Ministério do Desenvolvimento Agrário e Agricultura Familiar

Comitê de Governança Digital e Segurança da Informação
Subcomitê Técnico de Privacidade e Proteção de Dados Pessoais

Plano de Gestão de **INCIDENTES CIBERNÉTICOS**

Brasília - DF
Maio, 2026

Ministério do Desenvolvimento Agrário e Agricultura Familiar

Ministra de Estado
Fernanda Machiaveli Morão de Oliveira

Secretário-Executivo
Eric Sousa Moura

Secretária-Executiva Adjunta
Marina Godoi de Lima

Encarregada pelo Tratamento de Dados Pessoais
Silvana Stadniki Morato Miranda

Gestor de Segurança da Informação
Diego Donizetti Gonçalves Machado

Gestora de Tecnologia da Informação
Pamela Santiago Hilário

Comitê de Governança Digital e Segurança da Informação e Comunicação

Titulares	Suplentes
Marina Godoi de Lima	Guilherme Vasques Tavira
Marcus Vinicius Boente	Caio Correia Baccini
Silvana Stadniki Morato Miranda	Luana Sena Ferreira
Carlos Henrique Naegeli Gondim	Aline Paula Gomes Costa
Ana Terra Reis	Regilane Fernandes da Silva
Arthur Reis Rimoldi	Vivian Libório de Almeida
Shirley Anny Abreu do Nascimento	Ana Elsa Munarini
Edmilton Cerqueira	Welliton Hassegawa
Viviana Bezerra de Mesquita	Patrícia de Lucena Mourão
Diego Donizetti Gonçalves Machado	Renato das Neves Iwakawa
Patrícia Apolinário	Vanessa Moreira Gonçalves
Pamela Santiago Hilário	Frederico Augusto Del Isola e Diniz

Subcomitê Técnico de Privacidade e Proteção de Dados Pessoais

Titulares	Suplentes
Silvana Stadniki Morato Miranda	Luana Sena Ferreira
Tatiana Freitas de Oliveira	Maria Cláudia Nascimento dos Santos
Ernesto Pereira Galindo	Marcelo Cabreira Bastos
Pamela Santiago Hilário	Fernando de Britto e Silva

Sumário

1. Introdução

O presente Plano de Gestão de Incidentes Cibernéticos complementa as políticas, estratégias e instruções normativas sobre o tema e deve ser observado pelos gestores e profissionais de segurança da informação do Ministério do Desenvolvimento Agrário e Agricultura Familiar (MDA).

Os procedimentos estabelecidos incluem ações a serem desenvolvidas pelos diversos atores e unidades administrativas do MDA que atuam em temas relacionados à segurança da informação, à proteção e à privacidade de dados, sendo fundamental a atuação da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) deste Ministério, instituída pela Portaria MDA nº 50, de 2 de outubro de 2025.

A Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, que trata da estrutura de gestão da segurança da informação, prevê, em seu artigo 9º, a obrigatoriedade da implementação da política de segurança da informação nos órgãos e entidades que compõem a administração pública federal. Tal previsão encontra ainda amparo no art. 10 do Decreto nº 12.572, de 4 de agosto de 2025, que institui a Política Nacional de Segurança da Informação (PNSI).

Como instrumento de implementação da Política de Segurança da Informação do Ministério do Desenvolvimento Agrário e Agricultura Familiar (POSIN/MDA), este Plano visa estabelecer processo de gestão de incidentes cibernéticos, descrevendo fluxos e ações a serem adotados pelo MDA, considerando os requisitos de segurança dispostos na Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), e em outros normativos referentes ao tema, tais como o Decreto nº 10.748, de 16 de julho de 2021, que institui a Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC); a Resolução CD/ANPD nº 15, de 24 de abril

de 2024, que aprova o Regulamento de Comunicação de Incidente de Segurança; a Portaria GSI/PR nº 120, de 21 de dezembro de 2022, que publica o Plano de Gestão de Incidentes Cibernéticos para a Administração Pública Federal (PlanGIC), e demais normativos aplicáveis.

2. Atividades Preparatórias

As atividades preparatórias consistem na execução das seguintes ações:

- designar gestor de segurança da informação;
- instituir e implementar a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) ou estrutura equivalente;
- informar ao Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República (DSI/GSI/PR) o contato direto do ponto focal responsável pelo compartilhamento de informações relacionadas às atividades da ETIR ou da estrutura equivalente;
- designar o Encarregado pelo Tratamento de Dados Pessoais e publicar as informações de contato e nomeação no sítio eletrônico do Controlador, de forma clara e objetiva;
- implementar, no mínimo, os processos de mapeamento de ativos de informação, de gestão de riscos de segurança da informação, de gestão de continuidade de negócios em segurança da informação e de gestão de mudanças nos aspectos de segurança da informação; e
- disponibilizar infraestrutura mínima para realização das atividades de segurança da informação, com capacidade de execução dos processos de prevenção, detecção, tratamento e resposta a incidentes cibernéticos.

3. Procedimentos em incidentes de segurança

a. Prevenção

A prevenção é um processo constante de ações proativas, com o objetivo de reduzir a probabilidade de ataques cibernéticos bem-sucedidos. Entre essas ações, enfatizam-se as de definição e de implementação de controles de segurança, de gerenciamento de vulnerabilidades, de conscientização e de capacitação.

As ações preventivas de segurança cibernética deverão contemplar aquelas previstas na Política de Segurança da Informação (POSIN/MDA) e em demais normativos internos correlatos.

I. Definição e implementação de controles de segurança preventivos

Os controles de segurança preventivos constituem-se em tecnológicos, organizacionais e físicos. Os controles tecnológicos são aqueles utilizados para reduzir vulnerabilidades no hardware e no software, incluindo, entre outros:

- dispositivos *endpoint* do usuário;
- restrição de acesso à informação;
- autenticação segura;
- proteção contra *malware*;
- backup das informações;
- atividades de monitoramento (log);
- segurança de redes;
- norma de segurança da informação para uso de serviços em nuvem;
- uso de criptografia; e
- gestão de mudanças.

Por sua vez, os controles organizacionais são destinados a assegurar a adequação contínua da gestão de segurança da informação. Entre os principais controles organizacionais a serem adotados, destacam-se:

- Política de Segurança da Informação (POSIN/MDA);
- definição de papéis e responsabilidades pela segurança da informação;
- segregação de funções;
- mapeamento de ativos de informação;
- controle de acesso; e
- classificação e rotulagem de informações.

Por fim, os controles físicos têm por finalidade prevenir ou evitar o acesso não autorizado a áreas e materiais sensíveis, bem como evitar danos e interferências a ambientes que contenham informações críticas ou sensíveis. Entre os principais controles físicos, citamse os seguintes:

- definição dos perímetros de segurança física;
- monitoramento de segurança física;
- proteção contra ameaças físicas e ambientais;
- localização e proteção de equipamentos;
- segurança de ativos fora das instalações da organização; e
- manutenção de ativos.

II. Gerenciamento de vulnerabilidades

Trata-se de um processo contínuo e proativo, com o objetivo de controlar riscos, realizar monitoramento, corrigir falhas e adotar ações de proteção contra ataques cibernéticos e violação de dados. O objetivo desse processo é reduzir a exposição geral da organização a riscos, mitigando o maior número possível de vulnerabilidades.

Esse processo é desafiador em virtude do número crescente de possíveis vulnerabilidades e da limitação de recursos disponíveis tempestivamente para correção. Em função disso, as ações de prevenção devem ser sempre complementadas pelas ações de detecção e de tomada de decisão sobre o ativo da informação vulnerável.

Para tanto, a unidade de segurança da informação deverá, no mínimo, coordenar, em conjunto com as demais unidades organizacionais, as seguintes ações, por meio do mapeamento de ativos de informação:

- classificar os ativos de informação de acordo com sua criticidade;
- identificar continuamente as vulnerabilidades neles existentes; e
- priorizar as ações de correção e de mitigação por meio da avaliação do nível de ameaça e de criticidade da vulnerabilidade.

A fim de operacionalizar as atividades supracitadas, a Coordenação-Geral de Tecnologia da Informação (CGTI) deverá:

- acompanhar as notificações, os alertas e as recomendações emitidas por parceiros, entre eles, o CTIR Gov e os fornecedores de ativos constantes de seu mapeamento de ativos, adotando as ações necessárias;
- estabelecer um processo para gerenciamento de patches; e
- estabelecer um processo para gerenciamento de configuração e de correção de vulnerabilidades.

As orientações sobre correção ou mitigação, bem como o procedimento para aplicação de medidas corretivas, deverão ser estabelecidas em documentação interna, registradas no Sistema Eletrônico de Informações (SEI) ou outro meio de comunicação.

III. Educação - conscientização e capacitação em cibernética

Visando aprimorar a educação em segurança cibernética, o Gestor de Segurança da Informação deverá estimular iniciativas de capacitação em segurança da informação e promover ações de conscientização sobre boas práticas aos agentes públicos. A capacitação em cibernética deverá constar no Plano de Desenvolvimento de Pessoas do Ministério (PDP/MDA).

Ainda, o Gestor de Segurança da Informação deverá estabelecer, para todos os seus colaboradores, processo de divulgação de boas práticas sobre o tema segurança cibernética, utilizando canais de comunicação adequados, além de possuírem linguagem adequada ao público-alvo. Poderão ser realizadas iniciativas no âmbito da própria organização, tais como seminários, colóquios, estágios, treinamentos, palestras, boletins informativos e memorandos.

É necessário que a conscientização sobre a segurança da informação contemple alguns aspectos:

- compromisso da Alta Administração com a segurança da informação;
- responsabilização dos colaboradores por ações e omissões; e
- familiarização e compliance em relação às regras e obrigações aplicáveis de segurança da informação.

Com relação à capacitação, é necessário:

- preparação de um plano de treinamento adequado para equipes técnicas cujos papéis requerem habilidades e conhecimentos específicos; e
- constante atualização e aprimoramento do conhecimento técnico e profissional.

b. Detecção

Conceitua-se detecção como um processo de melhoria contínua que analisa todo o ambiente de informação, a fim de identificar atividades maliciosas que possam comprometer os ativos de informação. Tem por objetivo reduzir o impacto do incidente cibernético, antecipando o início do processo de tratamento e de resposta. Logo, a detecção pressupõe o estabelecimento de linhas de base, de monitoramento contínuo e de comunicação dos incidentes cibernéticos.

I. Estabelecimento de linhas de base

A CGTI deverá estabelecer linhas de base que caracterizem o uso normal da rede. As anormalidades são consideradas indícios de incidente e, se identificadas, devem ser investigadas. Os critérios para analisar e caracterizar uma anormalidade como suposto incidente são essenciais para a eficácia do processo.

II. Monitoramento contínuo

A CGTI deverá estabelecer o monitoramento contínuo de seus ativos de informação, cabendo a verificação contínua de:

- alteração de comportamento pela comparação com as linhas de base;
- acesso de usuários, particularmente quanto a horários e ativos acessados;
- volumetria do tráfego de saída;
- logs;
- funcionamento e atualização das ferramentas de segurança cibernética, em especial as de *antimalware*; e
- execução não autorizada de serviço, *software* ou código.

Esse processo pode ser complementado com ações de detecção proativa, que incluem:

- exploração controlada de vulnerabilidades;
- atividades proativas de equipes de análise;
- correlação de log e eventos;
- teste de penetração; e
- monitoramento proativo de rede.

Uma vez identificada uma anomalia, as informações referentes ao evento adverso deverão ser encaminhadas para triagem, e, em seguida, serão direcionadas para as áreas de atuação.

III. Comunicação

O MDA deverá informar o endereço de correio eletrônico institucional (abuse@mda.gov.br) de sua ETIR para troca de informações relacionadas a incidentes cibernéticos com o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov), por intermédio do termo de adesão disponibilizado no sítio eletrônico do CTIR Gov. Esse canal será empregado futuramente na operacionalização de uma plataforma computacional dedicada.

Havendo indisponibilidade da comunicação por meio do correio eletrônico, excepcionalmente, poderão ser utilizados outros canais para comunicação, como:

- voz;
- *Inter-Network Operation Center Dial By Autonomous System Number* (INOCDBA);
- mensagem instantânea;
- reunião por videoconferência;
- sítios eletrônicos e mídias sociais institucionais; e
- reunião presencial de representantes.

As principais mensagens que serão transmitidas por meio desses canais de comunicação dizem respeito à notificação de incidentes cibernéticos, as quais devem seguir a padronização definida e disponibilizada pelo CTIR Gov em seu sítio eletrônico.

c. Tratamento

O tratamento de incidentes cibernéticos inicia-se imediatamente após a sua detecção pela ETIR devido ao monitoramento contínuo ou à notificação por parte de algum usuário, passando pelo processo de triagem, seguido pelo processo de análise.

I. Triagem e análise

- confirmar se a ocorrência se trata de um incidente cibernético e, caso este não pertença à *constituency*, redirecionar a informação para o responsável pelo tratamento;
- verificar se há correlação com outros incidentes;
- estabelecer a prioridade para o tratamento do incidente;
- registrar o incidente na base de incidentes cibernéticos; e
- atribuir o tratamento do incidente ao analista ou à equipe responsável.

Após estabelecer essa priorização, a ETIR deverá classificar o incidente cibernético de acordo com o impacto na disponibilidade, integridade, confidencialidade e autenticidade no ativo de informação em um dos seguintes níveis: crítico, alto, médio ou baixo.

II. Avaliação interna

O processo de análise consiste nas atividades listadas abaixo:

- validar as informações tratadas na triagem, ratificando-as, complementandoas ou retificando-as;
- identificar e avaliar atividades anômalas em relação à linha de base conhecida;
- identificar pelo menos uma parte da cadeia de ataque para permitir a definição das atividades de resposta;
- complementar e adicionar novos dados a partir da colaboração das fontes utilizadas na detecção; e
- incluir todos os dados coletados na documentação sobre o incidente para viabilizar as ações de pós-incidente.

Na atividade de colaboração, é obrigatória a comunicação ao CTIR Gov apenas dos incidentes que:

- possam implicar perda de vidas;
- afetem a disponibilidade, integridade, confiabilidade e autenticidade de ativos de informação de:

a) infraestruturas críticas – energia, água, transporte, finanças, comunicações, defesa e biossegurança; e

b) serviços governamentais digitais;

c) implique em vazamento de:
- ▶ dados pessoais;
- ▶ informação classificada ou sensível; e
- ▶ dados que possuam potencial de exploração danosa em larga escala.

d. Resposta

O processo de resposta a um incidente cibernético consiste em ações de contenção, erradicação, recuperação, documentação, colaboração e validação.

I. Contenção

O objetivo da contenção é limitar os danos causados pelo atual incidente de segurança e evitar outros. Devem ser aplicadas medidas para mitigar o incidente, evitando-se a destruição de provas que possam servir de subsídios para possível processo cível, penal ou administrativo. A ação de contenção poderá envolver as seguintes atividades:

- contenção a curto prazo, que consiste em:

  a) limitar os danos antes que o incidente piore;
  b) isolar segmentos de rede; e
  c) executar um *failover routing* (desvio de tráfego de rede para os recursos que estejam saudáveis e disponíveis);

- realização de imagem forense do ambiente afetado; e
- contenção a longo prazo, que consiste em:

  a) identificar vulnerabilidades exploradas pelos atacantes e os mecanismos que permitiram o ataque; e

b) aplicar correções temporárias que permitam a volta ao funcionamento dos sistemas afetados.

II. Erradicação

A erradicação consiste em remover ou inutilizar artefatos utilizados pelos atacantes e em restaurar o ambiente afetado. A ação de erradicação poderá envolver as seguintes atividades:

- restauração completa das imagens de unidades de armazenamento, implicando na exclusão de todos os dados atuais;
- recuperação dos dados a partir dos backups existentes;
- identificação das causas principais que originaram o ataque;
- realização dos procedimentos necessários para limpar a unidade de armazenamento, removendo ou isolando os artefatos utilizados pelos atacantes; e
- correção das vulnerabilidades encontradas.

III. Recuperação

O objetivo da recuperação é restabelecer o pleno funcionamento do ambiente afetado após garantir que as ameaças foram neutralizadas ou removidas. A ação de recuperação poderá envolver as seguintes atividades:

- definição de cronograma para a restauração das operações pelos responsáveis dos ativos de informação afetados, com base em subsídios apresentados pela ETIR;

- realização de varredura completa do ambiente recuperado, de forma a garantir que este esteja apto para uso seguro;
- realização de testes de funcionamento do ambiente recuperado, validando os resultados com as linhas de base definidas, à medida em que estarão novamente disponibilizados para uso; e
- monitoramento do ambiente recuperado, a ser executado num período após o incidente cibernético, de forma a verificar comportamentos atípicos ou anormalidade nas operações.

Após o término do processo de recuperação, o MDA deverá encaminhar ao CTIR Gov um relatório do incidente, contendo as seguintes informações:

- atores atacantes e atacados;
- atores envolvidos no tratamento e resposta do incidente;
- evidências coletadas;
- indicadores de comprometimento (IoCs), bem como táticas, técnicas e procedimentos (TTPs);
- ativos de infraestrutura, serviços e total de usuários afetados;
- volume de dados exfiltrados;
- cronologia dos fatos;
- medidas de contenção, erradicação e recuperação adotadas; e
- medidas preventivas propostas para ocorrências similares.

As ações de contenção, erradicação e recuperação devem constar do plano de continuidade de negócios em segurança da informação e devem ser baseadas na POSIN/MDA, em demais normativos aplicáveis e nos seguintes critérios:

a) criticidade dos ativos afetados;

b) tipo e gravidade do incidente;

c) necessidade de preservar a evidência;

d) importância de quaisquer sistemas afetados para processos de negócio críticos; e

e) recursos necessários para implementar a estratégia.

IV. Documentação

a) incluir todos os dados coletados na documentação sobre o incidente para viabilizar as ações de pós incidente; e

b) atualizar os dados disponíveis de boas práticas e prevenção indicadores de comprometimento elaboração do plano de resposta.

V. Colaboração

a) complementar e adicionar novos dados a partir da colaboração das fontes utilizadas na detecção;

b) informar ao CTIR Gov;

c) pesquisar ou solicitar dados complementares às diversas fontes de ataque;

d) identificar pelo menos uma parte da cadeia de ataque para permitir a definição das atividades de resposta técnicas, táticas e procedimentos (TTP), indicadores de comprometimento (IoC); inteligência de fontes abertas (OSINT); inteligência de ameaças causa raiz:

- identificar e avaliar atividades anômalas em relação à linha de base conhecida, fluxo de dados, horário de acesso, logs, autenticações de usuários;

VI. Validação

a) validar as informações tratadas na triagem, ratificando-as, complementando-as ou retificando-as.

OBS.: Ações imediatas (fluxos de resposta).

A ETIR deverá encaminhar, tempestivamente, em função do tipo e do impacto, os dados relativos ao incidente cibernético para o Gestor de Segurança da Informação, os quais deverão ser analisados em conjunto com a Consultoria Jurídica do MDA, de forma que sejam adotadas as medidas legais, administrativas e cíveis cabíveis, incluindo a comunicação com as autoridades policiais competentes.

Havendo exfiltração de dados pessoais, o Encarregado pelo Tratamento de Dados Pessoais deverá informar o incidente à ANPD de acordo com os procedimentos previstos em legislação, normativos e orientações, bem como aos titulares dos dados, utilizando, sempre que aplicável, os formulários disponíveis nos Anexos I e II deste Plano.

e. Pós-incidente

O objetivo desta fase é realizar a análise da documentação dos incidentes e o processo de comunicação e verificar as regras de proteção do ambiente para evitar incidentes semelhantes e aperfeiçoar os processos existentes.

I. Comunicação Interna

Após o incidente cibernético devidamente tratado, deverá ser realizada a comunicação interna ao Ministério, no âmbito de todas as suas unidades organizacionais, de modo a informar acerca do incidente, bem como as ações tomadas para mitigação e as orientações pertinentes à sua prevenção.

II. Comunicação à Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC) e aos titulares e Comunicação a órgãos de resposta cibernética

Após o devido tratamento de um incidente cibernético ou ao encontrar dificuldades em mitigá-lo, deve-se realizar a comunicação à ReGIC. A comunicação de um incidente cibernético à ReGIC deve seguir procedimentos formais definidos pelo CTIR Gov. Os pontos principais a serem informados são:

- identificação do incidente: o evento deve ser caracterizado como incidente cibernético, ou seja, algo que comprometa ou ameace a confidencialidade, integridade ou disponibilidade de sistemas e informações;
- registro e descrição detalhada: é necessário elaborar relatório com informações claras, entre elas tipo de incidente, sistemas afetados, impacto percebido, medidas já adotadas e dados de contato da equipe responsável;

- canal oficial de comunicação: a notificação deve ser enviada ao CTIR Gov, que coordena a ReGIC, por meio do e-mail institucional cisc@gestao.gov.br; e
- agilidade e confidencialidade: a comunicação deve ser feita de forma imediata, garantindo sigilo das informações sensíveis e priorizando a resposta coordenada.

III. Melhoria contínua dos processos

No intuito de evoluir em maturidade e nas ações perante incidentes cibernéticos, a ETIR deverá realizar continuamente a análise dos processos de prevenção, detecção, tratamento e resposta ao incidente. Os principais objetivos da análise pós-incidente incluem:

- confirmar se a causa raiz foi eliminada ou mitigada;
- estabelecer medidas preventivas para incidentes similares;
- identificar os erros ou ausências de infraestrutura a serem resolvidos;
- identificar as oportunidades de melhoria na política organizacional, normativos ou nos processos;
- revisar e atualizar as funções, as responsabilidades, o processo de comunicação, considerando a autonomia da ETIR, para garantir a resposta oportuna e adequada;
- identificar necessidades de treinamento técnico ou operacional; e
- melhorar as ferramentas, ações e capacidades necessárias para realizar a prevenção, a detecção, o tratamento e a resposta.

A ETIR, em conjunto com o Gestor de Segurança da Informação, deverá atualizar as atividades preparatórias e os processos de prevenção, detecção, tratamento e resposta a partir das análises do pós-incidente, devendo:

- identificar IoCs ou TTPs da ameaça, encaminhando esses dados obrigatoriamente ao CTIR Gov, a fim de realizar ações colaborativas no âmbito da ReGIC;
- adicionar outros critérios para detecção e triagem da ameaça; e
- identificar e propor soluções para situações omissas verificadas no incidente.

4. Procedimentos específicos em caso de incidente com Dados Pessoais

Em caso de incidente que coloque em risco a segurança de dados pessoais, devem ser realizados os seguintes procedimentos específicos pela ETIR:

I. Avaliar internamente o incidente com o objetivo de obter informações iniciais sobre impacto do evento, natureza, categoria e quantidade de titulares de dados pessoais afetados, categoria e quantidade de dados afetados, consequências do incidente para os titulares e Ministério, criticidade e probabilidade e, ainda, preservar todas as evidências do incidente:

- **qual vulnerabilidade foi explorada no evento, abrangendo situações, tais 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 pela entidade, comprometimento de senhas de acesso, entre outras;
- **fonte dos dados pessoais:** verificar 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;
- **categoria de dados pessoais:** levantar dados sensíveis, dados pessoais de crianças e adolescentes;
- **extensão do vazamento:** quantificar os titulares e os dados pessoais que tiveram a sua segurança violada no evento;
- **avaliação do impacto ao titular:** avaliar quais são os impactos que o incidente pode gerar aos titulares;
- **avaliação do impacto no serviço:** avaliar os impactos que o incidente pode gerar ao MDA, como, por exemplo, perda de confiabilidade do cidadão, ações judiciais, danos à imagem do Ministério em âmbito nacional e internacional, prejuízo ao MDA em contratos com fornecedores e clientes e impacto total ou parcial nas atividades desenvolvidas pelo órgão.

Nesse cenário, todos os passos devem ser devidamente documentados, via processo SEI sigiloso e específico para esse fim, desde o momento inicial de atuação até a contenção e os efeitos. Isso inclui, mas não se limita a:

- todos os logs dos sistemas internos e externos envolvidos no incidente;
- interações das unidades organizacionais envolvidas e todas as medidas adotadas;
- eventuais contratações de ferramentas e equipes de especialistas e auditores para atuação pontual no incidente a ser tratado; e
- atas das reuniões relevantes.

II. Comunicar o Encarregado do MDA sobre a existência do incidente, caso envolva dados pessoais

III. Comunicar o Controlador (nos termos da LGPD) sobre a existência do incidente, considerando os seguintes papéis:

- o Operador, se existente, deve comunicar incidentes com dados pessoais ao Controlador o mais rápido possível, a fim de viabilizar que o Controlador exerça seu papel tempestivamente;
- o Controlador é responsável por comunicar incidentes com dados pessoais à ANPD, por meio do Encarregado, e aos titulares de dados, por meio da ETIR. Caso a relação entre Controlador e Operador seja feita em razão de contrato administrativo, tal obrigação de notificação tempestiva deve constar nas cláusulas contratuais, conforme a Instrução Normativa SGD/ME nº 31, de 23 de março de 2021;

- o Controlador é responsável por manter o registro do incidente de segurança, mesmo que não tenha sido comunicado à ANPD e aos titulares, conforme art. 10 da Resolução CD/ANPD nº 15/2024. Tal registro, a ser realizado pela ETIR, deverá conter minimamente os seguintes itens:

a) data de conhecimento do incidente;

b) descrição geral das circunstâncias em que o incidente ocorreu;

c) natureza e a categoria de dados afetados;

d) número de titulares afetados;

e) avaliação do risco e os possíveis danos aos titulares;

f) medidas de correção e mitigação dos efeitos do incidente, quando aplicável;

g) forma e conteúdo da comunicação, se o incidente tiver sido comunicado à ANPD e aos titulares; e

h) motivos da ausência de comunicação, quando for o caso.

IV. Comunicar à ANPD e ao titular de dados pessoais a existência do incidente. A comunicação à ANPD, pelo Encarregado, deverá ser feita nos moldes do Formulário contido no Anexo I, considerando o que se segue:

- a ANPD estipula o prazo de três dias úteis para comunicação de incidente de segurança a proteção de dados que será contado a partir do conhecimento pelo Controlador de que o incidente afetou os dados pessoais por ele tratados;
- o incidente deve ser comunicado pelo Controlador, por meio do Encarregado (acompanhado de documento comprobatório de vínculo contratual, empregatício ou funcional), ou por meio de representante constituído respeitando o prazo estabelecido;
- 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 ANPD poderá determinar ampla divulgação do incidente em meios de comunicação;
- os profissionais que estarão na linha de frente do atendimento dos impactados pelo evento devem ser capacitados para conseguir lidar, satisfatoriamente e com segurança, com os diferentes aspectos do incidente. Isso inclui, mas não se limita a responder às seguintes questões:

a) quais informações foram objeto do incidente?

b) o titular pode ser vítima de fraude em razão do incidente?

c) o incidente foi devidamente comunicado às autoridades?

d) o que o titular pode fazer em benefício da sua proteção?

e) onde o titular pode obter mais informações sobre o incidente?

- cabe ao Encarregado, diante das informações levantadas internamente e dos parâmetros estabelecidos pelo MDA, pela ANPD ou com base em boas práticas, avaliar a necessidade e a profundidade da comunicação com a ANPD e com os titulares de dados. Nessas tarefas, a LGPD e os demais normativos infralegais vigentes sobre proteção de dados pessoais deverão ser sempre consultados e utilizados como balizas;

- a ANPD 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 Agência através do formulário seguinte link: https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca;
- canais de comunicação de incidentes com dados pessoais:

a) ANPD: formulário de comunicação de incidentes disponível no link a seguir https://www.gov.br/anpd/pt-br/canais_atendimento/agente-detratamento/comunicado-de-incidente-de-seguranca-cis. CISC Gov.br - Centro Integrado de Segurança Cibernética do Governo Digital: e-mail para cisc@economia.gov.br;

b) CTIR Gov: e-mail para ctir@ctir.gov.br - a comunicação deve ser realizada preferencialmente pela equipe especializada (ETIR) seguindo os padrões de notificação de incidentes de segurança do CTIR Gov;

c) Polícia Federal: apenas quando houver indícios de crime, de acordo com a Lei nº 12.737, de 30 de novembro de 2012, ou outras normas presentes na legislação penal extravagante, a Polícia Federal deverá ser comunicada através de ofício diretamente enviado ao Diretor.

V. Comunicar ao CTIR GOV ao realizar a confirmação de um evento de incidente. Deve ser realizada a comunicação ao CTIR Gov e, se necessária, deve ser realizada ação conjunta entre o MDA e o CTIR Gov para a correspondente resolução.

VI. Notificar os titulares de dados pessoais, da seguinte forma:

- cabe ao Controlador, por meio da ETIR, comunicar ao titular dos dados pessoais a ocorrência de incidente de segurança que tenha potencial de lhe gerar riscos ou danos relevantes;
- paralelamente, a ETIR 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;
- a comunicação do incidente aos titulares deve ser feita em linguagem clara e simplificada, por meio do Formulário contido no Anexo II, mencionando, no que couber, os elementos previstos na legislação vigente, tais como:

a) descrição geral do incidente e a data da ocorrência;

b) natureza dos dados pessoais afetados e os riscos relacionados ao incidente com a identificação dos possíveis impactos aos titulares;

c) medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;

d) motivo da demora, no caso de a comunicação não ter sido feita no prazo determinado;

e) medidas tomadas e recomendadas para reverter ou mitigar os efeitos do incidente;

f) data do conhecimento do incidente de segurança;

g) contato do Encarregado ou o ponto de contato para que os titulares obtenham informações a respeito do incidente; e

h) outras informações que possam auxiliar os titulares a prevenirem possíveis danos;

- a comunicação deve ser feita de forma individual e diretamente aos titulares, sempre que possível. 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 sítio eletrônico, aplicativos, 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 três meses, conforme a Resolução CD/ANPD nº 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, em até três dias úteis, contados do término do prazo da comunicação ao titular.

VII. Extinguir o processo de comunicação do incidente: caso o problema tenha sido resolvido ou verificado que os dados pessoais não foram afetados, o processo de comunicação de incidente de segurança será declarado extinto. 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;
- após a realização da comunicação aos titulares e adoção das providências pertinentes pelo Controlador, em conformidade com a LGPD e as determinações da ANPD.

VIII. Emitir o relatório final com todas as informações coletadas, as ações realizadas para o tratamento efetivo do evento e as considerações necessárias para promover a melhoria contínua no atendimento de incidentes e para atualizar o Relatório de Impacto à Proteção de Dados Pessoais (RIPD), levando em consideração as seguintes orientações

- o RIPD poderá ser solicitado em casos específicos previstos na LGPD e descritos abaixo:

a) para tratamento de dados pessoais realizados para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (art. 4º, inciso III, da LGPD);

b) quando houver infração à LGPD em decorrência do tratamento de dados pessoais por órgãos públicos (art. 31 c/c art. 32 da LGPD); e

c) a qualquer momento, sob determinação da ANPD (art. 38).

- o MDA deverá implementar o processo de elaboração e manutenção do Inventário de Dados Pessoais (IDP), que deverá mostrar detalhes da utilização dos dados pessoais por diversos programas, sistemas de informação ou processos existentes. O IDP contribui para a avaliação das atividades que possam gerar impactos à proteção dos dados pessoais, a fim de verificar a necessidade de elaboração ou atualização do RIPD;
- além dos casos específicos previstos pela LGPD relativos à elaboração do RIPD, é indicada a elaboração ou atualização do Relatório de Impacto sempre que existir a possibilidade de ocorrer impacto na privacidade dos dados pessoais.

5. Glossário

Para auxílio na leitura deste Plano, serão adotadas as seguintes definições relacionadas a incidentes cibernéticos no âmbito da administração pública federal, as quais, em sua maioria, foram extraídas do Glossário do Gabinete de Segurança Institucional da Presidência da República (Portaria GSI/PR nº 93, de 18 de outubro de 2021) e de publicações e resoluções da Agência Nacional de Proteção de Dados (ANPD):

- **Agentes de Tratamento:**

a) CONTROLADOR: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

b) 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. Ex.: Controladoria conjunta ou co-Controladores).

- **ANONIMIZAÇÃO**: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.
- **ANPD**: Agência Nacional de Proteção de Dados Pessoais, autarquia de natureza especial vinculada ao Ministério da Justiça e Segurança Pública;
- **AMPLA DIVULGAÇÃO DO INCIDENTE EM MEIOS DE COMUNICAÇÃO**: providência que pode ser determinada pela ANPD ao Controlador, nos termos do art. 48, § 2º, I, da LGPD, no âmbito do processo de comunicação de incidente de segurança, como a publicação no sítio eletrônico, nas redes sociais do Controlador ou em outros meios de comunicação.

- **APF:** Administração Pública Federal.
- **CATEGORIA DE DADOS PESSOAIS:** classificação dos dados pessoais de acordo com o contexto de sua utilização, tais como dados de identificação pessoal, dados de autenticação em sistemas e dados financeiros.
- **COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA**: ato do Controlador que comunica à ANPD e ao titular de dados a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.
- **CTIR Gov:** Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov), integrante do Departamento de Segurança de Informação e Cibernética (DSIC) da Secretaria de Segurança da Informação e Cibernética (SSIC) do Gabinete de Segurança Institucional (GSI) da Presidência da República (PR). É responsável por coordenar e integrar as ações de gestão de incidentes de Tecnologia da Informação (TI) no âmbito da APF, abrangendo incidentes de segurança da informação e de privacidade. Nos casos de incidentes em redes computacionais, devem ser observadas as diretrizes da Norma Complementar nº 21/IN01/DSIC/GSIPR, de 8 de outubro de 2014, relativas ao registro, à coleta e à preservação de evidências, bem como à comunicação às autoridades competentes.
- **DADO DE AUTENTICAÇÃO EM SISTEMAS:** dado pessoal utilizado como credencial para permitir acesso a sistemas ou para confirmar a identificação de usuário, tais como contas de login, tokens e senhas.

- **DADO FINANCEIRO:** dado pessoal relacionado às transações financeiras do titular, inclusive para contratação de serviços e aquisição de produtos.
- **DADO PESSOAL:** toda informação relacionada a pessoa natural identificada ou identificável.
- **DADO PESSOAL AFETADO:** dado pessoal cuja confidencialidade, integridade, disponibilidade ou autenticidade tenha sido comprometida em um incidente de segurança.
- **DADOS PROTEGIDOS POR SIGILO LEGAL OU JUDICIAL:** dado pessoal cujo sigilo decorra de norma jurídica ou decisão judicial.
- **DADO PROTEGIDO POR SIGILO PROFISSIONAL**: dado pessoal protegido pelo sigilo decorrente do exercício de cargo ou função, ofício ou profissão, cuja revelação possa produzir dano a outrem.
- **ENCARREGADO:** pessoa indicada pelo Controlador ou Operador para atuar como canal de comunicação entre o Controlador, os titulares dos dados e a ANPD.
- **ETIR:** Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos dos órgãos e entidades que compõem a APF.
- **EXFILTRAÇÃO DE DADOS:** movimento não autorizado de dados, também chamado de data exfil, exportação de dados, extrusão de dados, vazamento de dados e roubo de dados.
- **GSI:** Gabinete de Segurança Institucional da Presidência da República, responsável pela assistência direta ao Presidente da República no desempenho de suas atribuições, especialmente quanto aos assuntos militares e de segurança.
- **IDP:** Inventário de Dados Pessoais, instrumento destinado a documentar o tratamento de dados pessoais realizados pela instituição, em conformidade com o art. 37 da LGPD.

- **INCIDENTE:** interrupção não planejada ou redução da qualidade de um serviço, ou seja, ocorrência, 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 a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;
- **INCIDENTE CIBERNÉTICO:** ocorrência que pode comprometer, real ou potencialmente, a disponibilidade, a integridade, a confidencialidade ou a autenticidade de sistema de informação ou das informações processadas, armazenadas ou transmitidas por esse sistema. Poderá também ser caracterizada pela tentativa de exploração de vulnerabilidade de sistema de informação que caracterize violação de norma, política de segurança, procedimento de segurança ou política de uso. De maneira geral, os tipos de atividades comumente reconhecidas como incidentes cibernéticos são: a) tentativas de obter acesso não-autorizado a um sistema ou a dados armazenados; b) tentativa de utilização não-autorizada de sistemas para a realização de atividades de processamento ou armazenamento de dados; c) mudanças não-autorizadas de firmware, hardware ou software em um ambiente computacional; d) ataques de negação de serviço (DoS); e e) demais ações que visem afetar a disponibilidade ou integridade dos dados.

- **INCIDENTE COM DADOS EM LARGA ESCALA**: ocorrência que abrange número significativo de titulares, considerando o volume de dados afetados, a duração, a frequência e a extensão geográfica de localização dos titulares.
- **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:** evento adverso confirmado que comprometa a confidencialidade, integridade ou disponibilidade de dados pessoais. Pode decorrer de ações voluntárias ou acidentais que resultem em divulgação, alteração, perda ou acesso não autorizado a dados pessoais, independentemente do meio em que estão armazenados.
- **LGPD:** Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais, destinada à proteção dos direitos fundamentais de privacidade e de liberdade de cada indivíduo.
- **MEDIDAS DE SEGURANÇA:** medidas técnicas e/ou administrativas adotadas para proteger os dados pessoais contra acessos não autorizados e contra situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.
- **NATUREZA DOS DADOS PESSOAIS:** classificação dos dados pessoais, nos termos da LGPD, em dados pessoais e dados pessoais sensíveis.

- **PROCESSO DE COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA:** processo administrativo instaurado no âmbito da ANPD que pode abranger o procedimento de comunicação de incidente de segurança e/ou procedimento de apuração de incidente de segurança não comunicado, com vistas à análise, fiscalização e eventual responsabilização.
- **RELATÓRIO DO INCIDENTE:** documento elaborado pelo Controlador que contém cópias, em meio físico ou digital, de dados e informações relevantes para descrever o incidente e as providências adotadas para reverter ou mitigar os seus efeitos.
- **ReGIC:** Rede Federal de Gestão de Incidentes Cibernéticos que tem como finalidade o fortalecimento da cooperação e parceria do Governo Federal com os entes federativos, a sensibilização dos órgãos e da população em geral para a necessidade de segurança cibernética e elevação da maturidade da sociedade brasileira em segurança da informação e cibernética.
- **RELATÓRIO FINAL:** documento conclusivo que consolida as evidências, ações e resultados obtidos no tratamento do incidente.
- **RIPD:** Relatório de Impacto à Proteção de Dados Pessoais, documentação do Controlador, no qual são descritos os processos de tratamento de dados pessoais, que identificam os riscos às liberdades civis e aos direitos fundamentais dos titulares, as medidas de salvaguarda, bem como mecanismos de mitigação de riscos.

- **SGD:** Secretaria de Governo Digital, responsável pela definição de políticas e diretrizes, por orientar normativamente e supervisionar as atividades de gestão dos recursos de tecnologia da informação e comunicação do sistema.

Anexo I – Formulário de Comunicação de Incidente de Segurança com Dados Pessoais à ANDP

Formulário de Comunicação de Incidente de Segurança com Dados Pessoais à ANAP

Dados do Controlador	
Razão Social/Nome:	
CNPJ/CPF:	
Endereço:	
Cidade:	Estado:
CEP:	
Telefone:	E-mail:
Dados do Encarregado	
Possui um Encarregado pela proteção de dados:	☐ 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 em até 30 dias corridos da comunicação preliminar.
☐ Complementar	Complementação de informações prestadas em 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.

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 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 ANDP
Quando comunicou aos titulares
Justifique, se cabível, a não realização da comunicação à ANDP 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:

Da Comunicação do Incidente aos Titulares dos Dados	
Os titulares dos dados afetados foram comunicados sobre o incidente?	
☐ Sim.	☐ Não, por não haver risco ou dano relevante a eles.
☐ Não, mas o processo de comunicação está em andamento.	☐ 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.)	☐ Anúncio público no sítio eletrônico, mídias sociais ou aplicativos do controlador.
☐ Comunicado individual por escrito com confirmação de recebimento. (mensagem eletrônica / carta / e-mail / etc.)	☐ Ampla divulgação do fato em meios de comunicação, por iniciativa do controlador. (especifique abaixo)
☐ Outros. (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 par 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.

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?

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	☐ Genética
☐ Referente à vida sexual	☐ Filiação a organização sindical, religiosa, filosófica ou política.	

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

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

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

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
Qual a quantidade aproximada de titulares afetados pelo incidente?
Quais a categorias de titulares foram afetadas pelo incidente?

☐ 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?		
☐ 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?
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 de dados foram aplicados:

Antes do incidente, quais das seguintes medidas de segurança eram adotadas?

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

- ☐ Políticas de segurança da informação e privacidade.
- ☐ Controle de acesso físico.
- ☐ Criptografia/Anonimiza-ção.
- ☐ Antivírus.
- ☐ Registros de acesso (logs).
- ☐ Processo de Gestão de Riscos.
- ☐ Controle de acesso lógico.
- ☐ Cópias de segurança. (backups)
- ☐ Firewall.
- ☐ Monitoramento de uso de rede e sistemas.
- ☐ Registro de incidentes.
- ☐ Segregação de rede.
- ☐ Gestão de ativos.
- ☐ Atualização de Sistemas.
- ☐ Múltiplos fatores de autenticação.

☐ Testes de invasão.	☐ Plano de resposta a incidentes.	☐ Outras (especifique).
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>

Anexo II – Formulário de Comunicação ao Titular de Dados Pessoais

Formulário de Comunicação de Incidente de Segurança com Dados Pessoais à ANAP

Da Comunicação Individual do Incidente aos Titulares dos Dados
Data de ocorrência do incidente
Data do conhecimento do incidente
Resumo da ocorrência do incidente
Descrição dos dados pessoais afetados
Medidas técnicas e de segurança utilizadas previamente para a proteção dos dados
Riscos e impactos (consequências) ao titular de dados pessoais

Medidas adotadas para reverter ou mitigar os efeitos do incidente
Dados do Controlador
Nome:
E-mail:

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

<ASSINATURA>

www.gov.br/mda

MINISTÉRIO DO DESENVOLVIMENTO AGRÁRIO E AGRICULTURA FAMILIAR
Esplanada dos Ministérios, Bloco C, 5° andar
CEP: 70046-900 Brasília/DF
Tel.: (61) 3218-3077 • (61) 3218-4175