CIA ESTADUAL DE ENGENHARIA DE TRANSPORTES E LOGÍSTICA CENTRAL	**Código: POP-CENTRAL-030**

Plano de Resposta a Incidentes de Segurança em Dados Pessoais

Órgão gestor: Encarregado pelo Tratamento de Dados Pessoais	**Órgão aprovador:** DIREXE
Nº Processo: SEI-100006/000772/2024	**Data de aprovação:** 21/07/2025
Tipo: POP - Padrão de Procedimento	**Status:** Ativo
Processo: Tratamento de Dados Pessoais	**Versão:** 1.0

1. OBJETIVOS

- Definir os procedimentos a serem adotados no caso de suspeita ou confirmação de incidente de segurança envolvendo dados pessoais;
- Definir os papéis e responsabilidades de cada um dos membros do Comitê de Resposta a Incidentes de Segurança com Dados Pessoais, no âmbito da Companhia Estadual de Engenharia e Logística de Transportes – CENTRAL;
- Minimizar os impactos dos incidentes de segurança;
- Restabelecer a normalidade dos serviços o mais rápido possível;
- Documentar e aprender com os incidentes para evitar recorrências.

2. APLICAÇÃO E ABRANGÊNCIA

Este procedimento aplica-se a todo o corpo de colaboradores da Companhia envolvidos no tratamento de dados pessoais e aos membros do Comitê de Resposta a Incidentes de Segurança com Dados Pessoais.

3. DOCUMENTOS DE REFERÊNCIA E COMPLEMENTARES

- Lei Geral de Proteção de Dados Pessoais (LGPD): Lei nº 13.709, de 14 de agosto de 2018;
- Decreto Estadual nº 48.891, de 10 de janeiro de 2024: Institui a Política de Governança em Privacidade e Proteção de Dados Pessoais do Estado do Rio de Janeiro;
- Resolução CD/ANPD nº 15, de 24 de abril de 2024: Aprova o Regulamento de Comunicação de Incidente de Segurança;
- Política de Divulgação de Informações e de Porta Vozes da CENTRAL: SEI-100006/000908/2021;
- Portaria CENTRAL SEI Nº 772 de 27 de junho de 2025: Designa os Encarregados da CENTRAL;
- Código de Conduta Ética e de Integridade da CENTRAL;
- Regimento Interno da CENTRAL.

4. UNIDADES FUNCIONAIS ENVOLVIDAS

a) Comitê de Resposta a Incidentes de Segurança com Dados Pessoais;

b) Comitê de Segurança da Informação – COMISEINF;
c) Diretor Presidente - PRESI;
d) Diretor de Administração e Finanças – DIRAF;
e) Encarregado pelo Tratamento de Dados Pessoais - ETD;
f) Superintendência de Tecnologia da Informação - SUPTIN;
g) Assessoria Jurídica - ASSJUR;
h) Assessoria de Comunicação - ASSCOM.

5. ATRIBUIÇÕES E RESPONSABILIDADES:

a) Comitê de Resposta a Incidentes de Segurança com Dados Pessoais: Responsável por aplicar procedimentos descritos neste documento no caso de suspeita ou confirmação de incidente de segurança envolvendo dados pessoais.

b) Encarregado pelo Tratamento de Dados Pessoais (DPO): Responsável por acionar o Comitê de Resposta a Incidentes de Segurança com Dados Pessoais em caso de ciência de incidente de segurança com dados pessoais e dar seguimento ao Plano de Resposta a Incidentes. Também compete a ele orientar e capacitar os funcionários e os contratados da Companhia a respeito das práticas a serem tomadas em relação à proteção de dados pessoais, além de ser responsável pela comunicação do Incidente para a ANPD, para o Encarregado Central e aos titulares de dados.

c) Diretor Presidente – PRESI: Responsável por conduzir as reuniões do Comitê de Resposta a Incidentes de Segurança com Dados Pessoais com apoio do Encarregado pelo Tratamento de Dados Pessoais (DPO).

d) Presidente do Comitê de Segurança da Informação: Responsável, em conjunto com a Superintendência de TI, por analisar o incidente ocorrido e coordenar o aperfeiçoamento e a implementação das políticas e procedimentos de segurança da informação da Companhia, a fim de evitar incidentes futuros.

e) Superintendente de TI: Responsável por investigar a origem e o escopo da violação de dados, tomar medidas para conter o incidente e implementar medidas corretivas para evitar futuros incidentes.

f) Chefe da Assessoria Jurídica: Realiza avaliação do impacto legal do incidente, além de gerenciar questões relacionadas à responsabilidade legal.

g) Chefe da Assessoria de Comunicação: Responsável por elaborar e coordenar mensagens e comunicar a violação de dados pessoais tanto interna quanto externamente, quando for o caso e assim for definido pelo Comitê, garantindo transparência e preservando a reputação da organização.

6. DIRETRIZES:

6.1 Detecção e Identificação de Incidentes

O possível incidente pode ser detectado por meio de uma comunicação feita pelo titular dos dados, por sistemas adotados para identificar vazamentos de informações, por relato de um operador ou, ainda, por alerta de um terceiro.

Todos os incidentes confirmados ou suspeitos devem ser imediatamente comunicados ao Encarregado de Proteção de Dados da CENTRAL, que coordenará a resposta conforme o Plano estabelecido.

6.2 Registro e Investigação

Todos os incidentes devem ser registrados no sistema SEI, com acesso restrito, incluindo informações como data e hora do incidente, método de detecção, categorias de dados afetados, número estimado de titulares afetados e causas preliminares.

6.3 Classificação de Incidentes

Os incidentes serão classificados para determinar a gravidade e a urgência das ações de resposta:

- ✓ **Crítica:** Incidentes de grande escala com impacto severo em operações ou segurança (ex.: ataque cibernético de grande escala, comprometimento de sistemas essenciais com perda significativa de dados);
- ✓ **Alta:** Incidentes com impacto significativo que podem afetar operações críticas ou envolver dados pessoais sensíveis (ex.: vazamento de dados sensíveis, comprometimento de sistemas críticos);
- ✓ **Média:** Incidentes com impacto moderado, que exigem intervenção (ex.: malware detectado e contido, acesso não autorizado a dados não sensíveis);
- ✓ **Baixa:** Incidentes com impacto mínimo e fácil resolução (ex.: spam, tentativas de phishing sem sucesso).

7. PROCEDIMENTO BÁSICO

PASSO	SETOR	AÇÃO A SER TOMADA
1	-	**Identificação e comunicação do incidente:** O possível incidente poderá ser detectado por meio de uma comunicação feita pelo titular dos dados, por sistemas adotados para identificar vazamentos de informações, por relato de um operador ou, ainda, por alerta de um terceiro. A comunicação do possível incidente deverá se dar preferencialmente através do contato de e-mail do Encarregado encarregado@central.rj.gov.br e, sendo **urgente**, através de todo e qualquer meio possível, incluso telefones, demais e-mails, etc. Importante salientar que, mesmo que algum outro setor da Companhia seja o primeiro a receber a informação, deverá comunicar imediatamente o Encarregado pelo Tratamento de Dados Pessoais
2	**Encarregado - DPO**	**a) Recebimento da notificação do incidente:** Todos os tipos de incidentes ou suspeitas de incidentes de segurança devem ser registrados via SEI, com acesso restrito. O registro deverá conter informações relevantes sobre o fato, como por exemplo: quando e como o incidente ocorreu, como a CENTRAL tomou conhecimento do

fato, quais categorias de dados foram afetadas, quantos e quais titulares possivelmente foram afetados, além das causas do incidente (se conhecidas).

Após receber a notificação de suspeita de incidente, o Encarregado deverá realizar a análise preliminar dentro de 2 (dois) dias úteis para verificar se o caso envolve dados pessoais e o potencial risco ou danos aos titulares dos dados.

b) Análise preliminar:

O Encarregado deverá realizar uma primeira avaliação dos fatos relatados para confirmar veracidade do incidente, quais sistemas foram afetados, como o incidente se desenvolveu, quem pode ter sido afetado, quais dados pessoais estavam envolvidos, a gravidade da violação ocorrida e se há risco de piora do incidente.

O encarregado, em conjunto com a Superintendência de TI, deverá coletar informações aptas à determinação e à identificação das irregularidades havidas, buscando definir a classificação da **"Gravidade do Impacto"** do incidente, conforme item 6.3 deste documento.

c) Resposta Imediata a Incidentes:

A depender da situação provocada pelo incidente, o Encarregado e/ou a Superintendência de TI, poderão tomar medidas imediatas para conter ou encerrar o incidente, visando restabelecer a normalidade dos serviços o mais rápido possível, com segurança;

Caso seja necessário divulgar informações referentes ao incidente à imprensa ou em meios de comunicação, essa divulgação deve ser conduzida com a **orientação e intermediação da Assessoria de Comunicação Social (ASSCOM)**, seguindo às diretrizes estabelecidas na **Política de Divulgação de Informações e de Porta-Vozes da CENTRAL**.

Caso sejam adotadas medidas, deverá ser preparado um registro ou relatório, a depender do caso, e do tempo hábil e ser encaminhado ao **Comitê de Resposta a Incidentes de Segurança com Dados Pessoais** para análise.

d) Comunicação / Notificação a Autoridades e Titulares dos Dados:

Comunicação ao Encarregado Central:

Ao receber a comunicação sobre o possível incidente de segurança, o Encarregado deverá comunicá-lo ao Encarregado Central para que este acompanhe as providências adotadas.

Notificação a Autoridades – ANPD:

Se confirmado o comprometimento da segurança dos dados pessoais e identificado risco ou dano relevante, o Encarregado analisará a necessidade de notificar preliminarmente a ANPD.

		Com a confirmação do Incidente de Segurança e Privacidade, o Encarregado deve formalizar a **Declaração de Incidente dentro do prazo de 3 (três) dias úteis** para notificação à ANPD, a contar da data do conhecimento pelo controlador de que o incidente afetou dados pessoais. As informações **poderão ser complementadas**, de maneira fundamentada, no **prazo de 20 (vinte) dias úteis**, a contar da data da comunicação. **Comunicação ao Titulares dos Dados:** A comunicação de incidente de segurança ao titular deverá ser realizada pelo controlador **no prazo de 3 (três) dias úteis** contados do conhecimento pelo controlador de que o incidente afetou dados pessoais. A comunicação do incidente aos titulares de dados deverá fazer uso de linguagem simples e de fácil entendimento e ocorrer de forma direta e individualizada, caso seja possível identificá-los. **Comunicação ao Controlador de Dados:** Se a CENTRAL desempenhar o papel de operadora de dados, deve comunicar oficialmente o controlador, para que este tome as medidas adequadas conforme exigido pela ANPD. **e) Convocação do Comitê de Resposta a Incidentes de Segurança com Dados Pessoais:** Assim que um incidente é identificado e classificado, e não sendo possível a ação imediata pelo Encarregado e/ou a Superintendência de TI, deverá ser elaborado um breve relatório do ocorrido e o Comitê deverá ser convocado para apreciar o caso imediatamente. O Encarregado e/ou a Superintendência de TI deverá enviar junto com a convocação para a reunião do Comitê o relatório mencionado no item c) ou e).
3	**Comitê de Resposta a Incidentes de Segurança com Dados Pessoais**	Recebido o Relatório, os membros do Comitê analisarão o documento para poder definir o encaminhamento e a tomada de decisão de como tratar o incidente, podendo adotar as seguintes medidas. **a) Investigação** Sendo necessário, o Comitê pode determinar que o Encarregado, em conjunto com a Superintendência de TI, realize apurações aprofundadas da irregularidade ocorrida, coletando informações aptas à determinação e à identificação das irregularidades havidas (ex.: spam, vírus, atuação de hacker, compartilhamento indevido de dados, etc), incluso a causa do incidente, endereços IP e credenciais envolvidas, transações e transferências de dados irregulares, métodos e vulnerabilidades exploradas. Após identificar todos os sistemas e serviços afetados relacionados com o incidente, deve-se avaliar o impacto do incidente e os potenciais riscos dos

sistemas afetados (dados vazados, informações de instituições parceiras, impacto na própria organização e na reputação).

b) <u>Indicação de medidas de segurança</u>

Após a apuração, e mesmo nos casos em que o incidente já tenha sido remediado, o Comitê deverá indicar as medidas de segurança utilizadas para prevenir recorrências, bem como as medidas adotadas após a descoberta do incidente. Essas medidas devem conter o incidente de maneira a atenuar os danos e evitar que demais recursos sejam comprometidos, além de eliminar as causas do incidente, removendo todos os eventos relacionados.

c) <u>Elaboração do Relatório do Comitê</u>

O Comitê deve elaborar um relatório detalhado, integrando todas as informações das etapas anteriores. O relatório deve:

- ✓ Registrar dados relevantes do incidente, incluindo sua natureza, impacto e possíveis consequências para os titulares dos dados afetados;
- ✓ Listar as medidas adotadas para mitigar ou reverter danos;
- ✓ Consolidar evidências para investigações regulatórias;
- ✓ Avaliar criticamente as ações tomadas para resolver o incidente;
- ✓ Documentar o processo de tratamento, incluindo lições aprendidas e a eficácia das soluções implementadas;
- ✓ Identificar falhas e recursos insuficientes para ajustar futuras respostas a incidentes;
- ✓ Aprimorar os procedimentos existentes e identificar características de incidentes úteis para treinamento;
- ✓ Fornecer estatísticas relevantes e coletar informações para procedimentos legais, se aplicável; e
- ✓ Realizar uma revisão das lições aprendidas para sugerir melhorias na segurança e nos procedimentos de resposta.

d) <u>Comunicação</u>

O Comitê deverá comunicar as decisões tomadas e as recomendações para prevenir incidentes futuros à área afetada, de forma a promover um consenso sobre a implementação de melhorias.

Em casos de incidentes não confirmados, a decisão deve ser fundamentada nas conclusões do relatório.

Caso seja necessário divulgar informações referentes ao incidente **<u>à imprensa ou em meios de comunicação</u>**, essa divulgação deve ser conduzida com a orientação e intermediação da **<u>Assessoria de Comunicação Social (ASSCOM)</u>** e deve atender às diretrizes estabelecidas na **Política de Divulgação de Informações e de Porta-Vozes da CENTRAL.**

		Encaminhar ao DPO para as providências cabíveis e posterior arquivamento.
4	**Encarregado - DPO**	Toma as medidas que ainda sejam necessárias, providencia o arquivamento dos relatórios produzidos e, quando for o caso, elabora um relatório final, observando as determinações da LGPD

8. REVISÕES E ALTERAÇÕES

Este procedimento padrão deve ser revisado e atualizado periodicamente pelos colaboradores designados para a função de **Encarregado pelo Tratamento de Dados Pessoais – DPO**, no mínimo anualmente, caso não ocorram eventos ou fatos relevantes que exijam uma revisão imediata.

As alterações devem ser aprovadas pelo **Comitê de Resposta a Incidentes de Segurança com Dados Pessoais** e pela **Diretoria Executiva**.

9. ANEXOS

Não aplicável

Sumário de Revisões		
Revisões:	**Data:**	**Descrição e/ou Itens Atingidos:**
0	21/07/2025	Emissão Original. Plano elaborado pelos Encarregado pelo Tratamento de Dados Pessoais (DPO/CENTRAL – Portaria Central Nº 772/2025) e ASSGER, processo SEI-100006/000772/2024. Aprovação DIREXE em 21/07/25.

Documento Assinado Eletronicamente
DIRETORIA EXECUTIVA
COMPANHIA ESTADUAL DE ENGENHARIA DE TRANSPORTES E LOGÍSTICA - CENTRAL

Distribuição: Geral

Chancela Técnica: Assessoria de Governança, Risco e Compliance - ASSGER

Rio de Janeiro, 21 julho de 2025

Documento assinado eletronicamente por **Daiti Augusto Hamanaka**, **Assessor Chefe da ASSGER**, em 22/07/2025, às 09:42, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

Documento assinado eletronicamente por **Fabricio Abilio Duarte de Moura**, **Diretor-Presidente**, em 23/07/2025, às 17:24, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

A autenticidade deste documento pode ser conferida no site http://sei.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **105028677** e o código CRC **DB46F186**.

Referência: Processo nº SEI-100006/000772/2024 SEI nº 105028677