

ANEXO I - TERMO DE REFERÊNCIA

PROCESSO: 43012.000961/2026-35

UNIDADE INSTRUTORA: GETER – GERÊNCIA DE TERCEIRIZAÇÃO

**UNIDADE DEMANDANTE: GERENCIA DE TECNOLOGIA DA INFORMAÇÃO E
COMUNICAÇÃO - GETIC**

1. DO OBJETO:

1.1. Dispensa de licitação para contratação de empresa na prestação de serviços de mão-de-obra terceirizada, cujos empregados sejam regidos pela Consolidação das Leis Trabalhistas (CLT) e demais legislações vigentes, para a realização de serviços sistemáticos e continuados de Tecnologia da Informação em Fortaleza, de acordo com as especificações e quantitativos previstos neste Termo de Referência.

1.2. Este objeto será realizado através de dispensa de licitação, do tipo MENOR PREÇO, sob o regime de execução indireta: empreitada por preço global.

2. DAS ESPECIFICAÇÕES E QUANTITATIVOS E ESTIMATIVA DO VALOR DA CONTRATAÇÃO

ITEM	ESPECIFICAÇÃO	UNIDADE DE MEDIDA	QUANT	VALOR
1.	Serviços contínuos a serem executados com dedicação exclusiva de mão de obra terceirizada.	UNIDADE	01	R\$ 21.952.513,80

2.1. Especificação Detalhada:

Contratação de empresa na prestação de serviços de mão-de-obra terceirizada, cujos empregados sejam regidos pela Consolidação das Leis Trabalhistas (CLT) e demais legislações vigentes, para a realização de serviços sistemáticos e continuados de Tecnologia da Informação em Fortaleza, de acordo com as especificações e quantitativos previstos neste Termo de Referência.				
Subitens	CATEGORIA(S)	CÓDIGO CBO	CARGA HORARIA SEMANAL	QUANTIDADES
1.1	Analista de Sistemas/Suporte I	2124-05	40 horas	20
1.2	Analista de Sistemas/Suporte II	2124-05	40 horas	15
1.3	Analista de Sistemas/Suporte III	2124-05	40 horas	19
1.4	Analista de Sistemas/Suporte IV	2124-05	40 horas	18
1.5	Gerente de Projetos I	1425-20	40 horas	05
1.6.	Gerente de Projetos II	1425-20	40 horas	05
1.7.	Gerente de Projetos III	1425-20	40 horas	04

1.8.	Gerente de Projetos IV	1425-20	40 horas	04
1.9.	Programador Pleno	3171-10	40 horas	15
1.10.	Suporte Operacional em HardWare e SoftWare	3172-10	40 horas	11
1.11.	Suporte Operacional em HardWare e SoftWare (com EPI)	3172-10	40 horas	08
TOTAL				124

2.1.1. Havendo divergências entre as especificações deste anexo e as do sistema, prevalecerão as deste anexo.

2.2. Descrição e qualificação da categoria:

2.2.1. Descrição das atividades inerentes ao Serviço de Analista de Sistemas/Suporte I:

Requisitos Gerais:

Diploma de graduação em curso de Informática ou equivalente expedido por instituição brasileira reconhecida pelo MEC, ou por instituições estrangeiras devidamente revalidado por órgão competente no Brasil; Especificamente para compor a equipe de Business Intelligence - BI e vinculação impreterivelmente na STI: Diploma de graduação em curso de Matemática ou Estatística em instituição reconhecida pelo MEC; Especificamente para compor a equipe do Georreferenciamento e vinculação impreterivelmente na STI: Diploma de graduação em curso de Geografia em instituição reconhecida pelo MEC.

OUTROS REQUISITOS POR ÁREA DE TIC:

Desenvolvimento	Infraestrutura	Segurança/Governança	
EQUIPE ERP	SISTEMAS OPERACIONAIS	Certificações LPIC	Equipe de governança: Experiência mínima de 2 anos na área de governança de TI; Desejável pós-graduação em governança de TI ou Gestão de TI; Experiência na execução dos processos ITIL; Desejável certificação ITIL.
Desejável experiência em aplicar mudanças/customizações no ERP		Information Security Foundation based on ISO IEC 27001	Equipe de Projetos: Experiência mínima de 2 anos na área de gerenciamento de projetos de TI.
		Certificações Comp TIA Security+	Equipe de Processos: Experiência mínima de 2 anos na área de processos e BPM.
Desejável cursos oficiais da TOTVs referente ao ERP (versão AP11 ou AP12): Configurador, ADVPL, IDE e Integração com Office (Excel e Word) e LibreOffice (Calc e Writer)			Equipe de Prospecção: Experiência mínima de 2 anos na área de TI.

Desenvolvimento	Infraestrutura	Segurança/Governança	
EQUIPE BI	Desejável possuir certificação Microsoft Technology Associate (MTA) ou Microsoft Certified Professional (MCP) ou superior.		
Desejável experiência com suíte Pentaho	Desejável possuir certificação Microsoft Certified System Administrator (MCSA) em Windows 2003 ou Microsoft Certified Technology Specialist (MCTS) em Windows Server ou Microsoft Certified Solutions Associate (MCSA) em Windows Server 2008 ou superior.		
	Desejável possuir certificação Linux Professional Institute Certification Level 1 (LPIC-1).		
	GERENCIAMENTO DE SERVIÇOS		
	Desejável possuir Dynatrace Associate		
	Desejável possuir Zabbix Certified Professional (ZCP)		
	Desejável possuir Certificações em Power BI		
	Desejável possuir Certificações em ferramenta de gerenciamento de serviços ITIL (Service Now, Soft Expert, Service Desk Manager)		
	REDES E SEGURANÇA		



Desenvolvimento	Infraestrutura	Segurança/Governança	
	Desejável possuir certificação Cisco Certified Network Associated (CCNA) ou Cisco Certified Design Associate (CCDA) ou CompTIA Network+;		
	SISTEMAS OPERACIONAIS		
	Desejável possuir certificação Microsoft Technology Associate (MTA) ou Microsoft Certified Professional (MCP) ou superior.		
	Desejável possuir certificação Microsoft Certified System Administrator (MCSA) em Windows 2003 ou Microsoft Certified Technology Specialist (MCTS) em Windows Server ou Microsoft Certified Solutions Associate (MCSA) em Windows Server 2008 ou superior.		
	Desejável possuir certificação Linux Professional Institute Certification Level 1 (LPIC-1).		
	BACKUP/RESTORE e STORAGE		
	Desejável possuir certificações de Backup		
	BANCO DE DADOS		
	Desejável possuir certificação Microsoft Certified Technology Specialist (MCTS) em SQL Server ou Microsoft Certified Solutions Associate		

Desenvolvimento	Infraestrutura	Segurança/Governança	
	(MCSA: SQL Server 2008 ou MCSA: SQL Server 2012) ou superior.		
	Desejável possuir Certificação em banco de dados Oracle (PL/SQL) ou certificação em banco de dados SQL Server (MCP)		
	Desejável possuir OCA – Oracle Certified Associate		
	Desejável possuir Certificações em Power BI		
	Desejável possuir Certificado Profissional de Business Intelligence (CBIP)		
	Desejável possuir Microsoft Certified: Power BI Data Analyst Associate		
	Desejável possuir PostgreSQL Associate Certification		
	DEVOPS		
	Desejável certificações que comprovem conhecimento de Devops		

COMPETÊNCIAS REQUERIDAS POR ÁREA DE TIC:

Desenvolvimento	Infraestrutura	Segurança/Governança	
EQUIPE ERP	TODAS AS EQUIPES	Servidores Linux	Equipe de Projetos e processos de TI
Experiência em desenvolvimento com linguagem ADVPL, IDE Eclipse/VS Code e Integração com Office (Excel e Word) e LibreOffice (Calc e Writer)	Experiência mínima de 3 (três) anos na área de Tecnologia da Informação, preferencial com Infraestrutura	Shell Script	Gerenciamento de projetos
Experiência no ERP em, pelo menos, dois módulos	Experiência mínima de 2 (dois) anos na	Active Directory	PMP

Desenvolvimento	Infraestrutura	Segurança/Governança	
implantados na Cagece	especialidade solicitada		
EQUIPE WEB/MOBILE	Conhecimento na LGPD – Lei Geral de Proteção de Dados	GPO	BPM
Experiência em desenvolvimento backend com tecnologia Java	Desejável conhecimento na metodologia ITIL, COBIT	Conhecimento em servidores Windows	Automação de processos
Experiência em desenvolvimento frontend com frameworks Javascript	EQUIPE SISTEMAS OPERACIONAIS	Conhecimento em Soluções de WAF.	Scrum
Experiência em desenvolvimento de soluções Mobile Android / iOS	Conhecimento de arquitetura de computadores (exemplo: servidores, internet/intranet)	Firewall, IDS/IPS	Kanban
Experiência em UI/UX	Conhecimento no Funcionamento dos sistemas operacionais	Família ISO 27000	Design thinking
Experiência com IDE Eclipse ou VS Code	Experiência e Conhecimento em Linux – Red Hat, Debian e Suse	Conhecimento de sistemas de rede e de protocolos de segurança	Project model canvas
EQUIPE BI	Experiência e Conhecimento em virtualização – VMWare	Conhecimento de programas e de implementação de softwares de segurança da informação	Equipe de prospecção de soluções de TI
Experiência na área de Business Intelligence/ Data Warehouse	Experiência e Conhecimento em Windows Server – AD/DNS/DHCP/R ADIUS/GPO	Conhecimento de infraestrutura de redes e protocolos de comunicação	Levantamento de requisitos
Experiência em modelagem relacional	BACKUP/RESTORE e STORAGE	Inglês técnico (leitura)	Implantação de sistemas;
Experiência em modelagem dimensional	Experiência e Conhecimento em rotinas de Backup (EMC, Network Tape, disco (datadomain) e VEEAM (Nuvem e Exagrid)		Infraestrutura de TI;
Experiência com ferramentas de BI (ETL, Analytics, Dicionário de dados)	Experiência e Conhecimento em rotinas de Backup (EMC, Network Tape, disco		Segurança da informação;

Desenvolvimento	Infraestrutura	Segurança/Governança	
	(datadomain) e VEEAM (Nuvem e Exagrid)		
Experiência com desenvolvimento Python ou R	BANCO DE DADOS		Condução de provas de conceito de soluções de TI.
Experiência com pipeline de fluxos de machine learning	Desejável Conhecimento em bancos (Vertica, Greenplum, MongoDB, NoSQL)		Equipe de Governança de TI
Experiência com construção de dashboards/relatórios	Experiência e Conhecimento em bancos Oracle database In-Memory		ISO 20000.
TODAS AS EQUIPES	Experiência e Conhecimento em bancos postgresQL		Família ISO 27000.
Experiência com modelagem orientada a objetos utilizando UML	Experiência e Conhecimento em estrutura de banco de dados (diagrama entidade-relacionamento)		Cloud(foundation).
Experiência em desenvolvimento utilizando metodologias ágeis	Experiência e Conhecimento na linguagem estruturada SQL		NIST
Experiência com comandos SQL p/ Oracle ou Comandos SQL p/ Postgresql	Experiência e Conhecimento na administração de SGBDs Oracle, PostgreSQL, Microsoft SQL Server, MySQL		Conhecimentos em conceito de gestão de riscos operacionais (avaliação de risco, matriz de risco etc.), gestão de Crises/Gestão de Incidentes;
Experiência com ferramenta de controle de versão GIT	Experiência na área de banco de dados e análise de sistemas		CMMI
Experiência com Test Driven Development (TDD)	Conhecimento em Ferramenta Case de modelagem		Experiência na implantação dos processos ITIL.
Experiência com Ferramenta case de modelagem	Experiência em modelagem orientada a objetos utilizando UML		COBIT
	DEVOPS		ITIL
	Conhecimento e execução de tarefas orientadas à DevOps		Gestão de riscos

Desenvolvimento	Infraestrutura	Segurança/Governança	
	Conhecimento em linguagens de programação (Java, ASP, Delphi)		Família ISO 27000.
	Experiência e Conhecimento em Devops		
	Experiência e Conhecimento em Docker		
	Experiência e Conhecimento em Jenkins		
	Experiência e Conhecimento em Kubernetes		
	Experiência e Conhecimento em Node.js (servidor web completo e robusto para projetos rápidos)		
	GERENCIAMENTO DE SERVIÇOS		
	Experiência e Conhecimento em Administrar e customizar o Zabbix		
	Experiência e Conhecimento em análise de aplicações com datadog e dynatrace		
	Experiência e Conhecimento em criar dahsboards e/ou relatórios		
	Experiência e Conhecimento em ERP Totvs (infraestrutura)		
	Experiência e Conhecimento em Kibana, Elastic Search, Zabbix, Nagios, Power BI, Grafana		
	Experiência e Conhecimento no software Zimbra		
	REDES E SEGURANÇA		



Desenvolvimento	Infraestrutura	Segurança/Governança	
	Conhecimento de infraestrutura de redes e protocolos de comunicação		
	Conhecimento em redes TCP/IP, bem como operação e manutenção em redes wireless, switches, hubs		
	Experiência e Conhecimento como administrador de rede		
	Experiência e Conhecimento em Asterisk		
	Experiência e Conhecimento em F5, NGINX		
	Experiência e Conhecimento em firewall Fortigate, SDWAN, Fortimail e fortianalyser		
	Experiência e Conhecimento em Switches Huawei e 3com		
	Experiência e Conhecimento em Wi-fi Fortinet e Aruba		
	Experiência e Conhecimento em Firewall, IDS/IPS		
	Conhecimento de sistemas de rede e de protocolos de segurança		
	Possuir conhecimento em ferramentas de Antivírus (F-Secure, SEP, etc)		
	Possuir conhecimento em protocolos de roteamento (OSPF, EIGRP, BGP e MPBGP) e LDP, L2VPN, MPLS-TE e MPLS, ATOM, switching,		



Desenvolvimento	Infraestrutura	Segurança/Governança	
	VSS, Multicast, protocolos TCP/IP (versão 4 e 6), Conhecimento em Load Balancer e firewall de aplicação (Cisco CSM/ACE/GSS, PIX, ASA), Citrix Netscaler, A10 AX, F5 Vipron, produtos e ferramentas de gerenciamento e análise de capacidade de rede (Ciscoworks, DCNM, MRTG, TIVOLI, CA Spectrum, Netflow).		
	Possuir conhecimento em firewall Cisco PIX/ASA e CheckPoint (SecurePlatform), VPN GRE, IPSEC, TACACS, RADIUS, ACS, CISCO WORKS e mitigador de ataque (SNORT, ARBOR PeakFlow, IPS SourceFire, Citrix NetScaler, A10 AX, F5 Vipron).		

PRINCIPAIS ATIVIDADES POR ÁREA DE TIC:

Desenvolvimento	Infraestrutura	Segurança/Governança	
Codificação e testes de aplicações	TODAS AS EQUIPES	Realizar atividades técnicas/ operacionais na implantação de controle de Segurança da Informação	Garantir que os processos de TI estejam alinhados com políticas de compliance, normas técnicas e boas práticas do mercado
Manutenção de sistemas	Definição de ferramentas a serem utilizadas	Análise de vulnerabilidades, hardening de servidores, aplicação de checklists, suporte e manutenção em Proxy Squid, Antispam, Firewall e IPS	Otimizar a aplicação de recursos;
Análise de sistemas com levantamento	Manter a documentação do	Monitoramento de conformidade com a	Garantir a entrega de valor da TI para o negócio da empresa

Desenvolvimento	Infraestrutura	Segurança/Governança	
de requisitos, elaboração de diagramas UML (caso de uso, colaboração e classe Estudo de concepção	modelo de dados atualizada e de fácil consulta	PSI (evitar violações da política de segurança)	
• Suporte funcional e operacional de usuários	• Realizar pesquisas e desenvolvimento	• Registro/acompanhamento de incidentes de segurança	• Gerenciamento de projetos de TI
• Propor melhorias nos sistemas implantados, juntamente com área usuária	• Desenhar e redesenhar processos de infraestrutura de Tecnologia da Informação;	• Execução de planos de recuperação de desastres e de continuidade dos negócios da organização para os sistemas de informação	• Automação de processos
• Manter documentação dos sistemas atualizada	• Elaboração de projetos e especificações técnicas De Infraestrutura de TIC	• Gestão de Riscos	• Prospecção de soluções de TI
• Manter documentação das atividades desempenhadas atualizadas	• Definir, desenhar e manter indicadores de performance;	• Gerenciamento de Mudanças no Ambiente de TI	• Definição de métricas e indicadores
• Elaboração do plano de testes	• Automatizar, em plataformas de gerenciamento de processos de negócios, a execução de processos;		• Planejamento estratégico da TI
• Elaboração de casos de testes	• Levantar e registrar dados para promover diagnósticos, sugerir modificações e auxiliar no aperfeiçoamento de métodos e processos de trabalho;		• Gerenciar os riscos de TI
• Treinamento e de implantação sistemas	• Elaborar Instruções Operacionais;		
	• Sugerir melhorias em processos.		
	• Mapear, modelar e analisar processos de infraestrutura		

Desenvolvimento	Infraestrutura	Segurança/Governança	
	de Tecnologia da Informação;		
	Garantir o atendimento conforme SLA e priorização		
	Realizar Análise de desempenho do ambiente e garantir as correções ou melhorias		
	EQUIPE SISTEMAS OPERACIONAIS		
	Elaboração de projetos que envolvam as plataformas RISC e CISC		
	Instalação e suporte nos ambientes operacionais Windows e Linux		
	Administração e Manutenção de servidores com os sistemas operacional Linux RedHat, com no mínimo um Cluster RedHat		
	Administração e Manutenção de servidores com os sistemas operacional Microsoft Windows Server, tendo no ambiente no mínimo um Cluster Microsoft, com dois ou mais nós em cada cluster		
	Suporte e manutenção de servidores e data center, planejar capacidade e desenvolve projetos de melhorias dos serviços corporativos. Realiza criação de usuários e manutenção de		

Desenvolvimento	Infraestrutura	Segurança/Governança	
	grupos para concessão de privilégios com permissão de acesso		
	BACKUP/RESTORE e STORAGE		
	Definição das rotinas de backup e restore dos dados da Companhia		
	Definir padrão de documentação e armazenamento dos dados		
	BANCO DE DADOS		
	Criação, manutenção e controle dos SGBDs da Companhia		
	Manutenção do projeto de Data Warehouse		
	Administração e Manutenção de SGBD		
	DEVOPS		
	Avaliar solicitações de Desenvolvimento de Sistemas		
	REDES E SEGURANÇA		
	Suporte e manutenção de switches, roteadores, núcleo e data center, planeja capacidade e desenvolve projetos de melhorias dos serviços corporativos.		
	Suporte a redes de computadores com ativos de rede (switches, roteadores etc.)		

2.2.2. Descrição das atividades inerentes ao Serviço de Analista de Sistemas/Suporte II:



Requisitos Gerais:

Diploma de graduação em curso de Informática ou equivalente expedido por instituição brasileira reconhecida pelo MEC, ou por instituições estrangeiras devidamente revalidado por órgão competente no Brasil; Especificamente para compor a equipe de Business Intelligence - BI e vinculação impreterivelmente na STI: Diploma de graduação em curso de Matemática ou Estatística em instituição reconhecida pelo MEC; Especificamente para compor a equipe do Georreferenciamento e vinculação impreterivelmente na STI: Diploma de graduação em curso de Geografia em instituição reconhecida pelo MEC.

OUTROS REQUISITOS POR ÁREA DE TIC:

Desenvolvimento	Infraestrutura	Segurança/Governança	
EQUIPE ERP	SISTEMAS OPERACIONAIS	Experiência de no mínimo 04 anos em da segurança Informação	Equipe de governança: Experiência mínima de 3 anos na área de governança de TI; Desejável pós-graduação em governança de TI ou Gestão de TI; Experiência na execução dos processos ITIL; Desejável certificação ITIL.
Desejável experiência em manutenção de infraestrutura de aplicação do ERP	Desejável possuir certificação Microsoft Technology Associate (MTA) ou Microsoft Certified Professional (MCP) ou superior.	Certificações LPIC	Equipe de Projetos: Experiência mínima de 3 anos na área de gerenciamento de projetos de TI. Desejável pós-graduação na área de gerenciamento de projetos ou certificação PMP.
Desejável experiência em aplicar mudanças/customiz ações no ERP	Desejável possuir certificação Microsoft Certified System Administrator (MCSA) em Windows 2003 ou Microsoft Certified Technology Specialist (MCTS) em Windows Server ou Microsoft Certified Solutions Associate (MCSA) em Windows Server 2008 ou superior.	Certificações Comp TIA Security+	Equipe de Processos: Experiência mínima de 3 anos na área de processos e BPM.
Desejável cursos oficiais da TOTVs referente ao ERP (versão AP11 ou AP12): Configurador, ADVPL, IDE e Integração com Office (Excel e	Desejável possuir certificação Microsoft Certified Systems Engineer (MCSE) em Windows 2003 ou Microsoft Certified IT Professional (MCITP): Enterprise	Information Security Foundation based on ISO IEC 27001	Equipe de Prospecção: Experiência mínima de 3 anos na área de TI.

Desenvolvimento	Infraestrutura	Segurança/Governança	
Word) e LibreOffice (Calc e Writer)	Administrator ou Microsoft Certified Solutions Expert (MCSE: Server Infrastructure).		
EQUIPE BI	Desejável possuir certificação Linux Professional Institute Certification Level 2 (LPIC-2).	CompTIA Cybersecurity Analyst (CSA +)	
Desejável experiência com suíte Pentaho	Desejável possuir certificação Linux Professional Institute Certification Level 1 (LPIC-1).	Especialização em Segurança da Informação	
Desejável experiência com base colunar e/ou noSQL	Desejável possuir certificação VMware Certified Professional 5 – Data Center Virtualization (VCP5-DCV) ou superior.		
Desejável experiência com desenvolvimento Python ou R	BACKUP/RESTORE e STORAGE		
TODAS AS EQUIPES	Desejável possuir certificação Storage Networking Industry Association – SNIA Certified Professional (SCSP) ou superior.		
Desejável experiência como Scrum Master em projetos	Desejável possuir Certificação Dell EMC		
Desejável experiência como PO (Product Owner) em projetos	Desejável possuir Huawei IT HCIA Storage – BSSN Certified Network Associate		
	Desejável possuir Veeam Certified Architect		
	Desejável possuir Veeam Certified Engineer		

Desenvolvimento	Infraestrutura	Segurança/Governança	
	Desejável possuir certificações de Storage		
	Desejável possuir certificações de Backup		
	BANCO DE DADOS		
	Desejável possuir certificação Microsoft Certified Technology Specialist (MCTS) em SQL Server ou Microsoft Certified Solutions Associate (MCSA: SQL Server 2008 ou MCSA: SQL Server 2012) ou superior.		
	Desejável possuir certificação Microsoft IT Professional: Database Administrator ou Microsoft Certified Solutions Expert (MCSE: Data Platform) ou MCSE: Business Intelligence.		
	Desejável possuir Certificação em banco de dados Oracle (PL/SQL) ou certificação em banco de dados SQL Server (MCP)		
	Desejável possuir OCA – Oracle Certified Associate		
	Desejável possuir OCE – Oracle Certified Expert		
	Desejável possuir Certificações em Power BI		
	Desejável possuir Certificado Profissional de Business Intelligence (CBIP)		



Desenvolvimento	Infraestrutura	Segurança/Governança	
	Desejável possuir MCSA: SQL 2016 BI Development		
	Desejável possuir Microsoft Certified: Power BI Data Analyst Associate		
	Desejável possuir Oracle Business Intelligence Foundation Suite 11g Certified Implementation Specialist		
	Desejável possuir OCP – Oracle Certified Professional		
	Desejável possuir PostgreSQL Associate Certification		
	Desejável possuir PostgreSQL Professional Certification		
	DEVOPS		
	Desejável possuir Certificação Docker Certified Associate (DCA)		
	Desejável possuir Certified Kubernetes Administrator (CKA)		
	Desejável possuir Certified Kubernetes Application Developer (CKAD)		
	Desejável possuir DevOps Master		
	Desejável possuir DevOps Professional		
	Desejável possuir Engenheiro Certificado Jenkins (CJE)		
	Desejável possuir Engenheiro DevOps Certificado AWS		

Desenvolvimento	Infraestrutura	Segurança/Governança	
	Desejável possuir Google Professional Cloud DevOps Engineer		
	Desejável possuir Microsoft Certified DevOps Engineer Expert		
	GERENCIAMENTO DE SERVIÇOS		
	Desejável possuir Dynatrace Associate		
	Desejável possuir Zabbix Certified Professional (ZCP)		
	Desejável possuir Certificações em Power BI		
	Desejável possuir Certificações em ferramenta de gerenciamento de serviços ITIL (Service Now, Soft Expert, Service Desk Manager)		
	REDES E SEGURANÇA		
	Desejável possuir certificação Cisco Certified Network Associated (CCNA) ou Cisco Certified Design Associate (CCDA) ou CompTIA Network+;		
	Desejável possuir certificação Cisco Certified Network Professional (CCNP) ou Cisco Certified Design Professional (CCDP) ou Cisco Certified Network Professional in Voice (CCNP Voice) ou Cisco Certified Internetwork Expert (CCIE) ou Cisco Certified Internetwork Professional		



Desenvolvimento	Infraestrutura	Segurança/Governança	
	(CCIP) ou Cisco Certified Network Professional in Service Provider Operations (CCNP Service Provider);		
	Desejável possuir certificação no F-Secure		
	Possuir conhecimento em ferramentas de Antivírus (F-Secure, SEP, etc)		

COMPETÊNCIAS REQUERIDAS POR ÁREA DE TIC:

Desenvolvimento	Infraestrutura	Segurança/Governança	
EQUIPE ERP	TODAS AS EQUIPES	Conhecimento em Servidores Linux	Equipe de Projetos e processos de TI
Experiência em desenvolvimento com linguagem ADVPL, IDE Eclipse/VS Code e Integração com Office (Excel e Word) e LibreOffice (Calc e Writer)	Experiência mínima de 4 (quatro) anos na área de Tecnologia da Informação, preferencial com Infraestrutura	Conhecimento em Desenvolvimento Seguro	Gerenciamento de projetos
Experiência em desenvolvimento de Web services REST	Experiência mínima de 3 (três) anos na especialidade solicitada com o perfil de liderança técnica e Gerenciamento de Projetos de pequeno e médio porte;	Active Directory	PMP
Experiência no ERP em, pelo menos, dois módulos implantados na Cagece	Conhecimento na LGPD – Lei Geral de Proteção de Dados	GPO	BPM
EQUIPE WEB/MOBILE	Desejável conhecimento na metodologia ITIL, COBIT	Squid	Automação de processos
Experiência em desenvolvimento backend com tecnologia Java	EQUIPE SISTEMAS OPERACIONAIS	Apache	Scrum
Experiência em desenvolvimento	Conhecimento de arquitetura de de	Firewall, IDS/IPS	Kanban

Desenvolvimento	Infraestrutura	Segurança/Governança	
frontend com frameworks Javascript	computadores (exemplo: servidores, internet/intranet)		
• Experiência em desenvolvimento de soluções Mobile Android / iOS	• Conhecimento no Funcionamento dos sistemas operacionais	• Syslog	• Design thinking
• Experiência em UI/UX	• Experiência e Conhecimento em Linux – Red Hat, Debian e Suse	• Família ISO 27000	• Project model canvas
• Experiência com IDE Eclipse ou VS Code	• Experiência e Conhecimento em virtualização – VMWare	• ISO 22301	Equipe de prospecção de soluções de TI
• Experiência em configuração de servidor de aplicação Jboss e/ou Tomcat	• Experiência e Conhecimento em Windows Server – AD/DNS/DHCP/R ADIUS/GPO	• Conhecimento de sistemas de rede e de protocolos de segurança	• Levantamento de requisitos
• Experiência no desenvolvimento de apis REST	BACKUP/RESTORE e STORAGE	• Conhecimento de programas e de implementação de softwares de segurança da informação	• Implantação de sistemas;
EQUIPE BI	• Experiência e Conhecimento em rotinas de Backup (EMC, Network Tape, disco (datadomain) e VEEAM (Nuvem e Exagrid)	• Conhecimento de infraestrutura de redes e protocolos de comunicação	• Infraestrutura de TI;
• Experiência na área de Business Intelligence/ Data Warehouse	• Experiência e Conhecimento em Mirror de LUN com Recover Point (Dell EMC, Hwauei)	• Inglês técnico (leitura)	• Segurança da informação;
• Experiência em modelagem relacional	• Experiência e Conhecimento em rotinas de Backup (EMC, Network Tape, disco (datadomain) e VEEAM (Nuvem e Exagrid)	• ITIL	• Condução de provas de conceito de soluções de TI.
• Experiência em modelagem dimensional	• Experiência e Conhecimento em Storage EMC e Huawei	• COBIT	Equipe de Governança de TI
• Experiência com ferramentas de BI (ETL, Analytics, Dicionário de dados)	• Experiência e Conhecimento em Suporte Storage (Subsistema de		• ISO 20000.

Desenvolvimento	Infraestrutura	Segurança/Governança	
	Discos de Alta Performance, Fitoteca, Switches e Rede SAN)		
Experiência com desenvolvimento Python ou R	Experiência e Conhecimento em Switch SAN FC (Dell, Hwauei)		Família ISO 27000.
Experiência com pipeline de fluxos de machine learning	BANCO DE DADOS		Cloud(foundation).
Experiência com otimização de fluxos já construídos	Desejável Conhecimento em bancos (Vertica, Greenplum, MongoDB, NoSQL)		NIST
Experiência com construção de dashboards/relatórios	Experiência e Conhecimento em bancos Oracle database In-Memory		Conhecimentos em conceito de gestão de riscos operacionais (avaliação de risco, matriz de risco etc.), gestão de Crises/Gestão de Incidentes;
Experiência em desenvolvimento de datasets	Experiência e Conhecimento em bancos postgresQL		CMMI
TODAS AS EQUIPES	Experiência e Conhecimento em estrutura de banco de dados (diagrama entidade-relacionamento)		Experiência na implantação dos processos ITIL.
Experiência com modelagem orientada a objetos utilizando UML	Experiência e Conhecimento na linguagem estruturada SQL		LGPD(Foundation).
Experiência em desenvolvimento utilizando metodologias ágeis	Experiência e Conhecimento na administração de SGBDs Oracle, PostgreSQL, Microsoft SQL Server, MySQL		ISO 31000
Experiência com comandos SQL p/ Oracle ou Comandos SQL p/ Postgresql	Experiência na área de banco de dados e análise de sistemas		COBIT
Experiência com ferramenta de controle de versão GIT	Conhecimento em Ferramenta Case de modelagem		ITIL



Desenvolvimento	Infraestrutura	Segurança/Governança	
Experiência com Test Driven Development (TDD)	Conhecimento em Ferramentas ETL e OLAP		Continuidade do negócio
Ferramenta case de modelagem	Experiência em Modelagem orientada a objetos utilizando UML		Gestão de riscos
	DEVOPS		Família ISO 27000.
	Conhecimento e execução de tarefas orientadas à DevOps		
	Conhecimento em linguagens de programação (Java, ASP, Delphi)		
	Experiência e Conhecimento em Devops		
	Experiência e Conhecimento em Docker		
	Experiência e Conhecimento em Jenkins		
	Experiência e Conhecimento em Kubernetes		
	Experiência e Conhecimento em Node.js (servidor web completo e robusto para projetos rápidos)		
	GERENCIAMENTO DE SERVIÇOS		
	Experiência e Conhecimento em Administrar e customizar o Zabbix		
	Experiência e Conhecimento em análise de aplicações com datadog e dynatrace		
	Experiência e Conhecimento em criar dahsboards e/ou relatórios		
	Experiência e Conhecimento em ERP Totvs (infraestrutura)		

Desenvolvimento	Infraestrutura	Segurança/Governança	
	Experiência e Conhecimento em Kibana, Elastic Search, Zabbix, Nagios, Power BI, Grafana		
	Experiência e Conhecimento no software Zimbra		
	REDES E SEGURANÇA		
	Conhecimento de infraestrutura de redes e protocolos de comunicação		
	Conhecimento em redes TCP/IP, bem como operação e manutenção em redes wireless, switches, hubs		
	Conhecimento em Design de circuito		
	Experiência e Conhecimento como administrador de rede		
	Experiência e Conhecimento em Asterisk		
	Experiência e Conhecimento em F5, NGINX		
	Experiência e Conhecimento em firewall Fortigate, SDWAN, Fortimail e fortianalyser		
	Experiência e Conhecimento em Switches Huawei e 3com		
	Experiência e Conhecimento em Wi-fi Fortinet e Aruba		
	Experiência e Conhecimento em Firewall, IDS/IPS		
	Conhecimento de sistemas de rede e de protocolos de segurança		



Desenvolvimento	Infraestrutura	Segurança/Governança	
	Possuir conhecimento em ferramentas de Antivírus (F-Secure, SEP, etc)		
	Possuir conhecimento em protocolos de roteamento (OSPF, EIGRP, BGP e MPBGP) e LDP, L2VPN, MPLS-TE e MPLS, ATOM, switching, VSS, Multicast, protocolos TCP/IP (versão 4 e 6), Conhecimento em Load Balancer e firewall de aplicação (Cisco CSM/ACE/GSS, PIX, ASA), Citrix Netscaler, A10 AX, F5 Vipron, produtos e ferramentas de gerenciamento e análise de capacidade de rede (Ciscoverks, DCNM, MRTG, TIVOLI, CA Spectrum, Netflow).		
	Possuir conhecimento em firewall Cisco PIX/ASA e CheckPoint (SecurePlatform), VPN GRE, IPSEC, TACACS, RADIUS, ACS, CISCO WORKS e mitigador de ataque (SNORT, ARBOR PeakFlow, IPS SourceFire, Citrix NetScaler, A10 AX, F5 Vipron).		

PRINCIPAIS ATIVIDADES POR ÁREA DE TIC:



Desenvolvimento	Infraestrutura	Segurança/Governança	
Codificação e de testes de aplicações	TODAS AS EQUIPES	Realizar atividades técnicas/ operacionais na implantação de controle de Segurança da Informação	Garantir que os processos de TI estejam alinhados com políticas de compliance, normas técnicas e boas práticas do mercado
Manutenção de sistemas	Definição de ferramentas a serem utilizadas	Análise de vulnerabilidades, hardening de servidores, aplicação de checklists, suporte e manutenção em Proxy Squid, Antispam, Firewall e IPS.	Otimizar a aplicação de recursos;
Análise de sistemas com levantamento de requisitos, elaboração de diagramas UML (caso de uso, colaboração, classe, etc) Estudo de concepção	Manter a documentação do modelo de dados atualizada e de fácil consulta	Monitoramento de conformidade com a PSI (evitar violações da política de segurança)	Garantir a entrega de valor da TI para o negócio da empresa
Suporte funcional e operacional de usuários	Realizar pesquisas e desenvolvimento	Registro/ acompanhamento de incidentes de segurança	Gerenciamento de projetos de TI
Propor melhorias nos sistemas implantados, acompanhado da área usuária	Desenhar e redesenhar processos de infraestrutura de Tecnologia da Informação;	Execução de planos de recuperação de desastres e de continuidade dos negócios da organização para os sistemas de informação	Automação de processos
Manter documentação dos sistemas atualizada	Elaboração de projetos e especificações técnicas De Infraestrutura de TIC	Gestão de Riscos	Prospecção de soluções de TI
Manter documentação das atividades desempenhadas atualizadas	Definir, desenhar e manter indicadores de performance;	Gerenciamento de Mudanças no Ambiente de TI	Definição de métricas e indicadores
Elaboração do plano de testes	Automatizar, em plataformas de gerenciamento de processos de negócios, a execução de processos;	Elaboração de projetos técnicos diversos relacionados à segurança da informação	Planejamento estratégico da TI
Elaboração de casos de testes	Levantar e registrar dados para promover diagnósticos, sugerir	Desenvolvimento de pareceres técnicos e outros documentos	Gerenciar os riscos de TI

Desenvolvimento	Infraestrutura	Segurança/Governança	
	modificações e auxiliar no aperfeiçoamento de métodos e processos de trabalho;	relacionados a sua área de atuação	
• Treinamento e de implantação de sistemas	• Elaborar Instruções Operacionais;		
	• Sugerir melhorias em processos.		
	• Mapear, modelar e analisar processos de infraestrutura de Tecnologia da Informação;		
	• Garantir o atendimento conforme SLA e priorização		
	• Realizar Análise de desempenho do ambiente e garantir as correções ou melhorias		
	EQUIPE SISTEMAS OPERACIONAIS		
	• Elaboração de projetos que envolvam as plataformas RISC e CISC		
	• Instalação e suporte nos ambientes operacionais Windows e Linux		
	• Administração e Manutenção de servidores com os sistemas operacional Linux RedHat, com no mínimo um Cluster RedHat		
	• Administração e Manutenção de servidores com os sistemas operacional Microsoft Windows Server, tendo no ambiente no mínimo um Cluster Microsoft, com dois		



Desenvolvimento	Infraestrutura	Segurança/Governança	
	ou mais nós em cada cluster		
	• Suporte e manutenção de servidores e data center, planejar capacidade e desenvolve projetos de melhorias dos serviços corporativos. Realiza criação de usuários e manutenção de grupos para concessão de privilégios com permissão de acesso		
	BACKUP/RESTORE e STORAGE		
	• Definição das rotinas de backup e restore dos dados da Companhia		
	• Definir padrão de documentação e armazenamento dos dados		
	BANCO DE DADOS		
	• Criação, manutenção e controle dos SGBDs da Companhia		
	• Manutenção do projeto de Data Warehouse		
	• Administração e Manutenção de SGBD		
	DEVOPS		
	• Avaliar solicitações de Desenvolvimento de Sistemas		
	REDES E SEGURANÇA		
	• Suporte e manutenção de switches, roteadores, núcleo e data center, planeja capacidade e desenvolve projetos de melhorias dos		



Desenvolvimento	Infraestrutura	Segurança/Governança	
	serviços corporativos.		
	Suporte a redes de computadores com ativos de rede (switches, roteadores etc.)		

2.2.3. Descrição das atividades inerentes ao Serviço de Analista de Sistemas/Suporte III:

REQUISITOS GERAIS POR ÁREA DE TIC:

Diploma de graduação em curso de Informática ou equivalente expedido por instituição brasileira reconhecida pelo MEC, ou por instituições estrangeiras devidamente revalidado por órgão competente no Brasil; Especificamente para compor a equipe de Business Intelligence - BI e vinculação impreterivelmente na STI: Diploma de graduação em curso de Matemática ou Estatística em instituição reconhecida pelo MEC; Especificamente para compor a equipe do Georreferenciamento e vinculação impreterivelmente na STI: Diploma de graduação em curso de Geografia em instituição reconhecida pelo MEC.

OUTROS REQUISITOS POR ÁREA DE TIC:

Desenvolvimento	Infraestrutura	Segurança/Governança	
EQUIPE ERP	SISTEMAS OPERACIONAIS	Experiência de no mínimo 06 anos em da segurança Informação	Equipe de governança: Experiência mínima de 4 anos na área de governança de TI; Desejável pós-graduação em governança de TI ou Gestão de TI; Experiência na implantação dos processos ITIL; Desejável certificação COBIT e ITIL.
Desejável experiência em manutenção de infraestrutura de aplicação do ERP	Desejável possuir certificação Microsoft Technology Associate (MTA) ou Microsoft Certified Professional (MCP) ou superior.	CompTIA Cybersecurity Analyst (CSA +)	Equipe de Projetos: Experiência mínima de 4 anos na área de gerenciamento de projetos de TI. Desejável pós-graduação na área de gerenciamento de projetos ou certificação PMP.
Desejável experiência em aplicar mudanças/customizações no ERP	Desejável possuir certificação Microsoft Certified System Administrator (MCSA) em Windows 2003 ou Microsoft Certified Technology Specialist (MCTS) em Windows Server ou Microsoft Certified Solutions Associate (MCSA) em Windows Server 2008 ou superior.	Certificações CompTIA Security+	Equipe de Processos: Experiência mínima de 4 anos na área de processos e BPM.



Desenvolvimento	Infraestrutura	Segurança/Governança	
Desejável cursos oficiais da TOTVs referente ao ERP (versão AP11 ou AP12): Configurador, ADVPL, IDE e Integração com Office (Excel e Word) e LibreOffice (Calc e Writer)	Desejável possuir certificação Microsoft Certified Systems Engineer (MCSE) em Windows 2003 ou Microsoft Certified IT Professional (MCITP): Enterprise Administrator ou Microsoft Certified Solutions Expert (MCSE: Server Infrastructure).	Information Security Foundation based on ISO IEC 27001	Equipe de Prospecção: Experiência mínima de 4 anos na área de TI.
EQUIPE BI	Desejável possuir certificação Linux Professional Institute Certification Level 2 (LPIC-2).	Certificação LPIC	
Desejável experiência em Machine Learning	Desejável possuir certificação Linux Professional Institute Certification Level 3 (LPIC-3) ou Red Hat Certified System Administrator — RHCSA ou Red Hat Certified Datacenter Specialist – RHCDs ou Red Hat Certified Architect – RHCA.	Certificação CEH	
Desejável experiência com suíte Pentaho	Desejável possuir certificação Linux Professional Institute Certification Level 1 (LPIC-1).	Certificação MCSA ou equivalente	
Desejável experiência com base colunar e/ou noSQL	Desejável possuir certificação VMware Certified Professional 5 – Data Center Virtualization (VCP5-DCV) ou superior.	Especialização em da Segurança Informação	
Desejável experiência com desenvolvimento Python ou R	BACKUP/RESTORE e STORAGE	Especialização em Infraestrutura de redes	
TODAS AS EQUIPES	Desejável possuir certificação Storage Networking Industry Association – SNIA Certified	Certificação em privacidade de dados DPOExin ou equivalente	

Desenvolvimento	Infraestrutura	Segurança/Governança	
	Professional (SCSP) ou superior.		
• Desejável experiência como Scrum Master em projetos	• Desejável possuir Certificação Dell EMC		
• Desejável experiência como PO (Product Owner) em projetos	• Desejável possuir Huawei IT HCIA Storage – BSSN Certified Network Associate		
• Desejável Certificação de Scrum Master	• Desejável possuir Veeam Certified Architect		
	• Desejável possuir Veeam Certified Engineer		
	• Desejável possuir certificações de Storage		
	• Desejável possuir certificações de Backup		
	BANCO DE DADOS		
	• Desejável possuir certificação Microsoft Certified Technology Specialist (MCTS) em SQL Server ou Microsoft Certified Solutions Associate (MCSA: SQL Server 2008 ou MCSA: SQL Server 2012) ou superior.		
	• Desejável possuir certificação Microsoft IT Professional: Database Administrator ou Microsoft Certified Solutions Expert (MCSE: Data Platform) ou MCSE: Business Intelligence.		
	• Desejável possuir Certificação em banco de dados Oracle (PL/SQL) ou certificação em banco de dados SQL Server (MCP)		

Desenvolvimento	Infraestrutura	Segurança/Governança	
	Desejável possuir OCA – Oracle Certified Associate		
	Desejável possuir OCE – Oracle Certified Expert		
	Desejável possuir OCM – Oracle Certified Master		
	Desejável possuir Certificações em Power BI		
	Desejável possuir Certificado Profissional de Business Intelligence (CBIP)		
	Desejável possuir MCSA: SQL 2016 BI Development		
	Desejável possuir Microsoft Certified: Power BI Data Analyst Associate		
	Desejável possuir Oracle Business Intelligence Foundation Suite 11g Certified Implementation Specialist		
	Desejável possuir OCP – Oracle Certified Professional		
	Desejável possuir PostgreSQL Associate Certification		
	Desejável possuir PostgreSQL Professional Certification		
	DEVOPS		
	Desejável possuir Certificação Docker Certified Associate (DCA)		
	Desejável possuir Certified Kubernetes Administrator (CKA)		
	Desejável possuir Certified Kubernetes		



Desenvolvimento	Infraestrutura	Segurança/Governança	
	Application Developer (CKAD)		
	• Desejável possuir DevOps Master		
	• Desejável possuir DevOps Professional		
	• Desejável possuir Engenheiro Certificado Jenkins (CJE)		
	• Desejável possuir Engenheiro DevOps Certificado AWS		
	• Desejável possuir Google Professional Cloud DevOps Engineer		
	• Desejável possuir Microsoft Certified DevOps Engineer Expert		
	GERENCIAMENTO DE SERVIÇOS		
	• Desejável possuir Dynatrace Associate		
	• Desejável possuir Zabbix Certified Professional (ZCP)		
	• Desejável possuir Certificações em Power BI		
	• Desejável possuir Certificações em ferramenta de gerenciamento de serviços ITIL (Service Now, Soft Expert, Service Desk Manager)		
	REDES E SEGURANÇA		
	• Desejável possuir certificação Cisco Certified Network Associated (CCNA) ou Cisco Certified Design Associate (CCDA) ou CompTIA Network+;		
	• Desejável possuir certificação Cisco Certified Network Professional (CCNP) ou Cisco Certified		

Desenvolvimento	Infraestrutura	Segurança/Governança	
	Design Professional (CCDP) ou Cisco Certified Network Professional in Voice (CCNP Voice) ou Cisco Certified Internetwork Expert (CCIE) ou Cisco Certified Internetwork Professional (CCIP) ou Cisco Certified Network Professional in Service Provider Operations (CCNP Service Provider);		
	Desejável possuir certificação no F-Secure		
	Possuir conhecimento em ferramentas de Antivírus (F-Secure, SEP, etc)		

COMPETÊNCIAS REQUERIDAS POR ÁREA DE TIC:

Desenvolvimento	Infraestrutura	Segurança/Governança	
EQUIPE ERP	TODAS AS EQUIPES	Servidores Linux	Equipe de Projetos e processos de TI
Experiência em desenvolvimento com linguagem ADVPL, IDE Eclipse/VS Code e Integração com Office (Excel e Word) e LibreOffice (Calc e Writer)	Experiência mínima de 5 (cinco) anos na área de Tecnologia da Informação, preferencial com Infraestrutura	Shell Script	Gerenciamento de projetos
Experiência em desenvolvimento de Web services REST	Experiência mínima de 4 (quatro) anos na especialidade solicitada com o perfil de liderança técnica e Gerenciamento de Projetos de pequeno e médio porte;	Active Directory	PMP
Experiência no ERP em, pelo menos, módulos implantados na Cagece	Conhecimento na LGPD – Lei Geral de Proteção de Dados	GPO	BPM



Desenvolvimento	Infraestrutura	Segurança/Governança	
EQUIPE WEB/MOBILE	Desejável conhecimento na metodologia ITIL, COBIT	Squid	Automação de processos
Experiência em desenvolvimento backend com tecnologia Java	EQUIPE SISTEMAS OPERACIONAIS	Apache	Scrum
Experiência em desenvolvimento frontend com frameworks Javascript	Conhecimento de arquitetura de computadores (exemplo: servidores, internet/intranet)	Firewall, IDS/IPS	Kanban
Experiência em desenvolvimento de soluções Mobile Android / iOS	Conhecimento no Funcionamento dos sistemas operacionais	Análise de vulnerabilidades	Design thinking
Experiência em UI/UX	Experiência e Conhecimento em Linux – Red Hat, Debian e Suse	Família ISO 27000	Project model canvas
Experiência com ferramentas de testes funcionais	Experiência e Conhecimento em virtualização – VMWare	ISO 22301	Equipe de prospecção de soluções de TI
Experiência com IDE Eclipse ou VS Code	Experiência e Conhecimento em Windows Server – AD/DNS/DHCP/RA DIUS/GPO	ISO 31000	Levantamento de requisitos
Experiência em configuração de servidor de aplicação Jboss e/ou Tomcat	BACKUP/RESTORE e STORAGE	Conhecimento de programas e de implementação de softwares de segurança	Implantação de sistemas;
Experiência no desenvolvimento de apis REST	Experiência e Conhecimento em rotinas de Backup (EMC, Network Tape, disco (datadomain) e VEEAM (Nuvem e Exagrid)	Conhecimento das melhores práticas de desenvolvimento de procedimentos e de infraestrutura de segurança	Infraestrutura de TI;
EQUIPE BI	Experiência e Conhecimento em Mirror de LUN com Recover Point (Dell EMC, Hwauei)	Softwares e ferramentas de segurança da informação	Segurança da informação;
Experiência na área de Business Intelligence/ Data Warehouse	Experiência e Conhecimento em rotinas de Backup (EMC, Network Tape, disco (datadomain) e	Conhecimento de infraestrutura de redes e protocolos de comunicação	Condução de provas de conceito de soluções de TI.

Desenvolvimento	Infraestrutura	Segurança/Governança	
	VEEAM (Nuvem e Exagrid)		
• Experiência em modelagem de relacionamento	• Experiência e Conhecimento em Storage EMC e Huawei	• Inglês técnico (leitura)	Equipe de Governança de TI
• Experiência em modelagem dimensional	• Experiência e Conhecimento em Suporte Storage (Subsistema de Discos de Alta Performance, Fitoteca, Switches e Rede SAN)	• Syslog	• ISO 20000.
• Experiência com ferramentas de BI (ETL, Analytics, Dicionário de dados)	• Experiência e Conhecimento em Switch SAN (Dell, Hwauei) FC	• Gestão de Segurança da Informação	• Família ISO 27000.
• Experiência com desenvolvimento Python ou R	BANCO DE DADOS	• ITIL	• Cloud(foundation).
• Experiência com pipeline de fluxos de machine learning	• Desejável Conhecimento em bancos (Vertica, Greenplum, MongoDB, NoSQL)	• COBIT	• Dev Ops(Foundation).
• Experiência com otimização de fluxos já construídos	• Experiência e Conhecimento em bancos Oracle database In-Memory		• NIST
• Experiência com construção de dashboards/relatórios	• Experiência e Conhecimento em bancos postgresSQL		• Conhecimentos em conceito de gestão de riscos operacionais (avaliação de risco, matriz de risco etc.), gestão de Crises/Gestão de Incidentes;
• Experiência com projetos Machine Learning	• Experiência e Conhecimento em estrutura de banco de dados (diagrama entidade-relacionamento)		• CMMI
• Experiência em desenvolvimento de datasets	• Experiência e Conhecimento na linguagem estruturada SQL		• Experiência na implantação dos processos ITIL.
TODAS AS EQUIPES	• Experiência e Conhecimento na administração de SGBDs Oracle, PostgreSQL, Microsoft SQL Server, MySQL		• LGPD(Foundation).
• Experiência com modelagem	• Experiência na área de banco de dados e análise de sistemas		• ISO 31000

Desenvolvimento	Infraestrutura	Segurança/Governança	
orientada a objetos utilizando UML			
Experiência em desenvolvimento utilizando metodologias ágeis	Conhecimento em Ferramenta Case de modelagem		COBIT
Experiência com comandos SQL p/ Oracle ou Comandos SQL p/ Postgresql	Conhecimento em Ferramentas ETL e OLAP		ITIL
Experiência com ferramenta de controle de versão GIT	Experiência em modelagem orientada a objetos utilizando UML		Continuidade do negócio
Experiência com Test Driven Development (TDD)	DEVOPS		Gestão de riscos
Experiência com ferramenta case de modelagem	Conhecimento e execução de tarefas orientadas à DevOps		Família ISO 27000.
Experiência com DevOps	Conhecimento em linguagens de programação (Java, ASP, Delphi)		Cloud(Cloud computing foundation).
	Experiência e Conhecimento em Devops		Lean IT(Lean IT Foundation).
	Experiência e Conhecimento em Docker		Conhecimento em análise de negócios (BCS Business analysis foundation).
	Experiência e Conhecimento em Jenkins		
	Experiência e Conhecimento em Kubernetes		
	Experiência e Conhecimento em Node.js (servidor web completo e robusto para projetos rápidos)		
	GERENCIAMENTO DE SERVIÇOS		
	Experiência e Conhecimento em Administrar e customizar o Zabbix		
	Experiência e Conhecimento em análise de		

Desenvolvimento	Infraestrutura	Segurança/Governança	
	aplicações com datadog e dynatrace		
	Experiência e Conhecimento em criar dahsboards e/ou relatórios		
	Experiência e Conhecimento em ERP Totvs (infraestrutura)		
	Experiência e Conhecimento em Kibana, Elastic Search, Zabbix, Nagios, Power BI, Grafana		
	Experiência e Conhecimento no software Zimbra		
	REDES E SEGURANÇA		
	Conhecimento de infraestrutura de redes e protocolos de comunicação		
	Conhecimento em redes TCP/IP, bem como operação e manutenção em redes wireless, switches, hubs		
	Conhecimento em Design de circuito		
	Experiência e Conhecimento como administrador de rede		
	Experiência e Conhecimento em Asterisk		
	Experiência e Conhecimento em F5, NGINX		
	Experiência e Conhecimento em firewall Fortigate, SDWAN, Fortimail e fortianalyser		
	Experiência e Conhecimento em Switches Huawei e 3com		
	Experiência e Conhecimento em		



Desenvolvimento	Infraestrutura	Segurança/Governança	
	Wi-fi Fortinet e Aruba		
	Experiência e Conhecimento em Firewall, IDS/IPS		
	Conhecimento de sistemas de rede e de protocolos de segurança		
	Possuir conhecimento em ferramentas de Antivírus (F-Secure, SEP, etc)		
	Possuir conhecimento em protocolos de roteamento (OSPF, EIGRP, BGP e MPBGP) e LDP, L2VPN, MPLS-TE e MPLS, ATOM, switching, VSS, Multicast, protocolos TCP/IP (versão 4 e 6), Conhecimento em Load Balancer e firewall de aplicação (Cisco CSM/ACE/GSS, PIX, ASA), Citrix Netscaler, A10 AX, F5 Vipron, produtos e ferramentas de gerenciamento e análise de capacidade de rede (Ciscoworks, DCNM, MRTG, TIVOLI, CA Spectrum, Netflow).		
	Possuir conhecimento em firewall Cisco PIX/ASA e CheckPoint (SecurePlatform), VPN GRE, IPSEC, TACACS, RADIUS, ACS, CISCO WORKS e mitigador de ataque (SNORT, ARBOR PeakFlow, IPS SourceFire, Citrix NetScaler, A10 AX, F5 Vipron).		

PRINCIPAIS ATIVIDADES POR ÁREA DE TIC:



Desenvolvimento	Infraestrutura	Segurança/Governança	
Codificação e testes de aplicações	TODAS AS EQUIPES	Realizar atividades técnicas/ operacionais na implantação de controle de Segurança da Informação	Garantir que os processos de TI estejam alinhados com políticas de compliance, normas técnicas e boas práticas do mercado
Manutenção de sistemas	Definição de ferramentas a serem utilizadas	Análise de vulnerabilidades, hardening de servidores, aplicação de checklists, suporte e manutenção em Proxy Squid, Antispam, Firewall e IPS	Otimizar a aplicação de recursos;
Análise de sistemas com levantamento de requisitos, elaboração de diagramas UML (caso de uso, colaboração, classe, etc) Estudo de concepção	Manter a documentação do modelo de dados atualizada e de fácil consulta	Monitoramento de conformidade com a PSI (evitar violações da política de segurança)	Garantir a entrega de valor da TI para o negócio da empresa
Suporte funcional e operacional de usuários	Realizar pesquisas e desenvolvimento	Registro/ acompanhamento de incidentes de segurança	Gerenciamento de projetos de TI
Propor melhorias nos sistemas implantados, acompanhado da área usuária	Desenhar e redesenhar processos de infraestrutura de Tecnologia da Informação;	Elaborar planos de recuperação de desastres e de continuidade dos negócios da organização para os sistemas de informação	Automação de processos
Manter documentação dos sistemas atualizada	Elaboração de projetos e especificações técnicas De Infraestrutura de TIC	Planejamento para Continuidade de Negócios e Recuperação de Desastres	Prospecção de soluções de TI
Manter documentação das atividades desempenhadas atualizadas	Definir, desenhar e manter indicadores de performance;	Gestão de Riscos	Definição de métricas e indicadores
Elaboração do plano de testes	Automatizar, em plataformas de gerenciamento de processos de negócios, a execução de processos;		Planejamento estratégico da TI
Elaboração de casos de testes	Levantar e registrar dados para promover diagnósticos, sugerir		Gerenciar os riscos de TI

Desenvolvimento	Infraestrutura	Segurança/Governança	
	modificações e auxiliar no aperfeiçoamento de métodos e processos de trabalho;		
• Treinamento e de implantação de sistemas	• Elaborar Instruções Operacionais;		
	• Sugerir melhorias em processos.		
	• Mapear, modelar e analisar processos de infraestrutura de Tecnologia da Informação;		
	• Garantir o atendimento conforme SLA e priorização		
	• Realizar Análise de desempenho do ambiente e garantir as correções ou melhorias		
	EQUIPE SISTEMAS OPERACIONAIS		
	• Elaboração de projetos que envolvam as plataformas RISC e CISC		
	• Instalação e suporte nos ambientes operacionais Windows e Linux		
	• Administração e Manutenção de servidores com os sistemas operacional Linux RedHat, com no mínimo um Cluster RedHat		
	• Administração e Manutenção de servidores com os sistemas operacional Microsoft Windows Server, tendo no ambiente no mínimo um Cluster Microsoft, com dois ou mais nós em cada cluster		



Desenvolvimento	Infraestrutura	Segurança/Governança	
	Suporte e manutenção de servidores e data center, planejar capacidade e desenvolve projetos de melhorias dos serviços corporativos. Realiza criação de usuários e manutenção de grupos para concessão de privilégios com permissão de acesso		
	BACKUP/RESTORE e STORAGE		
	Definição das rotinas de backup e restore dos dados da Companhia		
	Definir padrão de documentação e armazenamento dos dados		
	BANCO DE DADOS		
	Criação, manutenção e controle dos SGBDs da Companhia		
	Manutenção do projeto de Data Warehouse		
	Administração e Manutenção de SGBD		
	DEVOPS		
	Avaliar solicitações de Desenvolvimento de Sistemas		
	REDES E SEGURANÇA		
	Suporte e manutenção de switches, roteadores, núcleo e data center, planeja capacidade e desenvolve projetos de melhorias dos serviços corporativos.		



Desenvolvimento	Infraestrutura	Segurança/Governança	
	• Suporte a redes de computadores com ativos de rede (switches, roteadores etc.)		

2.2.4. Descrição das atividades inerentes ao Serviço de Analista de Sistemas/Suporte IV:

REQUISITOS GERAIS POR ÁREA DE TIC:

Diploma de graduação em curso de Informática ou equivalente expedido por instituição brasileira reconhecida pelo MEC, ou por instituições estrangeiras devidamente revalidado por órgão competente no Brasil; Especificamente para compor a equipe de Business Intelligence - BI e vinculação impreterivelmente na STI: Diploma de graduação em curso de Matemática ou Estatística em instituição reconhecida pelo MEC; Especificamente para compor a equipe do Georreferenciamento e vinculação impreterivelmente na STI: Diploma de graduação em curso de Geografia em instituição reconhecida pelo MEC.

OUTROS REQUISITOS POR ÁREA DE TIC:

Desenvolvimento	Infraestrutura	Segurança/Governança	
EQUIPE ERP	SISTEMAS OPERACIONAIS	• Experiência de no mínima de 08 anos em da segurança Informação	• Equipe de governança: Experiência mínima de 5 anos na área de governança de TI; Desejável pós-graduação em governança de TI ou Gestão de TI; Experiência na implantação dos processos ITIL; Desejável certificação COBIT e ITIL.
• Experiência em de migração versão do ERP	• Desejável possuir certificação Microsoft Technology Associate (MTA) ou Microsoft Certified Professional (MCP) ou superior.	• Especialização em da Segurança Informação	• Equipe de Projetos: Experiência mínima de 5 anos na área de gerenciamento de projetos de TI.
• Experiência em de manutenção de infraestrutura de aplicação do ERP	• Desejável possuir certificação Microsoft Certified System Administrator (MCSA) em Windows 2003 ou Microsoft Certified Technology Specialist (MCTS) em Windows Server ou Microsoft Certified Solutions Associate (MCSA) em Windows Server 2008 ou superior.	• Especialização em Infraestrutura de redes	• Equipe de Processos: Experiência mínima de 5 anos na área de processos e BPM. Desejável pós-graduação na área de gerenciamento de projetos ou certificação PMP.
• Experiência em aplicar mudanças/customizações no ERP	• Desejável possuir certificação Microsoft Certified Systems Engineer (MCSE) em	• Certificação CISSP OU OSCP	• Equipe de Prospecção: Experiência mínima de 5 anos na área de TI.

Desenvolvimento	Infraestrutura	Segurança/Governança	
	Windows 2003 ou Microsoft Certified IT Professional (MCITP): Enterprise Administrator ou Microsoft Certified Solutions Expert (MCSE: Server Infrastructure).		
Desejável cursos oficiais da TOTVs referente ao ERP (versão AP11 ou AP12): Configurador, ADVPL, IDE e Integração com Office (Excel e Word) e LibreOffice (Calc e Writer)	Desejável possuir certificação Linux Professional Institute Certification Level 2 (LPIC-2).	CompTIA Cybersecurity Analyst (CSA +)	
EQUIPE BI	Desejável possuir certificação Linux Professional Institute Certification Level 3 (LPIC-3) ou Red Hat Certified System Administrator — RHCSA ou Red Hat Certified Datacenter Specialist – RHCDS ou Red Hat Certified Architect – RHCA.	Certificações CompTIA Security+	
Desejável experiência em Machine Learning	Desejável possuir certificação Linux Professional Institute Certification Level 1 (LPIC-1).	Information Security Foundation based on ISO IEC 27001	
Desejável experiência em Big Data	Desejável possuir certificação VMware Certified Professional 5 – Data Center Virtualization (VCP5-DCV) ou superior.	Certificação LPIC	
Desejável experiência com suíte Pentaho	BACKUP/RESTORE e STORAGE	Certificação CEH	
Desejável experiência com base colunar e/ou noSQL	Desejável possuir certificação Storage Networking Industry Association – SNIA Certified	Certificação MCSA ou equivalente	

Desenvolvimento	Infraestrutura	Segurança/Governança	
	Professional (SCSP) ou superior.		
Desejável experiência com desenvolvimento Python ou R	Desejável possuir Certificação Dell EMC	Certificação em privacidade de dados DPOExin ou equivalente	
Desejável experiência com pipeline de fluxos de machine learning	Desejável possuir Huawei IT HCIA Storage – BSSN Certified Network Associate		
Desejável experiência com projetos Machine Learning	Desejável possuir Veeam Certified Architect		
Desejável experiência em customização de catálogo Data Lake	Desejável possuir Veeam Certified Engineer		
TODAS AS EQUIPES	Desejável possuir certificações de Storage		
Desejável experiência com liderança de equipe	Desejável possuir certificações de Backup		
Desejável experiência como Scrum Master em projetos	BANCO DE DADOS		
Desejável experiência como PO (Product Owner) em projetos	Desejável possuir certificação Microsoft Certified Technology Specialist (MCTS) em SQL Server ou Microsoft Certified Solutions Associate (MCSA: SQL Server 2008 ou MCSA: SQL Server 2012) ou superior.		
Desejável Certificação de Scrum Master	Desejável possuir certificação Microsoft IT Professional: Database Administrator ou Microsoft Certified Solutions Expert (MCSE: Data Platform) ou MCSE: Business Intelligence.		



Desenvolvimento	Infraestrutura	Segurança/Governança	
	Desejável possuir Certificação em banco de dados Oracle (PL/SQL) ou certificação em banco de dados SQL Server (MCP)		
	Desejável possuir OCA – Oracle Certified Associate		
	Desejável possuir OCE – Oracle Certified Expert		
	- Desejável possuir OCM – Oracle Certified Master - Desejável possuir Certificações em Power BI		
	Desejável possuir Certificado Profissional de Business Intelligence (CBIP)		
	Desejável possuir MCSA: SQL 2016 BI Development		
	Desejável possuir Microsoft Certified: Power BI Data Analyst Associate		
	Desejável possuir Oracle Business Intelligence Foundation Suite 11g Certified Implementation Specialist		
	Desejável possuir OCP – Oracle Certified Professional		
	Desejável possuir PostgreSQL Associate Certification		
	Desejável possuir PostgreSQL Professional Certification		
	DEVOPS		
	Desejável possuir Certificação Docker		



Desenvolvimento	Infraestrutura	Segurança/Governança	
	• Certified Associate (DCA)		
	• Desejável possuir Certified Kubernetes Administrator (CKA)		
	• Desejável possuir Certified Kubernetes Application Developer (CKAD)		
	• Desejável possuir DevOps Master		
	• Desejável possuir DevOps Professional		
	• Desejável possuir Engenheiro Certificado Jenkins (CJE)		
	• Desejável possuir Engenheiro DevOps Certificado AWS		
	• Desejável possuir Google Professional Cloud DevOps Engineer		
	• Desejável possuir Microsoft Certified DevOps Engineer Expert		
	GERENCIAMENTO DE SERVIÇOS		
	• Desejável possuir Dynatrace Associate		
	• Desejável possuir Zabbix Certified Professional (ZCP)		
	• Desejável possuir Certificações em Power BI		
	• Desejável possuir Certificações em ferramenta de gerenciamento de serviços ITIL (Service Now, Soft		

Desenvolvimento	Infraestrutura	Segurança/Governança	
	Expert, Service Desk Manager)		
	REDES E SEGURANÇA		
	Desejável possuir certificação Cisco Certified Network Associated (CCNA) ou Cisco Certified Design Associate (CCDA) ou CompTIA Network+;		
	Desejável possuir certificação Cisco Certified Network Professional (CCNP) ou Cisco Certified Design Professional (CCDP) ou Cisco Certified Network Professional in Voice (CCNP Voice) ou Cisco Certified Internetwork Expert (CCIE) ou Cisco Certified Internetwork Professional (CCIP) ou Cisco Certified Network Professional in Service Provider Operations (CCNP Service Provider);		
	Desejável possuir certificação no F-Secure		
	Possuir conhecimento em ferramentas de Antivírus (F-Secure, SEP, etc)		

COMPETÊNCIAS REQUERIDAS POR ÁREA DE TIC:

Desenvolvimento	Infraestrutura	Segurança/Governança	
EQUIPE ERP	TODAS AS EQUIPES	Conhecimento em gestão de Firewalls de aplicação -WAF	Equipe de Projetos e processos de TI
Experiência em desenvolvimento com linguagem ADVPL, IDE Eclipse/VS Code e Integração com	Experiência mínima de 5 (cinco) anos na área de Tecnologia da Informação, preferencial com Infraestrutura	Conhecimento em Gerenciamento de projetos de segurança da informação;	Gerenciamento de projetos

Desenvolvimento	Infraestrutura	Segurança/Governança	
Office (Excel e Word) e LibreOffice (Calc e Writer)			
Experiência em desenvolvimento de Web services REST	Experiência mínima de 5 (cinco) anos na especialidade solicitada com o perfil de liderança técnica e Gerenciamento de Projetos de pequeno e médio porte;	Conhecimento sobre criptografia;	PMP
Experiência no ERP em, pelo menos, dois módulos implantados na Cagece	Conhecimento na LGPD – Lei Geral de Proteção de Dados	Conhecimento em segurança em ambiente de nuvem, pública e privada;	BPM
EQUIPE WEB/MOBILE	Desejável conhecimento na metodologia ITIL, COBIT	Conhecimento em servidores Linux	Automação de processos
Experiência em desenvolvimento backend com tecnologia Java	EQUIPE SISTEMAS OPERACIONAIS	Shell Script	Scrum
Experiência em desenvolvimento frontend com frameworks Javascript	Conhecimento de arquitetura de computadores (exemplo: servidores, internet/intranet)	Active Directory	Kanban
Experiência em desenvolvimento de soluções Mobile Android / iOS	Conhecimento no Funcionamento dos sistemas operacionais	Conhecimento em segurança de active directory	Design thinking
Experiência em UI/UX	Experiência e Conhecimento em Linux – Red Hat, Debian e Suse	Conhecimento sobre soluções de gestão de acesso privilegiado	Project model canvas
Experiência com ferramentas de testes funcionais	Experiência e Conhecimento em virtualização – VMWare	Conhecimento sobre gestão de riscos de segurança da informação	Equipe de prospecção de soluções de TI
Experiência com IDE Eclipse ou VS Code	Experiência e Conhecimento em Windows Server – AD/DNS/DHCP/RA DIUS/GPO	Conhecimento em privacidade dados e leis relacionadas;	Levantamento de requisitos
Experiência em configuração de servidor de aplicação Jboss e/ou Tomcat	BACKUP/RESTORE e STORAGE	Firewall, IDS/IPS	Implantação de sistemas;

Desenvolvimento	Infraestrutura	Segurança/Governança	
Experiência no desenvolvimento de apis REST	Experiência e Conhecimento em rotinas de Backup (EMC, Network Tape, disco (datadomain) e VEEAM (Nuvem e Exagrid)	Análise de vulnerabilidades	Infraestrutura de TI;
Experiência em configuração de projetos Mobile Android / iOS	Experiência e Conhecimento em Mirror de LUN com Recover Point (Dell EMC, Hwauei)	Família ISO 27000	Segurança da informação;
EQUIPE BI	Experiência e Conhecimento em rotinas de Backup (EMC, Network Tape, disco (datadomain) e VEEAM (Nuvem e Exagrid)	ISO 22301	Condução de provas de conceito de soluções de TI.
Experiência na área de Business Intelligence/ Data Warehouse	Experiência e Conhecimento em Storage EMC e Huawei	Conhecimento de programas e de implementação de softwares de segurança	Equipe de Governança de TI
Experiência em modelagem relacional	Experiência e Conhecimento em Suporte Storage (Subsistema de Discos de Alta Performance, Fitoteca, Switches e Rede SAN)	Conhecimento das melhores práticas de desenvolvimento de procedimentos e de infraestrutura de segurança	ISO 20000.
Experiência em modelagem dimensional	Experiência e Conhecimento em Switch SAN FC (Dell, Hwauei)	Softwares e ferramentas de segurança da informação	Família ISO 27000.
Experiência com ferramentas de BI (ETL, Analytics, Dicionário de dados)	BANCO DE DADOS	Conhecimento de infraestrutura de redes e protocolos de comunicação	Cloud(foundation).
Experiência com desenvolvimento Python ou R	Desejável Conhecimento em bancos (Vertica, Greenplum, MongoDB, NoSQL)	Inglês técnico (leitura)	Dev Ops(Foundation).
Experiência com otimização de fluxos já construídos	Experiência e Conhecimento em bancos Oracle database In-Memory	Syslog	NIST
Experiência com construção de dashboards/relatórios	Experiência e Conhecimento em bancos postgresQL	Gestão de Segurança da Informação	Conhecimentos em conceito de gestão de riscos operacionais (avaliação de risco, matriz de risco etc.), gestão de Crises/Gestão de Incidentes;

Desenvolvimento	Infraestrutura	Segurança/Governança	
Experiência em desenvolvimento de datasets	Experiência e Conhecimento em estrutura de banco de dados (diagrama entidade-relacionamento)	ITIL	CMMI
	Experiência e Conhecimento na linguagem estruturada SQL	COBIT	Experiência na implantação dos processos ITIL.
	Experiência e Conhecimento na administração de SGBDs Oracle, PostgreSQL, Microsoft SQL Server, MySQL		LGPD(Foundation).
	Experiência na área de banco de dados e análise de sistemas		ISO 31000
TODAS AS EQUIPES	Conhecimento em Ferramenta Case de modelagem		COBIT
Experiência com modelagem orientada a objetos utilizando UML	Conhecimento em Ferramentas ETL e OLAP		ITIL
Experiência em desenvolvimento utilizando metodologias ágeis	Experiência em Modelagem orientada a objetos utilizando UML		Continuidade do negócio
Experiência com comandos SQL p/ Oracle ou Comandos SQL p/ Postgresql	DEVOPS		Gestão de riscos
Experiência com ferramenta de controle de versão GIT	Conhecimento e execução de tarefas orientadas à DevOps		Liderança técnica de equipe.
Test Driven Development (TDD)	Conhecimento em linguagens de programação (Java, ASP, Delphi)		Família ISO 27000.
Experiência em setup/configuração de ambientes kubernetes	Experiência e Conhecimento em Devops		Cloud(Cloud computiong foundation).
Ferramenta case de modelagem	Experiência e Conhecimento em Docker		Lean IT(Lean IT Foundation).
Experiência com DevOps	Experiência e Conhecimento em Jenkins		Conhecimento em análise de negócios (BCS Business analysis foundation).

Desenvolvimento	Infraestrutura	Segurança/Governança	
	Experiência e Conhecimento em Kubernetes		
	Experiência e Conhecimento em Node.js (servidor web completo e robusto para projetos rápidos)		
	GERENCIAMENTO DE SERVIÇOS		
	Experiência e Conhecimento em Administrar e customizar o Zabbix		
	Experiência e Conhecimento em análise de aplicações com datadog e dynatrace		
	Experiência e Conhecimento em criar dahsboards e/ou relatórios		
	Experiência e Conhecimento em ERP Totvs (infraestrutura)		
	Experiência e Conhecimento em Kibana, Elastic Search, Zabbix, Nagios, Power BI, Grafana		
	Experiência e Conhecimento no software Zimbra		
	REDES E SEGURANÇA		
	Conhecimento de infraestrutura de redes e protocolos de comunicação		
	Conhecimento em redes TCP/IP, bem como operação e manutenção em redes wireless, switches, hubs		
	Conhecimento em Design de circuito		
	Experiência e Conhecimento como administrador de rede		



Desenvolvimento	Infraestrutura	Segurança/Governança	
	Experiência e Conhecimento em Asterisk		
	Experiência e Conhecimento em F5, NGINX		
	Experiência e Conhecimento em firewall Fortigate, SDWAN, Fortimail e fortianalyser		
	Experiência e Conhecimento em Switches Huawei e 3com		
	Experiência e Conhecimento em Wi-fi Fortinet e Aruba		
	Experiência e Conhecimento em Firewall, IDS/IPS		
	Conhecimento de sistemas de rede e de protocolos de segurança		
	Possuir conhecimento em ferramentas de Antivírus (F-Secure, SEP, etc)		
	Possuir conhecimento em protocolos de roteamento (OSPF, EIGRP, BGP e MPBGP) e LDP, L2VPN, MPLS-TE e MPLS, ATOM, switching, VSS, Multicast, protocolos TCP/IP (versão 4 e 6), Conhecimento em Load Balancer e firewall de aplicação (Cisco CSM/ACE/GSS, PIX, ASA), Citrix Netscaler, A10 AX, F5 Vipron, produtos e ferramentas de gerenciamento e análise de capacidade de rede (Ciscoworks, DCNM,		

Desenvolvimento	Infraestrutura	Segurança/Governança	
	MRTG, TIVOLI, CA Spectrum, Netflow).		
	Possuir conhecimento em firewall Cisco PIX/ASA e CheckPoint (SecurePlatform), VPN GRE, IPSEC, TACACS, RADIUS, ACS, CISCO WORKS e mitigador de ataque (SNORT, ARBOR PeakFlow, IPS SourceFire, Citrix NetScaler, A10 AX, F5 Vipron).		

PRINCIPAIS ATIVIDADES POR ÁREA DE TIC:

Desenvolvimento	Infraestrutura	Segurança/Governança	
Codificação e testes de aplicações	TODAS AS EQUIPES	Realizar atividades técnicas/ operacionais na implantação de controle de Segurança da Informação	Garantir que os processos de TI estejam alinhados com políticas de compliance, normas técnicas e boas práticas do mercado
Manutenção de sistemas	Definição de ferramentas a serem utilizadas	Análise de vulnerabilidades, hardening de servidores, aplicação de checklists, suporte e manutenção em Proxy Squid, Antispam, Firewall e IPS	Otimizar a aplicação de recursos;
Análise de sistemas com levantamento de requisitos, elaboração de diagramas UML (caso de uso, colaboração, classe, etc) Estudo de concepção	Manter a documentação do modelo de dados atualizada e de fácil consulta	Monitoramento de conformidade com a PSI (evitar violações da política de segurança)	Garantir a entrega de valor da TI para o negócio da empresa
Suporte funcional e operacional de usuários	Realizar pesquisas e desenvolvimento	Registro/ acompanhamento de incidentes de segurança	Gerenciamento de projetos de TI
Propor melhorias nos sistemas implantados, acompanhado da área usuária	Desenhar e redesenhar processos de infraestrutura de Tecnologia da Informação;	Implantar gestão da Segurança da Infraestrutura	Automação de processos

Desenvolvimento	Infraestrutura	Segurança/Governança	
Manter documentação dos sistemas atualizada	Elaboração de projetos e especificações técnicas De Infraestrutura de TIC	Elaborar projetos de melhoria de TI	Prospecção de soluções de TI
Manter documentação das atividades desempenhadas atualizadas	Definir, desenhar e manter indicadores de performance;	Gerenciar planos de recuperação de desastres e de continuidade dos negócios da organização para os sistemas de informação	Definição de métricas e indicadores
Elaboração do plano de testes	Automatizar, em plataformas de gerenciamento de processos de negócios, a execução de processos;	Gestão de Continuidade de Negócios e Recuperação de Desastres	Planejamento estratégico da TI
Elaboração de casos de testes	Levantar e registrar dados para promover diagnósticos, sugerir modificações e auxiliar no aperfeiçoamento de métodos e processos de trabalho;	Gestão de Riscos	Gerenciar os riscos de TI
Treinamento e de implantação sistemas	Elaborar Instruções Operacionais;	Gerenciamento de Mudanças no Ambiente de TI	Controle de demandas de auditoria interna / externa e prover visibilidade dos planos de ação dos pontos de risco identificados.
Definição de arquitetura solução	Sugerir melhorias em processos.	Elaboração de projetos técnicos diversos relacionados à segurança da informação	Participação no processo de avaliação de fornecedores e prestadores de serviços de TI.
	Mapear, modelar e analisar processos de infraestrutura de Tecnologia da Informação;	Atuação como consultoria interna na sua área de competência	Apoiar no gerenciamento de contratos de TI.
	Garantir o atendimento SLA e priorização	Desenvolvimento de pareceres técnicos e outros documentos relacionados a sua área de atuação	Acompanhar periodicamente as medições de SLA. Conhecimento em ferramentas de gestão da qualidade (PDCA, 5W2H, Pareto e Diagrama de Causa e Efeito);
	Realizar Análise de desempenho do ambiente e garantir as correções ou melhorias		Desenvolver indicadores estratégicos.

Desenvolvimento	Infraestrutura	Segurança/Governança	
	EQUIPE SISTEMAS OPERACIONAIS		Estruturar planos de curto e longo prazo com link na visão e estratégia de negócios;
	Elaboração de projetos que envolvam as plataformas RISC e CISC		Apoiar a equipe de prospecção e aquisição em demandas relacionadas a aquisições de produtos e serviços específicos da TI quando for necessário.
	Instalação e suporte nos ambientes operacionais Windows e Linux		Elaboração de dashboards.
	Administração e Manutenção de servidores com os sistemas operacional Linux RedHat, com no mínimo um Cluster RedHat		
	Administração e Manutenção de servidores com os sistemas operacional Microsoft Windows Server, tendo no ambiente no mínimo um Cluster Microsoft, com dois ou mais nós em cada cluster		
	Suporte e manutenção de servidores e data center, planejar capacidade e desenvolve projetos de melhorias dos serviços corporativos. Realiza criação de usuários e manutenção de grupos para concessão de privilégios com permissão de acesso		
	BACKUP/RESTORE e STORAGE		
	Definição das rotinas de backup e restore dos dados da Companhia		



Desenvolvimento	Infraestrutura	Segurança/Governança	
	Definir padrão de documentação e armazenamento dos dados		
	BANCO DE DADOS		
	Criação, manutenção e controle dos SGBDs da Companhia		
	Manutenção do projeto de Data Warehouse		
	Administração e Manutenção de SGBD		
	DEVOPS		
	Avaliar solicitações de Desenvolvimento de Sistemas		
	REDES E SEGURANÇA		
	Suporte e manutenção de switches, roteadores, núcleo e data center, planeja capacidade e desenvolve projetos de melhorias dos serviços corporativos.		
	Suporte a redes de computadores com ativos de rede (switches, roteadores etc.)		

2.2.5. Descrição das atividades inerentes ao Serviço de Gerente de Projetos I:

Requisitos Gerais:

Diploma de nível superior em instituição reconhecida pelo MEC.

OUTROS REQUISITOS POR ÁREA DE TIC:

Desenvolvimento	Infraestrutura	Segurança/Governança	
EQUIPE ERP	SISTEMAS OPERACIONAIS	Experiencia de no mínimo de 05 anos em segurança da Informação	Equipe de governança: Experiência mínima de 5 anos na área de governança de TI; desejável pós-graduação em governança de TI ou Gestão de TI; Experiência na implantação dos

Desenvolvimento	Infraestrutura	Segurança/Governança	
			processos ITIL; desejável certificação COBIT e ITIL.
Experiência em implantação de ERP	Possuir certificação Microsoft Certified System Administrator (MCSA) em Windows 2003 ou Microsoft Certified Technology Specialist (MCTS) em Windows Server ou Microsoft Certified Solutions Associate (MCSA) em Windows Server 2008 ou superior.	Especialização em Segurança da Informação	Equipe de Projetos: Experiência mínima de 5 anos na área de gerenciamento de projetos de TI.
Experiência em migração de versão do ERP	Desejável possuir certificação Microsoft Certified Systems Engineer (MCSE) em Windows 2003 ou Microsoft Certified IT Professional (MCITP): Enterprise Administrator ou Microsoft Certified Solutions Expert (MCSE: Server Infrastructure).	Especialização em Infraestrutura de redes	Equipe de Processos: Experiência mínima de 5 anos na área de processos e BPM. Desejável pós-graduação na área de gerenciamento de projetos ou certificação PMP.
EQUIPE BI	Possuir certificação Linux Professional Institute Certification Level 2 (LPIC-2).	Especialização em Gerenciamento de Projetos	Equipe de Prospecção: Experiência mínima de 5 anos na área de TI.
Desejável experiência em Machine Learning	Desejável possuir certificação Linux Professional Institute Certification Level 3 (LPIC-3) ou Red Hat Certified System Administrator — RHCSA ou Red Hat Certified Datacenter Specialist — RHCDs ou Red Hat Certified Architect — RHCA.	Certificação CISSP	
Desejável experiência em Big Data	Desejável possuir certificação Linux Professional Institute Certification Level 3 (LPIC-3) ou Red Hat Certified System Administrator — RHCSA ou Red Hat Certified Datacenter Specialist — RHCDs ou Red Hat Certified Architect — RHCA.	Certificação PMP – Project Management Professional (desejável)	

Desenvolvimento	Infraestrutura	Segurança/Governança	
Desejável experiência com desenvolvimento Python ou R	Possuir certificação Linux Professional Institute Certification Level 1 (LPIC-1).	Certificação Scrum Master	
TODAS AS EQUIPES	Desejável possuir certificação VMware Certified Professional 5 – Data Center Virtualization (VCP5-DCV) ou superior.	Certificação CEH	
Experiência com liderança de equipe	BACKUP/RESTORE e STORAGE	CompTIA Cybersecurity Analyst (CSA +)	
Desejável experiência como Scrum Master em projetos	Desejável possuir certificação Storage Networking Industry Association – SNIA Certified Professional (SCSP) ou superior.	Certificações LPIC	
Desejável Certificação PMP Project Management Professional ou Especialização em Gerenciamento de Projetos	Desejável possuir Certificação Dell EMC	Certificações CompTIA Security+	
Desejável Certificação de Scrum Master	Desejável possuir Huawei IT HCIA Storage – BSSN Certified Network Associate	Information Security Foundation based on ISO IEC 27001	
	Desejável possuir Veeam Certified Architect	Certificação CCNA ou equivalente	
	Desejável possuir Veeam Certified Engineer	Certificação em privacidade de dados DPOEXIN ou equivalente;	
	Desejável possuir certificações de Storage	Certificação Microsoft Certified Systems Administrator	
	Desejável possuir certificações de Backup	Certificação COBIT	
	BANCO DE DADOS	Certificação ITIL	
	Possuir certificação Microsoft Certified Technology Specialist (MCTS) em SQL Server ou Microsoft Certified Solutions Associate (MCSA: SQL Server 2008 ou MCSA: SQL Server 2012) ou superior.		

Desenvolvimento	Infraestrutura	Segurança/Governança	
	Desejável possuir certificação Microsoft IT Professional: Database Administrator ou Microsoft Certified Solutions Expert (MCSE: Data Platform) ou MCSE: Business Intelligence.		
	Desejável possuir Certificação em banco de dados Oracle (PL/SQL) ou certificação em banco de dados SQL Server (MCP)		
	Possuir OCA – Oracle Certified Associate		
	Desejável possuir OCE – Oracle Certified Expert		
	Desejável possuir OCM – Oracle Certified Master		
	Desejável possuir Certificações em Power BI		
	Desejável possuir Certificado Profissional de Business Intelligence (CBIP)		
	Desejável possuir MCSA: SQL 2016 BI Development		
	Desejável possuir Microsoft Certified: Power BI Data Analyst Associate		
	Desejável possuir Oracle Business Intelligence Foundation Suite 11g Certified Implementation Specialist		
	Possuir OCP – Oracle Certified Professional		
	Possuir PostgreSQL Associate Certification		
	Possuir certificação PostgreSQL Professional Certification		
	DEVOPS		



Desenvolvimento	Infraestrutura	Segurança/Governança	
	Possuir Certificação Docker Certified Associate (DCA)		
	Possuir Certified Kubernetes Administrator (CKA)		
	Desejável possuir Certified Kubernetes Application Developer (CKAD)		
	Desejável possuir DevOps Master		
	Possuir DevOps Professional		
	Desejável possuir Engenheiro Certificado Jenkins (CJE)		
	Desejável possuir Engenheiro DevOps Certificado AWS		
	Desejável possuir Google Professional Cloud DevOps Engineer		
	Desejável possuir Microsoft Certified DevOps Engineer Expert		
	GERENCIAMENTO DE SERVIÇOS		
	Desejável possuir Dynatrace Associate		
	Desejável possuir Zabbix Certified Professional (ZCP) ou ferramentas de monitoramento similares		
	Desejável possuir Certificações em Power BI		
	Desejável possuir Certificações em ferramenta de gerenciamento de serviços ITIL (Service Now, Soft Expert, Service Desk Manager)		
	REDES E SEGURANÇA		
	Possuir certificação Cisco Certified Network Associated (CCNA) ou Cisco		

Desenvolvimento	Infraestrutura	Segurança/Governança	
	Certified Design Associate (CCDA) ou CompTIA Network+;		
	Desejável possuir certificação Cisco Certified Network Professional (CCNP) ou Cisco Certified Design Professional (CCDP) ou Cisco Certified Network Professional in Voice (CCNP Voice) ou Cisco Certified Internetwork Expert (CCIE) ou Cisco Certified Internetwork Professional (CCIP) ou Cisco Certified Network Professional in Service Provider Operations (CCNP Service Provider);		
	Desejável possuir certificação no F-Secure		

COMPETÊNCIAS REQUERIDAS POR ÁREA DE TIC:

Desenvolvimento	Infraestrutura	Segurança/Governança	
EQUIPE BI	TODAS AS EQUIPES	Conhecimento em Gestão e análise de vulnerabilidades;	Equipe de Projetos e processos de TI
Experiência na área de Business Intelligence/ Data Warehouse	Experiência mínima de 5 (cinco) anos na área de Tecnologia da Informação, preferencial com Infraestrutura	Conhecimento em Gestão de Segurança da Informação;	Gerenciamento de projetos
Experiência com projetos Machine Learning	Experiência mínima de 2 (três) anos na especialidade solicitada com o perfil de liderança técnica e Gerenciamento de Projetos de pequeno e médio porte;	Conhecimento em gestão de Firewalls de aplicação - WAF	PMP
TODAS AS EQUIPES	Conhecimento na LGPD – Lei Geral de Proteção de Dados	Conhecimento em Gerenciamento de projetos de segurança da informação;	BPM
Experiência em gerenciamento de Projetos PMBOK	Desejável conhecimento na metodologia ITIL, COBIT	Conhecimento sobre criptografia;	Automação de processos

Desenvolvimento	Infraestrutura	Segurança/Governança	
Experiência em gerenciamento de projetos – Scrum	EQUIPE SISTEMAS OPERACIONAIS	Conhecimento em segurança em ambiente de nuvem, pública e privada;	Scrum
Experiência em gerenciamento de equipe	Conhecimento básico de arquitetura de computadores (exemplo: servidores, internet/intranet)	Conhecimento sobre soluções de backup corporativo;	Kanban
	Conhecimento no Funcionamento dos sistemas operacionais	Conhecimento sobre soluções de gestão de acesso privilegiado	Design thinking
	Experiência e Conhecimento em Linux – Red Hat, Debian e Suse	Conhecimento sobre gestão de riscos de segurança da informação	Project model canvas
	Experiência e Conhecimento em virtualização – VMWare	Conhecimento em privacidade dados e leis relacionadas;	Equipe de prospecção de soluções de TI
	Experiência e Conhecimento em Windows Server – AD/DNS/DHCP/RADI US/GPO	Conhecimento em soluções de desenvolvimento Seguro;	Levantamento de requisitos
	BACKUP/RESTORE e STORAGE	Conhecimento em gestão de Logs;	Implantação de sistemas;
	Experiência e Conhecimento em rotinas de Backup (EMC, Network Tape, disco (datadomain) e VEEAM (Nuvem e Exagrid)	Conhecimento em administração de Firewall;	Infraestrutura de TI;
	Experiência e Conhecimento em Switch SAN FC (Dell, Hwauei)	Conhecimento em IDS/IPS;	Segurança da informação;
	Experiência e Conhecimento em rotinas de Backup (EMC, Network Tape, disco (datadomain) e VEEAM (Nuvem e Exagrid)	Conhecimento sobre os riscos elencados pela OWASP;	Condução de provas de conceito de soluções de TI.
	Experiência e Conhecimento em Storage EMC e Huawei	Conhecimento sobre a Família ISO 27000;	Equipe de Governança de TI
	Experiência e Conhecimento em Suporte Storage (Subsistema de Discos de Alta Performance, Fitoteca, Switches e Rede SAN)	Conhecimento sobre a ISO 22301;	ISO 20000.

Desenvolvimento	Infraestrutura	Segurança/Governança	
	Experiência e Conhecimento em Mirror de LUN com Recover Point (Dell EMC, Hwauei)	Conhecimento de programas e de implementação de softwares de segurança;	Família ISO 27000.
	BANCO DE DADOS	Conhecimento das melhores práticas de desenvolvimento de procedimentos e de infraestrutura de segurança;	Cloud(foundation).
	Desejável Conhecimento em bancos (Vertica, Greenplum, MongoDB, NoSQL)	Softwares e ferramentas de segurança da informação;	Dev Ops(Foundation).
	Experiência e Conhecimento em bancos Oracle database In-Memory	Conhecimento de infraestrutura de redes e protocolos de comunicação;	NIST
	Experiência e Conhecimento em bancos postgresQL	Inglês intermediário;	Conhecimentos em conceito de gestão de riscos operacionais (avaliação de risco, matriz de risco etc.), gestão de Crises/Gestão de Incidentes;
	Experiência e Conhecimento em estrutura de banco de dados (diagrama entidade-relacionamento)		CMMI
	Experiência e Conhecimento na linguagem estruturada SQL		Experiência na implantação dos processos ITIL.
	Experiência e Conhecimento na administração de SGBDs Oracle, PostgreSQL, Microsoft SQL Server, MySQL		LGPD(Foundation).
	Experiência na área de banco de dados e análise de sistemas		ISO 31000
	Conhecimento em Ferramenta Case de modelagem		COBIT
	Conhecimento em Ferramentas ETL e OLAP		ITIL
	Experiência em Modelagem orientada a objetos utilizando UML		Continuidade do negócio

Desenvolvimento	Infraestrutura	Segurança/Governança	
	DEVOPS		Gestão de riscos
	Conhecimento e execução de tarefas orientadas à DevOps		Liderança técnica de equipe.
	Conhecimento em linguagens de programação (Java, ASP, Delphi)		Família ISO 27000.
	Experiência e Conhecimento em Devops		Cloud(Cloud computing foundation).
	Experiência e Conhecimento em Docker		Lean IT(Lean IT Foundation).
	Experiência e Conhecimento em Jenkins		Conhecimento em análise de negócios (BCS Business analysis foundation).
	Experiência e Conhecimento em Kubernetes		
	Experiência e Conhecimento em Node.js (servidor web completo e robusto para projetos rápidos)		
	GERENCIAMENTO DE SERVIÇOS		
	Experiência e Conhecimento em Administrar e customizar o Zabbix		
	Experiência e Conhecimento em análise de aplicações com datadog e dynatrace		
	Experiência e Conhecimento em criar dahsboards e/ou relatórios		
	Experiência e Conhecimento em ERP Totvs (infraestrutura)		
	Experiência e Conhecimento em Kibana, Elastic Search, Zabbix, Nagios, Power BI, Grafana		
	Experiência e Conhecimento no software Zimbra		
	REDES E SEGURANÇA		



Desenvolvimento	Infraestrutura	Segurança/Governança	
	Conhecimento de infraestrutura de redes e protocolos de comunicação		
	Conhecimento em redes TCP/IP, bem como operação e manutenção em redes wireless, switches, hubs		
	Conhecimento em Design de circuito		
	Experiência e Conhecimento como administrador de rede		
	Experiência e Conhecimento em Asterisk		
	Experiência e Conhecimento em F5, NGINX		
	Experiência e Conhecimento em firewall Fortigate, SDWAN, Fortimail e fortianalyser		
	Experiência e Conhecimento em Switches Huawei e 3com		
	Experiência e Conhecimento em Wi-fi Fortinet e Aruba		
	Experiência e Conhecimento em Firewall, IDS/IPS		
	Conhecimento de sistemas de rede e de protocolos de segurança		
	Possuir conhecimento em ferramentas de Antivírus (F-Secure, SEP, etc)		
	Possuir conhecimento em protocolos de roteamento (OSPF, EIGRP, BGP e MPBGP) e LDP, L2VPN, MPLS-TE e MPLS, ATOM, switching, VSS, Multicast, protocolos TCP/IP (versão 4 e 6), Conhecimento em		

Desenvolvimento	Infraestrutura	Segurança/Governança	
	Load Balancer e firewall de aplicação (Cisco CSM/ACE/GSS, PIX, ASA), Citrix Netscaler, A10 AX, F5 Vipron, produtos e ferramentas de gerenciamento e análise de capacidade de rede (Ciscoworks, DCNM, MRTG, TIVOLI, CA Spectrum, Netflow).		
	Possuir conhecimento em firewall Cisco PIX/ASA e CheckPoint (SecurePlatform), VPN GRE, IPSEC, TACACS, RADIUS, ACS, CISCO WORKS e mitigador de ataque (SNORT, ARBOR PeakFlow, IPS SourceFire, Citrix NetScaler, A10 AX, F5 Vipron).		

PRINCIPAIS ATIVIDADES POR ÁREA DE TIC:

Desenvolvimento	Infraestrutura	Segurança/Governança	
Propor melhorias nos sistemas implantados, acompanhado da área usuária	TODAS AS EQUIPES	Identificar, analisar e monitorar os riscos cibernéticos;	Garantir que os processos de TI estejam alinhados com políticas de compliance, normas técnicas e boas práticas do mercado
Manter documentação das atividades desempenhadas atualizadas	Definição de ferramentas a serem utilizadas	Identificar as fragilidades dos controles internos e propor melhorias;	Otimizar a aplicação de recursos;
Liderança técnica de equipe	Manter a documentação do modelo de dados atualizada e de fácil consulta	Acompanhar as auditorias e tratar seus resultados;	Garantir a entrega de valor da TI para o negócio da empresa
Liderar equipe técnica de desenvolvimento	Realizar pesquisas e desenvolvimento	Desenvolver e Gerir Campanhas de Conscientização em segurança da informação;	Gerenciamento de projetos de TI
Gerenciar projetos utilizando metodologias ágeis e/ou PMBOK	Desenhar e redesenhar processos de infraestrutura de Tecnologia da Informação;	Elaborar e manter políticas e normas de segurança da informação;	Automação de processos

Desenvolvimento	Infraestrutura	Segurança/Governança	
Promover reuniões com os interessados do projeto ou do sistema sustentado	Elaboração de projetos e especificações técnicas De Infraestrutura de TIC	Buscar de forma contínua novas tecnologias e ferramentas de suporte à segurança da informação para melhor proteção dos dados e das operações de tecnologia;	Prospecção de soluções de TI
Promover comunicação entre a equipe liderada com as demais	Definir, desenhar e manter indicadores de performance;	Conduzir varreduras de vulnerabilidades no ambiente de Infraestrutura e Aplicações Web.	Definição de métricas e indicadores
Gerenciar as demandas da equipe	Automatizar, em plataformas de gerenciamento de processos de negócios, a execução de processos;	Gerenciar projetos de segurança da informação	Planejamento estratégico da TI
Acompanhar os indicadores de desenvolvimento e qualidade	Levantar e registrar dados para promover diagnósticos, sugerir modificações e auxiliar no aperfeiçoamento de métodos e processos de trabalho;		Gerenciar os riscos de TI
	Elaborar Instruções Operacionais;		Controle de demandas de auditoria interna / externa e prover visibilidade dos planos de ação dos pontos de risco identificados.
	Sugerir melhorias em processos.		Participação no processo de avaliação de fornecedores e prestadores de serviços de TI.
	Mapear, modelar e analisar processos de infraestrutura de Tecnologia da Informação;		Apoiar no gerenciamento de contratos de TI.
	Garantir o atendimento conforme SLA e priorização		Acompanhar periodicamente as medições de SLA. Conhecimento em ferramentas de gestão da qualidade (PDCA, 5W2H, Pareto e Diagrama de Causa e Efeito);
	Realizar Análise de desempenho do ambiente e garantir as correções ou melhorias		Desenvolver indicadores estratégicos.
	EQUIPE SISTEMAS OPERACIONAIS		Estruturar planos de curto e longo prazo com link na

Desenvolvimento	Infraestrutura	Segurança/Governança	
			visão e estratégia de negócios;
	Elaboração de projetos que envolvam as plataformas RISC e CISC		Apoiar a equipe de prospecção e aquisição em demandas relacionadas a aquisições de produtos e serviços específicos da TI quando for necessário.
	Instalação e suporte nos ambientes operacionais Windows e Linux		Elaboração de dashboards.
	Administração e Manutenção de servidores com os sistemas operacional Linux RedHat, com no mínimo um Cluster RedHat		
	Administração e Manutenção de servidores com os sistemas operacional Microsoft Windows Server, tendo no ambiente no mínimo um Cluster Microsoft, com dois ou mais nós em cada cluster		
	Suporte e manutenção de servidores e data center, planejar capacidade e desenvolve projetos de melhorias dos serviços corporativos. Realiza criação de usuários e manutenção de grupos para concessão de privilégios com permissão de acesso		
	Implantar servidores, incluindo configuração de clusters para alta disponibilidade com acompanhamento e cumprimento das políticas dos recursos computacionais.		
	BACKUP/RESTORE e STORAGE		
	Definição das rotinas de backup e restore dos dados da Companhia		



Desenvolvimento	Infraestrutura	Segurança/Governança	
	Definir padrão de documentação e armazenamento dos dados		
	BANCO DE DADOS		
	Criação, manutenção e controle dos SGBDs da Companhia		
	Manutenção do projeto de Data Warehouse		
	Administração e Manutenção de SGBD		
	DEVOPS		
	Avaliar solicitações de Desenvolvimento de Sistemas		
	REDES E SEGURANÇA		
	Suporte e manutenção de switches, roteadores, núcleo e data center, planeja capacidade e desenvolve projetos de melhorias dos serviços corporativos.		
	Suporte a redes de computadores com ativos de rede (switches, roteadores etc.)		

2.2.6. Descrição das atividades inerentes ao Serviço de Gerente de Projetos II:

Requisitos Gerais:

Diploma de nível superior em instituição reconhecida pelo MEC.

OUTROS REQUISITOS POR ÁREA DE TIC:

Desenvolvimento	Infraestrutura	Segurança/Governança	
EQUIPE ERP	SISTEMAS OPERACIONAIS	Experiencia de no mínimo de 07 anos em segurança da Informação	Equipe de governança: Experiência mínima de 6 anos na área de governança de TI; Desejável pós-graduação em governança de TI ou Gestão de TI; Experiência na implantação dos processos ITIL; Desejável certificação COBIT e ITIL.

Desenvolvimento	Infraestrutura	Segurança/Governança	
Experiência em implantação de ERP	Possuir certificação Microsoft Certified System Administrator (MCSA) em Windows 2003 ou Microsoft Certified Technology Specialist (MCTS) em Windows Server ou Microsoft Certified Solutions Associate (MCSA) em Windows Server 2008 ou superior.	Especialização em Segurança da Informação	Equipe de Projetos: Experiência mínima de 6 anos na área de gerenciamento de projetos de TI.
Experiência em migração de versão do ERP	Desejável possuir certificação Microsoft Certified Systems Engineer (MCSE) em Windows 2003 ou Microsoft Certified IT Professional (MCITP): Enterprise Administrator ou Microsoft Certified Solutions Expert (MCSE: Server Infrastructure).	Especialização em Infraestrutura de redes	Equipe de Processos: Experiência mínima de 6 anos na área de processos e BPM. Pós-graduação na área de gerenciamento de projetos ou certificação PMP.
EQUIPE BI	Possuir certificação Linux Professional Institute Certification Level 2 (LPIC-2).	Especialização em Gerenciamento de Projetos	Equipe de Prospecção: Experiência mínima de 6 anos na área de TI.
Desejável experiência em Machine Learning	Desejável possuir certificação Linux Professional Institute Certification Level 3 (LPIC-3) ou Red Hat Certified System Administrator — RHCSA ou Red Hat Certified Datacenter Specialist — RHCDSS ou Red Hat Certified Architect — RHCA.	Certificação CISSP	
Desejável experiência em Big Data	Possuir certificação Linux Professional Institute Certification Level 1 (LPIC-1).	Certificação PMP – Project Management Professional (desejável)	
Desejável experiência com desenvolvimento Python ou R	Desejável possuir certificação VMware Certified Professional 5 – Data Center Virtualization (VCP5-DCV) ou superior.	Certificação Scrum Master	
TODAS AS EQUIPES	BACKUP/RESTORE e STORAGE	Certificação em desenvolvimento seguro	

Desenvolvimento	Infraestrutura	Segurança/Governança	
Experiência com liderança de equipe	Desejável possuir certificação Storage Networking Industry Association – SNIA Certified Professional (SCSP) ou superior.	Certificação CEH	
Desejável experiência como Scrum Master em projetos	Desejável possuir Certificação Dell EMC	CompTIA Cybersecurity Analyst (CSA +)	
Desejável Certificação PMP Project Management Professional ou Especialização em Gerenciamento de Projetos	Desejável possuir Huawei IT HCIA Storage – BSSN Certified Network Associate	Certificação de segurança em Cloud Computing	
Desejável Certificação de Scrum Master	Desejável possuir Veeam Certified Architect	Certificações LPIC	
	Desejável possuir Veeam Certified Engineer	Certificações CompTIA Security+	
	Desejável possuir certificações de Storage	Information Security Foundation based on ISO IEC 27001	
	Desejável possuir certificações de Backup	Certificação CCNA ou equivalente	
	BANCO DE DADOS	Certificação em privacidade de dados DPOEXIN ou equivalente;	
	Possuir certificação Microsoft Certified Technology Specialist (MCTS) em SQL Server ou Microsoft Certified Solutions Associate (MCSA: SQL Server 2008 ou MCSA: SQL Server 2012) ou superior.	Certificação Microsoft Certified Systems Administrator	
	Desejável possuir certificação Microsoft IT Professional: Database Administrator ou Microsoft Certified Solutions Expert (MCSE: Data Platform) ou MCSE: Business Intelligence.	Certificação COBIT	

Desenvolvimento	Infraestrutura	Segurança/Governança	
	Desejável possuir Certificação em banco de dados Oracle (PL/SQL) ou certificação em banco de dados SQL Server (MCP)	Certificação ITIL	
	Possuir OCA – Oracle Certified Associate		
	Desejável possuir OCE – Oracle Certified Expert		
	Desejável possuir OCM – Oracle Certified Master		
	Desejável possuir Certificações em Power BI		
	Desejável possuir Certificado Profissional de Business Intelligence (CBIP)		
	Desejável possuir Microsoft Certified: Power BI Data Analyst Associate		
	Desejável possuir Oracle Business Intelligence Foundation Suite 11g Certified Implementation Specialist		
	Possuir OCP – Oracle Certified Professional		
	Possuir PostgreSQL Associate Certification		
	Possuir certificação PostgreSQL Professional Certification		
	DEVOPS		
	Possuir Certificação Docker Certified Associate (DCA)		
	Possuir Certified Kubernetes Administrator (CKA)		
	Desejável possuir Certified Kubernetes Application Developer (CKAD)		
	Desejável possuir DevOps Master		

Desenvolvimento	Infraestrutura	Segurança/Governança	
	Possuir DevOps Professional		
	Desejável possuir Engenheiro Certificado Jenkins (CJE)		
	Desejável possuir Engenheiro DevOps Certificado AWS		
	Desejável possuir Google Professional Cloud DevOps Engineer		
	Desejável possuir Microsoft Certified DevOps Engineer Expert		
	GERENCIAMENTO DE SERVIÇOS		
	Desejável possuir Dynatrace Associate		
	Desejável possuir Zabbix Certified Professional (ZCP) ou ferramentas de monitoramento similares		
	Desejável possuir Certificações em Power BI		
	Desejável possuir Certificações em ferramenta de gerenciamento de serviços ITIL (Service Now, Soft Expert, Service Desk Manager)		
	REDES E SEGURANÇA		
	Possuir certificação Cisco Certified Network Associated (CCNA) ou Cisco Certified Design Associate (CCDA) ou CompTIA Network+;		
	Desejável possuir certificação Cisco Certified Network Professional (CCNP) ou Cisco Certified Design Professional (CCDP) ou Cisco Certified Network Professional in Voice (CCNP Voice) ou		

Desenvolvimento	Infraestrutura	Segurança/Governança	
	Cisco Certified Internetwork Expert (CCIE) ou Cisco Certified Internetwork Professional (CCIP) ou Cisco Certified Network Professional in Service Provider Operations (CCNP Service Provider);		
	Desejável possuir certificação no F-Secure		

COMPETÊNCIAS REQUERIDAS POR ÁREA DE TIC:

Desenvolvimento	Infraestrutura	Segurança/Governança	
EQUIPE BI	TODAS AS EQUIPES	Conhecimento em Gestão e análise de vulnerabilidades;	Equipe de Projetos e processos de TI
Experiência na área de Business Intelligence/ Data Warehouse	Experiência mínima de 7 (sete) anos na área de Tecnologia da Informação, preferencial com Infraestrutura	Conhecimento em Gestão de Segurança da Informação;	Gerenciamento de projetos
Experiência com projetos Machine Learning	Experiência mínima de 4 (quatro) anos na especialidade solicitada com o perfil de liderança técnica e Gerenciamento de Projetos de pequeno e médio porte;	Conhecimento em gestão de Firewalls de aplicação - WAF	PMP
TODAS AS EQUIPES	Conhecimento na LGPD – Lei Geral de Proteção de Dados	Conhecimento em Gerenciamento de projetos de segurança da informação;	BPM
Experiência em gerenciamento de Projetos PMBOK	Desejável conhecimento na metodologia ITIL, COBIT	Conhecimento na execução de testes de invasão;	Automação de processos
Experiência em gerenciamento de projetos – Scrum	EQUIPE SISTEMAS OPERACIONAIS	Conhecimento sobre criptografia;	Scrum
Experiência em gerenciamento de equipe	Administração e Manutenção de servidores com os sistemas operacional Linux RedHat, com no mínimo um Cluster RedHat,	Conhecimento em segurança em ambiente de nuvem, pública e privada;	Kanban
	Conhecimento de arquitetura de computadores	Conhecimento sobre soluções de backup corporativo;	Design thinking

Desenvolvimento	Infraestrutura	Segurança/Governança	
	(exemplo: servidores, internet/intranet)		
	Conhecimento no Funcionamento dos sistemas operacionais	Conhecimento sobre soluções de gestão de acesso privilegiado	Project model canvas
	Experiência e Conhecimento em Linux – Red Hat, Debian e Suse	Conhecimento sobre gestão de riscos de segurança da informação	Equipe de prospecção de soluções de TI
	Experiência e Conhecimento em virtualização – VMWare	Conhecimento em privacidade dados e leis relacionadas;	Levantamento de requisitos
	Experiência e Conhecimento em Windows Server – AD/DNS/DHCP/RADI US/GPO	Conhecimento em soluções de desenvolvimento Seguro;	Implantação de sistemas;
	BACKUP/RESTORE e STORAGE	Conhecimento em gestão de Logs;	Infraestrutura de TI;
	Experiência e Conhecimento em rotinas de Backup (EMC, Network Tape, disco (datadomain) e VEEAM (Nuvem e Exagrid)	Conhecimento em administração de Firewall;	Segurança da informação;
	Experiência e Conhecimento em Mirror de LUN com Recover Point (Dell EMC, Hwauei)	Conhecimento em IDS/IPS;	Condução de provas de conceito de soluções de TI.
	Experiência e Conhecimento em rotinas de Backup (EMC, Network Tape, disco (datadomain) e VEEAM (Nuvem e Exagrid)	Conhecimento sobre os riscos elencados pela OWASP;	Equipe de Governança de TI
	Experiência e Conhecimento em Storage EMC e Huawei	Conhecimento sobre a Família ISO 27000;	ISO 20000
	Experiência e Conhecimento em Suporte Storage (Subsistema de Discos de Alta Performance, Fitoteca, Switches e Rede SAN)	Conhecimento sobre a ISO 22301;	Família ISO 27000.
	Experiência e Conhecimento em Switch SAN FC (Dell, Hwauei)	Conhecimento de programas e de implementação de softwares de segurança;	Cloud(foundation).
	BANCO DE DADOS	Conhecimento das melhores práticas de desenvolvimento de	Dev Ops(Foundation).

Desenvolvimento	Infraestrutura	Segurança/Governança	
		procedimentos e de infraestrutura de segurança;	
	Desejável Conhecimento em bancos (Vertica, Greenplum, MongoDB, NoSQL)	Softwares e ferramentas de segurança da informação;	NIST
	Experiência e Conhecimento em bancos Oracle database In-Memory	Conhecimento de infraestrutura de redes e protocolos de comunicação;	Conhecimentos em conceito de gestão de riscos operacionais (avaliação de risco, matriz de risco etc.), gestão de Crises/Gestão de Incidentes;
	Experiência e Conhecimento em bancos postgresSQL	Inglês intermediário;	CMMI
	Experiência e Conhecimento em estrutura de banco de dados (diagrama entidade-relacionamento)		Experiência na implantação dos processos ITIL.
	Experiência e Conhecimento na linguagem estruturada SQL		LGPD(Foundation).
	Experiência e Conhecimento na administração de SGBDs Oracle, PostgreSQL, Microsoft SQL Server, MySQL		ISO 31000
	Experiência na área de banco de dados e análise de sistemas		COBIT
	Conhecimento em Ferramenta Case de modelagem		ITIL
	Conhecimento em Ferramentas ETL e OLAP		Continuidade do negócio
	Experiência em modelagem orientada a objetos utilizando UML		Gestão de riscos
	DEVOPS		Liderança técnica de equipe.
	Conhecimento e execução de tarefas orientadas à DevOps		Família ISO 27000.
	Conhecimento em linguagens de		Cloud(Cloud computing foundation).

Desenvolvimento	Infraestrutura	Segurança/Governança	
	programação (Java, ASP, Delphi)		
	• Experiência e Conhecimento em Devops		• Lean IT(Lean IT Foundation).
	• Experiência e Conhecimento em Docker		• Conhecimento em análise de negócios (BCS Business analysis foundation).
	• Experiência e Conhecimento em Jenkins		
	• Experiência e Conhecimento em Kubernetes		
	• Experiência e Conhecimento em Node.js (servidor web completo e robusto para projetos rápidos)		
	GERENCIAMENTO DE SERVIÇOS		
	• Experiência e Conhecimento em administrar e customizar o Zabbix		
	• Experiência e Conhecimento em análise de aplicações com datadog e dynatrace		
	• Experiência e Conhecimento em criar dahsboards e/ou relatórios		
	• Experiência e Conhecimento em ERP Totvs (infraestrutura)		
	• Experiência e Conhecimento em Kibana, Elastic Search, Zabbix, Nagios, Power BI, Grafana		
	• Experiência e Conhecimento no software Zimbra		
	REDES E SEGURANÇA		
	• Conhecimento de infraestrutura de redes e protocolos de comunicação		
	• Conhecimento em redes TCP/IP, bem como operação e		

Desenvolvimento	Infraestrutura	Segurança/Governança	
	manutenção em redes wireless, switches, hubs		
	Conhecimento em design de circuito		
	Experiência e Conhecimento como administrador de rede		
	Experiência e Conhecimento em Asterisk		
	Experiência e Conhecimento em F5, NGINX		
	Experiência e Conhecimento em firewall Fortigate, SDWAN, Fortimail e fortianalyser		
	Experiência e Conhecimento em Switches Huawei e 3com		
	Experiência e Conhecimento em Wi-fi Fortinet e Aruba		
	Experiência e Conhecimento em firewall, IDS/IPS		
	Conhecimento de sistemas de rede e de protocolos de segurança		
	Possuir conhecimento em ferramentas de Antivírus (F-Secure, SEP, etc)		
	Possuir conhecimento em protocolos de roteamento (OSPF, EIGRP, BGP e MPBGP) e LDP, L2VPN, MPLS-TE e MPLS, ATOM, switching, VSS, Multicast, protocolos TCP/IP (versão 4 e 6), Conhecimento em Load Balancer e firewall de aplicação (Cisco CSM/ACE/GSS, PIX, ASA), Citrix Netscaler, A10 AX, F5 Vipron, produtos e ferramentas		

Desenvolvimento	Infraestrutura	Segurança/Governança	
	de gerenciamento e análise de capacidade de rede (Ciscoworks, DCNM, MRTG, TIVOLI, CA Spectrum, Netflow).		
	Possuir conhecimento em firewall Cisco PIX/ASA e CheckPoint (SecurePlatform), VPN GRE, IPSEC, TACACS, RADIUS, ACS, CISCO WORKS e mitigador de ataque (SNORT, ARBOR PeakFlow, IPS SourceFire, Citrix NetScaler, A10 AX, F5 Vipron).		

PRINCIPAIS ATIVIDADES POR ÁREA DE TIC:

Desenvolvimento	Infraestrutura	Segurança/Governança	
Propor melhorias nos sistemas implantados, acompanhado da área usuária	TODAS AS EQUIPES	Identificar, analisar e monitorar os riscos cibernéticos;	Garantir que os processos de TI estejam alinhados com políticas de compliance, normas técnicas e boas práticas do mercado
Manter documentação das atividades desempenhadas atualizadas	Definição de ferramentas a serem utilizadas	Identificar as fragilidades dos controles internos e propor melhorias;	Otimizar a aplicação de recursos;
Liderar equipe técnica de desenvolvimento	Manter a documentação do modelo de dados atualizada e de fácil consulta	Acompanhar as auditorias e tratar seus resultados;	Garantir a entrega de valor da TI para o negócio da empresa
Gerenciar projetos utilizando metodologias ágeis e/ou PMBOK	Realizar pesquisas e desenvolvimento	Desenvolver e Gerir Campanhas de Conscientização em segurança da informação;	Gerenciamento de projetos de TI
Promover reuniões com os interessados do projeto ou do sistema sustentado	Desenhar e redesenhar processos de infraestrutura de Tecnologia da Informação;	Elaborar e manter políticas e normas de segurança da informação;	Automação de processos
Promover comunicação entre a equipe	Elaboração de projetos e especificações técnicas De Infraestrutura de TIC	Buscar de forma contínua novas tecnologias e ferramentas de suporte à segurança da informação	Prospecção de soluções de TI

Desenvolvimento	Infraestrutura	Segurança/Governança	
liderada com as demais		para melhor proteção dos dados e das operações de tecnologia;	
• Gerenciar as demandas da equipe	• Definir, desenhar e manter indicadores de performance;	• Conduzir varreduras de vulnerabilidades no ambiente de Infraestrutura e Aplicações Web.	• Definição de métricas e indicadores
• Acompanhar os indicadores de desenvolvimento e qualidade	• Automatizar, em plataformas de gerenciamento de processos de negócios, a execução de processos;	• Dar suporte no desenvolvimento e supervisão de projetos e/ou treinamentos de conscientização dos colaboradores sobre o tema;	• Planejamento estratégico da TI
	• Levantar e registrar dados para promover diagnósticos, sugerir modificações e auxiliar no aperfeiçoamento de métodos e processos de trabalho;	• Analisar os gaps e/ou vulnerabilidades de segurança da informação;	• Gerenciar os riscos de TI
	• Elaborar Instruções Operacionais;	• Dar suporte ao programa de resposta à incidentes de segurança da informação e cibernéticos.	• Controle de demandas de auditoria interna / externa e prover visibilidade dos planos de ação dos pontos de risco identificados.
	• Sugerir melhorias em processos.	• Gerenciar projetos de segurança da informação.	• Participação no processo de avaliação de fornecedores e prestadores de serviços de TI.
	• Mapear, modelar e analisar processos de infraestrutura de Tecnologia da Informação;		• Apoiar no gerenciamento de contratos de TI.
	• Garantir o atendimento conforme SLA e priorização		• Acompanhar periodicamente as medições de SLA. Conhecimento em ferramentas de gestão da qualidade (PDCA, 5W2H, Pareto e Diagrama de Causa e Efeito);
	• Realizar Análise de desempenho do ambiente e garantir as correções ou melhorias		• Desenvolver indicadores estratégicos.
	EQUIPE SISTEMAS OPERACIONAIS		• Estruturar planos de curto e longo prazo com link na visão e estratégia de negócios;
	• Elaboração de projetos que envolvam as plataformas RISC e CISC		• Apoiar a equipe de prospecção e aquisição em demandas relacionadas a aquisições de produtos e

Desenvolvimento	Infraestrutura	Segurança/Governança	
			serviços específicos da TI quando for necessário.
	Instalação e suporte nos ambientes operacionais Windows e Linux		Elaboração de dashboards.
	Administração e Manutenção de servidores com os sistemas operacional Linux RedHat, com no mínimo um Cluster RedHat		
	Administração e Manutenção de servidores com os sistemas operacional Microsoft Windows Server, tendo no ambiente no mínimo um Cluster Microsoft, com dois ou mais nós em cada cluster		
	Suporte e manutenção de servidores e data center, planejar capacidade e desenvolver projetos de melhorias dos serviços corporativos. Realiza criação de usuários e manutenção de grupos para concessão de privilégios com permissão de acesso		
	BACKUP/RESTORE e STORAGE		
	Definição das rotinas de backup e restore dos dados da Companhia		
	Definir padrão de documentação e armazenamento dos dados		
	BANCO DE DADOS		
	Criação, manutenção e controle dos SGBDs da Companhia		
	Manutenção do projeto de Data Warehouse		
	Administração e Manutenção de SGBD		

Desenvolvimento	Infraestrutura	Segurança/Governança	
	DEVOPS		
	Avaliar solicitações de Desenvolvimento de Sistemas		
	REDES E SEGURANÇA		
	Suporte e manutenção de switches, roteadores, núcleo e data center, planeja capacidade e desenvolve projetos de melhorias dos serviços corporativos.		
	Suporte a redes de computadores com ativos de rede (switches, roteadores etc.)		

2.2.7. Descrição das atividades inerentes ao Serviço de Gerente de Projetos III:

Requisitos Gerais:

Diploma de nível superior em instituição reconhecida pelo MEC.

OUTROS REQUISITOS POR ÁREA DE TIC:

Desenvolvimento	Infraestrutura	Segurança/Governança	
EQUIPE ERP	SISTEMAS OPERACIONAIS	Experiência de no mínima de 10 anos em segurança da Informação	Equipe de governança: Experiência mínima de 7 anos na área de governança de TI; Desejável pós-graduação em governança de TI ou Gestão de TI; Experiência na implantação dos processos ITIL; Desejável certificação COBIT e ITIL.
Experiência em implantação de ERP	Possuir Certificação Microsoft Certified System Administrator (MCSA) em Windows 2003 ou Microsoft Certified Technology Specialist (MCTS) em Windows Server ou Microsoft Certified Solutions Associate (MCSA) em Windows Server 2008 ou superior.	Especialização em Segurança da Informação	Equipe de Projetos: Experiência mínima de 7 anos na área de gerenciamento de projetos de TI.
Experiência em migração de versão do ERP	Possuir Certificação Microsoft Certified Systems Engineer	Especialização em Infraestrutura de redes	Equipe de Processos: Experiência mínima de 7 anos na área de processos

Desenvolvimento	Infraestrutura	Segurança/Governança	
	(MCSE) em Windows 2003 ou Microsoft Certified IT Professional (MCITP): Enterprise Administrator ou Microsoft Certified Solutions Expert (MCSE: Server Infrastructure).		e BPM. Pós-graduação na área de gerenciamento de projetos ou certificação PMP.
EQUIPE BI	Possuir Certificação Linux Professional Institute Certification Level 2 (LPIC-2).	Especialização em Gerenciamento de Projetos	Equipe de Prospecção: Experiência mínima de 7 anos na área de TI.
Desejável experiência em Machine Learning	Possuir Certificação Linux Professional Institute Certification Level 3 (LPIC-3) ou Red Hat Certified System Administrator — RHCSA ou Red Hat Certified Datacenter Specialist – RHCDL ou Red Hat Certified Architect – RHCA.	Certificação CISSP	
Desejável experiência em Big Data	Possuir Certificação VMware Certified Professional 5 – Data Center Virtualization (VCP5-DCV) ou superior.	Certificação PMP – Project Management Professional (desejável)	
Desejável experiência com desenvolvimento Python ou R	BACKUP/RESTORE e STORAGE	Certificação em gestão de Riscos PMI-RP ou equivalente	
TODAS AS EQUIPES	Desejável possuir certificação Storage Networking Industry Association – SNIA Certified Professional (SCSP) ou superior.	Certificação Scrum Master	
Experiência com liderança de equipe	Desejável possuir Certificação Dell EMC	Certificação em desenvolvimento seguro	
Desejável experiência como Scrum Master em projetos	Desejável possuir Huawei IT HCIA Storage – BSSN Certified Network Associate	Certificação CEH	
Desejável Certificação PMP Project Management	Desejável possuir Veeam Certified Architect	CompTIA Cybersecurity Analyst (CSA +)	

Desenvolvimento	Infraestrutura	Segurança/Governança	
Professional ou Especialização em Gerenciamento de Projetos			
• Desejável Certificação de Scrum Master	• Desejável possuir Veeam Certified Engineer	• Certificação de segurança em Cloud Computing	
	• Possuir Certificação de escopo de Storage	• Certificações LPIC	
	• Possuir Certificação de escopo de Backup	• Certificações CompTIA Security+	
	BANCO DE DADOS	• Information Security Foundation based on ISO IEC 27001	
	• Possuir certificação Microsoft Certified Technology Specialist (MCTS) em SQL Server ou Microsoft Certified Solutions Associate (MCSA: SQL Server 2008 ou MCSA: SQL Server 2012) ou superior.	• Certificação CCNA ou equivalente	
	• Possuir certificação Microsoft IT Professional: Database Administrator ou Microsoft Certified Solutions Expert (MCSE: Data Platform) ou MCSE: Business Intelligence.	• Certificação em privacidade de dados DPOEXIN ou equivalente;	
	• Possuir Certificação OCE – Oracle Certified Expert	• Certificação Microsoft Certified Systems Administrator	
	• Possuir Certificação OCM – Oracle Certified Master	• Certificação COBIT	
	• Desejável possuir Certificado Profissional de Business Intelligence (CBIP)	• Certificação ITIL	
	• Desejável Possuir MCSA: SQL 2016 BI Development		
	• Desejável possuir Microsoft Certified: Power BI Data Analyst Associate		
	• Possuir Certificação Oracle Business		

Desenvolvimento	Infraestrutura	Segurança/Governança	
	Intelligence Foundation Suite 11g Certified Implementation Specialist		
	• Possuir Certificação PostgreSQL Professional Certification		
	DEVOPS		
	• Possuir Certificação Docker Certified Associate (DCA)		
	• Possuir Certified Kubernetes Administrator (CKA)		
	• Possuir Certified Kubernetes Application Developer (CKAD)		
	• Possuir Certificação DevOps Master		
	• Possuir Certificação DevOps Professional		
	• Desejável possuir Engenheiro Certificado Jenkins (CJE)		
	• Desejável possuir Engenheiro DevOps Certificado AWS		
	• Desejável possuir Google Professional Cloud DevOps Engineer		
	• Desejável possuir Microsoft Certified DevOps Engineer Expert		
	GERENCIAMENTO DE SERVIÇOS		
	• Desejável possuir Dynatrace Associate		
	• Desejável possuir Zabbix Certified Professional (ZCP) ou de ferramentas de escopo de monitoramento		
	• Desejável possuir Certificações em Power BI		
	• Desejável possuir Certificações em ferramenta de gerenciamento de		

Desenvolvimento	Infraestrutura	Segurança/Governança	
	serviços ITIL (Service Now, Soft Expert, Service Desk Manager)		
	REDES E SEGURANÇA		
	Possuir certificação Cisco Certified Network Associated (CCNA) ou Cisco Certified Design Associate (CCDA) ou CompTIA Network+;		
	Possuir certificação Cisco Certified Network Professional (CCNP) ou Cisco Certified Design Professional (CCDP) ou Cisco Certified Network Professional in Voice (CCNP Voice) ou Cisco Certified Internetwork Expert (CCIE) ou Cisco Certified Internetwork Professional (CCIP) ou Cisco Certified Network Professional in Service Provider Operations (CCNP Service Provider);		
	Desejável possuir certificação no F-Secure		

COMPETÊNCIAS REQUERIDAS POR ÁREA DE TIC:

Desenvolvimento	Infraestrutura	Segurança/Governança	
EQUIPE BI	TODAS AS EQUIPES	Conhecimento em Gestão e análise de vulnerabilidades;	Equipe de Projetos e processos de TI
Experiência na área de Business Intelligence/ Data Warehouse	Experiência mínima de 8 (oito) anos na área de Tecnologia da Informação, preferencial com Infraestrutura	Conhecimento em Gestão de Segurança da Informação;	Gerenciamento de projetos
Experiência com projetos Big Data	Experiência mínima de 5 (cinco) anos na especialidade solicitada com o perfil de liderança técnica e Gerenciamento de Projetos de médio e grande porte;	Conhecimento em gestão de Firewalls de aplicação - WAF	PMP

Desenvolvimento	Infraestrutura	Segurança/Governança	
Experiência com projetos Machine Learning	Conhecimento na LGPD – Lei Geral de Proteção de Dados	Conhecimento em Gerenciamento de projetos de segurança da informação;	BPM
TODAS AS EQUIPES	Desejável conhecimento na metodologia ITIL, COBIT	Conhecimento na execução de testes de invasão;	Automação de processos
Experiência em gerenciamento de Projetos PMBOK	EQUIPE SISTEMAS OPERACIONAIS	Conhecimento sobre criptografia;	Scrum
Experiência em gerenciamento de projetos – Scrum	Conhecimento de arquitetura de computadores (exemplo: servidores, internet/intranet)	Conhecimento em segurança em ambiente de nuvem, publica e privada;	Kanban
Experiência em gerenciamento de equipe	Conhecimento no Funcionamento dos sistemas operacionais	Conhecimento sobre soluções de backup corporativo;	Design thinking
	Experiência e Conhecimento em Linux – Red Hat, Debian e Suse	Conhecimento sobre soluções de gestão de acesso privilegiado	Project model canvas
	Experiência e Conhecimento em virtualização – VMWare	Conhecimento sobre gestão de riscos de segurança da informação	Equipe de prospecção de soluções de TI
	Experiência e Conhecimento em Windows Server – AD/DNS/DHCP/RADI US/GPO	Conhecimento em privacidade dados e leis relacionadas;	Levantamento de requisitos
	BACKUP/RESTORE e STORAGE	Conhecimento em soluções de desenvolvimento Seguro;	Implantação de sistemas;
	Experiência e Conhecimento em rotinas de Backup (EMC, Network Tape, disco (datadomain) e VEEAM (Nuvem e Exagrid)	Conhecimento em gestão de Logs;	Infraestrutura de TI;
	Experiência e Conhecimento em Mirror de LUN com Recover Point (Dell EMC, Hwauei)	Conhecimento em administração de Firewall;	Segurança da informação;
	Experiência e Conhecimento em rotinas de Backup (EMC, Network Tape, disco (datadomain) e VEEAM (Nuvem e Exagrid)	Conhecimento em IDS/IPS;	Condução de provas de conceito de soluções de TI.

Desenvolvimento	Infraestrutura	Segurança/Governança	
	Experiência e Conhecimento em Suporte Storage (Subsistema de Discos de Alta Performance, Fitoteca, Switches e Rede SAN)	Conhecimento sobre os riscos elencados pela OWASP;	Equipe de Governança de TI
	Experiência e Conhecimento em Storage EMC e Huawei	Conhecimento sobre a Família ISO 27000;	ISO 20000.
	Experiência e Conhecimento em Switch SAN FC (Dell, Hwauei)	Conhecimento sobre a ISO 22301;	Família ISO 27000.
	BANCO DE DADOS	Conhecimento de programas e de implementação de softwares de segurança;	Cloud(foundation).
	Desejável Conhecimento em bancos (Vertica, Greenplum, MongoDB, NoSQL)	Conhecimento das melhores práticas de desenvolvimento de procedimentos e de infraestrutura de segurança;	Dev Ops(Foundation).
	Experiência e Conhecimento em bancos Oracle database In-Memory	Softwares e ferramentas de segurança da informação;	NIST
	Experiência e Conhecimento em bancos postgresSQL	Conhecimento de infraestrutura de redes e protocolos de comunicação;	Conhecimentos em conceito de gestão de riscos operacionais (avaliação de risco, matriz de risco etc.), gestão de Crises/Gestão de Incidentes;
	Experiência e Conhecimento em estrutura de banco de dados (diagrama entidade-relacionamento)	Inglês intermediário;	CMMI
	Experiência e Conhecimento na linguagem estruturada SQL		Experiência na implantação dos processos ITIL.
	Experiência e Conhecimento na administração de SGBDs Oracle, PostgreSQL, Microsoft SQL Server, MySQL		LGPD(Foundation).
	Experiência na área de banco de dados e análise de sistemas		ISO 31000

Desenvolvimento	Infraestrutura	Segurança/Governança	
	Conhecimento em Ferramenta Case de modelagem		COBIT
	Conhecimento em Ferramentas ETL e OLAP		ITIL
	Experiência em modelagem orientada a objetos utilizando UML		Continuidade do negócio
	DEVOPS		Gestão de riscos
	Conhecimento e execução de tarefas orientadas à DevOps		Liderança técnica de equipe.
	Conhecimento em linguagens de programação (Java, ASP, Delphi)		Família ISO 27000.
	Experiência e Conhecimento em Devops		Cloud(Cloud computing foundation).
	Experiência e Conhecimento em Docker		Lean IT(Lean IT Foundation).
	Experiência e Conhecimento em Jenkins		Conhecimento em análise de negócios (BCS Business analysis foundation).
	Experiência e Conhecimento em Kubernetes		
	Experiência e Conhecimento em Node.js (servidor web completo e robusto para projetos rápidos)		
	GERENCIAMENTO DE SERVIÇOS		
	Experiência e Conhecimento em administrar e customizar o Zabbix		
	Experiência e Conhecimento em análise de aplicações com datadog e dynatrace		
	Experiência e Conhecimento em criar dahsboards e/ou relatórios		
	Experiência e Conhecimento em ERP Totvs (infraestrutura)		

Desenvolvimento	Infraestrutura	Segurança/Governança	
	Experiência e Conhecimento em Kibana, Elastic Search, Zabbix, Nagios, Power BI, Grafana		
	Experiência e Conhecimento no software Zimbra		
	REDES E SEGURANÇA		
	Conhecimento de infraestrutura de redes e protocolos de comunicação		
	Conhecimento em redes TCP/IP, bem como operação e manutenção em redes wireless, switches, hubs		
	Conhecimento em design de circuito		
	Experiência e Conhecimento como administrador de rede		
	Experiência e Conhecimento em Asterisk		
	Experiência e Conhecimento em F5, NGINX		
	Experiência e Conhecimento em firewall Fortigate, SDWAN, Fortimail e fortianalyser		
	Experiência e Conhecimento em Switches Huawei e 3com		
	Experiência e Conhecimento em Wi-fi Fortinet e Aruba		
	Experiência e Conhecimento em Firewall, IDS/IPS		
	Conhecimento de sistemas de rede e de protocolos de segurança		
	Possuir conhecimento em ferramentas de Antivírus (F-Secure, SEP, etc)		



Desenvolvimento	Infraestrutura	Segurança/Governança	
	Possuir conhecimento em protocolos de roteamento (OSPF, EIGRP, BGP e MPBGP) e LDP, L2VPN, MPLS-TE e MPLS, ATOM, switching, VSS, Multicast, protocolos TCP/IP (versão 4 e 6), conhecimento em Load Balancer e firewall de aplicação (Cisco CSM/ACE/GSS, PIX, ASA), Citrix Netscaler, A10 AX, F5 Vipron, produtos e ferramentas de gerenciamento e análise de capacidade de rede (Ciscoworks, DCNM, MRTG, TIVOLI, CA Spectrum, Netflow).		
	Possuir conhecimento em firewall Cisco PIX/ASA e CheckPoint (SecurePlatform), VPN GRE, IPSEC, TACACS, RADIUS, ACS, CISCO WORKS e mitigador de ataque (SNORT, ARBOR PeakFlow, IPS SourceFire, Citrix NetScaler, A10 AX, F5 Vipron).		

PRINCIPAIS ATIVIDADES POR ÁREA DE TIC:

Desenvolvimento	Infraestrutura	Segurança/Governança	
Propor melhorias nos sistemas implantados, acompanhado da área usuária	TODAS AS EQUIPES	Identificar, analisar e monitorar os riscos cibernéticos;	Garantir que os processos de TI estejam alinhados com políticas de compliance, normas técnicas e boas práticas do mercado
Manter documentação das atividades desempenhadas atualizadas	Definição de ferramentas a serem utilizadas	Identificar as fragilidades dos controles internos e propor melhorias;	Otimizar a aplicação de recursos;
Liderar equipe técnica de desenvolvimento	Manter a documentação do modelo de dados atualizada e de fácil consulta	Acompanhar as auditorias e tratar seus resultados;	Garantir a entrega de valor da TI para o negócio da empresa



Desenvolvimento	Infraestrutura	Segurança/Governança	
Gerenciar projetos utilizando metodologias ágeis e/ou PMBOK	Realizar pesquisas e desenvolvimento	Desenvolver e Gerir Campanhas de Conscientização em segurança da informação;	Gerenciamento de projetos de TI
Promover reuniões com os interessados do projeto ou do sistema sustentado	Desenhar e redesenhar processos de infraestrutura de Tecnologia da Informação;	Elaborar e manter políticas e normas de segurança da informação;	Automação de processos
Promover comunicação entre a equipe liderada com as demais	Elaboração de projetos e especificações técnicas De Infraestrutura de TIC	Buscar de forma contínua novas tecnologias e ferramentas de suporte à segurança da informação para melhor proteção dos dados e das operações de tecnologia;	Prospecção de soluções de TI
Gerenciar as demandas da equipe	Definir, desenhar e manter indicadores de performance;	Conduzir varreduras de vulnerabilidades no ambiente de Infraestrutura e Aplicações Web.	Definição de métricas e indicadores
Acompanhar os indicadores de desenvolvimento e qualidade	Automatizar, em plataformas de gerenciamento de processos de negócios, a execução de processos;	Dar suporte no desenvolvimento e supervisão de projetos e/ou treinamentos de conscientização dos colaboradores sobre o tema;	Planejamento estratégico da TI
	Levantar e registrar dados para promover diagnósticos, sugerir modificações e auxiliar no aperfeiçoamento de métodos e processos de trabalho;	Analisar os gaps e/ou vulnerabilidades de segurança da informação;	Gerenciar os riscos de TI
	Elaborar Instruções Operacionais;	Dar suporte ao programa de resposta à incidentes de segurança da informação e cibernéticos.	Controle de demandas de auditoria interna / externa e prover visibilidade dos planos de ação dos pontos de risco identificados.
	Sugerir melhorias em processos.	Apoiar nos processos de contratação, implantação de projetos e ferramentas de segurança da informação;	Participação no processo de avaliação de fornecedores e prestadores de serviços de TI.
	Mapear, modelar e analisar processos de infraestrutura de Tecnologia da Informação;	Participar de discussões técnicas e de avaliações de vulnerabilidades/requisitos de segurança com times internos e externos;	Apoiar no gerenciamento de contratos de TI.
	Garantir o atendimento conforme SLA e priorização	Realizar pesquisas e estar atento à novas ameaças, para mitigá-las e corrigi-las no ambiente	Acompanhar periodicamente as medições de SLA. Conhecimento em ferramentas de gestão da

Desenvolvimento	Infraestrutura	Segurança/Governança	
			qualidade (PDCA, 5W2H, Pareto e Diagrama de Causa e Efeito);
	Realizar Análise de desempenho do ambiente e garantir as correções ou melhorias	Gerenciar projetos de segurança da informação.	Desenvolver indicadores estratégicos.
	EQUIPE SISTEMAS OPERACIONAIS		Estruturar planos de curto e longo prazo com link na visão e estratégia de negócios;
	Elaboração de projetos que envolvam as plataformas RISC e CISC		Apoiar a equipe de prospecção e aquisição em demandas relacionadas a aquisições de produtos e serviços específicos da TI quando for necessário.
	Instalação e suporte nos ambientes operacionais Windows e Linux		Elaboração de dashboards.
	Administração e Manutenção de servidores com os sistemas operacional Linux RedHat, com no mínimo um Cluster RedHat		
	Administração e Manutenção de servidores com os sistemas operacional Microsoft Windows Server, tendo no ambiente no mínimo um Cluster Microsoft, com dois ou mais nós em cada cluster		
	Suporte e manutenção de servidores e data center, planejar capacidade e desenvolve projetos de melhorias dos serviços corporativos. Realiza criação de usuários e manutenção de grupos para concessão de privilégios com permissão de acesso		
	BACKUP/RESTORE e STORAGE		
	Definição das rotinas de backup e restore dos dados da Companhia		

Desenvolvimento	Infraestrutura	Segurança/Governança	
	Definir padrão de documentação e armazenamento dos dados		
	BANCO DE DADOS		
	Criação, manutenção e controle dos SGBDs da Companhia		
	Manutenção do projeto de Data Warehouse		
	Administração e Manutenção de SGBD		
	DEVOPS		
	Avaliar solicitações de Desenvolvimento de Sistemas		
	REDES E SEGURANÇA		
	Suporte e manutenção de switches, roteadores, núcleo e data center, planeja capacidade e desenvolve projetos de melhorias dos serviços corporativos.		
	Suporte a redes de computadores com ativos de rede (switches, roteadores etc.)		

2.2.8. Descrição das atividades inerentes ao Serviço de Gerente de Projetos IV:

Requisitos Gerais:

Diploma de nível superior em instituição reconhecida pelo MEC.

OUTROS REQUISITOS POR ÁREA DE TIC:

Desenvolvimento	Infraestrutura	Segurança/Governança	
EQUIPE ERP	SISTEMAS OPERACIONAIS	Experiência de no mínima de 12 anos em segurança da Informação	Equipe de governança: Experiência mínima de 8 anos na área de governança de TI; Desejável pós-graduação em governança de TI ou Gestão de TI; Experiência na implantação dos processos ITIL; Desejável certificação COBIT e ITIL.
Experiência em implantação de ERP	Possuir Certificação Microsoft Certified System Administrator (MCSA) em Windows	Especialização em Segurança da Informação	Equipe de Projetos: Experiência mínima de 8 anos na área de

Desenvolvimento	Infraestrutura	Segurança/Governança	
	2003 ou Microsoft Certified Technology Specialist (MCTS) em Windows Server ou Microsoft Certified Solutions Associate (MCSA) em Windows Server 2008 ou superior.		gerenciamento de projetos de TI.
Experiência em migração de versão do ERP	Possuir Certificação Microsoft Certified Systems Engineer (MCSE) em Windows 2003 ou Microsoft Certified IT Professional (MCITP): Enterprise Administrator ou Microsoft Certified Solutions Expert (MCSE: Server Infrastructure).	Especialização em Infraestrutura de redes	Equipe de Processos: Experiência mínima de 8 anos na área de processos e BPM. Pós-graduação na área de gerenciamento de projetos ou certificação PMP.
EQUIPE BI	Possuir Certificação Linux Professional Institute Certification Level 2 (LPIC-2).	Especialização em perícia Forense computacional	Equipe de Prospecção: Experiência mínima de 8 anos na área de TI.
Desejável experiência em Machine Learning	Possuir Certificação Linux Professional Institute Certification Level 3 (LPIC-3) ou Red Hat Certified System Administrator — RHCSA ou Red Hat Certified Datacenter Specialist — RHCDs ou Red Hat Certified Architect — RHCA.	Especialização em Gerenciamento de Projetos	
Desejável experiência em Big Data	Possuir Certificação VMware Certified Professional 5 – Data Center Virtualization (VCP5-DCV) ou superior.	Certificação CISSP	
Desejável experiência com desenvolvimento Python ou R	BACKUP/RESTORE e STORAGE	Certificação PMP – Project Management Professional (desejável)	
TODAS AS EQUIPES	Desejável possuir certificação Storage Networking Industry Association – SNIA Certified Professional (SCSP) ou superior.	Certificação em gestão de Riscos PMI-RP ou equivalente	

Desenvolvimento	Infraestrutura	Segurança/Governança	
Experiência com liderança de equipe	Desejável possuir Certificação Dell EMC	Certificação Scrum Master	
Desejável experiência como Scrum Master em projetos	Desejável possuir Huawei IT HCIA Storage – BSSN Certified Network Associate	Certificação em desenvolvimento seguro	
Desejável Certificação PMP Project Management Professional ou Especialização em Gerenciamento de Projetos	Desejável possuir Veeam Certified Architect	Certificação CEH	
Desejável Certificação de Scrum Master	Desejável possuir Veeam Certified Engineer	CompTIA Cybersecurity Analyst (CSA +)	
	Possuir Certificação de escopo de Storage	Certificação de segurança em Cloud Computing	
	Possuir Certificação de escopo de Backup	Certificações LPIC	
	BANCO DE DADOS	Certificações CompTIA Security+	
	Possuir certificação Microsoft Certified Technology Specialist (MCTS) em SQL Server ou Microsoft Certified Solutions Associate (MCSA: SQL Server 2008 ou MCSA: SQL Server 2012) ou superior.	Information Security Foundation based on ISO IEC 27001	
	Possuir certificação Microsoft IT Professional: Database Administrator ou Microsoft Certified Solutions Expert (MCSE: Data Platform) ou MCSE: Business Intelligence.	Certificação CCNA ou equivalente	
	Possuir Certificação OCE – Oracle Certified Expert	Certificação em privacidade de dados DPOEXIN ou equivalente;	
	Possuir Certificação OCM – Oracle Certified Master	Certificação Microsoft Certified Systems Administrator	
	Desejável possuir Certificações em Power BI	Certificação COBIT	

Desenvolvimento	Infraestrutura	Segurança/Governança	
	Desejável possuir Certificado Profissional de Business Intelligence (CBIP)	Certificação ITIL	
	Desejável Possuir MCSA: SQL 2016 BI Development		
	Desejável possuir Microsoft Certified: Power BI Data Analyst Associate		
	Possuir Certificação Oracle Business Intelligence Foundation Suite 11g Certified Implementation Specialist		
	Possuir Certificação PostgreSQL Professional Certification		
	DEVOPS		
	Possuir Certificação Docker Certified Associate (DCA)		
	Possuir Certified Kubernetes Administrator (CKA)		
	Possuir Certified Kubernetes Application Developer (CKAD)		
	Possuir Certificação DevOps Master		
	Possuir Certificação DevOps Professional		
	Desejável possuir Engenheiro Certificado Jenkins (CJE)		
	Desejável possuir Engenheiro DevOps Certificado AWS		
	Desejável possuir Google Professional Cloud DevOps Engineer		
	Desejável possuir Microsoft Certified DevOps Engineer Expert		
	GERENCIAMENTO DE SERVIÇOS		
	Desejável possuir Dynatrace Associate		

Desenvolvimento	Infraestrutura	Segurança/Governança	
	Desejável possuir Zabbix Certified Professional (ZCP) ou de ferramentas de escopo de monitoramento		
	Desejável possuir Certificações em Power BI		
	Desejável possuir Certificações em ferramenta de gerenciamento de serviços ITIL (Service Now, Soft Expert, Service Desk Manager)		
	REDES E SEGURANÇA		
	Possuir certificação Cisco Certified Network Associated (CCNA) ou Cisco Certified Design Associate (CCDA) ou CompTIA Network+;		
	Possuir certificação Cisco Certified Network Professional (CCNP) ou Cisco Certified Design Professional (CCDP) ou Cisco Certified Network Professional in Voice (CCNP Voice) ou Cisco Certified Internetwork Expert (CCIE) ou Cisco Certified Internetwork Professional (CCIP) ou Cisco Certified Network Professional in Service Provider Operations (CCNP Service Provider);		
	Desejável possuir certificação no F-Secure		

COMPETÊNCIAS REQUERIDAS POR ÁREA DE TIC:

Desenvolvimento	Infraestrutura	Segurança/Governança	
EQUIPE BI	TODAS AS EQUIPES	Conhecimento em Gestão e análise de vulnerabilidades;	Equipe de Projetos e processos de TI



Desenvolvimento	Infraestrutura	Segurança/Governança	
Experiência na área de Business Intelligence/ Data Warehouse	Experiência mínima de 10 (dez) anos na área de Tecnologia da Informação, preferencial com Infraestrutura	Conhecimento em Gestão de Segurança da Informação;	Gerenciamento de projetos
Experiência com projetos Big Data	Experiência mínima de 7 (sete) anos na especialidade solicitada com o perfil de liderança técnica e Gerenciamento de Projetos de médio e grande porte;	Conhecimento em gestão de Firewalls de aplicação - WAF	PMP
Experiência com projetos Machine Learning	Conhecimento na LGPD – Lei Geral de Proteção de Dados	Conhecimento em Gerenciamento de projetos de segurança da informação;	BPM
TODAS AS EQUIPES	Desejável conhecimento na metodologia ITIL, COBIT	Conhecimento na execução de testes de invasão;	Automação de processos
Experiência em gerenciamento de Projetos PMBOK	EQUIPE SISTEMAS OPERACIONAIS	Conhecimento sobre criptografia;	Scrum
Experiência em gerenciamento de projetos – Scrum	Conhecimento básico de arquitetura de computadores (exemplo: servidores, internet/intranet)	Conhecimento em segurança em ambiente de nuvem, pública e privada;	Kanban
Experiência em gerenciamento de equipe	Conhecimento no Funcionamento dos sistemas operacionais	Conhecimento sobre soluções de backup corporativo;	Design thinking
	Experiência e Conhecimento em Linux – Red Hat, Debian e Suse	Conhecimento sobre soluções de gestão de acesso privilegiado	Project model canvas
	Experiência e Conhecimento em virtualização – VMWare	Conhecimento sobre gestão de riscos de segurança da informação	Equipe de prospecção de soluções de TI
	Experiência e Conhecimento em Windows Server – AD/DNS/DHCP/RADI US/GPO	Conhecimento em privacidade dados e leis relacionadas;	Levantamento de requisitos
	BACKUP/RESTORE e STORAGE	Conhecimento em soluções de desenvolvimento Seguro;	Implantação de sistemas;
	Experiência e Conhecimento em rotinas de Backup (EMC, Network Tape, disco (datadomain) e	Conhecimento em gestão de Logs;	Infraestrutura de TI;

Desenvolvimento	Infraestrutura	Segurança/Governança	
	VEEAM (Nuvem e Exagrid)		
	Experiência e Conhecimento em Mirror de LUN com Recover Point (Dell EMC, Hwauei)	Conhecimento em administração de Firewall;	Segurança da informação;
	Experiência e Conhecimento em rotinas de Backup (EMC, Network Tape, disco (datadomain) e VEEAM (Nuvem e Exagrid)	Conhecimento em IDS/IPS;	Condução de provas de conceito de soluções de TI.
	Experiência e Conhecimento em Storage EMC e Huawei	Conhecimento sobre os riscos elencados pela OWASP;	Equipe de Governança de TI
	Experiência e Conhecimento em Suporte Storage (Subsistema de Discos de Alta Performance, Fitoteca, Switches e Rede SAN)	Conhecimento sobre a Família ISO 27000;	ISO 20000.
	Experiência e Conhecimento em Switch SAN FC (Dell, Hwauei)	Conhecimento sobre a ISO 22301;	Família ISO 27000.
	BANCO DE DADOS	Conhecimento de programas e de implementação de softwares de segurança;	Cloud(foundation).
	Desejável Conhecimento em bancos (Vertica, Greenplum, MongoDB, NoSQL)	Conhecimento das melhores práticas de desenvolvimento de procedimentos e de infraestrutura de segurança;	Dev Ops(Foundation).
	Experiência e Conhecimento em bancos Oracle database In-Memory	Softwares e ferramentas de segurança da informação;	NIST
	Experiência e Conhecimento em bancos postgresSQL	Conhecimento de infraestrutura de redes e protocolos de comunicação;	Conhecimentos em conceito de gestão de riscos operacionais (avaliação de risco, matriz de risco etc.), gestão de Crises/Gestão de Incidentes;
	Experiência e Conhecimento em estrutura de banco de dados (diagrama entidade-relacionamento)	Inglês intermediário;	CMMI

Desenvolvimento	Infraestrutura	Segurança/Governança	
	Experiência e Conhecimento na linguagem estruturada SQL		Experiência na implantação dos processos ITIL.
	Experiência e Conhecimento na administração de SGBDs Oracle, PostgreSQL, Microsoft SQL Server, MySQL		LGPD(Foundation).
	Experiência na área de banco de dados e análise de sistemas		ISO 31000
	Conhecimento em Ferramenta Case de modelagem		COBIT
	Conhecimento em Ferramentas ETL e OLAP		ITIL
	Experiência em modelagem orientada a objetos utilizando UML		Continuidade do negócio
	DEVOPS		Gestão de riscos
	Conhecimento e execução de tarefas orientadas à DevOps		Liderança técnica de equipe.
	Conhecimento em linguagens de programação (Java, ASP, Delphi)		Família ISO 27000.
	Experiência e Conhecimento em Devops		Cloud(Cloud computing foundation).
	Experiência e Conhecimento em Docker		Lean IT(Lean IT Foundation).
	Experiência e Conhecimento em Jenkins		Conhecimento em análise de negócios (BCS Business analysis foundation).
	Experiência e Conhecimento em Kubernetes		
	Experiência e Conhecimento em Node.js (servidor web completo e robusto para projetos rápidos)		
	GERENCIAMENTO DE SERVIÇOS		
	Experiência e Conhecimento em Administrar e customizar o Zabbix		

Desenvolvimento	Infraestrutura	Segurança/Governança	
	Experiência e Conhecimento em análise de aplicações com datadog e dynatrace		
	Experiência e Conhecimento em criar dashboards e/ou relatórios		
	Experiência e Conhecimento em ERP Totvs (infraestrutura)		
	Experiência e Conhecimento em Kibana, Elastic Search, Zabbix, Nagios, Power BI, Grafana		
	Experiência e Conhecimento no software Zimbra		
	REDES E SEGURANÇA		
	Conhecimento de infraestrutura de redes e protocolos de comunicação		
	Conhecimento em redes TCP/IP, bem como operação e manutenção em redes wireless, switches, hubs		
	Conhecimento em Design de circuito		
	Experiência e Conhecimento como administrador de rede		
	Experiência e Conhecimento em Asterisk		
	Experiência e Conhecimento em F5, NGINX		
	Experiência e Conhecimento em firewall Fortigate, SDWAN, Fortimail e fortianalyser		
	Experiência e Conhecimento em Switches Huawei e 3com		

Desenvolvimento	Infraestrutura	Segurança/Governança	
	Experiência e Conhecimento em Wi-fi Fortinet e Aruba		
	Experiência e Conhecimento em Firewall, IDS/IPS		
	Conhecimento de sistemas de rede e de protocolos de segurança		
	Possuir conhecimento em ferramentas de Antivírus (F-Secure, SEP, etc)		
	Possuir conhecimento em protocolos de roteamento (OSPF, EIGRP, BGP e MPBGP) e LDP, L2VPN, MPLS-TE e MPLS, ATOM, switching, VSS, Multicast, protocolos TCP/IP (versão 4 e 6), Conhecimento em Load Balancer e firewall de aplicação (Cisco CSM/ACE/GSS, PIX, ASA), Citrix Netscaler, A10 AX, F5 Vipron, produtos e ferramentas de gerenciamento e análise de capacidade de rede (Ciscoworks, DCNM, MRTG, TIVOLI, CA Spectrum, Netflow).		
	Possuir conhecimento em firewall Cisco PIX/ASA e CheckPoint (SecurePlatform), VPN GRE, IPSEC, TACACS, RADIUS, ACS, CISCO WORKS e mitigador de ataque (SNORT, ARBOR PeakFlow, IPS SourceFire, Citrix NetScaler, A10 AX, F5 Vipron).		

PRINCIPAIS ATIVIDADES POR ÁREA DE TIC:



Desenvolvimento	Infraestrutura	Segurança/Governança	
Propor melhorias nos sistemas implantados, acompanhado da área usuária	TODAS AS EQUIPES	Identificar, analisar e monitorar os riscos cibernéticos;	Garantir que os processos de TI estejam alinhados com políticas de compliance, normas técnicas e boas práticas do mercado
Manter documentação das atividades desempenhadas atualizadas	Definição de ferramentas a serem utilizadas	Identificar as fragilidades dos controles internos e propor melhorias;	Otimizar a aplicação de recursos;
Liderar equipe técnica de desenvolvimento	Manter a documentação do modelo de dados atualizada e de fácil consulta	Acompanhar as auditorias e tratar seus resultados;	Garantir a entrega de valor da TI para o negócio da empresa
Gerenciar projetos utilizando metodologias ágeis e/ou PMBOK	Realizar pesquisas e desenvolvimento	Desenvolver e Gerir Campanhas de Conscientização em segurança da informação;	Gerenciamento de projetos de TI
Promover reuniões com os interessados do projeto ou do sistema sustentado	Desenhar e redesenhar processos de infraestrutura de Tecnologia da Informação;	Elaborar e manter políticas e normas de segurança da informação;	Automação de processos
Promover comunicação entre a equipe liderada com as demais	Elaboração de projetos e especificações técnicas De Infraestrutura de TIC	Buscar de forma contínua novas tecnologias e ferramentas de suporte à segurança da informação para melhor proteção dos dados e das operações de tecnologia;	Prospecção de soluções de TI
Gerenciar demandas da equipe	Definir, desenhar e manter indicadores de performance;	Conduzir varreduras de vulnerabilidades no ambiente de Infraestrutura e Aplicações Web.	Definição de métricas e indicadores
Acompanhar os indicadores de desenvolvimento e qualidade	Automatizar, em plataformas de gerenciamento de processos de negócios, a execução de processos;	Dar suporte no desenvolvimento e supervisão de projetos e/ou treinamentos de conscientização dos colaboradores sobre o tema;	Planejamento estratégico da TI
	Levantar e registrar dados para promover diagnósticos, sugerir modificações e auxiliar no aperfeiçoamento de métodos e processos de trabalho;	Analisar os gaps e/ou vulnerabilidades de segurança da informação;	Gerenciar os riscos de TI
	Elaborar Instruções Operacionais;	Dar suporte ao programa de resposta à incidentes de segurança da informação e cibernéticos.	Controle de demandas de auditoria interna / externa e prover visibilidade dos planos de ação dos pontos de risco identificados.

Desenvolvimento	Infraestrutura	Segurança/Governança	
	Sugerir melhorias em processos.	Apoiar nos processos de contratação, implantação de projetos e ferramentas de segurança da informação;	Participação no processo de avaliação de fornecedores e prestadores de serviços de TI.
	Mapear, modelar e analisar processos de infraestrutura de Tecnologia da Informação;	Participar de discussões técnicas e de avaliações de vulnerabilidades/requisitos de segurança com times internos e externos;	Apoiar no gerenciamento de contratos de TI.
	Garantir o atendimento conforme SLA e priorização	Realizar pesquisas e estar atento à novas ameaças, para mitigá-las e corrigi-las no ambiente	Acompanhar periodicamente as medições de SLA. Conhecimento em ferramentas de gestão da qualidade (PDCA, 5W2H, Pareto e Diagrama de Causa e Efeito);
	Realizar Análise de desempenho do ambiente e garantir as correções ou melhorias	Realizar a condução de demandas com outras áreas da empresa, realizando o acompanhamento da evolução;	Desenvolver indicadores estratégicos.
	EQUIPE SISTEMAS OPERACIONAIS	Avaliar novos projetos, produtos e serviços sob o viés de segurança cibernética, endereçando com os times responsáveis os riscos identificados;	Estruturar planos de curto e longo prazo com link na visão e estratégia de negócios;
	Elaboração de projetos que envolvam as plataformas RISC e CISC	Participar das atividades de elaboração, implementação, avaliação e melhorias em controles, processos e arquiteturas de Segurança da Informação.	Apoiar a equipe de prospecção e aquisição em demandas relacionadas a aquisições de produtos e serviços específicos da TI quando for necessário.
	Instalação e suporte nos ambientes operacionais Windows e Linux	Gerenciar projetos de segurança da informação.	Elaboração de dashboards.
	Administração e Manutenção de servidores com os sistemas operacional Linux RedHat, com no mínimo um Cluster RedHat		
	Administração e Manutenção de servidores com os sistemas operacional Microsoft Windows Server, tendo no ambiente no mínimo um Cluster Microsoft, com		

Desenvolvimento	Infraestrutura	Segurança/Governança	
	dois ou mais nós em cada cluster		
	Suporte e manutenção de servidores e data center, planejar capacidade e desenvolve projetos de melhorias dos serviços corporativos. Realiza criação de usuários e manutenção de grupos para concessão de privilégios com permissão de acesso		
	BACKUP/RESTORE e STORAGE		
	Definição das rotinas de backup e restore dos dados da Companhia		
	Definir padrão de documentação e armazenamento dos dados		
	BANCO DE DADOS		
	Criação, manutenção e controle dos SGBDs da Companhia		
	Manutenção do projeto de Data Warehouse		
	Administração e Manutenção de SGBD		
	DEVOPS		
	Avaliar solicitações de Desenvolvimento de Sistemas		
	REDES E SEGURANÇA		
	Suporte e manutenção de switches, roteadores, núcleo e data center, planeja capacidade e desenvolve projetos de melhorias dos serviços corporativos.		
	Suporte a redes de computadores com ativos de rede (switches, roteadores etc.)		



2.2.9. Descrição das atividades inerentes ao Serviço de Programador Pleno:

Requisitos Gerais:

Ensino médio concluído em instituição reconhecida pelo MEC

OUTROS REQUISITOS POR ÁREA DE TIC:

Desenvolvimento	Infraestrutura	Segurança/Governança	
EQUIP E ERP			
Desejável cursos oficiais da TOTVs referente ao ERP (versão AP11 ou AP12): Configurador, ADVPL, IDE e Integração com Office (Excel e Word) e LibreOffice (Calc e Writer)			
EQUIP E BI			
Desejável experiência com suíte Pentaho			

COMPETENCIAS REQUERIDAS POR ÁREA DE TIC:

Desenvolvimento	Infraestrutura	Segurança/Governança	
EQUIPE ERP	Conhecimento e execução de tarefas orientadas à DevOps	Conhecimento de programas e de implementação de softwares de segurança da informação	Conhecimento em automação de processos
Experiência em desenvolvimento com linguagem ADVPL, IDE Eclipse/VS Code e Integração com Office (Excel e Word) e LibreOffice (Calc e Writer)	Conhecimento em LGPD – Lei Geral de Proteção de Dados.	Conhecimento de infraestrutura de redes e protocolos de segurança	Conhecimento em integrações REST e SOAP;
EQUIPE WEB/MOBILE		Inglês técnico (leitura)	Conhecimento em banco de dado
Experiência em desenvolvimento backend com tecnologia Java			
Experiência em desenvolvimento frontend com frameworks Javascript			

Desenvolvimento	Infraestrutura	Segurança/Governança	
Experiência com IDE Eclipse ou VS Code			
EQUIPE BI			
Experiência na área de Business Intelligence/ Data Warehouse			
Experiência em modelagem de relacional			
Experiência em modelagem de dimensional			
Experiência com ferramentas de BI (ETL, Analytics, Dicionário de dados)			
TODAS AS EQUIPES			
Experiência com comandos SQL p/ Oracle ou Comandos SQL p/ Postgresql			
Experiência com ferramenta de controle de versão GIT			

PRINCIPAIS ATIVIDADES POR ÁREA DE TIC:

Desenvolvimento	Infraestrutura	Segurança/Governança	
Codificação e testes de aplicações		Monitoramento e correlação de logs de servidores e hardware de rede relacionado	Automatização de processos
Manutenção de sistemas		Realizar atividades técnicas/ operacionais na implantação de controle de Segurança da Informação	Integração das ferramentas de automação de processos com os sistemas corporativos;
Suporte funcional e operacional de usuários		Utilização de softwares e ferramentas de segurança da informação	
Manter documentação das atividades desempenhadas atualizadas		Análise de informações e produção de relatórios	
		Registro/ acompanhamento de incidentes de segurança	
		Elaborar relatórios de recuperação de desastres e	

Desenvolvimento	Infraestrutura	Segurança/Governança	
		de continuidade dos negócios da organização para os sistemas de informação	
		• Monitoramento dos planos de continuidade de negócios e recuperação de desastres	

2.2.10. Descrição das atividades inerentes ao Serviço de Suporte Operacional em HardWare e SoftWare:

Requisitos Gerais:

Ensino médio concluído em instituição reconhecida pelo MEC.

COMPETENCIAS REQUERIDAS:

Projeto, manutenção e operação de sistemas operacionais Windows e Linux; Conhecimento em redes TCP/ IP (física e wireless); Conhecimento em manutenção e montagem de computadores e impressoras, bem como instalação de sistemas operacionais (Windows e Linux); Service Desk; Conhecimento e execução de tarefas orientadas à DevOps; Conhecimento em LGPD – Lei Geral de Proteção de Dados.

PRINCIPAIS ATIVIDADES:

Identificar o funcionamento e relacionamento entre os componentes de computadores e seus periféricos; Instalar e configurar computadores, isolados ou em redes, periféricos e softwares; Identificar a origem de falhas no funcionamento de computadores, periféricos e softwares avaliando seus efeitos; Instalar e configurar equipamentos de telefonia IP, isolados ou em redes, periféricos e softwares; Analisar e operar os serviços e funções de sistemas operacionais; Selecionar programas de aplicação a partir da avaliação das necessidades do usuário; Identificar arquiteturas de redes; Identificar meios físicos, dispositivos e padrões de comunicação, reconhecendo as implicações de sua aplicação no ambiente de rede; Identificar arquitetura de redes e tipos, serviços e funções de servidores; Identificar os serviços de administração de sistemas operacionais de rede; Manutenção de servidores e suas tecnologias; Suporte Linux em geral; Acompanhamento de projeto VOIP; Atendimento ao usuário, local e remotamente; Acompanhamento de rádios e links; Manutenção e gerenciamento do servidor Antivírus; Permissões e segurança no Active Directory; Elaboração de scripts remotos; Protocolo SIP; Estrutura de rede de comunicação LAN, WAN, Wi-Fi, suas topologias e protocolos; Manutenção do Active Directoy (AD); Identificar arquitetura de redes e tipos, serviços e funções de servidores; Monitoramento e manutenção preventiva do antivírus corporativo; Auxiliar na revisão e manutenção de procedimentos e documentações de TI; Monitoramento dos equipamentos de segurança; Monitoramento da gestão de vulnerabilidades; Acompanhamento das rotinas de backups; Auxiliar nas auditorias de vulnerabilidades de redes ou aplicações.

OUTRAS ATIVIDADES

Conduzir, quando necessário, veículos oficiais da CONTRATANTE para trabalhos externos, mediante apresentação da Carteira Nacional de Habilitação, documentação comprobatória de regularidade com as autoridades de trânsito e compatíveis com os veículos a conduzir.

2.2.11. Descrição das atividades inerentes ao Serviço de Suporte Operacional em HardWare e SoftWare (com EPI):

Requisitos Gerais:

Ensino médio concluído em instituição reconhecida pelo MEC.



COMPETENCIAS REQUERIDAS:

Projeto, manutenção e operação de sistemas operacionais Windows e Linux; Conhecimento em redes TCP/ IP (física e wireless); Conhecimento em manutenção e montagem de computadores e impressoras, bem como instalação de sistemas operacionais (Windows e Linux); Service Desk; Conhecimento e execução de tarefas orientadas à DevOps; Conhecimento em LGPD – Lei Geral de Proteção de Dados.

PRINCIPAIS ATIVIDADES:

Atuar na área de service desk; Realizar upgrades nos equipamentos de informática; Gerar e emitir relatórios dos sistemas quando necessário; Controlar, instalar e configurar rádios; Instalação e manutenção na rede sem fio wireless; Instalação de antenas para suporte dos equipamentos e realizar a orientação das mesmas, bem como escalar torres/ postes conforme a necessidade (fazendo uso de EPI); Instalação e manutenção de HUBs, ROTEADORES, SWITCHs e cabeamento de redes; Instalação e manutenção de sistemas de comunicação de dados (Telefonia IP); Instalação e manutenção de sistemas de comunicação de dados (centrais telefônicas);

OUTRAS ATIVIDADES

Conduzir, quando necessário, veículos oficiais da CONTRATANTE para trabalhos externos, mediante apresentação da Carteira Nacional de Habilitação, documentação comprobatória de regularidade com as autoridades de trânsito e compatíveis com os veículos a conduzir.

2.3. Da Matriz de Risco

2.3.1. A estimativa de custo levou em consideração o risco envolvido na contratação e sua alocação entre contratante e contratado.

2.3.2. São riscos assumidos pelo contratado e que não ensejam a revisão do contrato para restabelecer a relação que as partes pactuaram inicialmente:

2.3.2.1. As variações de custos e de despesas, inclusive os aduaneiros, relacionados à aquisição dos bens e à instalação de equipamentos, entre a data de apresentação da proposta comercial e a sua efetiva aquisição;

2.3.2.2. A variação cambial ordinária;

2.3.2.3. A incidência de responsabilidade civil, administrativa, tributária, ambiental ou criminal por ações, omissões ou fatos imputáveis exclusivamente ao contratado;

2.3.2.4. A ocorrência de greves ou de paralisações de empregados do contratado e de seus subcontratados ou a interrupção ou falha no fornecimento de materiais ou serviços pelos seus contratados;

2.3.2.5. Fatores imprevisíveis, fatores previsíveis de consequências incalculáveis, caso fortuito ou força maior se, à época da materialização do risco, sejam seguráveis no Brasil, há pelo menos 3 (três) anos, até o limite da média dos valores de apólices normalmente praticados em mercado, por, pelo menos, três empresas do ramo.

2.3.3. São riscos assumidos pelo contratante e ensejam a revisão do contrato:

2.3.3.1. Determinações ou omissões, judiciais ou administrativas, relacionadas ao objeto do contrato, desde que o contratado, seus empregados, seus prepostos ou seus contratados não tenham, direta ou indiretamente, dado causa à situação sobre a qual estiverem fundadas as referidas decisões;

2.3.3.2. A criação, a alteração ou a extinção de tributos ou encargos legais que tenham comprovada repercussão nos preços contratados, em conformidade com o imposto na legislação aplicável e excetuados os tributos incidentes sobre a renda;

2.3.3.3 As alterações normativas ou da regulação setorial que representam aumentos de encargos do contratado;



2.3.3.4. Quando ocorrerem circunstâncias supervenientes, em razão de caso fortuito ou força maior, que não possam ser objeto de cobertura de seguros oferecidos no Brasil;

2.3.4. Na hipótese de ocorrência de um dos eventos listados nesta cláusula, o contratado deverá, no prazo de 01 (um) dia útil, informar ao contratante sobre o ocorrido, contendo as seguintes informações mínimas:

2.3.4.1. Detalhamento do evento ocorrido, incluindo sua natureza, a data da ocorrência e sua duração estimada, as medidas que estavam em vigor para mitigar o risco de materialização do evento, quando houver; as medidas que tomará para fazer cessar os efeitos do evento e o prazo estimado para que esses efeitos cessem e as obrigações contratuais que não foram cumpridas ou que não irão ser cumpridas em razão do evento.

2.3.4.2. Após a notificação, o contratante decidirá quanto ao ocorrido ou poderá solicitar esclarecimentos adicionais ao contratado. Em sua decisão o contratante poderá isentar temporariamente o contratado do cumprimento das obrigações contratuais afetadas pelo evento.

2.3.4.3. A concessão de isenção não exclui a possibilidade de aplicação das sanções previstas neste instrumento, se identificado que o contratado concorreu para a materialização do evento;

2.3.4.4. Os fatos imprevisíveis, ou previsíveis, porém de consequências incalculáveis, retardadores ou impeditivos da execução do contrato, não previstos nesta cláusula, serão decididos mediante acordo entre as partes, no que diz respeito à recomposição do equilíbrio econômico e financeiro do contrato.

3. DO PRAZO DE VIGÊNCIA E DA ALTERAÇÃO

3.1. O prazo de vigência do contrato será de até 180 (cento e oitenta) dias, contados a partir do dia seguinte ao término do contrato vigente, ou seja, 15 de julho de 2026.

3.2. O contrato poderá ser alterado nos casos previstos nos arts. 72 e 81 da Lei Federal nº 13.303/2016 e conforme dispuser o Regulamento de Licitações e Contratos da Cagece.

4. REQUISITOS DA CONTRATAÇÃO

4.1. Subcontratação

4.1.1. Não será admitida a subcontratação do objeto contratual.

4.2. Garantia contratual

4.2.1. A contratação conta com garantia de execução, inclusive para pagamento de obrigações de natureza trabalhista, previdenciária e para com o FGTS, o proponente deverá apresentar ao contratante, no prazo máximo de 10 (dez) dias úteis, contados da publicação da ratificação, comprovante de prestação de garantia de 5% (cinco por cento) sobre o valor contratual, em conformidade com o disposto no art. 70 da Lei Federal nº 13.303/2016 e no artigo 96 do Regulamento de Licitações e Contratos da Cagece.

4.2.1.1. A não prestação de garantia equivale à recusa injustificada para a contratação, caracterizando descumprimento total da obrigação assumida, ficando a adjudicatária sujeita às penalidades legalmente estabelecidas, inclusive multa.

4.2.2. A garantia contratual terá prazo de validade de até 90 (noventa) dias após a data de encerramento do contrato, conforme disposto no inciso IV do art. 16 do Decreto nº 35.790/2023.

4.2.3. O atraso superior a 25 (vinte e cinco) dias, em relação ao prazo máximo para apresentação da garantia, autoriza a Administração a promover o bloqueio dos pagamentos devidos ao CONTRATADO, até o limite estabelecido no item 4.2.1, a título de garantia.

4.2.4. A garantia prestada sob uma das modalidades previstas no art. 96, item 1, alínea “a” do Regulamento de Licitações e Contratos da Cagece, deverá:

4.2.4.1. Cobrir o período de execução do contrato e estender-se até 3 (três) meses após o término da vigência contratual, devendo ser renovada a cada prorrogação ou renovação contratual e complementada em casos de aditivos e apostilas para reajustes.

4.2.4.2. Assegurar, qualquer que seja a modalidade escolhida, o pagamento dos eventos previstos no caput do art. 19 do Decreto Estadual 35.790/2023 e no art. 96 do Regulamento de Licitações da Cagece, tais como:

4.2.4.2.1. Prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;

4.2.4.2.2. Prejuízos diretos causados ao CONTRATANTE decorrentes de culpa ou dolo durante a execução do contrato;

4.2.4.2.3. Multas moratórias e punitivas aplicadas pelo CONTRATANTE ao CONTRATADO; e

4.2.4.2.4. Obrigações de natureza trabalhista, previdenciária e para com o FGTS, em valor correspondente a 5% (cinco por cento) do valor inicial do contrato, podendo ser majorado até 10% (dez por cento), mediante análise da complexidade técnica e dos riscos envolvidos, com prazo de validade de até noventa dias, após a data de encerramento do contrato, conforme disposto no inciso IV do art. 16 do Decreto nº 35.790/2023.

4.2.4.2.5. A garantia em dinheiro deverá ser efetuada com correção monetária em favor da Cagece, em conta preferencialmente no Banco Bradesco S.A, ou outro banco por ele indicado.

4.2.5. Será permitida a substituição da apólice de seguro-garantia na data de renovação ou de aniversário, desde que mantidas as condições e coberturas da apólice vigente e nenhum período fique descoberto, ressalvado o disposto no subitem 4.2.7, deste Termo.

4.2.6. A garantia contratual somente será liberada mediante a comprovação de que o CONTRATADO pagou todas as verbas rescisórias trabalhistas decorrentes da contratação, e que, caso esse pagamento não ocorra até 30 (trinta) dias após o encerramento da vigência contratual, a garantia será utilizada para o pagamento dessas verbas trabalhistas, observada a legislação que rege a matéria, de acordo com o disposto no inciso VI do art. 16 do Decreto nº 35.790/2023.

4.2.7. Na hipótese de suspensão do contrato por ordem ou inadimplemento da Administração, o CONTRATADO ficará desobrigado de renovar a garantia ou de endossar a apólice de seguro até a ordem de reinício da execução ou o adimplemento pela Administração.

4.2.8. A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados no subitem 4.2.4.2, observada a legislação que rege a matéria.

4.2.9. No caso de garantia na modalidade de fiança bancária, deverá ser emitida por banco ou instituição financeira devidamente autorizada a operar no País pelo Banco Central do Brasil, e deverá constar expressa renúncia do fiador aos benefícios do art. 827 do Código Civil.

4.2.10. Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação, o CONTRATADO obriga-se a fazer a respectiva reposição no prazo máximo de 10 (dez) dias úteis, contados da data em que for notificada.

4.2.11. O CONTRATANTE executará a garantia na forma prevista na legislação que rege a matéria.

4.2.12. O emitente da garantia ofertada pelo CONTRATADO deverá ser notificado pelo CONTRATANTE quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais.

4.2.13. Caso se trate da modalidade seguro-garantia, ocorrido o sinistro durante a vigência da apólice, sua caracterização e comunicação poderão ocorrer fora desta vigência, não caracterizando fato que justifique a negativa do sinistro, desde que respeitados os prazos prescricionais aplicados ao contrato de seguro, nos termos do art. 20 da Circular Susep nº 662, de 11 de abril de 2022.

4.2.14. O CONTRATADO autoriza o CONTRATANTE a reter, a qualquer tempo, a garantia, na forma prevista neste contrato, conforme art. 23 do Decreto Estadual nº 35.790/2023.

4.2.15. No caso da multa for de valor superior ao valor da garantia prestada, além da perda desta, responderá o CONTRATADO pela sua diferença, a qual será descontada dos pagamentos eventualmente devidos pela CAGECE ou, ainda, quando for o caso, cobrada judicialmente.

5. DA EXECUÇÃO DO OBJETO



5.1. Os serviços, objeto do contrato serão realizados nas dependências da contratante sito a Av. Lauro Vieira Chaves, 1030 - Vila União, Fortaleza - CE, 60422-700 – ISS 5% (LEI COMPLEMENTAR Nº 159, DE 23 DE DEZEMBRO DE 2013);

5.2. Para a execução dos serviços, o contratado deverá disponibilizar epi, nas quantidades estimadas e qualidades a seguir estabelecidas, promovendo sua substituição quando necessário;

6. MODELO DE GESTÃO DO CONTRATO

6.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei Federal nº 13.303/2016, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

6.2. Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

6.3. As comunicações entre contratante e contratado devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

6.4. O contratante poderá convocar representante do contratado para adoção de providências que devam ser cumpridas de imediato.

6.5. Após a assinatura do contrato, o contratante poderá convocar o representante do contratado para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução do contratado, quando houver, do método de aferição dos resultados, quando houver, e das sanções aplicáveis, dentre outros. No ato da reunião será realizado apresentação com pautas referentes ao vínculo contratual, registrado em Ata.

6.6. A execução do contrato deverá ser acompanhada e fiscalizada por um agente ou grupo de agentes da Cagece que integram a unidade demandante, conforme art. 98, 3 do Regulamento de Licitações e Contratos da Cagece.

6.7. A fiscalização se responsabilizará pelo acompanhamento da execução do objeto contratual, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração.

6.7.1. O fiscal do contrato anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados.

6.7.2. Identificada qualquer inexatidão ou irregularidade, o fiscal emitirá notificações para a correção da execução do contrato, determinando prazo para a correção.

6.7.3. O fiscal informará ao gestor do contrato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso.

6.7.4. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal comunicará o fato imediatamente ao gestor do contrato.

6.7.5. O fiscal comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual.

6.8. O gestor do contrato coordenará a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de fornecimento, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração.

6.9. O gestor do contrato acompanhará a manutenção das condições de habilitação do contratado, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais.

6.10. O gestor do contrato acompanhará os registros realizados pelo fiscal do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassem a sua competência.

6.11. O gestor do contrato emitirá documento comprobatório da avaliação realizada pelo fiscal quanto ao cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, quando for o caso, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações.

6.12. O gestor do contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções.

6.13. A execução do Contrato será acompanhada e fiscalizada, sistematicamente, pelo representante do contratante, conforme o estabelecido no modelo de Avaliação dos Serviços do Contratado, constantes no ANEXO A deste termo, dentro dos seguintes critérios:

a) Desempenho excelente: quando o contratado obtiver conceito final acumulado menor ou igual a 100% ou maior ou igual a 90%.

b) Desempenho bom: quando o contratado obtiver conceito final acumulado menor que 90% ou maior ou igual a 70%.

c) Desempenho regular: quando o contratado obtiver conceito final acumulado menor que 70% ou maior ou igual a 50%.

d) Desempenho ruim: quando o contratado obtiver conceito final acumulado menor que 50%.

6.14. O representante anotará em registro próprio todas as ocorrências relacionadas com a execução deste; Instrumento, determinando o que for necessário à regularização das faltas ou defeitos observados.

7. DAS CONDIÇÕES DE PAGAMENTO

7.1. O pagamento será efetuado, mediante a apresentação da nota fiscal, até o 30º (trigésimo) dia contado da data do encerramento da medição no módulo de contratos do sistema utilizado pela Cagece, devidamente atestada pelo gestor da contratação, mediante crédito em conta-corrente em nome do contratado.

7.1.1. Identificadas desconformidades em algum documento necessário ao pagamento, o contratado terá 5 (cinco) dias para reapresentá-lo. Na hipótese de ser ultrapassado este prazo, os 30 (trinta) dias citados no subitem 7.1 somente começarão a contar a partir da data de entrega do último documento requerido.

7.1.2. Para fins de averiguação pela CAGECE da manutenção das condições de habilitação, o contratado deverá instruir o pedido de pagamento com a Certidão Conjunta Negativa de Débitos relativos aos Tributos Federais e à Dívida Ativa da União, Certidão Negativa de Débitos Estaduais, Certidão Negativa de Débitos Municipais, Certificado de Regularidade do FGTS – CRF e Certidão Negativa de Débitos Trabalhistas – CNDT.

7.1.2.1. A ausência de quaisquer das certidões referidas no subitem 7.1.2, apesar de não se constituir em causa impeditiva do pagamento, conforme art. 100, item 6 do Regulamento de Licitações e Contratos da CAGECE, ensejará a instauração de processo administrativo para a aplicação de sanção, tendo em vista descumprimento das condições de habilitação exigidas na licitação.

7.2. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

7.2.1. Independentemente do percentual de tributo inserido na Planilha de Custos e Formação de Preços, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.

7.3. É vedada a realização de pagamento antes da execução do objeto ou se o mesmo não estiver de acordo com as especificações deste instrumento, nos termos do art. 100, item 10, do Regulamento de Licitações e Contratos da CAGECE.

7.4. A ausência da comprovação do cumprimento das obrigações trabalhistas, previdenciárias e relativas ao FGTS implicará a retenção do pagamento da fatura mensal, em valor proporcional ao inadimplemento, mediante prévia comunicação, até que a situação seja regularizada, sem prejuízo das demais sanções cabíveis.

7.5. Os pagamentos encontram-se ainda condicionados a apresentação mensal da folha de pagamento dos funcionários com listagem e comprovantes de pagamento de vale-alimentação, vale-transporte, plano de saúde, INSS e GFD (Guia do FGTS Digital com detalhamento da guia emitida).

7.6. Nos casos de eventuais antecipações de quitação do débito, haverá desconto de 1% (um por cento) ao mês “pro rata die”, acrescido da última taxa mensal do CDI disponível na data do pedido de antecipação pela contratada, calculado a partir da data do vencimento e da data do efetivo pagamento, conforme art. 100, item 3 do Regulamento de Licitações e Contratos da CAGECE.

7.7. Nas hipóteses de eventuais atrasos de pagamentos provocados exclusivamente pela Cagece, o valor devido deve ser acrescido de juros de mora de 0,5% (cinco décimos por cento) ao mês “pro rata die” e atualização financeira pela última taxa mensal do CDI disponível na data do pagamento, calculado a partir da data do vencimento e da data do efetivo pagamento, conforme art. 100, item 4 do Regulamento de Licitações e Contratos da CAGECE.

7.8. Em caso do não pagamento das rubricas previstas nos subitens 7.6 e 7.7 acima, bem como de outras verbas inadimplidas, naquilo que não for alcançada pela conta corrente vinculada – bloqueada para movimentação, a contratante fica autorizada a proceder à retenção de valores a que porventura faça jus a contratada, até o limite da inadimplência, e a realizar os pagamentos de salários e demais benefícios aos empregados, bem como das contribuições previdenciárias e do FGTS, quando estes não forem honrados pela empresa contratada, conforme art. 102, 1, a, v do Regulamento de Licitações e Contratos da CAGECE.

7.8.1. Quando do encerramento contratual, o contratado deverá comprovar o pagamento das verbas rescisórias ou que os empregados estão realocados em outra atividade de prestação de serviços, sem a interrupção do contrato de trabalho, devendo o contratante, até que ocorra referida comprovação, reter a garantia prestada e os valores das faturas correspondentes a 1 (um) mês de serviços, podendo utilizá-los para o pagamento direto aos trabalhadores no caso de a contratada não efetuar os pagamentos em até 2 (dois) meses do encerramento da vigência contratual, conforme artigo 102, itens 6 e 7 do Regulamento de Licitações e Contratos da CAGECE.

7.9. As repactuações, revisões, atualizações por atraso de pagamento ou por outras razões, compensações financeiras e qualquer outro direito patrimonial relativo ao período do contrato que não forem solicitadas durante a vigência do contrato são objeto de preclusão com a assinatura do termo aditivo de prorrogação ou renovação ou com o encerramento do contrato, de acordo com artigo 107, item 6 do Regulamento de Licitações e Contratos da CAGECE.

7.10. Toda a documentação exigida deverá ser apresentada em original ou por qualquer processo de reprografia, autenticada por cartório competente ou por servidor da Administração, ou publicação em órgão da imprensa oficial. Caso a documentação tenha sido emitida pela internet, só será aceita após a confirmação de sua autenticidade.

8. DAS OBRIGAÇÕES DO CONTRATANTE

8.1. Exigir o cumprimento de todas as obrigações assumidas pelo contratado, de acordo com este instrumento e seus anexos;

8.2. Notificar o contratado, por escrito, sobre vícios, defeitos ou incorreções verificadas no objeto contratado, para que seja por ele substituído, reparado ou corrigido, no total ou em parte, às suas expensas;

8.3. Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações pelo contratado através de sua unidade competente, podendo solicitar providências do CONTRATADO, que atenderá ou justificará de imediato.

8.4. Comunicar o contratado para emissão de nota fiscal relativa à parcela incontroversa da execução do objeto, para efeito de pagamento, quando houver controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade;

8.5. Determinar o horário da realização dos serviços podendo ser variável em cada local e passível de alteração, conforme conveniência da contratante com observância das leis trabalhistas.

- 8.6. Efetuar o pagamento ao contratado do valor correspondente a execução do objeto, no prazo, forma e condições estabelecidos neste termo.
- 8.7. Providenciar, quando solicitado pelo contratado e mediante demonstração analítica da variação dos custos, a repactuação contratual, observado o interregno mínimo de 1 (um) ano.
- 8.8. Aplicar as sanções previstas na lei e edital, quando do descumprimento de obrigações pelo contratado;
- 8.9. Emitir explicitamente decisão sobre todas as solicitações e reclamações relacionadas à execução do contrato, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do contrato.
- 8.9.1. A Administração observará os prazos fixados nos arts. 88, 107 e 108 do Regulamento de Licitações e Contratos da Cagece, a contar da data do protocolo do requerimento para decidir, admitida a prorrogação motivada, por igual período.
- 8.10. Não responder por quaisquer compromissos assumidos pelo contratado com terceiros, ainda que vinculados à execução do contrato, bem como por qualquer dano causado a terceiros em decorrência de ato do contratado, de seus empregados, prepostos ou subordinados.
- 8.11. Fiscalizar mensalmente o cumprimento das obrigações trabalhistas, previdenciária e para com o FGTS, em relação aos empregados do contratado que efetivamente participarem da execução dos serviços contratados, nos termos do inciso V do art. 16 do Decreto Estadual nº 35.790/2023, em especial, quanto:
- 8.11.1. ao pagamento de salários, adicionais, horas extras, repouso semanal remunerado e décimo terceiro salário;
- 8.11.2. à concessão de férias remuneradas e pagamento do respectivo adicional;
- 8.11.3. à concessão de benefícios, como: auxílio-transporte, auxílio-alimentação, plano de saúde, auxílios creche e funeral, quando for devido;
- 8.11.4. aos depósitos do FGTS; e
- 8.11.5. ao pagamento de obrigações trabalhistas e previdenciárias dos empregados dispensados até a data da extinção do contrato.
- 8.12. Reembolsar o contratado os valores de despesas, devidamente comprovadas, decorrentes de pagamentos de horas extras, diárias, auxílio creche, auxílio funeral e outros conforme Planilha de Custos e Formação de Preços aprovada pela SEPLAG.
- 8.12.1. Reembolsar os valores decorrentes de pagamentos de diárias, devidamente comprovados, em caso de indispensável deslocamento de funcionário do CONTRATADO a serviço em outra localidade diferente da sua lotação, na forma e condições estabelecidas na legislação pertinente e no valor estabelecido na Convenção/Dissídios coletivos de trabalho da categoria profissional respectiva.
- 8.13. Receber e validar o cronograma de férias em tempo hábil para que a contratada emita os avisos e conceda as férias dentro dos prazos legais. Se houver necessidade a contratante poderá revisar o cronograma junto com o preposto e propor novo calendário.
- 8.14. Efetuar o pagamento dos serviços contratados de acordo com a planilha de custo, anexa neste termo, sendo a remuneração dos profissionais que prestarão serviços de responsabilidade exclusiva do Contratado, conforme legislação vigente.
- 8.15. Definir o dimensionamento da quantidade de equipes para cada tipo de serviço e alocação, considerando sempre o resultado mais otimizado.
- 8.16. Solicitar a substituição dos funcionários da contratada que, a seu critério, forem considerados inconvenientes ou incompatíveis com o trabalho.
- 8.17. Solicitar a contratada diária para viagem com antecedência de 48 horas, salvo os casos emergenciais, que serão pagos durante a viagem.
- 8.18. Notificar a contratada quando da ocorrência de atrasos de obrigações trabalhistas, de natureza salarial ou não, com um ou mais empregados terceirizados, para regularização da situação, sendo garantido o contraditório e a ampla defesa.

8.19. Comunicar ao Ministério Público do Trabalho os atrasos reiterados de pagamento por parte do CONTRATADO referentes a salários, contribuições previdenciárias, FGTS e demais obrigações inerentes a contratação, além de verbas rescisórias, quando estes não forem honrados pelas empresas até a data própria.

8.20. Verificar quando da rescisão do contrato, o efetivo pagamento pelo contratado das verbas rescisórias ou dos documentos que comprovem que os empregados serão realocados em outra atividade de prestação de serviços, sem que ocorra a interrupção do contrato de trabalho.

8.21. Efetuar o pagamento das obrigações trabalhistas diretamente aos empregados do contratado, no prazo de quinze dias, quando não for comprovada a quitação das respectivas obrigações por parte do contratado. Tais pagamentos não configuram vínculo empregatício, bem como não implicam a assunção de responsabilidade por quaisquer obrigações dele decorrentes entre o contratante e os empregados do contratado, nos termos do art. 10 c/c § 3º do art. 16 do Decreto Estadual nº 35.790/2023.

8.22. Informar ao contratado que a garantia contratual somente será liberada mediante a comprovação de que houve o pagamento de todas as verbas rescisórias trabalhistas decorrentes da contratação, e que, caso esse pagamento não ocorra até o fim do segundo mês após o encerramento da vigência contratual, a garantia será utilizada para o pagamento dessas verbas trabalhistas, observada a legislação que rege a matéria.

8.23. Proporcionar ao contratado todas as condições necessárias ao pleno cumprimento das obrigações decorrentes do termo contratual, fornecendo quando for o caso, equipamentos e materiais necessários a execução do contrato.

8.24. Observar, no que couber, o disposto no art. 6º do Decreto Estadual nº 35.790/2023, e as disposições especiais sobre empregados terceirizados contidas no Regulamento de Licitações e Contratos da Cagece.

9. DAS OBRIGAÇÕES DO CONTRATADO

9.1. O contratado deve cumprir todas as obrigações constantes do edital e seus anexos e observar as disposições especiais sobre empregados terceirizados contidas no Regulamento de Licitações e Contratos da Cagece, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto, observando, ainda, as obrigações a seguir dispostas:

9.2. Atender às determinações regulares emitidas pelo fiscal ou gestor do contrato ou autoridade superior e prestar todo esclarecimento ou informação por eles solicitados.

9.3. Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de materiais empregados, e responderá por danos causados diretamente a terceiros ou à empresa pública ou sociedade de economia mista, independentemente da comprovação de sua culpa ou dolo na execução do contrato, conforme art. 76 da Lei Federal nº 13.303/2016.

9.4. Responsabilizar-se pelos encargos trabalhistas, previdenciários, fiscais e comerciais resultantes da execução do contrato, cuja inadimplência do contratado, não transferirá à Administração a responsabilidade pelo seu pagamento e não poderá onerar o objeto do contrato, conforme art. 77 da Lei Federal nº 13.303/2016;

9.5. Quando não for possível a verificação da regularidade no Sistema de Cadastramento Unificado de Fornecedores(SICAF), ou no Certificado de Registro Cadastral (CRC) do Estado do Ceará, o contratado deverá entregar ao setor responsável pela fiscalização do contrato, junto com a nota fiscal para fins de pagamento, os seguintes documentos: 1) prova de regularidade relativa à Seguridade Social; 2) Certidão Conjunta relativa aos Tributos Federais e à Dívida Ativa da União; 3) certidões que comprovem a regularidade perante a Fazenda Estadual ou Distrital do domicílio ou sede do contratado; 4) Certidão de Regularidade do FGTS – CRF; e 5) Certidão Negativa de Débitos Trabalhistas – CNDT;

9.6. Responsabilizar-se pelo cumprimento das obrigações previstas em Acordo, Convenção, Dissídio Coletivo de Trabalho ou equivalentes das categorias abrangidas pelo contrato, por todas

as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade o contratante.

9.7. Não serão incluídas nas planilhas de custos e formação de preços as disposições contidas em Acordos, Dissídios ou Convenções Coletivas que tratem de pagamento de participação dos trabalhadores nos lucros ou resultados do contratado, de matéria não trabalhista, de obrigações e direitos que somente se aplicam aos contratos com a Administração Pública, ou que estabeleçam direitos não previstos em lei, tais como valores ou índices obrigatórios de encargos sociais ou previdenciários, bem como de preços para os insumos relacionados ao exercício da atividade.

9.8. Efetuar o pagamento mensal dos salários dos empregados alocados na execução contratual exclusivamente mediante crédito em conta bancária de titularidade individual do trabalhador, preferencialmente do tipo conta-salário, conforme previsto no art. 464 da Consolidação das Leis do Trabalho (CLT) e nas Resoluções CMN nº 5.058/2022 e BCB nº 284/2023, ou normas que as substituam.

9.8.1. Para os fins de atendimento ao subitem 9.8, conta-salário é a conta de depósito à vista aberta pelo empregador, em nome do empregado, isenta de tarifas bancárias, destinada exclusivamente ao crédito de remuneração, vedado o crédito de quaisquer outros valores, sendo facultado ao trabalhador transferir gratuitamente os recursos para outra instituição financeira de sua escolha, nos termos da regulamentação vigente do Banco Central do Brasil.

9.8.2. Para fins de atendimento ao subitem 9.8.1 é vedado à CONTRATADA:

I – exigir que o empregado abra conta-corrente, poupança ou digital em instituição financeira específica, diversa da conta-salário;

II – utilizar contas que impliquem cobrança de tarifas de manutenção, contratação de cestas de serviços, seguros, cartões, produtos ou pacotes correlatos;

III – permitir o desconto automático ou compulsório de valores decorrentes de operações de crédito, consignações não autorizadas ou contratação automática de produtos financeiros, em especial aqueles ofertados por fintechs ou plataformas digitais;

9.8.3. A CONTRATADA responderá integralmente por quaisquer prejuízos decorrentes de descontos indevidos, tarifas bancárias, consignações não autorizadas ou contratação compulsória de produtos financeiros, devendo adotar medidas corretivas imediatas e comprovar a restituição dos valores aos empregados, quando cabível.

9.9. Autorizar o contratante, fornecendo os cálculos e os documentos necessários, a realizar os pagamentos de salários e demais verbas trabalhistas diretamente aos trabalhadores, bem como das contribuições previdenciárias e do FGTS, quando não demonstrado o cumprimento tempestivo e regular dessas obrigações, até o momento da regularização, sem prejuízo das sanções cabíveis, nos termos do art. 10 c/c § 3º do art. 16 do Decreto Estadual nº 35.790/2023.

9.9.1. Quando não for possível a realização desses pagamentos pela própria Administração (ex.: por falta da documentação pertinente, tais como folha de pagamento, rescisões dos contratos e guias de recolhimento), os valores retidos cautelarmente serão depositados junto à Justiça do Trabalho, com o objetivo de serem utilizados exclusivamente no pagamento de salários e das demais verbas trabalhistas, bem como das contribuições sociais e FGTS decorrentes.

9.10. Manter durante toda a execução contratual, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

9.11. Responder por todas as despesas diretas e indiretas que incidam ou venham a incidir sobre a execução contratual, inclusive as obrigações relativas a salários, previdência social, impostos, encargos sociais e outras providências, respondendo obrigatoriamente pelo fiel cumprimento das leis trabalhistas e específicas de acidentes do trabalho e legislação correlata, aplicáveis ao pessoal empregado para execução do contrato. A inadimplência do contratado quanto aos encargos trabalhistas, fiscais e comerciais não transfere ao contratante a responsabilidade por seu pagamento, nem poderá onerar o objeto do contrato, conforme art. 77, caput e § 1º, da Lei Federal nº 13.303/2016.

9.11.1. Responsabilizar-se integralmente pela observância do dispositivo no título II, capítulo V, da CLT, e demais normas do Ministério do Trabalho, relativos a segurança e a medicina do trabalho, bem como a Legislação correlata em vigor a ser exigida.

9.12. Cadastrar-se e manter atualizado cadastro da Companhia de Água e Esgoto do Ceará - CAGECE para fins de gestão de contratos e efetivação de pagamento, disponível no endereço eletrônico <https://www.cagece.com.br/portal-do-fornecedor>.

9.13. Apresentar mensalmente junto ao contratante no prazo máximo de cinco dias úteis subsequente ao término dos serviços prestados, as folhas de pagamentos e as guias de recolhimentos dos encargos sociais exigidos em legislação vigente, em que se comprove a inclusão de empregados utilizados nos serviços contratados, os quais não terão, em tempo algum, durante o período contratual, nenhum vínculo empregatício com o contratante ou com o Governo do Estado do Ceará, sendo também de responsabilidade do contratado, o pagamento de todos os tributos que, direta ou indiretamente, incidam sobre a prestação dos serviços contratados, inclusive as contribuições previdenciárias fiscais e parafiscais, (FGTS, PIS, EMOLUMENTOS, SEGUROS DE ACIDENTES DE TRABALHO e outros previstos em lei), ficando excluída qualquer solidariedade da contratante por eventuais autuações administrativas e/ou judiciais, uma vez que a inadimplência do contratado com referência às suas obrigações não se transfere a contratante. Em nenhuma hipótese, e sob qualquer pretexto, poderá o contratado vincular pagamentos de sua responsabilidade, inclusive os devidos a seus empregados, aos pagamentos a ele devidos pelo contratante.

9.14. Apresentar o contratante, previamente, a escala de férias dos empregados que estiverem à disposição do contratante, bem como fazer suas reposições com as mesmas características profissionais daqueles beneficiados por férias ou licenças.

9.15. Instalar em prazo máximo de 30 (trinta) dias, escritório em Fortaleza-CE a contar da celebração do contrato, nos termos do art. 102, 1, a, iv do Regulamento de Licitações e Contratos da CAGECE.

9.16. Observar os ditames do Código de Conduta e Integridade da Companhia de Água e Esgoto do Ceará - CAGECE, disponível em <https://www.cagece.com.br/wp-content/uploads/2019/01/Cagece-Codigo-de-Conduta.pdf>.

9.17. Cumprir a Política de Dados Pessoais da Companhia de Água e Esgoto do Ceará - CAGECE, disponível em <https://www.cagece.com.br/politica-de-privacidade/>.

9.18. Observar a vedação de contratação de pessoas para prestação de serviço que sejam cônjuges, companheiros, ou que possuam parentesco consanguíneo, em linha reta ou colateral, ou por afinidade até o terceiro grau com empregado público que possua função gratificada ou com ocupante de cargo em comissão na Companhia.

9.19. Entregar ao setor responsável pela fiscalização do contrato, até o dia trinta do mês seguinte ao da prestação dos serviços, os seguintes documentos: 1) prova de regularidade relativa à Seguridade Social; 2) certidão conjunta relativa aos tributos federais e à Dívida Ativa da União; 3) certidões que comprovem a regularidade perante as Fazendas Federal, Estadual e Municipal do domicílio ou sede do contratado; 4) Certidão de Regularidade do FGTS – CRF; e 5) Certidão Negativa de Débitos Trabalhistas – CNDT.

9.19.1. Apresentar mensalmente os seguintes documentos:

a) Arquivo GFIP-SEFIP constando: Relação dos trabalhadores; Protocolo de envio de arquivos Conectividade Social; Comprovante de Declaração das Contribuições a recolher a Previdência Social e a outras Entidades e Fundos por FAPS; Relatório analítico da GRF; Relatório de Compensações, quando houver;

b) GPS- Guia de previdência e comprovante de pagamento, correspondente ao mês da última nota fiscal ou fatura vencida, quanto aos empregados diretamente vinculados à execução contratual, excetuando o pagamento da primeira medição;

c) FGTS- Guia do Fundo de Garantia do Tempo de Serviço, correspondente ao mês da última nota fiscal ou fatura vencida, quanto aos empregados diretamente vinculados à execução contratual, excetuando o pagamento da primeira medição;

d) Folha de Pagamento, correspondente ao mês da última nota fiscal ou fatura vencida, quanto aos empregados diretamente vinculados à execução contratual, excetuando o pagamento da primeira medição;

e) Declaração de Contabilidade Regular com data igual ou superior a emissão da Nota Fiscal.

9.20. Responder pela cotação correta dos encargos tributários, inclusive considerando eventuais benefícios fiscais que faça jus. Em caso de erro ou cotação incompatível com o regime tributário a que se submete, serão adotadas as orientações a seguir:

9.20.1. Cotação de percentual menor que o adequado: o percentual será mantido durante toda a execução contratual.

9.20.2. Cotação de percentual maior que o adequado: o excesso será suprimido, unilateralmente, da planilha e haverá glosa, quando do pagamento, e/ou redução, quando da repactuação, para fins de total ressarcimento do débito. (atendendo as orientações dos Acórdãos TCU nº 3.037/2009-Plenário, nº 1.696/2010-2ª Câmara, nº 1.442/2010-2ª Câmara, nº 387/2010-2ª Câmara e nº 2622/2013-Plenário).

9.21. Providenciar a substituição de qualquer profissional envolvido na execução do objeto contratual, cuja conduta seja considerada indesejável pela fiscalização do contratante.

9.21.1. Substituir no prazo de 24 horas da solicitação formal, integrante da equipe que por qualquer motivo não possa desempenhar adequadamente sua função.

9.22. Comunicar ao fiscal do contrato, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal ou acidente que se verifique no local da execução do objeto.

9.23. Paralisar, por determinação do contratante, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas ou bens de terceiros.

9.24. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato.

9.25. Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da contratação, exceto para restabelecer o equilíbrio econômico-financeiro inicial do contrato em caso de força maior, caso fortuito ou fato do príncipe ou em decorrência de fatos imprevisíveis ou previsíveis de consequências incalculáveis, que inviabilizem a execução do contrato tal como pactuado, respeitada, em qualquer caso, a repartição objetiva de risco estabelecida no contrato.

9.26. Alocar os empregados necessários, com habilitação e conhecimento adequados, ao perfeito cumprimento das cláusulas do contrato, fornecendo, quando for o caso, os materiais, equipamentos, ferramentas e utensílios demandados, cuja quantidade, qualidade e tecnologia deverão atender às recomendações de boa técnica e a legislação de regência.

9.27. Não permitir a utilização de qualquer trabalho do menor de dezesesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos, nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre.

9.28. Promover, se for o caso a guarda, manutenção e vigilância de materiais, ferramentas, e tudo o que for necessário à execução do objeto, durante a vigência do contrato.

9.29. Disponibilizar vagas destinadas ao cumprimento do Decreto Estadual nº 35.790/2023, observando a disponibilidade de vaga(s) para todas as categorias constantes no subitem 2.1, do Anexo I – Termo de Referência.

9.29.1. A reserva de vagas para presos sujeitos ao regime semiaberto, aberto e em livramento condicional não se aplica aos contratos que envolvam serviços de segurança, vigilância e serviços a serem prestados aos órgãos de segurança pública, conforme §1º do art. 42 do Decreto Estadual nº 35.790/2023.

9.29.2. Sempre que solicitado pela Administração, a empresa deverá apresentar provas do cumprimento da reserva dos respectivos cargos. Eventual descumprimento durante a execução

contratual pode constituir motivo para a extinção do contrato, assegurado o direito de defesa, tudo em conformidade com o art. 44 do mesmo decreto.

9.30. Respeitar os princípios de proteção de dados pessoais elencados na Lei Geral de Proteção de Dados, Lei Federal nº 13.709 de 14 de agosto de 2018 e suas alterações.

9.31. Atender além dos critérios de sustentabilidade eventualmente inseridos na descrição do objeto, atender ainda os seguintes requisitos de sustentabilidade:

9.31.1. Respeitar a legislação relativa à disposição final ambientalmente adequada dos resíduos gerados, mitigação dos danos ambientais por meio de medidas condicionantes e de compensação ambiental e outros, conforme § 1º do art. 32 da Lei 13.303/2016.

9.32. Fazer cumprir as jornadas de trabalho estipuladas pela legislação vigente.

9.33. Utilizar no desempenho de suas atividades equipes bem treinadas e aptas para executar as tarefas especificadas no item 2 deste Termo de Referência. Neste sentido, a contratada é obrigada a manter treinado cada profissional objetivando o desempenho perfeito da equipe como um todo e a correta execução do serviço.

9.34. Executar perfeitamente os serviços, dentro dos horários estabelecidos pela cagece, através de pessoas idôneas e tecnicamente capacitadas, assumindo total responsabilidade sobre os equipamentos, imóveis e utensílios colocados à disposição para execução dos serviços. Obriga-se ainda, indenizar a cagece, mesmo em caso de ausência ou omissão de fiscalização de sua parte, por quaisquer danos causados aos seus sistemas, equipamentos, instalações, móveis, utensílios e bens, quer sejam eles praticados por empregado, preposto ou mandatários seus. A responsabilidade se estenderá aos danos causados a terceiros.

9.35. Diligenciar para que seus empregados não executem serviços que não os previstos no objeto deste Termo de Referência.

9.36. Atender as solicitações da cagece para a prorrogação do turno contratado, cabendo-lhe a adoção das providências pertinentes junto aos Sindicatos ou às Superintendências Regionais do Trabalho e Emprego.

9.37. Recrutar e contratar a mão de obra especializada em seu nome e sob sua responsabilidade, sem qualquer solidariedade da CAGECE, cabendo-lhe efetuar todos os pagamentos, inclusive os relativos aos encargos previstos na legislação trabalhista, previdenciária e fiscal, bem como de seguros e quaisquer outros decorrentes de sua condição de empregadora, assumindo, ainda, com relação ao contingente alocado, total responsabilidade pela coordenação e supervisão dos encargos administrativos, tais como: controle, fiscalização e orientação técnica, controle de frequência, ausências permitidas, licenças autorizadas, férias, punições, admissões, demissões e transferências.

9.38. Disponibilizar preposto específico para o contrato capaz de lhe representar perante a cagece, responsabilizando-se pela direção dos serviços contratados, assiduidade e pontualidade dos funcionários nos postos de trabalho, contabilização de horas extras e diárias, envio de medições, entrega (conforme o caso) de vale-transporte, vale-alimentação e fardas, dentre outras atividades inerentes ao bom desempenho dos serviços.

9.39. Disponibilizar relógio de ponto ou cartão magnético para controlar a frequência dos funcionários envolvidos na execução do contrato, respondendo por todas as despesas de instalação/manutenção derivadas dos controles de frequência. A instalação/manutenção de qualquer equipamento de controle de ponto deverá ser acompanhada por técnico da área especialista (GESAM ADM).

9.40. Entregar aos empregados até o primeiro dia do mês da prestação dos serviços, todos os vales-transportes e vales-alimentação referentes ao mês em curso.

9.41. Efetuar o pagamento do salário dos terceirizados até o quinto dia útil do mês subsequente a prestação do serviço, por meio de conta em banco comercial. A não obediência aos prazos preestabelecidos implicará a aplicação das penalidades previstas na legislação.

9.42. Efetuar se for o caso, o pagamento da diária e/ou do adiantamento de viagem até o dia anterior à realização da despesa;



9.43. Dar ciência a CAGECE, imediatamente e por escrito, de qualquer anormalidade que verificar na execução dos serviços.

9.44. Fornecer, até 15 (quinze) dias após a assinatura do contrato, crachás de identificação para todos os terceirizados, conforme modelo da CAGECE no ANEXO B deste termo.

9.45. Cumprir as demais disposições do art. 102 do Regulamento de Licitações e Contratos da CAGECE, nos prazos nele estipulados.

9.46. Responsabilizar-se exclusivamente pelo cometimento de erro ou fraude no enquadramento sindical e pelo eventual ônus financeiro decorrente, por repactuação ou por força de decisão judicial, em razão da necessidade de se proceder ao pagamento de diferenças salariais e de outras vantagens, ou ainda por intercorrências na execução dos serviços contratados, resultante da adoção de instrumento coletivo do trabalho inadequado.

10. CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

10.1. Para fins de habilitação, deverá o licitante comprovar os seguintes requisitos:

10.2. Habilitação jurídica

10.2.1. A documentação relativa à habilitação jurídica consistirá em:

10.2.1.1. Microempresas e empresas de pequeno porte: Certificado da condição de microempresa ou empresa de pequeno porte, cuja aceitação ficará condicionada à verificação da autenticidade no sítio <https://www.gov.br/empresas-e-negocios/pt-br/empreendedor>;

10.2.1.2. Sociedade empresarial, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada - EIRELI: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

10.2.1.3. Sociedade empresarial estrangeira: portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução Normativa DREI/ME nº 77, de 18 de março de 2020.

10.2.1.4. Sociedade simples: inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;

10.2.1.5. Filial, sucursal ou agência de sociedade simples ou empresária: inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz;

10.3. Qualificação técnico-operacional

10.3.1. A documentação relativa à qualificação técnico-operacional consistirá em:

10.3.1.1. Comprovação de aptidão para o desempenho de atividade pertinente e compatível em características com o objeto da licitação, mediante apresentação de atestado(s) fornecido(s) por pessoa(s) jurídica(s) de direito público ou privado.

10.3.1.1.1. Para fins da comprovação, o(s) atestado(s) deverá(ão) dizer respeito a contrato(s) executado(s) compatível(is) ao objeto, com um mínimo de 50% (cinquenta por cento) dos postos a serem contratados.

10.3.1.2. Atestados comprovando que a licitante possui experiência mínima de 01 (um) ano na execução de objeto semelhante ao da contratação.

10.3.2. O licitante disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pelo pregoeiro, cópia do contrato que deu suporte à contratação, endereço atual do contratante e local em que foi executado o contrato, dentre outros documentos.

10.3.3. Os atestados para efeito de comprovação de execução dos serviços só serão aceitos quando expedidos após a conclusão dos contratos ou decorridos no mínimo um ano do início de sua execução, exceto se houver sido firmado para ser executado em prazo inferior.

10.3.4. Serão aceitos atestados ou outros documentos hábeis emitidos por entidades estrangeiras quando acompanhados de tradução para o português, salvo se comprovada a inidoneidade da entidade emissora.

10.3.5. Não há necessidade de realização de avaliação prévia do local de execução dos serviços.

10.4. Habilitações fiscal, social e trabalhista

10.4.1. As habilitações fiscal, social e trabalhista serão aferidas mediante a verificação dos seguintes requisitos:

10.4.1.1. A inscrição no Cadastro Nacional da Pessoa Jurídica (CNPJ);

10.4.1.2. A inscrição no cadastro de contribuintes estadual e/ou municipal, se houver, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

10.4.1.3. A regularidade perante a Fazenda federal, estadual e/ou municipal do domicílio ou sede do licitante, ou outra equivalente, na forma da lei;

10.4.1.4. A regularidade relativa à Seguridade Social e ao FGTS, que demonstre cumprimento dos encargos sociais instituídos por lei;

10.4.1.5. A regularidade perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452/1943, e considerando o disposto no art. 3º da Lei nº 12.440, de 7 de julho de 2011.

10.4.1.6. O cumprimento do disposto no inciso XXXIII do art. 7º da Constituição Federal.

10.4.2. Caso o licitante seja considerado isento dos tributos estaduais e/ou municipais relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.

10.4.3. Os documentos enumerados no subitem 10.4.1. poderão ser substituídos ou supridos, no todo ou em parte, por outros meios hábeis a comprovar a regularidade do licitante, inclusive por meio eletrônico. Quanto a comprovação de atendimento do disposto nos subitens 10.4.1.3, 10.4.1.4 e 10.4.1.5 deverá ser feita na forma da legislação específica.

10.4.4. Para os Estados e Municípios que emitam prova de regularidade fiscal em separado, os proponentes deverão apresentar as respectivas certidões.

10.4.5. Os documentos relativos à regularidade fiscal somente serão exigidos, em qualquer caso, em momento posterior ao julgamento das propostas, e apenas do licitante melhor classificado.

10.5. Habilitação econômico-financeira

10.5.1. A habilitação econômico-financeira será aferida mediante a apresentação da seguinte documentação:

10.5.1.1. Certidão negativa de feitos sobre falência expedida pelo distribuidor da sede do licitante.

10.5.1.1.1. Na ausência da certidão negativa, o licitante em recuperação judicial deverá comprovar sua regularidade e viabilidade econômico-financeira mediante a apresentação de, ao menos, um dos seguintes documentos: decisão judicial que reconheça a situação de recuperação judicial; plano de recuperação em execução; demonstrações contábeis atualizadas; e, quando aplicável, prestação de garantias adicionais ou substitutivas, na forma prevista neste edital e em Lei.

10.5.1.2. Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais que comprovem a boa situação financeira da empresa, vedada a sua substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais quando encerrados há mais de três meses da data da apresentação da proposta.

10.5.1.2.1. No caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos, a demonstração de resultado de exercício e demais demonstrações contábeis limitar-se-ão ao último exercício.

10.5.1.2.2. Tratando-se de pessoas jurídicas submetidas à Escrituração Contábil Digital (ECD) por meio do Sistema Público de Escrituração Digital (Sped), admite-se a apresentação da ECD, em observância à data limite definida nas Normas da Secretaria da Receita Federal.

10.5.1.2.3. A comprovação da boa situação financeira do licitante será atestada por documento assinado por profissional legalmente habilitado, demonstrando que a empresa apresenta índices de Liquidez Geral (LG), Liquidez Corrente (LC) e Solvência Geral (SG) superiores a 1 (um);

10.5.1.2.4. Capital Circulante Líquido (CCL) ou Capital de Giro (Ativo Circulante - Passivo Circulante) de, no mínimo, 16,66% (dezesesseis inteiros e sessenta e seis centésimos por cento) do valor estimado para a contratação, índices calculados com base nas demonstrações contábeis dos 2 (dois) últimos exercícios sociais;

10.5.1.3. Patrimônio líquido mínimo de 10% (dez por cento) do valor estimado da contratação.

10.5.1.4. Patrimônio líquido igual ou superior a 1/12 (um doze avos) do valor total dos contratos firmados pelo licitante com a Administração Pública e com empresas privadas vigentes na data de abertura da licitação, levando-se em consideração apenas os valores remanescentes. Tal informação deverá ser comprovada por meio de declaração conforme Anexo III, acompanhada da Demonstração do Resultado do Exercício (DRE) relativa ao último exercício social, e se houver divergência superior a 10% (para cima ou para baixo) em relação à receita bruta discriminada na DRE, o licitante deverá apresentar as devidas justificativas para tal diferença.

10.5.1.4.1. Na declaração de que trata o subitem acima, a supressão de contratos e/ou valores remanescentes ensejará em desclassificação, se o acréscimo dos valores suprimidos ensejarem no descumprimento do disposto no subitem 10.5.1.4.

10.5.2. As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura.

10.6. Os documentos deverão ser apresentados ou pela matriz ou pela filial que estiver participando do certame, com exceção dos documentos que são válidos tanto para matriz como para as filiais como é o caso dos atestados de capacidade técnica. O contrato será celebrado com a sede que apresentou a documentação.

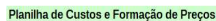
10.7. O documento obtido através de sítios oficiais, que esteja condicionado à aceitação via internet, terá sua autenticidade verificada pelo pregoeiro.

10.7.1. Os documentos têm que se encontrar dentro do prazo de validade. Na hipótese de o documento não constar expressamente a validade, este deverá ser acompanhado de declaração ou regulamentação do órgão emissor que disponha sobre sua validade. Na ausência de tal declaração ou regulamentação, o documento será considerado válido pelo prazo de 90 (noventa) dias, contados a partir da data de sua emissão, quando se tratar de documentos referentes à habilitação fiscal e econômico-financeira.

11. PLANILHA DE CUSTO E FORMAÇÃO DE PREÇOS POR CATEGORIAS

11.1. Planilha de Custos e Formação de Preços por categoria de acordo com Convenção Coletiva de Trabalho 2026/2026 e Catálogo de funções da Seplag, aprovada pela Secretária do Planejamento e Gestão do Ceará – SEPLAG-CE, conforme subitem 12.16. do edital.





Obs.1: Planilha equalizada nos parâmetros referenciais aceitos pela Administração Pública Estadual para contratação de mão de obra terceirizada
Obs.2: Planilha elaborada observando o da Convenção Coletiva 2025/2026 de Informática (CE00175/2026) e Aditivo da Convenção Coletiva de Trabalho 2025/2026 de Informática (CE000299/2026)

Memória de Cálculo

Salário-base: Definido em Convenção Coletiva de Trabalho (CCT).
13^ª, Férias e Adicional: Percentual do Submódulo 2.1, aplicado sobre o Total do Módulo 1 (EXCETO a "Intrajornada").
INSS: Percentual da Contribuição Previdenciária, aplicado sobre o Módulo 1 + Submódulo 2.1.
Outras Contribuições: Somatório dos itens (Salário Educação, SES/SESC, SENAI/SENAC, INCR, RATxVAP, SEBRAE), aplicado sobre o Módulo 1 (EXCETO a "Intrajornada") + Submódulo 2.1.
FGTS: Percentual do FGTS, aplicado sobre o Módulo 1 (EXCETO a "Intrajornada") + Submódulo 2.1.
Vale Alimentação: Valor diário do benefício definido em Convenção Coletiva de Trabalho (CCT) x Quantidade de dias trabalhados, em regra, 22 dias úteis. No caso de jornada 12x36 horas, multiplica-se por 15 dias trabalhados por mês. Descontando o percentual informando em CCT.
Cesta Básica: Valor mensal do benefício definido em Convenção Coletiva de Trabalho (CCT).
Plano de Saúde: Valor mensal do benefício definido em Convenção Coletiva de Trabalho (CCT).
API: Percentual provisionado, aplicado sobre Módulo 1 (EXCETO a "Intrajornada") + Submódulo 2.1 + Alínea 2.2.H.
API: Percentual provisionado, aplicado sobre Módulo 1 (EXCETO a "Intrajornada") + Submódulo 2.1 + Submódulo 2.2.
Multa do FGTS do API: Percentual provisionado, aplicado sobre Módulo 1 (EXCETO a "Intrajornada") + Submódulo 2.1.
Ausências: Percentual provisionado, aplicado sobre Módulo 1 (EXCETO a "Intrajornada").
EPI: Todos os itens relacionados ao EPI deverão ser objeto de pesquisa de preços.
Custos Indiretos: Percentual estimado pela licitante aplicado sobre o somatório dos Módulos 1 a 5.
Lucro: Percentual estimado pela licitante aplicado sobre o somatório dos Módulos 1 a 5, mais os Custos Indiretos.
Tributos: Tem como base de cálculo o custo unitário, que é calculado por meio do somatório dos Módulos 1 a 5, mais os Custos Indiretos e, ainda, o lucro, dividindo-se, ainda, pela diferença entre a unidade (1) e o somatório dos tributos PIS, Cofins e ISS. Por fim, o resultado dessa equação é multiplicado pelo respectivo custo unitário. Somatório dos Módulos 1 a 5.
Provisionamento: Percentual definido aplicado sobre o TOTAL, para o pagamento de verbas descritos no Termo de Referência.
SOLUÇÃO DE CONSULTA N.º 108/2023 – COSIT - A VERBA PAGA EM RAZÃO DA SUPRESSÃO PARCIAL OU TOTAL DO INTERVALO INTRAJORNADA INTEGRÀ A BASE DE CÁLCULO PARA FINS DE INCIDÊNCIA DAS CONTRIBUIÇÕES SOCIAIS PREVIDENCIÁRIAS (INSS), NÃO HAVENDO INCIDÊNCIA DE FGTS E OUTRAS CONTRIBUIÇÕES (SALÁRIO EDUCAÇÃO, SES/SESC, SENAI/SENAC, INCR, RATxVAP, SEBRAE).
Nota - Os PERCENTUAIS REFERENTES AO RISCO AMBENTAL DO TRABALHO (RAT) E AO FATOR ACIDENTÁRIO DE PREVENÇÃO (FAP), BEM COMO OS ITENS CUSTOS INDIRETOS E LUCRO, CONSTANTES DA PRESENTE PLANILHA, POSSUAM CARÁTER MERAMENTE REFERENCIAL, NÃO CONSTITUINDO PARÂMETROS MÁXIMOS OU FÍXOS. AS LICITAÇÕES DEVERÃO AUSTAR OS RESPECTIVOS PERC REALIDADE OPERACIONAL E TRIBUTÁRIA, OBSERVANDO A LEGISLAÇÃO VIGENTE APLICAR AO RATxVAP E DEMAIS NOMEAS TRABALHISTAS E PREVIDENCIÁRIAS.

11.1.7. Para dias efetivamente trabalhados, consideram-se os dias efetivos da jornada de trabalho. Exemplo: 22 (vinte e dois) dias para a jornada de 44 e 40 horas semanais, e 15 (quinze) dias para jornada 12x36.

11.1.8. O custo dos uniformes inclui todos os itens que compõem o uniforme do empregado e deve ser obtido por meio de pesquisa de preços no mercado, conforme orientações específicas da legislação vigente.

11.1.9. O custo dos equipamentos deve ser obtido por meio de pesquisa de preços no mercado, conforme orientações específicas da legislação vigente.

11.1.10. O percentual do provisionamento será definido pela Cagece, observando a necessidade de despesas consideradas eventuais e variáveis em decorrência das atividades desenvolvidas durante a prestação dos serviços, bem como o limite estabelecido no §2º do art. 9º da Instrução Normativa SEPLAG nº 004/2024, sendo vedada a alteração do referido percentual pela licitante.

11.1.11. As despesas decorrentes de auxílio-creche e auxílio-funeral, quando houver, serão pagas por meio de provisionamento.

11.1.12. O modelo da planilha de que trata este subitem encontra-se no link <https://www.seplag.ce.gov.br/gestao/terceirizacao/>

11.2. ENCARGOS SOCIAIS E TRABALHISTAS (conforme Anexo II da Instrução Normativa SEPLAG nº 004/2024)

11.2.1. MÓDULO 2.1: 13º Salário, Férias e Adicional de Férias

2.1	13º Salário, Férias e Adicional de Férias	%	Memória de Cálculo
A	13º Salário	8,33	$(1/12) \times 100$
B	Férias	8,33	$(1/12) \times 100$
C	Adicional de Férias	2,78	$[(1/3)/12] \times 100$
TOTAL		19,44	

11.2.2. MÓDULO 2.2: Encargos Previdenciários, FGTS e Outras Contribuições

2.2	Encargos Previdenciários, FGTS e Outras Contribuições	%
A	INSS	20,00
B	Salário Educação	2,50
C	Riscos Ambientais do Trabalho (RAT x FAP)	3,00 ¹
D	SESC	1,50
E	SENAC	1,00
F	SEBRAE	0,60
G	INCRA	0,20
H	FGTS	8,00
TOTAL		36,80

11.2.3. MÓDULO 3: Provisão para Rescisão

3	Provisão para Rescisão	%	Memória de Cálculo
A	Aviso Prévio Indenizado - API	0,42	$5,00\% \times 1/12$
B	Aviso Prévio Trabalhado - APT	1,85	$95,00\% \times (7/30)/12$

C	Multa do FGTS sobre o APT	3,04	$40\% \times 8,00\% \times 95,00\%$
TOTAL		5,31	

11.2.4. MÓDULO 4: Custo de Reposição do Profissional Ausente

4	Custo de Reposição do Profissional Ausente	%	Memória de Cálculo
A	Ausências Legais	2,22	$8/30/12$
B	Licença Paternidade	0,02	$1,416\%/12 \times 5/30$
C	Ausência por Acidente de Trabalho	0,05	$1,22\%/12 \times 15/30$
D	Afastamento Maternidade	0,04	$1,416\%/12 \times 4/12$
TOTAL		2,33	

1. Deve ser ajustado de acordo com o RAT da empresa. Caso haja previsão na proposta do licitante, o índice do FAP deverá ser comprovado por meio de documento hábil, conforme o item 18 do Parecer CORAG/SEORI/AUDIN-MPU nº 111/2014, bem como arredondado para 2 (duas) casas decimais.

2. Os percentuais referentes ao risco ambiental do trabalho (RAT) e ao fator acidentário de prevenção (FAP), bem como os itens custos indiretos e lucro, constantes da presente planilha, possuem caráter meramente referencial, não constituindo parâmetros máximos ou fixos. As licitantes deverão ajustar os respectivos percentuais de acordo com sua realidade operacional e tributária, observando a legislação vigente aplicável ao RAT/FAP e demais normas trabalhistas e previdenciárias.

OBS.: O valor do RAT corresponde à alíquota constante na relação de atividades preponderantes e correspondentes graus de risco, conforme a classificação nacional de atividades econômicas. (Anexo V, Decreto nº 6.957/2009)

TABELA DE TRIBUTOS	
Discriminação	Percentuais (%)
ISS	5,00
COFINS	7,60
PIS	1,65
TOTAL	14,25

12. DOS RECURSOS ORÇAMENTÁRIOS

12.1. As despesas decorrentes da contratação serão provenientes dos recursos próprios.

13. PROVISIONAMENTO:



13.1. Deverá ser incluída a previsão de provisionamento para cobrir despesas abaixo, que só serão pagas se efetivamente ocorrer, até o limite do percentual indicado na planilha de composição de custos no item 11.

- HORA EXTRA - Salário base/220*75%, conforme definido em convenção.
- HORA EXTRA DOMINGOS E FERIADOS - Salário base/220*100%, conforme definido em convenção.
- REFLEXO SOBRE O REPOUSO SEMANAL REMUNERADO - conforme definido em convenção.
- ADICIONAL NOTURNO SOBRE A HORA EXTRA - Salário base/220*21% conforme definido em convenção.
- VALE LANCHE - R\$ 14,40 (quatorze reais e quarenta centavos), conforme definido em convenção.
- DIÁRIA - R\$ 121,75 (cento e vinte e um reais e setenta e cinco centavos), conforme definido em convenção.
- AUXILIO CRECHE – R\$ R\$ 269,81 (duzentos e sessenta e nove reais e oitenta e um centavos), conforme definido em convenção coletiva.
- AUXILIO FUNERAL – valor equivalente a 03 (três) pisos salariais da categoria, na faixa que o empregado falecido estiver enquadrado, conforme definido em convenção coletiva.

14. ANEXOS DESTE TERMO DE REFERENCIA

ANEXO A - DA AVALIAÇÃO DA CONTRATADA

ANEXO B - MODELO DE CRACHÁ

ANEXO C - SEGURANÇA E MEDICINA NO TRABALHO

ANEXO A - DA AVALIAÇÃO DA CONTRATADA

DATA	AVALIAÇÃO DOS SERVIÇOS DA CONTRATADA			PERIODO
GERÊNCIA AVALIADORA:				
NOME:			MATRICULA:	
CONTRATADA:				
EMPRESA:		Nº DO CONTRATO	INICIO:	FIM:
Indicador	Peso	Descrição	Conceito	Pontuação
Obrigações Contratuais	Contratos com EPI:45% Contratos sem EPI: 55%	Efetua o pagamento dos salários até o 5º (quinto) dia útil.		
		Fornece os vales-alimentação sem atraso*		
		Realiza recolhimento dos impostos, previdência social, FGTS e todas as certidões legais exigidas no contrato*		
		Entrega os vales-transportes em dia		
		Forneceu as diárias na data avençada		
		Forneceu a farda completa na data prevista		
		Forneceu o crachá na data prevista		

		O Preposto atua de forma proativa e resolutive, responsabiliza-se pela direção dos serviços contratados, assiduidade e pontualidade dos funcionários nos postos de trabalho, contabilização de horas extras e diárias, envio de medições, entrega de vale-transporte, vale-alimentação e fardas, dentre outras atividades inerentes ao bom desempenho dos serviços.		
Segurança do Trabalho	Contratos com EPI: 10% Contratos sem EPI: 0%	Fornecer os EPI's necessários à execução dos serviços, aplicando com prioridade ações corretivas e preventivas relacionadas com acidentes de trabalho. *		
Supervisão	10%	Atua com autonomia, segurança, iniciativa, criatividade, liderança e outras qualidades inerentes à boa supervisão*		
Competência	10%	Utiliza profissionais com aceitável nível de capacitação técnica, habilidades, atitudes, apresentação pessoal e pontualidade necessária à realização dos serviços prestados*		
Comunicação	15%	Demonstra nível aceitável de relacionamento e comunicação entre seus profissionais, bem como com os da contratante*		
Planejamento, organização e controle	10%	Apresenta capacidade de planejamento e controle na execução dos serviços solicitados*		
Resultado	100%			

1. Conceitos:

Atendido (A) = peso individual total

Parcialmente Atendido (PA) = peso individual total / 2

Raramente Atendido (RA) = peso individual total / 3

Não atendido (NA) = peso individual total = 0

1. Notas explicativas sobre a Avaliação dos Serviços da Contratada:

Os itens com (*) são obrigatórios.

Os itens sobre fornecimento de fardamento e crachá serão avaliados até a data da entrega dos mesmos. No caso do crachá, será avaliado no primeiro mês do contrato ou até sua entrega e para o fardamento, a cada 06 (seis) meses ou até sua entrega.

2. Definições:

Atendido (A) = quando a contratada atende na íntegra as cláusulas contratuais dentro do prazo previsto;

Parcialmente Atendido (PA) = quando a contratada atende as cláusulas contratuais fora do prazo previsto e após recebimento de notificação por parte do gestor do contrato;

Raramente Atendido (RA) = quando a contratada atende as cláusulas contratuais fora do prazo previsto e após o recebimento de reiteradas notificações por parte do gestor do contrato;

Não atendido (NA) = quando a contratada não atende as cláusulas contratuais dentro do prazo previsto mesmo após vários recebimentos de notificações por parte do gestor do contrato.

ANEXO B - MODELO DE CRACHÁ



Crachá funcional produzido em cartão Mifare de 1K de aproximação Frequência 13,56 MHZ com número do cartão impresso. Cordão digital 25 mm, 80 cm, 100% poliéster, impressão digital, costurado e mosquete 1166 de tipo jacaré com argola. Porta crachá tipo bolsa plástica cristal, 54mm x 86mm, modelo vertical com furo. A arte dos cordões e crachás deverá ser confirmada na ASINT SEGURANÇA.

ANEXO C - SEGURANÇA E MEDICINA DO TRABALHO

As previsões gerais contidas neste anexo são gerais para as questões de Medicina e Segurança do Trabalho. As condições individuais para a prestação dos serviços, tais como EPI, insalubridade, periculosidade etc, estão identificadas nas planilhas de custos.

RESPONSABILIDADES DA CONTRATADA REFERENTES A SEGURANÇA E SAÚDE DO TRABALHADOR

1. DISPOSIÇÕES GERAIS

1.1. Cabe à empresa contratada cumprir, e fazer cumprir na execução de qualquer atividade, trabalho ou serviço solicitado pela contratante, observando rigorosamente as exigências da legislação vigente, quer sejam federais, estaduais e/ou municipais relativas à segurança, higiene e saúde do trabalho, principalmente aquelas pertinentes à Lei Nº 6.514, de 22 de Dezembro de 1977 e Portaria 3.214, de 8 de Junho de 1978, onde estão contidas as Normas Regulamentadoras - NRs.

1.2. Além da observância obrigatória anteriormente citada, a contratada também deverá obedecer a todas as normas, instruções, orientações, especificações e outras solicitações pertinentes à segurança, higiene e saúde do trabalho, estabelecidas pela CAGECE (contratante), visando à prevenção de acidentes e doenças ocupacionais e do trabalho.

1.3. A contratada deverá dimensionar seu SESMT conforme o Quadro II da NR-4 – Serviços Especializados em Engenharia de Segurança e em Medicina do Trabalho, tomando como referência o grau de risco “3”, o mesmo da CAGECE (contratante), ou “4”, no caso em que a atividade principal da contratada esteja enquadrada nesse risco.

1.4. Nos casos em que a Contratada não for legalmente obrigada a manter profissional especializado conforme o Quadro II, deverá a mesma designar ou contratar um profissional de Segurança e/ou Medicina do Trabalho (engenheiro, médico ou técnico) para cumprir as exigências da legislação vigente, de acordo com as características dos trabalhos que serão executados.

Nota: O SESMT da CAGECE (contratante), bem como qualquer preposto da CAGECE (contratante), poderá tomar qualquer medida preventiva ou corretiva que julgar necessária para manter a integridade física e prestar os primeiros socorros aos colaboradores da contratada.

2. PROGRAMAS DE SEGURANÇA E SAÚDE

2.1. A Contratada deve elaborar os seguintes Programas de Segurança e Saúde do Trabalhador:

- Programa de Prevenção de Riscos Ambientais – PPRA (NR-09);
- Programa de Condições e Meio Ambiente de Trabalho na Indústria da Construção – PCMAT (NR-18);
- Programa de Controle Médico e Saúde Ocupacional – PCMSO (NR-07).

2.2. Os programas deverão estar de acordo com as características dos trabalhos que serão executados, com ações que visem preservar a integridade física e mental dos colaboradores.

2.3. A Contratada deve submeter os Programas de Segurança e Saúde (PPRA e PCMSO) e os Laudos Técnicos de Condições do Ambiente de Trabalho (LTCAT) para análise do SESMT da CAGECE (contratante) visando sua aprovação, em até trinta dias após o início do contrato, podendo a mesma a Cagece propor modificações, adequações e correções. A CAGECE (contratante) poderá, durante o período de vigência do contrato, solicitar alterações nos Programas de Segurança e Saúde.

2.4. É de responsabilidade da Contratada a execução integral dos Programas de Segurança e Saúde e LTCAT.

2.5. A CAGECE (contratante) supervisionará a execução dos Programas de Segurança e Saúde da Contratada, através de inspeções realizadas pelo SESMT, ou por preposto designado para tal.

2.6. Os Programas de Segurança e Saúde deverão ser elaborados de forma a atender plenamente todas as Normas Regulamentadoras da Portaria 3.214/78, Normas da ABNT – Associação Brasileira de Normas Técnicas, Normas e Orientações emitidas pela CAGECE e outros documentos pertinentes.

2.7. Os Programas de Segurança e Saúde deverão ser compostos por ações que explicitem seus objetivos, períodos em que serão realizadas, responsáveis pela execução, locais onde serão realizados, públicos alvo e recursos utilizados.

2.8. Contratada deverá elaborar um “Plano de Inspeção”, com o objetivo de realizar o acompanhamento técnico dos seus empregados nos locais de trabalho, em relação às obrigações e ao cumprimento das normas de Segurança e Medicina do Trabalho, conforme atendimento de número mínimo de inspeções mensais que se segue no quadro abaixo:

Quadro de Inspeções de Segurança Mensais

ÁREA/ATIVIDADES DE ATUAÇÃO	Nº MÍNIMO DE INSPEÇÕES MENSAIS
MANUTENÇÃO DO SISTEMA DE DISTRIBUIÇÃO DE ÁGUA – CAMPO	01 INSPEÇÃO POR EQUIPE NA UNIDADE
ESTAÇÃO DE TRATAMENTO DE ÁGUA OU ELEVATÓRIA	10 INSPEÇÕES EM ETAs OU ELEV. COM EMPREGADOS
REFORMAS, MANUTENÇÃO PREDIAL OU OBRAS DE SANEAMENTO.	05 INSPEÇÕES EM FRENTES DE SERVIÇOS.
ESCRITÓRIO	01 INSPEÇÃO POR CADA GRUPO DE 10 EMPREGADOS
LABORATÓRIOS	03 INSPEÇÕES POR CADA GRUPO DE 10 EMPREGADOS
ALMOXARIFADOS	01 INSPEÇÃO
ARQUIVOS	01 INSPEÇÃO
OFICINAS ELETROMECÂNICAS	02 INSPEÇÕES

PITOMETRIA – MEDIÇÃO DE VAZÃO	04 INSPEÇÕES
OFICINA DE HIDROMETRO	02 INSPEÇÕES
MANUTENÇÃO DE REDES DE TRANSMISSÃO DE DADOS PARA INFORMÁTICA	03 INSPEÇÕES

3. COMISSÃO INTERNA DE PREVENÇÃO DE ACIDENTES – CIPA

3.1. Contratada deverá formar a Comissão Interna de Prevenção de Acidentes – CIPA, de acordo com os Quadros I e II da NR-5.

3.2. No caso em que a Contratada for legalmente obrigada a constituir a CIPA, a documentação referente às atividades da CIPA deverá ser enviada ao SESMT da CAGECE (contratante), a saber:

- Documentos referentes ao processo eleitoral e
- Calendário anual de reuniões;

3.3. No caso da desobrigação de constituição da CIPA, a Contratada deverá nomear e indicar ao SESMT da CAGECE (contratante) preposto para tratar dos assuntos relativos à Segurança e à Saúde do Trabalhador.

3.4. Quando solicitado previamente, a Contratada deverá enviar colaborador(es) ou prepostos para assistir(em), como convidado(s), às reuniões de CIPA da CAGECE (contratante).

4. FARDAMENTO E EQUIPAMENTO DE PROTEÇÃO INDIVIDUAL - EPI

4.1 (Se for o caso) A contratada, de acordo com a NR-6, deve fornecer gratuitamente aos seus colaboradores os EPIs necessários e adequados à execução dos serviços com segurança, bem como exigir o seu uso, substituí-los quando danificados ou extraviados e fazer a sua manutenção e higienização periódica.

4.2 Todos os equipamentos de proteção individual e coletiva deverão estar especificados no Programa de Prevenção de Riscos Ambientais – PPRA da Contratada.

4.3 Todo EPI deve possuir o Certificado de Aprovação - C.A., emitido pelo Ministério do Trabalho e Emprego - MTE, que deve estar gravado de forma indelével em seu corpo.

4.4 Quando for o caso, é de responsabilidade da contratada o fornecimento, desde o início ao fim do contrato, de 02 (dois) conjuntos de fardamento por semestre, sendo cada conjunto composto de no mínimo 01 (calça), 01 (camisa ou bata), 01 par de botas (botas, sapatos ou tênis), definidos a critério da contratante. O modelo do fardamento encontra-se definido no ANEXO D deste termo.

4.5 No caso das funções destinadas a trabalhar com esgoto serão fornecidos 03 (três) conjuntos de fardamentos por semestre, sendo cada conjunto composto de no mínimo 01 (calça), 01 (camisa ou bata), 01 par de botas (botas, sapatos ou tênis), definidos a critério da contratante.

4.6 Após a publicação do contrato no DOE, a empresa contratada terá 07 (sete) dias para produzir as peças pilotos dos fardamentos e apresentá-los na sede da Cagece, para aprovação das unidades GEPES SEG e GESEC em até 02 (dois) dias úteis. Somente mediante a validação por parte da Cagece, os fardamentos definitivos deverão ser confeccionados e fornecidos em até 30 (trinta) dias corridos a contar da validação das peças pilotos, a serem entregues nos locais de trabalho dos colaboradores terceirizados.

4.7 Durante a execução do contrato, semestralmente, a empresa contratada submeterá amostras dos fardamentos confeccionados à GEPES SEG e GESEC, para verificação de conformidade com a peça piloto, antes de serem distribuídos nos locais de trabalho dos terceirizados.

4.8 A contratada deverá providenciar o recolhimento dos fardamentos fornecidos aos seus colaboradores durante a vigência do contrato, por ocasião das eventuais movimentações em razão de substituições e desligamentos, nas trocas semestrais de fardamentos e no término da vigência contratual.

4.9 Quando for o caso, fornecer e manter equipamentos de proteção individual EPI adequados aos riscos das diversas funções e atividades, desde o início ao fim do contrato, não sendo permitida a realização das atividades sem a utilização dos devidos EPIs, conforme Programa de Prevenção de Riscos Ambientais (PPRA) da contratada e Norma Regulamentadora NR – 06, devendo os mesmos serem substituídos imediatamente quando inadequados, danificados ou extraviados.

4.10 Fornecer orientação sobre o uso adequado, guarda e conservação dos EPIs na entrega dos mesmos, e manter fiscalização periódica quanto a utilização.

5. COMUNICAÇÃO DE ACIDENTES DE TRABALHO – CAT

5.1. Quando da ocorrência de acidentes com lesão, a Contratada deverá adotar os seguintes procedimentos:

5.2. Providenciar a Comunicação de Acidente do Trabalho – CAT e registrá-la no posto do INSS, em no prazo máximo de 24 horas do acontecido.

5.3. Comunicar a Coordenação de Segurança, Medicina do Trabalho e Qualidade de Vida através dos telefones (085) 3101-1765 ou (085) 3101-1939.

5.4. Fazer a investigação do acidente, enviando cópia do relatório no prazo máximo de 03 (três) dias a Coordenação de Segurança, Medicina do Trabalho e Qualidade de Vida da Contratante.

5.5. Quando da ocorrência de acidente com danos materiais (veículos, equipamentos, etc.) ou acidentes com alto potencial de risco (energização acidental, falha em manobra, etc.), a contratada deverá tomar as seguintes providências.

5.6. Comunicar imediatamente a Coordenação de Segurança, Medicina do Trabalho e Qualidade de Vida da Contratante.

5.7. Promover a investigação do ocorrido e encaminhar relatório conclusivo a Coordenação de Segurança, Medicina do Trabalho e Qualidade de Vida da Contratante.

6. DAS CONDIÇÕES SANITÁRIAS E DE CONFORTO NOS LOCAIS DE TRABALHO

6.1. Sempre que a Contratada disponibilizar o local de trabalho, este deverá possuir instalações que propiciem a seus funcionários as condições exigidas pela NR-24 – Condições Sanitárias e de Conforto nos Locais de Trabalho e nos canteiros de obras, as exigências da NR-18 – Condições e Meio Ambiente de Trabalho na Indústria da Construção do Ministério do Trabalho e Emprego (MTE).

7. INÍCIO DE ATIVIDADE

7.1. Quando os perigos e riscos associados à atividade forem relevantes (atividades nas áreas de tratamento e manutenção de água, manutenção eletromecânica e elétrica e operação de equipamentos especiais), o responsável pelo SESMT (Serviço Especializado em Saúde e Medicina do Trabalho) da Contratada, ou o colaborador designado para representá-la junto a CAGECE, deverá, em até 30 dias antes do início das atividades, conhecer os locais de trabalho, acompanhado por um profissional da Coordenação de Segurança, Medicina do Trabalho e Qualidade de Vida da CAGECE.

7.2. Todos os colaboradores recém admitidos da Contratada deverão receber orientação através de treinamento com carga horária mínima de 8 horas aula no próprio local de trabalho sobre:

- Procedimentos e condições operacionais de trabalho;
- Os riscos existentes nas atividades a serem exercidas e os riscos presentes nos locais de trabalho;
- Importância da comunicação, investigação e análise de acidentes e incidentes;
- Noções básicas de Legislação em Segurança e Saúde do Trabalhador;
- Importância e obrigatoriedade do uso dos EPI e fardamentos.

7.3. A Contratada deverá promover a conscientização e prevenção de acidentes do trabalho para seus colaboradores, bem como liberá-los para participar de atividades para a prática da prevenção

de acidentes do trabalho e saúde ocupacional, quando solicitado pelo SESMT ou CIPAs da CAGECE (contratante).

7.4. Todas as ações que envolvam a segurança e saúde ocupacional deverão ser relatadas por escrito ao SESMT da CAGECE (contratante – Coordenação de Segurança, Medicina do Trabalho e Qualidade de Vida – GEPEs).

8. QUANTO A CAPACITAÇÃO DE MÃO DE OBRA SOBRE NORMAS DE SEGURANÇA

8.1. Todos os colaboradores que exercem função em área de risco elétrico e espaço confinado devem estar qualificados de acordo com o que dispõe a NR-10 – Instalações e Serviços em Eletricidade e a NR-33 - Segurança e Saúde no Trabalho em Espaços Confinados e NR-35 Trabalhos em Altura, conforme Portaria 3.214, de 08/06/78, do Ministério do Trabalho e Emprego. Os cursos de capacitação devem atender integralmente aos programas mínimos estabelecidos pelas normas regulamentadoras NR-10, NR-33 e NR-35, de forma a capacitar os colaboradores de acordo com as atividades que irão desenvolver na CAGECE.

8.2. Os trabalhadores autorizados a intervir em instalações elétricas devem possuir treinamento específico sobre os riscos decorrentes do emprego da energia elétrica e as principais medidas de prevenção de acidentes em instalações elétricas, de acordo com o estabelecido no Anexo II, da NR 10/TEM.

8.3. Os colaboradores com atuação nas estações de tratamento de água, com sistema de cloro gás (atividades com cilindro de cloro gás) somente poderão exercer suas atividades, após treinamento ou com a apresentação do certificado de treinamento em Segurança, Manuseio e Armazenamento de Cloro Gás em Cilindros usados no tratamento para desinfecção.

9. QUANTO A IDENTIFICAÇÃO DO PROFISSIONAL EM ÁREAS DE RISCO

9.1. Todos os colaboradores qualificados a executar serviços em áreas de risco (perigosas) deverão, em sua identificação profissional (crachá), possuir uma tarja amarela, conforme NISAD 018 (Norma Interna da CAGECE).

10. QUANTO À SAÚDE

10.1. A Contratada deve atender plenamente a NR-7 – Programa de Controle Médico e Saúde Ocupacional – PCMSO e realizar os exames admissionais, periódicos e demissionais, visando preservar a saúde dos colaboradores.

10.2. É de responsabilidade da Contratada arcar com todos os custos de implantação e manutenção do PCMSO, através de serviços médicos próprios ou por ela contratados.

10.3. O médico do trabalho da Contratada deve manter arquivados os prontuários dos colaboradores e emitir os atestados de saúde ocupacional, que poderão ser solicitados, a qualquer tempo, pela Coordenação de Segurança, Medicina do Trabalho e Qualidade de Vida da CAGECE (contratante) para análise.

11. QUANTO AO PAGAMENTO DO ADICIONAL DE PERICULOSIDADE OU INSALUBRIDADE

11.1. Todos os colaboradores que exercem atividades em área de risco elétrico, em condições de periculosidade, de acordo com a Lei 12.740 de 08/12/2012, que alterou o art. 193 da CLT para caracterização de atividades ou operações perigosas, fazem jus à percepção do adicional de periculosidade por eletricidade, que deve ser pago pela Contratada, mediante comprovação através de laudo técnico atualizado emitido por profissional habilitado e registrado no Conselho Regional de Engenharia e Agronomia – CREA.

11.2. Todos os colaboradores que exercem atividades em áreas insalubres de acordo com a NR-15 e seus anexos, fazem jus à percepção do adicional de insalubridade que deve ser pago pela Contratada, mediante comprovação através de laudo técnico atualizado emitido por profissional habilitado e registrado no CREA.



11.3. Os percentuais de insalubridade poderão ser alterados e atualizados por Laudo Técnico de Insalubridade e/ou Periculosidade atualizado em conformidade com as exigências da NR-15 ou NR-16 do MTE. Quando este percentual de insalubridade e periculosidade for definido em Convenção Coletiva em vigor da categoria, este percentual será adotado, desde que não venha a trazer prejuízo para o empregado, prevalecendo sobre o Laudo Técnico. E, ainda, em caso de divergência entre Laudo e Convenção, prevalecerá documento que apresentar composição de insalubridade (percentual de insalubridade e base de incidência) em que mais beneficie o empregado.

