SUPERINTENDÊNCIA DE SEGUROS PRIVADOS

RESOLUÇÃO SUSEP Nº 59, DE 16 DE SETEMBRO DE 2025

Estabelece a Política de Gestão de Continuidade de Serviços de TI da Superintendência de Seguros Privados - Susep.

O SUPERINTENDENTE DA SUPERINTENDÊNCIA DE SEGUROS PRIVADOS - SUSEP, torna público que o Conselho Diretor da Autarquia, em reunião ordinária realizada em 10 de setembro de 2025, no uso das atribuições que lhe confere o inciso V do art. 8º do Anexo I da Resolução CNSP nº 468, de 25 de abril de 2024 e o que consta do Processo SUSEP n.° 15414.635413/2028-52,

R E S O L V E :

Art. 1º Esta resolução estabelece a Política de Gestão de Continuidade de Serviços de TI da Superintendência de Seguros Privados - Susep.

CAPÍTULO I

DO ESCOPO

Art. 2º A Política de Gestão de Continuidade de Serviços de TI visa a estabelecer as diretrizes e as responsabilidades a serem observadas no Processo de Gestão de Continuidade de Serviços de TI da Susep, de forma a minimizar os impactos operacionais, legais, regulatórios e financeiros decorrentes de indisponibilidades de serviços de TI.

CAPÍTULO II

DOS CONCEITOS E DEFINIÇÕES

Art. 3º Para efeitos desta política, entende-se:

I - Análise de Impacto nos Negócios - BIA: avaliação cuja finalidade é determinar prioridades de continuidade e recuperação dentre os processos de trabalho, levando em conta os impactos de interrupção que suportam os serviços da Susep;

II - declaração de acionamento ou ativação do plano: ato de declarar que o Plano de Continuidade de Serviços de TI da Susep precisa ser colocado em prática de forma a continuar o fornecimento de serviços fundamentais;

III - Gestão de Continuidade de Negócios - GCN: processo de gestão abrangente responsável por oferecer uma estrutura que permita à Susep desenvolver resiliência organizacional e capacidade de resposta a eventos inesperados, salvaguardando os interesses das partes interessadas, a reputação e a imagem da autarquia;

IV - incidente: qualquer evento que possa causar a interrupção de processos ou funções;

V - interrupção: evento, previsível ou não, que cause um desvio negativo na execução de serviços, de acordo com os objetivos da Susep;

VI - objetivos de recuperação: requisitos para a recuperação de um processo ou função crítica, que dependem do impacto causado pela interrupção;

VII - partes interessadas - *stakeholders*: aqueles que possuem algum interesse nos resultados da Susep; termo abrangente que inclui, entre outros, mercado supervisionado, servidores, terceirizados, consumidores, fornecedores, entre outros;

VIII - Plano de Continuidade de Serviços de TI: é o conjunto do Plano de Contingência Operacional de Serviços de TI e do Plano de Recuperação de Serviços de TI, cobertos pelo Plano de Gerenciamento de Comunicação, necessário para coordenar as informações e comunicações necessárias para sincronizar os outros planos;

IX - Plano de Contingência Operacional de Serviços de TI: documentação dos procedimentos, recursos e informações necessários para que, em caso de interrupção do funcionamento normal de serviços críticos de TI, a Susep mantenha seus processos críticos funcionando de maneira alternativa;

X - Plano de Gerenciamento de Comunicação: documentação dos responsáveis e atividades a serem realizadas para o suporte aos demais Planos, indicando a sequência de divulgação e o conteúdo dos comunicados para cada serviço da Susep;

XI - Plano de Recuperação de Serviços de TI: documentação dos procedimentos, recursos e informações necessários para que a Susep realize o retorno dos serviços críticos de TI à normalidade;

XII - Processo de Gestão da Continuidade de Serviços de TI: processo contínuo de governança e gestão suportado pela alta direção e que recebe recursos apropriados para garantir que os passos necessários estão sendo tomados de forma a identificar o impacto de perdas em potencial, manter estratégias e planos de recuperação viáveis e garantir a continuidade de fornecimento de serviços de TI por intermédio de análises críticas, testes, treinamentos e manutenção;

XIII - recursos: todos os ativos, pessoas, competências, informação, tecnologia (incluindo instalações e equipamentos), locais, suprimentos e dados (em meio eletrônico ou não) que a Susep deve ter disponíveis para uso, quando necessário, a fim de operar e atingir seus objetivos;

XIV - resiliência: capacidade de a Susep de resistir aos efeitos de um incidente;

XV - serviço de TI: conjunto de recursos, processos e outros serviços tecnológicos que suportam atividade, negócios ou serviços da organização;

XVI - teste: atividade na qual o Plano de Continuidade de Serviços de TI e seus componentes são exercitados parcial ou integralmente, de forma a garantir que eles contenham as informações apropriadas e produzam o resultado desejado quando colocados em prática; e

XVII - Unidade responsável por serviços de TI: Unidade de negócio responsável por serviço de TI cuja continuidade será gerenciada.

CAPÍTULO III

DAS DIRETRIZES

Art. 4º O Processo de Gestão da Continuidade de Serviços de TI da Susep deve prever mecanismos que permitam:

I - identificar os serviços de TI que serão objeto desta política;

II - identificar as unidades responsáveis pelos serviços de TI cuja continuidade será gerenciada;

III - identificar as ameaças internas e externas que possam comprometer a continuidade das operações da Susep;

IV - identificar os possíveis impactos à operação decorrentes da concretização de tais ameaças;

V - identificar os requisitos para a continuidade dos negócios, incluindo os legais e os regulatórios;

VI - estabelecer papéis e responsabilidades das partes internas e externas à Susep;

VII - desenvolver estrutura de gerenciamento e resposta a crises, suportada por níveis adequados de autoridade e competência, que assegurem a comunicação efetiva às partes interessadas;

VIII - desenvolver processos e mecanismos que viabilizem a recuperação das atividades em caso de interrupção; e

IX - realizar treinamentos, testes e análises que garantam a manutenção e o bom funcionamento dos planos de continuidade.

CAPÍTULO IV

DA ESTRUTURA

Art. 5º As estruturas envolvidas na continuidade de serviços de TI da Susep são:

I - Conselho Diretor;

II - Comitê de Segurança de Informação - CSI;

III - Gestor de Segurança da Informação;

IV - Gestores de unidades responsáveis por serviços de TI;

V - Unidades responsáveis por serviços de TI; e

VI - demais colaboradores da Susep.

CAPÍTULO V

DAS COMPETÊNCIAS

Art. 6º Ao gestor das unidades responsáveis por serviços de TI compete:

I - declarar o acionamento ou ativação do Plano de Continuidade de Serviços de TI, no que tange ao serviço afetado;

II - garantir a participação ativa das equipes sob sua gestão nos processos de elaboração e teste do Plano de Continuidade de Serviços de TI; e

III - realizar a análise de impacto nos negócios para os casos de interrupção de serviços de TI sob responsabilidade da unidade de que é gestor.

Art. 7º Às unidades responsáveis por serviços de TI compete, no que tange aos respectivos serviços:

I - definir as atividades do Processo Gestão de Continuidade de Serviços de TI aplicáveis;

II - elaborar e manter o Plano de Continuidade de Serviços de TI;

III - consolidar os resultados de testes e exercícios do Plano de Continuidade de Serviços de TI; e

IV - propor projetos e iniciativas para o aperfeiçoamento do Processo de Continuidade de Serviços de TI da Susep, buscando alinhamento às boas práticas existentes.

Art. 8º Ao Gestor de Segurança da Informação compete:

I - coordenar, com apoio das partes interessadas, a elaboração e exercício periódico do Plano de Continuidade de Serviços de TI - PCSTI;

II - elaborar e submeter ao CSI relatório anual de continuidade de serviços de TI, no qual conste a síntese das atividades de elaboração, manutenção e exercício do PCSTI bem como os incidentes relevantes ocorridos no período a que se refere; e

III - cumprir e estimular o cumprimento do definido neste ato normativo.

Art. 9º Aos demais colaboradores da Susep compete:

I - cumprir o disposto nos documentos de continuidade de serviços de TI;

II - buscar orientação junto às unidades responsáveis por serviços de TI em caso de dúvidas relacionadas à Política e aos Planos de Continuidade de Serviços de TI; e

III - participar ativamente dos processos de teste e planejamento, sempre que requisitados.

CAPÍTULO VI

DO PROCEDIMENTO

Art. 10. No Processo de Gestão de Continuidade de Serviços de TI serão realizadas as seguintes atividades:

I - documentar as diretrizes do Plano de Continuidade de Serviços de TI;

II - definir os serviços críticos de TI da Susep;

III - definir as estratégias de continuidade para os serviços críticos;

IV - desenvolver e implementar os Planos previstos no Plano de Continuidade de Serviços de TI para respostas tempestivas a interrupções;

V - realizar exercícios, testes e manutenção periódica dos Planos, promovendo as revisões necessárias; e

VI - elaborar os relatórios relativos às atividades de gestão de continuidade de serviços de TI.

Art. 11. Os procedimentos previstos no Plano de Continuidade de Serviços de TI serão executados em conformidade com os requisitos de segurança da informação necessários à proteção dos ativos de informação críticos, tratando as atividades de forma abrangente, o que inclui as pessoas, os processos, a infraestrutura e os recursos de tecnologia da informação.

Art. 12. O Plano de Continuidade de Serviços de TI da Susep será composto pelos seguintes Planos, a fim de assegurar a disponibilidade dos ativos de informação e a recuperação das atividades críticas:

I - Plano de Gerenciamento de Comunicação - PGCTI;

II - Plano de Contingência Operacional de Serviços de TI - PCOTI; e

III - Plano de Recuperação de Serviços de TI - PRSTI.

Art. 13. Cada um dos Planos deverá conter, no mínimo:

I - Plano de Gerenciamento de Comunicação:

a) objetivo e escopo;

b) papéis e responsabilidades;

c) condições para a ativação de Planos;

d) autoridade responsável;

e) detalhes de contato;

f) lista de tarefas e ações;

g) atividades das pessoas; e

h) comunicação à mídia;

II - Plano de Contingência Operacional de Serviços de TI:

a) objetivo e escopo;

b) papéis e responsabilidades;

c) autoridade responsável;

d) detalhes de contato;

e) lista de tarefas; e

f) recursos necessários; e

III - Plano de Recuperação de Serviços de TI:

a) objetivo e escopo;

b) papéis e responsabilidades;

c) autoridade responsável;

d) detalhes de contato;

e) lista de tarefas; e

f) recursos necessários.

Art. 14. Os Planos serão exercitados e testados periodicamente, bem assim os resultados documentados, para garantir a sua efetividade.

Art. 15. A revisão dos Planos será realizada sempre que os testes periódicos indicarem sua

necessidade ou após mudanças significativas nos ativos que suportam os serviços de TI;

Art. 16. Os contratos firmados com empresas terceirizadas que suportem serviços críticos de TI devem estar em acordo com os requisitos de continuidade de negócio estabelecidos nos Planos da Susep.

CAPÍTULO VII

DAS DISPOSIÇÕES GERAIS

Art. 17. As normas complementares relativas à gestão e uso de recursos de TI devem harmonizar-se com as disposições desta Política.

Art. 18. Fica revogada a DELIBERAÇÃO SUSEP Nº 218, DE 12 DE FEVEREIRO DE 2019.

Art. 19. Esta Resolução entra em vigor na data de sua publicação.



Documento assinado eletronicamente por **ALESSANDRO SERAFIN OCTAVIANI LUIS (MATRÍCULA 1860655)**, **Superintendente da Susep**, em 30/09/2025, às 11:52, conforme horário oficial de Brasília, de acordo com o art. 6º do Decreto nº 8.539/2015.



A autenticidade do documento pode ser conferida no site https://sei.susep.gov.br/sei/controlador_externo.php?acao=documento_conferir&acao_origem=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2504920** e o código CRC **2F1CAE9B**.
