecido por instituição de ensino superior reconhecida pelo Ministério da Educação, ou diploma de curso de graduação de nível superior em qualquer área de formação acompanhado de certificado de conclusão de especialização na área de Tecnologia da Informação de, no mínimo, 360 horas/aula.
- Experiência mínima de 02 (dois) anos na instalação, administração e sustentação de ambientes Windows Server 2008R2 e 2012.
- Possuir Certificado em ambiente Microsoft Windows Server.
- Conhecimento avançado envolvendo a instalação, administração e configuração de servidores e storages, utilizando sistemas operacionais GNU/Linux (Debian/Ubuntu e Suse Linux Enterprise Server - SLES), VMware, e Scripting (shell script)
- Conhecimentos em boas práticas de gestão e governança de TI com base nos frameworks ITIL e COBIT.
- Inglês Técnico.

4.4 Requisitos para a Equipe Especializada III:

- Configurar e administrar as redes LAN / MAN / WAN. Análise e correção de problemas em redes de transmissão de dados, diagnóstico e análise de desempenho das redes de dados do CONTRATANTE.
- Instalar e manter ativos de rede tais como switches e roteadores, em qualquer um dos sítios de prestação de serviço, de acordo com as políticas institucionais de segurança de informação.
- Criar e remover rotas e redes locais virtuais (VLANs) a partir da configuração dos ativos de rede.
- Auxiliar no diagnóstico e análise de desempenho dos circuitos da rede DPFNet de longa distância que operam nos protocolos Ethernet, ATM ou MPLS, gerenciados pelo consórcio que provê o

serviço.

- Fazer o contato e atuar na resolução de incidentes em conjunto com as empresas provedoras de enlaces de dados de longa distância.
- Configurar e monitorar as implementações e aplicações que utilizam mecanismos de
- qualidade de serviço (QoS) e priorização de tráfego.
- Atuar local ou remotamente nos ativos de rede para realizar configurações ou solucionar incidentes.
- Elaborar a documentação de infraestrutura de rede.
- Manter atualizada a Base de Dados de Configuração de todos os ativos de rede. Garantir a consistência e a segurança das informações.
- Manter a documentação dos desenhos das topologias de rede atualizada e completa.
- Executar configurações necessárias para correções de problemas ou proposição de melhorias.
- Subsidiar os servidores do CONTRATANTE na elaboração de projetos de estruturas físicas e lógicas das redes
- Aplicar de forma proativa os patches para atualização de software e correção de falhas e vulnerabilidades nos ativos de rede.
- Executar periodicamente testes de alta disponibilidade na infraestrutura do CONTRATANTE com o objetivo de validar o seu funcionamento.
- Apoiar a configuração e operação dos ativos e recursos de rede dedicados à infraestrutura de armazenamento dados (Storage Area Network – SAN) e ao backup via rede.
- Operar os softwares e plataformas de gerenciamento de ativos de rede.
- Executar procedimentos e operações programadas em ambiente de produção.
- Analisar previamente a viabilidade e o impacto da instalação de novas soluções e correções.
- Apoiar o projeto e a implantação de redes sem fio nas unidades do CONTRATANTE.
- Efetuar abertura junto a fornecedores e acompanhar chamados técnicos para solução de problemas em equipamentos de rede.
- Prestar suporte, estatísticas e relatórios ao planejamento do CONTRATANTE.
- Administrar o funcionamento dos protocolos de roteamento e de balanceamento de tráfego de rede
- Criar e administrar rotas e domínios de roteamento nos equipamentos de rede TCP/IP do CONTRATANTE.
- Elaborar e sugerir serviços de rede tolerantes à falha, com o intuito de aumentar o
- desempenho e a disponibilidade dos serviços do CONTRATANTE.
- Elaborar e implementar processos e soluções de TI que reduzam a complexidade na
- administração dos servidores e serviços de rede.
- Auxiliar os serviços e a infraestrutura de voz sobre IP (VoIP) do CONTRATANTE.
- Apoiar o monitoramento da infraestrutura de rede IP de longa distância utilizada no sistema de comunicação policial via rádio (TETRAPOL).
- Implantar as práticas de segurança na infraestrutura de rede Windows Server conforme definido pelo CONTRATANTE.
- Instalar, configurar e gerenciar a solução Microsoft System Center 2012: Configuration Manager e Operations Manager.
- Criar dashboards e telas de informações administrativas no System Center Operations Manager, contendo as informações solicitadas pelo CONTRATANTE.
- Administrar e manter os serviços de controle de Domínio – Instalar, configurar, monitorar e gerenciar os controladores de domínio das unidades do CONTRATANTE definidas neste Termo de

Referência.

- Monitorar e manter os serviços de autenticação dos usuários na rede Windows da PF.
- Implementar a automação da configuração de servidores de rede Windows Server.
- Realizar a inclusão, exclusão e bloqueio de contas de usuários do domínio, e a administração dos dados do serviço de diretório Active Directory em conjunto com a equipe especializada II.
- Manter e configurar os serviços de Replicação e Manutenção do Active Directory.
- Manter e configurar o Windows Server Update Services – WSUS, testar e controlar a aplicação de patches de segurança.
- Montar e Configurar o servidor de arquivos (file server) e configurar o serviço de cotas, políticas de segurança de acesso aos arquivos e manutenção de permissão de acesso, de acordo com as políticas definidas institucionalmente para o Active Directory.
- Administrar repositório de logs do Event Viewer de todas as transações realizadas nos
- serviços de autenticação no domínio, de DHCP e nos servidores de arquivos, para fins de auditoria.
- Montagem, configuração e manutenção do servidor de impressoras (Print Server), instalar e configurar novas impressoras e administrar as políticas de acesso.
- Configurar e manter o System State de todos os serviços de rede Microsoft.
- Verificar os status de replicação de informações de diretório e de acesso entre os servidores de domínio da SRPE e os das unidades descentralizadas.
- Instalar, configurar e manter serviço de DNS, WINS e DHCP integrado ao domínio
- Windows Server (interno) e verificar logs.
- Criar, configurar e manter políticas de grupo (GPOs) para os usuários do domínio Windows Server.
- Instalar, configurar e manter cluster de serviços Windows.
- Auxiliar nos testes de backup e restore, e apoiar a restauração a partir do backup de todos os serviços baseados em Windows Server.
- Instalar os agentes, extrair relatórios, configurar novas funcionalidades, realizar inventário e configuração remota através do System Center Configuration Manager.
- Executar migrações, atualizações, implantações e testes de novos produtos.
- Manter atualizada a Base de Dados de Configuração de todos os ativos de serviços de rede e domínio Microsoft. Garantir a consistência e a segurança das informações.
- Apoiar o CONTRATANTE na adoção de mecanismos de segurança nos ativos de TI, compatíveis com as políticas institucionais de segurança da informação.
- Apoiar o CONTRATANTE na adoção de mecanismos de segurança nos ativos de TI, compatíveis com as políticas institucionais de segurança da informação.
- Apoiar o CONTRATANTE nos projetos de Arquiteturas de Segurança da Informação e Comunicações.
- Apoiar o gerenciamento de projetos de implantação, substituição e atualização de soluções destinadas à Segurança da Informação e Comunicações.
- Apoiar o CONTRATANTE na elaboração e revisão de normas relacionadas à Segurança da Informação e Comunicações.
- Cumprir e dar suporte ao monitoramento do cumprimento da Política de Segurança da
- Informação (PSI) e demais normas estipuladas pelo CONTRATANTE.
- Instalar e customizar softwares aplicativos e equipamentos relacionados à segurança de rede adquiridos e/ou homologados pelo CONTRATANTE.
- Apoiar ações conjuntas de Segurança da Informação e Comunicações junto às demais equipes de Infraestrutura, fábrica de software, serviço de atendimento ao usuário e gestores de TI.

- Fornecer suporte técnico para o CONTRATANTE em assuntos relacionados à Segurança da Informação e Comunicações.
- Pesquisar vulnerabilidades e atualizações de segurança, e apoiar o planejamento de mudanças para a sua implementação.
- Apoiar a análise e definição das regras de uso dos recursos computacionais do CONTRATANTE.
- Gerar e consolidar para o CONTRATANTE, no âmbito do GATI (Grupo de Atendimento e Tratamento de Incidentes), os relatórios de ataques e vulnerabilidades nos ambiente de TI, bem como das contramedidas adotadas (atualização de ativos, aplicação de patches e fixes, implementação de sistemas de proteção – antivírus, IPS, firewall, proxy, balanceadores de carga, etc.)
- Realizar testes de vulnerabilidades periódicos conforme as melhores práticas de Segurança da Informação.
- Apoiar a elaboração ou redefinição dos Planos de Continuidade de Serviços para a área de TI (ITSCM), realizando levantamentos e auditorias sobre os potenciais riscos à infraestrutura e medidas para mitigá-los, de forma convergente com a Política de Gestão de Continuidade de Negócios (PGCN) do CONTRATANTE.
- Realizar prospecção, teste e indicação de soluções de Segurança da Informação e
- Comunicações, inclusive baseadas em código aberto.
- Implantar e configurar os acessos remotos seguros dos usuários nas plataformas CISCO e Checkpoint, ou outras que vierem a ser utilizadas pelo CONTRATANTE.
- Apoiar o CONTRATANTE na implantação e consolidação de ferramenta específica para a análise e correlação de eventos e gestão de riscos a partir dos logs e demais registros de eventos existentes no ambiente de TI.
- Administrar a solução de Antivírus Corporativo, com a configuração de estações e de servidores de distribuição, remoções de vírus, resolução de problemas e manutenção dos servidores da plataforma Symantec Endpoint Protection e outras que vierem futuramente a ser utilizadas pelo CONTRATANTE.
- Administrar solução de detecção e prevenção de intrusões (IPS/IDS), incluindo configuração e testes de regras, filtragem de tráfego malicioso, resolução de problemas, atualização de regras, e outros, nas plataformas utilizadas pelo CONTRATANTE.
- Apoiar a implementação de mecanismos de Prevenção à Evasão de Dados (DLP – Data Loss Prevention) no ambiente corporativo.
- Fazer uso de sniffers e scanners para levantar possíveis vulnerabilidades na rede local (LAN).
- Participar do tratamento de incidentes de segurança da informação e comunicações e, quando solicitado, participar em atividades de auditoria e análise forense.
- Apoiar o CONTRATANTE em projetos/atividades de conscientização e palestras em segurança da informação.
- Apoiar na manutenção e administração dos sistemas que envolvem criptografia e assinaturas digitais.
- Auxiliar na manutenção e administração da infraestrutura de Certificação Digital do CONTRATANTE, inclusive com a criação e revogação de certificados digitais.
- Apoiar à execução das atividades das demais equipes de suporte especializado no que tange à segurança da informação.
- Monitorar o funcionamento e consumo de recursos dos appliances e demais ativos de segurança da informação.
- Manter atualizada a Base de Dados de Configuração dos ativos relacionados com mecanismos de segurança. Garantir a consistência e a segurança das informações.
- Realizar o monitoramento proativo do ambiente de infraestrutura do CONTRATANTE

- visando detectar, antecipadamente à queda de desempenho ou indisponibilidade de serviços, os problemas de infraestrutura.
- Operar a plataforma de monitoramento e alarmes de incidentes Zabbix, Cacti, ou outra que venha a ser utilizada pelo CONTRATANTE.
- Registrar manualmente os incidentes que forem observados e para os quais não exista rotina definida para registro automático
- Automatizar, a partir dos alertas emitidos pela ferramenta de monitoramento, o registro de incidentes na plataforma de requisição de serviço e gerenciamento de TI.
- Apoiar a criação e implementação de novas rotinas e itens de monitoramento, em conjunto com a equipe especializada de apoio à governança de TI
- Monitorar todos os ativos, tais como elementos de rede (switches e roteadores LAN/MAN/WAN/SAN, enlaces de rede), aplicações, bancos de dados e qualquer outro item de configuração que componha serviços de TI críticos ou essenciais.
- Monitorar os equipamentos de infraestrutura de data center, tais como: ar condicionado, nobreak, sistema de detecção de incêndio e intrusos, sistema de vigilância, grupo gerador, etc.
- Monitorar todas as atividades, processos e serviços que forem exigidos para o atendimento dos Níveis Mínimos de Serviço.
- Abrir chamados para qualquer incidente detectado para o qual não tenha sido definido um gatilho automático na ferramenta de monitoramento.
- Execução de rotinas padrão, consultas ou relatórios estabelecidos para a equipe de monitoramento.
- Configurar agentes SNMP (Simple Network Management Protocol) ou outros para enviar informações sobre os serviços.
- Implementar o monitoramento dos sistemas em Produção e em Homologação.
- Monitorar a execução das rotinas de backup CONTRATADA.
- Realizar o controle de acesso ao Data Center, com encaminhamento de relatório mensal do acesso para o CONTRATANTE.
- Instalar, configurar e manter os softwares de apoio utilizados pelo CONTRATANTE, tais como os sistemas de controle de tarefas (Mantis, Redmine), sistema de controle de documentação (wiki), dentre outros.
- Administração dos Bancos de Dados nas plataformas PostgreSQL, e MySQL e outros
- utilizadas pela PF.
- Monitoramento do desempenho dos bancos de dados no ambiente de produção - análise da capacidade física e da disponibilidade dos bancos de dados da PF.
- Execução de atividades de manutenção referentes ao Banco de Dados tais como migração de base de dados para outros servidores, criação de instâncias de bancos de dados e instalação de bancos de dados.
- Execução de procedimentos para garantir a segurança dos Bancos de Dados, contemplando desde a adição e remoção de usuários até a auditoria e verificação de problemas de segurança, executando as políticas de gestão da segurança da informação definidas pela PF.
- Instalação e aplicação de pacotes de atualização e segurança nos SGBD, quando necessária configuração ou atualização do Sistema Operacional em um servidor que hospeda um SGBD.
- Auxílio no desenvolvimento ou evolução de rotinas de banco de dados com o intuito de garantir alto desempenho, disponibilidade e integridade.
- As atividades relativas às Redes Locais, Metropolitanas e de Longa Distância, a Domínio Microsoft, Apoio a Processos de Segurança da Informação e Monitoramento de Ativos deverão estar disponíveis para o CONTRATANTE, local ou remotamente, no regime 24/7/365 (todos os dias do ano em horário integral, de forma ininterrupta). Todos os níveis mínimos de serviço especificados

neste Termo de Referência deverão ser atendidos, independentemente do momento de abertura do chamado.

- Os colaboradores da CONTRATADA diretamente envolvidos na execução das atividades da Equipe III devem possuir diploma de conclusão de curso de graduação em nível superior em qualquer área de Tecnologia da Informação (ou área correlata), fornecido por instituição de ensino superior reconhecida pelo Ministério da Educação, ou diploma de curso de graduação de nível superior em qualquer área de formação acompanhado de certificado de conclusão de especialização na área de Tecnologia da Informação de, no mínimo, 360 horas/aula.
- Possuir experiência mínima de dois (02) ano na atividade de monitoramento de ambiente de TI.
- Possuir conhecimentos básicos sobre os mecanismos e protocolos de monitoramento e gerência de TI (SNMP, etc.)
- Possuir experiência mínima de 02 (dois) anos em atividades relacionadas ao apoio à elaboração de normativos de segurança, à implantação de processo de gestão de riscos e continuidade de negócios e ainda, à implantação de políticas de segurança da informação.
- Possuir experiência mínima de 04 (quatro) anos na administração de ambiente de rede IP e MPLS, roteadores, gateway de voz, switches, VLAN, redes wireless, segurança de redes, endereçamento e roteamento IP, protocolos autônomos de roteamento (BGP, OSPF), telefonia IP (VoIP – SIP e H.323) e implantação de QoS em redes corporativas.
- Possuir conhecimentos avançados em boas práticas de gestão e governança de TI com base nos frameworks ITIL e COBIT.
- Conhecimento em PostgreSQL, Mysql e SQL Server.
- Possuir Certificado em ambiente Microsoft Windows Server.
- Inglês Técnico

A G4F apoia e auxilia a equipe técnica do Superintendência da Polícia Federal no desenvolvimento de atividades descritas no Termo de Referência que deu origem ao Contrato em referência.

5. Locais para prestação de Serviço e quantitativos de usuários:

	UNIDADES NOMECLATURAS	ENDEREÇOS	USUÁRIOS(estimados)
1	SR/PF/PE E demais UNIDADES DE PERNAMBUCO		
TOTAL DE USUÁRIOS (estimados)			615

Atestamos ainda que, de acordo com as informações contidas no termo de referência, tais serviços estão sendo executados de acordo com os parâmetros técnicos de qualidade exigidos e no prazo pactuado, não existindo em nossos registros, até a presente data, fatos que desabonem sua conduta e responsabilidade com as obrigações assumidas.

NTI/SR/PF/PE
Superintendência Regional da Polícia Federal



Documento assinado eletronicamente por **FABIO UANDERSON BIZERRA CAVALCANTI, Administrador(a)**, em 28/07/2020, às 16:14, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site http://sei.dpf.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **15508015** e o código CRC **70ABDBC0**.

Referência: Processo nº 08400.005439/2020-80

SEI nº 15508015