Universidade Estadual do Centro-Oeste

Comitê de Gestor de Proteção de Dados Pessoais, CGPDP

PLANO DE RESPOSTAS A INCIDENTES DE SEGURANÇA COM DADOS PESSOAIS DA UNICENTRO

APROVADO EM: 02 de Julho de 2024 – Ata nº 2/2024 - CGPDP

Jul/2024

SUMÁRIO

1 Introdução

Este Plano de Resposta a Incidentes de Segurança com dados pessoais foi elaborado como complemento da Política de Segurança da Informação (PSI) e da Política de Privacidade e Proteção de dados Pessoais (PPPDP), elaborados e publicados pela Universidade Estadual do Centro-Oeste, Unicentro.

O propósito do documento é estabelecer os procedimentos para Comunicação, Registro e Resposta a Incidentes de Segurança com dados pessoais, que possam acarretar risco ou dano relevante aos titulares de dados pessoais e/ou possam ocasionar danos à imagem da Universidade, inclusive, as medidas de comunicação à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares de dados pessoais, quando for o caso.

O presente plano será atualizado continuamente para incorporar melhorias, à medida que forem publicadas novas normas e aprimoramentos nos processos de proteção de dados existentes.

2 DEFINIÇÕES GERAIS

Para facilitar o entendimento na compreensão deste Plano de Resposta a Incidentes de Segurança com dados pessoais, serão adotadas as seguintes definições:

AGENTE DE TRATAMENTO: são agentes de tratamento aqueles que podem ter alguma ação no tratamento de um incidente que coloque em risco a segurança dos dados pessoais. Esses agentes são:

- **CONTROLADOR:** pessoa natural ou jurídica, de direito público ou privado, a quem competem 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.

A depender do contexto, uma mesma operação de tratamento de dados pessoais pode envolver mais de um operador ou controlador (controladoria conjunta, ou co-controladores).

ENCARREGADO: pessoa indicada pelo controlador e pelo operador para atuar como canal de comunicação com os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS: A LGPD atribui à Autoridade Nacional de Proteção de Dados (ANPD) a responsabilidade por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional, conforme as competências descritas no art. 55-J da LGPD e no Decreto Federal nº 10.474, de 26 de agosto de 2020.

CGPDP: Comitê Gestor de Proteção de Dados Pessoais, criado pela Resolução nº 6-CAD/UNICENTRO, de 23 de março de 2022, é responsável por planejar, organizar, controlar e orientar o processo de tratamento de dados pessoais no âmbito da Unicentro.

DADO PESSOAL: é toda informação relacionada a pessoa natural identificada ou identificável.

IDP: O Inventário de Dados Pessoais representa um artefato primordial para documentar o tratamento de dados pessoais realizado pela instituição.

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: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores.

INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS: qualquer evento adverso, confirmado ou sob suspeita, relacionado à violação de dados pessoais, sendo acesso não autorizado, acidental ou ilícito que resulte em destruição, perda, alteração, vazamento ou qualquer forma de tratamento de dados ilícita ou inadequada, que tem a capacidade de pôr em risco os direitos e as liberdades dos titulares dos dados pessoais.

LGPD: Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), cujo objetivo é proteger os direitos fundamentais de privacidade e de liberdade de cada indivíduo.

RELATÓRIO FINAL: relatório que contenha todas as evidências e ações realizadas para tratamento do incidente e que deve ser emitido ao final das tratativas.

RIPD: conforme a LGPD, o Relatório de Impacto a Proteção de Dados (RIPD) é uma 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 riscos.

3 PROCEDIMENTOS DE TRATAMENTO DE INCIDENTES DE SEGURANÇA COM DADOS PESSOAIS

Conforme prevê o artigo 46 da LGPD, os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais de incidentes de segurança, de acordo com as regras de boas práticas de governança para o tratamento de dados pessoais.

3.1 ETAPAS A SEREM ADOTADAS EM CASO DE INCIDENTES QUE COLOQUEM EM RISCO A SEGURANÇA DE DADOS PESSOAIS:

a) Comunicar ao Encarregado a existência do incidente, caso envolva dados pessoais;

b) Avaliar internamente o incidente com o objetivo de obter informações iniciais sobre o impacto do evento, tais como: natureza, categoria e quantidade de titulares de dados pessoais afetados, consequências do incidente para os titulares de dados e para a Unicentro. O registro e avaliação serão realizados em formulário, conforme anexo I deste Plano.

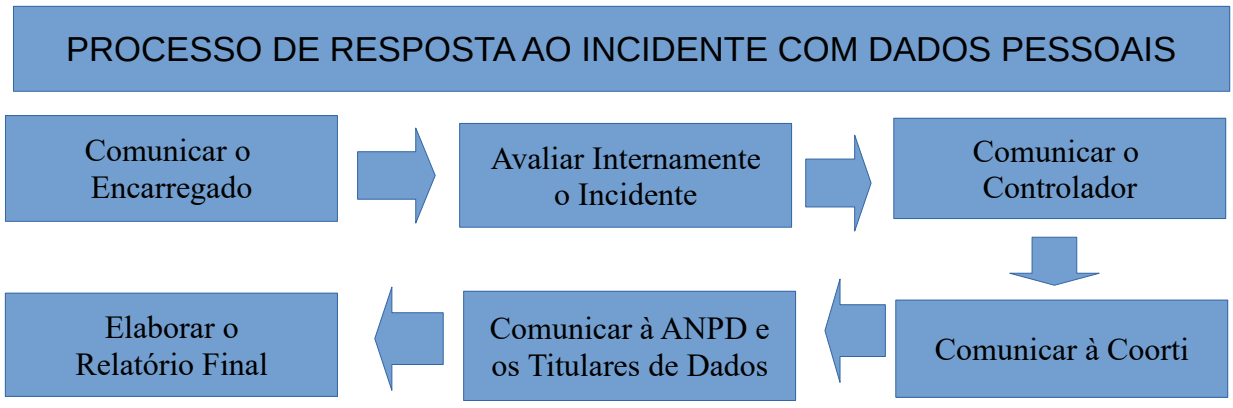
c) Comunicar ao Controlador, nos termos da LGPD, a existência do incidente, caso envolva dados pessoais;

d) Comunicar à Coordenadoria de Tecnologia da Informação, Coorti, nos casos de incidente relacionado a segurança da informação;

e) Comunicar à ANPD e ao titular de dados pessoais a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares (art. 48 da LGPD).

f) Elaborar o relatório final do incidente com todas as informações coletadas, as ações realizadas para o tratamento efetivo do incidente e as considerações necessárias para promover a melhoria contínua no atendimento de tais eventos, bem como para atualizar o Relatório de Impacto à Proteção dos Dados Pessoais (RIPD) e para o cumprimento do princípio de responsabilização e prestação de contas (art. 6º inciso X, da LGPD).

A figura a seguir apresenta de maneira simplificada o processo de resposta ao incidente de segurança com dados pessoais.



A seguir, apresenta-se o detalhamento dos procedimentos, mencionados no item 3.1, a serem adotados em caso de possível incidente de segurança com dados pessoais.

3.1.1 Comunicação ao Encarregado pelo tratamento de dados pessoais da Unicentro

A comunicação de incidente de segurança deverá ser realizada por meio do Canal da Ouvidoria da Unicentro.

3.1.2 Avaliação Interna do Incidente

Assim, que o Encarregado receber a comunicação de um incidente, o mesmo iniciará uma avaliação interna, conforme o anexo I, a fim de que sejam obtidas informações como:

a) Vulnerabilidade explorada no evento, abrangendo situações como: acesso indevido ou não autorizado aos dados pessoais; perda, furto ou roubo de dados; ataques cibernéticos; erros de programação de aplicativos e de sistemas internos; engenharia social; descartes indevidos; repasses indevidos de dados pessoais; venda e utilização de dados; comprometimento de senhas de acesso, entre outras.

b) Fonte dos dados pessoais: meios pelos quais foram obtidos os dados pessoais, tais como: preenchimento de formulário eletrônico ou não eletrônico pelo titular de dados; uso compartilhado de dados pessoais; sistemas eletrônicos; banco de dados.

c) Categoria de dados pessoais: dados sensíveis; dados de crianças, adolescentes e pessoas idosas; dados públicos; dados anonimizados; dados pseudoanonimizados.

d) Extensão do vazamento: quantificar os titulares e os dados pessoais que tiveram a sua segurança violada no evento.

e) Avaliação do impacto ao titular: avaliar quais são os impactos que o incidente pode gerar aos títulares.

f) Avaliação do impacto no serviço: avaliar os impactos que o incidente pode gerar à Universidade, como: perda de confiabilidade do cidadão; ações judiciais; danos à imagem em âmbito nacional e internacional; prejuízo à entidade em contratos com fornecedores e clientes; impacto total ou parcial nas atividades desenvolvidas pela Instituição.

Nesta etapa é importante que seja preservado o máximo de evidências do incidente e de todas as medidas adotadas a partir de sua ciência, a fim de que se demonstre, para eventuais autoridades que posteriormente vierem a apurar os fatos, inteiramente a cadeia de diligências realizadas para entendimento do evento e mitigação dos seus efeitos.

A figura a seguir demonstra, de forma ilustrativa, o processo de avaliação interna a ser realizada pelo Encarregado/Controlador, no caso, de incidente com dados pessoais.

PROCESSO DE AVALIAÇÃO INTERNA

Análise da vulnerabilidade	Fonte dos Dados pessoais	Categoria dos Dados Pessoais	Extensão do Vazamento	Avaliação de Impacto

No processo de avaliação do incidente com dados pessoais deve-se considerar o tipo de incidente, conforme seguinte classificação:

a) Ciberespaço: quando o incidente está relacionado à Tecnologia da Informação;

b) Material: quando o incidente envolve dados armazenados em dispositivos físicos;

c) Pessoas: quando envolve atitude humana, falha ao manusear o sistema, ao inserir documentos e divulgar sem as devidas anonimizações ou violação verbal, quando há vazamento de dados de forma verbal, seja por indiscrição (comentários acerca de dados

pessoais que são percebidos por terceiros e utilizados de má-fé) ou de forma intencional, repassando indevidamente.

Para que se possa avaliar o impacto do incidente, é necessário considerar os seguintes níveis de riscos padrões:

a) Risco Baixo: classificação utilizada quando um incidente de segurança de dados afetar apenas dados pessoais, não incluindo o número do CPF;

b) Risco Moderado: classificação utilizada quando o incidentente de segurança de dados afetar apenas dados pessoais, incluindo do CPF, e/ou pelo menos um dado sensível, não incluindo raça, religião, nome social e dados de saúde;

c) Risco Alto: classificação utilizada quando o incidente de segurança de dados afetar dados pessoais, incluindo o número do CPF e/ou mais que um dado sensível, incluindo raça, religião, nome social e dados de saúde.

De acordo com nível de risco identificado, o agente de tratamento deverá adotar as providências específicas.

3.1.3 Comunicação ao controlador

O Encarregado deverá dar ciência ao controlador da notificação de incidentes, que tomar conhecimento.

O operador deve comunicar incidentes com dados pessoais ao controlador o mais breve possível, a fim de viabilizar que este exerça seu papel tempestivamente, conforme disposto no art. 48 da LGPD.

3.1.4 Comunicação à Coordenadoria de Tecnologia – Coorti

O Encarregado deverá comunicar à Coorti, quando a comunicação de incidentes recebida envolver incidentes Cibernéticos.

3.1.5 Comunicação à ANPD e aos Titulares de Dados

Na comunicação à ANPD e ao titular o controlador deve considerar a ocorrência de incidentes de segurança que possam acarretar risco ou dano relevante aos titulares (art. 4º da Resolução nº 15/2024 – CD/ANPD). 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 (art. 5º da Resolução nº 15/2024 – CD/ANPD):

I dados pessoais sensíveis;

II dados de crianças, de adolescentes ou de idosos;

III dados financeiros;

IV dados de autenticação em sistemas;

V dados protegidos por sigilo legal, judicial ou profissional; ou

VI dados de larga escala.

A ANPD, considera incidente com dados pessoias 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.

O Encarregado avaliará a relevância do risco ou dano do incidente para determinar se deverá comunicar à ANPD e ao titular. Se for tomada a decisão de não notificar, a justificativa para essa decisão deve ser documentada no Formulário de Registro de Incidente de Segurança com Dados Pessoais (anexo I).

A Unicentro deve continuar a monitorar as circunstâncias e os efeitos de uma violação. Além disso, à medida que novas informações surgirem, esta poderá fazer ou atualizar notificações à ANPD ou comunicações do titular dos dados.

3.1.5.1 Comunicação à ANPD

A comunicação à ANPD deverá ser realizada pelo Controlador, exclusivamente por meio de canal específico no sítio eletrônico da ANPD.

A ANPD estipula na Resolução CD/ANPD nº 15, de 24 de abril de 2024, o prazo de três dias úteis para comunicação do incidente de segurança a proteção de dados. Caso, não seja possível fornecer todas as informações no momento da comunicação, estas poderão ser complementadas, de maneira fundamentada, no prazo de vinte dias úteis, a contar da data da comunicação preliminar (§ 3º do art. 6º da Resolução nº 15/2024 -CD/ANPD).

A comunicação à ANPD de incidentes de segurança deve conter as seguintes informações (art. 6º da Resolução 15/2024-CD/ANPD):

I a descrição da natureza dos 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 seguranças 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 da comunicação não ter sido feita no prazo previsto na legislação;

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 seu conhecimento pelo controlador;

VIII os dados do encarregado ou de quem represente o controlador;

IX a identificação do controlador;

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 de tratamento afetadas pelo incidente.

3.1.5.2 Comunicação ao titular dos dados pessoais

A Comunicação aos titulares de dados, quando necessária, dar-se-á no prazo de três dias úteis contados do conhecimento pelo controlador de que o incidente afetou dados pessoais, e deverá conter as seguintes Informações (Resolução nº 15/2024 – CD/ANPD):

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

II as medidas técnicas e de seguranças utilizadas para a proteção dos dados, observados os segredos comercial e industrial;

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 estipulado pela ANPD;

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 E ncarregado.

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.

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

3.1.6 Elaboração do relatório final do incidente

Após a conclusão das atividades do procedimento "Resposta ao incidente", o Encarregado de dados encaminhará ao gabinete da reitoria, o relatório final.

O Relatório final será realizado com base em todas as evidências coletadas desde a identificação do incidente até o final das apurações. Nesse documento constarão, 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 pela Unicentro frente as autoridades, é importante para que todos os envolvidos 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.

Adotados todos os procedimentos para o tratamento do incidente com dados pessoais, inclusive quanto ao registro das lições aprendidas, o processo administrativo instaurado deve ser encerrado, e arquivado pelo prazo mínimo de cinco anos, conforme prevê o art. 10 da Resolução CD/ANPD nº 15, de 24 de abril de 2024.

A ANPD poderá solicitar esse relatório para análise, com o propósito de:

- avaliar as ações tomadas durante o incidente em que dados pessoais tenham sido expostos ou comprometidos;
- publicar e atualizar normas referentes à proteção de dados;
- cumprir o princípio da responsabilização;

- utilizá-lo como subsídio para eventuais questionamentos, facilitando a comprovação de conformidade.

4 RESPOSTAS AOS INCIDENTES DE SEGURANÇA

A Unicentro vai dar respostas aos incidentes notificados ou detectados utilizando das orientações da PPPDP e da PSI, bem como de normas e procedimentos complementares necessários à contenção e erradicação do incidente de maneira a limitar o dano e isolar os sistemas e processos afetados.

4.1 CONTENÇÃO, ERRADICAÇÃO E RECUPERAÇÃO

Os responsáveis pelos sistemas/processos impactados devem ser acionados para se manifestarem sobre os procedimentos de respostas: contenção, erradicação e recuperação. O objetivo das medidas de contenção, erradicação e recuperação é limitar o dano e isolar os sistemas afetados para evitar mais danos. Todos os cuidados devem ser adotados para não impactar evidências que poderiam ser usadas para identificar a autoria, origem e métodos usados para quebrar a segurança.

4.1.1 Contenção

Na etapa de contenção adotam-se ações, a fim de evitar que outros recursos sejam comprometidos, impedindo que o incidente se agrave. As ações específicas a serem executadas dependerão das circunstâncias do incidente. Durante a contenção, deve haver o registro do incidente e das medidas que foram adotadas, evitando ao máximo a perda de evidências e das provas do ocorrido.

4.1.2 Erradicação

Na etapa de erradicação eliminam-se as causas do incidente, removendo todos os eventos a ele relacionados.

4.1.3 Recuperação

Na etapa de recuperação restaura-se o sistema/processo ao seu estado inicial/normal, e implementa medidas de segurança para evitar novos comprometimentos.

4.2 ATIVIDADES PÓS-INCIDENTE

Na fase de atividades pós-incidente, serão implementadas atividades e procedimentos necessários à melhoria contínua dos processos institucionais de resposta a incidentes, e serão definidos procedimentos para retenção de evidências e uso dos dados coletados em incidentes.

REFERÊNCIAS

BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). **Comunicação de Incidentes de segurança**. Disponível em: http://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

BRASIL. **Resolução CD/ANPD nº 15, de 24 de abril de 2024**. Regulamento de Comunicação de Incidente de Segurança. Disponível em: http://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-16-de-7-de-maio-de-2024-558531744

BRASIL. Universidade Federal de Itajubá – UNIFEI. **Plano de Tratamento de Incidentes de Segurança**. Disponível em: https://drive.unifei.edu.br/index.php/s/yrNs6Z94AhaNnLZ

ESTADO DE SANTA CATARINA. **Guia de Resposta a Incidentes de Segurança** – Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.sea.sc.gov.br/wp-content/uploads/2022/12/Plano-de-Resposta-a-Incidentes-da-SEA.pdf

GOVERNO FEDERAL. **Guia de Respostas a Incidentes de Segurança**. Disponível em: http://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_resposta_incidentes.pdf

HISTÓRICO DE VERSÕES			
Data	**Versão**	**Descrição**	**Autor**
24/05/2024	1.0	Criação do Documento	Encarregado pelo Tratamento d e Dados
02/07/2024	1.0	Revisado/Aprovado	CGPDP

ANEXO I - FORMULÁRIO DE REGISTRO E AVALIAÇÃO DE INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS
1 Notificador: (nome/contato)
2 Incidente de segurança com dados pessoais (descrever brevemente):
3 Quando o incidente ocorreu? (Data/hora)
4 Quando a organização teve ciência do incidente de segurança?
5 Qual a natureza dos dados afetados?
☐ Origem racial ou étnica ☐ Convicção religiosa. ☐ Opinião política. ☐ Filiação Sindical. ☐ Filiação a organização de caráter regioso, filosófico ou político. ☐ Dado referente à saúde. ☐ Dado referente à vida sexual.

	☐ Dado genético ou biométrico. ☐ Dado de Comprovação de identificação oficial (RG, CPF, CNH). ☐ Dado financeiro. ☐ Nomes de usuário ou senhas de sistemas de informação. ☐ Dado de geolocalização. ☐ Dado de criança ou adolescente. ☐ Dado relacionado a consumo. ☐ Dado relacionado a crédito pessoal. ☐ Outros
6	Os dados pessoais afetados no incidente, podem impedir ou dificultar alguma garantia ou direito fundamental do indivíduo?
	☐ sim ☐ não. ☐ não sei.
7	Qual a categoria dos titulares afetados?
	☐ servidores públicos. ☐ Contratados. ☐ Alunos ☐ Crianças e adolescentes ☐ Outros

8	Qual a quantidade de titulares afetados?
9	Classificação da categoria de violação de segurança:
	☐ Material: quando o incidente envolve dados armazenados em dispositivos físicos. Exemplos: perda de portadores de dados (pen drives/cd), pastas de arquivos, processos ou documentos perdidos, smartphones perdidos, etc. ☐ Ciberespaço: quando o incidente está relacionado à Tecnologia da Informação. Nessa categoria enquadram-se o hackeamento, mau gerenciamento de patches, codificação incorreta, medidas de segurança insuficientes, etc. ☐ Pessoal: atitude humana onde houve falha ao manusear o sistema, ao inserir documentos, e divulgar sem as devidas anonimizações; ou violação verbal, quando há vazamento de dados de forma verbal, seja por indiscrição (comentários acerca de dados pessoais que são percebidos por terceiros e utilizados em má-fé) ou de forma intencional, repassando indevidamente informações sigilosas.
10	Avaliação da criticidade de segurança:
	☐ Risco Baixo: classificação utilizada quando o incidente de segurança de dados afetar apenas dados pessoais, não incluído o número do CPF; ☐ Risco Moderado: classificação utilizada quando o incidente de segurança de dados afetar dados pessoais, incluído o número do CPF, e/ou pelo menos um dado sensível, não incluído raça, religião, nome social e dados de saúde; ☐ Risco Alto: classificação utilizada quando o incidente de segurança de dados afetar dados pessoais, incluído o número do CPF e/ou mais que um dado sensível, incluindo raça, religião, nome social e dados de saúde.

11 - Consequências concretas e prováveis que o incidente poderá trazer ao Titular de dados: (Descrever:)
Resultado da Avaliação do Incidente
Considerando as respostas anteriores, o Controlador deve responder a seguinte questão: Existe um risco ou dano relevante aos direitos e liberdades individuais dos titulares afetados em razão do incidente de segurança? ☐ Sim – Comunique à ANPD e ao titular. Preencher o Formulário de comunicação de incidente de segurança com dados pessoais à Autoridade Nacional de Proteção de Dados (ANPD) ☐ Não – A comunicação à ANPD não será necessária. O Controlador pode demonstrar à ANPD, se for o caso, de forma irrefutável, que a violação da segurança dos dados pessoais não constituiu um risco relevante para os direitos e liberdades do titular dos dados .
Guarapuava, _____de _____de 20xx Assinatura do Encarregado Assinatura do Controlador