Portaria AGEMS nº 347 de 23 de outubro de 2026.

Aprova o Plano de Resposta a Incidentes de Segurança de Dados Pessoais da Agência Estadual de Regulação de Serviços Públicos de Mato Grosso do Sul – AGEMS, em conformidade com a Lei Geral de Proteção de Dados (LGPD) e a Resolução CD/ANPD nº 15/2024.

O **DIRETOR-PRESIDENTE** DA AGÊNCIA ESTADUAL DE REGULAÇÃO DE SERVIÇOS PÚBLICOS DE MATO GROSSO DO SUL — **AGEMS**, no exercício de suas atribuições, tendo em vista o disposto no art. 19, inciso I, do Decreto Estadual nº 15.796, de 27 de outubro de 2021,

CONSIDERANDO o disposto no art. 48 da Lei Federal nº 13.709, de 14 de agosto de 2018 (LGPD), na Resolução CD/ANPD nº 15, de 24 de abril de 2024, e na Deliberação CETI nº 02, de 3 de maio de 2022, que aprova a Política de Segurança da Informação do Estado de Mato Grosso do Sul; e

CONSIDERANDO a deliberação da Diretoria-Executiva lavrada na Ata de Reunião n° 43, de 22 de outubro de 2026, por meio da qual foi aprovada a presente Portaria, conforme o processo administrativo nº 51.007.449-2026.

R E S O L V E:

Art. 1º Fica aprovado o Plano de Resposta a Incidentes de Segurança de Dados Pessoais da Agência Estadual de Regulação de Serviços Públicos de Mato Grosso do Sul – AGEMS, constante do Anexo Único desta Portaria, destinado a estabelecer diretrizes e procedimentos para a prevenção, a detecção, a contenção, a investigação, o registro, a resolução e a comunicação de incidentes de segurança que envolvam dados pessoais, de modo a assegurar a capacidade institucional de resposta a tais ocorrências.

§ 1º O Plano de que trata esta Portaria observa as diretrizes estaduais de governança da Política de Segurança da Informação do Estado de Mato Grosso do Sul, estabelecidas pela Deliberação CETI nº 02/2022, as disposições da Lei Federal nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), e o Regulamento de Comunicação de Incidente de Segurança, aprovado pela Resolução CD/ANPD nº 15, de 24 de abril de 2024.

§ 2º As disposições desta Portaria aplicam-se a todas as unidades organizacionais da AGEMS e a todas as pessoas que, em razão de vínculo funcional, contratual, de estágio ou de colaboração com a Autarquia, realizem operações de tratamento de dados pessoais em seu âmbito, incluindo agentes de tratamento, servidores, estagiários, colaboradores e prestadores de serviços terceirizados.

Art. 2º Para os fins desta Portaria, considera-se incidente de segurança com dados pessoais qualquer evento adverso confirmado que comprometa a confidencialidade, a integridade, a disponibilidade ou a autenticidade de dados pessoais, incluindo, entre outras hipóteses, o acesso não autorizado, a divulgação indevida, a perda, a destruição, a alteração, o vazamento ou o tratamento ilícito de dados pessoais.

Art. 3º A governança e a estrutura de resposta a incidentes de segurança com dados pessoais no âmbito da AGEMS compreendem as seguintes instâncias e atribuições:

I – Controlador: a AGEMS, a quem compete, por intermédio de seu Diretor-Presidente, deliberar sobre as providências institucionais decorrentes do incidente, apreciar o relatório final e assegurar a realização das comunicações legalmente exigidas à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares afetados, nos prazos e nas condições previstos na legislação e na regulamentação aplicáveis;

II – Encarregado pelo Tratamento de Dados Pessoais: responsável por coordenar a execução do Plano, realizar a triagem inicial do incidente, orientar os procedimentos de resposta e atuar como canal de comunicação entre a AGEMS, a ANPD e os titulares, sem prejuízo das competências legalmente atribuídas ao controlador;

III – Equipe de Resposta a Incidentes de Segurança com Dados Pessoais: equipe multidisciplinar coordenada pelo Encarregado e integrada por representantes do Núcleo de Tecnologia da Informação (NTI), da unidade organizacional afetada, da diretoria responsável pela área, da Coordenadoria Jurídica (CJUR) e da Diretoria de Inovação, Relações Institucionais e Assuntos Correlatos (DIR), incumbida de executar as medidas de contenção, erradicação e investigação do incidente, preservar as evidências e elaborar relatório circunstanciado sobre a ocorrência e as providências adotadas;

IV – Diretoria de Inovação, Relações Institucionais e Assuntos Correlatos (DIR): responsável por planejar e executar, em articulação com o Encarregado e as demais unidades competentes, as ações de comunicação

institucional relacionadas ao incidente, inclusive a elaboração e a divulgação de notas oficiais, observadas as restrições legais de acesso à informação e a proteção dos dados pessoais envolvidos.

Art. 4º A resposta aos incidentes de segurança com dados pessoais observará as etapas, os procedimentos e os prazos operacionais estabelecidos no Plano de Resposta a Incidentes de Segurança com Dados Pessoais, sem prejuízo da adoção imediata das medidas necessárias à contenção dos riscos, da preservação das evidências e do cumprimento dos prazos legais e regulamentares de comunicação.

Parágrafo único. Todos os incidentes deverão ser registrados em instrumento institucional próprio, inclusive aqueles que não ensejem comunicação externa, mantendo-se os respectivos registros pelo prazo mínimo de 5 (cinco) anos, ressalvadas as hipóteses de prazo superior previstas na legislação aplicável.

Art. 5º A comunicação de incidente de segurança com dados pessoais à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares afetados será realizada pelo Controlador quando o incidente puder acarretar risco ou dano relevante aos titulares, observado o prazo de 3 (três) dias úteis, contado do conhecimento de que o incidente afetou dados pessoais, ressalvadas as hipóteses de prazo específico previstas na legislação aplicável, nos termos da Resolução CD/ANPD nº 15, de 24 de abril de 2024.

Parágrafo único. Para a avaliação da necessidade de comunicação, deverão ser considerados, entre outros elementos, a natureza e a categoria dos dados pessoais afetados, a quantidade de titulares envolvidos, a eventual presença de dados pessoais sensíveis, de dados de crianças, adolescentes ou idosos, de dados financeiros, de autenticação ou protegidos por sigilo legal, judicial ou profissional, a escala do incidente e os potenciais impactos sobre os direitos e interesses dos titulares, bem como as medidas de mitigação adotadas.

Art. 6º As evidências técnicas coletadas durante a resposta aos incidentes deverão ser preservadas de modo a assegurar sua integridade, autenticidade, rastreabilidade e confiabilidade, mediante a adoção de procedimentos documentados de coleta, identificação, armazenamento, acesso e transferência, com observância da cadeia de custódia, quando aplicável.

Parágrafo único. Sempre que tecnicamente viável e pertinente à natureza da evidência, deverão ser gerados e registrados valores de resumo criptográfico (hash), preferencialmente pelo algoritmo SHA-256, bem como emitidos termos ou registros de custódia que identifiquem os responsáveis pela coleta, guarda e transferência das evidências.

Art. 7º Esta Portaria entra em vigor na data de sua publicação.

Campo Grande - MS, 23 de outubro de 2026.

CARLOS ALBERTO DE ASSIS
Diretor-Presidente

ANEXO ÚNICO DA PORTARIA AGEMS Nº 347 DE 23 DE OUTUBRO DE 2026

PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA DE DADOS PESSOAIS

Este Plano alinha-se com as diretrizes estaduais de governança fixadas pela Política de Segurança da Informação do Estado de Mato Grosso do Sul (Deliberação CETI nº 02/2022). Seu objetivo é assegurar capacidade institucional para prevenir, detectar, conter, investigar, registrar, solucionar e reportar situações de violação de dados pessoais, resguardando os direitos e liberdades fundamentais dos titulares de dados (art. 48 da Lei nº 13.709/2018 — LGPD e Resolução CD/ANPD nº 15/2024).

- ✓ **Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 — LGPD):** Norma nacional que disciplina o tratamento de dados pessoais em meios físicos e digitais.
- ✓ **Resolução CD/ANPD nº 15/2024:** Aprova o Regulamento de Comunicação de Incidente de Segurança

perante a Autoridade Nacional de Proteção de Dados (ANPD).

- ✓ **Deliberação CETI nº 02/2022 (DOE nº 10.767/2022):** Aprova a Política de Segurança da Informação do Estado de Mato Grosso do Sul.

O que é um Incidente de Segurança de Dados Pessoais:

Qualquer evento adverso confirmado relacionado à violação das propriedades de confidencialidade, integridade, disponibilidade ou autenticidade da segurança de dados pessoais (acesso não autorizado, perda, destruição, alteração, vazamento ou tratamento ilícito).

A tabela a seguir ilustra exemplos de tipos de incidentes e como eles podem ocorrer na prática.

Tipologia e Matriz de Incidentes de Segurança da Informação e Proteção de Dados

Tipologia do Incidente	Descrição Prática e Detalhada	Tríade Afetada (C-I-D)	Fundamento / Aspecto de Governança
Item 1. **Violação de dados**	Acesso não autorizado a informações confidenciais que contenham dados pessoais ou sensíveis.	Confidencialidade	Art. 46 e Art. 48 da LGPD. Exige restrição de acesso por perfil (RBAC).
Item 2. **Vazamento de dados pessoais**	Divulgação não autorizada, por meios físicos ou digitais, de dados pessoais ou dados pessoais sensíveis a terceiros não autorizados.	Confidencialidade	Art. 46 da LGPD. Avaliação obrigatória de risco e dano relevante ao titular.
Item 3. **Erros humanos**	Ações não intencionais que resultam em violações de segurança, como envio inadvertido de documentos com dados pessoais/sensíveis para destinatários errados ou publicação não proposital.	Confidencialidade / Integridade	Exige ações contínuas de conscientização, treinamento e implementação de ferramentas de DLP.
Item 4. **Código malicioso (Malware / Ransomware)**	Infecção por malware, ransomware (sequestro de dados mediante criptografia), ataques de phishing e engenharia social direcionados à instituição.	Confidencialidade / Integridade / Disponibilidade	Alto risco de paralisação e exfiltração de dados. Necessidade de backup imutável e antimalware EDR.
Item 5. **Negação de serviço**	Tentativa maliciosa de sobrecarregar servidor, rede ou serviço online com	Disponibilidade	Impacta a prestação de serviços públicos. Exige mitigação em camada

Tipologia do Incidente	Descrição Prática e Detalhada	Tríade Afetada (C-I-D)	Fundamento / Aspecto de Governança
(DoS/DDoS)	volume excessivo de tráfego via redes comprometidas ("bots"/"zumbis"), tornando o serviço inacessível aos usuários legítimos.		de rede e Web Application Firewall (WAF).
Item 6. **Acesso físico ou lógico prejudicado / impossibilitado**	Acesso prejudicado com relação a sistemas que armazenem dados pessoais, comprometendo a integridade ou disponibilidade dos mesmos de forma permanente ou temporária.	Integridade / Disponibilidade	Necessita de Plano de Continuidade de Negócios (PCN) e redundância de infraestrutura.
Item 7. **Intrusões de rede**	Acesso não autorizado a sistemas ou redes internas por meio da exploração de vulnerabilidades não corrigidas ou falhas de segurança no ambiente.	Confidencialidade / Integridade	Requer monitoramento contínuo (SOC/SIEM) e testes periódicos de intrusão (Pentest).
Item 8. **Acesso não autorizado**	Tentativas ou efetivações de acesso físico ou lógico a sistemas que possuam dados pessoais ou sensíveis sem a devida permissão ou credencial adequada.	Confidencialidade	Gestão rigorosa do ciclo de vida de identidades e implementação de Autenticação Multi-Fator (MFA).
Item 9. **Uso inapropriado**	Violação das Políticas de Uso de Dados, incluindo descumprimento das Políticas de Segurança da Informação (PSI) e de Privacidade institucionais.	Confidencialidade / Integridade	Aplicação de normas disciplinares e auditoria periódica de logs de uso e acessos.
Item 10. **Exploração de vulnerabilidades**	Aproveitamento de falhas de segurança em softwares, sistemas ou infraestrutura para obter acesso não autorizado a dados pessoais ou sensíveis.	Confidencialidade / Integridade / Disponibilidade	Processo estruturado de Gestão de Vulnerabilidades e aplicação célere de patches de segurança.

Riscos, Impactos e Medidas Mitigatórias

Categoria de Incidente	Principais Riscos e Impactos Institucionais	Ações Mitigatórias
Vazamento / Violação de Dados (Itens 1, 2)	• Sanções administrativas pela ANPD. • Danos reputacionais graves ao órgão público. • Responsabilização civil e administrativa de agentes.	• Criptografia em trânsito e em repouso. • Implementação de controle de acesso.
Falha Humana e Uso Inapropriado (Itens 3, 9)	• Exposição acidental de informações sigilosas. • Envio indevido de processos com dados pessoais a terceiros.	• Programa contínuo de conscientização e treinamento. Verificação e confirmação antes do envio de e-mails/arquivos.
Ataques Cibernéticos Severos (Itens 4, 5)	• Paralisação dos serviços públicos digitais. • Perda irreversível ou indisponibilidade de dados. • Extorsão e comprometimento da reputação institucional.	• Rotina de backups imutáveis e mantidos offline. • Implementação de soluções de monitoramento
Falhas Físicas, Lógicas e de Infraestrutura (Itens 6, 7, 8, 10)	• Persistência maliciosa de atacantes na rede. • Exfiltração silenciosa e contínua de bases de dados. • Comprometimento da integridade das informações públicas.	• Implementação de soluções de monitoramento • Política ativa de Gestão de Patches e Atualizações. • Execução regular de testes de intrusão e auditorias de log.

Diretrizes Práticas de Governança

Eixo de Ação	Obrigação Legal e Prática Operacional
Notificação de Incidentes (Art. 48, LGPD)	Avaliar todo incidente de segurança que envolva dados pessoais, independentemente de sua tipologia, para verificar a possibilidade de risco ou dano relevante aos titulares e a consequente necessidade de comunicação à ANPD e aos titulares, observados os critérios e os prazos regulamentares.
Registro de Incidentes (Accountability)	Manter registro centralizado e atualizado de todos os incidentes (*mesmo os contidos internamente e sem impacto direto aos titulares),* para comprovação de governança perante órgãos de controle e auditorias.
Plano de Resposta a Incidentes (PRI)	Assegurar a definição clara de papéis, responsabilidades e fluxos de comunicação entre o Encarregado (DPO), a equipe de Tecnologia da Informação/Segurança e a Alta Administração.

3. OBJETIVOS E DIRETRIZES DO PLANO DE RESPOSTA

- Assegurar prontidão e eficácia operacional no isolamento, contenção e mitigação de danos em situações de emergência de segurança.
- Estabelecer fluxo claro de responsabilidades entre a Diretoria, Encarregado (DPO), NTI, Jurídico e Comunicação.
- Garantir a integridade e a cadeia de custódia das evidências técnicas para apuração de responsabilidades e eventual perícia.
- Cumprir com rigor os prazos legais e regulamentares para notificação à ANPD e aos titulares, quando verificado risco ou dano relevante.
- Manter registro detalhado de todos os incidentes pelo prazo mínimo de 5 (cinco) anos.
- Promover a melhoria contínua dos controles organizacionais e cibernéticos da AGEMS a partir das lições aprendidas.

4. GOVERNANÇA E ESTRUTURA DE RESPOSTA

4.1. Controlador (Presidência da AGEMS)

- Apreciar o Relatório final do incidente formulado pela Equipe de Resposta.
- Decidir conclusivamente sobre a notificação compulsória ou voluntária à ANPD e aos titulares.
- Determinar a instauração de Processo Administrativo Disciplinar (PAD) ou providências contratuais, se houver responsabilidade funcional ou de fornecedores.
- Proferir o voto desempate nas deliberações técnicas da Equipe de Resposta.

4.2. Encarregado pelo Tratamento de Dados Pessoais (DPO)

- Liderar e coordenar a execução das fases do Plano de Resposta a Incidentes.
- Efetuar a triagem inicial e classificar o evento quanto ao impacto e relevância sobre dados pessoais.
- Atuar como canal oficial de comunicação perante a ANPD, os titulares afetados e os órgãos estaduais de controle.

4.3. Equipe de Resposta a Incidentes de Dados Pessoais

Promover a contenção, erradicação, preservação de evidências, investigação da causa raiz e elabora o Relatório ***em até 24 (vinte e quarto) horas***. Estrutura multidisciplinar composta por:

- 01 (um) Encarregado pelo Tratamento de Dados Pessoais (Coordenador da Equipe);
- 02 (dois) servidores do Núcleo de Tecnologia da Informação (NTI);
- 01 (um) servidor da área afetada responsável por prestar informações técnicas e operacionais; *(Preferencialmente não envolvido na ocorrência)*
- 01 (um) membro da Diretoria do setor afetado
- 01 (um) membro da Coordenadoria Jurídica (CJUR);
- 01 (um) membro da Diretoria de Inovação, Relações Institucionais e Assuntos Correlatos (DIR)

4.4. Validar o relatório com prazo de revisão de 6 horas (em caso de correções) e o Encarregado submete ao Controlador.

4.5. Diretoria de Comunicação (DIR)

Gerenciar a estratégia de comunicação social, formulando notas oficiais transparentes e orientações aos titulares em alinhamento com o DPO.

4.6. Gestão de Incidentes com Empresas Operadoras e Terceiros

Sempre que o incidente de segurança envolver dados pessoais tratados por empresas contratadas, provedores de nuvem ou prestadores de serviço em nome da AGEMS (na qualidade de OPERADORES), adotar-se-á obrigatoriamente o padrão fixado pelo *Guia Orientativo da Unidade Central de Proteção de Dados Pessoais (UCPDP/SEGOV):*

- **Acionamento Imediato:** A área técnica ou o DPO exigirá da operadora a comunicação preliminar imediata e a preservação rigorosa de evidências e logs, sem aguardar a conclusão da investigação contratual.
- **Requisitos Mínimos do Relatório Técnico:** O relatório técnico de investigação fornecido pela operadora deverá observar os elementos mínimos de qualidade exigidos pelo Estado (cronologia, inventário de dados e titulares, análise de causa raiz, gradação de risco e declaração de limitações), servindo de subsídio técnico para a tomada de decisão do Controlador.
- **Independência de Prazos:** Ressalta-se que a instauração de investigação ou a elaboração de relatórios pela operadora **não suspendem nem prorrogam** o prazo legal e improrrogável de **3 (três) dias úteis** da AGEMS para a eventual notificação à ANPD e aos titulares.

5. CANAIS DE NOTIFICAÇÃO DO INCIDENTE

- **Público Interno (Servidores/Colaboradores):** Comunicação imediata do fato à chefia direta, que acionará a Unidade de Proteção de Dados Pessoais (UPD) via sistema e-MS (Comunicação Interna) ou e-mail encarregadolgpd@agems.ms.gov.br.
- **Público Externo (Cidadãos/Usuários):** Registro oficial de denúncias ou avisos através da Plataforma Fala.BR (Ouvidoria: https://falabr.cgu.gov.br).

6. FLUXO OPERACIONAL DE ATENDIMENTO A INCIDENTES

Etapa	Fase Operacional	Prazos e Ações
01	**Detecção e Notificação**	Comunicação imediata (ou em no máximo 1 hora da constatação) do fato suspeito ou confirmado à UPD/AGEMS e NTI pelos canais oficiais: e-MS ou e-mail funcional.
02	**Triagem Inicial (em até 4h para incidentes críticos e máximo de 12h para os demais)**	O Encarregado, em conjunto com o NTI, avalia imediatamente a presença de dados pessoais. Se ausente o impacto a dados pessoais, o caso será encaminhado a NTI/AGEMS para tratamento como incidente de TI conforme a PSI (Deliberação CETI nº 02/2022). Se presente, convoca imediatamente a Equipe de Resposta.

Etapa	Fase Operacional	Prazos e Ações
03	**Contenção, Erradicação e Preservação**	Isolamento imediato de redes/sistemas, revogação de acessos, remoção de malwares e extração/preservação de cópia de segurança e logs originais, garantindo a inviolabilidade técnica dos vestígios.
04	**Relatório Circunstanciado em até 24h**	A Equipe consolida os fatos, causa raiz e gravidade em até 24 horas do acionamento, aprova o relatório com prazo de revisão sumária de até 2 horas e o Encarregado o envia imediatamente ao Controlador.
05	**Deliberação do Controlador e Notificação Externa**	O Controlador delibera sobre a notificação à ANPD e aos titulares, a ser transmitida pelo Encarregado (DPO) com a máxima celeridade, respeitando rigorosamente o prazo máximo improrrogável de 3 (três) dias úteis do conhecimento oficial do incidente.
06	**Registro Obrigatório e Lições Aprendidas**	Lançamento de todas as informações no Registro Institucional de Incidentes (guarda por 5 anos) e revisão dos controles de segurança da AGEMS.

7. CHECKLIST DE REGISTRO DO INCIDENTE

A Unidade de Proteção de Dados da AGEMS deve obrigatoriamente coletar e registrar os seguintes itens para compor o processo do incidente:

Campo Obrigatório de Registro	Detalhamento Exigido
Origem e Contato	Setor/unidade de origem e dados de contato do informante da ocorrência.
Datas e Endereçamento Técnico	Data/hora da ocorrência, data/hora do conhecimento oficial e endereço IP afetado.
Quantitativo de Titulares	Quantidade estimada ou exata de titulares afetados.

Campo Obrigatório de Registro	Detalhamento Exigido
Recursos e Técnicas Envolvidas	Portas, protocolos de rede, códigos de erro, programas e procedimentos adotados na ação maliciosa.
Categorização de Dados	Natureza dos dados afetados (cadastrais, financeiros, sensíveis, credenciais de autenticação).
Sistemas e Serviços Impactados	Identificação dos softwares, bancos de dados, servidores ou serviços interrompidos.
Evidências Físicas / Digitais	Preservação e anexo de logs de auditoria, imagens de tela, arquivos corrompidos e cópia preservada dos dados vazados para fins de perícia.
Ações Mitigatórias	Medidas imediatas e definitivas implementadas para estancar a violação.

8. PROTOCOLO DE COMUNICAÇÃO EXTERNA (ANPD e Titulares)

8.1. Parâmetros Objetivos para Avaliação de Risco ou Dano Relevante A notificação compulsória à ANPD é acionada quando o incidente envolver dados pessoais sujeitos à LGPD e puder causar risco ou dano relevante aos direitos e liberdades fundamentais dos titulares. *Para fins de subsídio à decisão do Controlador, adota-se a seguinte matriz de gravidade (considerando a cumulação ou relevância dos critérios):*

- *Natureza e sensibilidade dos dados: Envolvimento de dados pessoais sensíveis (art. 5º, II, da LGPD), dados de crianças e adolescentes, dados financeiros, de saúde, biométricos ou credenciais de autenticação (senhas e chaves de acesso);*
- *Volume e abrangência: Grande escala de titulares afetados ou potencial repercussão institucional e social;*
- *Vulnerabilidade dos titulares: Possibilidade concreta de prejuízo material ou moral, discriminação, violação à integridade física, roubo de identidade, fraudes financeiras ou restrição de direitos;*
- *Capacidade de mitigação: Efetividade das medidas técnicas adotadas imediatamente após a violação para neutralizar o risco materializado.*

8.2. Prazos, Obrigatoriedade e Conteúdo Mínimo da Comunicação (Resolução CD/ANPD nº 15/2024)

- **Prazo:** A comunicação à ANPD e, quando verificado risco ou dano relevante, aos titulares afetados, deverá ser realizada no **prazo máximo de 3 (três) dias úteis**, contados da data do conhecimento, pelo Controlador, de que o incidente afetou dados pessoais, em estrita observância ao art. 6º e seguintes da Resolução CD/ANPD nº 15/2024. *(Caso a identificação ou comunicação individualizada direta aos titulares seja inviável ou exija esforço desproporcional, a AGEMS solicitará/adotará a ampla divulgação em canais oficiais, mantendo a ANPD ciente).*
- **Comunicação aos Titulares**: Quando verificado risco ou dano relevante, a comunicação aos titulares afetados será realizada de forma individualizada (ou por ampla divulgação em canais oficiais da AGEMS caso a identificação direta seja inviável ou excessivamente onerosa, conforme diretriz da ANPD). A comunicação aos titulares ocorrerá de forma simultânea ou imediatamente subsequente à notificação da Autoridade, contendo orientações claras e diretas sobre as ações de autoproteção.
- **Comunicação Voluntária:** Caso o incidente não atinja o patamar de risco ou dano relevante, a AGEMS poderá realizar a comunicação voluntária à ANPD como demonstração de transparência, cooperação e boa-fé, servindo como elemento atenuante em eventuais procedimentos fiscalizatórios.
- **Conteúdo Mínimo do Comunicado:** Descrição da natureza dos dados pessoais afetados; informações sobre os titulares envolvidos e quantitativo estimado; indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados; riscos e possíveis consequências decorrentes do incidente; medidas adotadas ou que serão adotadas para reverter ou mitigar os efeitos; contatos do Encarregado (DPO) para prestação de esclarecimentos**;** e orientações explícitas aos titulares sobre como mitigar os potenciais efeitos (ex.: alteração de senhas, monitoramento de transações e atenção a contatos suspeitos).

9. ASPECTOS OPERACIONAIS E CADEIA DE CUSTÓDIA

Diretriz técnica para salvaguardar a validade das provas em auditorias, investigações internas e perante órgãos de controle externo (TCE-MS e ANPD).

9.1. Cadeia de Custódia e Preservação de Evidências: Para assegurar a integridade probatória em eventuais apurações administrativas, judiciais ou auditorias externas, a Equipe de Resposta adotará obrigatoriamente protocolos estritos de cadeia de custódia:

- **Isolamento e Inviolabilidade:** Dispositivos, servidores, contas de acesso ou redes comprometidas deverão ser isolados logicamente e/ou fisicamente de imediato para evitar a sobrescrita ou alteração de vestígios digitais.
- **Geração de Assinaturas Digitais (Hashes):** Toda extração de logs de auditoria, cópias de segurança (snapshots) ou arquivos corrompidos deverá ter sua integridade garantida mediante o cálculo de funções hash criptográficas (como SHA-256), registrando-se o carimbo de tempo (timestamp) da coleta.
- **Termo de Custódia:** Todo vestígio digital coletado será acautelado sob responsabilidade formal de um membro da Equipe de Resposta, com registro minucioso de quem o coletou, quem o custodiou e quais acessos foram realizados, prevenindo contestações sobre a fidedignidade das evidências técnicas apresentadas à ANPD ou ao Tribunal de Contas.

10. GLOSSÁRIO

- ✓ **Acesso Indevido a Dados Pessoais:** Entrada irregular ou não autorizada em ambiente físico ou lógico/virtual contendo dados pessoais.
- ✓ **Agentes de Tratamento:** O Controlador (AGEMS) e o Operador (terceiros contratados que tratam dados em nome da Agência).
- ✓ **Ampla Divulgação do Incidente:** Providência em meios de comunicação (site, redes sociais ou imprensa) determinada pela ANPD quando inviável a notificação direta aos titulares ou para mitigar danos em larga escala.
- ✓ **Comprometimento de Senha:** Exposição inadvertida ou ilícita de credenciais de acesso corporativo a terceiros não autorizados.
- ✓ **Dado de Autenticação em Sistemas:** Qualquer dado pessoal utilizado como credencial para determinar ou confirmar o acesso do usuário a sistemas (logins, tokens, senhas, chaves de acesso).
- ✓ **Dado Financeiro:** Dado pessoal referente a transações bancárias, remunerações, contabilidade ou histórico financeiro do titular.
- ✓ **Operação de Tratamento:** Toda atividade realizada com dados pessoais (coleta, recepção, classificação, utilização, acesso, processamento, arquivamento, eliminação, transferência).