ANEXO DA PORTARIA NORMATIVA TRE-SE Nº 185/2026

Procedimento Operacional Padrão de Resposta a Incidentes Críticos de Serviços de Tecnologia da Informação e Comunicação Fora do Expediente Ordinário

1. Objetivo

Estabelecer o procedimento técnico-operacional para resposta a incidentes críticos fora do expediente no âmbito da **STI**, assegurando tratamento ágil, rastreável e seguro de incidentes que possam comprometer a disponibilidade, integridade ou segurança dos serviços de TIC do TRE-SE.

2. Escopo

Aplica-se exclusivamente às equipes técnicas da COINF e da ASSEC, nos casos de falhas, indisponibilidades ou incidentes — operacionais ou de segurança da informação - classificados como de impacto alto ou crítico, ocorridos fora do horário regular de expediente, sem caracterizar regime contínuo de sobreaviso.

3. Base Normativa

- COBIT 2019 - Domínios DSS02, DSS04, DSS05 e MEA03.
- ITIL v4 - Práticas de Gerenciamento de Incidentes, Continuidade de Serviço, Gerenciamento de Problemas e Gestão de Mudanças.
- CIS Controls v8 - Controles 5 (Acessos), 13 (Monitoramento de Rede), 1 (Logs) e 17 (Resposta a Incidentes).

4. Definições

- Incidente: evento não planejado que cause interrupção ou diminuição da qualidade de um serviço de TI, ou que comprometa a confidencialidade, integridade ou autenticidade da informação. Exemplos incluem ataques de ransomware, vazamento de dados, falhas de hardware ou software, phishing e acesso não autorizado. O objetivo principal ao lidar com um incidente é a contenção rápida para minimizar os danos e o retorno da operação normal o mais rápido possível

- Técnico Acionado: servidor habilitado e autorizado a atuar em atendimento emergencial.
- Canal de Acionamento: meio formal de contato utilizado para mobilizar o técnico responsável.
- Registro de Atendimento: documento padronizado contendo data, hora, origem, ações, resultados e assinatura de validação.

5. Responsabilidades

Unidade	Responsabilidades Principais
COINF/ ASSEC	Executar atendimento técnico, restabelecer serviços, registrar e documentar ocorrências, devendo cientificar o STI com brevidade.
ASSEC	Avaliar impactos de cibersegurança e orientar ações de contenção e comunicação.
STI	Tomar ciência do relatório de execução dos serviços.
SEREF/ SGP	Controlar registros de horas efetivamente trabalhadas.
NIS/SAO	Realizar contato imediato em caso de incidentes físicos ou ambientais, tais como falhas de energia, indícios de incêndio, acesso físico indevido ou

Unidade	Responsabilidades Principais
	outras ocorrências correlatas.
Servidores acionados	Atender ao chamado, registrar as ações executadas, manter a confidencialidade das informações e seguir rigorosamente os protocolos de segurança. **Ressalta-se, contudo, que poderá ocorrer indisponibilidade de técnico habilitado para atendimento, uma vez que, devido às limitações de pessoal e aos riscos operacionais identificados, não há, até presente momento, viabilidade para a implantação do regime de sobreaviso permanente.**

6. Níveis de Incidentes

Nível	Descrição	Exemplo	Ação
Crítico	Interrupção total de serviços essenciais ou risco físico à infraestrutura.	Incidentes que envolvam queda total de rede, falha no gerador de energia, falha no sistema de climatização, acesso físico indevido ao Datacenter, alerta de incêndio, tentativa de intrusão, sequestro de dados (ransomware) ou escalada indevida de privilégios.	Acionamento imediato via canal principal.
Alto	Degradação grave ou falha de segurança com risco iminente.	Incidentes cuja falha comprometa a disponibilidade ou a integridade dos serviços essenciais.	Avaliar impacto; acionar se persistente >30 min.
Médio/ Baixo	Incidentes sem impacto em missão crítica.	Incidentes que não se enquadrem nas categorias anteriores são considerados falhas em serviços não essenciais, cujo atendimento poderá ser iniciado no próximo dia útil.	Registrar para tratamento no expediente.

7. Fluxo de Ações

- **Identificação do Incidente**: por alerta de sistema, equipe de segurança predial ou usuário autorizado.
- **Acionamento**: contato via canal principal (telefone dos técnicos habilitados).
- **Atendimento**: intervenção remota ou presencial conforme gravidade.
- **Avaliação do nível do incidente**: técnico ou analista de segurança avalia impacto.
- **Registro**: preenchimento do Formulário POP-STI (Anexo II).
- **Validação**: envio do Formulário POP-STI ao Secretário de Tecnologia da Informação e Comunicação e ao Diretor-Geral.
- **Comunicação:** o Diretor-Geral comunicará a ocorrência ao Comitê de Crises Cibernéticas (CCC), ao Comitê Gestor de Tratamento e Proteção de Dados Pessoais (CGTPDP) e ao Comitê Gestor de Crise (CGC).

- **Encerramento**: arquivamento no SEI e atualização do histórico de incidentes.
- **Solicitação de banco de horas**: o Secretário de Tecnologia da Informação e Comunicação preencherá o formulário específico para solicitação de inclusão das horas trabalhadas em banco de horas e submetê-lo-á à autorização da Administração.

8. Comunicação e Contatos

Canal principal:

- Telefone direto dos técnicos (Lista de Contatos - Anexo I).
- Em casos de falha de entrada do gerador de energia, alerta de princípio de incêndio, falha no sistema de refrigeração ou acesso indevido a ambientes técnicos (Data Center, salas técnicas, racks de rede ou energia), o acionamento será realizado pela equipe do NIS.
- O técnico deverá atender, no menor tempo possível, e orientar os próximos passos de contenção e verificação.

Canal alternativo:

- Mensagem de alerta gerada por ferramentas automáticas de monitoramento de infraestrutura ou cibersegurança ou empresas contratadas de NOC/SOC, mediante comunicação direta com o técnico responsável.

Registro de voz ou mensagem:

- Autorizado somente para comprovação do acionamento, devendo ser anexado ao registro de atendimento quando houver.

9. Registro e Evidências

Todos os acionamentos e evidências devem constar no Formulário de Ocorrências POP-STI (Anexo II)

10. Segurança da Informação

- Todo acesso remoto deverá ocorrer via VPN institucional com autenticação multifator (MFA).
- É vedado o uso de dispositivos pessoais para intervenção.
- Preservar logs e evidências técnicas para auditoria.
- Notificar a ASSEC sobre qualquer suspeita de tentativa de ataque.

11. Monitoramento e Melhoria Contínua

- Após cada incidente, será realizada reunião da equipe técnica envolvida com o STI, visando a melhoria contínua do processo.
- O POP será revisado anualmente ou sempre que houver alteração de infraestrutura ou fluxo de acionamento.

12. Disposições Finais

- A execução deste POP não caracteriza regime de sobreaviso.
- As horas efetivamente trabalhadas — quando o servidor é acionado e realiza o atendimento — serão integralmente computadas no banco de horas.

ANEXO DA PORTARIA NORMATIVA TRE-SE Nº 185/2026

Procedimento Operacional Padrão de Resposta a Incidentes Críticos de Serviços de Tecnologia da Informação e Comunicação Fora do Expediente Ordinário

- Fica previamente autorizado o acesso às dependências do Tribunal, fora do horário regular de expediente, aos servidores relacionados no Anexo I, sendo obrigatório o registro fundamentado no controle de acesso da portaria.

ANEXO I
Lista de Contatos de Emergência (COINF/ASSEC)

Nome	Unidade	Função	Telefone *
Cosme Rodrigues de Souza	COINF	Coordenador de Infraestrutura	(79) 9[redacted]
Wagner Ferreira Toledo	SESOP	Chefe de Seção	(79) 9[redacted]
Selmo Pereira de Almeida	ASSEC	Assessor de Segurança Cibernética	(79) 9[redacted]

* Dados tarjados em cumprimento ao art. 23 c/c os arts. 6º, 7º, 10 da Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), para fins de publicação da Portaria Normativa TRE-SE nº 185/2026 e deste Anexo.

ANEXO II
Formulário de Ocorrência POP-STI

Descrição do Incidente			
Nome do Técnico Acionado		**Data**	**Hora**
Atendimento Presencial			
Serviços Afetados		**Horário**	
Medidas Executadas		**Início**	**Término**
Resultado Obtido			
Evidências			