SERVIÇO PÚBLICO FEDERAL
CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA DE MINAS GERAIS – CREA-MG

PORTARIA Nº 091, DE 7 DE MARÇO DE 2022.

O PRESIDENTE DO CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA DE MINAS GERAIS – CREA-MG, no uso de suas atribuições legais e regimentais, e

Considerando o disposto nos incisos V e XLV do artigo 96 do Regimento do Crea-MG, homologado *'ad referendum'* do Plenário do Confea através da Portaria AD n.º 009, de 27 de janeiro de 2009, referendada pela Decisão PL n.º 0061 do Confea, de 04 de fevereiro de 2009;

Considerando que o Plano de Resposta a Incidentes com Dados Pessoais do Crea-MG (PRIDP-Crea-MG) é parte da estrutura de documentos para a proteção de dados e está baseado nos princípios da Lei Geral de Proteção de Dados Pessoais (LGPD) – Lei Federal n. 13.709/2018.

RESOLVE:

Art. 1º Instituir o **Plano de Resposta a Incidentes com Dados Pessoais do Crea-MG (PRIDP-Crea-MG)**, parte integrante desta Portaria, em anexo.

Art. 2º Esta portaria entra em vigor na data da sua assinatura e revoga as disposições em contrário.

REGISTRE-SE, DIVULGUE-SE E CUMPRA-SE.

Belo Horizonte, 7 de março de 2022.

Engº Civil Lucio Fernando Borges
Presidente do Crea-MG

CREA - MG
Romy Cristhina S. Valadares
OAB/MG 117.944
PROCURADORIA

Plano de Resposta a Incidentes com Dados Pessoais do Conselho Regional de Engenharia e Agronomia de Minas Gerais (PRIDP - CREA-MG)

SUMÁRIO

CREA - MG
Romy Cristhine S. Valadares
OAB/MG 117.944
PROCURADORIA

1. INTRODUÇÃO

O Plano de Resposta a Incidentes com Dados Pessoais (PRIDP) é essencialmente um processo. Descreve a forma como o Crea-MG irá atuar em resposta às situações de emergência e exceção. Pelo potencial gravidade, a resposta do Conselho deve ser rápida e confiável, ao mesmo tempo resguardando evidências forenses que podem ajudar a prevenir novos incidentes e atendendo as exigências legais de comunicação e transparência.

2. DEFINIÇÕES

- **ANPD:** Autoridade Nacional de Proteção de Dados - órgão da administração pública direta federal do Brasil que faz parte da Presidência da República e possui atribuições relacionadas a proteção de dados pessoais e da privacidade e, sobretudo, fiscaliza o cumprimento da Lei nº 13.709/2018.
- **Notificador:** pessoa ou sistema de monitoração que notifica incidente.
- **CRI:** Comissão de Resposta a Incidentes.
- **Acionadores da CRI**: grupo que receberá notificações de incidentes em primeira mão para triagem, estruturado em níveis distintos para viabilizar a comunicação à ANPD em até 2 (dois) dias úteis.
- **Responsável por Sistema ou Controlador de Sistema**: indicado que deve ser contatado e pode autorizar ou vetar procedimentos de emergência.
- **Encarregado pelo Tratamento de Dados Pessoais (DPO):** membro especial da CRI, responsável por encaminhar comunicações formais no caso de incidentes envolvendo dados pessoais.
- **Desenvolvedores/ Operadores/ Fornecedores dos sistemas**: atuam no desenvolvimento de solução e instalação dos sistemas que operam no Crea-MG.

CREA - MG
Romy Cristhine S. Veladares
OAB/MG 117.944
PROCURADORIA

3. PREPARAÇÃO

Formação da Comissão de Resposta a Incidentes (CRI): Este é um grupo de colaboradores que deve ser designado, por meio de portaria, com acessos, habilidades, responsabilidades, treinamento e conhecimentos chave para responder aos mais variados tipos de incidentes.

A CRI deve ter reuniões periódicas para definir melhorias neste plano, verificação de pré-requisitos, mecanismos, atribuições, necessidade de preparo, bem como divulgação e treinamentos para os membros e demais empregados.

O Encarregado pelo Tratamento de Dados Pessoais (DPO) e, pelo menos, um representante da equipe da Gerência de Tecnologia da Informação devem fazer parte desse grupo.

Instalação e divulgação dos mecanismos de comunicação de incidente: Devem ser criadas, disponibilizadas e publicadas as formas de notificação ao Conselho quando ocorrerem incidentes. O §1º, do Artigo 41, da Lei 13709/2018, a LGPD, estabelece: *"A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador."*

Desse modo, deve ser divulgado o e-mail dpo@crea-mg.org.br, bem como os contatos do atendimento do Crea-MG. Deve haver indicação de quais mecanismos são considerados rápidos e seguros e se sugere o esclarecimento de quais as expectativas de anonimato que o notificador deve ter.

As informações devem ser claras e concisas. Além do que prescreve o § 1º do artigo 48 da LGPD, recomenda-se que a comunicação contenha as seguintes informações, disponíveis no formulário de comunicação de incidentes de segurança com dados pessoais da ANPD:

CREA-MG

CREA - MG
Romy Cristhine S. Veladares
OAB/MG 117.944
PROCURADORIA

Identificação e dados de contato de:

- Entidade ou pessoa responsável pelo tratamento.
- Encarregado de dados ou outra pessoa de contato.
- Indicação se a notificação é completa ou parcial. Em caso de comunicação parcial, indicar que se trata de uma comunicação preliminar ou de uma comunicação complementar.

Informações sobre o incidente de segurança com dados pessoais:

- Data e hora da detecção.
- Data e hora do incidente e sua duração.
- Circunstâncias em que ocorreram a violação de segurança de dados pessoais, por exemplo, perda, extravio, cópia, vazamento, dentre outros.
- Descrição dos dados pessoais e informações afetadas, como natureza e conteúdo dos dados pessoais, categoria e quantidade de dados e de titulares afetados
- Resumo do incidente de segurança com dados pessoais, com indicação da localização física e meio de armazenamento.
- Possíveis consequências e efeitos negativos sobre os titulares dos dados afetados.
- Medidas de segurança, técnicas e administrativas preventivas tomadas pelo controlador de acordo com a LGPD.
- Resumo das medidas implementadas até o momento para controlar os possíveis danos.
- Possíveis implicações de natureza transfronteiriça.
- Outras informações úteis às pessoas afetadas para proteger seus dados ou prevenir possíveis danos.

CREA-MG
Romy Cristhine S. Valadares
OAB/MG 117.944
PROCURADORIA

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

Definição do grupo de Acionadores da CRI: Responsáveis por receberem as notificações e a realização do tratamento inicial. Para viabilizar a comunicação à ANPD em até 2 (dois) dias úteis, este grupo deve incluir membros do atendimento e contatos qualificados para executar a triagem.

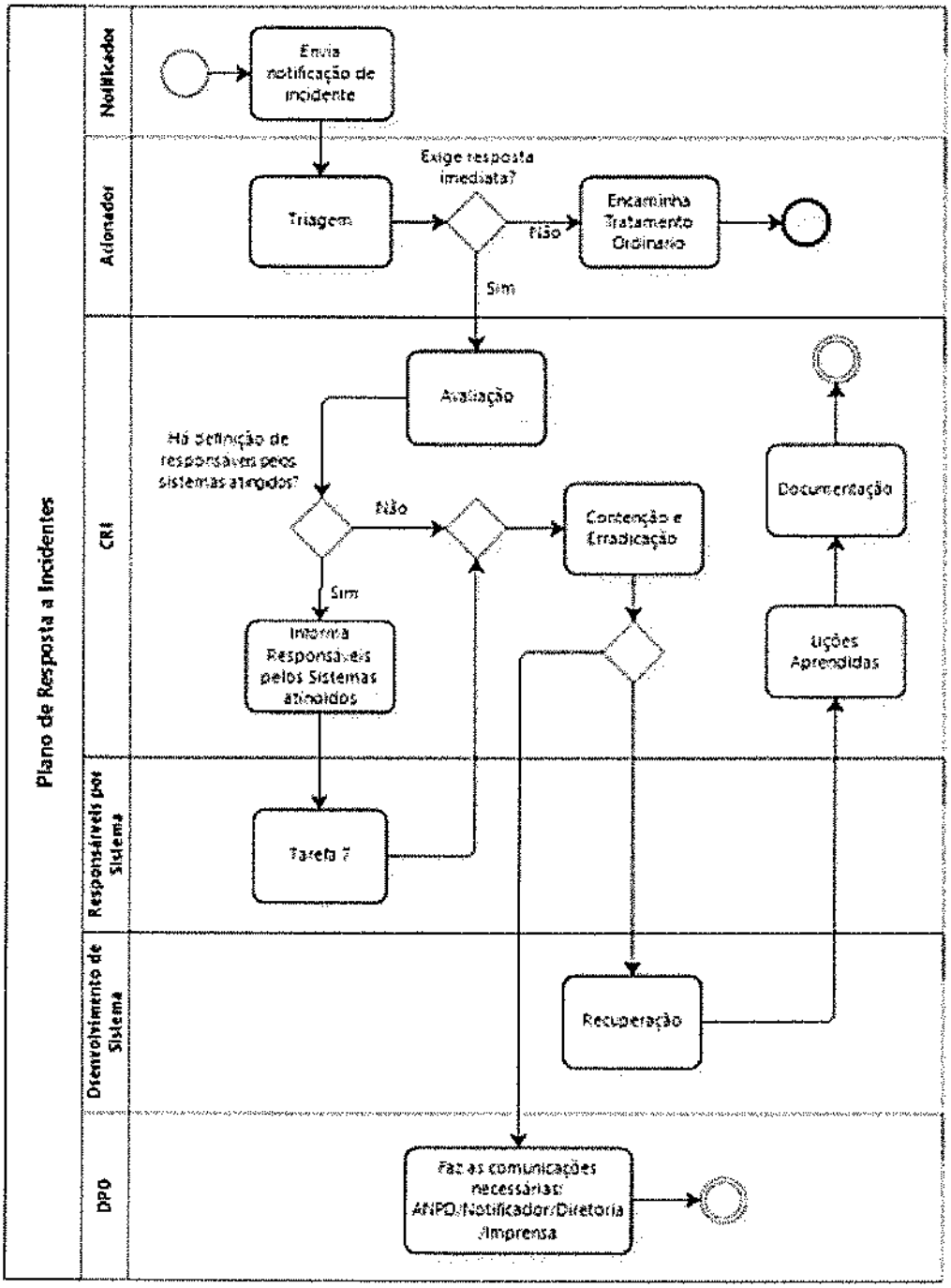
Instalação, configuração e definição de ferramentas de monitoria e alarmes: Devem ser criados e aprovados, pela CRI, mecanismos ou ferramentas de comunicação direta como, por exemplo: e-mail; WhatsApp ou outros meios capazes de informar, diretamente, à CRI, incidentes de vazamento de dados pessoais.

Preparo de um Plano de Comunicação de Incidentes: Para facilitar a comunicação ao Conselho deve ser criada e aprovada, pela CRI, uma biblioteca com modelos de documentos (*templates*) para comunicação formal do Encarregado pelo Tratamento de Dados Pessoais com a ANPD, titulares de dados, notificadores e imprensa.

CREA - MG
Ramy Cristhine S. Valadares
OAB/MG 117.944
PROCURADORIA

4. PROCEDIMENTO APÓS O INCIDENTE

4.1. Fluxograma



4.2. Início

Um novo incidente é notificado, por pessoa externa ou não ao Crea-MG ou, ainda, por algum meio de monitoramento, usando um dos mecanismos de comunicação definidos pela CRI, conforme item 3. Notificação é recebida por Acionador do CRI.

4.3. Triagem

O Acionador do CRI deve fazer a avaliação preliminar ou contatar imediatamente outro Acionador em condições de realizar a referida avaliação, descartando as notificações nulas ou claramente improcedentes, tomando os devidos cuidados.

Na avaliação preliminar, devem ser buscadas informações sobre os sistemas que foram alegadamente impactados, sua criticidade, quais os danos aparentes e o risco da situação se agravar se não houver resposta imediata.

Incidentes que não envolvem e que, seguramente, não apresentam riscos aumentados pela falta de ação imediata, podem ser reencaminhados, conforme avaliação preliminar dos Acionadores da CRI, para tramites regulares do Crea-MG pelo Encarregado pelo Tratamento de Dados Pessoais (DPO), ainda que o incidente envolva dados pessoais.

Em caso de incidentes que exigem resposta imediata ou melhor avaliação, a CRI deve ser acionada para proceder às seguintes fases.

4.4. Avaliação

Nesta fase deve ser iniciada uma avaliação mais detalhada do incidente. Deve-se procurar identificar por exemplo: a causa do incidente; qual o processo, nos casos de incidente com dados físicos; qual o sistema, nos casos de incidente com dados digitais; endereços IP e/ou credenciais envolvidas; transações e transferências de dados

irregulares; métodos e vulnerabilidades exploradas, de modo que seja possível determinar ações para as demais fases.

Pode ser importante engajar, a critério da CRI a qualquer momento que julgar adequado e viável, especialistas dos sistemas ou processos afetados, de modo que possam colaborar com a avaliação.

4.5. Contenção e Erradicação

Devem ser acionados os responsáveis pelos dados digitais ou dados físicos afetados, os quais serão responsáveis por orientar e se manifestar sobre os procedimentos de contenção e erradicação.

O objetivo das medidas de contenção e erradicação é limitar o dano e isolar os processos ou sistemas afetados, para evitar mais danos. Neste momento, conforme a necessidade e a autorização obtidas, será realizada a suspensão dos processos ou o desligamento dos sistemas inteiros ou de etapas ou funcionalidades especificas. É importante, sempre que possível, que sejam emitidos e colocados avisos de indisponibilidade para manutenção.

Devem ser tomados os devidos cuidados para que não haja a eliminação das evidências que possam ser usadas para identificar autoria, origem e método usado para quebrar a segurança.

4.6. Recuperação

A recuperação é o conjunto de medidas para restaurar os serviços completamente. Pode ser feita de forma gradual, conforme viabilidade e decisão do responsável pelo processo ou pelo sistema.

CREA-MG

CREA - MG
Romy Cristhine S. Valadares
OAB/MG 117.944
PROCURADORIA

A CRI tem a responsabilidade de passar as informações que obteve para o desenvolvimento da solução e sua instalação.

Para a recuperação devem ser tomadas medidas identificadas na Avaliação, tais como: reintegração dos dados físicos ao processo, restauração de backups, clonagem de máquinas virtuais, reinstalação de sistemas.

Pode ser necessário o desenvolvimento de um novo processo ou a instalação de atualizações de aplicação ou do Sistema Operacional. Por esse motivo, esta fase pode ser prolongada, de acordo com a priorização dada.

4.7. Lições Aprendidas

Com o incidente contido e sua resolução encaminhada, a CRI deve agendar e conduzir uma reunião de Lições Aprendidas, com convidados a seu critério, com o objetivo de discutir erros e dificuldades encontradas, propor melhorias para os sistemas e processos, inclusive deste Plano de Resposta a Incidentes.

As melhorias sugeridas na reunião, com o devido consenso, devem ser encaminhadas aos responsáveis para definição sobre a adoção.

4.8. Documentação

A CRI deve documentar o incidente em base de conhecimentos apropriada, detalhando as informações obtidas, linha de tempo, atores envolvidos, evidencias, conclusões, decisões, autorizações e ações tomadas, inclusive as da reunião de lições aprendidas.

4.9. Comunicações

Assim que possível, no caso de incidente relacionado A dados pessoais, o Encarregado de Tratamento de Dados (DPO) deve avaliar e fazer as comunicações obrigatórias por

Lei. Essas comunicações podem incluir agradecimentos ao notificador, informações para os titulares de dados, relatórios formais para a ANPD, entre outras.

CREA - MG
Romy Cristhine S. Valadares
OAB/MG 117.944
PROCURADORIA