INSTRUÇÃO DE SERVIÇO Nº 007-N, DE 16 DE JUNHO DE 2026

Institui e regulamenta a Sala de Crise do Instituto de Tecnologia da Informação e Comunicação do Estado do Espírito Santo – PRODEST.

O Diretor Geral do Instituto de Tecnologia da Informação e Comunicação do Estado do ES – PRODEST, no uso das atribuições que lhe confere a Lei Complementar nº 1.064, de 19 de dezembro de 2023;

CONSIDERANDO a necessidade de estabelecer mecanismos de governança para resposta coordenada a incidentes críticos que possam impactar serviços de tecnologia da informação e comunicação providos pelo PRODEST;

CONSIDERANDO a importância de garantir comunicação tempestiva, padronizada e transparente com a Diretoria, clientes e partes interessadas durante situações de crise;

CONSIDERANDO a necessidade de formalizar procedimentos para gestão, tratamento e acompanhamento de incidentes críticos, promovendo maior previsibilidade, rastreabilidade e melhoria contínua;

RESOLVE:

Art. 1º Fica instituída a Sala de Crise do PRODEST, mecanismo formal de coordenação estratégica destinado à gestão de incidentes críticos relacionados aos serviços de tecnologia da informação e comunicação providos pelo Instituto.

Art. 2º A Sala de Crise tem por objetivos:

I – centralizar a coordenação estratégica dos incidentes críticos;

II – garantir comunicação tempestiva e padronizada durante a ocorrência do incidente;

III – apoiar a tomada de decisão da Diretoria Setorial Técnica;

IV – reduzir ruídos operacionais e inconsistências de comunicação;

V – promover a rastreabilidade das ações executadas durante a resposta ao incidente;

VI – assegurar a formalização das ações corretivas e preventivas decorrentes dos incidentes tratados.

Art. 3º A Sala de Crise funcionará, preferencialmente, por meio de grupo virtual permanente destinado exclusivamente a essa finalidade.

Parágrafo único. Excepcionalmente, mediante convocação do Diretor Setorial Técnico, a Sala de Crise poderá ser realizada presencialmente.

Art. 4º São participantes permanentes da Sala de Crise:

I – Diretor Setorial Técnico;

II – Gerência de Integração – GEINT;

III – Gerência de Dados – GEDAD;

IV – Gerência de Infraestrutura de TIC – GEITIC;

V – Gerência de Plataforma de TIC – GEPTIC;

VI – Gerência de Sistemas – GESIT;

VII – Assessoria de Comunicação – ASCOM;

VIII – Assessoria de Relacionamento com o Cliente – ASCLI.

§ 1º Na ausência do gerente responsável pela área afetada, poderá ser incluído temporariamente o supervisor responsável pelo serviço ou ambiente impactado.

§ 2º Outros participantes poderão ser convocados conforme a natureza do incidente.

Art. 5º Considera-se incidente crítico aquele que atender a pelo menos um dos seguintes critérios:

I – indisponibilidade de serviço essencial ao Governo do Estado ou que impacte diretamente o atendimento ao cidadão;

II – impacto a múltiplos órgãos ou grande quantidade de usuários;

III – incidente com potencial de repercussão externa;

IV – incidente que represente risco institucional, legal ou de imagem;

V – determinação do Diretor Setorial Técnico.

Art. 6º A Sala de Crise será ativada:

I – quando identificado incidente enquadrado nos critérios definidos no artigo anterior;

II – por determinação do Diretor Setorial Técnico.

Art. 7º Compete ao Diretor Setorial Técnico autorizar a ativação da Sala de Crise.

Parágrafo único. Na ausência do Diretor Setorial Técnico, a ativação poderá ser realizada pelo Gerente da GEINT.

Art. 8º A Sala de Crise observará os seguintes papéis e responsabilidades:

I – Coordenador do Incidente, exercido pelo Diretor Setorial Técnico ou por representante formalmente designado;

a) exercer a coordenação estratégica do incidente;

b) definir prioridades;

c) apoiar a tomada de decisão;

d) realizar o alinhamento com a alta gestão.

II – Coordenador Técnico, exercido pelo gerente responsável pelo serviço, sistema ou infraestrutura afetada;

a) coordenar a resposta técnica;
b) consolidar informações técnicas;
c) reportar periodicamente a evolução do incidente.

III – Gestão de Comunicação, exercida pela Assessoria de Comunicação – ASCOM;

a) apoiar a comunicação institucional;
b) apoiar a comunicação com clientes e partes interessadas.

IV – Suporte Técnico, exercido pelas supervisões e equipes técnicas envolvidas na resolução do incidente;

a) executar as atividades necessárias para contenção, mitigação e resolução do incidente.

Art. 9º Durante a vigência da Sala de Crise:

I – o gerente responsável pelo incidente deverá realizar atualizações periódicas em intervalos máximos de 30 (trinta) minutos, ou em periodicidade definida pelo Coordenador do Incidente, observada a criticidade e a dinâmica do evento;

II – alterações relevantes de cenário deverão ser comunicadas imediatamente;

III – as atualizações deverão contemplar, sempre que possível:

a) status atual do incidente;
b) b) impacto ao negócio;
c) causa identificada ou hipótese;
d) ações em andamento;

e) próximos passos;

f) previsão de normalização;

g) responsável pela condução.

Art. 10º A comunicação externa será realizada pela ASCOM, mediante solicitação do Diretor Setorial Técnico.

§ 1º Na ausência do Diretor Setorial Técnico, a solicitação poderá ser realizada pelo gerente responsável pelo incidente.

§ 2º Toda comunicação externa deverá observar as informações validadas na Sala de Crise.

§ 3º Não deverão ser divulgadas informações técnicas sensíveis, hipóteses não confirmadas ou informações que possam comprometer a investigação ou a segurança dos ambientes tecnológicos.

§ 4º Sempre que aplicável, as comunicações externas deverão observar os modelos constantes do Anexo II desta Instrução de Serviço.

Art. 11º Nos incidentes relacionados à segurança da informação, a Assessoria de Segurança e Gestão de Riscos – ASSIG deverá ser obrigatoriamente convocada para participação na Sala de Crise.

§ 1º Consideram-se incidentes de segurança da informação, entre outros:

I – comprometimento de credenciais;

II – vazamento ou exposição indevida de dados;

III – ataques de negação de serviço;

IV – infecções por ransomware ou outros códigos maliciosos;

V – comprometimento de ativos críticos;

VI – demais eventos que possam afetar a confidencialidade, integridade ou disponibilidade das informações e dos serviços de TIC.

§ 2º Nos incidentes relacionados à segurança da informação, deverão ser observados adicionalmente os procedimentos definidos na Política de Segurança da Informação do PRODEST e demais normativos correlatos.

Art. 12º São regras de funcionamento da Sala de Crise:

I – a comunicação deverá tratar exclusivamente do incidente em tratamento;

II – discussões técnicas detalhadas deverão ocorrer em canais específicos das equipes operacionais;

III – não serão permitidas mensagens paralelas ou assuntos não relacionados ao incidente;

IV – os relatórios periódicos serão realizados pelo gerente responsável pelo incidente, salvo necessidade de complementação relevante.

Parágrafo único. Durante períodos sem incidentes ativos:

I – o canal da Sala de Crise deverá permanecer integralmente em silêncio;

II – não deverão ocorrer comunicações, avisos, mensagens ou interações de qualquer natureza entre os participantes;

III – o canal não deverá ser utilizado para comunicações gerais, avisos administrativos ou quaisquer outros assuntos institucionais que não estejam relacionados à gestão de incidentes críticos.

Art. 13º A Sala de Crise poderá ser encerrada quando, cumulativamente:

I – o serviço estiver normalizado;

II – o registro do incidente estiver formalizado no GLPI;

III – houver responsável formalmente designado para abertura e acompanhamento do problema no Azure DevOps;

IV – houver autorização do Diretor Setorial Técnico.

Art. 14º Todo incidente tratado por meio da Sala de Crise deverá possuir, obrigatoriamente, os seguintes artefatos mínimos:

I – registro do incidente no GLPI;

II – registro do problema no Azure DevOps para análise de causa raiz;

III – relatório de pós-incidente elaborado conforme modelo constante do Anexo III;

IV – plano de ação preventivo e corretivo contendo, no mínimo, ação, responsável e prazo.

§ 1º O registro do incidente e do problema deverão ser realizados antes do encerramento da Sala de Crise.

§ 2º O relatório de pós-incidente deverá ser elaborado e apresentado à Diretoria Geral, à Diretoria Setorial Técnica e às demais partes interessadas, quando aplicável, em até 5 (cinco) dias úteis após o encerramento da Sala de Crise.

§ 3º A abertura do problema no Azure DevOps deverá ocorrer em prazo compatível com a complexidade do incidente, observada a designação prevista no inciso III do Art. 12.

Art. 15º Compete à Gerência de Integração – GEINT exercer a governança da Sala de Crise, cabendo-lhe:

I – manter e revisar os procedimentos relacionados à Sala de Crise;

II – acompanhar a aplicação desta Instrução de Serviço;

III – consolidar e monitorar os relatórios de pós-incidente;

IV – acompanhar a execução das ações preventivas e corretivas decorrentes dos incidentes críticos;

V – propor melhorias nos processos, fluxos e mecanismos de comunicação relacionados à gestão de incidentes críticos;

VI – apoiar a Diretoria Setorial Técnica na avaliação da efetividade do processo de resposta a incidentes críticos;

VII – zelar pela observância dos papéis e responsabilidades definidos no Anexo IV – Matriz de Papéis e Responsabilidades (RACI).

Art. 16º Integram esta Instrução de Serviço:

I – Anexo I – Fluxo Básico da Sala de Crise;

II – Anexo II – Modelos de Comunicação Externa;

III – Anexo III – Modelo de Relatório Pós-Incidente;

IV – Anexo IV – Matriz de Papéis e Responsabilidades (RACI).

Art. 17º Esta Instrução de Serviço entra em vigor na data de sua publicação.

Marcelo Azeredo Cornélio
Diretor-Geral

ANEXO I - FLUXO BÁSICO DA SALA DE CRISE

1. IDENTIFICAÇÃO DO INCIDENTE

1.1 O incidente poderá ser identificado por monitoramento, usuários, clientes, equipes técnicas ou outros mecanismos de detecção.

1.2 A área técnica responsável deverá realizar avaliação preliminar do impacto e da abrangência do evento.

2. CLASSIFICAÇÃO

2.1 A área técnica deverá verificar se o incidente atende aos critérios estabelecidos no Art. 5º desta Instrução de Serviço.

2.2 Caso enquadrado como incidente crítico, deverá ser solicitado o acionamento da Sala de Crise.

3. ATIVAÇÃO DA SALA DE CRISE

3.1 O Diretor Setorial Técnico, ou o Gerente da GEINT em sua ausência, realizará a ativação da Sala de Crise.

3.2 Os participantes definidos nesta Instrução de Serviço serão convocados.

3.3 O gerente da área responsável pelo incidente assumirá a função de Coordenador Técnico.

4. INÍCIO DA COMUNICAÇÃO

4.1 A primeira atualização deverá ser realizada tão logo a Sala de Crise seja ativada, ainda que existam informações preliminares.

4.2 A atualização inicial deverá conter, sempre que possível:

I – descrição resumida do incidente;

II – serviços impactados;

III – impacto identificado;

IV – ações iniciais adotadas.

5. TRATAMENTO DO INCIDENTE

5.1 As equipes técnicas deverão atuar em seus canais operacionais específicos.

5.2 A Sala de Crise deverá permanecer focada na coordenação estratégica e na comunicação executiva.

5.3 As atualizações deverão ocorrer em intervalos máximos de 30 (trinta) minutos ou imediatamente em caso de alteração relevante do cenário.

6. ESTABILIZAÇÃO E NORMALIZAÇÃO

6.1 Após o restabelecimento do serviço, a área técnica deverá realizar monitoramento da estabilidade do ambiente.

6.2 O impacto ao cliente deverá estar cessado para que seja iniciado o processo de encerramento.

7. FORMALIZAÇÃO

7.1 Antes do encerramento da Sala de Crise deverão ser providenciados:

I – registro do incidente no GLPI;

II – designação formal de responsável pela abertura e acompanhamento do problema no Azure DevOps;

III – identificação preliminar da causa raiz, quando disponível.

8. ENCERRAMENTO

8.1 O encerramento da Sala de Crise dependerá de autorização do Diretor Setorial Técnico.

9. PÓS-INCIDENTE

9.1 A área responsável deverá elaborar o Relatório Pós-Incidente.

9.2 O relatório deverá ser apresentado à Diretoria Geral, à Diretoria Setorial Técnica e às demais partes interessadas, quando aplicável, no prazo máximo de 5 (cinco) dias úteis.

ANEXO II - MODELOS DE COMUNICAÇÃO EXTERNA

1. COMUNICADO DE INDISPONIBILIDADE

Assunto: Indisponibilidade de Serviço – [Nome do Sistema/Serviço]

Prezados,

Informamos que o serviço [Nome do Sistema/Serviço] encontra-se indisponível ou apresentando instabilidade neste momento.

Impacto:

[Descrever de forma objetiva o impacto percebido pelo usuário.]

Status:

Nossa equipe técnica encontra-se atuando para restabelecimento do serviço.

Previsão de Normalização:

[Informar previsão ou registrar “Em apuração”.]

Orientações:

[Informar procedimentos alternativos, quando aplicável.]

Novas atualizações serão comunicadas oportunamente.

Atenciosamente,

PRODEST

2. COMUNICADO RESUMIDO

Indisponibilidade – [Sistema/Serviço]

O serviço encontra-se indisponível neste momento.

Equipes técnicas atuando.

Previsão: [Informar previsão ou registrar “Em apuração”.]

Novas informações serão divulgadas em breve.

3. COMUNICADO DE ATUALIZAÇÃO

Atualização – [Sistema/Serviço]

O serviço permanece [indisponível/instável].

As equipes continuam atuando na resolução.

Previsão atualizada:

[Informar previsão ou registrar “Em apuração”.]

Novo comunicado será divulgado em até [tempo estimado].

4. COMUNICADO DE NORMALIZAÇÃO

Normalização – [Sistema/Serviço]

Informamos que o serviço foi restabelecido e encontra-se operando normalmente.

O incidente ocorreu em decorrência de [descrição resumida e não sensível].

O ambiente permanece em monitoramento.

Permanecemos à disposição.

Atenciosamente,

PRODEST

ANEXO III - MODELO DE RELATÓRIO PÓS-INCIDENTE

DADOS GERAIS

Título do Incidente:

Gerência Responsável:

Data do Incidente:

ID do Incidente (GLPI):

ID do Problema (Azure DevOps):

Data do Relatório:

Responsável pela Elaboração:

1. SUMÁRIO EXECUTIVO

Descrição resumida do incidente, contexto, período de ocorrência, serviços afetados e impacto gerado ao Governo, órgão cliente ou cidadão.

2. LINHA DO TEMPO

Registrar cronologicamente os principais eventos relacionados ao incidente.

Data/Hora Evento

3. ANÁLISE TÉCNICA DA CAUSA RAIZ

Descrever a causa identificada ou as hipóteses em investigação.

Registrar fatores contribuintes que favoreceram a ocorrência do incidente.

4. AÇÕES DE RESOLUÇÃO

Descrever as ações executadas para:

I – contenção do incidente;

II – mitigação dos impactos;

III – recuperação do serviço;

IV – validação da normalização.

5. ANÁLISE DE IMPACTO

5.1 Impacto Técnico e de Segurança

5.2 Impacto Operacional e de Negócio

5.3 Impacto Jurídico e Legal

5.4 Impacto Institucional

6. PLANO DE AÇÃO PREVENTIVO E CORRETIVO

Ação	Tipo	Responsável	Prazo

Tipo:

- Preventiva
- Corretiva

7. LIÇÕES APRENDIDAS

7.1 O que funcionou

Registrar práticas, decisões, ferramentas ou ações que contribuíram positivamente para a resolução do incidente.

7.2 O que não funcionou

Registrar dificuldades, falhas de processo, gargalos ou oportunidades de melhoria identificadas.

8. CONCLUSÃO

Registrar a situação final do incidente, a efetividade das ações executadas e eventuais recomendações adicionais.

Responsável pela elaboração:

Gerente da Área Responsável

Data: XX/XX/XXXX

ANEXO IV - MATRIZ DE PAPÉIS E RESPONSABILIDADES (RACI)

1. OBJETIVO

Estabelecer de forma clara as responsabilidades dos participantes envolvidos no processo de gestão da Sala de Crise do PRODEST, garantindo alinhamento quanto à tomada de decisão, execução das atividades, comunicação e governança.

2. LEGENDA

R (*Responsible*) – Responsável pela execução da atividade.

A (*Accountable*) – Responsável final pela decisão, aprovação ou resultado.

C (*Consulted*) – Deve ser consultado durante a execução da atividade.

I (*Informed*) – Deve ser mantido informado sobre o andamento ou resultado da atividade.

3. PARTICIPANTES

DSTEC – Diretoria Setorial Técnica;

GEINT – Gerência de Integração;

ÁREA RESPONSÁVEL – Gerência responsável pelo serviço, sistema ou infraestrutura impactada. Nos incidentes relacionados à Segurança da Informação, deverão ser observadas adicionalmente as disposições do Art. 10-A desta Instrução de Serviço;

ASCOM – Assessoria de Comunicação;

ASCLI – Assessoria de Clientes;

ASSIG – Assessoria de Segurança e Gestão de Riscos;

EQUIPE TÉCNICA – Supervisões e equipes operacionais envolvidas na resolução do incidente.

4. MATRIZ RACI

Atividade	DSTEC	GEINT	Área Responsável	ASCOM	ASCLI	Equipe Técnica
Classificação do incidente	A	C	R	I	I	C
Ativação da Sala de Crise	A/R	C/R	C	I	I	I
Coordenação estratégica da crise	A/R	C	C	I	I	I

Coordenação técnica da resposta	I	I	A/R	I	I	R
Atualizações periódicas da Sala de Crise	I	C	A/R	I	I	C
Comunicação externa aos clientes e partes interessadas	A	I	C	R	C	I
Registro do incidente no GLPI	I	C	A	I	I	R
Registro do problema no Azure DevOps	I	C	A	I	I	R
Elaboração do Relatório Pós-Incidente	I	C	A/R	C	C	C
Apresentação executiva do Pós-Incidente	A	C	R	I	I	I
Acompanhamento das ações corretivas e preventivas	I	A/R	R	I	I	C
Revisão e melhoria do processo da Sala de Crise	C	A/R	C	C	C	C
Encerramento da Sala de Crise	A	C	R	I	I	I
Tratamento de Incidentes de Segurança da Informação	A	C	R	I	I	R

5. DISPOSIÇÕES COMPLEMENTARES

5.1. A responsabilidade pela resolução técnica do incidente permanece com a gerência responsável pelo serviço, sistema ou infraestrutura afetada.

5.2. A GEINT exerce papel de governança do processo, atuando na coordenação metodológica, acompanhamento dos artefatos obrigatórios, monitoramento das ações corretivas e preventivas e promoção da melhoria contínua do processo.

5.3. A atuação da GEINT não substitui as responsabilidades operacionais das áreas técnicas envolvidas na resolução do incidente.

5.4. Em situações excepcionais, a DSTEC poderá definir responsabilidades complementares ou convocar participantes adicionais em razão da criticidade, abrangência ou impacto do incidente.

5.5 Na ausência da DSTEC, a GEINT poderá realizar a ativação da Sala de Crise, conforme previsto nesta Instrução de Serviço.

5.6. Nos incidentes relacionados à Segurança da Informação, a Assessoria de Segurança e Gestão de Riscos – ASSIG deverá ser obrigatoriamente convocada para participação na Sala de Crise, observando-se o disposto no Art. 10-A desta Instrução de Serviço.

5.7. Quando convocada, a ASSIG atuará como unidade consultiva especializada, apoiando a análise, contenção, investigação, tratamento e comunicação dos incidentes de Segurança da Informação, sem prejuízo das responsabilidades atribuídas à área responsável pelo serviço, sistema ou infraestrutura afetada.

Documento original assinado eletronicamente, conforme MP 2200-2/2001, art. 10, § 2º, por:

MARCELO AZEREDO CORNÉLIO
DIRETOR GERAL
PRODEST - PRODEST - GOVES
assinado em 17/06/2026 08:49:14 -03:00

INFORMAÇÕES DO DOCUMENTO
Documento capturado em 17/06/2026 08:49:14 (HORÁRIO DE BRASÍLIA - UTC-3)
por MARILÉA FERNANDES DA SILVA PIMENTA (SECRETARIA EXECUTIVA - SECEX - PRODEST - GOVES)
Valor Legal: ORIGINAL | Natureza: DOCUMENTO NATO-DIGITAL

A disponibilidade do documento pode ser conferida pelo link: https://e-docs.es.gov.br/d/2026-XFM7CV