**** Publicada no DOETC/MS nº 3955, de 22 de janeiro de 2025, página 2.***

INSTRUÇÃO NORMATIVA TCE-MS Nº 44, DE 21 DE JANEIRO DE 2025.

Dispõe sobre o Plano de Resposta a Incidentes de Segurança da informação com Dados Pessoais no âmbito do Tribunal de Contas do Estado de Mato Grosso do Sul.

O PRESIDENTE DO TRIBUNAL DE CONTAS DO ESTADO DE MATO GROSSO DO SUL, no uso das atribuições que lhe são conferidas pelo artigo 74, III, e § 1º, V, do Regimento Interno, aprovado pela Resolução TCE-MS nº 98, de 05 de dezembro de 2018;

Considerando a necessidade de adequação à Lei Geral de Proteção de Dados Pessoais (Lei Federal n. 13.709/2018) e a importância da proteção dos dados pessoais no âmbito do TCE-MS;

Considerando a relevância de estabelecer diretrizes claras e procedimentos eficazes para a resposta a incidentes de segurança que envolvam dados pessoais, visando à proteção dos direitos dos titulares de dados pessoais no âmbito do TCE-MS;

RESOLVE:

Art. 1º Aprovar o Plano de Resposta a Incidentes de Segurança da Informação com Dados Pessoais à Autoridade Nacional de Proteção de Dados -ANPD e aos Titulares de Dados Pessoais, conforme o Anexo I;

Art. 2º A implementação do Plano de Resposta a Incidentes de Segurança com Dados Pessoais deverá ser acompanhada e monitorada pelo Encarregado pelo Tratamento de Dados Pessoais, Núcleo de Gestão de Incidentes e com a colaboração de todas as áreas do TCE-MS;

Art. 3º Esta Instrução Normativa entra em vigor na data de sua publicação.

Campo Grande, 21 de janeiro de 2025.

Conselheiro Jerson Domingos
Presidente

LGPD - Lei Geral de Proteção de Dados

Plano de Resposta a Incidentes de Segurança da Informação e Dados Pessoais

do Tribunal de Contas do Estado de Mato Grosso do Sul

Edição 2025

Comitê de Segurança da Informação

TRIBUNAL DE CONTAS
Estado de Mato Grosso do Sul

Expediente

Rovena Ceccon
Coordenadora - CSI

Ana Carla L. Brum de Oliveira
Encarregada de Dados

Geanlucas Júlio de Freitas
Membro

Jonathan Aldori A. de Oliveira
Membro

Rafaela Guedes A. Tamiozzo
Membro

Viviane Lacerda L. Nogueira
Membro

Washington Schaustz
Membro

Revisão
Departamento de Normas
Tércio W. Albuquerque
Thais Xavier F. da Costa

Criação
Secretaria de Comunicação

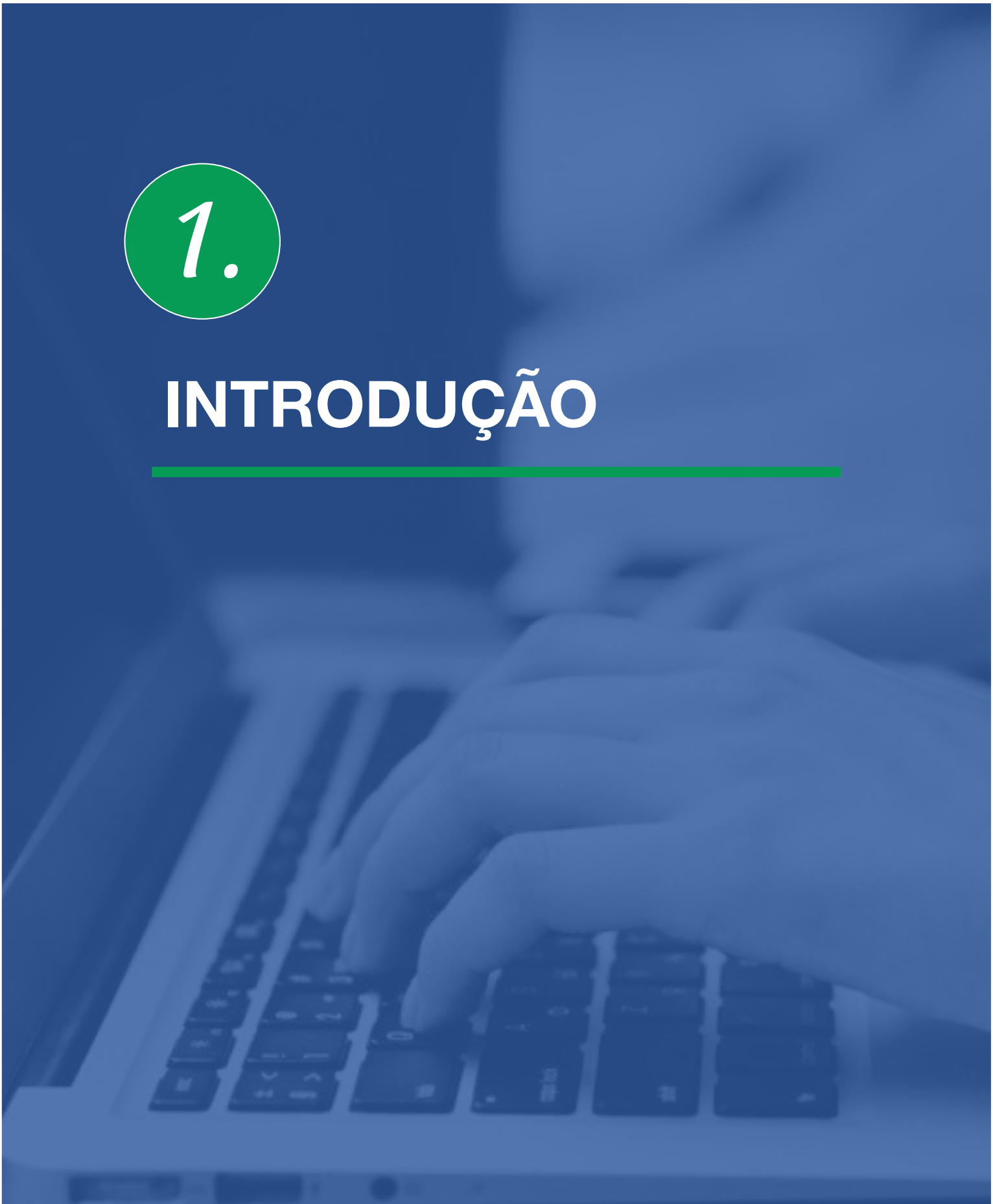
Comitê de Segurança da Informação

TRIBUNAL DE CONTAS
Estado de Mato Grosso do Sul

Sumário

1.

INTRODUÇÃO



Introdução

Este **Plano de Resposta a Incidentes de Segurança com Dados Pessoais e Informações** foi elaborado com base no guia utilizado pelo Governo Federal, constituindo-se como um complemento aos demais planos da Política de Segurança da Informação e Comunicação (POSIC).

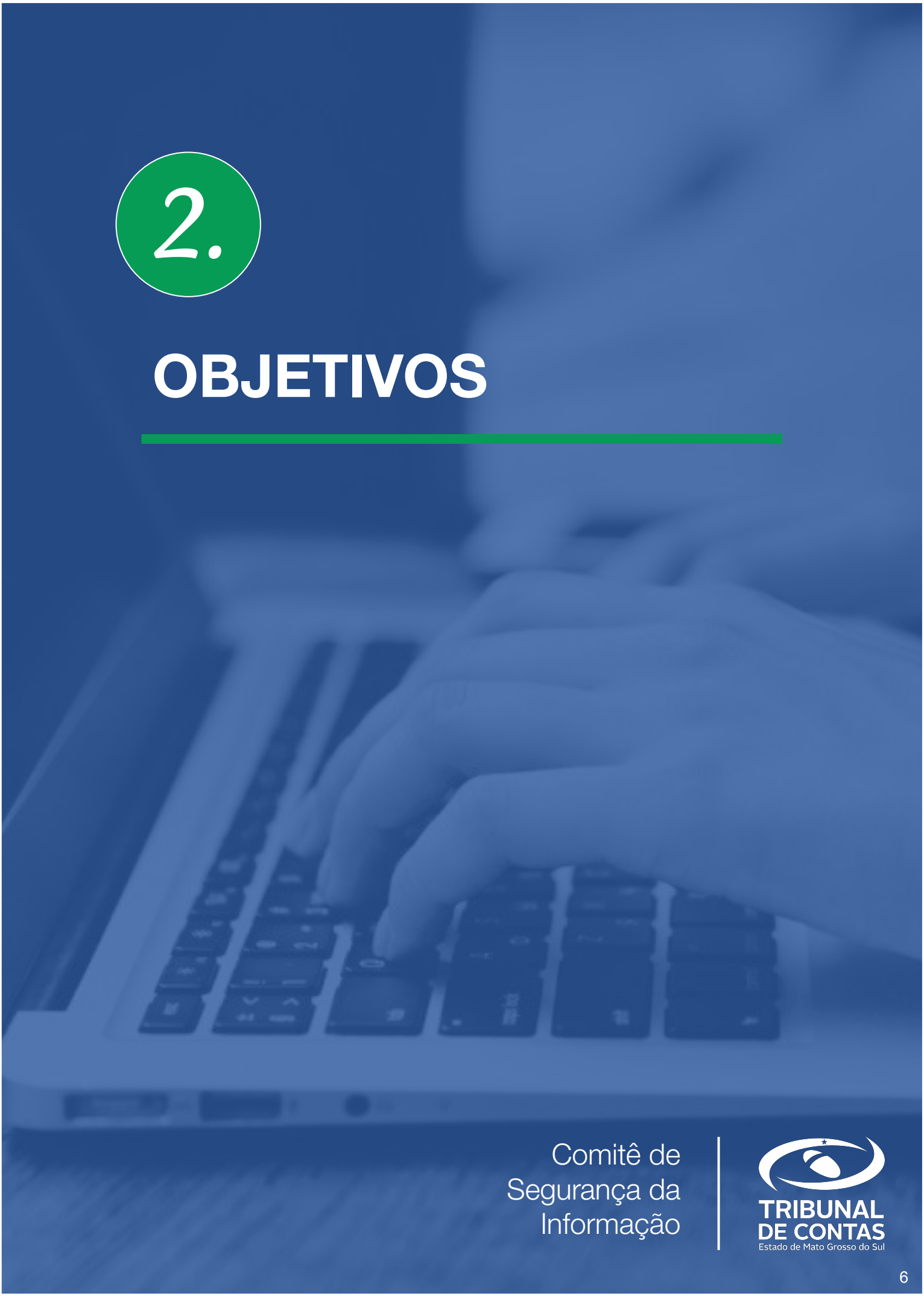
O propósito do presente documento é trazer uma visão macro sobre resposta a incidentes de segurança específicos do Tribunal, para fomentar a adequação à Lei Geral de Proteção de Dados Pessoais (LGPD).

O plano dispõe de medidas que devem ser adotadas no caso de uma situação de emergência ou evento de risco que possa ocasionar danos aos ativos tecnológicos do Tribunal, viabilizando, inclusive, a comunicação apropriada e tempestiva à Autoridade Nacional de Proteção de Dados (ANPD), quando for o caso.

Este plano será atualizado pelo Núcleo de Gestão de Incidentes (NGI), continuamente para incorporar melhorias, à medida que forem publicadas novas normas e que os processos de proteção de dados existentes sejam amadurecidos no contexto desta Corte.

Neste sentido, o presente Plano de Resposta a Incidentes de Segurança da Informação e Dados Pessoais, em conformidade com o que dispõe a Resolução CD/ANPD nº 15/2024 e Resolução TCE/MS nº 200/2023, é apresentado para conhecimento de todos os servidores, prestadores de serviços e colaboradores do TCE/MS, objetivando, também viabilizar a comunicação oportuna, tempestiva à ANPD, quando e se for o caso.

2. OBJETIVOS



Objetivos

Objetivo geral

Orientar os setores do Tribunal de Contas de Mato Grosso do Sul em como responder às situações de emergência 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.

Objetivos específicos

- Conferir clareza sobre o fluxo de procedimentos adequados e responsáveis no caso de incidentes;
- Adequar as condutas internas às diretrizes estabelecidas pela LGPD;
- Preservar a reputação e imagem do Tribunal;
- Assegurar respostas rápidas, efetivas e coordenadas para evitar maiores danos ao titular de dados e ao Tribunal ;
- Quantificar e monitorar desempenho;
- Evoluir continuamente com as lições aprendidas;
- Tornar o Tribunal referência em proteção de dados pessoais e segurança da informação.

3.

DEFINIÇÕES GERAIS

Definições Gerais

Para auxílio na leitura deste plano, serão adotadas as seguintes definições no que se refere a incidentes ocorridos no âmbito do TCE-MS:

Agentes de Tratamento

Os agentes de tratamento são o controlador (pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais) e o operador (pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador e de acordo com suas instruções).

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).

Dado Pessoal

É toda informação relacionada à pessoa natural identificada ou identificável.

Dado Pessoal Sensível

Dado pessoal sobre 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.

Encarregado - DPO

Também conhecido como DPO (*Data Protection Officer*), é a pessoa indicada pelo controlador para atuar como canal de comunicação com os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Definições Gerais

Incidente de Segurança

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

Autoridade Nacional de Proteção de Dados - ANPD

Os arts. 55-A e seguintes da LGPD cria a Autoridade Nacional de Proteção de Dados (ANPD) e seus Conselhos Deliberativos e conforme as atribuições descritas no art. 55-J da LGPD e no Decreto nº 10.474, de 26 de agosto de 2020 define as competências da ANPD como entidade responsável por zelar, implementar e fiscalizar o cumprimento da Lei Federal - LGPD.

Inventário de Dados - IDP / Registro de Operações de Processos Administrativos - ROPA

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

Relatório de Impacto de Proteção de Dados - 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 risco.

Relatório final

Relatório que contém todas as evidências e ações realizadas para tratamento do incidente e que deve ser emitido ao final das tratativas e encaminhado à ANPD.

Incidente de Segurança

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

Definições Gerais

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.

Comitê Gestor de Proteção de Dados - COGPD

O Comitê Gestor de Proteção de Dados Pessoais (COGPD), é um órgão colegiado de natureza consultiva, deliberativa, de caráter permanente, e vinculado à Presidência do TCE-MS com atribuições de cunho estratégico, com o objetivo de promover a implementação das disposições da Lei Federal nº 13.709/2018 - LGPD disposto pela Resolução TCE/MS nº 200/2023.

Incidente de segurança com dados pessoais

Incidente de segurança à proteção de dados pessoais é 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.

Lei Geral de Proteção de Dados - LGPD

A Lei Geral de Proteção de Dados Pessoais – LGPD (Lei Federal nº. 13.709, de 2018) dispõe sobre o tratamento de dados pessoais das pessoas naturais, definindo as hipóteses em que tais dados podem legitimamente ser utilizados por terceiros e estabelecendo mecanismos para proteger os titulares dos dados contra usos inadequados.

Definições Gerais

Comitê de Segurança da Informação - CSI

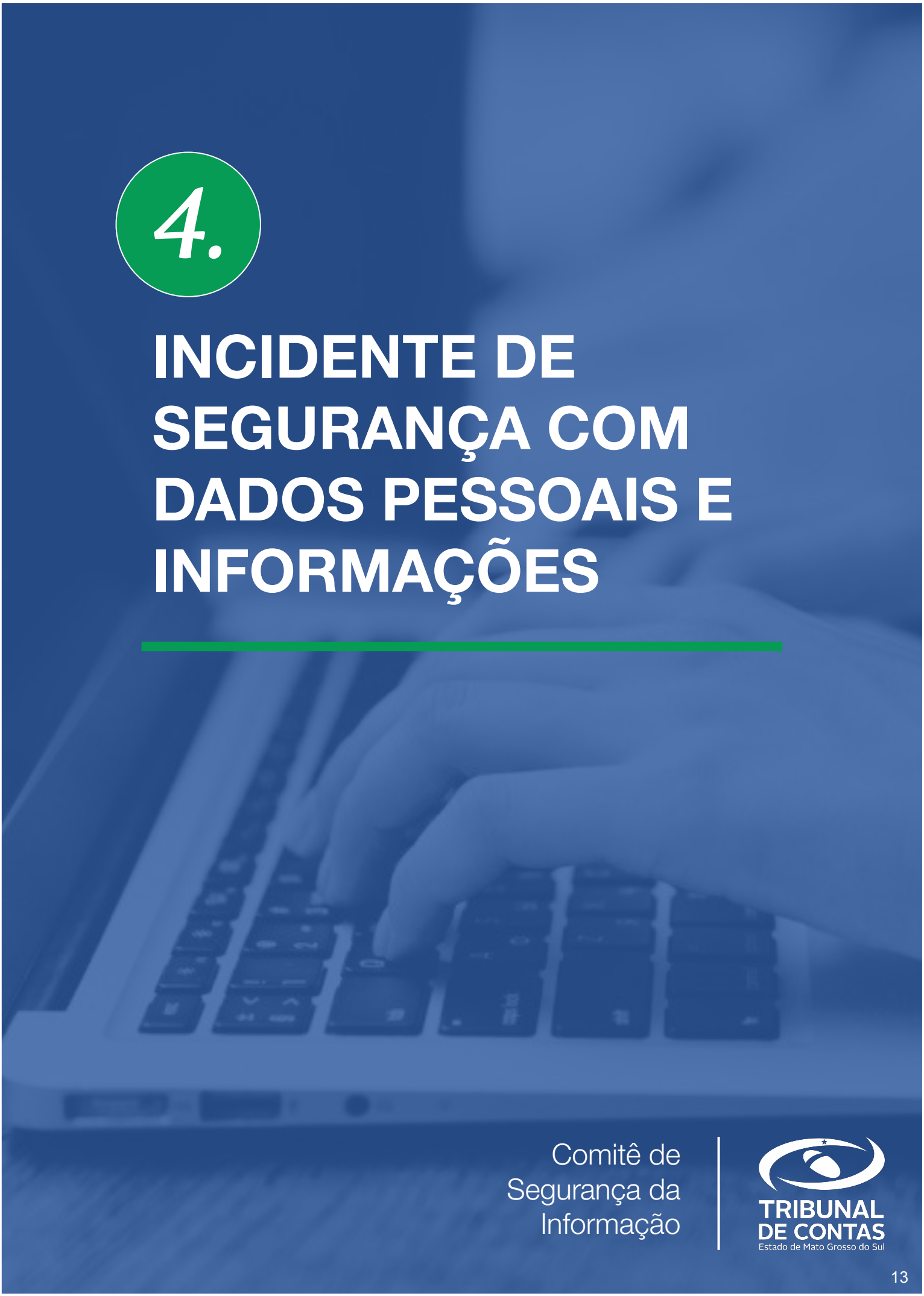
O Comitê de Segurança da Informação (CSI), tem por finalidade formular e conduzir diretrizes para a Política Corporativa de Segurança da Informação do Tribunal de Contas de Mato Grosso do Sul (PCSI/TCE/MS), analisar periodicamente sua efetividade, propor normas e mecanismos institucionais para melhoria contínua, bem como assessorar, em matérias correlatas, a Presidência do Tribunal de Contas de MS em conformidade com a Resolução Administrativa TC/MS N° 100, de 18 de novembro de 2009.

Núcleo de Gestão a Incidentes - NGI

O Núcleo de Gestão a Incidentes é composto por: Encarregado, CSI, COGPD, Presidência e DTI. Têm por finalidade elaborar o Plano de resposta a incidentes de segurança (PRIS), sendo convocado sempre que houver casos de incidente que coloque em risco a segurança de dados pessoais e informações.

4.

INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS E INFORMAÇÕES



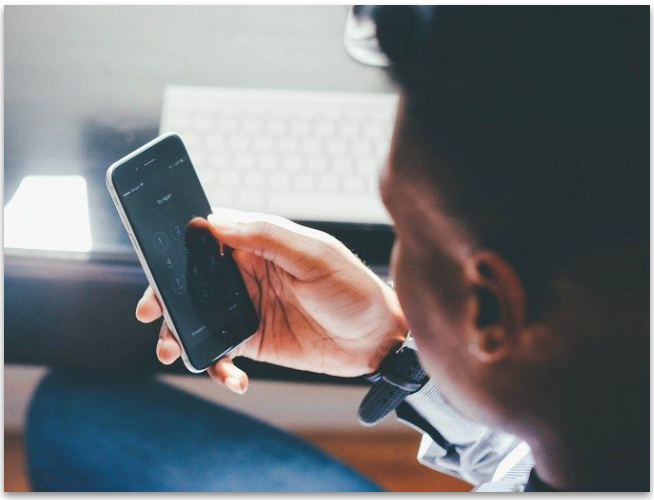
Comitê de Segurança da Informação

TRIBUNAL DE CONTAS
Estado de Mato Grosso do Sul

Incidente de Segurança com Dados Pessoais e Informações

Conforme estabelecido no artigo 46 da LGPD, os agentes de tratamento devem adotar medidas de segurança para proteger os dados pessoais desde a concepção até a sua execução.

Ainda, o artigo 50 do referido normativo estabelece que controladores e operadores poderão formular regras de boas práticas e de governança para o tratamento de dados pessoais, podendo ser implementado um programa de governança e privacidade que conte com plano de resposta a incidentes e remediações.



Imagens ilustrativas

Incidente de Segurança com Dados Pessoais e Informações

Em caso de incidente que coloque em risco a segurança de dados pessoais e informações devem ser realizados alguns procedimentos específicos:

4.1 AVALIAR INTERNAMENTE O INCIDENTE

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

A) Origem;
B) Categoria;
C) Quantidade de titulares e de dados pessoais afetados, quando houver;
D) Categoria e quantidade de dados afetados; consequências do incidente para os titulares e para a entidade;
E) Criticidade;
F) Analisar se houve vazamento de dados pessoais e dados sensíveis e,
G) Além disso, é necessário preservar todas as evidências do incidente em relatório específico do órgão.

Incidente de Segurança com Dados Pessoais e Informações

4.2 COMUNICAR O CONTROLADOR

Comunicar o Controlador sobre o incidente para que este tome as devidas providências.

O Encarregado de Dados deve também ser comunicado sobre o ocorrido para que haja os comunicados oficiais às autoridades conforme previsão na LGPD e Resolução TCE - MS nº 200/2023.

4.3 CONSULTAR O NGI

Consultar o grupo de trabalho interno do TCE - MS em caso de incidentes na rede computacional. O CSI deve dar ciência aos gestores das áreas afetadas.

4.4 COMUNICAR A TODOS OS ENVOLVIDOS

Comunicar a todos os envolvidos a existência do incidente, nos termos da LGPD, através do Encarregado de dados.

4.5 COMUNICAR À ANPD

O DPO/Encarregado de Dados comunicará a ANPD e ao titular de dados pessoais (conforme art. 48 da LGPD) a existência do incidente e encaminhará o relatório inicial subsidiado pelo NGI.

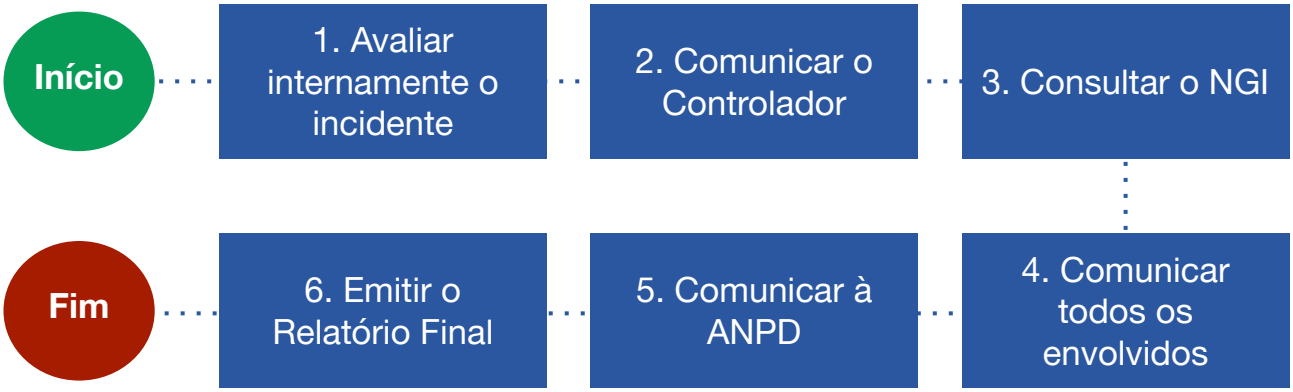
Incidente de Segurança com Dados Pessoais e Informações

4.6 EMITIR O RELATÓRIO FINAL

O NGI emitirá o relatório final contendo os tipos de dados e a quantidade de titulares afetados para o Controlador.

Deve também acompanhar um relatório técnico de tratamento que permita avaliar a extensão e adequação de medidas para incidentes futuros.

A FIGURA A SEGUIR APRESENTA DE MANEIRA SIMPLIFICADA ESTE PROCESSO:

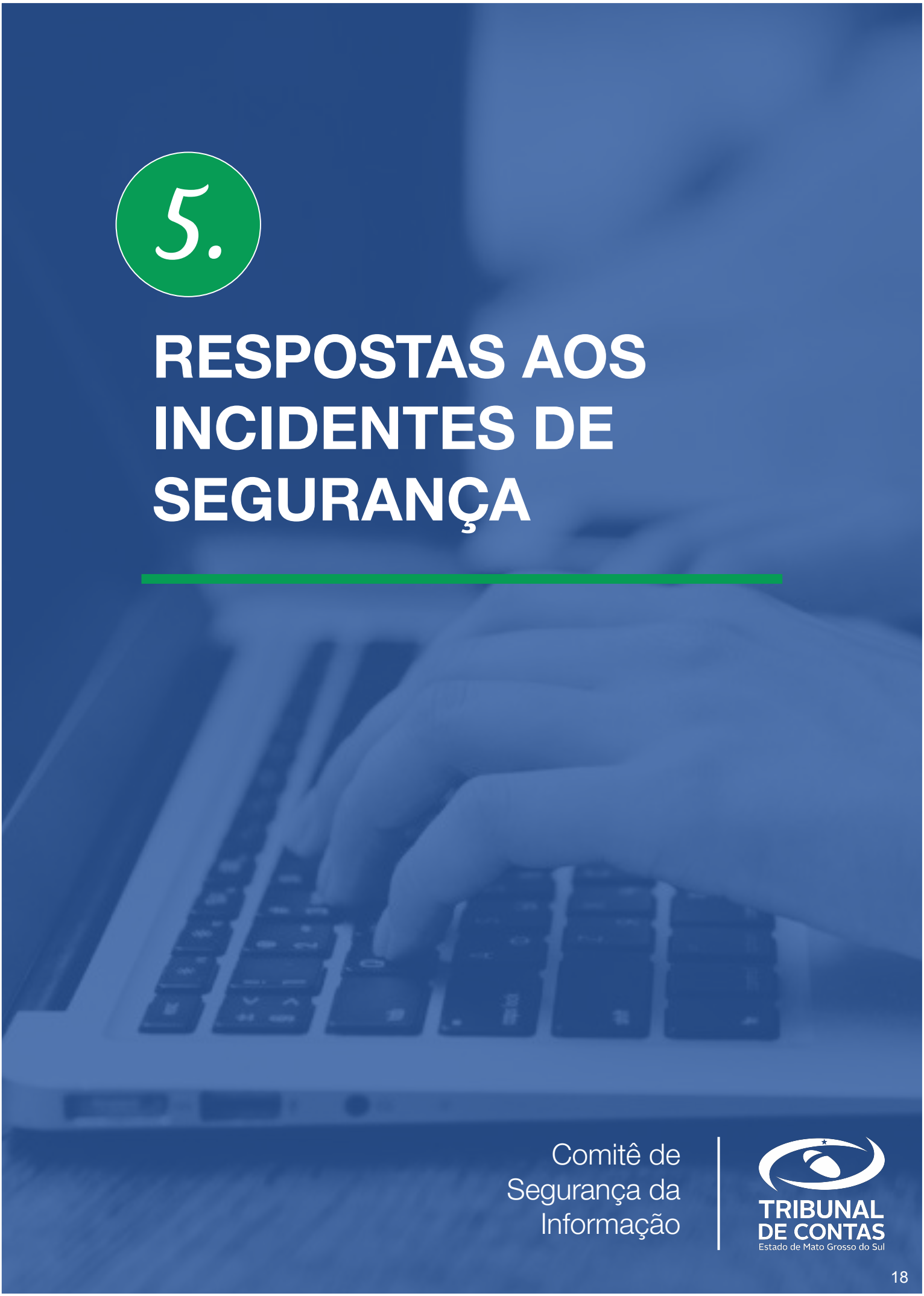


ATENÇÃO!

O artigo 48 da LGPD afirma que, em caso de incidente de segurança, que venha a gerar risco ou dano considerado relevante aos titulares, o controlador tem a obrigação de comunicar por meio do Encarregado de Dados à ANPD e ao titular dos dados pessoais. O prazo que a ANPD recomenda para essa comunicação é de 3 (três) dias úteis à contar da data da ciência do incidente, conforme dispõe a Resolução CD/ANPD nº 15/2024.

5.

RESPOSTAS AOS INCIDENTES DE SEGURANÇA



Comitê de Segurança da Informação

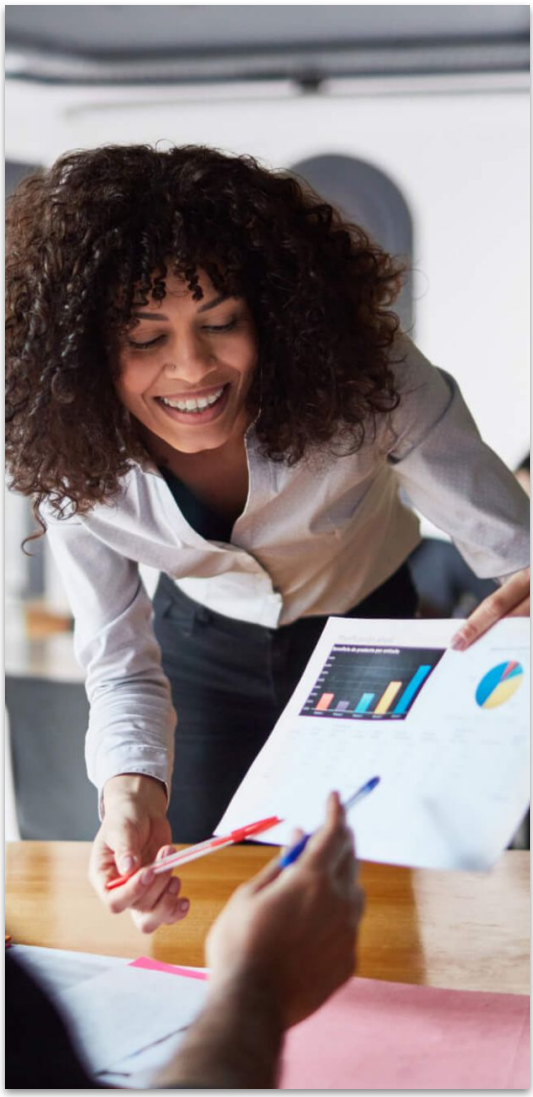
TRIBUNAL DE CONTAS
Estado de Mato Grosso do Sul

Respostas aos Incidentes de Segurança

O Tribunal vai dar respostas aos seus incidentes utilizando as orientações do plano de resposta a incidentes de segurança e as fases descritas abaixo utilizando o fluxo detalhado e o *checklist* no final deste documento.

5.1 PREPARAÇÃO/NOTIFICAÇÃO

Esta fase é de suma importância, pois estabelece a capacidade de resposta para que o Tribunal esteja pronto para responder a incidentes, como também a evitá-los e garantir que sistemas, redes e aplicativos sejam suficientemente seguros. Na fase de preparação e notificação o DPO, CSI, COGPD, Presidência e DTI 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 Tribunal. Assim que o órgão for notificado será iniciada uma avaliação mais detalhada do incidente pelo DPO, CSI e DTI, que farão a classificação e definirão a sua criticidade.

Respostas aos Incidentes de Segurança

5.3 CONTENÇÃO, ERRADICAÇÃO E RECUPERAÇÃO

Os responsáveis pelos sistemas/processos impactados 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.

Aqui, 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.

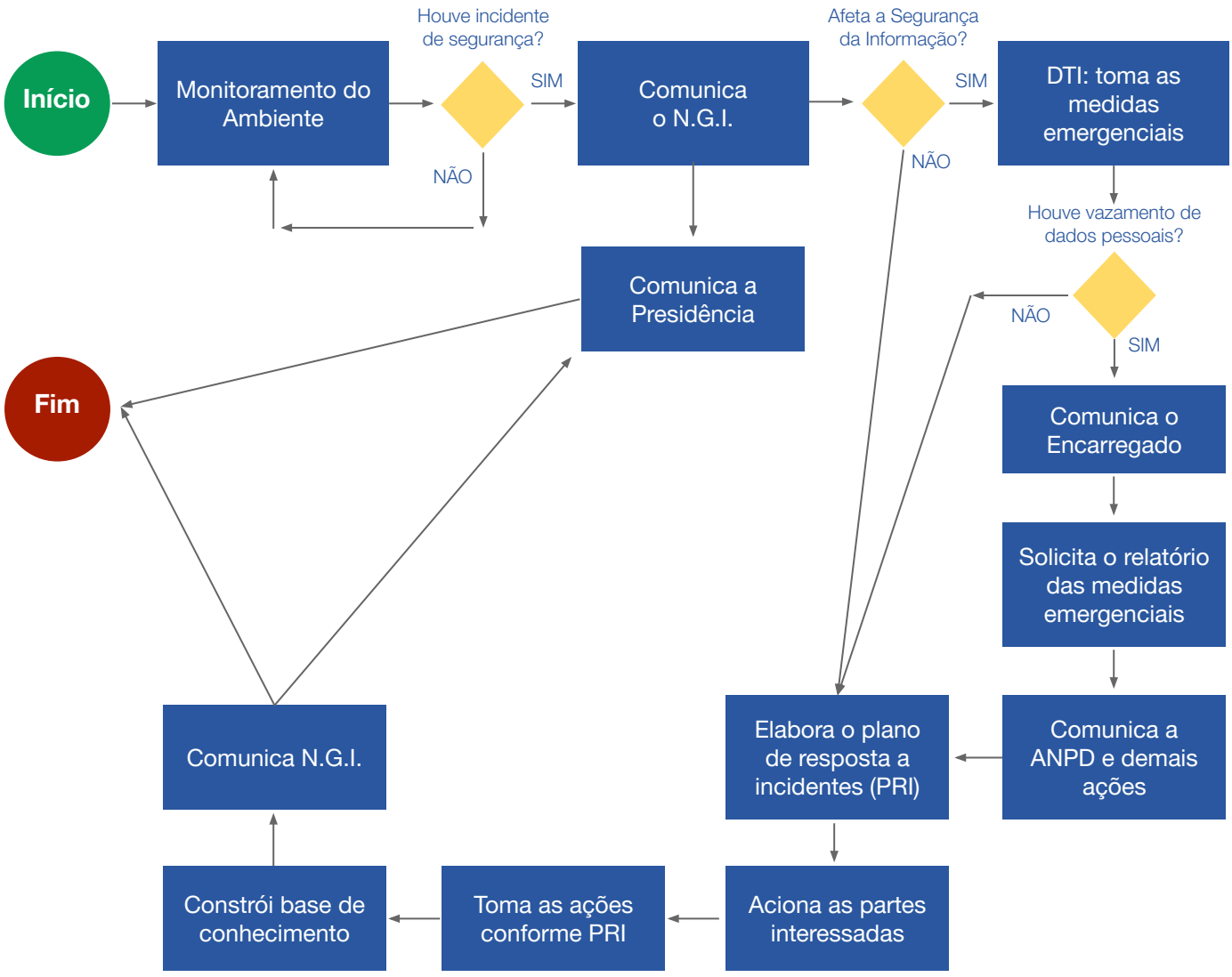
Todos os cuidados devem ser adotados para não impactar evidências que poderiam ser usadas para identificar autoria, origem e método usado para quebrar a segurança.

Respostas aos Incidentes de Segurança

5.4 ATIVIDADES PÓS-INCIDENTE

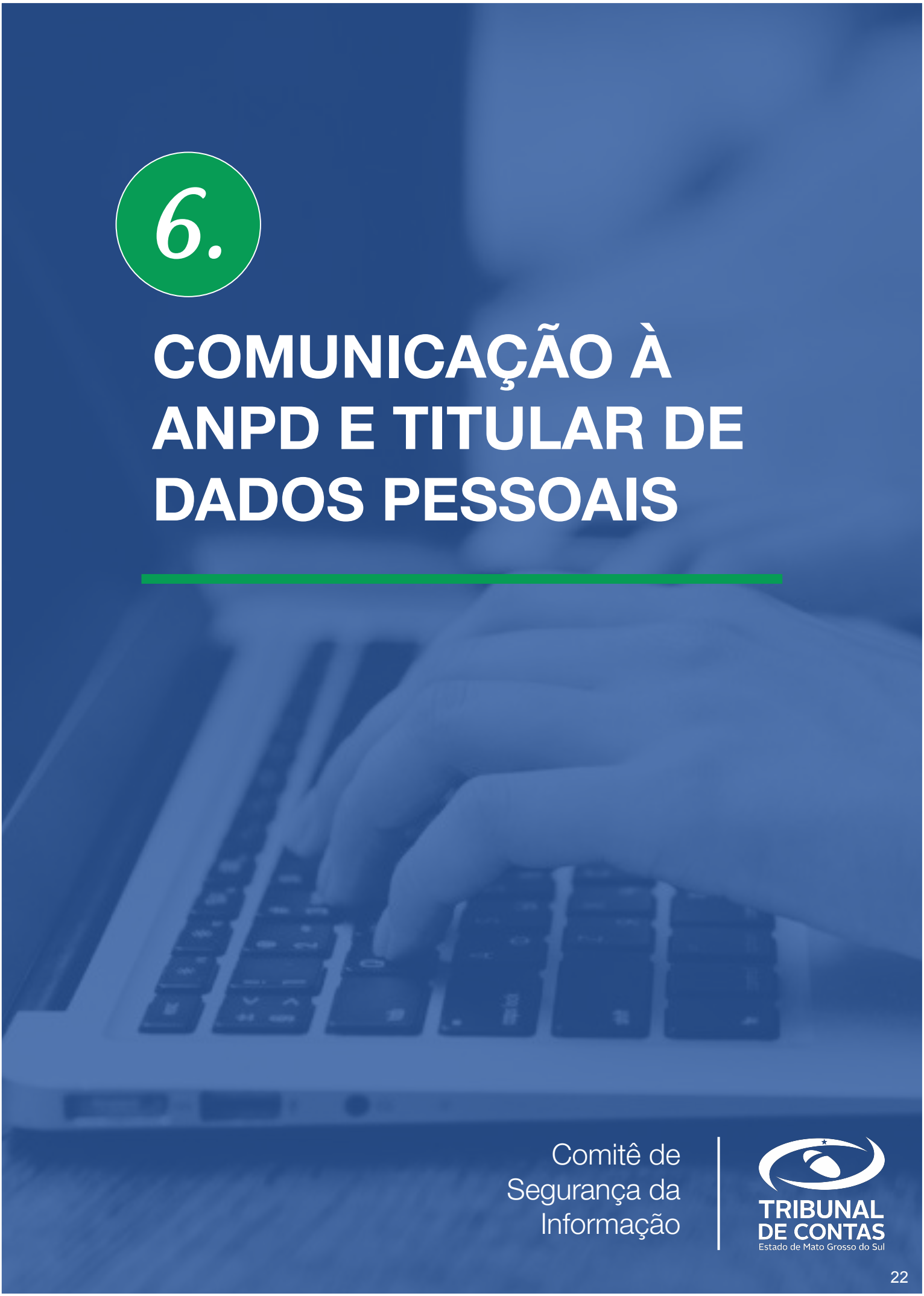
Na fase de atividades pós-incidente, serão implementadas algumas atividades em busca da melhoria contínua de seus processos de resposta a incidentes, além de definir procedimentos para retenção de evidências e uso dos dados coletados em incidentes.

ABAIXO O FLUXO COMPLETO PARA RESPOSTAS A INCIDENTES



6.

COMUNICAÇÃO À ANPD E TITULAR DE DADOS PESSOAIS



Comitê de Segurança da Informação

TRIBUNAL DE CONTAS
Estado de Mato Grosso do Sul

Comunicação à ANPD e Titular de Dados Pessoais

A comunicação à ANPD e ao Titular dos Dados será realizada por intermédio do Encarregado de Dados, designado pelo Tribunal.

A ANPD disponibiliza um Formulário de Comunicação de Incidente de Segurança com dados pessoais, conforme anexo.

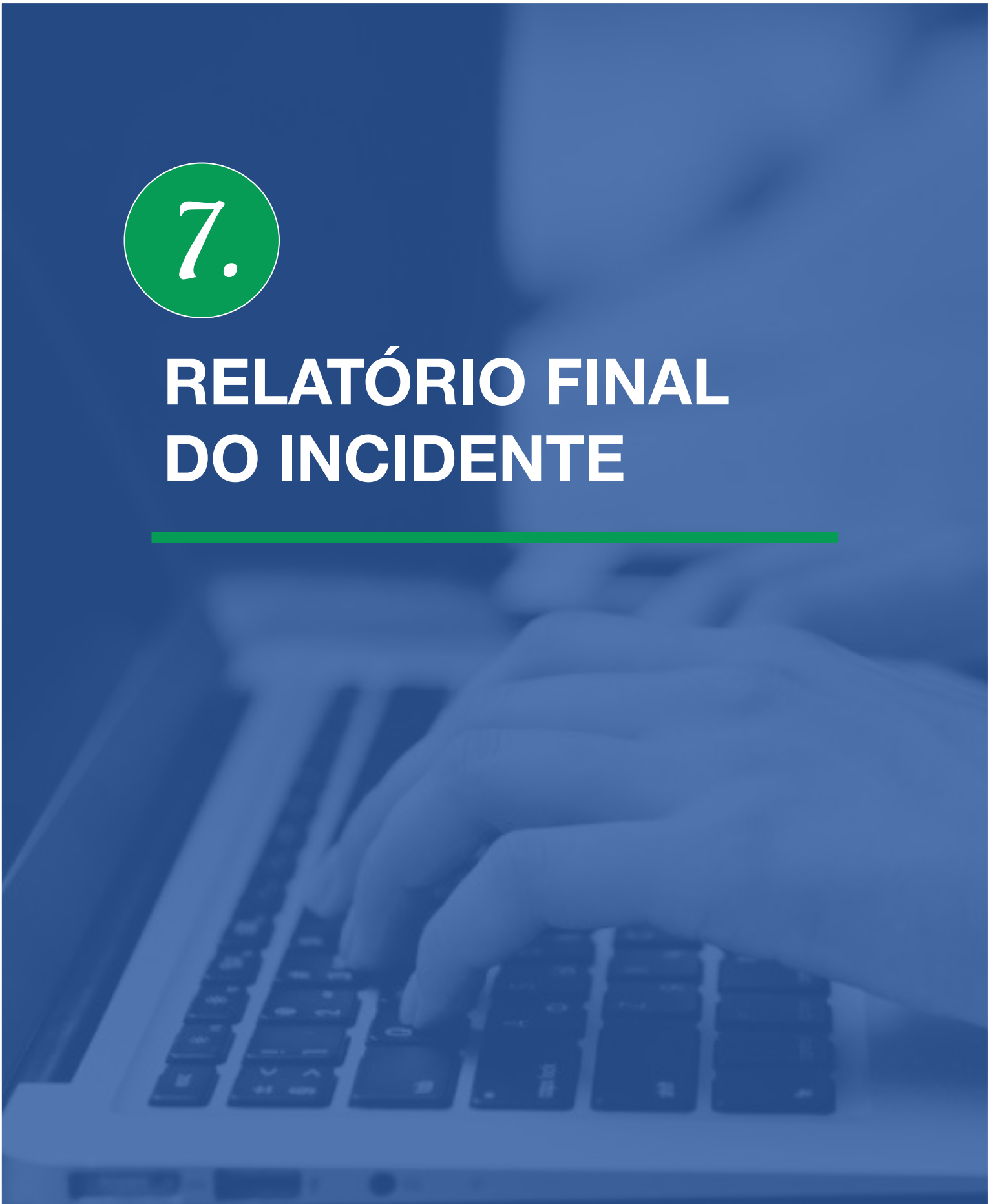
A comunicação ocorre pelo encaminhamento do documento pelo sistema eletrônico do Governo Federal, disponível no link: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis/formulario_cis_anpd1.docx

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 notificação 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.

O Controlador, com o apoio do Encarregado de Dados e GTI, deverá avaliar o risco no âmbito interno, com objetivo de estipular se há ou não risco ou dano relevante para a comunicação do incidente ao titular, sendo necessário a justificativa para os casos em que se decidir por não comunicar o incidente.

7.

RELATÓRIO FINAL DO INCIDENTE



Comitê de Segurança da Informação

TRIBUNAL DE CONTAS
Estado de Mato Grosso do Sul

Relatório Final do Incidente

Após a coleta de todas as informações e evidências, o Encarregado de Dados com o apoio do NGI, 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 pela DTI frente às autoridades, é importante para que todos os envolvidos e demais servidores 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 Controlador e pelo Encarregado de Dados e deve ficar disponível para consulta em caso de atualização do relatório de impacto à proteção de dados (RIPD). Esse relatório poderá, ainda, ser apresentado a autoridades policiais, órgãos reguladores ou demais envolvidos.

8.

CHECKLIST
para verificação do Tratamento de Incidentes

Comitê de Segurança da Informação

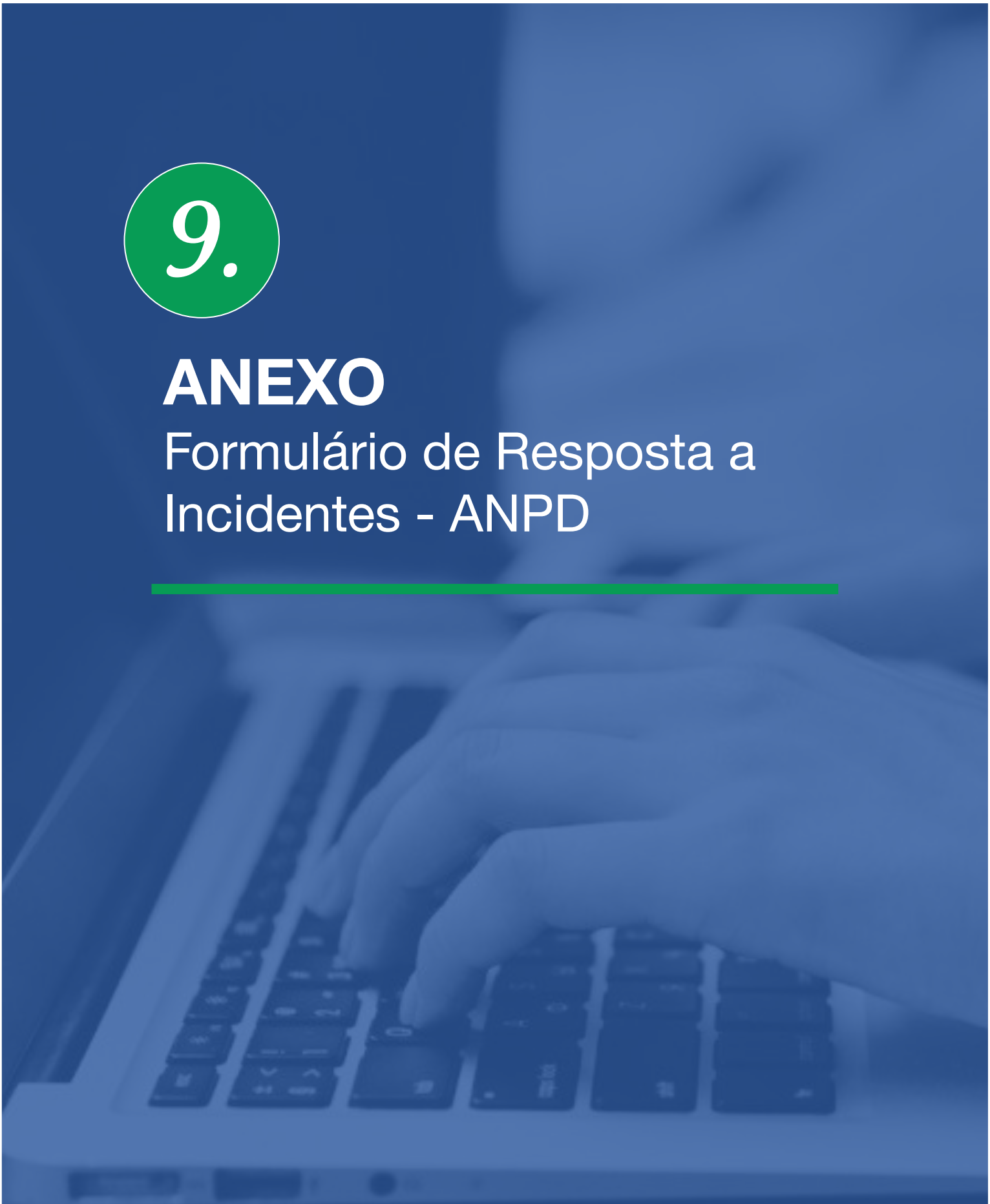
TRIBUNAL DE CONTAS
Estado de Mato Grosso do Sul

	AÇÃO	REALIZADO?
	Detecção e Análise	
1	Determinar se ocorreu um incidente	
1.1	Analisar os precursores e os indicadores	
1.2	Buscar por informações correlatas	
1.3	Realizar pesquisa do incidente (via mecanismos de busca bases de conhecimento)	
1.4	Documentar, investigar e reunir as evidências assim que a equipe identificar a ocorrência do incidente	
2	Priorizar o tratamento com base em sua relevância (impacto de negócio, impacto de informação e recuperabilidade)	
3	Comunicar o incidente às equipes internas envolvidas e, quando necessário, aos atores externos	
	Contenção, erradicação e recuperação	
4	Coletar, preservar, proteger e documentar as evidências	
5	Conter o incidente	
6	Erradicar o incidente	
6.1	Identificar e mitigar todas as vulnerabilidades exploradas	
6.2	Remover malware, materiais impróprios e outros componentes	
6.3	Se mais hosts afetados forem descobertos (por exemplo, novas infecções por malware), repetir as etapas de detecção e análise (1.1, 1.2) para identificar todos os outros hosts afetados, para então conter (5) e erradicar (6) o incidente em tais hosts	
7	Recuperar-se do incidente	
7.1	Retornar os sistemas afetados ao estado operacional	
7.2	Confirmar se os sistemas afetados estão funcionando normalmente	
7.3	Se necessário, implementar monitoração adicional para encontrar futuras atividades relacionadas	
	Atividades pós-incidente	
8	Criar o relatório de acompanhamento	
9	Realizar uma reunião de lições aprendidas (tal reunião é obrigatória para incidentes graves e opcional para os demais incidentes)	

9.

ANEXO

Formulário de Resposta a Incidentes - ANPD



Comitê de Segurança da Informação

TRIBUNAL DE CONTAS
Estado de Mato Grosso do Sul

ANEXO
Formulário de Resposta a Incidentes - ANPD

Dados do Controlador			
Razão Social / Nome:			
CNPJ/CPF:			
Endereço:			
Cidade:		Estado:	
CEP:			
Telefone:		E-mail:	
Declara ser Microempresa ou Empresa de Pequeno Porte:		☐ Sim	☐ Não
Declara ser Agente de Tratamento de Pequeno Porte:		☐ Sim	☐ Não
Informe o número aproximado de titulares cujos dados são tratados por sua organização:			

Dados do Encarregado			
Possui um encarregado pela proteção de dados pessoais?		☐ Sim	☐ Não
Nome:			
CNPJ/CPF:			
Telefone:		E-mail:	

Dados do Notificante / Representante Legal	
☐ O próprio encarregado pela proteção de dados.	
☐ Outros (especifique):	
Nome:	
CNPJ/CPF:	
Telefone:	
E-mail:	

A documentação comprobatória da legitimidade para representação do controlador junto à ANPD deve ser protocolada em conjunto com o formulário de comunicação de incidente.

- *Encarregado*: ato de designação/nomeação/procuração
- *Representante*: contrato social e procuração, se cabível.

Tipo de Comunicação	
☐ Completa	*Todas as informações a respeito do incidente estão disponíveis e* ***a comunicação aos titulares já foi realizada****.*
☐ Preliminar	*Nem todas as informações sobre o incidente estão disponíveis, justificadamente, ou a* ***comunicação aos titulares ainda não foi realizada****.* *A complementação deverá ser encaminhada no prazo de* ***20 dias úteis*** *a contar da data da comunicação* – Art. 6º § 3º do Regulamento de Comunicação de Incidentes.
☐ Complementar	*Complementação de informações prestadas em comunicação preliminar.*
A comunicação complementar deve ser protocolada no mesmo processo que a comunicação preliminar.	

A comunicação preliminar é insuficiente para o cumprimento da obrigação estabelecida pelo art. 48 da LGPD e deve ser complementada pelo controlador no prazo estabelecido.

ANEXO
Formulário de Resposta a Incidentes - ANPD

Avaliação do Risco do Incidente
☐ O incidente de segurança pode acarretar risco ou dano relevante aos titulares.
☐ O incidente não acarretou risco ou dano relevante aos titulares. **(Comunicação Complementar)**
☐ O risco do incidente aos titulares ainda está sendo apurado. **(Comunicação Preliminar)**
Justifique, se cabível, a avaliação do risco do incidente:

Da Ciência da Ocorrência do Incidente		
Por qual meio se tomou conhecimento do incidente?		
☐ Identificado pelo próprio controlador.	☐ Notificação do operador de dados.	☐ Denúncia de titulares/terceiros.
☐ Notícias ou redes sociais.	☐ Notificação da ANPD.	☐ Outros. (especifique)
Descreva, resumidamente, de que forma a ocorrência do incidente foi conhecida:		

Caso o incidente tenha sido comunicado ao controlador por um operador, informe:	
Dados do Operador	
Razão Social / Nome:	
CNPJ/CPF:	
E-mail:	

Cabe ao controlador solicitar ao operador as informações necessárias à comunicação do incidente.

Da Tempestividade da Comunicação do Incidente	
Informe as seguintes datas, sobre o incidente:	
Quando ocorreu	
Quando tomou ciência	
Quando comunicou à ANPD	
Quando comunicou aos titulares	
Justifique, se cabível, a não realização da comunicação à ANPD e aos titulares de dados afetados no prazo de 3 (três) dias úteis conforme prevê o Art. 6º da Resolução CD/ANPD nº 15, de 24 de abril de 2024 que aprova o Regulamento de Comunicação de Incidente de Segurança.	

Se cabível, informe quando e a quais outras autoridades o incidente foi comunicado:

ANEXO
Formulário de Resposta a Incidentes - ANPD

Da Comunicação do Incidente aos Titulares dos Dados

Os titulares dos dados afetados foram comunicados sobre o incidente?

☐ Sim.

☐ Não, mas o processo de comunicação está em andamento.

☐ Não, por não haver risco ou dano relevante a eles.

☐ Não, vez que o risco do incidente ainda está sendo apurado. (**comunicação preliminar**)

Se cabível, quando os titulares serão comunicados sobre o incidente?

De que forma a ocorrência do incidente foi comunicada aos titulares?

☐ Comunicado individual por escrito. *(mensagem eletrônica / carta / e-mail / etc.)*

☐ Comunicado individual por escrito com confirmação de recebimento. *(mensagem eletrônica / carta / e-mail / etc.)*

☐ Outros. (*especifique abaixo*)

☐ Anúncio público no sítio eletrônico, mídias sociais ou aplicativos do controlador.

☐ Ampla divulgação do fato em meios de comunicação, por iniciativa do controlador. (*especifique abaixo*)

☐ Não se aplica.

Descreva como ocorreu a comunicação:

Quantos titulares foram comunicados individualmente sobre o incidente?

Justifique, se cabível, o que motivou a não realização da comunicação individual aos titulares:

O comunicado aos titulares deve utilizar linguagem clara e conter, ao menos, as seguintes informações:

1. resumo e data de ocorrência do incidente;
2. descrição dos dados pessoais afetados;
3. riscos e consequências aos titulares de dados;
4. medidas tomadas e recomendadas para mitigar seus efeitos, se cabíveis;
5. dados de contato do controlador para obtenção de informações adicionais sobre o incidente.

O comunicado aos titulares atendeu os requisitos acima?

☐ Sim ☐ Não

- Se não atendidos os requisitos, o comunicado aos titulares deverá ser devidamente retificado.
- Poderá ser solicitada pela ANPD, a qualquer tempo, cópia do comunicado aos titulares para fins de fiscalização.

ANEXO
Formulário de Resposta a Incidentes - ANPD

Descrição do Incidente	
Qual o tipo de incidente? (Informe o tipo mais específico)	
☐ Sequestro de Dados (*ransomware*) sem transferência de informações.	☐ Sequestro de dados (*ransomware*) com transferência e/ou publicação de informações.
☐ Exploração de vulnerabilidade em sistemas de informação.	☐ Vírus de Computador / *Malware*.
☐ Roubo de credenciais / Engenharia Social.	☐ Violação de credencial por força bruta.
☐ Publicação não intencional de dados pessoais.	☐ Divulgação indevida de dados pessoais.
☐ Envio de dados a destinatário incorreto.	☐ Acesso não autorizado a sistemas de informação.
☐ Negação de Serviço (DoS).	☐ Alteração/exclusão não autorizada de dados.
☐ Perda/roubo de documentos ou dispositivos eletrônicos.	☐ Descarte incorreto de documentos ou dispositivos eletrônicos.
☐ Falha em equipamento (hardware).	☐ Falha em sistema de informação (*software*).
☐ Outro tipo de incidente cibernético. (especifique abaixo)	☐ Outro tipo de incidente não cibernético. (especifique abaixo)
Descreva, resumidamente, como ocorreu o incidente:	
Explique, resumidamente, por que o incidente ocorreu (identifique a causa raiz, se conhecida):	
Que medidas foram adotadas para corrigir as causas do incidente?	

ANEXO
Formulário de Resposta a Incidentes - ANPD

Impactos do Incidente Sobre os Dados Pessoais	
De que forma o incidente afetou os dados pessoais (admite mais de uma marcação):	
☐ Confidencialidade	Houve acesso não autorizado aos dados, violando seu sigilo.
☐ Integridade	Houve alteração ou destruição de dados de maneira não autorizada ou acidental.
☐ Disponibilidade	Houve perda ou dificuldade de acesso aos dados por período significativo.

Se aplicável, quais os tipos de dados pessoais sensíveis foram violados? (admite mais de uma marcação)

☐Origem racial ou étnica.	☐Convicção religiosa.	☐Opinião política.
☐Referente à saúde.	☐Biométrico.	☐Genético.
☐Referente à vida sexual.	☐Filiação a organização sindical, religiosa, filosófica ou política.	

Se aplicável, descreva os tipos de dados pessoais sensíveis violados:

☐ Dados básicos de identificação *(ex: nome, sobrenome, data de nascimento, matrícula)*	☐ Número de documentos de identificação oficial. *(ex: RG, CPF, CNH, passaporte)*	☐ Dados de contato. *(ex: telefone, endereço, e-mail)*
☐ Dados de meios de pagamento. *(ex: cartão de crédito/débito)*	☐ Cópias de documentos de identificação oficial.	☐ Dados protegidos por sigilo profissional/legal.
☐ Dado financeiro ou econômico.	☐ Nomes de usuário de sistemas de informação.	☐ Dado de autenticação de sistema. *(ex: senhas, PIN ou tokens)*
☐ Imagens / Áudio / Vídeo	☐ Dado de geolocalização. *(ex: coordenadas geográficas)*	☐ Outros (especifique abaixo)

Quais os demais tipos de dados pessoais violados? (admite mais de uma marcação)

Descreva os tipos de dados pessoais não sensíveis violados:

Riscos e Consequências aos Titulares dos Dados	
Foi elaborado um Relatório de Impacto à Proteção de Dados Pessoais (RIPD) das atividades de tratamento afetadas pelo incidente?	
☐ Sim	☐ Não

Qual o número total de titulares cujos dados são tratados nas atividades afetadas pelo incidente?

Qual a quantidade aproximada de titulares afetados pelo incidente?	
Total de titulares afetados	
Crianças e/ou adolescentes	
Outros titulares vulneráveis	

ANEXO
Formulário de Resposta a Incidentes - ANPD

Se aplicável, descreva as categorias de titulares vulneráveis afetados:

Quais a categorias de titulares foram afetadas pelo incidente? (admite mais de uma marcação)

☐ Funcionários.	☐Prestadores de serviços.	☐ Estudantes/ Alunos.
☐ Clientes/Cidadãos.	☐ Usuários.	☐ Inscritos/Filiados.
☐ Pacientes de serviço de saúde.	☐Ainda não identificadas.	☐ Outros. (especifique abaixo)

Informe o quantitativo de titulares afetados, por categoria:

Quais as prováveis consequências do incidente para os titulares? (admite mais de uma marcação)

☐ Danos morais.	☐ Danos materiais.	☐ Violação à integridade física
☐ Discriminação social.	☐ Danos reputacionais.	☐ Roubo de identidade.
☐ Engenharia social / Fraudes.	☐ Limitação de acesso a um serviço.	☐ Exposição de dados protegidos por sigilo profissional/legal.
☐ Restrições de direitos.	☐ Perda de acesso a dados pessoais.	☐ Outros (especifique abaixo).

Se cabível, descreva as prováveis consequências do incidente para cada grupo de titulares:

Qual o provável impacto do incidente sobre os titulares? (admite só uma marcação)

☐ Podem não sofrer danos, sofrer danos negligenciáveis ou superáveis sem dificuldade.

☐ Podem sofrer danos, superáveis com certa dificuldade.

☐ Podem sofrer danos importantes, superáveis com muita dificuldade.

☐ Podem sofrer lesão ou ofensa a direitos ou interesses difusos, coletivos ou individuais, que, dadas as circunstâncias, ocasionam ou tem potencial para ocasionar dano significativo ou irreversível.

Se cabível, quais medidas foram adotadas para mitigação dos riscos causados pelo incidente aos titulares?

ANEXO
Formulário de Resposta a Incidentes - ANPD

Medidas de Segurança Técnicas e Administrativas para a Proteção dos Dados Pessoais

Os dados violados estavam protegidos de forma a impossibilitar a identificação de seus titulares?

☐ Sim, integralmente protegidos por criptografia / pseudonimização. ☐ Sim, parcialmente protegidos por criptografia / pseudonimização. ☐ Não.

Descreva os meios utilizados para proteger a identidade dos titulares, e a quais tipos dados foram aplicados:

Antes do incidente, quais das seguintes medidas de segurança eram adotadas? (admite mais de uma marcação)

☐ Políticas de segurança da informação e privacidade.	☐ Processo de Gestão de Riscos.	☐ Registro de incidentes.
☐ Controle de acesso físico.	☐ Controle de acesso lógico.	☐ Segregação de rede.
☐ Criptografia/Anonimização.	☐ Cópias de segurança. (*backups*)	☐ Gestão de ativos.
☐ Antivírus.	☐ Firewall.	☐ Atualização de Sistemas.
☐ Registros de acesso (logs).	☐ Monitoramento de uso de rede e sistemas.	☐ Múltiplos fatores de autenticação.
☐ Testes de invasão.	☐ Plano de resposta a incidentes.	☐ Outras (especifique).

Descreva as demais medidas de segurança técnicas e administrativas adotadas antes do incidente:

Após o incidente, foi adotada alguma nova medida de segurança? (admite mais de uma marcação)

☐ Políticas de segurança da informação e privacidade.	☐ Processo de Gestão de Riscos.	☐ Registro de incidentes.
☐ Controle de acesso físico.	☐ Controle de acesso lógico.	☐ Segregação de rede.
☐ Criptografia/Anonimização.	☐ Cópias de segurança. (*backups*)	☐ Gestão de ativos.
☐ Antivírus.	☐ Firewall.	☐ Atualização de Sistemas.
☐ Registros de acesso (logs).	☐ Monitoramento de uso de rede e sistemas.	☐ Múltiplos fatores de autenticação.
☐ Testes de invasão.	☐ Plano de resposta a incidentes.	☐ Outras (especifique).

Se cabível, descreva as medidas de segurança adicionais adotadas após o incidente:

As atividades de tratamento de dados afetadas estão submetidas a regulações de segurança setoriais?

☐ Sim ☐ Não

Se cabível, indique as regulamentações setoriais de segurança aplicáveis às atividades de tratamento de dados afetadas pelo incidente:

Declaro, sob as penas da lei, serem verdadeiras as informações prestadas acima.

<ASSINATURA>

10. DISPOSIÇÕES FINAIS

Disposições Finais

O Tribunal de Contas do Estado de Mato Grosso do Sul (TCE - MS) reforça a relevância deste Plano como um instrumento estratégico para a proteção dos dados pessoais e a continuidade dos serviços institucionais. A implementação de um processo estruturado para o tratamento de incidentes demonstra o compromisso do TCE - MS com a prevenção, a detecção rápida e a capacidade de adaptação a um cenário de ameaças cibernéticas em constante evolução.

Este Plano fortalece a cultura de segurança da informação no TCE - MS, promovendo a conscientização de todos os colaboradores e a adoção de práticas seguras no dia a dia. Ao responder de forma ágil e eficaz a incidentes de segurança, o Tribunal garante a integridade, a confidencialidade e a disponibilidade dos dados, reforçando a confiança do público nos serviços prestados.

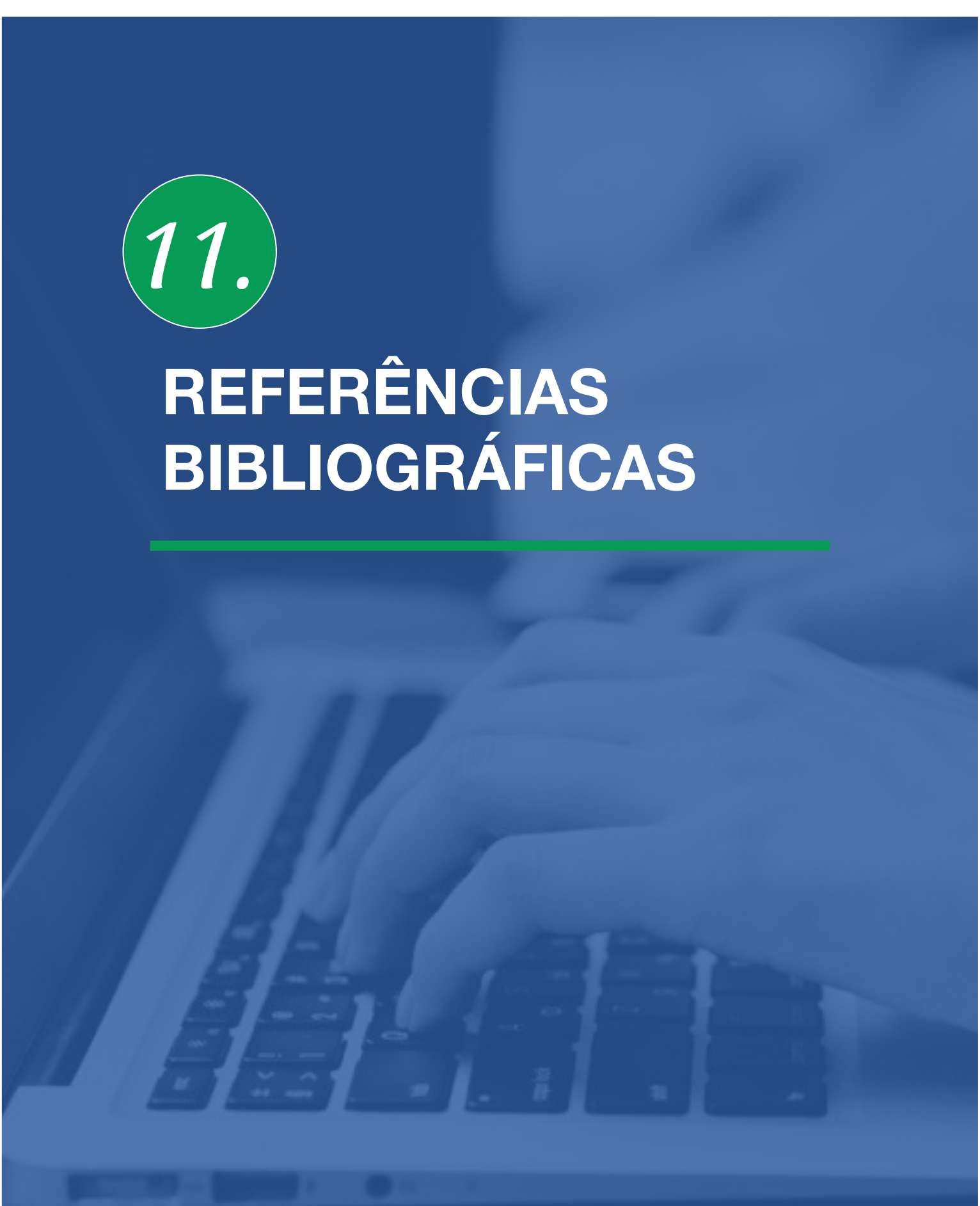
É fundamental ressaltar que este documento é dinâmico e será atualizado periodicamente para acompanhar as mudanças na legislação, as novas tecnologias e as melhores práticas de segurança. A conformidade com a Lei Geral de Proteção de Dados (LGPD) é uma prioridade e norteia todas as ações do TCE - MS nesse sentido.

Comitê de Segurança da Informação

TRIBUNAL DE CONTAS
Estado de Mato Grosso do Sul

11.

REFERÊNCIAS BIBLIOGRÁFICAS



Referências Bibliográficas

SECRETARIA DE ESTADO DA ADMINISTRAÇÃO - SEA/SC. Plano de Resposta a Incidentes de Segurança Lei Geral de Proteção de Dados Pessoais (LGPD) da Secretaria de Estado da Administração - SEA/SC.

BRASIL. Agência Nacional de Proteção de Dados – ANPD. Formulário de Comunicação de Incidente de Segurança. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis/formulario_cis_anpd1.docx .

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD). Lei nº 13.709, de 14 de agosto de 2018.

RESOLUÇÃO CD/ANPD Nº 15, de 24 de abril de 2024. Aprova o Regulamento de Comunicação de Incidente de Segurança.

RESOLUÇÃO TCE-MS Nº 200, de 21 de setembro de 2023. Regulamenta a aplicação da Lei Federal nº 13.709, de 14 de agosto de 2018, Lei de Proteção de Dados Pessoais (LGPD), no âmbito do Tribunal de Contas do Estado de Mato Grosso do Sul, revoga a Resolução TCE/MS 142, de 04 de março de 2021, e dá outras providências.

RESOLUÇÃO ADMINISTRATIVA TCE-MS Nº 100, de 18 de novembro de 2009. Dispõe sobre a Política Corporativa de Segurança da Informação do Tribunal de Contas de Mato Grosso do Sul.

DECRETO Nº 10.474, de 26 de agosto de 2020. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da Autoridade Nacional de Proteção de Dados e remaneja e transforma cargos em comissão e funções de confiança.

TRIBUNAL
DE CONTAS
Estado de Mato Grosso do Sul

E-mail: encarregado@tce.ms.gov.br

Sítio eletrônico: http://www.tce.ms.gov.br

Telefone: (67) 3317-1514

Av.: Des. José Nunes da Cunha, s/nº , Bloco 29 - Parque dos Poderes, Campo Grande - MS, 79031-902