PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA COM DADOS PESSOAIS

Belo Horizonte (MG)

2025

1. INTRODUÇÃO

Este Plano de Resposta a Incidentes de Segurança com Dados Pessoais tem por finalidade apresentar orientações, com o intuito de auxiliar os funcionários e colaboradores do Clube Certo responsáveis por realizarem a gestão de respostas à incidentes de segurança com dados pessoais no âmbito institucional, trazendo uma visão macro sobre resposta a esses incidentes, para fomentar a adequação e conformidade à Lei Geral de Proteção de Dados Pessoais.

O plano dispõe de medidas que devem ser adotadas no caso de uma emergência ou evento de risco / incidente que possa ocasionar danos aos ativos tecnológicos do Clube Certo, viabilizando, inclusive, a comunicação apropriada e tempestiva à ANPD, quando for o caso, notadamente a observância do disposto pelo art. 48[1] da Lei Geral de Proteção de Dados.

---

[1] **Art. 48**. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.
§ 1º A comunicação 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; e
VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.
§ 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como:
I - ampla divulgação do fato em meios de comunicação; e
II - medidas para reverter ou mitigar os efeitos do incidente.
§ 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.

2. OBJETIVOS

2.1. OBJETIVO GERAL

Orientar os responsáveis por realizarem a gestão de respostas à incidentes de segurança com dados pessoais do Clube Certo em como responder às emergências com incidentes de segurança da informação, de forma documentada, formalizada, rápida e confiável, ao passo em que resguarde as evidências que possam ajudar a prevenir novos incidentes e a atender às exigências legais de comunicação e transparência.

2.2 OBJETIVOS ESPECÍFICOS

Determina-se como objetivos específicos deste Plano:

- Conferir clareza sobre o fluxo de procedimentos adequados e responsáveis no caso de incidentes;
- Preservar a reputação e imagem do Clube Certo;
- Assegurar respostas rápidas, efetivas e coordenadas;
- Quantificar e monitorar desempenho; e
- Evoluir continuamente com as lições aprendidas.

3. DEFINIÇÕES GERAIS

Para auxílio na leitura deste Plano, serão adotadas as seguintes definições:

- **Agente de tratamento**: aqueles que podem ter alguma ação no tratamento de um incidente que coloque em risco a segurança dos dados pessoais.
- **Controlador**: pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais.
- **Operador**: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.
- **Encarregado pelo Tratamento de Dados Pessoais ou Data Privacy Officer (DPO)**: é a pessoa indicada pelo controlador e operador para atuar como

canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

- **Autoridade Nacional de Proteção de Dados (ANPD):** entidade responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional, conforme as atribuições descritas no art. 55-J da LGPD e no Decreto nº: 10.474 de 26 de agosto de 2020.
- **Dados pessoais**: é toda informação relacionada à pessoa natural identificada ou identificável.
- **Dados pessoais sensíveis:** são dados que digam respeito a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
- **Incidente**: evento, ação ou omissão que tenha permitido ou possa vir a permitir acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou, ainda, apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação.
- **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 em destruição, perda, alteração, vazamento ou, ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais.
- **Incidente de segurança:** qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores.
- **Medidas de segurança**: medidas técnicas e/ou administrativas adotadas para proteger os dados pessoais de acessos não autorizados e de

situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

- **Lei Geral de Proteção de Dados Pessoais (LGPD):** Lei nº: 13.709, de 14 de agosto de 2018, cujo objetivo é proteger os direitos fundamentais de privacidade e de liberdade de cada indivíduo
- **Relatório final:** documento que contém todas as evidências e ações realizadas para tratamento do incidente e que deve ser emitido ao final das tratativas.
- **Relatório de Impacto a Proteção de Dados (RIPD):** documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que tem o potencial de gerar riscos às liberdades civis e aos direitos fundamentais dos titulares, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

4. INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS

Em conformidade com a Lei Geral de Proteção de Dados, um incidente de segurança é um acontecimento indesejado ou inesperado, hábil a comprometer a segurança dos dados pessoais, de modo a expô-los a acessos não autorizados e a situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Em caso de incidente que coloque em risco a segurança de dados pessoais devem ser realizados alguns procedimentos específicos que são listados abaixo:

4.1. AVALIAÇÃO INTERNA DO INCIDENTE

Avaliar internamente o incidente para obter informações iniciais sobre o impacto do ocorrido, tais como:

- Origem;
- Categoria;

- Quantidade de titulares e de dados pessoais afetados;
- Categoria e quantidade de dados afetados;
- Consequências do incidente para os titulares e para a entidade;
- Criticidade; e
- Probabilidade.

Em função da combinação desses critérios, realizar a classificação de criticidade do incidente de acordo com as definições a seguir:

- Alta (impacto grave): incidente que afeta sistemas relevantes ou informações críticas, com potencial para gerar impacto negativo sobre o Clube Certo;
- Média (impacto significativo): incidente que afeta sistemas ou informações não críticas, sem impacto negativo ao Clube Certo;
- Baixa (impacto mínimo): possível incidente, sistemas não críticos, investigações de incidentes de colaboradores; investigações de longo prazo envolvendo pesquisa extensa e/ou trabalho forense detalhado.

Além disso, é necessário preservar todas as evidências do incidente.

4.2. COMUNICAÇÃO AO ENCARREGADO

Comunicar ao Encarregado do Clube Certo a existência do incidente, caso envolva dados pessoais, por intermédio de endereço eletrônico, a saber, encarregado.lgpd@clubecerto.com.br.

4.3. REGISTRAR INCIDENTE DE SEGURANÇA

É necessário o registro de informações sobre o incidente de segurança, sendo estas mantidas por um prazo de, no mínimo, cinco anos.

Conforme o art. 10 da Resolução CD/ANPD n.º: 15/2024, o Controlador é responsável por manter o registro do incidente de segurança, mesmo que não

tenha sido comunicado à ANPD e aos titulares. Tal registro deverá conter minimamente os seguintes itens:

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.

4.4. CONSULTAR O SETOR DE TECNOLOGIA DA INFORMAÇÃO

Consultar o Setor de Tecnologia da Informação em caso de incidentes na rede computacional. Após análise preliminar do incidente, o Setor deve dar ciência aos Diretores dos processos afetados, informando, por exemplo, registros de acesso e análise do fluxo de dados, identificando uma possível continuidade do ataque.

4.5. COMUNICAR A TODOS OS ENVOLVIDOS

O Controlador deve comunicar a existência do incidente a todos os envolvidos, conforme o caso e termos previstos na LGPD.

4.6. COMUNICAR À ANPD

Comunicar à ANPD e ao titular de dados pessoais (conforme art. 48 da LGPD) a existência do incidente, em conformidade com a regulamentação legal.

4.7. EMITIR O RELATÓRIO FINAL

Emitir o Relatório Final contendo os tipos de dados e a quantidade de titulares afetados. Deve também acompanhar um relatório técnico de tratamento que permita avaliar a extensão e adequação de medidas para incidentes futuros.

5. RESPOSTAS AOS INCIDENTES DE SEGURANÇA

O Clube Certo deverá dar respostas aos seus incidentes conforme as orientações das fases descritas abaixo, utilizando o fluxo detalhado e o checklist disponíveis no final deste documento.

5.1. PREPARAÇÃO/NOTIFICAÇÃO

Fase de importante estabelecimento da capacidade de resposta à incidentes, como também a evitá-los e garantir que sistemas, redes e aplicativos sejam suficientemente seguros. Nesta fase, o Encarregado pelo Tratamento de Dados Pessoais, o Setor de Tecnologia da Informação e a Equipe Técnica de Segurança da Informação estarão preparados para responder e dar os encaminhamentos para juntos atuarem na resposta aos incidentes.

5.2. ANÁLISE / AVALIAÇÃO

Os incidentes podem ser detectados por vários meios ou recebidos nos canais de comunicação do Clube Certo. Assim que o órgão for notificado deverá ser iniciada uma avaliação mais detalhada do incidente pelo Encarregado e a Equipe Técnica de Segurança da Informação, que farão a classificação e definirão a sua criticidade.

5.2.1. AVALIAÇÃO DO INCIDENTE

Quando o Clube Certo tem conhecimento do incidente de segurança, deve ser realizada uma avaliação interna para que sejam obtidas informações como:

a) qual vulnerabilidade foi explorada no evento, abrangendo situações como acesso indevido aos dados pessoais; roubo de dados; ataques cibernéticos; erros de programação de aplicativos e sistemas internos; engenharia social; descartes indevidos; repasse de dados pessoais; roubo, venda e utilização de dados tutelados; comprometimento de senhas de acesso; e outras.

b) fonte dos dados pessoais: meio pelo qual foram obtidos os dados pessoais, tais como preenchimento de formulário eletrônico ou não eletrônico por parte do titular, API, uso compartilhado de dados, XML e cookies.
c) categoria de dados pessoais: sensíveis e de crianças e adolescentes.
d) extensão do vazamento: quantificar os titulares e os dados pessoais que tiveram a sua segurança violada neste evento.
e) avaliação do impacto ao titular: avaliar quais são os impactos que o incidente pode gerar aos titulares.
f) avaliação do impacto no serviço: avaliar os impactos que o incidente pode gerar a entidade como perda de confiabilidade do cidadão, ações judiciais, danos à imagem da empresa em âmbito nacional e internacional, prejuízo à entidade em contratos com fornecedores e clientes, e impacto total ou parcial nas atividades desenvolvidas pela entidade.

5.3. CONTENÇÃO, ERRADICAÇÃO E RECUPERAÇÃO

O Gestor do Processo e o responsável pelo sistema impactados, quando for o caso, devem ser acionados para se manifestarem sobre os procedimentos de resposta, contenção e erradicação.

O objetivo das medidas de contenção e erradicação é limitar o dano e isolar os sistemas afetados para evitar mais danos. Nessa fase, conforme a necessidade e a autorização obtida, poderá ser realizado o desligamento dos sistemas inteiros ou de funcionalidades específicas e colocados avisos de indisponibilidade para manutenção. Todos os cuidados devem ser adotados para não impactar evidências que poderiam ser usadas para identificar autoria, origem e método usado para quebrar a segurança.

5.4. ATIVIDADES PÓS-INCIDENTE

Na fase de atividades pós-incidente, serão implementadas algumas atividades em busca da melhoria contínua de seus processos de resposta a incidentes, além de definir procedimentos para retenção de evidências e uso dos dados coletados em incidentes.

6. COMUNICAÇÃO À ANPD E TITULAR DE DADOS PESSOAIS

6.1. À ANPD

A ANPD estipula o prazo de 3 (três) dias úteis para comunicação de incidente de segurança à proteção de dados que será contado a partir do conhecimento pelo controlador de que o incidente afetou os dados pessoais por ele tratado. O incidente deve ser comunicado pelo Controlador, por meio do Encarregado, ou por meio de representante constituído respeitando o prazo estabelecido. O art. 48 da LGPD e o art. 5º da Resolução CD/ANPD n.º: 15/2024 determinam que o Controlador tem o dever de comunicar à ANPD e ao titular dos dados pessoais a ocorrência de incidente de segurança que tenha potencial de risco ou dano relevante que possam afetar consideravelmente seus interesses e direitos fundamentais e, cumulativamente, envolver, pelo menos, um dos seguintes critérios:

a) dados pessoais sensíveis;
b) dados de crianças, de adolescentes ou de idosos;
c) dados financeiros;
d) dados de autenticação em sistemas;
e) por sigilo legal, judicial ou profissional; ou
f) dados em larga escala.

A Autoridade Nacional de Proteção de Dados disponibiliza, em seu sítio eletrônico, uma página com as orientações para a comunicação de incidentes de segurança. A página pode ser acessada no site da ANPD através do seguinte link: https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca.

6.2. AO TITULAR DE DADOS PESSOAIS

Cabe ao Controlador comunicar ao titular dos dados pessoais a ocorrência de incidente de segurança que tenha potencial de lhe gerar riscos ou danos

relevantes. Tal comunicação deve ser realizada de maneira transparente, podendo ser realizada por meios diversos, incluindo mensagens diretas (e-mails, SMS), banners, notificações em sites, comunicações postais e anúncios.

A comunicação do incidente aos titulares deve ser feita em linguagem clara e simplificada e mencionar, no que couber, os elementos previstos no §1º do art. 48 da LGPD, e do art. 9º da Resolução CD/ANPD n.º: 15/2024, tais como:

- A descrição geral do incidente e a data da ocorrência;
- A natureza dos dados pessoais afetados e os riscos relacionados ao incidente com a identificação dos possíveis impactos aos titulares;
- As medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
- O motivo da demora, no caso de a comunicação não ter sido feita no prazo determinado;
- As medidas tomadas e recomendadas para reverter ou mitigar os efeitos do incidente;
- A data do conhecimento do incidente de segurança;
- O contato do encarregado ou o ponto de contato para que os titulares obtenham informações a respeito do incidente; e
- Outras informações que possam auxiliar os titulares a prevenirem possíveis danos.

Se, pela natureza do incidente, não for possível identificar individualmente os titulares afetados, o controlador deverá comunicar a ocorrência do incidente pelos meios de divulgação disponíveis, tais como seu sítio eletrônico, aplicativos, suas mídias sociais e canais de atendimento ao titular, de modo que a comunicação permita o conhecimento amplo, com direta e fácil visualização, pelo período mínimo de 3 (três) meses, conforme a Resolução CD/ANPD n.º: 15/2024. Além disso, o controlador deve incluir no processo de comunicação de incidente uma declaração de que a comunicação aos

titulares foi realizada, indicando os meios de comunicação ou divulgação utilizados.

7. RELATÓRIO FINAL DO INCIDENTE

Após a coleta de todas as informações e evidências, o Encarregado com o apoio da Equipe Técnica de Segurança da Informação, irá concluir o Relatório Final do Incidente. O Relatório final será realizado com base em todas as evidências coletadas desde a identificação do incidente até o final das apurações. Nesse documento constará, além de todas as informações sobre o incidente, todas as propostas de melhorias e/ou aquisições sugeridas para redução dos riscos de novas ocorrências. O relatório, além de ter uma função de comprovação das medidas tomadas pelo Clube Certo frente às autoridades, é importante para que todos os envolvidos e demais funcionários e colaboradores possam aprender com o ocorrido, podendo compreender suas causas, bem como avaliar em que sentido seu Plano de Respostas a Incidentes e seus procedimentos foram efetivos ou não, analisando a atuação dos responsáveis.

O Relatório Final do Incidente será assinado pelo Encarregado e deve ficar disponível para consulta em caso de atualização do Relatório de Impacto à Proteção de Dados. Esse relatório poderá, ainda, ser apresentado a autoridades policiais, órgãos reguladores ou demais envolvidos.

8. DA EXTINÇÃO DO PROCESSO DE COMUNICAÇÃO DO INCIDENTE

O processo de comunicação de incidente será considerado extinto nas seguintes hipóteses:

- Caso não sejam identificadas evidências suficientes da ocorrência do incidente;
- Caso a ANPD considere que o incidente não possui potencial para acarretar risco ou dano relevante aos titulares;
- Caso o incidente não envolva dados pessoais;

- Caso tenham sido tomadas todas as medidas adicionais para mitigação ou reversão dos efeitos gerados; ou
- Realização da comunicação aos titulares e adoção das providências pertinentes pelo controlador, em conformidade com a LGPD e as determinações da ANPD;

9. REFERÊNCIAS

BRASIL. Lei Federal n.º: 11.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Comunicação de Incidentes de Segurança. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Resolução CD/ANPD n.º: 15, de 24 de abril de 2024. Aprova o Regulamento de Comunicação de Incidente de Segurança. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024.

GET PRIVACY. Perguntas e respostas sobre o vazamento de dados pessoais. Disponível em: https://www.google.com/search?client=safari&rls=en&q=GET+PRIVACY+PERGUNTAS+E+RESPOSTAS+SOBRE+VAZAMENTO+DE+DADOS&ie=UTF-8&oe=UTF-8.

CONTROLADORIA GERAL DO ESTADO DO PARANÁ. Manual de Implementação da LGPD. Disponível em: https://www.cge.pr.gov.br/sites/default/arquivos_restritos/files/documento/2021-06/manual_implementacao_lgpd.pdf.