



**DELIBERAÇÃO CRCPR Nº 026/2022, DE 11 DE ABRIL DE 2022
(Ata 1.374ª)**

**APROVA A POLÍTICA DE REGISTRO DE
INCIDENTES DO CONSELHO REGIONAL DE
CONTABILIDADE DO PARANÁ (CRCPR).**

O Plenário do **CONSELHO REGIONAL DE CONTABILIDADE DO PARANÁ**, no uso de suas atribuições legais e regimentais,

Considerando a Lei n.º 13.709, de 14 de agosto de 2018, que trata da Lei Geral de Proteção de Dados Pessoais, assim com a legislação correlata à proteção de Dados Pessoais,

DELIBERA, no sentido de:

Art. 1º - Aprovar a Política de Registro de Incidentes do Conselho Regional de Contabilidade do Paraná.

Art. 2º - A presente Deliberação entrará em vigor na data de sua assinatura, revogando-se a Deliberação CRCPR nº 009/2022, bem como, as demais disposições em contrário.

ORIGINAL ASSINADO

Contador **LAUDELINO JOCHEM**

Presidente

CO – CRCPR Nº 44.143/O





POLÍTICA DE REGISTRO DE INCIDENTES

1. OBJETIVO

Definir regras e procedimentos de segurança para o registro de ocorrência de incidentes no ambiente de tecnologia e/ou analógico utilizado pelo CRCPR, em conformidade com o art. 48 da Lei nº 13.709/2018 (LGPD).

2. ABRANGÊNCIA

Este regulamento se aplica a todo o tratamento de dados pessoais realizados no CRCPR. Este regulamento está alinhado com a Política de Segurança da Informação do CRCPR.

3. IMPLEMENTAÇÃO

O departamento responsável pela Segurança da Informação e as chefias das áreas da empresa desenvolverão as ações necessárias e contínuas para implementação do regulamento, ficando o departamento de TI responsável pela coordenação das ações de tecnologia e a gerência operacional por atitudes referentes aos incidentes analógicos.

4. REGRAS E PROCEDIMENTOS

4.1. Ocorrência de incidente

Todo incidente envolvendo dados pessoais que possa acarretar risco ou dano relevante aos titulares de dados deve ser registrado pelos colaboradores e comunicado às equipes de Tecnologia da Informação e à gerência operacional, que adotarão os procedimentos necessários.

4.2. Tratamento da ocorrência do incidente

A equipe do setor de Tecnologia da Informação ou a gerência operacional deve:

- a) Registrar o incidente nos sistemas da empresa.
- b) Comunicar à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares de dados sobre o incidente e os possíveis riscos e/ou danos.
- c) A comunicação deverá ser realizada em prazo razoável e deverá mencionar, no mínimo:
 - Descrição da natureza dos dados pessoais afetados;
 - As informações sobre os titulares envolvidos;





- Indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
 - Os riscos relacionados ao incidente;
 - Os motivos da demora, no caso da comunicação não ter sido imediata;
 - As medidas que foram ou serão adotadas para reverter ou mitigar os efeitos do prejuízo.
- d) Acompanhar as ações desenvolvidas para solução definitiva da causa do incidente.
- e) Avaliar a necessidade de criação de novos mecanismos de controle de segurança da informação, com objetivo de evitar novos incidentes.
- f) Emitir relatório gerencial sobre o incidente ocorrido, indicando a solução encontrada para o caso, as medidas adotadas para minimização dos danos e as providências definidas pela ANPD.

4.3. Tratamento após a solução definitiva do incidente

O CRCPR deverá fazer o gerenciamento de causas mais frequentes, tipos de incidentes e áreas nas quais ocorreram, com intuito de fazer a gestão efetiva para identificar problemas que podem gerar incidentes e solucionar as questões.

5. CONTROLES E RESPONSABILIDADES

As equipes de Tecnologia da Informação e a gerência operacional, também responsáveis pela Segurança da Informação, deverão manter este manual atualizado e, se necessário, gerar outros documentos relativos aos procedimentos para o controle do acesso remoto pelo usuário ou para utilização de documentos físicos fora das dependências da empresa.

6. CONCLUSÃO

O descumprimento deste manual e/ou dos demais instrumentos normativos que complementam o processo de segurança da informação constitui falta grave, passível de penalidades administrativas e contratuais.

Situações de excepcionalidade não previstas deverão ser definidas pelas equipes de Tecnologia da Informação e outros setores responsáveis, com apoio da gestão, considerando as áreas da organização que estejam envolvidas.