

ANEXO - CATÁLOGO DE SERVIÇOS DE TIC PARA ASSINATURAS AVANÇADAS DO ITI

Categoria de serviços

Este anexo apresenta as principais atividades relacionadas ao serviço contrato, mas não limita a atuação da empresa nas competências e ações necessárias para a efetiva atuação.

A operação de infraestrutura de serviços de TIC abrange serviços continuados para monitoramento e sustentação do ambiente computacional que podem ser subdivididos nas seguintes categorias:

Gerência de serviços de TIC:

- Implantar e manter os processos de Gerenciamento de Serviços de TIC definidos pelo ITI, baseado nas melhores práticas, utilizando ferramenta(s) especializada(s);
- Implantar os recursos tecnológicos para o NOC e o SOC;
- Operar, manter, atualizar e criar fluxos de processos na ferramenta de Gerenciamento de Serviços de TIC;
- Adaptar os fluxos básicos de incidentes, requisição, mudanças, problemas e configuração, com o desenho de formulários e criação de regras e validações;
- Criar e adaptar outros fluxos de trabalho, ancorados nos processos básicos de gerenciamento de serviços de TI, o que inclui desenho de formulários e criação de regras e validações;
- Discutir os requisitos dos fluxos de trabalho, para propor a sua adequação às boas práticas de GSTI;
- Identificar melhorias nos processos básicos de gerenciamento de serviços de TIC sob a ótica das melhores práticas de GSTI preconizadas pelo ITIL;
- Utilizar os indicadores chave de desempenho para apoiar a atividade de evolução dos processos;
- Difundir o conhecimento de melhores práticas para as equipes de TIC;
- Realizar as integrações das ferramentas necessárias para o correto funcionamento dos processos;
- Resolver falhas relativas aos fluxos e à ferramenta de suporte ao gerenciamento de serviços de TIC;
- Elaborar, manter e atualizar os relatórios de acompanhamento dos processos e indicadores de níveis de serviço;
- Elaborar relatórios gerenciais e técnicos quando solicitados;
- Acompanhar fornecedores e outros prestadores de serviços relacionados ao escopo do contrato, caso necessário;
- Manter os processos de gerenciamento de incidente, catálogo de serviços, configuração e ativo de serviço, problema, mudança, conhecimento, disponibilidade e níveis de serviço (cabe ao ITI a decisão final sobre implantação ou modificação de processos no âmbito do escopo da contratação);

- Realizar a interface de comunicação entre as demais categorias de serviços e a contratante.

Suporte computacional

- Projetar, operar, administrar e manter o conjunto de soluções, ferramentas, softwares e hardwares que compõe a camada de sustentação de serviços e aplicações do ITI;
- Operar, administrar e manter os servidores físicos e virtuais do ITI;
- Tratar incidentes, problemas, requisições e mudanças relacionados à camada de sustentação de serviços e aplicações do ITI;
- Realizar configurações, alterações e otimizações no ambiente de sustentação de serviços e aplicações do ITI;
- Manter o ambiente atualizado observando as orientações previstas no gerenciamento de mudanças;
- Acompanhar fornecedores e outros prestadores de serviços relacionados ao escopo do contrato, caso necessário;
- Elaborar e manter atualizada a documentação de todo o ambiente.

Armazenamento e Backup

- Projetar, operar, administrar e manter o conjunto de soluções, ferramentas, softwares e hardwares que compõe o ambiente de backup e armazenamento do ITI;
- Executar, manter, atualizar, implantar e apoiar na criação das políticas de backup do ITI;
- Tratar incidentes, problemas, requisições e mudanças relacionados ao ambiente de backup e armazenamento do ITI;
- Realizar configurações, alterações e otimizações no ambiente de backup e armazenamento do ITI;
- Realizar testes de restore com definição de frequência a critério do ITI;
- Manter o ambiente atualizado observando as orientações previstas no gerenciamento de mudanças;
- Acompanhar fornecedores e outros prestadores de serviços relacionados ao escopo do contrato, caso necessário;
- Elaborar e manter atualizada a documentação de todo o ambiente.

Sustentação de Banco de Dados

- Projetar, instalar, implantar, operar, administrar e manter o conjunto de ferramentas, softwares e hardwares que compõe recursos e soluções relacionadas a bancos de dados do ITI;
- Tratar incidentes, problemas, requisições e mudanças relacionados ao ambiente de banco de dados do ITI;

- Realizar configurações, alterações e otimizações no ambiente de banco de dados do ITI;
- Manter o ambiente atualizado observando as orientações previstas no gerenciamento de mudanças;
- Acompanhar fornecedores e outros prestadores de serviços relacionados ao escopo do contrato, caso necessário;
- Registrar chamados para fornecedores das soluções;
- Elaborar e manter atualizada a documentação de todo o ambiente.

Administração de Dados

- Apoiar na auditoria, análise, revisão de documentação relativas à modelagem de dados;
- Construção de queries;
- Apoiar na manutenção de repositório de metadados;
- Manter esquemas de banco de dados;
- Elaborar e manter modelo de dados;
- Apoio na Elaboração e definição de política de segurança do Banco de Dados;
- Realizar apuração Especial;
- Confecção e manutenção de documentação e de procedimentos técnicos;
- Validação de modelos de dados quanto às melhores práticas de modelagem;
- Desenvolvimento, execução, teste e documentação de rotinas de ETL;
- Instalar, configurar, otimizar, parametrizar ferramenta ETL;
- Sugerir automatização das rotinas.

Redes e comunicação de dados

- Projetar, operar, administrar e manter o conjunto de soluções, ferramentas, softwares e hardwares que compõe o ambiente de conectividade e comunicação do ITI;
- Tratar incidentes, problemas, requisições e mudanças relacionados ao ambiente de conectividade e comunicação do ITI;
- Realizar configurações, alterações e otimizações no ambiente de conectividade e comunicação do ITI;
- Manter o ambiente atualizado observando as orientações previstas no gerenciamento de mudanças;
- Acompanhar fornecedores e outros prestadores de serviços relacionados ao escopo do contrato, caso necessário;
- Elaborar e manter atualizada a documentação de todo o ambiente.

Segurança de TIC

- Implantar ambiente de SOC para monitoramento da STI objeto deste contrato.

- Projetar, operar, administrar e manter o conjunto de soluções, ferramentas, softwares e hardwares que compõe o ambiente de segurança de TIC do ITI;
- Tratar incidentes, problemas, requisições e mudanças relacionados ao ambiente de segurança de TIC do ITI;
- Realizar configurações, alterações e otimizações no ambiente de segurança de TIC do ITI;
- Realizar testes de vulnerabilidades dos sistemas e serviços de TIC do ITI, identificando os riscos e sugerindo ações para o devido tratamento;
- Apoiar na elaboração e manutenção da política de segurança do ITI;
- Apoiar na elaboração e manutenção do plano de continuidade de negócio do ITI;
- Apoiar na elaboração e manutenção do plano de gerenciamento de risco do ITI;
- Manter o ambiente atualizado observando as orientações previstas no gerenciamento de mudanças;
- Acompanhar fornecedores e outros prestadores de serviços relacionados ao escopo do contrato, caso necessário;
- Configurar, monitorar, operar e gerenciar equipamentos relacionados ao ambiente de SOC, como firewall, IPS, e outros;
- Atuar na detecção de falhas e brechas;
- Prover respostas rápidas a eventuais ataques;
- Realizar testes de penetração (Pentest);
- Elaborar e manter atualizada a documentação de todo o ambiente.

Monitoramento de Serviços de TIC

- Implantar ambiente de NOC para monitoramento da STI objeto deste contrato.
- Realizar o monitoramento dos sistemas, aplicações, serviços e infraestrutura de TIC do ITI através de ferramenta(as) especializada(s);
- Executar o plano de comunicação realizando os acionamentos dos responsáveis pela resolução dos incidentes, bem como manter informadas as partes interessadas;
- Operar, administrar e manter o conjunto de ferramentas e softwares que compõe a solução de monitoramento de TIC do ITI;
- Realizar configurações, alterações e otimizações na solução de monitoramento de TIC do ITI;
- Manter o ambiente atualizado observando as orientações previstas no gerenciamento de mudanças;
- Acompanhar fornecedores e outros prestadores de serviços relacionados ao escopo do contrato, caso necessário;
- Elaborar e manter atualizada a documentação de toda a solução;
- Outros requisitos complementares estão descritos na seção "**Monitoração de Ambiente Tecnológico (NOC e SOC)**" deste anexo.

Atividades complementares / Apoio Técnico

- Acompanhar fornecedores e outros prestadores de serviços relacionados ao escopo do contrato, caso necessário;
- Elaborar e manter atualizada a documentação de todo o ambiente;
- Identificar, mapear e atualizar o inventário de ativos de TIC;
- Apoiar e acompanhar os processos de gerenciamento de incidente, catálogo de serviços, configuração e ativo de serviço, problema, mudança, conhecimento, disponibilidade e níveis de serviço;
- Apoiar a elaboração de manuais e procedimentos operacionais;
- Apoiar a elaboração de boas práticas e da base de conhecimento.

Macro atividades por domínio

Ativos de Rede - Instalação; Configuração; Manutenção preventiva; Manutenção corretiva; Otimização de performance; Investigação de falha; Investigação de incidente; e Atualização.

Servidores - Instalação; Configuração; Manutenção preventiva; Manutenção corretiva; Otimização de performance; Investigação de falha; Investigação de incidente; e Atualização.

Aplicações - Instalação (*deploy*); Configuração; Manutenção preventiva; Manutenção corretiva; Otimização de performance; Investigação de falha; Investigação de incidente; e Atualização.

Banco de dados - Instalação; Configuração; Manutenção preventiva; Manutenção corretiva; Otimização de performance; Investigação de falha; Investigação de incidente; Atualização; Criação de área de dados; Remoção de dados; Migração de dados; Execução de scripts; e Alteração de privilégios.

Backup - Execução de rotinas; Restauração; Checagem de backups; Simulação; e Atualização.

Armazenamento e Storage - Instalação; Configuração; Manutenção preventiva; Manutenção corretiva; Otimização de performance; Investigação de falha; Investigação de incidente; Atualização; Criação de área de dados; Remoção de dados; Migração de dados; Execução de scripts; e Alteração de privilégios.

Segurança da informação - Instalação; Configuração; Manutenção preventiva; Manutenção corretiva; Otimização de performance; Investigação de falha; Investigação de incidente; Atualização; e Adequação de regras.

Documentação - Manutenção Procedimentos operacionais; testes e simulações; relatórios estatísticos; relatórios de falhas; relatórios de incidentes; relatórios investigativos; notas técnicas; e desenhos arquiteturais de TIC.

Tecnologias de Domínio

Ambiente de armazenamento e rede de dados SAN - Storage Area Network (Rede de Armazenamento de Dados), utilizando fibre channel, ethernet e iscsi, composta por software e hardware de armazenamento de dados suportando minimamente um total de 200 (duzentos) Terabytes e solução de backup (Tape Library) com tecnologia LTO-4 ou superior e capacidade mínima de 100 fitas;

Redes físicas e endereçamento IP – planejamento, atualização, criação, desenho, implantação, administração e manutenção de redes e serviços TCP/IP – incluindo implementações em IPV4 e IPv6 que comprove minimamente o envolvimento dos seguintes componentes, serviços e soluções: Desenho de infraestrutura para redes IPV4 e IPV6, configuração de endereçamentos para alcance global, otimização de entrega de pacotes com formato de cabeçalho simplificado, IPSec nativo, comunicação fim a fim, VPN site to site, multipath, loadbalancing, autonomous system com load sharing, bloco de endereçamento próprio, roteamento entre redes físicas e virtuais (VLAN's), implementação de IPSec para redes IPV4 e IPv6 em plataformas Unix-like (OpenBSD, FreeBSD) e Linux, configuração de serviço de DNS, DHCP e escopos DHCP6, IPV6 em dupla pilha, configuração de switches core considerando o uso de IPV6;

Plataforma de computação em nuvem privada, administração, orquestração e configuração de containers kubernetes e docker através de ferramentas (HELM, RANCHER, OPENSIFT e semelhantes);

Sistemas de proxy, balanceamento de carga e filtro de conteúdo (WAF);

Soluções de segurança da informação para proteção de rede e de host (Antivirus, Firewall, HIDS/IDS/IPS, SIEM e SOAR);

Solução de armazenamento em massa, consolidada e de forma centralizada como DELL Unity, VMAX, Powervault ou semelhantes;

Solução para monitoramento de ativos de redes, links de rede e servidores corporativos, recursos, serviços e aplicações, por meio de instalação e configuração de clientes ou agentes para plataformas Unix-like (OpenBSD, FreeBSD), Linux e Windows, incluindo a configuração de alertas de forma integrada com escalonamento por e-mail, be/ou SMS com a disponibilização de painéis, mapas ou dashboards de monitoramento para visualização do estado atual do ambiente e problemas.

Plataforma de sistemas operacionais e bancos de dados para servidores corporativos, suportando e executando ao menos as plataformas de sistemas operacionais e de bancos de dados abaixo:

- Plataformas de Sistemas Operacionais:
 - Ubuntu – versões 18, 20 ou superior;
 - FreeBSD – versão 11, 12 ou superior;
 - OpenBSD – versão 6, 7 ou superior;
 - CentOS 7 ou superior;

- Microsoft Windows Server – versões 2019 ou superior;
- RedHat Linux – versões 6, 7 ou superior;
- Plataformas de Bancos de Dados:
 - MySQL (MariaDB);
 - PostgreSQL;
 - MongoDB;
 - Elastic;
 - Redis;
 - Microsoft SQL Server.

Solução de gerenciamento, orquestração e provisionamento automático de máquinas virtuais e físicas, implementada e gerenciada pelas soluções de código aberto (Open Source) e Vmware;

Solução de provisionamento automatizado de servidores físicos e virtuais, bem como, de contêineres em Docker e Kubernetes, utilizando sistemas operacionais nas plataformas Microsoft Windows, Debian, Ubuntu, RedHat, CentOS, e Unix-like (OpenBSD e FreeBSD), integrando ainda, ambientes de armazenamento de dados que tenha capacidade de suportar storage;

Solução de gerenciamento de containers e aplicações, utilizando ferramentas de Desenvolvimento Contínuo e Integrados (CICD) com GITLAB ou GITHUB;

Ferramentas de ITSM (OTRS, ZUNNY, REDMINE ou similar) para abertura automática e automação de chamados através de integrações;

Soluções de gestão e registro de eventos de sistema como Graylog, Prometheus, Nagios (ou Zabbix e similares), instalação, configuração, operação e integração, para ambiente composto por pelo menos 100 (cem) servidores virtualizados, no mínimo 8 hosts principais e integração de plataformas de virtualização VMWare ESXi;

Solução de backup utilizando robôs Tandberg NEOxl 40 (ou similares) e suítes de backup Veeam, Bacula (ou similares);

Soluções em shell scripting e operação de sistemas operacionais através de terminais, e em automatização de configuração e orquestração de infraestrutura utilizando Ansible, Puppet, Chef ou solução similar.

Perfis profissionais

Os perfis profissionais que atuarão nas diferentes categorias são padronizados com vistas a possibilitar publicação periódica de pesquisa salarial pela SGD.

Cada perfil profissional possui uma característica e um propósito de atuação, conforme descrito a seguir:

Cod. CBO de Referência	PERFIL PROFISSIONAL DE REFERÊNCIA	DESCRIÇÃO DA ATUAÇÃO
42124-20	Analista de suporte computacional Júnior e Pleno	<p>Profissional associado ao centro de dados. Presta serviços de gerenciamento físico e lógico de equipamentos, servidores, storages, entre outros equipamentos do centro de dados ou no ambiente virtualizado. Atua também no gerenciamento de backups, configuração de procedimentos de recuperação de desastres computacionais, gerenciamento de recursos computacionais avançados (a exemplo de Servidores de arquivos, de impressão, de comunicação institucional) que demandam alocação, configuração ou instalação de softwares ou construção e execução de scripts para o controle, monitoramento e gerenciamento desses recursos.</p> <p>Experiência mínima de dois anos para o perfil Pleno e de um ano para o perfil Júnior nos serviços supracitados, comprovada por meio de registro em Carteira de Trabalho ou contrato(s) executado(s) pelo funcionário, além da devida documentação necessária para que se comprove a participação do funcionário na execução das atividades.</p> <p>A experiência mínima poderá ser de 50% do solicitado caso o profissional tenha atuado em operações de Centro de Dados (CCD) na Presidência da República ou no ITI OU caso o profissional apresente <u>ao menos duas</u> das certificações a seguir: a) HDI SCTL - Support Center Team Lead (ou superior); b) ITIL® intermediário SOA - Service Offerings and Agreements; c) ITIL Foundation v3 ou superior; d) ITIL® intermediário – Operational Support and Analysis Capability (OSA); e) ITIL® intermediário – Planning, Protection and Optimization (PPO); f) HDI SCTL - Support Center Team Lead (ou superior); g) ITIL® intermediário SOA - Service Offerings and Agreements; h) Veritas Certified Specialist (VCS) Netbackup; i) Veeam Certified Engineer (VMCE); j) Veeam Certified Architect (VMCA).</p> <p>Formação em curso superior completo na área de Tecnologia da Informação, ou qualquer formação de nível superior com pós-graduação na área de Tecnologia da Informação, com diploma, devidamente registrado, de conclusão de curso de graduação na área de Tecnologia da Informação ou nível superior em qualquer área com pós-graduação na área de Tecnologia da Informação em nível de especialização ou superior, fornecido por instituição de ensino superior reconhecido pelo Ministério da Educação – MEC.</p> <p>A ausência da formação acadêmica supracitada poderá ser compensada por profissional que apresente <u>ao menos quatro</u> das certificações indicadas.</p>
51425-5, 1425-15	Gerente de infraestrutura de tecnologia da informação	<p>Profissional com responsabilidade de coordenar e gerenciar a atuação dos demais profissionais alocados no monitoramento, controle e operação da infraestrutura de TIC, garantindo a adequada prestação dos serviços, bem como controlando e planejamento operacionalmente as ações dessa equipe. Presta também apoio à tomada de decisão do órgão auxiliando na prospecção de soluções de infraestrutura de TIC, fornecimento de</p>

		<p>informações táticas e operacionais, e proposição de ações de aprimoramento dos serviços de operações na infraestrutura de TIC.</p> <p>Experiência mínima de três anos nos serviços supracitados, comprovada por meio de registro em Carteira de Trabalho ou contrato(s) executado(s) pelo funcionário, além da devida documentação necessária para que se comprove a participação do funcionário na execução das atividades.</p> <p>A experiência mínima poderá ser de 50% do solicitado caso o profissional apresente <u>ao menos duas</u> das certificações a seguir: a) HDI SCTL - Support Center Team Lead (ou superior); b) ITIL® intermediário SOA - Service Offerings and Agreements; c) ITIL Foundation v3 ou superior; d) ITIL® intermediário – Operational Support and Analysis Capability (OSA); e) ITIL® intermediário – Planning, Protection and Optimization (PPO); f) Certificação da Extreme Networks ECS Data CenterVDX; g) Cisco Certified Network Professional (CCNP); h) Cisco Certified Networking Associate (CCNA); i) Cisco Certified Network Professional (CCNP); j) Huawei Certified ICT Associate (HCIA); k) Extreme Networks ECS Data Center VDX.</p> <p>Formação em curso superior completo na área de Tecnologia da Informação, ou qualquer formação de nível superior com pós-graduação na área de Tecnologia da Informação, com diploma, devidamente registrado, de conclusão de curso de graduação na área de Tecnologia da Informação ou nível superior em qualquer área com pós-graduação na área de Tecnologia da Informação em nível de especialização ou superior, fornecido por instituição de ensino superior reconhecido pelo Ministério da Educação – MEC.</p> <p>A ausência da formação acadêmica supracitada poderá ser compensada por profissional que apresente <u>ao menos quatro</u> das certificações indicadas.</p>
62123-5	Administrador de banco de dados Pleno	<p>Profissional responsável pela administração, operação, gerenciamento, carga de dados, otimização e monitoramento dos recursos de banco de dados. Presta serviços de gerenciamento dos esquemas de banco de dados, alocação e administração de recursos físicos e lógicos, realiza dimensionamentos e prospecções de uso, monitora incidentes e promove adequações, aprimoramentos e expansão dos recursos. Pode atuar na análise de dados propondo padrões e assegurando a normalização e melhor uso dos recursos para armazenamento e utilização de dados corporativos.</p> <p>Experiência mínima de dois anos nos serviços supracitados, comprovada por meio de registro em Carteira de Trabalho ou contrato(s) executado(s) pelo funcionário, além da devida documentação necessária para que se comprove a participação do funcionário na execução das atividades.</p> <p>A experiência mínima poderá ser de apenas 50% do solicitado caso o profissional apresente certificação oficial de DBA nas tecnologias: a) Oracle (OCP ou OCA); ou b) Postgree.</p> <p>Formação em curso superior completo na área de Tecnologia da Informação, ou qualquer formação de nível superior com pós-graduação</p>

		<p>na área de Tecnologia da Informação, com diploma, devidamente registrado, de conclusão de curso de graduação na área de Tecnologia da Informação ou nível superior em qualquer área com pós-graduação na área de Tecnologia da Informação em nível de especialização ou superior, fornecido por instituição de ensino superior reconhecido pelo Ministério da Educação – MEC.</p> <p>A ausência da formação acadêmica supracitada poderá ser compensada por profissional que apresente <u>ao menos uma</u> das certificações indicadas.</p>
72123-15	Administrador de sistemas operacionais Pleno	<p>Profissional que atua na camada de virtualização e orquestração de sistema operacionais de servidores de dados. Presta serviços de configuração, instalação e ampliação de ambientes de containers . Responsável pela adequada operação, desempenho e uso racional de recursos utilizados pelos softwares básicos, orquestradores de containers e virtualizadores.</p> <p>Experiência mínima de dois anos nos serviços supracitados, comprovada por meio de registro em Carteira de Trabalho ou contrato(s) executado(s) pelo funcionário, além da devida documentação necessária para que se comprove a participação do funcionário na execução das atividades. A experiência mínima poderá ser de apenas um ano caso o profissional tenha atuado em operações de Centro de Dados (CCD) na Presidência da República ou no ITI.</p> <p>A experiência mínima poderá ser de 50% do solicitado caso o profissional apresente ao menos três das certificações a seguir: a) HDI SCTL - Support Center Team Lead (ou superior); b) ITIL® intermediário SOA - Service Offerings and Agreements; c) ITIL Foundation v3 ou superior; d) ITIL® intermediário – Operational Support and Analysis Capability (OSA); e) ITIL® intermediário – Planning, Protection and Optimization (PPO); f) Certificação da Extreme Networks ECS Data CenterVDX; g) Cisco Certified Network Professional (CCNP); h) Cisco Certified Networking Associate (CCNA); i) Cisco Certified Network Professional (CCNP); j) Huawei Certified ICT Associate (HCIA); k) Extreme Networks ECS Data Center VDX; l) Certificação Certified Linux Administrator (LPIC-1 ou LPIC-2); m) Certificação Red Hat Certified System Administrator (RHCSA); n) Certificação Linux Enterprise Mixed Environment (LPIC-3); o) Certificação Red Hat Certified Engineer (RHCE).</p> <p>Formação em curso superior completo na área de Tecnologia da Informação, ou qualquer formação de nível superior com pós-graduação na área de Tecnologia da Informação, com diploma, devidamente registrado, de conclusão de curso de graduação na área de Tecnologia da Informação ou nível superior em qualquer área com pós-graduação na área de Tecnologia da Informação em nível de especialização ou superior, fornecido por instituição de ensino superior reconhecido pelo Ministério da Educação – MEC.</p> <p>A ausência da formação acadêmica supracitada poderá ser compensada por profissional que apresente <u>ao menos cinco</u> das certificações indicadas.</p>

82124-10, 2123-10	Analista de redes e de comunicação de dados Pleno	<p>Profissional que atua na intercomunicação de redes locais e de longa distância, com ou sem fio, assegurando a operação, desempenho e qualidade dos serviços de rede e comunicação de dados, bem como no aprimoramento e funcionamento adequados dos ativos de redes. Presta serviços de execução, aprimoramento e manutenção dos projetos de redes, além da configuração e otimização de recursos de interconexão de dados.</p> <p>Experiência mínima de dois anos nos serviços supracitados, comprovada por meio de registro em Carteira de Trabalho ou contrato(s) executado(s) pelo funcionário, além da devida documentação necessária para que se comprove a participação do funcionário na execução das atividades. A experiência mínima poderá ser de apenas um ano caso o profissional tenha atuado em operações de Centro de Dados (CCD) na Presidência da República ou no ITI.</p> <p>A experiência mínima poderá ser de 50% do solicitado caso o profissional apresente ao menos três das certificações a seguir: a) HDI SCTL - Support Center Team Lead (ou superior); b) ITIL® intermediário SOA - Service Offerings and Agreements; c) ITIL Foundation v3 ou superior; d) ITIL® intermediário – Operational Support and Analysis Capability (OSA); e) ITIL® intermediário – Planning, Protection and Optimization (PPO); f) Certificação da Extreme Networks ECS Data Center VDX; g) Cisco Certified Network Professional (CCNP); h) Cisco Certified Networking Associate (CCNA); i) Cisco Certified Network Professional (CCNP); j) Huawei Certified ICT Associate (HCIA); k) Extreme Networks ECS Data Center VDX; l) Certificação Certified Linux Administrator (LPIC-1 ou LPIC-2); m) Certificação Red Hat Certified System Administrator (RHCSA); n) Certificação Linux Enterprise Mixed Environment (LPIC-3); o) Certificação Red Hat Certified Engineer (RHCE).</p> <p>Formação em curso superior completo na área de Tecnologia da Informação, ou qualquer formação de nível superior com pós-graduação na área de Tecnologia da Informação, com diploma, devidamente registrado, de conclusão de curso de graduação na área de Tecnologia da Informação ou nível superior em qualquer área com pós-graduação na área de Tecnologia da Informação em nível de especialização ou superior, fornecido por instituição de ensino superior reconhecido pelo Ministério da Educação – MEC.</p> <p>A ausência da formação acadêmica supracitada poderá ser compensada por profissional que apresente <u>ao menos cinco</u> das certificações indicadas.</p>
102124-15, 2124-25	Analista de sistemas de automação Pleno	<p>Profissional responsável por assegurar utilização adequada de soluções de integração (CI) ou de entrega contínua (CD). Pode atuar como arquiteto de soluções e propor, projetar, executar e aprimorar arquiteturas de soluções necessárias à manutenção e melhoria das operações na infraestrutura de TIC. Pode atuar também como arquiteto de computação em nuvem, ou ainda como arquiteto de soluções híbridas.</p> <p>Experiência mínima de dois anos nos serviços supracitados, comprovada por meio de registro em Carteira de Trabalho ou contrato(s) executado(s)</p>

		<p>pelo funcionário, além da devida documentação necessária para que se comprove a participação do funcionário na execução das atividades. A experiência mínima poderá ser de apenas um ano caso o profissional tenha atuado em operações de Centro de Dados (CCD) na Presidência da República ou no ITI.</p> <p>A experiência mínima poderá ser de 50% do solicitado caso o profissional apresente ao menos duas das certificações a seguir: a) ferramentas de automação robótica de processos (RPA); b) Certified Kubernetes Administrator (CKA); c) Certified Kubernetes Security Specialist (CKS); d) Red Hat Certified Specialist in Containers and Kubernetes; e) Red Hat Certified System Administrator (RHCSA); f) Red Hat Certified Engineer (RHCE). A experiência mínima poderá ser de apenas um ano caso o profissional tenha atuado em operações de Centro de Dados (CCD) na Presidência da República ou no ITI.</p> <p>Formação em curso superior completo na área de Tecnologia da Informação, ou qualquer formação de nível superior com pós-graduação na área de Tecnologia da Informação, com diploma, devidamente registrado, de conclusão de curso de graduação na área de Tecnologia da Informação ou nível superior em qualquer área com pós-graduação na área de Tecnologia da Informação em nível de especialização ou superior, fornecido por instituição de ensino superior reconhecido pelo Ministério da Educação – MEC.</p> <p>A ausência da formação acadêmica supracitada poderá ser compensada por profissional que apresente <u>ao menos quatro</u> das certificações indicadas.</p>
122123-20	Administrador em segurança da informação Pleno e Sênior	<p>Profissional responsável por assegurar a prestação de serviços de segurança da informação, incluindo o monitoramento e tratamento de incidentes, ações preventivas, implantação e monitoramento de controles de segurança, realização dos diferentes testes e inspeções de segurança. presta serviços e controle de segurança preventivo e reativo relacionado aos diferentes ativos da infraestrutura, bem como apoia na implementação das ações técnicas previstas na política de segurança.</p> <p>Experiência mínima de quatro anos nos serviços supracitados para o perfil Sênior e de dois anos para o perfil Pleno, comprovada por meio de registro em Carteira de Trabalho ou contrato(s) executado(s) pelo funcionário, além da devida documentação necessária para que se comprove a participação do funcionário na execução das atividades. A experiência mínima poderá ser de 50% do solicitado caso o profissional tenha atuado em operações de Centro de Dados (CCD) na Presidência da República ou no ITI.</p> <p>A experiência mínima poderá ser de apenas 50% do solicitado caso o profissional apresente certificação oficial ou curso de graduação/especialização (acima de 80h/aula) em Segurança da Informação OU caso o profissional apresente <u>ao menos três</u> das certificações a seguir: a) Certificação Check Point Certified Security Expert (CCSE); b) Certified Information Security Manager (CISM); c) Systems Security Certified Practitioner (SSCP); d) Certified Information Systems</p>

		<p>Security Professional (CISSP); e) CompTIA Advanced Security Practitioner (CASP+); f) GIAC Security Expert (GSE).</p> <p>Formação em curso superior completo na área de Tecnologia da Informação, ou qualquer formação de nível superior com pós-graduação na área de Tecnologia da Informação, com diploma, devidamente registrado, de conclusão de curso de graduação na área de Tecnologia da Informação ou nível superior em qualquer área com pós-graduação na área de Tecnologia da Informação em nível de especialização ou superior, fornecido por instituição de ensino superior reconhecido pelo Ministério da Educação – MEC.</p> <p>A ausência da formação acadêmica supracitada poderá ser compensada por profissional que apresente <u>ao menos cinco</u> das certificações indicadas.</p>
131425-25	Gerente de segurança da informação	<p>Profissional com responsabilidade de coordenar e gerenciar a atuação dos demais profissionais de segurança da informação, garantindo a adequada prestação dos serviços, bem como controlando e planejamento operacionalmente as ações dessa equipe. Presta também apoio à tomada de decisão do órgão auxiliando na prospecção de soluções de segurança da informação, fornecimento de informações táticas e operacionais, e proposição de ações de aprimoramento dos serviços de segurança da informação seja preventiva ou reativa.</p> <p>Experiência mínima de três anos nos serviços supracitados, comprovada por meio de registro em Carteira de Trabalho ou contrato(s) executado(s) pelo funcionário, além da devida documentação necessária para que se comprove a participação do funcionário na execução das atividades.</p> <p>A experiência mínima poderá ser de 50% do solicitado caso o profissional apresente certificação oficial ou curso de graduação/especialização (acima de 80h/aula) em Segurança da Informação OU caso o profissional apresente ao menos três das certificações a seguir: a) Certificação Check Point Certified Security Expert (CCSE); b) Certified Information Security Manager (CISM); c) Systems Security Certified Practitioner (SSCP); d) Certified Information Systems Security Professional (CISSP); e) CompTIA Advanced Security Practitioner (CASP+); f) GIAC Security Expert (GSE).</p> <p>Formação em curso superior completo na área de Tecnologia da Informação, ou qualquer formação de nível superior com pós-graduação na área de Tecnologia da Informação, com diploma, devidamente registrado, de conclusão de curso de graduação na área de Tecnologia da Informação ou nível superior em qualquer área com pós-graduação na área de Tecnologia da Informação em nível de especialização ou superior, fornecido por instituição de ensino superior reconhecido pelo Ministério da Educação – MEC.</p> <p>A ausência da formação acadêmica supracitada poderá ser compensada por profissional que apresente <u>ao menos quatro</u> das certificações indicadas.</p>
n/a	Preposto	<p>O Preposto e seu substituto serão os responsáveis administrativos, com poderes de representante legal para tratar de todos os assuntos</p>

		<p>relacionados ao contrato, atuando à luz da Instrução Normativa nº 01/2019 da SGD/ME e suas revisões, e em atenção ao art. 68 da Lei nº. 8.666/93. Será atribuída sua gerir a execução do serviço, objeto do contrato, por parte da contratada, objetivando garantir a execução e entrega dos serviços dentro dos prazos estabelecidos e atendendo todos os requisitos especificados neste Termo de Referência; Gerir as solicitações de mudanças feitas pelo ITI, formalmente encaminhadas; Responder, perante o ITI, pela execução das solicitações; Participar periodicamente, a critério do ITI, de reuniões de acompanhamento das atividades referentes à prestação do serviço em execução. Não há obrigatoriedade do preposto disponível fisicamente nas dependências do ITI. Todavia, o preposto, obrigatoriamente, deverá estar disponível fisicamente nas dependências do ITI, quando solicitado, principalmente enquanto houver a execução da prestação de serviços por parte da contratada ao ITI.</p> <p>Experiência mínima de um ano nos serviços supracitados.</p> <p>Formação segundo grau completo.</p>
--	--	---

Observação 1: Cada Perfil profissional está associado a um ou mais CBO (Códigos Brasileiro de Ocupação) com vistas a estabelecer uma referência mais acurada a bases salariais de governo.

Observação 2: Caso a empresa opte por alocar parte da equipe dentro das instalações do ITI/PR, será cedido mobiliário completo e equipamentos de TIC para até três postos de trabalho. Neste caso, a permanência do profissional não configurará dedicação exclusiva de mão de obra.

Além das competências individuais supracitadas, específicas do cargo, a equipe deverá possuir as seguintes competências de atuação transversal: Controle de versão; Integração contínua; Testes contínuos; Gerenciamento de configuração e deployment; Monitoramento contínuo; Containerização; Orquestração; Segurança integrada; e Gerenciamento integrado de demandas integrada.

Todos os prestadores deverão ser registrados pelo regime CLT ou possuir contratos de prestação de serviços junto à contratada.

Monitoração de Ambiente Tecnológico (NOC e SOC)

O serviço de monitoração do ambiente tecnológico deverá contemplar todos os elementos de hardware e software necessários a disponibilização dos serviços de TIC descritos neste TR e anexos.

Deverá também monitorar as instalações (*facilities*) de centro de dados e salas técnicas, quando houver disponível ferramenta adequada a esta monitoração.

Para a realização do monitoramento da infraestrutura de rede de dados e componentes de segurança da informação, a contratada deverá utilizar as ferramentas já implantadas no ambiente do ITI, ou sugerir novas quando as atuais se demonstrarem insuficientes para a gestão adequada. No caso de eventuais custos extras (licenciamento, implantação, configuração, adaptação, customização, migração, administração, etc), estes serão de inteira responsabilidade da contratada.

O serviço de Monitoração dos Serviços é responsável pela análise dos ativos, aplicações e serviços de TI do ITI em regime integral 24x7 (24 horas por dia, em 7 dias por semana), e deverá ser Remoto.

Os Serviços de TIC que serão objeto da avaliação de disponibilidade para efeito de mensuração de NMS deverão ser monitorados conforme determinação do ITI. Os demais ativos e serviços de TIC deverão ser monitorados a critério da contratada, sendo facultada à equipe técnica do ITI a solicitação de monitoração de itens específicos.

A equipe do NOC e SOC deverá ser capaz de tratar incidentes por meio de scripts ou procedimentos para reduzir o tempo de resolução dos mesmos.

A equipe do NOC e SOC deverá ser capaz de escalar para especialista de plantão, ou para outro que tenha maior capacidade técnica para resolução do incidente, de acordo com a necessidade específica do caso.

A contratada deverá implementar esquema de escalação de incidentes para analistas de maior conhecimento técnico, inclusive fora do horário de expediente, em regime 24x7.

Os serviços terão a disponibilidade mensurada conforme critérios estabelecidos pelo ITI.

No processo de gestão de incidentes, a equipe do NOC e SOC deverá tornar disponível as informações de detecção e tratamento de incidentes/problemas à respectiva equipe técnica responsável, para que esta tenha capacidade de responder o incidente/problema de forma mais célere.

A ferramenta de monitoração deverá ser configurada para automaticamente cadastrar incidentes na ferramenta de ITSM associados ao item/ativo adequado, a fim de permitir a tratativa e gestão dos incidentes.

A ferramenta de monitoração deverá ser capaz de prover dados para compor relatório específico de disponibilidade de Serviços de TIC ou de soluções de TIC.

Ao término do contrato, toda documentação e dados gerados pelas ferramentas deverão ser entregues ao ITI em modelo e padrões definidos por este.

Operação de Infraestrutura de TI.

Este serviço assemelha-se ao terceiro nível de atendimento, onde especialistas da contratada realizam as diversas atividades técnicas preestabelecidas para manutenção periódica e atividades de reparo/restauro quando da ocorrência de incidentes e problemas.

O serviço de Operação de infraestrutura deverá ser capaz de projetar, planejar, implementar, administrar, operar e restabelecer serviços locais (*On-premises*) ou em cenário de infraestrutura híbrida nas diversas modalidades como: IaaS, PaaS e SaaS.

Os serviços de Operação de Infraestrutura deverão atuar no processo de tratamento de incidentes em regime de plantão 24x7, inclusive para incidentes específicos de segurança de TIC, que venham a ser reportados no escopo de serviço de outros contratos do ITI, sem custo adicional.

Os serviços de Operação de Infraestrutura, quando necessário ou demandados por catálogo de serviços, deverão investigar incidentes e problemas a fim de identificar a causa raiz, propor e executar as correções necessárias, e também elaborar relatórios detalhados. Quando necessário deverá inclusive atuar em conjunto com outras contratadas do ITI, ou terceiros indicados e necessários.

Os serviços de Operação de Infraestrutura também compreenderão:

1. Solucionar ou viabilizar os diversos serviços da rede, analisando as ocorrências e diagnosticando os problemas, visando normalizar os procedimentos e cumprir os padrões de qualidade, prazo e prioridade estabelecidos;
2. Definir procedimentos de testes dos equipamentos e softwares implantados ou que sofrerão manutenção, antes de substituir os efetivos, visando manter controle dos impactos sobre as rotinas vigentes;
3. Definir e implementar configurações contra ataques de vírus de computador e invasão da rede local;
4. Auxiliar e propor mudanças nas definições dos requisitos de segurança, infraestrutura e tecnologia a serem utilizadas na implementação das soluções de TI;
5. Alimentar a base de conhecimento, com a descrição de solução de problemas resolvidos;
6. 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;
7. Instalar e manter ativos de rede tais como switches e roteadores, em qualquer um dos sítios de prestação de serviço, conforme as políticas institucionais de segurança de informação;
8. Criar e remover rotas e redes locais virtuais (VLANs) a partir da configuração dos ativos de rede;
9. Fazer o contato e atuar na resolução de incidentes em conjunto com as empresas provedoras de enlaces de dados de longa distância;

10. Configurar e monitorar as implementações e aplicações que utilizam mecanismos de qualidade de serviço (QoS) e priorização de tráfego;
11. Atuar local ou remotamente nos ativos de rede para realizar configurações ou solucionar incidentes;
12. Elaborar a documentação de infraestrutura de rede, manuais para base de conhecimento e desenhos de topologia de rede;
13. Subsidiar os servidores da rede na elaboração de projetos de estruturas físicas e lógicas das redes;
14. Aplicar de forma proativa os patches para atualização de software e correção de falhas e vulnerabilidades nos ativos de rede;
15. Executar periodicamente testes de alta disponibilidade na infraestrutura da rede com o objetivo de validar o seu funcionamento;
16. Realizar configuração e operação dos ativos e recursos de rede dedicados à infraestrutura de armazenamento de dados e ao backup via rede;
17. Executar as rotinas de operação e administração do firewall, WAF, Proxy, GPO, visando garantir a disponibilidade, o melhor desempenho, a segurança e a continuidade da operação;
18. Administrar as soluções 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 ITI;
19. Realizar suporte técnico por meio da administração, da análise, do diagnóstico e da solução de incidentes/problemas relacionados ao ambiente de virtualização (Hyper-v e VMware);
20. Realizar configuração, automatização e operação de ferramentas de "Operations Manager";
21. Administração, sustentação e suporte em máquinas virtuais virtualizadas envolvendo criação, clone, migração e crescimento horizontal;
22. Desenvolver templates de máquinas virtuais com os sistemas operacionais indicados pelo ITI;
23. Gerenciar cluster de virtualização com os recursos Físicos fornecidos pelo ITI;
24. Administrar e gerenciar servidores de aplicação/web;
25. Administrar, Operar e Suportar Banco de Dados;
26. Desenvolver Procedures, Querys, Scripts, Cargas de Dados em BD, Views, Triggers e Functions;
27. Modelar dados (Transacional e Multidimensional);
28. Construir mapas e processos de ETL. Apoiar à equipe de desenvolvimento de sistemas;
29. Recomendar as melhores práticas na área de Banco de Dados voltada para o negócio do ITI;
30. Utilizar ferramentas ETL de extração de dados, DW e Data Mining;
31. Acompanhar rotinas de backup por meio da ferramenta de monitoração para identificar possíveis erros;

32. Analisar logs de erros na ferramenta de backup para identificar melhor forma de correção;
33. Corrigir job's de backup por meio da ferramenta utilizada para restaurar o backup;
34. Desenhar e criar políticas de backup de acordo com a demanda do órgão, implementando as definições na ferramenta para atender os requisitos do ITI;
35. Restaurar dados de acordo com a demanda do ITI para recuperar informações perdidas;
36. Gerenciar armazenamento analisando o espaço utilizado por meio de relatórios para alertar sobre a disponibilidade de espaço;
37. Analisar o funcionamento do backup por meio de relatórios para apresentar e propor melhorias ao ITI;
38. Documentar e automatizar processos;
39. Realizar auditorias;
40. Emitir notas técnicas.

Os serviços abaixo representam as operações de Infraestrutura pré-determinados para outro ambiente do ITI, e que podem, em algum momento, fazerem parte do escopo das atividades periódicas da contratada:

1. Acompanhamento da manutenção do ambiente seguro (ongoing) - 52 vezes ao ano;
2. Tratamento dos registros de acesso - 52 vezes ao ano;
3. Backup do Sistema de CFTV (verificação) - 12 vezes ao ano;
4. Restauração de Backup do CFTV - 4 vezes ao ano;
5. Backup do Servidor Syslog (verificação) - 12 vezes ao ano;
6. Restauração de Backup do Syslog - 4 vezes ao ano;
7. Análise de registros de acesso aos Repositórios das Assinaturas Avançadas - 12 vezes ao ano;
8. Backup do Servidor de Arquivos (verificação) - 12 vezes ao ano;
9. Restauração de Backup do Servidor de Arquivos - 4 vezes ao ano;
10. Backup das bases de dados e arquivos de configuração (verificação) - 12 vezes ao ano;
11. Restauração de Backup da base de dados e arquivos de configuração - 4 vezes ao ano;
12. Backup do Sistema de Controle de Acesso (verificação) - 12 vezes ao ano;
13. Restauração de Backup do Sistema de Controle de Acesso - 4 vezes ao ano;
14. Backup do Sistema Antifraude (verificação) - 12 vezes ao ano;
15. Restauração de Backup do Sistema Antifraude - 4 vezes ao ano;
16. Análise da disponibilidade dos Repositórios das Assinaturas Avançadas - 12 vezes ao ano;
17. Atualização do SO dos Servidores - 4 vezes ao ano;
18. Backup do Servidor SFTP (verificação) - 12 vezes ao ano;

19. Restauração de Backup do Servidor SFTP - 4 vezes ao ano;
20. Revisão de acessos físicos - 4 vezes ao ano;
21. Revisão de acessos lógicos (servidores Intranet) - 4 vezes ao ano;
22. Revisão de acessos lógicos (servidores Internet) - 4 vezes ao ano;
23. Revisão de acessos lógicos (servidores offline) - 4 vezes ao ano;
24. Revisão de acessos lógicos (ativos de rede) - 2 vezes ao ano;
25. Revisão de acessos ao SIGAS - 4 vezes ao ano;
26. Revisão das topologias de rede e mapa de switches - 2 vezes ao ano;
27. Análises de vulnerabilidades - 12 vezes ao ano;
28. Teste do Plano de Continuidade de Negócio (PCN) - 2 vezes ao ano;
29. Encaminhar informações de disponibilidade/ indisponibilidade da infraestrutura das Assinaturas Avançadas para o setor de comunicação Social - 12 vezes ao ano;
30. Limpeza de logs dos scripts dos repositórios das Assinaturas Avançadas - 6 vezes ao ano;
31. Revisão dos documentos, termos e dossiês (Colaboradores, Vigilantes e Coordenadores) - 4 vezes ao ano;
32. Revisão das listas de profissionais (Site Principal (Brasília) e Site Contingência (Florianópolis/SC)) - 4 vezes ao ano;
33. Verificação dos hiperlinks e apontamentos no Site Web do ITI (Documentos principais e Repositórios) - 4 vezes ao ano;
34. Atualizar Formulário de Avaliação de Desempenho da Função - 1 vez ao ano;
35. Revisão das documentações (Manual de Administração do CCD) - 2 vezes ao ano;
36. Revisão das documentações (Análise e Avaliação de Risco) - 2 vezes ao ano;
37. Revisão das documentações (Análise de Risco de Firewall) - 2 vezes ao ano;
38. Revisão das documentações (Plano de Continuidade de Negócio) - 2 vezes ao ano;
39. Revisão das documentações (Manual Gestão de Pessoas) - 4 vezes ao ano;
40. Revisão das documentações (Matriz de Perfil de Acesso) - 2 vezes ao ano;
41. Revisão dos manuais de sistemas e tabela de equipamentos (Wiki) - 4 vezes ao ano.

Obs: durante a vigência contratual esta lista poderá ser ajustada tanto no quantitativo como na frequência, de acordo com necessidades do ITI.

Fim do documento