



política de

tratamento de incidentes à privacidade de dados

Política aprovada na 340ª Reunião do Conselho de Administração, em 29/07/2020.
Revisada na 364ª Reunião do Conselho de Administração, em 27/07/2022, com vigência a partir desta data.



SUMÁRIO

CAPÍTULO I – OBJETIVOS.....	1
CAPÍTULO II – CANAL DE COMUNICAÇÃO.....	1
CAPÍTULO III – VIOLAÇÃO DE PRIVACIDADE DE DADOS.....	2
CAPÍTULO IV – ATRIBUIÇÕES DO ENCARREGADO DE DADOS EM CASOS DE VIOLAÇÃO À PRIVACIDADE DE DADOS PESSOAIS.....	2
CAPÍTULO V – ATIVIDADES DE PREVENÇÃO E DE TREINAMENTO.....	4
CAPÍTULO VI – RELATÓRIO DE OCORRÊNCIAS DE INCIDENTES.....	4

CAPÍTULO I – OBJETIVOS

Art. 1. A Política de Tratamento de Incidentes à Privacidade de Dados Pessoais da Celepar visa estabelecer responsabilidades e procedimentos para uma resposta rápida, efetiva e ordenada a incidentes envolvendo dados pessoais, em atendimento ao que preceitua o art. 48 da Lei Federal nº 13.709 de 14 de agosto de 2018 – Lei Geral de Proteção de Dados (LGPD).

CAPÍTULO II – CANAL DE COMUNICAÇÃO

Art. 2. Deverá haver um canal direto para a comunicação de incidentes e notificação de eventuais fragilidades que comprometam a companhia com relação ao que dispõe a LGPD, que estará diretamente ligado ao Encarregado de Proteção de Dados (D.P.O) e ao Diretor-Presidente da Celepar para o tratamento específico deste tema.

Art. 3. No caso em que os administradores, os empregados do quadro regular, os ocupantes de cargo em comissão, os cedidos à companhia, os terceirizados e os estagiários presenciarem eventual incidente deverão, obrigatoriamente, realizar a comunicação ao canal sob pena de tal omissão ser enquadrada como infração ao Código de Conduta da Celepar.

Art. 4. Na comunicação realizada neste canal deverão ser apresentadas as seguintes informações:

I - Identificação do comunicante;

II - Data e hora do incidente;

III - Localização e descrição do problema;

IV - Tipo de incidente (violação de confidencialidade ou de integridade ou indisponibilidade); **(redação dada na 364ª Reunião Ordinária do CAD, em 27/07/2022)**

V - Como foi descoberto;

VI - Quais pessoas foram informadas do incidente;

VII - Outras informações que entenda ser necessário.

Art. 5. Os incidentes devem ser imediatamente comunicados por quem o causou ou dele tomou conhecimento.

CAPÍTULO III – VIOLAÇÃO DE PRIVACIDADE DE DADOS

Art. 6. Violação de privacidade de dados consiste em incidente de segurança que resulta em uma violação de dados pessoais, de forma acidental ou ilícita, na destruição, perda, alteração, divulgação não autorizada ou acesso não autorizado aos dados pessoais tratados.

Art. 7. As violações de privacidade de dados classificam-se em violação de confidencialidade, violação de disponibilidade e violação de integridade.

Art. 8. Ocorre violação de confidencialidade quando os dados são divulgados sem autorização ou quando quem não tem autorização acessa os dados pessoais, seja de forma acidental ou ilícita.

Art. 9. A violação da privacidade por falta de disponibilidade dos dados ocorre quando há a perda permanente de acesso aos dados ou a sua destruição sem autorização ou de forma acidental.

Art. 10. Já a violação de integridade ocorre quando os dados são alterados de forma indevida, seja por ausência de autorização ou de forma acidental.

Art. 11. Os riscos de violação de privacidade podem ser escalonados em níveis/métricas a serem definidos de acordo com a probabilidade de ocorrência do dano e a severidade do impacto do dano aos direitos e liberdades dos titulares dos dados.

Art. 12. A comunicação relativa às violações de dados pessoais que acarretem risco ou dano relevante aos titulares deve seguir a regulamentação da Autoridade Nacional de Proteção de Dados. **(redação dada na 364ª Reunião Ordinária do CAD, em 27/07/2022)**

Art. 13. A classificação dos riscos relativos à privacidade de dados pessoais deverá constar em política específica.

CAPÍTULO IV – ATRIBUIÇÕES DO ENCARREGADO DE DADOS EM CASOS DE VIOLAÇÃO À PRIVACIDADE DE DADOS PESSOAIS

Art. 14. Em caso de violação de dados pessoais envolvendo a Celepar, na qualidade de controladora, o Encarregado de Proteção de Dados (D.P.O) compromete-se a:

I - Comunicar de imediato o Diretor-Presidente da Celepar, bem como a área de Governança;

II - Apurar e relatar como se deu a violação de dados pessoais e quais dados foram atingidos;

III - Orientar os empregados e os contratados da Celepar sobre medidas de proteção adequadas a fim de sanar a violação de dados pessoais ou mitigar o seu impacto;

IV - Executar as demais atribuições definidas pela Celepar.

Art. 15. Em caso de violação de dados pessoais controlados por outra Entidade e processados pela Celepar, o Encarregado de Dados (D.P.O.) compromete-se a:

I - Comunicar imediatamente o Encarregado de Proteção de Dados do Controlador e ao Diretor-Presidente da Celepar, bem como a área de Governança;

II - Apurar e relatar como se deu a violação de dados pessoais e quais dados foram afetados;

III - Aplicar as medidas de proteção adequadas a fim de sanar a violação de dados pessoais ou mitigar o seu impacto, de acordo com as orientações determinadas pelo Controlador;

IV - Adotar as medidas determinadas à Celepar pelo Controlador na sua Política de Tratamento de Incidentes

Art. 16. Nos casos de incidentes envolvendo dados pessoais, armazenados em meio físico ou digital, que não acarretarem risco ou dano relevante aos titulares dos dados, o Encarregado (D.P.O) deverá elaborar um relatório para fins de registro contendo as seguintes informações:

I - Descrição do incidente;

II - Classificação da categoria do risco de violação à privacidade (integridade, disponibilidade, confidencialidade);

III - Medidas organizacionais, técnicas e físicas de segurança que foram adotadas para mitigar ou reverter os efeitos do incidente. **(redação dada na 364ª Reunião Ordinária do CAD, em 27/07/2022)**

Art. 17. Havendo risco ou dano relevante aos direitos e liberdades dos titulares dos dados, o Encarregado de Proteção de Dados deverá comunicar à Autoridade Nacional de Proteção de Dados em prazo definido pela ANPD, e aos titulares dos dados sobre a ocorrência do incidente de segurança, com as seguintes informações:

I - Descrição da natureza dos dados pessoais afetados;

II - As informações sobre titulares envolvidos;

III - A indicação das medidas organizacionais, técnicas e físicas de segurança utilizadas para a proteção de dados, observados os segredos comercial e industrial;

IV - Os riscos relacionados ao incidente;

V - Os motivos de eventual demora, no caso de a comunicação não ter sido imediata;

VI - As medidas que foram e que estão sendo adotadas para reverter ou mitigar os efeitos do risco/dano;

VII - Contato do Encarregado de Proteção de dados - e-mail, telefone e endereço.

Art. 18. Quando houver esforço desproporcional para a notificação de cada titular de dado individualmente, poderá ser feita uma comunicação pública ou outra forma de comunicação eficaz.

Art. 19. Depois de encerrado o incidente, o Encarregado deverá fazer um balanço dos resultados e das ações que foram tomadas e, principalmente, refazer as avaliações de vulnerabilidade e riscos.

CAPÍTULO V – ATIVIDADES DE PREVENÇÃO E DE TREINAMENTO

Art. 20. Com a finalidade de prevenção e de preparação para eventual ocorrência de incidentes envolvendo a privacidade de dados pessoais, o Encarregado de Proteção de Dados deverá:

I - Realizar e registrar treinamentos de ocorrências de incidentes de violação de privacidade, de periodicidade anual, que sirvam para testar o plano de resposta à violação da privacidade de dados; **(redação dada na 364ª Reunião Ordinária do CAD, em 27/07/2022)**

II - Elaborar relatórios de violações de privacidade de dados, incluindo a análise da causa raiz para que sejam consultados e possibilitem uma resposta em um menor tempo em caso de um incidente semelhante.

CAPÍTULO VI – RELATÓRIO DE OCORRÊNCIAS DE INCIDENTES

Art. 21. O Encarregado de Proteção de Dados deverá preencher relatório no qual constarão as seguintes informações:

I - Data e horário da comunicação da ocorrência do incidente;

II - Nome e contato de quem comunicou o incidente;

III - Descrição do incidente;

IV - Classificação da violação à privacidade de dados (confidencialidade, integridade, disponibilidade);

V - Data e horário de comunicação da ocorrência ao Diretor-Presidente da Celepar e ao Controlador dos dados, se for o caso;

VI - Medidas organizacionais, técnicas e físicas de segurança que haviam sido adotadas que impediram a ocorrência do dano, ou que foram adotadas para mitigar ou reverter o dano;

VII - Indicação do nível de severidade do dano;

VIII - Indicação dos danos ocorridos em função do incidente relatado;

IX - Relação de dados que foram afetados;

X - Indicação se há a necessidade de comunicação do incidente à Autoridade Nacional de Proteção de Dados ou aos titulares dos dados;

XI - Relação de titulares de dados que foram comunicados, se for o caso, ou da cópia do comunicado geral realizado;

XII - Indicação da causa raiz do incidente, ou possíveis/prováveis causas;

XIII - Indicação de medidas a serem adotadas nos processos por padrão para evitar ou diminuir as chances de que incidente semelhante ocorra.

Art. 22. A Celepar deverá elaborar o Plano de Contingenciamento no qual deverá conter as Medidas Preventivas de Incidentes, Medidas de Detecção, Medidas Repressivas e Medidas Corretivas para os casos identificados na política de riscos de privacidade de dados pessoais a fim de evitar eventuais danos aos direitos e liberdades dos titulares dos dados.

Art. 23. No plano de contingenciamento deverá conter, ainda:

I - Contato de especialistas por temas os quais deverão apoiar o Encarregado de Proteção de Dados para averiguação da ocorrência do dano, proposta de melhor forma de mitigar os danos, se ocorridos, e investigação da origem da falha;

II - Contato da área jurídica e de comunicação que deverão apoiar o Encarregado de Proteção de Dados na formulação de respostas à Autoridade Nacional de Proteção de Dados e na comunicação aos titulares de dados, no caso de ocorrência de incidente que cause risco ou danos relevantes aos direitos dos titulares dos dados; **(redação dada na 364ª Reunião Ordinária do CAD, em 27/07/2022)**

III - Medidas organizacionais, técnicas e físicas de segurança que são adotadas por padrão para a prevenção do dano ligado ao risco identificado referente à privacidade dos dados pessoais.

Art. 24. A presente Política será revisada sempre que necessário ou, pelo menos, a cada 2 (dois) anos.