CRCES
CONSELHO REGIONAL DE CONTABILIDADE DO ESPÍRITO SANTO

RESOLUÇÃO CRCES N.º 452, DE 15 DE DEZEMBRO DE 2022.

Institui a Política de Notificação de Incidentes de Segurança com Dados Pessoais no âmbito do Conselho Regional de Contabilidade do Espírito Santo - CRCES.

O **PLENÁRIO DO CONSELHO REGIONAL DE CONTABILIDADE DO ESPÍRITO SANTO,** no uso de suas atribuições legais e regimentais, nos termos do inciso XVIII, art. 11, da Resolução n.º 342/2014;

CONSIDERANDO a necessária conformidade do CRCES aos termos da Lei Geral de Proteção de Dados Pessoais, Lei n.º 13.709, de 14 de agosto de 2018;

CONSIDERANDO a Portaria CRCES n.º 59, de 17 de maio de 2022, que criou o Comitê de Segurança da Informação (CSI) no âmbito do Conselho Regional de Contabilidade do Espírito Santo;

CONSIDERANDO que os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito;

CONSIDERANDO que os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta política em relação aos dados pessoais, mesmo após o seu término;

R E S O L V E:

Art. 1º. Instituir a Política de Notificação de Incidentes de Segurança com Dados Pessoais por meio do Manual de Notificação de Incidentes de Segurança com Dados Pessoais, nos termos do Anexo desta Resolução.

Art. 2º. Esta Resolução entra em vigor na data de sua assinatura.

Contadora **Carla Cristina Tasso**
Presidente

Aprovada na 1650ª Reunião Plenária, realizada em 15 de dezembro de 2022

ANEXO

MANUAL DE NOTIFICAÇÃO DE INCIDENTES DE SEGURANÇA COM DADOS PESSOAIS

1. INTRODUÇÃO

O Conselho Regional de Contabilidade do Espírito Santo resolveu instituir a presente Política tendo em vista o mandamento legal contido na Lei n.º 13.709, de 14 de agosto de 2018, que trata da Lei Geral de Proteção de Dados Pessoais (LGPD);

É certo que os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito e que estes agentes ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista na LGPD em relação aos dados pessoais, mesmo após o seu término.

Sendo assim, se faz necessário tal manual que objetiva para orientar os colaboradores do CRCES e principalmente os membros do Comitê Comissão de Segurança da Informação.

2. TERMINOLOGIA

Além das terminologias já especificadas no art. 5º da Lei Geral de Proteção de Dados Pessoais - LGPD, destaca-se ainda alguns outros termos, quais sejam:

1. Comitê de Segurança da Informação (CSI): comissão responsável pela avaliação dos mecanismos de tratamento, privacidade e proteção de dados existentes e pela proposição de ações voltadas ao seu aperfeiçoamento com vistas ao cumprimento das disposições da Lei n.º 13.709, de 14 de agosto de 2018, no âmbito do CRCES;

2. Notificação: ato ou efeito de informar ou de dar a conhecer sobre uma ocorrência e/ou incidente de segurança com dados pessoais;

3. Incidente de segurança com dados pessoais: qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou, ainda, qualquer forma de tratamento de dados inadequada ou ilícita, que possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais.

3. OBJETIVO

A Política de Notificação de Incidentes de Segurança com Dados Pessoais do CRCES tem por objetivo descrever os procedimentos necessários para a identificação, comunicação e notificação do incidente de segurança com dados pessoais.

4. COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS

A identificação do incidente pode ocorrer das seguintes formas:

I. denúncia por parte de titular ou terceiro;

II. reporte por parte do operador;

III. pelo emprego de ferramentas automatizadas que detectam vazamentos de dados;

Todas as violações de dados pessoais devem ser comunicadas ao Encarregado pelo Tratamento de Dados Pessoais do CRCES, sem demora injustificada, para registro e avaliação das medidas a tomar.

Em caso de um incidente de segurança com dados pessoais, o operador deverá encaminhar a comunicação ao Encarregado pelo Tratamento de Dados Pessoais do CRCES, pelo e-mail privacidade@crc-es.org.br, no prazo de 24 (vinte e quatro) horas, contadas da data do conhecimento do incidente. No caso do titular ou terceiro, a comunicação de um incidente de segurança com dados pessoais poderá ser enviada ao Encarregado pelo Tratamento de Dados Pessoais do CRCES, pelo e-mail privacidade@crc-es.org.br, preferencialmente, em até 48 (quarenta e oito) horas, contadas da data do conhecimento do incidente.

Na comunicação, o operador, o terceiro ou o titular dos dados pessoais deverão descrever sucintamente o incidente ocorrido, atentando para informações, tais como:

I. descrever 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 aproximado de registros de dados pessoais em causa;

II. descrever as consequências prováveis da violação de dados pessoais;

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

O Encarregado pelo Tratamento de Dados Pessoais do CRCES será responsável pelo registro e análise inicial do incidente e pela resposta sobre o incidente relatado.

Após o registro e a análise inicial do incidente, o Encarregado pelo Tratamento de Dados Pessoais do CRCES compartilhará a comunicação com o Comitê de Segurança da Informação (CSI), que fará a avaliação das medidas a tomar e caso necessário, poderá acionar o Setor de TI e o Setor Jurídico.

O Comitê de Segurança da Informação não realiza procedimentos de investigação criminal, e eventuais desdobramentos relacionados aos incidentes deverão ser encaminhados às autoridades policiais competentes.

As partes envolvidas devem seguir as orientações do Encarregado pelo Tratamento de Dados Pessoais do CRCES, pois a adoção de medidas por conta própria pode agravar o problema ou danificar evidências do incidente com dados pessoais. Devem ainda 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.

5. DA NOTIFICAÇÃO DE INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS

O CRCES deverá notificar a Agência Nacional de Proteção de Dados e o titular da ocorrência de incidente de segurança com dados pessoais que possa acarretar risco ou dano relevante aos titulares.

Antes de se fazer a notificação, será avaliado internamente se a relevância do risco ou dano do incidente de segurança foram severos e graves o suficiente para se determinar a necessidade de tal notificação.

Sendo que, para a avaliação interna, deverão ser analisados os incidentes que envolvam especialmente:

I. descrever 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 aproximado de registros de dados pessoais em causa;

II. descrever as consequências prováveis da violação de dados pessoais.

Tal notificação 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 liberdades do titular dos dados.

Caso necessária, a notificação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:

I. a descrição da natureza dos dados pessoais afetados;

II. as informações sobre os titulares envolvidos;

III. a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;

IV. os riscos relacionados ao incidente;

V. os motivos da demora, no caso de a comunicação não ter sido imediata;

VI. as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo

Caso não seja possível fornecer todas as informações no momento da notificação preliminar, informações adicionais poderão ser fornecidas posteriormente, sendo que no momento da notificação preliminar deverá ser informado à ANPD se serão fornecidas mais informações posteriormente, bem como quais meios estão sendo utilizados para obtê-las.

A notificação à ANPD será feita por intermédio do Encarregado pelo Tratamento de Dados Pessoais do CRCES que comunicará o incidente com dados pessoais à ANPD,

com base nas análises técnicas e jurídicas realizadas pelo Comitê de Segurança da Informação.

O Encarregado pelo Tratamento de Dados Pessoais do CRCES 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, imprensa e usuários;

III. orientar e/ou informar as equipes interessadas a respeito das 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 CRCES perante a ANPD, demais autoridades competentes e os usuários, supervisionando os contatos e comunicações com o público, decorrentes do incidente com dados pessoais, dentre outras atividades.