



JUSTIÇA ELEITORAL

TRIBUNAL REGIONAL ELEITORAL DO PARÁ

Catálogo de Serviços

**COORDENADORIA DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO
E INFRAESTRUTURA DE DATA CENTER**

SUMÁRIO

I. OBJETIVO	5
a. Termos Utilizados	5
b. Serviços da Coordenadoria por categoria	6
c. Normas Complementares à PSI JE	6
II. Matriz de Responsabilidade Técnica e Dimensionamento da Equipe CGSI	8
1.1. Correio Eletrônico Corporativo	11
1.2. Proteção e Segurança Contra Infecções nas Estações e Servidores	12
1.3. Drives Compartilhados	12
1.4. Acesso Remoto - Virtual Private Network (VPN)	14
1.5. Alteração ou Configuração de Parâmetros dos Serviços Corporativos	15
1.6. Disponibilidade de Sistemas Operacionais	16
1.7. Disponibilidade e Segurança de Aplicações WEB	17
1.8. Disponibilidade da Infraestrutura dos Ativos de Segurança	18
1.9. Gestão Contínua de Vulnerabilidades	19
1.10. Monitoramento e defesa da Rede	20
1.11. Monitoração e Operação do Ambiente de Infraestrutura	21
1.12. Executar rotinas de apoio à governança de TIC	22
1.13. Administração de Ambiente Virtualizado	23
1.14. Implantação e Configuração de Cluster Kubernetes	24
1.15. Processo de Backup e Restauração de dados	25
1.16. Criação de Escopos no DHCP e Zonas no DNS	26
1.17. Gestão de Acessos – Compartilhamento de Arquivos	27
1.18. Gestão de Acessos – Controlador de Domínio	28
1.19. Inclusão/Customização/Alteração de Configuração do Servidor Zabbix	29
1.20. Mudança de Configuração em Infraestrutura de Microserviços	29
1.21. Infraestrutura de Datacenter	31
1.22. Emissão de Certificado Digital	31
1.23. Gestão e Análise de Logs de Auditoria (SIEM)	33
1.24. Tratamento e Resposta a Incidentes de Segurança da Informação	34
1.25. Gestão da Ferramenta de Prevenção à Perda de Dados (DLP)	35
1.26. Operação de Campanhas de Phishing Simulado	36
1.27. Gestão de Acesso Privilegiado (PAM)	37
1.28. Suporte à Análise de Segurança de Aplicações (SAST/DAST)	38
1.29. Suporte à Execução de Testes de Intrusão (Pentest)	39
1.30. Suporte à Descoberta e Classificação de Dados	40
1.31. Gestão de Filtro de Conteúdo Web e E-mail Gateway	41
1.32. Suporte à Gestão de Segurança de Fornecedores	42
1.33. Inteligência de Ameaças Cibernéticas (CTI)	42
1.34. Atendimentos Excepcionais (Eventual e Programado)	44
1.35. Deslocamento para Atendimento Presencial	45
Anexo 1 - IT001/CS - Tempos de Solução	46
1. Definição de Prioridade	47
2. Usuários VIPs	49
Anexo 2 - Ciclo de Vida do Catálogo de Serviços	51
HISTÓRICO DE REVISÕES / ALTERAÇÕES	53

Índice de Tabelas

Tabela 1 - Matriz de Responsabilidade Técnica	10
Tabela 2 - Correio Eletrônico	11
Tabela 3 - Proteção e Segurança Contra Infecções nas Estações e Servidores	12
Tabela 4 - Drives Compartilhados	13
Tabela 5 - Acesso Remoto - Virtual Private Network (VPN)	14
Tabela 6 - Alteração ou Configuração de Parâmetros dos Serviços Corporativos	15
Tabela 7 - Disponibilidade de Sistemas Operacionais	16
Tabela 8 - Disponibilidade e Segurança de Aplicações WEB	17
Tabela 9 - Disponibilidade da Infraestrutura dos Ativos de Segurança	18
Tabela 10 - Gestão Contínua de Vulnerabilidades	19
Tabela 11 - Monitoramento e defesa da Rede	20
Tabela 12 - Monitoração e Operação do Ambiente de Infraestrutura	21
Tabela 13 - Executar rotinas de apoio à governança de TIC	22
Tabela 14 - Administração de Ambiente Virtualizado	23
Tabela 15 - Implantação e Configuração de Cluster Kubernetes	24
Tabela 16 - Processo de Backup e Restauração de dados	25
Tabela 17 - Criação de Escopos no DHCP e Zonas no DNS	26
Tabela 18 - Gestão de Acessos – Compartilhamento de Arquivos	27
Tabela 19 - Gestão de Acessos – Controlador de Domínio	28
Tabela 20 - Inclusão/Customização/Alteração de Configuração do Servidor Zabbix	29
Tabela 21 - Mudança de Configuração em Infraestrutura de Microserviços	30
Tabela 22 - Infraestrutura de Datacenter	31
Tabela 23 - Emissão de Certificado Digital	32
Tabela 24 - Gestão e Análise de Logs de Auditoria (SIEM)	33
Tabela 25 - Tratamento e Resposta a Incidentes de Segurança da Informação	34
Tabela 26 - Gestão da Ferramenta de Prevenção à Perda de Dados (DLP)	35
Tabela 27 - Operação de Campanhas de Phishing Simulado	36
Tabela 28 - Gestão de Acesso Privilegiado (PAM)	37
Tabela 29 - Suporte à Análise de Segurança de Aplicações (SAST/DAST)	38
Tabela 30 - Suporte à Execução de Testes de Intrusão (Pentest)	39
Tabela 31 - Suporte à Descoberta e Classificação de Dados	40
Tabela 32 - Gestão de Filtro de Conteúdo Web e E-mail Gateway	41
Tabela 33 - Suporte à Gestão de Segurança de Fornecedores	42
Tabela 34 - Inteligência de Ameaças Cibernéticas (CTI)	43
Tabela 35 - Atendimentos Excepcionais (Eventual e Programado)	44
Tabela 36 - Deslocamento para Atendimento Presencial	45
Tabela 34 - Definição de urgência, impacto e tempo estimado dos atendimentos	48
Tabela 35 - Definição de urgência, impacto e tempo estimado dos atendimentos VIPs	50
Tabela 36 - Histórico de Revisões/Alterações	53

TRIBUNAL REGIONAL ELEITORAL DO PARÁ

PRESIDENTE

Des. JOSÉ MARIA TEIXEIRA DO ROSÁRIO

VICE-PRESIDENTE E CORREGEDORA

Desa. MARIA FILOMENA DE ALMEIDA BUARQUE

DIRETOR-GERAL

BRUNO GIORGI ALMEIDA E SILVA

SECRETÁRIO DE TECNOLOGIA DA INFORMAÇÃO

FELIPE HOUAT DE BRITO

SECRETÁRIA DE GESTÃO DE PESSOAS

GISELLE DE OLIVEIRA TEIXEIRA PINTO

SECRETÁRIA JUDICIÁRIO

ROSIANE REVELLE DOS SANTOS MARTINELLI

SECRETÁRIO DE ORÇAMENTO, FINANÇAS E CONTABILIDADE

RICARDO SERRUYA DE MEDEIROS

SECRETÁRIA DE ADMINISTRAÇÃO

HÉRIKA CARLA DA COSTA SODRÉ DE SOUZA

SECRETÁRIA DE PLANEJAMENTO

ELAINE CRISTINA DE JESUS SANTANA DA SILVA MACHADO

SECRETÁRIO DE AUDITORIA

EVANDRO MOREIRA RAMOS

I. OBJETIVO

Este documento visa apresentar para os usuários do TRE-PA todos os serviços da Coordenadoria de Gestão de Segurança da Informação e Infraestrutura de Data Center em produção. Para garantir que este catálogo reflita as melhores práticas de defesa cibernética e esteja alinhado aos desafios contemporâneos da segurança da informação e proteção de dados, as atividades, tarefas e serviços nele descritos foram modelados e estruturados com base no framework de Controles do Center for Internet Security (CIS) v.8. Esta abordagem assegura que a prestação de serviços pela futura contratada esteja alinhada a um padrão robusto, priorizado e reconhecido internacionalmente, focado na mitigação efetiva dos riscos cibernéticos que afetam organizações como a Justiça Eleitoral do Pará. A adoção de catálogos de serviços cujos resultados esperados e níveis mínimos de qualidade exigidos são fundamentais para assegurar a estabilidade e previsibilidade do processo de gerenciamento dos serviços de TIC.

Este catálogo não é exaustivo, outros serviços de caráter restrito, relacionados a Incidentes de Segurança da Informação, poderão fazer parte das atividades, no entanto, não serão publicados neste documento.

Todos os serviços listados neste catálogo estão sob respaldo da Política de Segurança da Informação da Justiça Eleitoral (PSI/JE), Resolução Nº 23.644, DE 1º de Julho de 2021. Este documento é parte integrante do documento do processo de Cumprimento de Requisição, Gerenciamento de Incidente que, para solicitação devem seguir os requisitos publicados na Portaria Nº 17.803/2018 que regulamenta a Central de Serviços de TI.

a. Termos Utilizados

- Descrição do Serviço: Campo destinado para uma descrição resumida do serviço.
- Categoria do Serviço: Categoria que pertence o serviço.
- Serviços: São as atividades-fim do serviço que podem ser solicitadas através da Central de Serviços de TI.
- Gerente do Serviço: Responsável dentro da STI pelo serviço.
- Grupo Solucionador: Seção que é especializada na execução do serviço solicitado. O Grupo Solucionador está separado em níveis, sendo N1 para 1º Nível de Atendimento, N2 para 2º Nível de Atendimento e por fim, N3 para 3º Nível de Atendimento.
- Pré-requisitos: Pré-requisitos quanto à solicitação ou uso do serviço.
- Restrições: Restrições quanto à solicitação ou uso do serviço.

ELABORADO POR	DATA EMISSÃO	Página
CGSI	11/07/2025	
APROVADO POR	DATA APROVAÇÃO	5/53
Coordenador / Coordenadoria	14/04/2026	

- Disponibilidade: Disponibilidade padrão do serviço. Normalmente expressa em dias ou horas, podendo ser qualquer outra medida que esteja relacionada com tempo.
- Janela do Serviço: Período padrão em que o serviço fica disponível aos clientes e usuários realizarem a solicitação junto à STI, normalmente via Central de Serviços, ou outro meio, desde que não esteja nas restrições.
- Tempo de Atendimento: Tempo médio previsto de atendimento, desde o registro da solicitação até seu encerramento. O serviço pode ser conter outros tempos de atendimento que são estabelecidos conforme a Instrução de Trabalho Anexo 1 - IT001/CS que trata do relacionamento entre urgência e impacto, estabelecendo assim a prioridade e o tempo de atendimento da solicitação.
- OBS: Campo destinado para quaisquer outras observações inerentes ao serviço em questão.

b. Serviços da Coordenadoria por categoria

A Coordenadoria Geral de Serviços de Tecnologia da Informação (CGSI/STI) detém a responsabilidade pela provisão e suporte dos serviços de segurança cibernética e infraestrutura de datacenter disponibilizados ao Tribunal Regional Eleitoral do Pará (TRE-PA). A seguir, cada serviço fornecido pela CGSI/STI via Central de Serviço é amplamente detalhado com as respectivas atividades e equipes responsáveis pelo atendimento.

c. Normas Complementares à PSI JE

O TRE-PA alinhado às estratégias e políticas, que tratam da segurança da informação no Poder Judiciário e na Justiça Eleitoral, definiu sua Política de Segurança da Informação (PSI) tendo como princípio norteador a garantia da integridade, da autenticidade, da confidencialidade, da disponibilidade e da irretratabilidade dos ativos da informação e de processamento.

Em observância ao Art. 9º da RESOLUÇÃO TSE Nº 23.644/2021, por meio da PORTARIA TSE Nº 21369/2022, foram editadas as seguintes Normas Complementares de Segurança da Informação:

- **PORTARIA Nº 22804/2024** - Dispõe sobre as regras e os procedimentos para Desenvolvimento Seguro de Software do Tribunal Regional Eleitoral do Pará.

ELABORADO POR	DATA EMISSÃO	Página 6/53
CGSI	11/07/2025	
APROVADO POR	DATA APROVAÇÃO	
Coordenador / Coordenadoria	14/04/2026	

- **PORTARIA Nº 22805/2024**- Dispõe sobre as regras e os procedimentos para gerenciamento de backup e restauração de dados no âmbito da rede corporativa de dados do Tribunal Regional Eleitoral do Pará.
- **PORTARIA Nº 22806/2024** - Institui regras para a Gestão de Identidade e o Controle de Acesso Físico e Lógico ao ambiente cibernético do Tribunal Regional Eleitoral do Pará.
- **PORTARIA Nº 22807/2024**- Estabelece a Política de Uso Aceitável dos Recursos de Tecnologia da Informação no Tribunal Regional Eleitoral do Pará.
- **PORTARIA Nº 22808/2024** - Institui norma de gerenciamento contínuo de vulnerabilidades no âmbito do TRE-PA.
- **PORTARIA Nº 22809/2024**- Dispõe sobre as regras e os procedimentos para a realização da gestão e monitoramento de registro de atividades (logs) no ambiente computacional do Tribunal Regional Eleitoral do Pará.
- **PORTARIA Nº 22810/2024** - Institui norma de configuração segura de ambientes, referente à Política de Segurança da Informação da Justiça Eleitoral.
- **PORTARIA Nº 22811/2024**- Dispõe sobre as regras e os procedimentos para gestão de riscos de segurança da informação do Tribunal Regional Eleitoral do Pará.
- **PORTARIA Nº 22812/2024**- Revoga a Portaria CSI/TRE-PA n.º 21369/2022, de 20 de julho de 2022.
- **INSTRUÇÃO NORMATIVA Nº 3** - Institui a política de uso do correio eletrônico institucional no âmbito do Tribunal Regional Eleitoral do Pará.
- **PORTARIA Nº 20718/2021** - Institui o Comitê de Crises Cibernéticas e o Protocolo de Gerenciamento de Crises Cibernéticas no âmbito do Tribunal Regional Eleitoral do Estado do Pará.
- **INSTRUÇÃO NORMATIVA Nº 1** - Dispõe sobre a emissão, revogação e utilização de certificados digitais no âmbito do Tribunal Regional Eleitoral do Pará.
- **INSTRUÇÃO NORMATIVA Nº 10** - Dispõe sobre as regras e os procedimentos para a gestão de incidentes de segurança da informação no âmbito do Tribunal Regional Eleitoral do Pará.

Os serviços pertencentes a este catálogo possuem alinhamento às diretrizes contidas nas Normas Complementares acima.

ELABORADO POR	DATA EMISSÃO	Página 7/53
CGSI	11/07/2025	
APROVADO POR	DATA APROVAÇÃO	
Coordenador / Coordenadoria	14/04/2026	

II. Matriz de Responsabilidade Técnica e Dimensionamento da Equipe CGSI

Para subsidiar o dimensionamento técnico da equipe no Termo de Referência da Contratação, o quadro a seguir apresenta a correlação entre as atividades do Catálogo de Serviços e os perfis profissionais mais adequados à sua execução.

Item	Atividade	Perfil Principal	Perfil Apoio / Segundo Nível	Justificativa
1.1	Correio Eletrônico Corporativo	ASEG-01	ASEG-02	ASEG-01 para administração da plataforma (GWS/Cloud); ASEG-02 para políticas de segurança e filtros.
1.2	Proteção e Segurança Contra Infecções (Antivírus)	ASEG-02	ASEG-01	ASEG-02 gerencia a console e políticas; ASEG-01 atua na verificação e limpeza de estações.
1.3	Drives Compartilhados	ASEG-03	ASEG-02	ASEG-03 cuida da disponibilidade do Storage/FS; ASEG-01 executa as concessões de acesso.
1.4	Acesso Remoto - VPN	ASEG-02	ASEG-01	ASEG gerencia as políticas de acesso e autenticação; ASO apoia na integração com o servidor de diretório.
1.5	Alteração/Configuração de Parâmetros de Serviços	ASEG-03	ASEG-01	Depende do serviço, mas geralmente exige perfil sênior de segurança (ASEG).
1.6	Disponibilidade de Sistemas Operacionais	ASEG-03	-	Atividade fim do Administrador de Sistemas Operacionais.
1.7	Disponibilidade e Segurança de Aplicações WEB	ASEG-03	ASEG-02	ASEG-03 garante o servidor web/app; ASEG define regras de WAF e hardening.
1.8	Disponibilidade da Infraestrutura de Segurança	ASEG-03	ASEG-02	ASEG-03 garante o "up-time" dos appliances/servers; ASEG-02 garante a configuração lógica de segurança.
1.9	Gestão Contínua de Vulnerabilidades	ASEG-03	ASEG-02	ASEG-03 analisa riscos e falsos positivos; ASEG-02 executa os scans.

ELABORADO POR	DATA EMISSÃO	Página
CGSI	11/07/2025	
APROVADO POR	DATA APROVAÇÃO	
Coordenador / Coordenadoria	14/04/2026	8/53

1.10	Monitoramento e defesa da Rede	ASEG-02	ASEG-01	Monitoramento contínuo de alertas de segurança.
1.11	Monitoração e Operação de Infraestrutura	ASEG-02	ASEG-01	Monitoramento de disponibilidade de servidores e recursos (Zabbix/Grafana).
1.12	Rotinas de apoio à governança de TIC	GERSUP	-	Atividade de nível tático/estratégico, apoio à tomada de decisão.
1.13	Administração de Ambiente Virtualizado	ASEG-03	-	Gestão de Hypervisors (VMware, Hyper-V, etc.) é típica de ASO Sênior.
1.14	Implantação e Configuração de Cluster Kubernetes	ASEG-03	-	Exige conhecimento avançado em orquestração de containers.
1.15	Processo de Backup e Restauração de dados	ASEG-03	ASEG-02	ASEG-03 define rotinas e resolve falhas; ASEG-01 pode executar restores simples sob demanda.
1.16	Criação de Escopos DHCP e Zonas DNS	ASEG-03	-	Configuração core de serviços de rede em servidores.
1.17	Gestão de Acessos – Arquivos	ASEG-01	-	Atividade rotineira e procedimental de permissão de acesso.
1.18	Gestão de Acessos – Controlador de Domínio	ASEG-02	ASEG-01	Gestão de GPOs e estrutura do AD requer conhecimento pleno; ASO apoia na saúde do AD.
1.19	Configuração do Servidor Zabbix	ASEG-03	-	Customização de ferramenta de monitoramento de infraestrutura.
1.20	Configuração em de Infra. de Microserviços	ASEG-03	-	Alta complexidade em infraestrutura moderna.
1.21	Infraestrutura de Datacenter	ASEG-03	ASEG-02	Gestão física e lógica do ambiente de processamento.
1.22	Emissão de Certificado Digital	ASEG-01		Atividade operacional de validação e emissão.
1.23	Gestão e Análise de Logs (SIEM)	ASEG-02		Análise de correlação de eventos requer perfil Sênior; Operação da ferramenta pode ser Pleno.

ELABORADO POR	DATA EMISSÃO	Página 9/53
CGSI	11/07/2025	
APROVADO POR	DATA APROVAÇÃO	
Coordenador / Coordenadoria	14/04/2026	

1.24	Resposta a Incidentes de Segurança	ASEG-02	ASEG-02	Incidentes críticos exigem o especialista mais sênior e escalonamento para o Gerente.
1.25	Gestão de Prevenção à Perda de Dados (DLP)	ASEG-03	ASEG-02	Definição de regras e análise de violações complexas (Sênior).
1.26	Operação de Campanhas de Phishing	ASEG-02	ASEG-01	Configuração e execução das campanhas.
1.27	Gestão de Acesso Privilegiado (PAM)	ASEG-03	ASEG-02	Controle de credenciais críticas requer alta senioridade e confiança.
1.28	Análise de Segurança de Aplicações (SAST/DAST)	ASEG-03	-	Exige conhecimento de desenvolvimento seguro e vulnerabilidades de código.
1.29	Testes de Intrusão (Pentest)	ASEG-03	-	Atividade altamente especializada e técnica.
1.30	Descoberta e Classificação de Dados	GERSUP	ASEG-01	Envolve entendimento de negócio e privacidade (LGPD).
1.31	Filtro de Conteúdo Web e E-mail Gateway	ASEG-03	ASEG-02	Gestão de regras de bloqueio/liberação.
1.32	Gestão de Segurança de Fornecedores	GERSUP		Envolve análise de contratos, riscos e conformidade (Compliance).

Tabela 1 - Matriz de Responsabilidade Técnica

Legenda, Descrição e Quantidade Perfis previstos para o atendimento:

Código	Descrição	QTDE
GERSUP	Gerente de suporte técnico de tecnologia da informação	1
ASEG-03	Administrador em segurança da informação - Sênior	3
ASEG-02	Administrador em segurança da informação - Pleno	2
ASEG-01	Administrador em segurança da informação - Júnior	3
TOTAL		9

ELABORADO POR	DATA EMISSÃO	Página
CGSI	11/07/2025	
APROVADO POR	DATA APROVAÇÃO	10/53
Coordenador / Coordenadoria	14/04/2026	

1.1. Correio Eletrônico Corporativo

Descrição do Serviço			
Correio eletrônico ou e-mail, é um método que permite compor, enviar e receber mensagens através de sistemas eletrônicos de comunicação, de uso pessoal e intransferível como meio de comunicação interna e externa do domínio TRE-PA.JUS.BR.			
O serviço de correio eletrônico do TRE-PA pode ser acessado através do GOOGLE GMAIL (https://mail.google.com).			
Categoria do Serviço			
Gestão de Identidade (Baseado no CIS 9: Proteções de E-mail e Navegador)			
Serviços	Alterar Grupo	Gerente do Serviço	Grupo Solucionador
Criar Conta	Suporte Funcional ¹	SDC	N1 – CS
Excluir Conta			N3 – CONTRATADA
Criar Grupo			
Excluir Grupo			
Pré-Requisitos		Restrições	
A conta de correio eletrônico somente será disponibilizada mediante abertura de chamado técnico junto à Central de Serviços de TI pelo responsável da unidade onde o usuário for lotado (Capítulo II, Art. 5º, § 2º - Instrução Normativa Nº 3, 01/08/2018).		Atendimentos fora da janela de serviço somente com autorização do Secretário da STI.	
Disponibilidade	Janela do Serviço	Tempo de Atendimento	
24 horas por dia / 7 dias da semana (24/7)	08h00min às 17h00min segunda-feira à sexta-feira (exceto feriados)	TA1 = 4 HORAS TA2 = 8 HORAS TA3 = 12 HORAS	
OBS			
Os Tempos de Atendimento podem variar conforme a prioridade definida pelo relacionamento entre a urgência e impacto do serviço e são estabelecidos pela Instrução de Trabalho Anexo 1 - IT001/CS.			
O uso do Correio Eletrônico é instituído pela Instrução Normativa Nº 3, de 01 de Agosto de 2018.			
¹ N1 – CS (Central de Serviços).			

Tabela 2 - Correio Eletrônico

ELABORADO POR	DATA EMISSÃO	Página
CGSI	11/07/2025	
APROVADO POR	DATA APROVAÇÃO	
Coordenador / Coordenadoria	14/04/2026	11/53

1.2. Proteção e Segurança Contra Infecções nas Estações e Servidores

Descrição do Serviço			
Serviço de proteção contra infecções digitais voltado à prevenção, detecção e resposta a ameaças como vírus, malwares, ransomwares e outras ameaças cibernéticas, em estações de trabalho e servidores do domínio TRE-PA.JUS.BR. A solução atua de forma contínua, com monitoramento e aplicação de políticas de segurança para garantir a integridade, confidencialidade e disponibilidade dos ativos computacionais.			
Categoria do Serviço			
Segurança da Informação \ Segurança de Endpoints (Baseado no CIS 10: Defesas contra Malware)			
Serviços		Gerente do Serviço	Grupo Solucionador
Instalar/Ativar solução de proteção em estação de trabalho ¹	Aplicar quarentena ou remoção de ameaça detectada	SDC	N1 – CS N3: SDC (Análise de Amostras, Sandbox)
Atualizar política de segurança da solução	Reinstalar/Recuperar proteção		
Verificar alerta ou incidente de infecção	Emitir relatório de segurança da estação ou servidor		
Realizar varredura sob demanda	Resposta a Incidentes		
	Suporte funcional à solução de segurança		
Pré-Requisitos		Restrições	
Solicitação formal por meio de abertura de chamado na Central de Serviços de TI. A estação ou servidor deve estar devidamente inventariado no sistema de gestão de ativos da STI.		O serviço está limitado a estações e servidores sob a responsabilidade do TRE-PA. Não é permitida a instalação da solução em dispositivos pessoais ou fora do domínio institucional.	
Disponibilidade	Janela do Serviço	Tempo de Atendimento	
24 horas por dia / 7 dias da semana (24/7)	08h00min às 17h00min segunda-feira à sexta-feira (exceto feriados)	TA1 = 2 HORAS TA2 = 12 HORAS TA3 = 24 HORAS	
OBS			
Os Tempos de Atendimento variam conforme a prioridade definida pelo relacionamento entre urgência e impacto, conforme estabelecido pela Instrução de Trabalho Anexo 1 - IT001/CS.			
O uso da solução de proteção é regulamentado por políticas internas de segurança da informação e diretrizes estabelecidas pela STI.			

Tabela 3 - Proteção e Segurança Contra Infecções nas Estações e Servidores

ELABORADO POR	DATA EMISSÃO	Página
CGSI	11/07/2025	
APROVADO POR	DATA APROVAÇÃO	
Coordenador / Coordenadoria	14/04/2026	12/53

1.3. Drives Compartilhados

Descrição do Serviço			
Drives Compartilhados são espaços de armazenamento onde os arquivos pertencem à equipe em vez de a um indivíduo. Em resumo, eles facilitam a colaboração e garantem que os arquivos permaneçam acessíveis para o time, mesmo que membros entrem ou saiam da equipe, pois a propriedade é do grupo. Benefícios dos drives compartilhados do Google: • Facilidade de compartilhamento: Qualquer pessoa com acesso ao drive compartilhado pode ver, editar e criar novos arquivos. • Compartilhamento personalizado: Os administradores do drive compartilhado podem controlar quem tem acesso ao drive e a quais arquivos eles podem acessar. • Armazenamento seguro: Os arquivos armazenados em um drive compartilhado estão protegidos pelos sistemas de segurança do Google.			
Categoria do Serviço			
Drive \ Nuvem (Baseado no CIS 3: Proteção de Dados)			
Serviços		Gerente do Serviço	Grupo Solucionador
Criar Pasta de Unidade ou Comissão		SDC	N1: CS (Solicitação de acesso) N3: SDC (Gestão da Infra)
Excluir Pasta de Unidade ou Comissão			
Compartilhar pastas ou arquivos com usuário externo.			
Restaurar arquivos de usuários desativados			
Criação de Drives Compartilhados			
Gerenciamento de Permissões			
Cópia e Upload de Arquivos			
Suporte Funcional ¹			
Pré-Requisitos		Restrições	
Autorização da chefia superior para o cumprimento da requisição.		Solicitações fora da janela de serviço somente com autorização do Secretário da STI.	
Disponibilidade	Janela do Serviço	Tempo de Atendimento	
24 horas por dia / 7 dias da semana (24/7)	08h00min às 17h00min	TA1 = 4 HORAS	
	segunda-feira à sexta-feira (exceto feriados)	TA2 = 8 HORAS	
		TA3 = 36 HORAS	
OBS			
Os Tempos de Atendimento podem variar conforme a Prioridade definida pelo relacionamento entre a urgência e impacto do serviço e são estabelecidos pela Instrução de Trabalho Anexo 1 - IT001/CS.			
¹ N1 – CS (Central de Serviços).			

Tabela 4 - Drives Compartilhados

ELABORADO POR	DATA EMISSÃO	Página
CGSI	11/07/2025	
APROVADO POR	DATA APROVAÇÃO	
Coordenador / Coordenadoria	14/04/2026	13/53

1.4. Acesso Remoto - Virtual Private Network (VPN)

Descrição do Serviço			
Compreende a disponibilização, gerenciamento e suporte ao acesso seguro à rede interna do TRE-PA (Intranet, sistemas corporativos, pastas de rede) a partir de locais externos (e.g., domicílio, trabalho de campo). O objetivo é garantir a conectividade remota, com segurança e autenticação, para magistrados, servidores e colaboradores autorizados.			
Categoria do Serviço			
Infraestrutura de Rede e Segurança (Baseado no CIS 12: Controle de Acesso à Rede)			
Serviços	Reset de senha ou reconfiguração de autenticação de múltiplos fatores (MFA) para VPN. Suporte técnico para solução de problemas de conectividade VPN. Atualização de perfis de acesso (grupos) da VPN.	Gerente do Serviço SDC	Grupo Solucionador N1: CS (Registro) N3: SDC/SSC (Execução)
Concessão de permissão de acesso à VPN. Instalação, orientação e configuração do software cliente VPN. Revogação ou bloqueio de acesso VPN.			
Pré-Requisitos		Restrições	
A solicitação deve ser formalizada via chamado na Central de Serviços de TI. A concessão de acesso deve ser requisitada e aprovada pela chefia imediata do usuário. O usuário deve possuir vínculo ativo com o TRE-PA e ter lido e concordado com os termos da Política de Segurança da Informação (PSI).		O acesso VPN é pessoal, intransferível e monitorado. É vedado o compartilhamento de credenciais (login/senha/token). O equipamento utilizado para o acesso (notebook, desktop) deve possuir software de antivírus atualizado e estar em conformidade com as diretrizes da PSI. O acesso é restrito aos serviços e sistemas estritamente necessários para a atividade laboral remota do usuário.	
Disponibilidade	Janela do Serviço	Tempo de Atendimento	
O serviço de conectividade VPN está disponível 24x7. O atendimento e suporte ao serviço (abertura de chamados, instalação, troubleshooting) seguem a janela de serviço padrão.	08h00min às 17h00min segunda-feira à sexta-feira (exceto feriados)	TA1 = 4 HORAS TA2 = 12 HORAS TA3 = 24 HORAS	
OBS			
Os Tempos de Atendimento podem variar conforme a Prioridade definida pelo relacionamento entre a urgência e impacto do serviço e são estabelecidos pela Instrução de Trabalho Anexo 1 - IT001/CS.			
¹ N1 – CS (Central de Serviços).			

Tabela 5 - Acesso Remoto - Virtual Private Network (VPN)

ELABORADO POR	DATA EMISSÃO	Página
CGSI	11/07/2025	
APROVADO POR	DATA APROVAÇÃO	
Coordenador / Coordenadoria	14/04/2026	14/53

1.5. Alteração ou Configuração de Parâmetros dos Serviços Corporativos

Descrição do Serviço			
Serviço responsável pela gestão e aplicação automática de atualizações de sistemas operacionais e softwares homologados nas estações de trabalho do TRE-PA. Tem como objetivo manter os dispositivos atualizados com as versões mais recentes, corrigindo vulnerabilidades e garantindo maior estabilidade, desempenho e segurança no ambiente corporativo.			
Categoria do Serviço			
Segurança da Informação \ Segurança de Endpoints (Baseado no CIS 16: Segurança de Software Aplicativo)			
Serviços	Emitir relatório de conformidade de atualizações Excluir estação da política de atualização automática (casos autorizados) Suporte funcional à política de atualização automática	Gerente do Serviço	Grupo Solucionador
Aplicar atualização automática de sistema operacional		SSC	N1: CS (Registro)
Aplicar atualização automática de softwares homologados			N3: Equipe de Aplicações/SSC
Verificar falhas em atualizações aplicadas			
Realizar nova tentativa de atualização			
Pré-Requisitos		Restrições	
A estação de trabalho deve estar inventariada, vinculada ao domínio institucional e conectada à rede corporativa. A solicitação deve ser realizada via Central de Serviços de TI, quando não automatizada.		Atualizações manuais ou exceções só serão realizadas mediante autorização formal da STI. Estações fora do domínio ou em rede externa não são contempladas por este serviço.	
Disponibilidade	Janela do Serviço		Tempo de Atendimento
24 horas por dia / 7 dias da semana (24/7)	08h00min às 17h00min segunda-feira à sexta-feira (exceto feriados)		TA1 = 8 HORAS TA2 = 24 HORAS TA3 = PROGRAMADA
OBS			
Os Tempos de Atendimento podem variar conforme a prioridade definida pelo relacionamento entre a urgência e o impacto do serviço, conforme estabelecido na Instrução de Trabalho Anexo 1 - IT001/CS.			
A política de atualização automática segue as diretrizes de segurança e conformidade técnica da STI e está alinhada às boas práticas recomendadas de gestão de configuração.			

Tabela 6 - Alteração ou Configuração de Parâmetros dos Serviços Corporativos

ELABORADO POR	DATA EMISSÃO	Página
CGSI	11/07/2025	
APROVADO POR	DATA APROVAÇÃO	
Coordenador / Coordenadoria	14/04/2026	15/53

1.6. Disponibilidade de Sistemas Operacionais

Descrição do Serviço			
Serviço responsável por disponibilizar, homologar e manter imagens padrão de sistemas operacionais utilizadas nas estações de trabalho e servidores do TRE-PA. Engloba a preparação, validação, distribuição e suporte às versões de sistemas operacionais aprovadas pela STI, garantindo conformidade com os requisitos técnicos e de segurança institucionais.			
Categoria do Serviço			
Gestão de Ativos e Configuração (Baseado no CIS 4: Configuração Segura de Ativos e Softwares)			
Serviços	Registrar exceções de uso de sistema operacional não padronizado (casos autorizados)	Gerente do Serviço	Grupo Solucionador
Disponibilizar imagem padrão de sistema operacional	Emitir relatório de versões implantadas	SDC	N1: CS (Reportar indisponibilidade)
Atualizar imagem de sistema operacional homologado	Suporte funcional à instalação e uso de sistema operacional		N3: SSC (Admin. de SO)
Validar compatibilidade de hardware com sistema operacional ¹			
Instalar sistema operacional homologado em estação de trabalho ¹ ou servidor			
Pré-Requisitos		Restrições	
A estação ou servidor deve estar inventariado e vinculado ao domínio institucional. A solicitação de instalação ou reinstalação de sistema operacional deve ser realizada via Central de Serviços de TI, com a devida justificativa técnica quando aplicável.		Somente serão disponibilizados sistemas operacionais homologados pela STI. A instalação de versões não autorizadas ou não suportadas depende de análise e aprovação formal. Sistemas operacionais em dispositivos pessoais não são atendidos por este serviço.	
Disponibilidade	Janela do Serviço	Tempo de Atendimento	
24 horas por dia / 7 dias da semana (24/7)	08h00min às 17h00min segunda-feira à sexta-feira (exceto feriados)	TA1 = 2 HORAS TA2 = 4 HORAS TA3 = PROGRAMADA	
OBS			
Os Tempos de Atendimento variam conforme a prioridade definida pelo relacionamento entre urgência e impacto, conforme estabelecido pela Instrução de Trabalho Anexo 1 - IT001/CS.			
A disponibilização de sistemas operacionais segue as diretrizes técnicas e de segurança estabelecidas pela STI, em conformidade com as normas internas de padronização de ambientes computacionais.			
¹ N1 – CS (Central de Serviços).			

Tabela 7 - Disponibilidade de Sistemas Operacionais

ELABORADO POR	DATA EMISSÃO	Página
CGSI	11/07/2025	
APROVADO POR	DATA APROVAÇÃO	
Coordenador / Coordenadoria	14/04/2026	16/53

1.7. Disponibilidade e Segurança de Aplicações WEB

Descrição do Serviço			
Serviço responsável por garantir a disponibilidade e segurança de aplicações web institucionais no ambiente do TRE-PA. Engloba servidores, serviços de rede, recursos de segurança e monitoramento, assegurando desempenho, escalabilidade e alta disponibilidade das soluções desenvolvidas ou contratadas para acesso via navegador.			
Categoria do Serviço			
Execução e Proteção de Aplicações (Baseado no CIS 16: Segurança de Software Aplicativo)			
Serviços	Monitorar disponibilidade e desempenho da aplicação Provisionar ambiente para aplicação web institucional Realizar backup e restauração do ambiente Publicar nova aplicação ou sistema web Análise de Logs Atualizar ambiente de hospedagem Emitir relatório de disponibilidade Gerenciar certificados digitais para aplicações Suporte funcional à infraestrutura de hospedagem	Gerente do Serviço SSC	Grupo Solucionador N1: CS (Reportar bloqueio/ataque) N3: SSC(Gestão do WAF, Análise de Alertas)
Pré-Requisitos		Restrições	
A solicitação deve ser realizada via Central de Serviços de TI, acompanhada das informações técnicas mínimas exigidas (como linguagem, banco de dados, dependências e segurança). A aplicação deve ser homologada pela área responsável antes da publicação.		Somente serão hospedadas aplicações institucionais homologadas e autorizadas pela STI. Aplicações que não atendam aos padrões técnicos ou apresentem risco à segurança poderão ser recusadas ou descontinuadas.	
Disponibilidade	Janela do Serviço	Tempo de Atendimento	
24 horas por dia / 7 dias da semana (24/7)	08h00min às 17h00min segunda-feira à sexta-feira (exceto feriados)	TA1 = 4 HORA TA2 = 8 HORAS TA3 = 16 HORAS	
OBS			
Os Tempos de Atendimento podem variar conforme a prioridade definida pelo relacionamento entre urgência e impacto do serviço, conforme estabelecido na Instrução de Trabalho Anexo 1 - IT001/CS. A infraestrutura segue padrões de segurança, alta disponibilidade e boas práticas de gerenciamento, conforme as diretrizes da STI e políticas internas de tecnologia da informação.			

Tabela 8 - Disponibilidade e Segurança de Aplicações WEB

ELABORADO POR	DATA EMISSÃO	Página
CGSI	11/07/2025	
APROVADO POR	DATA APROVAÇÃO	
Coordenador / Coordenadoria	14/04/2026	17/53

1.8. Disponibilidade da Infraestrutura dos Ativos de Segurança

Descrição do Serviço			
Serviço responsável por manter em funcionamento a infraestrutura tecnológica dos ativos de segurança da informação utilizados no ambiente do TRE-PA. Inclui a disponibilidade e operação de ferramentas como firewall, antivírus corporativo, soluções de detecção e resposta (EDR/NDR), sistemas de prevenção contra intrusões (IPS), proxies, mecanismos de controle de acesso e demais componentes críticos à proteção do ambiente institucional.			
Categoria do Serviço			
Segurança da Informação (Baseado no CIS 12: Gerenciamento de Infraestrutura de Rede)			
Serviços		Gerente do Serviço	Grupo Solucionador
Manter infraestrutura de firewall e controle de borda disponível		SDC	N1: CS (Receber alerta)
Manter infraestrutura de antivírus/EDR funcional nas estações e servidores			N3: CONTRATADA (Gestão/Health Check das ferramentas)
Manter soluções de filtragem de conteúdo e controle de acesso ativas			
Operar e manter solução de detecção e resposta a ameaças (EDR/NDR)			
Garantir disponibilidade de sistemas de prevenção contra intrusão (IPS)			
Monitorar e manter ativos de segurança atualizados			
Emitir relatórios de disponibilidade e incidentes			
Suporte funcional aos ativos de segurança			
Pré-Requisitos		Restrições	
Os ativos de segurança devem estar devidamente implantados e integrados ao ambiente de rede e sistemas do TRE-PA. As solicitações relacionadas devem ser encaminhadas via Central de Serviços de TI, conforme os critérios de acesso definidos pela STI.		A indisponibilidade ou alteração nos ativos de segurança só será permitida mediante autorização expressa da STI. O escopo se limita aos ativos homologados e operados pela instituição.	
Disponibilidade	Janela do Serviço	Tempo de Atendimento	
24 horas por dia / 7 dias da semana (24/7)	08h00min às 17h00min segunda-feira à sexta-feira (exceto feriados)	TA1 = 4 HORA TA2 = 6 HORAS TA3 = 12 HORAS	
OBS			
Os Tempos de Atendimento são definidos de acordo com a criticidade e a prioridade do incidente, conforme critérios estabelecidos pela Instrução de Trabalho Anexo 1 - IT001/CS.			
A infraestrutura dos ativos de segurança é mantida conforme as diretrizes da Política de Segurança da Informação do TRE-PA, visando à proteção da confidencialidade, integridade e disponibilidade dos serviços de TI..			

Tabela 9 - Disponibilidade da Infraestrutura dos Ativos de Segurança

ELABORADO POR	DATA EMISSÃO	Página
CGSI	11/07/2025	
APROVADO POR	DATA APROVAÇÃO	
Coordenador / Coordenadoria	14/04/2026	18/53

1.9. Gestão Contínua de Vulnerabilidades

Descrição do Serviço			
Serviço responsável pela identificação, análise, priorização, tratamento e monitoramento contínuo de vulnerabilidades em ativos de tecnologia da informação do TRE-PA. A gestão contínua de vulnerabilidades visa reduzir riscos de segurança por meio de varreduras periódicas, correções orientadas, acompanhamento de exposições e relatórios de conformidade, alinhando-se às boas práticas de segurança da informação.			
Categoria do Serviço			
Segurança da Informação \ Gestão Contínua de Vulnerabilidades (Baseado no CIS 7: Gerenciamento Contínuo de Vulnerabilidades)			
Serviços	Monitorar a evolução e a resolução de vulnerabilidades críticas Apoiar na análise de riscos relacionados a vulnerabilidades Integrar resultados a processos de gestão de ativos e mudanças Emitir relatório técnico de vulnerabilidades detectadas Suporte funcional sobre o uso da ferramenta de varredura	Gerente do Serviço SDC/SSC	Grupo Solucionador N3: SDC (Execução de Scans, Análise, Relatórios)
Pré-Requisitos		Restrições	
Os ativos a serem analisados devem estar devidamente inventariados e integrados à rede institucional. A execução de varreduras deve ser previamente agendada, considerando o impacto nos serviços e a janela de operação.		As correções sugeridas devem respeitar os critérios de homologação de sistemas e infraestrutura definidos pela STI. A execução de varreduras fora da janela de serviço requer autorização da coordenação responsável.	
Disponibilidade	Janela do Serviço	Tempo de Atendimento	
24 horas por dia / 7 dias da semana (24/7)	08h00min às 17h00min segunda-feira à sexta-feira (exceto feriados)	TA1 = 6 HORAS TA2 = 8 HORAS TA3 = 36 HORAS	
OBS			
Os Tempos de Atendimento variam conforme a prioridade do chamado, considerando o impacto e a urgência definidos na Instrução de Trabalho Anexo 1 - IT001/CS.			
A Gestão Contínua de Vulnerabilidades é realizada conforme os princípios estabelecidos na Política de Segurança da Informação do TRE-PA e segue diretrizes nacionais e internacionais de cibersegurança.			

Tabela 10 - Gestão Contínua de Vulnerabilidades

ELABORADO POR	DATA EMISSÃO	Página
CGSI	11/07/2025	
APROVADO POR	DATA APROVAÇÃO	
Coordenador / Coordenadoria	14/04/2026	19/53

1.10. Monitoramento e defesa da Rede

Descrição do Serviço			
Serviço responsável pela supervisão contínua do tráfego de rede e pela implementação de mecanismos de defesa para identificar, prevenir e responder a acessos não autorizados, comportamentos anômalos e possíveis ameaças cibernéticas no ambiente do TRE-PA. Envolve o uso de ferramentas especializadas em detecção, análise de logs, alertas de segurança, correlação de eventos e resposta a incidentes.			
Categoria do Serviço			
Infraestrutura e Operações \ Observabilidade e Monitoramento (Baseado no CIS 13: Monitoramento e Defesa da Rede)			
Serviços	Suporte Funcional	Gerente do Serviço	Grupo Solucionador
Monitorar tráfego de rede em tempo real	Gerar alertas de segurança e encaminhar para análise técnica	SDC	N1: CS (Solicitar liberação)
Detectar comportamentos anômalos e atividades suspeitas	Apoiar na resposta a incidentes de segurança de rede		N3: CONTRATADA (Monitoramento, Gestão de Regras)
Operar e manter sistemas de detecção e prevenção de intrusão (IDS/IPS)	Emitir relatórios periódicos de segurança da rede		
Correlacionar eventos de segurança em ferramentas SIEM	Suporte funcional às ferramentas de monitoramento		
Pré-Requisitos		Restrições	
Os ativos de rede e segurança devem estar devidamente integrados à infraestrutura de monitoramento. Solicitações de análise específica devem ser formalizadas via Central de Serviços de TI com a devida justificativa técnica.		O acesso aos dados de monitoramento e alertas é restrito às equipes autorizadas pela STI. A coleta e análise dos dados seguem os critérios da Política de Segurança da Informação do TRE-PA e legislações aplicáveis.	
Disponibilidade	Janela do Serviço	Tempo de Atendimento	
24 horas por dia / 7 dias da semana (24/7)	08h00min às 17h00min segunda-feira à sexta-feira (exceto feriados)	TA1 = 8 HORAS TA2 = 16 HORAS TA3 = 24 HORAS	
OBS			
Os Tempos de Atendimento são definidos conforme o grau de impacto e urgência do evento, nos termos da Instrução de Trabalho Anexo 1 - IT001/CS.			
N1 – CS (Central de Serviços).			

Tabela 11 - Monitoramento e defesa da Rede

ELABORADO POR	DATA EMISSÃO	Página
CGSI	11/07/2025	
APROVADO POR	DATA APROVAÇÃO	
Coordenador / Coordenadoria	14/04/2026	20/53

1.11. Monitoração e Operação do Ambiente de Infraestrutura

Descrição do Serviço			
Serviço responsável pela monitoração contínua e pela operação técnica dos ativos de infraestrutura de tecnologia da informação do TRE-PA, incluindo servidores, storages, equipamentos de rede, virtualização, sistemas operacionais, ambientes em nuvem e demais componentes críticos. Tem como objetivo antecipar falhas, garantir alta disponibilidade, desempenho adequado e a resposta rápida a incidentes, mantendo o funcionamento estável dos serviços institucionais.			
Categoria do Serviço			
Infraestrutura e Operações \ Observabilidade e Monitoramento (Baseado no CIS 8: Gerenciamento de Logs de Auditoria)			
Serviços	Realizar o controle de capacidade, disponibilidade e desempenho dos ativos	Gerente do Serviço	Grupo Solucionador
Monitorar continuamente os ativos de infraestrutura (servidores, rede, armazenamento etc.)	Apoiar a execução de mudanças planejadas na infraestrutura	SDC	N1: CS (Receber alerta)
Detectar e registrar falhas, degradações de desempenho e indisponibilidades	Emitir relatórios periódicos de status e alertas críticos		N3: SSC (Monitoramento de Infra/SOC)
Atuar na contenção e recuperação de incidentes de infraestrutura	Suporte funcional às equipes envolvidas na sustentação de serviços		
Executar rotinas operacionais preventivas e corretivas			
Pré-Requisitos		Restrições	
Os ativos devem estar devidamente integrados ao sistema de monitoração institucional. As ações de operação e intervenção devem respeitar os fluxos autorizados pelo processo de gestão de mudanças da STI.		Alterações nos ativos de infraestrutura só poderão ser executadas mediante aprovação prévia da STI. A monitoração aplica-se exclusivamente aos ativos sob gestão do TRE-PA.	
Disponibilidade	Janela do Serviço		Tempo de Atendimento
24 horas por dia / 7 dias da semana (24/7)	08h00min às 17h00min segunda-feira à sexta-feira (exceto feriados)		TA1 = 2 HORAS TA2 = 4 HORAS TA3 = 18 HORAS
OBS			
Os Tempos de Atendimento são definidos de acordo com a urgência e o impacto do evento, conforme critérios estabelecidos na Instrução de Trabalho Anexo 1 - IT001/CS.			
O serviço de Monitoração e Operação do Ambiente de Infraestrutura é fundamental para garantir a continuidade dos serviços de TI e está em conformidade com as políticas e normas técnicas do TRE-PA.			

Tabela 12 - Monitoração e Operação do Ambiente de Infraestrutura

ELABORADO POR	DATA EMISSÃO	Página
CGSI	11/07/2025	
APROVADO POR	DATA APROVAÇÃO	
Coordenador / Coordenadoria	14/04/2026	21/53

1.12. Executar rotinas de apoio à governança de TIC

Descrição do Serviço			
Serviço responsável pela execução de atividades operacionais, técnicas e administrativas que subsidiam os processos de governança e contratações de Tecnologia da Informação e Comunicação no âmbito do TRE-PA. Envolve o acompanhamento de indicadores, atualização de controles, apoio a auditorias, cumprimento de normativos, suporte à gestão de riscos, planejamento estratégico de TIC, e demais práticas que promovem conformidade, transparência e alinhamento da TI com os objetivos institucionais.			
Categoria do Serviço			
Infraestrutura e Operações \ Executar rotinas de apoio à governança de TIC (Baseado no CIS 14: Conscientização e Treinamento em Segurança)			
Serviços	Apoiar tarefas administrativas, processos de gestão Gestão de Contratos de TIC Executar tarefas relacionadas à conformidade com normas e boas práticas (ex: Cobit, ITIL, Resoluções do CNJ e TSE) Apoiar a elaboração de relatórios e prestação de contas da área de TI Suporte funcional à área de governança de TIC	Gerente do Serviço CGSI-GAB STI-GAB	Grupo Solucionador N2: CGSI (Gestão) N3-Apoio: CONTRATADA (Geração de evidências e relatórios)
Atualizar e acompanhar o Plano Diretor de TIC (PDTIC) Apoiar o cumprimento de metas do planejamento tático de TIC Realizar levantamento e atualização de indicadores de desempenho Acompanhar planos de ação e não conformidades de auditorias Apoiar tarefas administrativas, processos de gestão de riscos e controles internos de TIC			
Pré-Requisitos		Restrições	
As atividades de apoio à Gestão e Governança de TIC devem ser formalizadas por meio de processo administrativo no SEI, sempre vinculadas a ações previamente definidas nos instrumentos de planejamento e governança de TIC.		Alterações nos ativos de infraestrutura só poderão ser executadas mediante aprovação prévia da STI. A monitoração aplica-se exclusivamente aos ativos sob gestão do TRE-PA.	
Disponibilidade	Janela do Serviço	Tempo de Atendimento	
N/A	08h00min às 17h00min segunda-feira à sexta-feira (exceto feriados)	TA1 = 16 HORAS TA2 = 32 HORAS TA3 = 64 HORAS	
OBS			
O serviço de apoio à Governança de TIC é essencial para assegurar o alinhamento da tecnologia às diretrizes estratégicas do TRE-PA e ao cumprimento dos normativos dos órgãos de controle.			

Tabela 13 - Executar rotinas de apoio à governança de TIC

ELABORADO POR	DATA EMISSÃO	Página
CGSI	11/07/2025	
APROVADO POR	DATA APROVAÇÃO	
Coordenador / Coordenadoria	14/04/2026	22/53

1.13. Administração de Ambiente Virtualizado

Descrição do Serviço			
Serviço responsável pela instalação, configuração e disponibilização de servidores com sistema operacional Windows em ambiente virtualizado do TRE-PA. A atividade compreende a criação da máquina virtual, aplicação das configurações básicas de rede e segurança, definição de recursos computacionais, aplicação de atualizações, e entrega do ambiente pronto para uso conforme as normas da instituição.			
Categoria do Serviço			
Infraestrutura e Operações \ Executar rotinas de apoio à governança de TIC (Baseado no CIS 4: Configuração Segura de Ativos e Softwares)			
Serviços	Análise de Desempenho de ambiente virtualizado Integração ao domínio institucional, quando aplicável Configuração de usuários e permissões básicas Entrega técnica da máquina ao solicitante Suporte funcional	Gerente do Serviço	Grupo Solucionador
Criação de máquina virtual no ambiente de virtualização institucional (produção/homologação) Instalação do sistema operacional Microsoft Windows ou Linux Server Aplicação de atualizações críticas e patches de segurança Configuração de rede, firewall e parâmetros de segurança		SDC/SSC	N1: CS (Solicitar VM) N3: SDC/SSC (Admin. Virtualização)
Pré-Requisitos		Restrições	
Solicitação formalizada via chamado técnico junto à Central de Serviços de TI, com aprovação da chefia da unidade solicitante e justificativa técnica. A solicitação deve conter os requisitos mínimos da máquina, como versão do sistema operacional, finalidade, recursos desejados (CPU, memória, disco) e responsáveis pela administração da VM.		A instalação será realizada apenas em ambientes homologados pelo TRE-PA. Não serão atendidas solicitações para finalidades incompatíveis com o ambiente institucional ou que representem riscos à segurança da informação.	
Disponibilidade	Janela do Serviço	Tempo de Atendimento	
08h00min às 17h00min segunda-feira à sexta-feira (exceto feriados)	08h00min às 17h00min segunda-feira à sexta-feira (exceto feriados)	TA1 = 8 HORAS TA2 = 16 HORAS TA3 = 36 HORAS	
OBS			
Os Tempos de Atendimento seguem critérios de urgência e impacto definidos pela Instrução de Trabalho Anexo 1 - IT001/CS.			
O serviço de Instalação de Servidor Windows em Máquina Virtual contribui para a padronização, agilidade e segurança na entrega de ambientes de servidores no âmbito do TRE-PA.			

Tabela 14 - Administração de Ambiente Virtualizado

ELABORADO POR	DATA EMISSÃO	Página
CGSI	11/07/2025	
APROVADO POR	DATA APROVAÇÃO	
Coordenador / Coordenadoria	14/04/2026	23/53

1.14. Implantação e Configuração de Cluster Kubernetes

Descrição do Serviço			
Serviço responsável pela implantação, configuração e disponibilização de ambientes de orquestração de contêineres baseados em Kubernetes, visando o suporte à execução de aplicações escaláveis e resilientes no ambiente do TRE-PA. Inclui a criação do cluster, configuração de nós, aplicação de boas práticas de segurança, integração com sistemas institucionais e entrega do ambiente operacional.			
Categoria do Serviço			
Infraestrutura e Operações (Baseado no CIS 4: Configuração Segura de Ativos e Softwares)			
Serviços	Configuração de monitoramento básico e dashboards (Prometheus, Grafana, etc.) Documentação da arquitetura do cluster Suporte funcional relacionado à implantação	Gerente do Serviço	Grupo Solucionador
Criação e configuração de cluster Kubernetes (on-premises ou em nuvem, conforme ambiente do TRE-PA)		SSC	N3: SSC (Admin. Kubernetes)
Configuração de nós mestres e nós de trabalho			
Definição e aplicação de políticas de segurança e autenticação			
Integração com serviços de rede e armazenamento			
Pré-Requisitos		Restrições	
Solicitação formalizada por meio de chamado técnico junto à Central de Serviços de TI, contendo aprovação da chefia imediata da unidade solicitante, justificativa da demanda, recursos estimados (quantidade de nós, CPU, memória, armazenamento), finalidade do cluster e responsáveis técnicos pela administração da aplicação.		A implantação será realizada exclusivamente em ambientes homologados pelo TRE-PA. Não serão atendidas demandas que envolvam tecnologias não suportadas ou que contrariem as normas de segurança da informação da instituição.	
Disponibilidade	Janela do Serviço	Tempo de Atendimento	
08h00min às 17h00min	08h00min às 17h00min	TA1 = 8 HORAS	
segunda-feira à sexta-feira (exceto feriados)	segunda-feira à sexta-feira (exceto feriados)	TA2 = 24 HORAS	
		TA3 = 36 HORAS	
OBS			
Os Tempos de Atendimento variam conforme urgência e impacto da solicitação, nos termos da Instrução de Trabalho Anexo 1 - IT001/CS.			
A implantação e configuração de cluster Kubernetes fortalece a modernização da infraestrutura tecnológica do TRE-PA, promovendo automação, escalabilidade e alta disponibilidade dos serviços.			

Tabela 15 - Implantação e Configuração de Cluster Kubernetes

ELABORADO POR	DATA EMISSÃO	Página
CGSI	11/07/2025	
APROVADO POR	DATA APROVAÇÃO	
Coordenador / Coordenadoria	14/04/2026	24/53

1.15. Processo de Backup e Restauração de dados

Descrição do Serviço			
O backup, ou cópia de segurança, é fundamental para a prevenção e mitigação da perda de dados. O processo de restauração, por sua vez, possibilita a recuperação desses dados em cenários de incidentes. Em conjunto, backup e restauração são responsáveis pela cópia periódica e pela custódia de informações críticas para o TRE-PA, assegurando a proteção dos dados. A cópia de dados é realizada em disco, fita (LTO 8) e nuvem (S3).			
Categoria do Serviço			
Infraestrutura e Operações (Baseado no CIS 11: Recuperação de Dados)			
Serviços	Incluir VM na Política de Backup Realizar Restauração de Dados Configurar política de Backup Aposentar VM em Fita LTO	Gerente do Serviço SDC SSC	Grupo Solucionador N1: CS (Solicitar restore) N3: SDC/SSC (Admin. Backup)
Realizar Backup de Arquivos na Rede			
Realizar Restore de Arquivos na Rede			
Suporte Funcional			
Pré-Requisitos		Restrições	
N/A.		Solicitações fora da janela de serviço somente com autorização do Secretário da STI.	
Disponibilidade	Janela do Serviço		Tempo de Atendimento
24 horas por dia / 7 dias da semana (24/7)	08h00min às 17h00min segunda-feira à sexta-feira (exceto feriados)		TA1 = 8 HORAS TA2 = 16 HORAS TA3 = 36 HORAS
OBS			
Os Tempos de Atendimento podem variar conforme a Prioridade definida pelo relacionamento entre a urgência e impacto do serviço e são estabelecidos pela Instrução de Trabalho Anexo 1 - IT001/CS.			

Tabela 16 - Processo de Backup e Restauração de dados

ELABORADO POR	DATA EMISSÃO	Página
CGSI	11/07/2025	
APROVADO POR	DATA APROVAÇÃO	
Coordenador / Coordenadoria	14/04/2026	25/53

1.16. Criação de Escopos no DHCP e Zonas no DNS

Descrição do Serviço			
Consiste na gestão dos serviços de rede fundamentais de endereçamento IP dinâmico (DHCP) e resolução de nomes (DNS). Este serviço atende às solicitações para criação, alteração ou exclusão de escopos de rede (faixas de IP), reservas de endereços, e a criação e manutenção de zonas e registros DNS para os domínios do TRE-PA..			
Categoria do Serviço			
Gestão de serviços de Rede (Baseado no CIS 12: Gerenciamento de Infraestrutura de Rede)			
Serviços		Gerente do Serviço	Grupo
Criar, alterar ou excluir escopo DHCP.		SDC SSC	Solucionador
Criar, alterar ou excluir reserva de endereço IP no DHCP.			N1: CS (Registro)
Criar, alterar ou excluir zona de pesquisa direta/reversa no DNS.			N3: SSC (Admin. Rede/Infra)
Suporte funcional para diagnóstico de problemas relacionados a DHCP e DNS.			
Pré-Requisitos		Restrições	
A solicitação deve ser realizada via abertura de chamado técnico na Central de Serviços de TI pela equipe técnica demandante (Infraestrutura, Sistemas, etc.), contendo a justificativa técnica e todos os parâmetros necessários para a configuração (e.g., VLAN, faixa de IP, máscara, gateway, nomes de host, etc.).		A criação de novos escopos DHCP ou zonas DNS deve estar alinhada ao plano de endereçamento IP (IPAM) e à arquitetura de rede do TRE-PA. Alterações em servidores DNS e DHCP de produção devem ser realizadas de forma controlada, preferencialmente em janelas de manutenção, devido ao alto impacto potencial.	
Disponibilidade	Janela do Serviço		Tempo de Atendimento
Os serviços de rede DHCP e DNS operam em regime de alta disponibilidade, 24 horas por dia / 7 dias da semana (24/7). As atividades de configuração e suporte seguem a janela de serviço.	08h00min às 17h00min segunda-feira à sexta-feira (exceto feriados)		TA1 = 8 HORAS TA2 = 16 HORAS TA3 = 36 HORAS
OBS			
Os Tempos de Atendimento podem variar conforme a prioridade definida pelo relacionamento entre a urgência e o impacto do serviço. A gestão precisa de DHCP e DNS é um controle fundamental de segurança da informação, permitindo a segmentação de redes e garantindo que os acessos sejam direcionados aos serviços legítimos da Justiça Eleitoral do Pará.			

Tabela 17 - Criação de Escopos no DHCP e Zonas no DNS

ELABORADO POR	DATA EMISSÃO	Página
CGSI	11/07/2025	
APROVADO POR	DATA APROVAÇÃO	
Coordenador / Coordenadoria	14/04/2026	26/53

1.17. Gestão de Acessos – Compartilhamento de Arquivos

Descrição do Serviço			
O serviço de Gestão de Acessos executa as atividades necessárias para conceder acesso ao serviço de Compartilhamento de Arquivos.			
Categoria do Serviço			
Gestão de Acessos \ Compartilhamento de Arquivos (Baseado no CIS 6: Gerenciamento de Controle de Acesso)			
Serviços	Liberação de acesso em pasta de rede – Primeiro nível	Gerente do Serviço	Grupo Solucionador
Alterar acesso em pasta de rede		SDC	N1: CS (Solicitação de acesso)
Alterar proprietário de pasta de rede	Liberação de acesso em pasta de rede		N3-Seg: CONTRATADA (Auditoria/Gestão de permissões)
Excluir acesso em pasta de rede			
Pré-Requisitos		Restrições	
Autorização da chefia superior para o cumprimento da requisição.		Solicitações fora da janela de serviço somente com autorização do Secretário da STI.	
Disponibilidade	Janela do Serviço	Tempo de Atendimento	
24 horas por dia / 7 dias da semana (24/7)	08h00min às 17h00min segunda-feira à sexta-feira (exceto feriados)	TA1 = 2 HORAS TA2 = 4 HORAS TA3 = 8 HORAS	
OBS			
Os Tempos de Atendimento podem variar conforme a Prioridade definida pelo relacionamento entre a urgência e impacto do serviço e são estabelecidos pela Instrução de Trabalho Anexo 1 - IT001/CS.			

Tabela 18 - Gestão de Acessos – Compartilhamento de Arquivos

ELABORADO POR	DATA EMISSÃO	Página 27/53
CGSI	11/07/2025	
APROVADO POR	DATA APROVAÇÃO	
Coordenador / Coordenadoria	14/04/2026	

1.18. Gestão de Acessos – Controlador de Domínio

Descrição do Serviço			
Serviço responsável pela administração dos acessos vinculados ao domínio institucional do TRE-PA, por meio do controlador de domínio (Active Directory). Inclui a criação, alteração e exclusão de contas de usuários e grupos, definição de permissões em objetos do domínio, aplicação de políticas de segurança e autenticação, além de suporte a unidades organizacionais (OUs) e integração com outros serviços de rede.			
Categoria do Serviço			
Gestão de Identidade \ Usuário (Baseado no CIS 5: Gerenciamento de Contas)			
Serviços		Gerente do Serviço	Grupo Solucionador
Criar, alterar e excluir contas de usuário no domínio		SDC	N1: CS (Solicitação de acesso)
Bloquear usuário			N3-Seg: CONTRATADA (Hardening, Auditoria/Gestão de permissões)
Desbloquear usuário			
Aplicar políticas de grupo (GPOs) em unidades organizacionais (OUs)			
Integrar contas com serviços conectados ao Active Directory			
Pré-Requisitos		Restrições	
Solicitação formal por meio de chamado técnico via Central de Serviços de TI, contendo identificação completa do usuário, justificativa, sistema/recurso solicitado, tipo de permissão e autorização da chefia imediata. O acesso será concedido conforme regras estabelecidas em normativos internos.		Não serão concedidos acessos sem autorização expressa ou em desconformidade com o perfil funcional do solicitante. O compartilhamento de credenciais é proibido. Toda concessão ou revogação está sujeita a registro e auditoria.	
Disponibilidade	Janela do Serviço		Tempo de Atendimento
24 horas por dia / 7 dias da semana (24/7)	08h00min às 17h00min segunda-feira à sexta-feira (exceto feriados)		TA1 = 2 HORAS TA2 = 4 HORAS TA3 = 8 HORAS
OBS			
Os Tempos de Atendimento podem variar conforme a Prioridade definida pelo relacionamento entre a urgência e impacto do serviço e são estabelecidos pela Instrução de Trabalho Anexo 1 - IT001/CS.			

Tabela 19 - Gestão de Acessos – Controlador de Domínio

ELABORADO POR	DATA EMISSÃO	Página
CGSI	11/07/2025	
APROVADO POR	DATA APROVAÇÃO	
Coordenador / Coordenadoria	14/04/2026	28/53

1.19. Inclusão/Customização/Alteração de Configuração do Servidor Zabbix

Descrição do Serviço			
O serviço de monitoramento de ativos de TIC utiliza a ferramenta Zabbix para acompanhar o desempenho e a disponibilidade da infraestrutura de tecnologia da informação e comunicação do TRE-PA. Este serviço permite a configuração de novos monitoramentos (hosts), a criação e ajuste de templates, a configuração de alertas (triggers) e a criação de telas e painéis (dashboards) para visualização dos dados.			
Categoria do Serviço			
Monitoramento de Ativos de TIC (Baseado no CIS 13: Monitoramento e Defesa da Rede)			
Serviços	Alterar/Ajustar triggers e alertas.	Gerente do Serviço	Grupo Solucionador
Incluir novo host para monitoramento.	Criar/Alterar dashboards e telas de visualização.	SSC	N1 – CS N3 – SSC
Excluir host do monitoramento.	Suporte Funcional.		
Customizar/Criar novo template de monitoramento.			
Pré-Requisitos		Restrições	
A solicitação deve ser realizada via abertura de chamado técnico na Central de Serviços de TI, contendo a justificativa e o detalhamento técnico necessário para a configuração, e deve ser requisitada pelo gestor da área ou responsável técnico pelo ativo de TIC.		A inclusão de novos ativos no monitoramento está sujeita à homologação da equipe técnica (N2). Solicitações fora da janela de serviço somente com autorização do Secretário da STI.	
Disponibilidade	Janela do Serviço	Tempo de Atendimento	
O serviço de monitoramento opera 24 horas por dia / 7 dias da semana (24/7). As atividades de configuração seguem a janela de serviço.	08h00min às 17h00min segunda-feira à sexta-feira (exceto feriados)	TA1 = 8 HORAS TA2 = 16 HORAS TA3 = 48 HORAS	
OBS			
A correta utilização deste serviço é fundamental para garantir a segurança da informação e a proteção de dados dos sistemas da Justiça Eleitoral do Pará.			

Tabela 20 - Inclusão/Customização/Alteração de Configuração do Servidor Zabbix

ELABORADO POR	DATA EMISSÃO	Página
CGSI	11/07/2025	
APROVADO POR	DATA APROVAÇÃO	
Coordenador / Coordenadoria	14/04/2026	29/53

1.20. Mudança de Configuração em Infraestrutura de Microserviços

Descrição do Serviço			
Fornece o suporte especializado para a gestão, configuração e troubleshooting da plataforma de orquestração de contêineres (e.g., Kubernetes) que hospeda as aplicações baseadas em microserviços do TRE-PA. O serviço abrange desde a implantação de novas aplicações/serviços até a resolução de incidentes e o apoio funcional às equipes de desenvolvimento.			
Categoria do Serviço			
Gestão de Ambiente de Aplicações (Baseado no CIS 16: Segurança de Software Aplicativo)			
Serviços	Configurar políticas de rede e regras de acesso (ingress). Analisar logs e métricas da infraestrutura para diagnóstico de falhas. Suporte funcional às equipes de desenvolvimento sobre a plataforma.	Gerente do Serviço	Grupo Solucionador
Realizar a implantação (deploy) de novas versões de microserviços.		SSC	N1 – CS
Ajustar configurações de recursos (CPU, memória) dos contêineres.			N3 – SSC
Configurar variáveis de ambiente e segredos (secrets).			
Diagnosticar e solucionar problemas de comunicação entre serviços.			
Pré-Requisitos		Restrições	
A solicitação deve ser realizada via abertura de chamado técnico na Central de Serviços de TI pela equipe de desenvolvimento ou sustentação, contendo o detalhamento da mudança ou do problema, incluindo nome do serviço, ambiente (desenvolvimento, homologação, produção) e artefatos necessários (e.g., imagem do contêiner).		Alterações no ambiente de produção devem ser previamente testadas em ambiente de homologação e agendadas em janelas de manutenção. Solicitações fora da janela de serviço somente com autorização do Secretário da STI.	
Disponibilidade	Janela do Serviço	Tempo de Atendimento	
O serviço de monitoramento opera 24 horas por dia / 7 dias da semana (24/7). As atividades de configuração seguem a janela de serviço.	08h00min às 17h00min segunda-feira à sexta-feira (exceto feriados)	TA1 = 4 HORAS TA2 = 12 HORAS TA3 = 48 HORAS	
OBS			
Os Tempos de Atendimento podem variar conforme a Prioridade definida pelo relacionamento entre a urgência e impacto do serviço e são estabelecidos pela Instrução de Trabalho Anexo 1 - IT001/CS.			
A correta utilização deste serviço é fundamental para garantir a segurança da informação e a proteção de dados dos sistemas da Justiça Eleitoral do Pará.			

Tabela 21 - Mudança de Configuração em Infraestrutura de Microserviços

ELABORADO POR	DATA EMISSÃO	Página
CGSI	11/07/2025	
APROVADO POR	DATA APROVAÇÃO	
Coordenador / Coordenadoria	14/04/2026	30/53

1.21. Infraestrutura de Datacenter

Descrição do Serviço			
Conjunto de atividades relacionadas ao suporte de Infraestrutura de Datacenter Tier 3			
Categoria do Serviço			
Infraestrutura de Datacenter			
Serviços		Gerente do Serviço	Grupo Solucionador
Acompanhar e registrar parâmetros de climatização e temperatura		SDC	N1 – N/A
Controlar o acesso físico ao ambiente do Datacenter			N3 – SDC
Desligamento e Reativação Total dos Equipamentos			
Pré-Requisitos		Restrições	
O acesso ao Datacenter é restrito a pessoas previamente autorizadas e identificadas. Toda intervenção deve seguir os protocolos de segurança e operação definidos em normativos internos e registros de controle.		Solicitações fora da janela de serviço somente com autorização do Secretário da STI.	
Disponibilidade	Janela do Serviço		Tempo de Atendimento
24 horas por dia / 7 dias da semana (24/7)	08h00min às 17h00min segunda-feira à sexta-feira (exceto feriados)		TA1 = 16 HORAS TA2 = 24 HORAS TA3 = PROGRAMADA
OBS			
Os Tempos de Atendimento podem variar conforme a Prioridade definida pelo relacionamento entre a urgência e impacto do serviço e são estabelecidos pela Instrução de Trabalho Anexo 1 - IT001/CS.			
¹ SDC (Gerente do Serviço e N1).			

Tabela 22 - Infraestrutura de Datacenter

ELABORADO POR CGSI	DATA EMISSÃO 11/07/2025	Página 31/53
APROVADO POR Coordenador / Coordenadoria	DATA APROVAÇÃO 14/04/2026	

1.22. Emissão de Certificado Digital

Descrição do Serviço			
Um Certificado Digital consiste em um arquivo eletrônico que funciona como uma assinatura digital com validade jurídica. Este recurso proporciona segurança e eficiência para transações online e diversos outros serviços realizados via internet, possibilitando que indivíduos e empresas se identifiquem e assinem documentos digitalmente.			
Categoria do Serviço			
Gestão de Identidade \ Usuário \ Certificado Digital (Baseado no CIS 3: Proteção de Dados)			
Serviços		Gerente do Serviço	Grupo Solucionador
Suporte Funcional		CGSI-Gab	N1: CS (Solicitação) N3: CONTRATADA (Emissão, Renovação, Instalação)
Revogar Certificado Digital			
Instalar Token de Certificado Digital ¹			
Desbloquear Token Criptográfico ²			
Autorizar emissão de Certificado Digital			
Emitir Voucher para emissão de certificado digital			
Pré-Requisitos		Restrições	
Autorização da chefia superior para o cumprimento da requisição.		Solicitações fora da janela de serviço somente com autorização do Secretário da STI.	
Disponibilidade	Janela do Serviço	Tempo de Atendimento	
24 horas por dia / 7 dias da semana (24/7)	08h00min às 17h00min segunda-feira à sexta-feira (exceto feriados)	TA1 = 4 HORAS TA2 = 8 HORAS TA3 = PROGRAMADA	
OBS			
Os Tempos de Atendimento podem variar conforme a prioridade definida pelo relacionamento entre a urgência e impacto do serviço e são estabelecidos pela Instrução de Trabalho Anexo 1 - IT001/CS.			
¹ N1 – SAU.			
² N1 – CS (Central de Serviços).			

Tabela 23 - Emissão de Certificado Digital

ELABORADO POR	DATA EMISSÃO	Página
CGSI	11/07/2025	
APROVADO POR	DATA APROVAÇÃO	
Coordenador / Coordenadoria	14/04/2026	32/53

1.23. Gestão e Análise de Logs de Auditoria (SIEM)

Descrição do Serviço			
Serviço destinado à coleta, gerenciamento, análise e correlação de logs de auditoria (SIEM) de diversos ativos de TIC, visando a detecção proativa de ameaças, suporte a investigações e conformidade.			
Categoria do Serviço			
Gestão de Logs e Monitoramento (Baseado no CIS Control 8)			
Serviços	Gerar relatórios de eventos de segurança e conformidade. Apoiar na retenção e armazenamento seguro dos logs.	Gerente do Serviço	Grupo Solucionador
Monitorar painéis (dashboards) de eventos de segurança no SIEM. Analisar e escalar eventos correlacionados suspeitos. Manter e otimizar regras de correlação de eventos.		CGSI-Gab	N2: CONTRATADA (Monitoramento, Análise, Threat Hunting) N3: Contratada (Gestão de Crise)
Pré-Requisitos		Restrições	
Acesso às ferramentas de SIEM (Splunk/ELK/etc.). Fontes de log (Firewall, AD, Servidores, Antivírus) devidamente configuradas.		Solicitações de novas regras de correlação complexas devem ser tratadas como projeto/demanda.	
Disponibilidade	Janela do Serviço	Tempo de Atendimento	
24 horas por dia / 7 dias da semana (24/7) - para monitoramento.	08h00min às 17h00min, segunda-feira à sexta-feira (exceto feriados) - para solicitações de relatórios e ajustes.	TA1 = 2 HORAS (para alertas críticos) TA2 = 8 HORAS (para alertas médios/baixos) TA3 = PROGRAMADA (para relatórios).	
OBS			
Este serviço é vital para a proteção de dados e resposta rápida a incidentes na Justiça Eleitoral do Pará.			

Tabela 24 - Gestão e Análise de Logs de Auditoria (SIEM)

ELABORADO POR	DATA EMISSÃO	Página
CGSI	11/07/2025	
APROVADO POR	DATA APROVAÇÃO	
Coordenador / Coordenadoria	14/04/2026	33/53

1.24. Tratamento e Resposta a Incidentes de Segurança da Informação

Descrição do Serviço			
Serviço de coordenação e execução das ações de contenção, erradicação e recuperação de incidentes de segurança cibernética (ex: ransomware, vazamento de dados, negação de serviço).			
Categoria do Serviço			
Resposta a Incidentes (Baseado no CIS Control 17)			
Serviços		Gerente do Serviço	Grupo Solucionador
Realizar a triagem e classificação do incidente de segurança reportado. Executar ações de contenção imediata da ameaça (ex: isolar máquina, bloquear IP). Apoiar na investigação (análise de logs/forense) para identificar a causa raiz.		Apoiar na erradicação da ameaça e recuperação dos sistemas afetados. Documentar o incidente e as lições aprendidas (Relatório Pós-Incidente). CGSI-Gab	N1: CS (Notificação) N3: CONTRATADA (Contenção, Erradicação, Recuperação)
Pré-Requisitos		Restrições	
Notificação formal do incidente pela Central de Serviços ou monitoramento (SIEM). Disponibilidade dos gestores dos ativos afetados.		Ações de recuperação de grande porte (ex: restauração de backups) devem ser coordenadas com as equipes de infraestrutura.	
Disponibilidade	Janela do Serviço	Tempo de Atendimento	
24 horas por dia / 7 dias da semana (24/7)	24 horas por dia / 7 dias da semana (24/7)	TA1 = 1 HORA (Início da análise e contenção) O tempo de resolução (TA2/TA3) dependerá da complexidade do incidente.	
OBS			
A eficácia deste serviço impacta diretamente a continuidade dos serviços críticos da Justiça Eleitoral do Pará.			

Tabela 25 - Tratamento e Resposta a Incidentes de Segurança da Informação

ELABORADO POR	DATA EMISSÃO	Página
CGSI	11/07/2025	
APROVADO POR	DATA APROVAÇÃO	
Coordenador / Coordenadoria	14/04/2026	34/53

1.25. Gestão da Ferramenta de Prevenção à Perda de Dados (DLP)

Descrição do Serviço			
Serviço de configuração, monitoramento e resposta a alertas de violação de políticas de proteção de dados (DLP), visando prevenir o vazamento ou exfiltração de informações sensíveis (LGPD).			
Categoria do Serviço			
Proteção de Dados (Baseado no CIS Control 3)			
Serviços	Apoiar na criação e ajuste fino de regras de DLP. Gerar relatórios de conformidade de proteção de dados.	Gerente do Serviço SDC	Grupo Solucionador N3: CGSI / DPO (Tratamento de Incidentes de Vazamento)
Monitorar os alertas gerados pela solução de DLP (endpoint, e-mail, rede).			
Analisar e tratar alertas confirmados (falsos positivos vs. violações reais).			
Escalar violações confirmadas ao Encarregado de Dados (DPO) e CGSI.			
Pré-Requisitos		Restrições	
Solução de DLP implantada e funcional. Definição (classificação) dos dados sensíveis a serem monitorados.		A definição das políticas macro de DLP é responsabilidade da Governança (CGSI/Comitê de PD). A equipe de suporte executa a operação da ferramenta.	
Disponibilidade	Janela do Serviço	Tempo de Atendimento	
24 horas por dia / 7 dias da semana (24/7) - para monitoramento de alertas.	08h00min às 17h00min, segunda-feira à sexta-feira (exceto feriados) - para solicitações de relatórios e ajustes de regras.	TA1 = 4 HORAS (para alertas críticos de vazamento) TA2 = 12 HORAS (demais alertas) TA3 = PROGRAMADA (relatórios/ajustes).	
OBS			
Serviço essencial para garantir a conformidade com a LGPD no âmbito da Justiça Eleitoral do Pará.			

Tabela 26 - Gestão da Ferramenta de Prevenção à Perda de Dados (DLP)

ELABORADO POR	DATA EMISSÃO	Página 35/53
CGSI	11/07/2025	
APROVADO POR	DATA APROVAÇÃO	
Coordenador / Coordenadoria	14/04/2026	

1.26. Operação de Campanhas de Phishing Simulado

Descrição do Serviço			
Serviço técnico de suporte à execução de campanhas de phishing simulado, visando avaliar e melhorar o nível de conscientização dos usuários contra ataques de engenharia social.			
Categoria do Serviço			
Conscientização em Segurança (Baseado no CIS Control 14)			
Serviços	Gerar relatórios estatísticos sobre o resultado da campanha. Apoiar na designação de treinamentos de remediação para os usuários que falharam no teste.	Gerente do Serviço CGSI-Gab	Grupo Solucionador N1 – CS N3 – SDC
Preparar tecnicamente a plataforma de simulação de phishing (modelos, listas de alvos).			
Executar o envio controlado das campanhas simuladas.			
Monitorar e coletar as métricas de resultados (cliques, reportes, dados inseridos).			
Pré-Requisitos		Restrições	
Autorização da CGSI e do Secretário da STI para a execução da campanha.		A definição do cronograma e do público-alvo é da CGSI. A equipe de suporte operacionaliza a campanha..	
Plataforma de simulação de phishing disponível.			
Disponibilidade	Janela do Serviço	Tempo de Atendimento	
N/A (Serviço sob demanda programada)	08h00min às 17h00min, segunda-feira à sexta-feira (exceto feriados)	TA3 = PROGRAMADA (Execução conforme cronograma definido pela CGSI).	
OBS			
O fator humano é um pilar da segurança da informação, e este serviço fornece métricas para o programa de conscientização.			

Tabela 27 - Operação de Campanhas de Phishing Simulado

ELABORADO POR	DATA EMISSÃO	Página
CGSI	11/07/2025	
APROVADO POR	DATA APROVAÇÃO	
Coordenador / Coordenadoria	14/04/2026	36/53

1.27. Gestão de Acesso Privilegiado (PAM)

Descrição do Serviço			
Serviço de operação e monitoramento da solução de Gestão de Acesso Privilegiado (PAM), garantindo que todo acesso administrativo a ativos críticos seja autenticado, autorizado, registrado e auditado.			
Categoria do Serviço			
Gestão de Acesso (Baseado no CIS Control 6)			
Serviços	Monitorar e auditar sessões privilegiadas gravadas em busca de atividades suspeitas. Prestar suporte a administradores de sistemas e usuários privilegiados no uso da ferramenta PAM. Gerar relatórios de conformidade sobre acessos privilegiados.	Gerente do Serviço	Grupo Solucionador
Realizar a integração (onboarding) de novos ativos críticos (servidores, bancos de dados, equipamentos de rede) na solução PAM. Gerenciar o cofre de senhas, incluindo a rotação automática e o provisionamento de credenciais temporárias (Just-in-Time).		CGSI-Gab, SDC	N1: CS (Solicitação de Acesso) N3: SDC (Gestão da Ferramenta, Onboarding)
Pré-Requisitos		Restrições	
Solução de PAM implantada e funcional. Definição dos ativos críticos e dos perfis de acesso privilegiado.		A aprovação para concessão de acesso privilegiado é de responsabilidade do gestor do ativo, não da equipe de suporte.	
Disponibilidade	Janela do Serviço	Tempo de Atendimento	
24 horas por dia / 7 dias da semana (24/7) - para acesso à ferramenta.	08h00min às 17h00min, segunda-feira à sexta-feira (exceto feriados) - para suporte, onboarding e relatórios.	TA1 = 2 HORAS (para falhas críticas de acesso ao PAM) TA2 = 8 HORAS (para suporte e onboarding) TA3 = PROGRAMADA (para relatórios).	
OBS			
Controlar o acesso privilegiado é essencial para prevenir movimentação lateral de atacantes e proteger os dados sensíveis da Justiça Eleitoral do Pará.			

Tabela 28 - Gestão de Acesso Privilegiado (PAM)

ELABORADO POR	DATA EMISSÃO	Página
CGSI	11/07/2025	
APROVADO POR	DATA APROVAÇÃO	
Coordenador / Coordenadoria	14/04/2026	37/53

1.28. Suporte à Análise de Segurança de Aplicações (SAST/DAST)

Descrição do Serviço			
Serviço de suporte à operação de ferramentas de Análise Estática (SAST) e Dinâmica (DAST) de Segurança de Aplicações, auxiliando as equipes de desenvolvimento a identificar e corrigir vulnerabilidades no código-fonte e em aplicações em execução.			
Categoria do Serviço			
Segurança de Aplicações (Baseado no CIS Control 16)			
Serviços		Gerente do Serviço	Grupo Solucionador
Executar varreduras SAST (Static Application Security Testing) em repositórios de código. Configurar e executar varreduras DAST (Dynamic Application Security Testing) em ambientes de homologação. Realizar a triagem inicial das vulnerabilidades encontradas (análise de falsos positivos).		Apoiar as equipes de desenvolvimento na compreensão e remediação das falhas. Gerar relatórios de postura de segurança das aplicações. CGSI-Gab, SSC	N1: COSIS (Solicitação de Acesso) N3: SSC, Admin das ferramentas de Análise Estática (SAST) e Dinâmica (DAST)
Pré-Requisitos		Restrições	
Ferramentas de SAST/DAST disponíveis. Acesso aos repositórios de código e ambientes de homologação.		A correção das vulnerabilidades é de responsabilidade da equipe de desenvolvimento; a equipe de segurança (contratada) atua como suporte e auditoria.	
Disponibilidade	Janela do Serviço		Tempo de Atendimento
N/A (Serviço programado)	08h00min às 17h00min, segunda-feira à sexta-feira (exceto feriados)		TA3 = PROGRAMADA (Execução conforme cronograma de desenvolvimento ou demanda).
OBS			
Fundamental para o ciclo de vida de desenvolvimento seguro e para a segurança da informação das aplicações da Justiça Eleitoral do Pará.			

Tabela 29 - Suporte à Análise de Segurança de Aplicações (SAST/DAST)

ELABORADO POR	DATA EMISSÃO	Página
CGSI	11/07/2025	
APROVADO POR	DATA APROVAÇÃO	
Coordenador / Coordenadoria	14/04/2026	38/53

1.29. Suporte à Execução de Testes de Intrusão (Pentest)

Descrição do Serviço			
Serviço de apoio técnico, acompanhamento e suporte à remediação durante a condução de Testes de Intrusão (Pentest) e exercícios de Red Team, sejam eles executados por equipes internas ou terceiros contratados.			
Categoria do Serviço			
Teste de Intrusão (Baseado no CIS Control 18)			
Serviços		Gerente do Serviço	Grupo Solucionador
Apoiar as equipes responsáveis na implementação das correções (remediação) das falhas identificadas.		CGSI-Gab, SDC, SSC	N2 – SDC/SSC N3 – Contratada
Preparar e validar o escopo técnico (ambientes, IPs, URLs) para os testes.			
Realizar testes de revalidação (reteste) das falhas corrigidas.			
Acompanhar os testes para garantir a estabilidade dos ambientes (atuando como "blue team" de sobreaviso).			
Receber, analisar e validar os relatórios de vulnerabilidades entregues pela equipe de pentest.			
Pré-Requisitos		Restrições	
Contratação ou designação de uma equipe de Teste de Intrusão.		A equipe de suporte (contratada) não executa o teste de intrusão (para evitar conflito de interesses), mas o suporta integralmente.	
Definição do escopo e regras de engajamento (RoE) pela CGSI.			
Disponibilidade	Janela do Serviço		Tempo de Atendimento
N/A (Serviço programado)	08h00min às 17h00min, segunda-feira à sexta-feira (exceto feriados)		TA3 = PROGRAMADA (conforme cronograma do Pentest)..
OBS			
Este serviço valida a eficácia dos controles de segurança da informação e é crucial para a proteção de dados contra ataques avançados.			

Tabela 30 - Suporte à Execução de Testes de Intrusão (Pentest)

ELABORADO POR	DATA EMISSÃO	Página
CGSI	11/07/2025	
APROVADO POR	DATA APROVAÇÃO	
Coordenador / Coordenadoria	14/04/2026	39/53

1.30. Suporte à Descoberta e Classificação de Dados

Descrição do Serviço			
Serviço de suporte à operação de ferramentas e processos de Descoberta (Data Discovery) e Classificação de Dados, visando identificar onde residem dados sensíveis (LGPD) e aplicar rótulos de classificação.			
Categoria do Serviço			
Proteção de Dados (Baseado no CIS Control 3)			
Serviços		Gerente do Serviço	Grupo Solucionador
Gerar relatórios de "data mapping" (mapeamento de dados) e riscos de exposição de dados.		CGSI-Gab	N4 – Equipe de Segurança / Proteção de Dados
Executar varreduras de descoberta de dados (Data Discovery) em repositórios (File Servers, Bancos de Dados, Nuvem).			
Apoiar a configuração de outras ferramentas de segurança (DLP, PAM) com base na classificação dos dados.			
Analisar os resultados das varreduras para identificar dados sensíveis (ex: CPFs, dados eleitorais) em locais inadequados.			
Apoiar na aplicação de rótulos de classificação de sensibilidade (Público, Interno, Confidencial) nos dados.			
Pré-Requisitos		Restrições	
Ferramenta de Data Discovery/Classification.		A definição das políticas e a responsabilidade final pelo dado é do "dono do dado" (área de negócio); a equipe de suporte operacionaliza a ferramenta.	
Política de Classificação da Informação definida pela Justiça Eleitoral do Pará.			
Disponibilidade	Janela do Serviço	Tempo de Atendimento	
N/A (Serviço programado)	08h00min às 17h00min, segunda-feira à sexta-feira (exceto feriados)	TA3 = PROGRAMADA (Execução conforme cronograma de varreduras).	
OBS			
Essencial para a conformidade com a LGPD, pois não é possível proteger (DLP, Controle de Acesso) o que não se sabe que existe ou onde está.			

Tabela 31 - Suporte à Descoberta e Classificação de Dados

ELABORADO POR	DATA EMISSÃO	Página
CGSI	11/07/2025	
APROVADO POR	DATA APROVAÇÃO	
Coordenador / Coordenadoria	14/04/2026	40/53

1.31. Gestão de Filtro de Conteúdo Web e E-mail Gateway

Descrição do Serviço			
Serviço de operação e monitoramento das soluções de Secure Web Gateway (Proxy/Filtro de Conteúdo) e Secure Email Gateway (Anti-spam), visando bloquear ameaças (phishing, malware) e aplicar políticas de uso aceitável.			
Categoria do Serviço			
Proteção de Dados (Baseado no CIS Control 3)			
Serviços	Analisar e tratar alertas de navegação em sites maliciosos ou bloqueados. Gerar relatórios sobre tráfego de e-mail e navegação web.	Gerente do Serviço	Grupo Solucionador
Monitorar e analisar e-mails maliciosos em quarentena (spam, phishing, malware). Ajustar e otimizar regras de filtragem de e-mail (listas brancas/negras, regras de fluxo). Gerenciar e atualizar políticas de filtro de conteúdo web (bloqueio de categorias, URLs).		CGSI-Gab	N3 – Equipe de Segurança
Pré-Requisitos		Restrições	
Soluções de Secure Email Gateway e Secure Web Gateway implantadas. Política de Uso Aceitável de E-mail e Internet definida.		A definição das políticas (o que pode ou não ser acessado) é da CGSI; a equipe de suporte operacionaliza a ferramenta.	
Disponibilidade	Janela do Serviço	Tempo de Atendimento	
24 horas por dia / 7 dias da semana (24/7) - para monitoramento de ameaças.	08h00min às 17h00min, segunda-feira à sexta-feira (exceto feriados) - para ajustes de regras e relatórios.	TA1 = 2 HORAS (para bloqueio de ameaças críticas ativas) TA2 = 8 HORAS (para liberação de e-mails/sites legítimos bloqueados) TA3 = PROGRAMADA (para relatórios).	
OBS			
Este serviço é a linha de frente da segurança da informação contra as ameaças mais comuns (phishing) que visam os usuários da Justiça Eleitoral do Pará.			

Tabela 32 - Gestão de Filtro de Conteúdo Web e E-mail Gateway

ELABORADO POR	DATA EMISSÃO	Página
CGSI	11/07/2025	
APROVADO POR	DATA APROVAÇÃO	
Coordenador / Coordenadoria	14/04/2026	41/53

1.32. Suporte à Gestão de Segurança de Fornecedores

Descrição do Serviço			
Serviço de apoio técnico à avaliação de riscos de segurança da informação e proteção de dados (LGPD) de terceiros, fornecedores e prestadores de serviço (incluindo serviços de nuvem - SaaS, PaaS, IaaS).			
Categoria do Serviço			
Gestão de Provedores de Serviço (Baseado no CIS Control 15)			
Serviços		Gerente do Serviço	Grupo Solucionador
Apoiar na aplicação de questionários de avaliação de segurança (Security Assessment Questionnaire) em novos fornecedores.		CGSI-Gab	N2/N3 – Equipe de Segurança (Governança/Risco)
Analisar documentação de segurança de fornecedores (certificações ISO 27001, SOC 2, relatórios de pentest).			
Monitorar o cumprimento de cláusulas contratuais de segurança e LGPD por parte dos fornecedores.			
Apoiar na análise de segurança de novas soluções em nuvem (SaaS) antes da contratação.			
Gerar relatórios de risco (Risk Score) de fornecedores.			
Pré-Requisitos		Restrições	
Processo de Gestão de Riscos de Terceiros (TRM) definido pela CGSI/Administração.		A decisão final sobre a contratação de um fornecedor (aceite do risco) é da Administração/CGSI; a equipe de suporte fornece a análise técnica.	
Inventário de fornecedores críticos.			
Disponibilidade	Janela do Serviço	Tempo de Atendimento	
N/A (Serviço programado)	08h00min às 17h00min, segunda-feira à sexta-feira (exceto feriados)	TA3 = PROGRAMADA (conforme demandas de novas contratações ou reavaliações).	
OBS			
Essencial para garantir a conformidade com a LGPD (responsabilidade solidária) e proteger a Justiça Eleitoral do Pará contra riscos na cadeia de suprimentos.			

Tabela 33 - Suporte à Gestão de Segurança de Fornecedores

ELABORADO POR	DATA EMISSÃO	Página
CGSI	11/07/2025	
APROVADO POR	DATA APROVAÇÃO	
Coordenador / Coordenadoria	14/04/2026	42/53

1.33. Inteligência de Ameaças Cibernéticas (CTI)

Descrição do Serviço			
Coleta, análise e disseminação de informações sobre ameaças e adversários que possam impactar os ativos de TIC e a imagem da Justiça Eleitoral do Pará.			
Categoria do Serviço			
Detecção e Resposta a Ameaças (Baseado no CIS Control 17 e Resolução CNJ 396/2021)			
Serviços		Gerente do Serviço	Grupo Solucionador
Monitorar fontes de ameaças (Surface, Deep e Dark Web) em busca de menções ao Tribunal ou vazamento de credenciais. Analisar indicadores de comprometimento (IoCs) e alimentar ferramentas de defesa (Firewall, EDR) proativamente.		CGSI-Gab / SSC	N3 – Equipe de Segurança (Inteligência/Resposta a Incidentes)
Produzir boletins de alerta sobre novas vulnerabilidades "Zero-Day" que afetem o parque tecnológico do Pará. Monitorar campanhas de desinformação técnica que visem comprometer a integridade dos sistemas eleitorais. Apoiar na caça a ameaças (Threat Hunting) dentro da rede do Tribunal.			
Pré-Requisitos		Restrições	
Acesso a feeds de inteligência (públicos ou assinados). Integração com as ferramentas de SIEM/SOC do Tribunal.		A equipe de suporte atua na análise e recomendação; a execução de bloqueios definitivos segue o rito de aprovação da CGSI.	
Disponibilidade	Janela do Serviço	Tempo de Atendimento	
08h00min às 17h00min (Análise); 24/7 (Alertas de criticidade Alta/Crítica).	08h00min às 17h00min, segunda-feira à sexta-feira (exceto feriados)	TA2 = 8 HORAS (Para análise de vulnerabilidades novas). TA1 = 1 HORA (Para disseminação de IoCs críticos detectados em ataques ativos).	
OBS			
Este serviço eleva o nível de maturidade da Justiça Eleitoral do Pará, permitindo uma postura defensiva baseada em dados reais de atacantes, conforme preconizado pelo CNJ.			

Tabela 34 - Inteligência de Ameaças Cibernéticas (CTI)

ELABORADO POR	DATA EMISSÃO	Página
CGSI	11/07/2025	
APROVADO POR	DATA APROVAÇÃO	
Coordenador / Coordenadoria	14/04/2026	43/53

1.34. Atendimentos Excepcionais (Eventual e Programado)

Descrição do Serviço			
Compreende a execução de atividades técnicas de alta especialização (Nível 3) realizadas em horários excepcionais para garantir a continuidade operacional, resposta a incidentes críticos e manutenção da infraestrutura de segurança cibernética.			
Categoria do Serviço			
Operação e Sustentação de Infraestrutura Crítica (Baseado no CIS 17: Gerenciamento de Resposta a Incidentes e CIS 11: Recuperação de Dados)			
Serviços	Executar atualizações críticas de segurança (patches) e hardening de infraestrutura em horários de baixo impacto. Realizar testes de integridade e restauração de backups em sistemas críticos (Disaster Recovery).	Gerente do Serviço	Grupo Solucionador
Apoiar tecnicamente pleitos eleitorais oficiais ou suplementares e Testes Públicos de Segurança (TPS). Realizar janelas de manutenção programada em ativos de rede, firewalls e sistemas operacionais de servidores.		SDC / SSC	N3 – CONTRATADA (Perfis Seniores e Plenos conforme criticidade)
Pré-Requisitos		Restrições	
Abertura de chamado ou registro de incidente crítico no sistema de ITSM. Autorização prévia da fiscalização do contrato para serviços programados. Acionamento formal via plano de escalonamento em casos eventuais.		Atividades limitadas aos ativos homologados pelo Tribunal; o acionamento eventual deve respeitar o tempo de resposta estabelecido no Plano de Resposta a Incidentes da Justiça Eleitoral do Pará.	
Disponibilidade	Janela do Serviço	Tempo de Atendimento	
24 horas por dia / 7 dias da semana (24/7) - Para acionamentos críticos e manutenções agendadas.	Fora do horário regular (antes das 08h00 ou após as 17h00), finais de semana e feriados.	TA1 = 2 HORAS (Início do atendimento para incidentes críticos eventuais). TA3 = PROGRAMADA (Conforme cronograma de manutenção ou calendário eleitoral).	
OBS			
Conforme o modelo da Portaria SGD/MGI 1.070/2023, não há ônus adicional por horas extraordinárias; os custos de prontidão e escalas devem estar embutidos no valor fixo mensal vinculado aos NMS.			

Tabela 35 - Atendimentos Excepcionais (Eventual e Programado)

ELABORADO POR	DATA EMISSÃO	Página
CGSI	11/07/2025	
APROVADO POR	DATA APROVAÇÃO	
Coordenador / Coordenadoria	14/04/2026	44/53

1.35. Deslocamento para Atendimento Presencial

Descrição do Serviço			
Execução de viagens técnicas para atendimento presencial, instalações, manutenções ou resposta a incidentes de segurança em unidades da Justiça Eleitoral do Pará situadas fora da Região Metropolitana de Belém.			
Categoria do Serviço			
Suporte Logístico e Operacional de TIC			
Serviços	Executar a coleta de ativos para perícia forense digital em caso de incidentes de segurança confirmados no interior.	Gerente do Serviço	Grupo Solucionador
Deslocar profissional técnico para atendimento de suporte às eleições em Zonas Eleitorais.		SDC / SSC	Equipe Técnica da CONTRATADA (conforme perfil demandado)
Realizar auditorias físicas de segurança e conformidade de ativos (hardwares) em polos descentralizados.	Participar de testes de segurança e testes de campo em outros Regionais.		
Prestar apoio técnico presencial durante o período de Eleições em locais de difícil acesso.	Participação em Congressos e Palestras, representando o Tribunal.		
Pré-Requisitos		Restrições	
Ordem de Serviço (OS) específica autorizada pela fiscalização do contrato.		O serviço de deslocamento não gera pagamento de hora-técnica adicional (já inclusa no valor mensal), apenas o ressarcimento das despesas de viagem conforme os limites estabelecidos no TR.	
Inviabilidade de resolução do problema por acesso remoto ou mãos remotas locais.			
Aprovação prévia do cronograma e modalidade de transporte (terrestre, fluvial ou aéreo).			
Disponibilidade	Janela do Serviço	Tempo de Atendimento	
Conforme demanda e calendário eleitoral.	Horário comercial ou excepcional (se enquadrado nas modalidades Eventual/Programada).	TA3 = PROGRAMADA (Conforme o plano de viagem aprovado).	
OBS			

Tabela 36 - Deslocamento para Atendimento Presencial

ELABORADO POR	DATA EMISSÃO	Página
CGSI	11/07/2025	
APROVADO POR	DATA APROVAÇÃO	
Coordenador / Coordenadoria	14/04/2026	45/53

Anexo 1 - IT001/CS - Tempos de Solução

Este anexo institui a metodologia e os tempos de atendimento que padronizam a prestação de serviços da CGSI. Os conceitos de Urgência, Impacto e Prioridade, bem como os tempos de solução associados, devem ser adotados como o modelo conceitual para o registro, tratamento e mensuração de todas as requisições e incidentes. Ressalva-se que, dependendo da complexidade específica de processos ou serviços de segurança cibernética, o tempo de solução do serviço pode divergir do modelo padrão adotado neste anexo.

Fundamentada nas práticas da ITIL V4, notadamente "Gerenciamento de Incidentes" e "Gerenciamento de Nível de Serviço", esta padronização é essencial para a co-criação de valor. A matriz de priorização assegura que os recursos de TI sejam alocados de forma otimizada, tratando primeiramente as demandas de maior impacto para o Tribunal, e garantindo transparência na gestão das expectativas dos usuários.

ELABORADO POR	DATA EMISSÃO	Página 46/53
CGSI	11/07/2025	
APROVADO POR	DATA APROVAÇÃO	
Coordenador / Coordenadoria	14/04/2026	

1. Definição de Prioridade

Urgência x Impacto

A urgência é definida pela rapidez com que o incidente deve ser resolvido. O impacto é definido pelas perdas que o incidente esteja causando. O impacto pode ser mensurado pelo número de usuários afetados. Porém, em alguns casos, um único usuário pode ter um impacto maior.

As tarefas a seguir detalham a instalação deste serviço.

Tarefas	Passos detalhados																											
Nota: A relação entre urgência e impacto serão dados pela sequência numérica das suas respectivas tabelas.																												
As informações abaixo são utilizadas pelos documentos: Processo de Gerenciamento de Incidente, Processo de Cumprimento de Requisição e Função Central de Serviços de TI.																												
Tabela com o relacionamento entre urgência e impacto.	Definir a urgência em no máximo 03 (três) valores. A nomenclatura de cada nível é livre, assim como seus valores numéricos. • Urgência: Alta = 1 • Urgência: Média = 2 • Urgência: Baixa = 3 Definir o impacto com o mesmo número de valores da urgência. A nomenclatura de cada nível é livre, assim como seus valores numéricos. • Impacto: Alto = 1 • Impacto: Médio = 2 • Impacto: Baixo = 3 Tabela com o relacionamento entre urgência e impacto: <table><tr><th colspan="2" rowspan="2"></th><th colspan="3">IMPACTO</th></tr><tr><th>Alto (1)</th><th>Médio (2)</th><th>Baixo (3)</th></tr><tr><th rowspan="3">URGÊNCIA</th><th>Alta (1)</th><td>1</td><td>2</td><td>3</td></tr><tr><th>Média (2)</th><td>2</td><td>3</td><td>4</td></tr><tr><th>Baixa (3)</th><td>3</td><td>4</td><td>5</td></tr></table> Tabela de prioridade: <table><tr><th>Prioridade</th></tr><tr><td>1 – Alta</td></tr><tr><td>2 – Média</td></tr><tr><td>3 – Baixa</td></tr><tr><td>4 – Muito Baixa</td></tr><tr><td>5 – Planejada</td></tr></table>			IMPACTO			Alto (1)	Médio (2)	Baixo (3)	URGÊNCIA	Alta (1)	1	2	3	Média (2)	2	3	4	Baixa (3)	3	4	5	Prioridade	1 – Alta	2 – Média	3 – Baixa	4 – Muito Baixa	5 – Planejada
				IMPACTO																								
		Alto (1)	Médio (2)	Baixo (3)																								
URGÊNCIA	Alta (1)	1	2	3																								
	Média (2)	2	3	4																								
	Baixa (3)	3	4	5																								
Prioridade																												
1 – Alta																												
2 – Média																												
3 – Baixa																												
4 – Muito Baixa																												
5 – Planejada																												

ELABORADO POR	DATA EMISSÃO	Página 47/53
CGSI	11/07/2025	
APROVADO POR	DATA APROVAÇÃO	
Coordenador / Coordenadoria	14/04/2026	

	Tempos de solução para as prioridades:			
	<i>Prioridade</i>	<i>Descrição</i>	<i>Início de Atendimento</i>	<i>Tempo de Solução</i>
	1	Alta	Grupo Solucionador	1 hora
	2	Média	Grupo Solucionador	3 horas
	3	Baixa	Central de Serviços	5 horas
	4	Muito Baixa	Central de Serviços	8 horas
	5	Planejada	Conforme classificação	Requer acordo

Tabela 34 - Definição de urgência, impacto e tempo estimado dos atendimentos

ELABORADO POR	DATA EMISSÃO	Página
CGSI	11/07/2025	
APROVADO POR	DATA APROVAÇÃO	48/53
Coordenador / Coordenadoria	14/04/2026	

2. Usuários VIPs

Os usuários VIPs podem ser definidos como sendo pessoas conforme sua importância na organização ou departamentos e até serviços de TI, como PJe, Magistrados, Secretarias do Tribunal em determinados períodos.

Tarefas	Passos detalhados																						
Nota: A relação entre urgência e impacto serão dados pela sequência numérica das suas respectivas tabelas.																							
As informações abaixo são utilizadas pelos documentos: Processo de Gerenciamento de Incidente, Processo de Cumprimento de Requisição e Função Central de Serviços de TI.																							
Tabela com o relacionamento entre urgência e impacto.	Usuários VIPs definidos <table><tr><th>VIP</th><th>Observação/critério</th></tr><tr><td>Presidência / Corregedoria</td><td>- Membros da Corte e Alta Administração e secretárias.</td></tr><tr><td>SEI</td><td>- Sistema Eletrônico de Informação.</td></tr><tr><td>PJe</td><td>- Processo Judicial Eletrônico.</td></tr><tr><td>ELO</td><td>- Eleitor online.</td></tr><tr><td>Direção Geral</td><td>- Diretor Geral e assessorias jurídicas.</td></tr><tr><td>Secretarias</td><td>- Gabinete das secretarias.</td></tr><tr><td>Juizes Membros</td><td>- Juizes membros.</td></tr><tr><td>Gabinete Juizes</td><td>- Gabinete de juizes membros.</td></tr><tr><td>Financeiro</td><td>- Dezembro em virtude da execução financeira e contábil do Tribunal.</td></tr><tr><td>Zonas Eleitorais</td><td>- Dia E; Revisão biométrica; Registro de Candidaturas para eleições municipais; Fechamento de Cadastro; Prestação de contas.</td></tr></table>	VIP	Observação/critério	Presidência / Corregedoria	- Membros da Corte e Alta Administração e secretárias.	SEI	- Sistema Eletrônico de Informação.	PJe	- Processo Judicial Eletrônico.	ELO	- Eleitor online.	Direção Geral	- Diretor Geral e assessorias jurídicas.	Secretarias	- Gabinete das secretarias.	Juizes Membros	- Juizes membros.	Gabinete Juizes	- Gabinete de juizes membros.	Financeiro	- Dezembro em virtude da execução financeira e contábil do Tribunal.	Zonas Eleitorais	- Dia E; Revisão biométrica; Registro de Candidaturas para eleições municipais; Fechamento de Cadastro; Prestação de contas.
VIP	Observação/critério																						
Presidência / Corregedoria	- Membros da Corte e Alta Administração e secretárias.																						
SEI	- Sistema Eletrônico de Informação.																						
PJe	- Processo Judicial Eletrônico.																						
ELO	- Eleitor online.																						
Direção Geral	- Diretor Geral e assessorias jurídicas.																						
Secretarias	- Gabinete das secretarias.																						
Juizes Membros	- Juizes membros.																						
Gabinete Juizes	- Gabinete de juizes membros.																						
Financeiro	- Dezembro em virtude da execução financeira e contábil do Tribunal.																						
Zonas Eleitorais	- Dia E; Revisão biométrica; Registro de Candidaturas para eleições municipais; Fechamento de Cadastro; Prestação de contas.																						

ELABORADO POR	DATA EMISSÃO	Página
CGSI	11/07/2025	
APROVADO POR	DATA APROVAÇÃO	49/53
Coordenador / Coordenadoria	14/04/2026	

	Tempos de solução para as prioridades para usuários VIPs:			
	Prioridade	Descrição	Início de Atendimento	Tempo de Solução
	1	Alta	Grupo Solucionador	1 hora
	2	Média	Grupo Solucionador	2 horas
	3	Baixa	Central de Serviços	3 horas
	4	Muito Baixa	Central de Serviços	4 horas
	5	Planejada	Conforme classificação	Requer acordo

Tabela 35 - Definição de urgência, impacto e tempo estimado dos atendimentos VIPs

ELABORADO POR	DATA EMISSÃO	Página 50/53
CGSI	11/07/2025	
APROVADO POR	DATA APROVAÇÃO	
Coordenador / Coordenadoria	14/04/2026	

Anexo 2 - Ciclo de Vida do Catálogo de Serviços

A revisão do Catálogo de Serviços será coordenada pela fiscalização do contrato e deverá ser formalmente iniciada sempre que houver a ocorrência de um ou mais dos seguintes "gatilhos" operacionais ou regulatórios:

- a) **Evolução de Processos:** Identificação de que os fluxos de trabalho ou os procedimentos operacionais padrão (POPs) para a execução dos serviços de segurança evoluíram, exigindo o ajuste das tarefas descritas no Catálogo para manter a aderência à realidade técnica do Tribunal;
- b) **Melhoria Contínua e Ajuste de Objeto da Contratação:** Necessidade de readequação das atividades técnicas para melhor alinhamento ao objeto contratual, visando o incremento da eficiência operacional, a correção de desvios ou a otimização da entrega dos serviços;
- c) **Atualização de Frameworks e Normativos:** Publicação de novas versões ou atualizações relevantes em frameworks de referência (ex: Controles CIS, ISO/IEC 27001, NIST) ou marcos regulatórios (ex: Resoluções do CNJ, LGPD e normas do TSE), que exijam a adequação imediata das tarefas contratadas para garantir a conformidade da **Justiça Eleitoral do Pará**.

A fiscalização do contrato será responsável por consolidar a nova versão do Catálogo, assegurando o registro histórico das versões anteriores para fins de auditoria e controle da execução contratual.

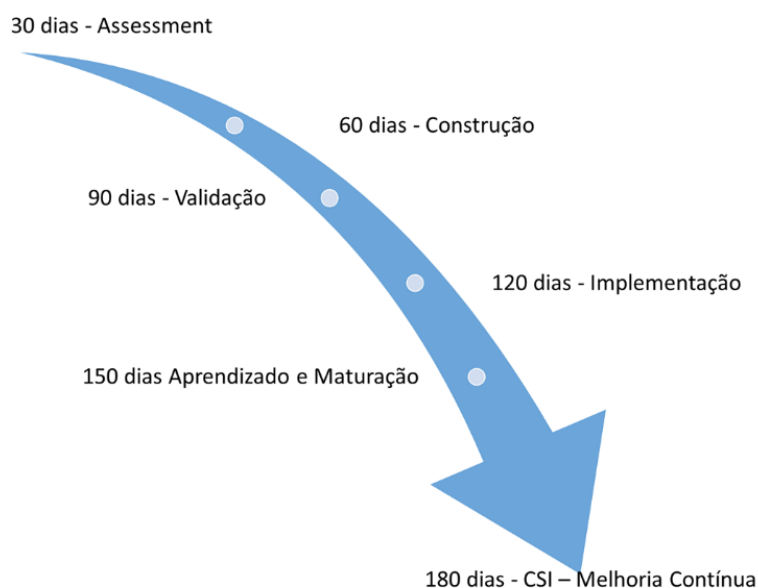
Ciclo de Implementação e Estabilização (Timeline T+)

Durante o ciclo de maturação e execução continuada, a equipe técnica promoverá a revisão estruturada do Catálogo seguindo o cronograma de 180 dias para a estabilização completa, conforme as etapas abaixo:

ELABORADO POR	DATA EMISSÃO	Página 51/53
CGSI	11/07/2025	
APROVADO POR	DATA APROVAÇÃO	
Coordenador / Coordenadoria	14/04/2026	

- **T+30 dias – Diagnóstico (Assessment):** Levantamento situacional e análise crítica das tarefas vigentes frente às necessidades de segurança.
- **T+60 dias – Planejamento e Redesenho:** Elaboração da minuta da nova versão do catálogo e revisão dos fluxos de atendimento.
- **T+90 dias – Validação Técnica:** Realização de testes de hipóteses e validação das novas atividades junto às áreas interessadas.
- **T+120 dias – Implantação Operacional:** Entrada em produção das novas definições e aferição inicial de produtividade.
- **T+150 dias – Maturação e Ajuste Fine-Tuning:** Monitoramento do desempenho das tarefas e ajustes finos nos procedimentos.
- **T+180 dias – CSI (Continual Service Improvement):** Consolidação da melhoria contínua e estabelecimento de ciclo de revisão periódica.

A figura a seguir exibe o ciclo de vida e os fluxos de interação que regem a manutenção da vitalidade técnica do Catálogo de Serviços:



Conforme ilustrado na figura acima, o Framework estrutura-se sobre dois eixos fundamentais:

- **Eixo de Reatividade (Gatilhos):** Representa as entradas (inputs) que forçam a revisão das tarefas, tais como a detecção de novos vetores de ataque, alterações em normativos de proteção de dados (LGPD/CNJ) ou a necessidade de correção de processos identificada pela fiscalização da Justiça Eleitoral do Pará.
- **Eixo de Maturação (Linha do Tempo):** Demonstra o rito de passagem de uma nova atividade desde a sua concepção técnica (T+30) até a sua estabilização e entrada no ciclo de Melhoria Contínua de Serviço (CSI), garantindo que nenhuma alteração seja implementada sem o devido teste de hipótese e validação de produtividade.

Formalização e Sustentabilidade Contratual

O framework prevê que todas as alterações sejam documentadas via Apostilamento, assegurando que a modernização das tarefas não desnature o objeto principal e mantenha a integridade do equilíbrio econômico-financeiro. Este ciclo garante à Justiça Eleitoral do Pará uma prestação de serviço resiliente, onde o Catálogo de Serviços deixa de ser um documento estático para se tornar uma ferramenta viva de gestão estratégica.

ELABORADO POR	DATA EMISSÃO	Página
CGSI	11/07/2025	
APROVADO POR	DATA APROVAÇÃO	52/53
Coordenador / Coordenadoria	14/04/2026	

HISTÓRICO DE REVISÕES / ALTERAÇÕES

Número	Data	Versão	Responsável	Motivo
001	17/05/2025	1.0	CGSI	Elaboração inicial do documento.
002	08/06/2025	1.1	CGSI	Documento atribuído para Revisão.
003	11/07/2025	1.2	CGSI	Documento emitido para Aprovação
004	14/07/2025	1.2	CGSI	Documento atribuído para Revisão.
005	08/11/2025	1.3	CGSI	Inclusão do Anexo 1
006	08/11/2025	1.4	CGSI	Emissão da versão final
007	06/01/2026	1.5	CGSI	Matriz de Responsabilidade Técnica e Dimensionamento da Equipe CGSI
008	08/01/2026	1.6	CGSI	Inclusão do Anexo II - Ciclo de Vida do catálogo.

Tabela 36 - Histórico de Revisões/Alterações

ELABORADO POR	DATA EMISSÃO	Página 53/53
CGSI	11/07/2025	
APROVADO POR	DATA APROVAÇÃO	
Coordenador / Coordenadoria	14/04/2026	