



CONSELHO REGIONAL DE CONTABILIDADE DE GOIÁS

RESOLUÇÃO CRCGO Nº 512, DE 28 DE JANEIRO DE 2025

Institui, ad-referendum, a Política de Comunicação de Incidente de Segurança com Dados Pessoais do Conselho Regional de Contabilidade de Goiás.

O CONSELHO REGIONAL DE CONTABILIDADE DE GOIÁS, no uso de suas atribuições legais e regimentais, resolve:

CAPÍTULO I

DA POLÍTICA E DO OBJETIVO

Art. 1º Fica instituída a Política de Comunicação de Incidente de Segurança com Dados Pessoais do Conselho Regional de Contabilidade de Goiás (CRCGO), em conformidade com a Lei nº 13.709, de 14 de agosto de 2018, que trata da Lei Geral de Proteção de Dados Pessoais (LGPD), e com a Resolução CD/ANPD nº 15, de 24 de abril de 2024, do Conselho Diretor (CD) da Autoridade Nacional de Proteção de Dados (ANPD), que aprova o Regulamento de Comunicação de Incidente de Segurança.

Art. 2º A Política tem por objetivo descrever os procedimentos necessários para a identificação e comunicação do incidente de segurança com dados pessoais.

CAPÍTULO II

DA IDENTIFICAÇÃO DE INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS

Art. 3º A identificação do incidente pode ocorrer das seguintes formas:

I – denúncia por parte do titular dos dados pessoais ou por parte de terceiros;

II – reporte por parte do operador; e

III – emprego de ferramentas automatizadas que detectam vazamentos de dados.

Art. 4º Todas as violações de dados pessoais devem ser informadas ao encarregado pelo tratamento de dados pessoais do CRCGO, sem demora injustificada, para registro e avaliação das medidas a serem

tomadas.

Art. 5º Em caso de incidente de segurança com dados pessoais, o operador deverá encaminhar a comunicação ao encarregado pelo tratamento de dados pessoais do CRCGO, pelo e-mail dpo@crcgo.org.br no prazo de 24 (vinte e quatro) horas, contadas da data do conhecimento do incidente.

Art. 6º Caso o titular ou um terceiro identifique um incidente de segurança com dados pessoais, a comunicação poderá ser enviada ao encarregado pelo tratamento de dados pessoais do CRCGO, pelo e-mail dpo@crcgo.org.br preferencialmente em até 48 (quarenta e oito) horas, contadas da data do conhecimento do incidente.

Art. 7º Na comunicação, o operador, terceiro ou titular dos dados pessoais deverá descrever o incidente, de forma sucinta, atentando para informações tais como:

I – a natureza da violação dos dados pessoais, incluindo, se possível, as categorias e o número aproximado de titulares de dados afetados, bem como as categorias e o número estimado de registros de dados pessoais em causa;

II – as consequências prováveis da violação de dados pessoais; e

III – as providências adotadas ou propostas para conduzir o caso, o que pode incluir medidas para mitigar os possíveis efeitos adversos da violação dos dados pessoais.

Art. 8º O encarregado pelo tratamento de dados pessoais do CRCGO será responsável pelo registro e pela análise inicial do incidente e pelo envio de resposta sobre o incidente relatado.

Art. 9º Após o registro e a análise inicial do incidente, o encarregado pelo tratamento de dados pessoais do CRCGO compartilhará a informação com o Comitê Gestor de Privacidade e Proteção de Dados (CGPPD) do CRCGO, que fará a avaliação das providências a serem tomadas.

§ 1º Caso necessário, o CGPPD poderá acionar a Coordenadoria de TI (CTI) e o Jurídico do CRCGO.

§ 2º O CGPPD não realiza procedimentos de investigação criminal, e eventuais desdobramentos relacionados aos incidentes deverão ser encaminhados às autoridades policiais competentes.

Art. 10. As partes envolvidas devem seguir as orientações do encarregado pelo tratamento de dados pessoais do CRCGO, pois a adoção de medidas por conta própria pode agravar o problema ou danificar evidências do incidente com dados pessoais.

Art. 11. As partes envolvidas devem manter sigilo sobre a comunicação recebida, pois tornar a informação pública pode prejudicar a investigação do suposto incidente com dados pessoais e a identificação do autor do incidente.

CAPÍTULO III

DA COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS

Seção I

Dos Critérios para Comunicação de Incidente de Segurança

Art. 12. O CRCGO deverá comunicar a ANPD e o titular da ocorrência de incidente de segurança com dados pessoais que possa acarretar risco ou dano relevante aos titulares.

§ 1º O CRCGO deverá avaliar internamente a relevância do risco ou dano do incidente de segurança, para determinar se deverá comunicar à ANPD e ao titular.

§ 2º O incidente de segurança pode acarretar risco ou dano relevante aos titulares quando puder afetar significativamente interesses e direitos fundamentais dos titulares e, cumulativamente, envolver, pelo menos, um dos seguintes critérios:

- I - dados pessoais sensíveis;
- II - dados de crianças, adolescentes ou idosos;
- III - dados financeiros;
- IV - dados de autenticação em sistemas;
- V - dados protegidos por sigilo legal, judicial ou profissional; ou
- VI - dados em larga escala.

§ 3º O incidente de segurança que possa afetar significativamente interesses e direitos fundamentais será caracterizado, entre outras situações, por ocorrências em que a atividade de tratamento puder impedir o exercício de direitos ou a utilização de um serviço, assim como ocasionar danos materiais ou morais aos titulares, tais como discriminação, violação à integridade física, ao direito à imagem e à reputação, fraudes financeiras ou roubo de identidade.

§ 4º Considera-se incidente com dados em larga escala aquele que abranger número significativo de titulares, considerando, ainda, o volume de dados envolvidos, bem como a duração, a frequência e a extensão geográfica de localização dos titulares.

§ 5º A comunicação não será necessária se o responsável pelo tratamento puder demonstrar, de forma irrefutável, que a violação da segurança dos dados pessoais não constitui um risco relevante para os direitos e as liberdades do titular dos dados.

Seção II

Da Comunicação de Incidente de Segurança à ANPD

Art. 13. Caso necessária, a comunicação de incidente de segurança à ANPD deverá ser realizada pelo CRCGO no prazo de três dias úteis.

§ 1º O prazo a que se refere o caput será contado do conhecimento pelo CRCGO de que o incidente afetou dados pessoais.

§ 2º A comunicação de incidente de segurança deverá conter as seguintes informações:

- I - a descrição da natureza e da categoria de dados pessoais afetados;
- II - o número de titulares afetados, discriminando, quando aplicável, o número de crianças, de adolescentes ou de idosos;
- III - as medidas técnicas e de segurança utilizadas para a proteção dos dados pessoais, adotadas antes e após o incidente;
- IV - os riscos relacionados ao incidente com identificação dos possíveis impactos aos titulares;
- V - os motivos da demora, no caso de a comunicação não ter sido realizada no prazo previsto no caput deste artigo;
- VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente sobre os titulares;
- VII - a data da ocorrência do incidente, quando possível determiná-la, e a de conhecimento pelo CRCGO;
- VIII - os dados do encarregado ou de quem represente o CRCGO;
- IX - a identificação do CRCGO;
- X - a identificação do operador, quando aplicável;
- XI - a descrição do incidente, incluindo a causa principal, caso seja possível identificá-la; e
- XII - o total de titulares cujos dados são tratados nas atividades afetadas pelo incidente.

Art. 14. As informações poderão ser complementadas, de maneira fundamentada, no prazo de vinte dias úteis, a contar da data da comunicação.

Art. 15. A comunicação de incidente de segurança deverá ocorrer por meio de formulário eletrônico disponibilizado pela ANPD e deverá ser realizada pelo CRCGO, por meio do encarregado, acompanhada de documento comprobatório de vínculo empregatício.

Parágrafo único. O encarregado pelo tratamento de dados pessoais do CRCGO comunicará o incidente com dados pessoais à ANPD, com base nas análises técnicas e jurídicas realizadas pelo CGPPD, pela CTI e pelo jurídico do CRCGO.

Seção III

Da Comunicação de Incidente de Segurança ao Titular

Art. 16. Caso necessária, a comunicação de incidente de segurança ao titular deverá ser realizada pelo CRCGO no prazo de três dias úteis contados do conhecimento de que o incidente afetou dados pessoais, e deverá conter as seguintes informações:

I - a descrição da natureza e da categoria de dados pessoais afetados;

II - as medidas técnicas e de segurança utilizadas para a proteção dos dados;

III - os riscos relacionados ao incidente com identificação dos possíveis impactos aos titulares;

IV - os motivos da demora, no caso de a comunicação não ter sido feita no prazo previsto no **caput** deste artigo;

V - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente, quando cabíveis;

VI - a data do conhecimento do incidente de segurança; e

VII - o contato para obtenção de informações e, quando aplicável, os dados de contato do encarregado.

§ 1º A comunicação do incidente aos titulares de dados deverá atender aos seguintes critérios:

I - fazer uso de linguagem simples e de fácil entendimento; e

II - ocorrer de forma direta e individualizada, caso seja possível identificá-los.

§ 2º Considera-se comunicação de forma direta e individualizada aquela realizada pelos meios usualmente utilizados pelo CRCGO para contatar o titular, tais como telefone, e-mail, mensagem eletrônica ou carta.

§ 3º Caso a comunicação direta e individualizada mostre-se inviável ou não seja possível identificar, parcial ou integralmente, os titulares afetados, o CRCGO deverá comunicar a ocorrência do incidente, no prazo e com base nas informações definidas no caput, pelos meios de divulgação disponíveis, tais como sítio eletrônico, aplicativos, mídias sociais e canais de atendimento ao titular, de modo que a comunicação permita o conhecimento amplo, com direta e fácil visualização, pelo período de, no mínimo, três meses.

§ 4º O CRCGO deverá juntar ao processo de comunicação de incidente uma declaração de que foi realizada a comunicação aos titulares, constando os meios de comunicação ou divulgação utilizados, em até três dias úteis, contados do término do prazo de que trata o caput deste artigo.

CAPÍTULO IV

DO REGISTRO DO INCIDENTE DE SEGURANÇA

Art. 17. O CRCGO deverá manter o registro do incidente de segurança, inclusive daquele não comunicado à ANPD e aos titulares, pelo prazo mínimo de cinco anos, contado a partir da data do registro, exceto se constatadas obrigações adicionais que demandem maior prazo de manutenção.

Parágrafo único. O registro do incidente deverá conter, no mínimo:

- I - a data de conhecimento do incidente;
- II - a descrição geral das circunstâncias em que o incidente ocorreu;
- III - a natureza e a categoria de dados afetados;
- IV - o número de titulares afetados;
- V - a avaliação do risco e os possíveis danos aos titulares;
- VI - as medidas de correção e mitigação dos efeitos do incidente, quando aplicável;
- VII - a forma e o conteúdo da comunicação, se o incidente tiver sido comunicado à ANPD e aos titulares;
e
- VIII - os motivos da ausência de comunicação, quando for o caso.

CAPÍTULO V DISPOSIÇÕES FINAIS

Art. 18. O encarregado pelo tratamento de dados pessoais do CRCGO ainda tem como responsabilidade:

- I – aprovar e autorizar a divulgação de comunicado aos titulares envolvidos no incidente com dados pessoais;
- II – validar quaisquer comunicados ao público, à imprensa e aos usuários;
- III – orientar e/ou informar as equipes interessadas sobre as práticas a serem adotadas com relação ao incidente com dados pessoais;
- IV – coordenar todas as ações decorrentes do incidente com dados, com o intuito de mitigar os impactos percebidos;
- V – atuar como porta-voz do CRCGO perante a ANPD, as demais autoridades competentes e os usuários, supervisionando os contatos e as comunicações com o público decorrentes do incidente com dados pessoais, dentre outras atividades.

Art. 19. Os casos omissos desta Política serão resolvidos pelo Comitê Gestor de Privacidade e Proteção de Dados (CGPPD) do CRCGO.

Art. 20. Esta Resolução entra em vigor na data de sua assinatura.

Art. 21. Fica revogada a Resolução CRCGO nº 454, de 11 de outubro de 2022.

CONTADORA SUCENA HUMMEL
Presidente