MANUAL DE SEGURANÇA DA INFORMAÇÃO

da Ouvidoria do MAPA



Ministério da Agricultura e Pecuária

Ministério da Agricultura e Pecuária - MAPA
Ouvidoria

MANUAL DE SEGURANÇA DA INFORMAÇÃO DA OUVIDORIA DO MAPA

Missão do Mapa:
Promover o desenvolvimento sustentável
das cadeias produtivas agropecuárias,
em benefício da sociedade brasileira

Brasília
Mapa
2026

1ª edição. Ano 2026

Elaboração, distribuição, informações:

Ministério da Agricultura e Pecuária

Gabinete do Ministro de Estado

Ouvidoria

Endereço: Ministério da Agricultura e Pecuária, Esplanada dos Ministérios, Bloco D - Térreo, CEP: 70043-900 Brasília - DF

Telefone: (61) 3218-2089

E-mail: ouvidoria@agro.gov.br

Editorial e Coordenação: Ouvidoria

Colaboração: Subsecretaria de Tecnologia da Informação - STI

Permitida a reprodução sem fins lucrativos, parcial ou total, por qualquer meio, se citada a fonte e o sítio da Internet onde pode ser encontrado o original (www.gov.br/agricultura).

Catalogação na Fonte
Biblioteca Nacional de Agricultura – BINAGRI

Dados Internacionais de Catalogação na Publicação (CIP)
Biblioteca Nacional de Agricultura – BINAGRI

Brasil. Ministério da Agricultura e Pecuária.

Manual de Segurançada Informaçãoda Ouvidoria do MAPA. / Ministério da Agricultura e Pecuária. Gabinete do Ministro de Estado da Agricultura e Pecuária. Ouvidoria. – Brasília : MAPA, 2026.

40 p. : il. color.

ISBN 978-85-7991-292-4

1.Segurança da informação. 2. Proteção de dados. 3. Ouvidoria. 4. Governança pública. 5. Acesso à informação. I. Ministério da Agricultura e Pecuária. II.Gabinete do Ministro de Estado da Agricultura e Pecuária. III. Ouvidoria. IV. Título.

AGRIS: E50
CDU: 004.056:35

Bibliotecária: Layla Alexandrina Barboza dos Santos (CRB1/ 3447)

INSTITUCIONAL

LUIZ INÁCIO LULA DA SILVA
Presidente da República

ANDRÉ CARLOS ALVES DE PAULA FILHO
Ministro de Estado da Agricultura e Pecuária

CLEBER OLIVEIRA SOARES
Secretário-Executivo

GUILHERME CAMPOS JÚNIOR
Secretário de Política Agrícola

CARLOS GOULART
Secretário de Defesa Agropecuária

AUGUSTO LUIS BILLI
Secretário de Comércio e Relações Internacionais

CLECIVALDO DE SOUSA RIBEIRO
Secretário de Desenvolvimento Rural

SIBELLE DE ANDRADE SILVA
Assessora Especial do Gabinete do Ministério da Agricultura e Pecuária

CARLA MADEIRA GONÇALVES SIMÕES DOS REIS
Chefe da Assessoria Especial de Comunicação Social do Ministério da Agricultura e Pecuária

MARIA DAS GRAÇAS GONÇALVES SALLES
Ouvidora do Ministério da Agricultura e Pecuária

JULIA GUERREIRO
Coodenadora de Ouvidoria do Ministério da Agricultura e Pecuária

PATRICIA DIAS DE BRITO
Coordenadora de Monitoramento e Qualidade dos Serviços da Ouvidoria do Ministério da Agricultura e Pecuária

ANA LÚCIA APARECIDA DA SILVA
Coordenadora do Serviço de Informação ao Cidadão do Ministério da Agricultura e Pecuária

SUMÁRIO

1. Boas Vindas 6
2. Objetivo geral 7
   2.1 Objetivos específicos 7
3. Metodologia de elaboração 8
4. Segurança da informação no tratamento das manifestações 9
   4.1 Segurança no acesso aos sistemas 10
      4.1.1 Controle de acesso ao Drive, ao Córtex e aos Painéis Internos da Ouvidoria 11
      4.1.2 Acesso externo pelo agente público participante do PGD ou atividades remotas 12
   4.2 Segurança na leitura e análise inicial 14
   4.3 Segurança no registro das manifestações e dos pedidos de acesso à informação 15
      4.3.1 Segurança no recebimento e conferência dos anexos 15
   4.4 Segurança na tramitação das manifestações de Ouvidoria 16
      4.4.1 Segurança na tramitação dos pedidos de acesso à informação 16
   4.5 Segurança do tratamento das denúncias 17
      4.5.1 Técnicas de proteção dados pessoais e outras informações sensíveis 17
   4.6 Segurança no tratamento de manifestações de Ouvidoria e dos pedidos de acesso à informação recebidos por e-mail 18
   4.7 Segurança da informação no atendimento por videoconferência 19
   4.8 Segurança da informação na elaboração e envio das respostas às manifestações 20
   4.9 Segurança da informação no tratamento de manifestações de ouvidoria ou pedidos de acesso à informação recebidos ou tratados pelo SEI 21
   4.10 Segurança da informação no atendimento presencial 22
   4.11 Segurança da informação no atendimento telefônico 23
   4.12 Guarda, retenção e descarte seguro de informações e documentos 24
5. Comunicação de erros e incidentes de segurança da informação 25
6. Uso de inteligência artificial nas atividades da Ouvidoria 28
7. Regras gerais de segurança da informação 30
   7.1 Deveres dos Agentes Públicos 31
   7.2 Tratamento e proteção das informações 32
   7.3 Segurança dos ambientes e dos recursos institucionais 33
8. Vigência, revisão e atualização do Manual 35
Anexo 36
Referências 40



1. BOAS VINDAS

Este Manual reúne orientações destinadas aos agentes públicos que atuam na Ouvidoria do MAPA. Sua observância contribui para prevenir acessos indevidos, perda, alteração, indisponibilidade ou divulgação não autorizada de informações.

A proteção das informações é indispensável à atuação da Ouvidoria, que trata dados pessoais, documentos e relatos cujo acesso deve ser limitado às pessoas autorizadas e conforme a necessidade de conhecimento. O conteúdo poderá ser atualizado em razão de alterações normativas, adoção de novas tecnologias ou identificação de novos riscos.

Para fins deste Manual, as orientações aplicam-se a servidores, empregados, terceirizados, estagiários e demais colaboradores que, em razão de suas atividades, tenham acesso a informações, sistemas ou outros ativos da Ouvidoria.



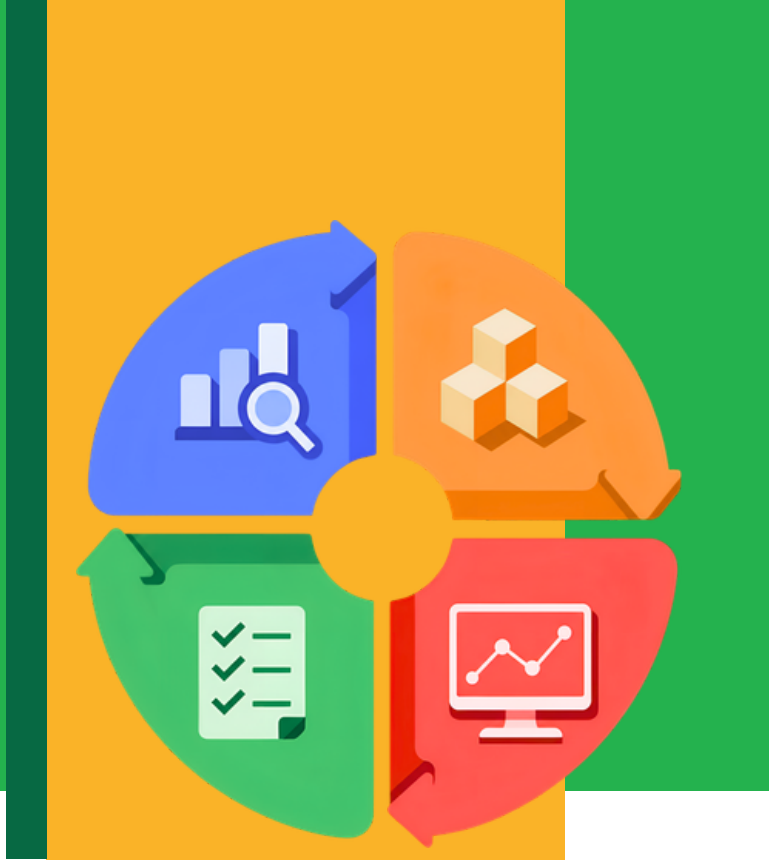
2. OBJETIVO GERAL

Orientar os agentes públicos que atuam na Ouvidoria do Ministério da Agricultura e Pecuária — MAPA quanto à aplicação das normas e das boas práticas de segurança da informação, de modo a proteger as informações institucionais, os dados pessoais, a identidade dos manifestantes e o conteúdo das manifestações.

2.1 OBJETIVOS ESPECÍFICOS

Este Manual tem como objetivos específicos:

- apresentar as normas e as boas práticas de segurança da informação aplicáveis às atividades da Ouvidoria;
- orientar o uso seguro dos canais de atendimento, sistemas, equipamentos e ferramentas de apoio;
- estabelecer cuidados para o acesso, a produção, o manuseio, o armazenamento, o compartilhamento e o descarte de informações e documentos;
- orientar a proteção dos dados pessoais, da identidade dos manifestantes e das informações submetidas a restrição de acesso; e
- indicar medidas de prevenção e de comunicação de erros, vulnerabilidades e incidentes de segurança da informação.



3. METODOLOGIA DA ELABORAÇÃO

Este Manual foi elaborado com base em pesquisa documental e na análise das atividades da Ouvidoria, com foco nos riscos relacionados ao acesso, ao uso, ao armazenamento, ao compartilhamento e à divulgação das informações.

Foram examinadas normas, políticas, manuais, guias, cartilhas e orientações oficiais sobre ouvidoria, proteção de dados pessoais, segurança da informação e uso de inteligência artificial na Administração Pública, especialmente a Política de Segurança da Informação do MAPA — PoSIC/MAPA e seus atos complementares.

As orientações foram organizadas segundo os canais, os sistemas e os ambientes utilizados pela Ouvidoria. O conteúdo foi revisto para assegurar conformidade normativa, clareza, uniformidade terminológica e aplicabilidade às atividades da unidade.

4. SEGURANÇA DA INFORMAÇÃO NO TRATAMENTO DAS MANIFESTAÇÕES



A segurança da informação deverá ser observada durante todo o tratamento das manifestações de ouvidoria e dos pedidos de acesso à informação. A proteção abrange o relato, os dados do manifestante e das pessoas mencionadas, os anexos, as informações obtidas durante a análise e os documentos produzidos pela Ouvidoria ou por outras unidades.

O acesso deverá ser restrito aos agentes públicos autorizados e limitado ao necessário para o exercício de suas atribuições, conforme o princípio da necessidade de conhecer. A consulta por interesse pessoal, curiosidade ou finalidade alheia à atividade constitui uso indevido da informação.

Deverão ser preservadas a confidencialidade, a integridade, a disponibilidade e a autenticidade das informações, bem como a rastreabilidade das ações realizadas nos sistemas institucionais.

ATENÇÃO!

Os acessos e as ações realizadas nos sistemas institucionais são registrados. As trilhas de auditoria poderão ser analisadas pelas unidades competentes na apuração de incidentes de segurança da informação e de acessos incompatíveis com as atribuições do agente público.

4.1 SEGURANÇA NO ACESSO AOS SISTEMAS

O acesso aos sistemas utilizados nas atividades da Ouvidoria é pessoal e deverá ser realizado por credencial individual e intransferível, conforme o mecanismo de autenticação definido para cada sistema, inclusive conta gov.br quando aplicável.

ATENÇÃO!

Antes de receber acesso ao sistema, o agente público deverá ler e assinar o Termo de Ciência e Responsabilidade. O perfil concedido deverá ser compatível com as atividades exercidas e limitado às funcionalidades necessárias.

Alterações funcionais, substituições, afastamentos e desligamentos que exijam modificação ou inativação do acesso deverão ser comunicados imediatamente à chefia ou à Ouvidoria.

Ao acessar os sistemas, o agente público deverá:

- conferir o endereço oficial dos sistemas antes de inserir as credenciais;
- proteger a senha e impedir seu armazenamento em local visível, arquivo desprotegido ou navegador de uso compartilhado;
- bloquear a tela sempre que se afastar do equipamento;
- manter abertas apenas as manifestações necessárias à atividade em execução;
- evitar a exposição de documentos, arquivos e anotações;
- encerrar a sessão ao concluir o trabalho; e
- comunicar imediatamente qualquer indício de acesso indevido, perda de credenciais ou comprometimento da conta.

É vedado acessar os sistemas com a conta de outro usuário ou permitir que terceiros utilizem uma sessão autenticada. As ações realizadas nos sistemas ficam vinculadas ao respectivo usuário.

4.1.1 CONTROLE DE ACESSO AO DRIVE, AO CÓRTEX E AOS PAINÉIS INTERNOS DA OUVIDORIA

O acesso às pastas do Drive da Ouvidoria deverá observar a necessidade de conhecer e ser compatível com as atribuições desempenhadas em cada unidade. As permissões deverão ser concedidas somente às pastas e aos conteúdos necessários ao exercício das atividades da respectiva unidade.

Os acessos concedidos aos agentes públicos deverão ser revistos sempre que houver alteração de suas atribuições ou da unidade de exercício. Em eventual movimentação interna entre unidades da própria Ouvidoria, as permissões deverão ser ajustadas, com a remoção dos acessos vinculados à unidade de origem que deixarem de ser necessários e a concessão daqueles compatíveis com as atividades desempenhadas na unidade de destino.
Quando o agente público deixar de atuar na Ouvidoria, todos os acessos às pastas do Drive da Ouvidoria deverão ser removidos.

O mesmo princípio deverá ser observado em relação ao Cortex da Ouvidoria, aplicação desenvolvida no Power Apps e utilizada pela unidade como espaço de compartilhamento e consulta de informações relacionadas às atividades das equipes, funcionando como base interna de conhecimento. Cada unidade da Ouvidoria responsável pelo tratamento de demandas dispõe de um Cortex próprio, cujos acessos deverão ser concedidos de acordo com a necessidade de conhecer e as atribuições desempenhadas pelo agente público.

Em eventual movimentação interna entre unidades da própria Ouvidoria, os acessos ao Cortex deverão ser ajustados, com a remoção das permissões relacionadas à unidade de origem que deixarem de ser necessárias e a concessão daquelas correspondentes à unidade de destino. Quando o agente público deixar de atuar na Ouvidoria, os acessos ao Cortex deverão ser removidos.

Os painéis internos utilizados pela Ouvidoria para acompanhamento, monitoramento ou gestão de informações deverão ter acesso restrito aos agentes públicos cuja atuação justifique a consulta às informações neles disponibilizadas. As permissões deverão observar a necessidade de conhecer e ser revistas sempre que houver alteração das atribuições, movimentação interna entre unidades da própria Ouvidoria ou desligamento.

Essa restrição não se aplica aos painéis de acesso público, disponibilizados na página institucional do MAPA ou em outros canais oficiais, cuja finalidade seja permitir a consulta das informações pela sociedade.

ATENÇÃO!

A concessão, a revisão, o ajuste e a remoção de acessos ao Drive, ao Cortex, aos painéis internos e a outros ambientes ou recursos informacionais de uso restrito da Ouvidoria deverão observar a necessidade de conhecer para o exercício das atribuições. As movimentações, alterações de atribuições, afastamentos ou desligamentos que repercutam nas permissões concedidas deverão ser comunicados tempestivamente à chefia da unidade e aos responsáveis pela gestão dos respectivos acessos, para adoção das providências necessárias.

Os responsáveis pela gestão dos acessos deverão realizar periodicamente a revisão das permissões concedidas, de modo a identificar e remover acessos que deixaram de ser necessários ou compatíveis com as atribuições atuais.

4.1.2 ACESSO EXTERNO PELO AGENTE PÚBLICO PARTICIPANTE DO PGD OU ATIVIDADES REMOTAS

O agente público participante do Programa de Gestão e Desempenho — PGD ou em eventual atividade remota deverá acessar os sistemas fora das dependências do MAPA utilizando equipamento institucional ou, quando admitido pelas normas do MAPA, equipamento pessoal que atenda aos requisitos de segurança aplicáveis, conexão privada e segura e ambiente que assegure a proteção das informações.

Durante o acesso externo, o agente público deverá:

- manter atualizados o sistema operacional, o navegador, o antivírus e os demais recursos de proteção;
- utilizar conta de usuário individual, protegida por senha ou outro mecanismo seguro de autenticação, e manter habilitado o bloqueio automático da tela;
- acessar os sistemas somente pelo endereço oficial e utilizar os mecanismos institucionais de acesso remoto, quando exigidos;
- utilizar rede privada e protegida por senha, vedado o uso de redes públicas, abertas ou de procedência desconhecida;
- trabalhar em local reservado e impedir que pessoas não autorizadas ouçam conversas, visualizem a tela ou acessem documentos e anotações;
- utilizar fones de ouvido em reuniões ou na reprodução de arquivos de áudio;
- não salvar arquivos das manifestações no equipamento pessoal, em serviço particular de nuvem ou em pasta particular sincronizada automaticamente;
- realizar download somente quando indispensável e eliminar a cópia local de forma segura após a utilização; e
- encerrar a sessão e fechar os documentos ao concluir a atividade.

ATENÇÃO!
Se o equipamento, a conexão ou o ambiente não oferecerem condições adequadas de segurança e privacidade, o agente público não deverá acessar os sistemas nem tratar informações relacionadas às manifestações.

4.2 SEGURANÇA NA LEITURA E ANÁLISE INICIAL

A leitura das manifestações de ouvidoria e dos pedidos de acesso à informação deverá ocorrer em ambiente reservado, com a tela protegida da visualização por visitantes, usuários atendidos ou outras pessoas não autorizadas.

Durante a leitura e a análise, o agente público deverá:

- manter abertas apenas as manifestações necessárias à atividade;
- não ler o conteúdo em voz alta em ambiente compartilhado;
- não fotografar nem capturar a tela, salvo quando indispensável a procedimento institucional e realizado em ambiente autorizado;
- não copiar informações para anotações pessoais;
- imprimir documentos somente quando indispensável, com guarda e descarte seguros;
- identificar dados pessoais, dados pessoais sensíveis, informações submetidas a restrição de acesso e elementos que possam revelar a identidade do manifestante; e
- examinar os anexos, inclusive nomes de arquivos, assinaturas, imagens, voz, propriedades e metadados.

A ausência de identificação no cadastro não impede a identificação indireta. Cargo, função, unidade, local de trabalho, datas, horários, relações funcionais ou pessoais, voz, imagens e outras circunstâncias podem revelar a pessoa envolvida.

ATENÇÃO!
Havendo risco de exposição indevida ou dúvida quanto ao tratamento seguro das informações, a atividade deverá ser suspensa até a adoção das medidas de proteção cabíveis ou a obtenção de orientação da chefia.

4.3 SEGURANÇA NO REGISTRO DAS MANIFESTAÇÕES E DOS PEDIDOS DE ACESSO À INFORMAÇÃO

O registro deverá ser realizado no sistema, com uso apenas dos dados necessários à finalidade institucional. Informações pessoais não deverão ser repetidas no relato, exceto em casos que sejam imprescindíveis para o tratamento da manifestação ou do pedido de acesso à informação, nem utilizadas ou compartilhadas para finalidade incompatível, sem necessidade funcional ou fundamento legal.

O conteúdo registrado deverá permanecer fiel às informações recebidas, sem acréscimo de interpretações ou de dados que ampliem desnecessariamente a exposição do manifestante ou de terceiros. Os arquivos deverão ser conferidos antes de sua inserção no respectivo sistema.

4.3.1 SEGURANÇA NO RECEBIMENTO E CONFERÊNCIA DOS ANEXOS

Os anexos deverão ser recebidos por canais institucionais e permanecer vinculados às manifestações. É vedado solicitar ou receber arquivos por conta pessoal de correio eletrônico, aplicativo de mensagens, serviço particular de armazenamento em nuvem ou outro meio não autorizado pelo MAPA.

Antes de abrir ou compartilhar um anexo, o agente público deverá conferir o nome, o formato e a extensão do arquivo, observar alertas de segurança e identificar dados pessoais, informações restritas e elementos que possam revelar a identidade do manifestante.

4.4 SEGURANÇA NA TRAMITAÇÃO DAS MANIFESTAÇÕES DE OUVIDORIA

Para o tratamento das manifestações de Ouvidoria a tramitação deverá ocorrer pelo módulo próprio do Fala.BR, que permite controlar o acesso, registrar as ações realizadas e manter o histórico do tratamento. Informações protegidas não deverão ser encaminhadas por correio eletrônico, Teams, aplicativos de mensagens, pastas compartilhadas ou outros meios não previstos para essa finalidade.

Antes do compartilhamento pelo Fala.BR, deverão ser conferidos a unidade e os destinatários selecionados, a necessidade das informações enviadas, a existência de dados que exijam proteção e a limitação do acesso às pessoas autorizadas.

Não deverão ser mantidas cópias da manifestação para acompanhamento pessoal. Controles auxiliares, quando necessários, deverão conter apenas os dados indispensáveis e permanecer em ambiente institucional com acesso restrito.

4.4.1 SEGURANÇA NA TRAMITAÇÃO DOS PEDIDOS DE ACESSO À INFORMAÇÃO

Para o tratamento dos pedidos de acesso à informação, a tramitação deverá ocorrer por meio de processo próprio no Sistema Eletrônico de Informações – SEI, com nível de acesso restrito observadas as regras de proteção aplicáveis ao teor do pedido inserido no formulário específico do Serviço de Informação ao Cidadão e aos documentos que integram o processo.

Não deverão ser mantidas cópias do pedido de acesso à informação ou dos documentos que o instruem para acompanhamento pessoal. Controles auxiliares, quando necessários, deverão conter apenas os dados indispensáveis ao acompanhamento do pedido e permanecer em ambiente institucional com acesso restrito.

4.5 SEGURANÇA NO TRATAMENTO DAS DENÚNCIAS

A denúncia exige proteção reforçada. Os elementos que permitam identificar direta ou indiretamente o denunciante deverão ter acesso restrito e ser preservados desde o recebimento, nos termos da legislação aplicável.

A proteção não se limita ao nome, CPF, endereço ou dados de contato. Conforme o contexto, cargo, função, local de trabalho, relações funcionais ou pessoais, datas, horários, assinatura, matrícula, endereço eletrônico, imagem, voz, propriedades de arquivos, metadados, narrativa em primeira pessoa e circunstâncias conhecidas por grupo reduzido também podem revelar a identidade.

O acesso à identidade deverá ser limitado aos agentes públicos que necessitem conhecê-la para o exercício de suas atribuições. Eventual compartilhamento não afasta a restrição de acesso nem autoriza a utilização dos dados para outra finalidade.

4.5.1 TÉCNICAS DE PROTEÇÃO DE DADOS PESSOAIS E OUTRAS INFORMAÇÕES SENSÍVEIS

PSEUDOMINIZAÇÃO

A pseudonimização retira a possibilidade de associação direta ou indireta do dado a uma pessoa, salvo mediante informação adicional mantida separadamente em ambiente controlado e seguro. O conteúdo original permanece protegido no Fala.BR, com acesso restrito.

O procedimento deverá abranger campos cadastrais, relato, anexos, imagens, gravações de áudio ou vídeo, propriedades, metadados e outros elementos que permitam a identificação. A retirada desses elementos não deverá comprometer as informações necessárias à compreensão dos fatos.

ANONIMIZAÇÃO

A anonimização consiste na 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.

Antes da utilização de informações anonimizadas em relatórios, estudos, apresentações ou estatísticas, deverá ser avaliado o risco de reidentificação pela combinação de dados, especialmente em grupos reduzidos ou situações específicas. O conteúdo original deverá permanecer protegido pelo período aplicável.

EXTRATO

O extrato consiste em preservar a identidade do manifestante e/ou dados sensíveis, retirando qualquer elemento que permita a associação, direta ou indireta, ao cidadão, tratando-se de uma ação prévia à tramitação da manifestação para unidades internas do MAPA ou encaminhamento para órgão externo, quando cabível.

ATENÇÃO

É vedado inserir relatos ou documentos das manifestações em serviços externos ou ferramentas não autorizadas pelo MAPA, inclusive plataformas de conversão, edição, tradução, compactação, desbloqueio ou tarjamento de arquivos, como o iLovePDF e serviços similares.

4.6 SEGURANÇA NO TRATAMENTO DE MANIFESTAÇÕES DE OUVIDORIA E DOS PEDIDOS DE ACESSO À INFORMAÇÃO DOS RECEBIDOS POR E-MAIL

As mensagens deverão ser tratadas exclusivamente pela conta institucional da unidade. É vedado utilizar contas pessoais, aplicativos de mensagens, dispositivos particulares ou serviços externos não autorizados para receber, responder, armazenar ou compartilhar relatos e anexos.

Antes de abrir arquivos ou acessar links, o agente público deverá verificar a relação da mensagem com as atividades da Ouvidoria e observar indícios de fraude ou conteúdo malicioso. Havendo alerta ou suspeita, o conteúdo não deverá ser aberto, baixado, executado ou encaminhado.

Mensagens e anexos que contenham dados identificadores ou informações protegidas não deverão ser retransmitidos sem a adoção das salvaguardas cabíveis. Cópias desnecessárias deverão ser eliminadas de forma segura.

4.7 SEGURANÇA DA INFORMAÇÃO NO ATENDIMENTO POR VIDEOCONFERÊNCIA

O atendimento por videoconferência deverá ocorrer por plataforma e conta institucionais, mediante conexão privada e segura. O agente público deverá permanecer em ambiente reservado e impedir que pessoas não autorizadas ouçam a conversa, visualizem a tela ou acessem documentos e informações.

Durante o atendimento, o agente público deverá:

- utilizar fones de ouvido quando houver comunicação por áudio;
- evitar o compartilhamento de tela e, quando indispensável, exibir somente o conteúdo necessário;
- receber arquivos exclusivamente pelos canais institucionais definidos e observar os alertas antes de abri-los;
- não acessar links suspeitos nem executar programas enviados pelo usuário;
- não utilizar contas pessoais, aplicativos de mensagens, redes públicas ou plataformas não autorizadas;
- não realizar fotografias, capturas de tela ou gravações por iniciativa própria; e
- encerrar a videoconferência e fechar os documentos ao término do atendimento.

A gravação da videoconferência, quando admitida e previamente consentida, deverá ser armazenada em ambiente institucional protegido, com acesso restrito e pelo período necessário à finalidade que justificou sua produção. Registros temporários deverão ser eliminados com segurança quando deixarem de ser necessários.

ATENÇÃO!
Se o ambiente ou o canal não oferecer condições adequadas de segurança e privacidade, o atendimento por videoconferência deverá ser interrompido e retomado somente após o restabelecimento dessas condições.

4.8 SEGURANÇA DA INFORMAÇÃO NA ELABORAÇÃO E ENVIO DAS RESPOSTAS ÀS MANIFESTAÇÕES

Antes do envio, a resposta e seus anexos deverão ser revistos para evitar a divulgação de dados pessoais, identidade de denunciantes, testemunhas ou terceiros, comentários, marcações e histórico de revisão.

Ressalta-se que ao agente da Ouvidoria caberá realizar a conferência da resposta no âmbito de suas atribuições, não lhe competindo substituir a unidade responsável na análise técnica do conteúdo, na identificação de informações cuja proteção dependa de conhecimento especializado ou na definição da existência de sigilo ou restrição de acesso de responsabilidade da unidade produtora ou custodiante da informação.

Deverão ser conferidos o destinatário, a manifestação correspondente e os anexos selecionados. A resposta deverá ser disponibilizada pelo canal institucional previsto, vedado o envio por conta pessoal de correio eletrônico, aplicativo de mensagens ou outro meio não autorizado.

Quando o compartilhamento por link for necessário, deverá ser utilizado exclusivamente o serviço de nuvem institucional, com link de validade limitada, sem permissão de edição, sem indexação, restrito ao arquivo específico, vedado o compartilhamento de pasta, e revogado ao término do prazo de disponibilização. Não sendo possível vincular o acesso ao requerente, o conteúdo disponibilizado deverá conter apenas informação apta à divulgação ao próprio requerente, adotadas previamente as medidas de proteção cabíveis.

ATENÇÃO!
Caso o agente da Ouvidoria identifique, na resposta ou nos anexos, informações aparentemente sujeitas a sigilo, restrição de acesso ou proteção legal, deverá suspender o envio e alertar a unidade técnica responsável, indicando o conteúdo que requer nova avaliação. Caberá à unidade produtora ou custodiante da informação promover os ajustes necessários ou confirmar, de forma expressa, a possibilidade de sua divulgação.

4.9 SEGURANÇA DA INFORMAÇÃO NO TRATAMENTO DE MANIFESTAÇÕES DE OUVIDORIA OU PEDIDOS DE ACESSO À INFORMAÇÃO RECEBIDOS OU TRATADOS PELO SEI

Os processos que contenham manifestações de ouvidoria ou pedidos de acesso à informação deverão ser autuados com nível de acesso restrito, com indicação da hipótese legal aplicável. A restrição do processo não impede a produção de documento ou de extrato de acesso público, quando a informação nele contida não estiver sujeita a restrição.

O conteúdo e os documentos deverão ser acessados somente pelas pessoas que participem formalmente do tratamento. Deverá ser evitada a reprodução desnecessária do relato, dos anexos e dos dados das pessoas envolvidas, especialmente em denúncias e representações.

A manifestação recebida por processo SEI deverá ser registrada no Fala.BR, conforme as orientações aplicáveis aos demais canais de recebimento. Os documentos relacionados ao relato e necessários à sua compreensão deverão ser baixados do processo e anexados ao respectivo registro na Plataforma, após a conferência dos arquivos e, quando cabível, a adoção das medidas de pseudonimização. Concluída a inserção, as cópias baixadas deverão ser imediatamente excluídas da pasta de downloads, da área de trabalho e de outros locais de armazenamento temporário. Os documentos originais permanecerão no processo SEI, que deverá manter o nível de acesso restrito.

4.10 SEGURANÇA DA INFORMAÇÃO NO ATENDIMENTO PRESENCIAL

O atendimento presencial deverá ocorrer em ambiente reservado, de modo a impedir que o relato seja ouvido, visualizado ou acessado por pessoas não autorizadas. A presença de acompanhante ou de outro agente público deverá limitar-se às situações necessárias e observar a concordância do manifestante e o princípio da necessidade de conhecer.

Documentos, formulários e anotações não deverão permanecer expostos em mesas, balcões, impressoras ou outros locais acessíveis a terceiros. A tela deverá permanecer protegida, e o acesso aos sistemas deverá ocorrer por credencial individual. O interessado poderá realizar diretamente o registro com sua própria conta gov.br e a orientação do agente público, sem compartilhamento de credenciais.

Quando houver digitalização, os arquivos deverão ser inseridos no ambiente institucional adequado, e os originais devolvidos ao interessado. Não deverão ser mantidas cópias desnecessárias em pastas de download, área de trabalho ou outros locais temporários. Anotações e cópias produzidas para o atendimento deverão receber destinação segura.

ATENÇÃO!
O conteúdo da manifestação não deverá ser comentado fora do ambiente de atendimento, reproduzido em canais não autorizados ou compartilhado com pessoas que não participem formalmente da atividade.

4.11 SEGURANÇA DA INFORMAÇÃO NO ATENDIMENTO TELEFÔNICO

O atendimento telefônico da Ouvidoria possui caráter exclusivamente orientativo e destina-se apenas a fornecer informações sobre o acesso e o registro de manifestações nos sistemas.

Por esse canal, o agente público não deverá solicitar dados pessoais, consultar manifestações ou processos administrativos específicos nem fornecer informações sobre seu conteúdo ou andamento.

A identidade do interlocutor não poderá ser presumida a partir das informações por ele apresentadas. É vedado confirmar, por telefone, a existência, o número, o teor ou o andamento de manifestação, inclusive quando o interlocutor se identificar como agente público, autoridade ou representante do manifestante, devendo a demanda ser encaminhada a canal institucional rastreável.

Caso o interessado comece a relatar uma denúncia ou outro tipo de manifestação, o agente público deverá interrompê-lo de forma respeitosa e esclarecer que o atendimento

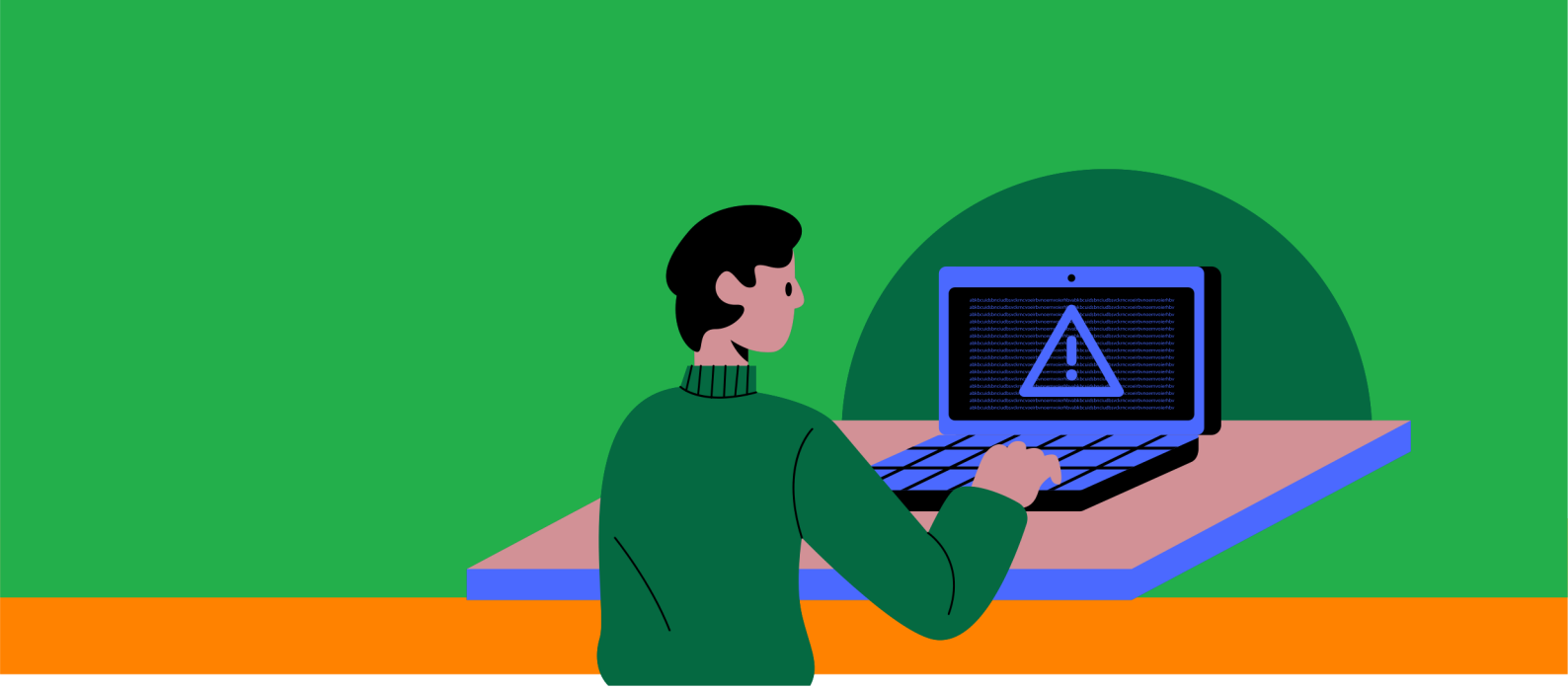
telefônico não é utilizado para o recebimento ou o registro de manifestações, pois a Ouvidoria não dispõe de tecnologia de gravação nem de meios para assegurar o adequado registro do relato por telefone. Em seguida, deverá orientá-lo a registrar a manifestação no sistema correspondente.

As informações eventualmente ouvidas antes da interrupção não deverão ser anotadas, reproduzidas, compartilhadas ou utilizadas para registrar manifestação.

4.12 GUARDA, RETENÇÃO E DESCARTE SEGURO DE INFORMAÇÕES E DOCUMENTOS

A guarda e a retenção de informações e documentos deverão observar os prazos e as orientações estabelecidos na tabela de temporalidade e destinação de documentos aplicável, bem como as normas de gestão documental vigentes no MAPA. A eliminação de documentos somente poderá ocorrer após o cumprimento dos prazos de guarda e dos procedimentos de avaliação e destinação estabelecidos pelas normas arquivísticas aplicáveis, sendo vedado ao agente público eliminar, por iniciativa própria, documentos que integrem processos ou registros institucionais.

Documentos em papel destinados à eliminação deverão ser descaracterizados de forma que seu conteúdo não possa ser recuperado, preferencialmente por fragmentação. Arquivos digitais e suas cópias temporárias, quando não mais necessários e desde que sua eliminação seja permitida, deverão ser excluídos de forma segura, inclusive da lixeira, da pasta de downloads, da área de trabalho e de outros locais de armazenamento temporário. Os documentos que devam ser preservados permanecerão armazenados nos sistemas e ambientes institucionais apropriados, sendo vedada sua manutenção em dispositivos ou locais de armazenamento pessoal.



5. COMUNICAÇÃO DE ERROS E INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Qualquer erro, suspeita ou ocorrência com potencial de comprometer informações deverá ser comunicado imediatamente à chefia.

Incidentes ou suspeitas de incidente de segurança da informação deverão ser comunicados à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR/MAPA, pelo e-mail etir@agro.gov.br.

Quando a ocorrência envolver dados pessoais, deverá ser observado também o fluxo institucional de comunicação ao Encarregado pelo Tratamento de Dados Pessoais do MAPA, por meio do e-mail encarregado.lgpd@agro.gov.br.

A comunicação deverá ser realizada mesmo quando houver dúvida sobre a gravidade da ocorrência.

Deverão ser comunicadas, conforme o fluxo aplicável a cada situação, entre outras, as seguintes ocorrências:

- envio de manifestação, resposta ou documento ao destinatário errado;
- suspeita de phishing, engenharia social ou tentativa de obtenção indevida de informações ou credenciais;
- acesso não autorizado, tentativa ou suspeita de acesso indevido a sistema, pasta, painel, Cortex ou outro ambiente restrito;
- exposição, compartilhamento ou disponibilização indevida de dados pessoais ou informações protegidas;
- perda, extravio, alteração indevida ou indisponibilidade de documento ou registro;
- compartilhamento de senha ou suspeita de comprometimento de conta ou credenciais;
- recebimento, abertura ou execução de arquivo ou link suspeito ou potencialmente malicioso;
- indício de código malicioso (malware) em equipamento, sistema ou arquivo;
- perda, furto ou comprometimento de equipamento utilizado na atividade;
- comportamento anormal de equipamento, sistema ou recurso tecnológico que apresente indícios de comprometimento de segurança; e
- divulgação indevida da identidade de manifestante, denunciante, testemunha ou terceiro.

A comunicação deverá conter as informações disponíveis sobre a ocorrência, sem ampliar a exposição dos dados nem utilizar canal inadequado. O agente público não deverá ocultar o fato, apagar registros, destruir evidências ou tentar solucionar por conta própria situação que exija atuação especializada.

ATENÇÃO!

A comunicação deverá ser realizada mesmo quando houver dúvida sobre a gravidade da ocorrência. Caberá às instâncias competentes analisar a notificação, avaliar a ocorrência e adotar as providências pertinentes, de acordo com suas respectivas atribuições.

Nos incidentes que envolvam dados pessoais, a comunicação interna tempestiva é essencial para viabilizar o cumprimento, pelo MAPA, dos prazos e deveres previstos na regulamentação aplicável. Nos termos da Resolução CD/ANPD nº 15, de 24 de abril de 2024, a comunicação do incidente à Autoridade Nacional de Proteção de Dados – ANPD e aos titulares, quando cabível, deverá ser realizada no prazo de três dias úteis, contado do conhecimento, pelo controlador, de que o incidente afetou dados pessoais. A Resolução estabelece, ainda, a manutenção do registro dos incidentes de segurança que envolvam dados pessoais, inclusive daqueles não comunicados à ANPD e aos titulares, pelo prazo mínimo de cinco anos.



6. USO DE INTELIGÊNCIA ARTIFICIAL NAS ATIVIDADES DA OUVIDORIA

Somente poderão ser utilizadas soluções institucionais ou autorizadas pelo MAPA para o tratamento de informações não públicas. Em ferramentas externas não autorizadas, somente poderão ser inseridas informações públicas, fictícias ou efetivamente anonimizadas, após avaliação do risco de reidentificação.

É vedada a inserção de manifestações, relatos, anexos, dados pessoais, dados pessoais sensíveis, identidade de denunciante, testemunha ou terceiro, informações de acesso restrito ou outros elementos protegidos, ainda que a finalidade seja resumir, revisar, traduzir, classificar ou organizar o conteúdo.

O agente público deverá limitar as informações inseridas ao estritamente necessário, conhecer as condições de armazenamento e retenção da ferramenta, evitar cópias desnecessárias, impedir o envio automático de resultados e comunicar qualquer exposição indevida.

Todo conteúdo produzido com apoio de inteligência artificial deverá ser revisto pelo agente público, que permanece responsável por sua exatidão, adequação, conformidade normativa e ausência de informações protegidas. A ferramenta não substitui a análise humana, a fonte oficial, o registro institucional ou a decisão administrativa.

Equiparam-se a ferramentas de inteligência artificial, para os fins deste Manual, os recursos de transcrição, resumo, gravação ou análise automática embarcados em plataformas de reunião, navegadores ou extensões. Tais recursos deverão permanecer desativados nos atendimentos e nas reuniões que envolvam manifestações, salvo quando institucionalmente autorizados.

ATENÇÃO!

A relação de soluções institucionais ou autorizadas deverá ser consultada no canal oficial definido pela unidade competente. Na ausência de confirmação de autorização, ou em caso de dúvida sobre a ferramenta, a natureza das informações ou a possibilidade de uso, o agente público não deverá utilizar a ferramenta para o tratamento de informações não públicas e deverá solicitar orientação à chefia ou à unidade institucional competente.



7. REGRAS GERAIS DE SEGURANÇA DA INFORMAÇÃO

Todos os agentes públicos em exercício na Ouvidoria deverão conhecer e observar a Política de Segurança da Informação do MAPA — PoSIC/MAPA, atualmente aprovada pela Portaria MAPA nº 136, de 25 de maio de 2021, ou norma que venha a substituí-la, seus atos complementares e as orientações expedidas pelas unidades competentes.

Também deverão ser observadas, conforme a atividade:

- a Política de Gestão de Controle de Acesso Lógico e Físico, aprovada pela Portaria MAPA nº 491, de 21 de setembro de 2022, ou norma que venha a substituí-la;
- a Política do Uso Seguro de Computação em Nuvem, aprovada pela Portaria MAPA nº 528, de 8 de dezembro de 2022, ou norma que venha a substituí-la;
- a Política de Cópia e Restauração de Dados Digitais do MAPA, instituída pela Portaria MAPA Nº 646, de 18 de janeiro de 2024, ou norma que venha a substituí-la;
- as normas internas sobre correio eletrônico, internet, mídias sociais, dispositivos, serviços em nuvem e demais recursos tecnológicos;

- as orientações da Subsecretaria de Tecnologia da Informação — STI e da unidade responsável pela segurança da informação e cibernética; e
- os procedimentos de comunicação de vulnerabilidades e incidentes à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos — ETIR/MAPA.

A segurança da informação abrange documentos, dados, sistemas, equipamentos, instalações, serviços, canais de comunicação e pessoas. As informações produzidas, recebidas, coletadas ou armazenadas pela Ouvidoria constituem ativos de informação do MAPA e deverão ser protegidas durante todo o seu ciclo de vida, de modo a preservar a disponibilidade, a integridade, a confidencialidade e a autenticidade.

7.1 DEVERES DOS AGENTES PÚBLICOS

No desempenho de suas atividades, os agentes públicos deverão:

- utilizar as informações e os recursos institucionais exclusivamente para o exercício de suas atribuições;
- acessar somente as informações necessárias à atividade sob sua responsabilidade, ainda que possuam permissão técnica para consultar outros conteúdos;
- utilizar credenciais individuais e intransferíveis e respeitar os controles de acesso lógico e físico;
- não compartilhar links, senhas ou códigos de acesso a reuniões virtuais com pessoas que não estejam autorizadas a participar, nem permitir o ingresso de terceiros utilizando suas credenciais ou sua sessão autenticada;
- proteger dados pessoais, informações sigilosas e demais conteúdos submetidos a restrição de acesso;
- preservar a privacidade, a honra e a imagem das pessoas cujas informações sejam tratadas;

- armazenar documentos e arquivos somente em sistemas e ambientes institucionais autorizados;
- evitar a crição e a manutenção de cópias desnecessárias;
- adotar medidas para impedir perda, alteração, idisponibilidade, acesso indevido ou divulgação não autorizada;
- comunicar imediatamente erros, suspeitas, vulnerabilidades e incidentes; e
- seguir as orientações das unidades competentes e manter-se atualizado sobre as normas aplicáveis.

A autorização técnica de acesso não permite consultar, reproduzir, armazenar, compartilhar ou divulgar informações para finalidade alheia às atribuições do agente público.

7.2 TRATAMENTO E PROTEÇÃO DE INFORMAÇÕES

O tratamento deverá estar relacionado à finalidade institucional e limitar-se ao necessário para a execução da atividade. O acesso deverá ser restrito às pessoas que precisem da informação para o desempenho de suas atribuições.

Os dados pessoais deverão ser tratados de acordo com a Lei nº 13.709, de 14 de agosto de 2018 — Lei Geral de Proteção de Dados Pessoais, e no Decreto nº 7.724, de 16 de maio de 2012. O fornecimento de informações ao titular ou a representante deverá observar a confirmação da identidade, a comprovação da representação e os procedimentos institucionais.

As informações classificadas em grau de sigilo deverão ser tratadas, armazenadas e compartilhadas de acordo com a Lei nº 12.527, de 18 de novembro de 2011, o Decreto nº 7.724, de 16 de maio de 2012, o Decreto nº 7.845, de 14 de novembro de 2012, e as orientações da Comissão Permanente de Avaliação de Documentos Sigilosos do MAPA — CPADS/MAPA.

A proteção deverá ser conciliada com o direito de acesso à informação pública. A restrição de acesso somente poderá ser aplicada nas hipóteses previstas em lei.

7.3 SEGURANÇA DOS AMBIENTES E DOS RECURSOS INSTITUCIONAIS

Os agentes públicos deverão observar os procedimentos de acesso e circulação nas instalações do MAPA e proteger documentos, equipamentos e demais ativos sob sua responsabilidade.

Ao término do expediente ou sempre que a sala ficar desocupada, o último agente público a deixar o ambiente deverá verificar o trancamento da porta, de modo a impedir o acesso de pessoas não autorizadas.

Documentos e informações não deverão permanecer expostos em mesas, balcões, impressoras, salas de reunião ou locais acessíveis a pessoas não autorizadas. A tela deverá ser bloqueada sempre que o agente se afastar do equipamento.

Correio eletrônico, internet, serviços em nuvem, mídias sociais, equipamentos e demais recursos deverão ser utilizados conforme as normas do MAPA. É vedado utilizar contas pessoais, dispositivos particulares ou serviços externos não autorizados para armazenar ou compartilhar informações institucionais protegidas, ressalvado o uso do equipamento pessoal nas condições de segurança previstas para o PGD ou trabalho remoto.

É vedado armazenar ou transportar informações protegidas da Ouvidoria em mídias removíveis não autorizadas. Quando o uso for excepcionalmente admitido, deverão ser observados os controles e procedimentos definidos pelas unidades competentes.

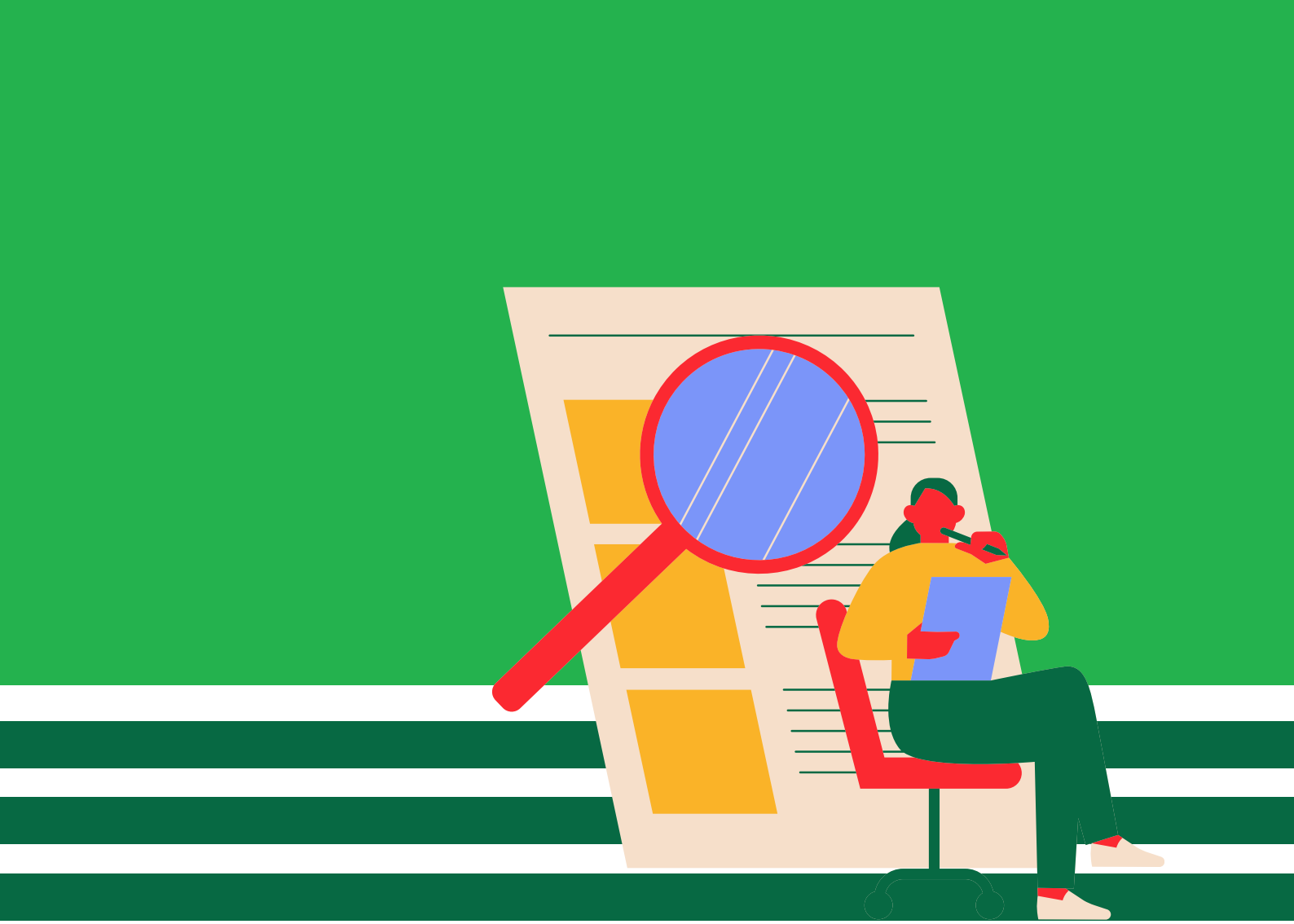
A indisponibilidade de um sistema institucional não autoriza, como medida de contingência, o uso de conta pessoal, serviço particular de armazenamento em nuvem ou outro canal não autorizado para armazenamento, compartilhamento ou transmissão de informações institucionais protegidas.

Os arquivos sujeitos às rotinas de cópia de segurança deverão ser mantidos no serviço de armazenamento disponibilizado e administrado pelo MAPA. A guarda apenas na estação de trabalho não assegura sua inclusão nas rotinas institucionais de cópia e restauração.

A adoção de tecnologia, sistema, aplicativo ou ferramenta deverá observar a autorização institucional e os requisitos de segurança da informação, proteção de dados pessoais, controle de acesso e armazenamento.

ATENÇÃO!

Na dúvida sobre a possibilidade de acessar, armazenar, utilizar ou compartilhar determinada informação, o agente público deverá interromper a atividade e solicitar orientação à chefia ou à unidade competente. A inobservância das normas poderá acarretar responsabilização administrativa, civil e penal, na forma da legislação.



8. VIGÊNCIA, REVISÃO E ATUALIZAÇÃO DO MANUAL

Este Manual será revisado a cada dois anos ou sempre que houver alteração normativa que o afete, sob gestão da Ouvidoria, com manifestação da unidade responsável pela segurança da informação e cibernética e do Encarregado pelo Tratamento de Dados Pessoais.

ANEXO

TERMO DE CIÊNCIA E RESPONSABILIDADE

Segurança da Informação nas Atividades da Ouvidoria do MAPA

Nome completo: _____

CPF ou matrícula: _____

Cargo, emprego ou função: _____

Unidade ou exercício: _____

Vínculo:

( ) servidor(a)

( ) empregado(a)

( ) terceirizado(a)

( ) estagiário(a)

( ) outro: _____

E-mail institucional: _____

1 - Finalidade

O presente Termo registra a ciência e o compromisso do agente quanto às normas de segurança da informação aplicáveis às atividades da Ouvidoria do Ministério da Agricultura e Pecuária — MAPA, especialmente ao acesso e ao tratamento de manifestações, dados pessoais, documentos, credenciais, sistemas e demais ativos de informação sob custódia do Ministério.

2 - Ciência das Normas

Declaro que recebi acesso ou orientação para consultar as normas abaixo e que estou ciente do dever de observá-las, inclusive suas alterações, seus atos complementares e as normas que venham a substituí-las:

- Portaria MAPA nº 136, de 25 de maio de 2021, que aprova a Política de Segurança da Informação do MAPA — PoSIC/MAPA, ou norma que venha a substituí-la, com destaque para os princípios da proteção de dados pessoais, da prevenção e do tratamento de incidentes, da necessidade de conhecer e da preservação da confidencialidade, integridade, disponibilidade e autenticidade das informações;
- Portaria MAPA nº 491, de 21 de setembro de 2022, que aprova a Política de Gestão de Controle de Acesso Lógico e Físico, e Portaria MAPA nº 528, de 8 de dezembro de 2022, que aprova a Política de Segurança da Informação para Computação em Nuvem, ou normas que venham a substituí-las, no que forem aplicáveis;
- Lei nº 12.527, de 18 de novembro de 2011 — Lei de Acesso à Informação, especialmente quanto à proteção das informações pessoais e às responsabilidades pelo acesso, uso, divulgação ou tratamento indevido de informação;
- Lei nº 13.709, de 14 de agosto de 2018 — Lei Geral de Proteção de Dados Pessoais, especialmente quanto aos princípios, aos deveres de segurança e ao tratamento de dados conforme as instruções institucionais;
- Lei nº 13.460, de 26 de junho de 2017; Decreto nº 9.492, de 5 de setembro de 2018; Decreto nº 10.153, de 3 de dezembro de 2019; Lei nº 13.608, de 10 de janeiro de 2018; e Portaria Normativa CGU nº 116, de 18 de março de 2024, quanto à proteção das informações de ouvidoria e à salvaguarda da identidade do denunciante; e
- Lei nº 8.112, de 11 de dezembro de 1990, quando aplicável ao vínculo, bem como o Código de Conduta Ética dos Agentes Públicos do MAPA e as demais normas administrativas, contratuais e profissionais incidentes.

3 - Compromissos Assumidos

No exercício de minhas atribuições, comprometo-me a:

1. acessar informações somente quando necessário ao desempenho das atividades que me forem atribuídas, respeitando os perfis de acesso e o princípio da necessidade de conhecer;
2. utilizar exclusivamente credenciais individuais, manter senhas e mecanismos de autenticação sob minha guarda e não permitir o uso de sessão autenticada por terceiros;
3. preservar, quando cabível, o sigilo e a confidencialidade do conteúdo dos pedidos de acesso à informação e das manifestações de ouvidoria, bem como dos dados pessoais, anexos, informações produzidas durante a análise e documentos relacionados, inclusive após o encerramento da atividade ou do vínculo com a Ouvidoria;

4. proteger a identidade do denunciante e adotar as salvaguardas definidas pela Ouvidoria antes de qualquer encaminhamento, compartilhamento ou reprodução de informações;
5. utilizar apenas sistemas, plataformas, canais e ambientes de armazenamento autorizados, sem transferir conteúdo para e-mail pessoal, aplicativo de mensagens, serviço particular de nuvem, mídia não autorizada ou ferramenta externa;
6. no trabalho remoto ou no Programa de Gestão e Desempenho — PGD, utilizar equipamento protegido, conexão privada e segura e ambiente que impeça que pessoas não autorizadas ouçam conversas, visualizem a tela ou tenham acesso a documentos e anotações;
7. não tratar manifestações em voz alta na presença de pessoas não autorizadas, não realizar gravações, fotografias ou capturas de tela sem necessidade institucional e autorização, e bloquear a tela sempre que me afastar do equipamento;
8. limitar cópias, downloads, impressões e compartilhamentos ao estritamente necessário, excluindo com segurança os arquivos temporários após sua inserção no ambiente institucional adequado;
9. não inserir dados pessoais, informações restritas, relatos, anexos ou documentos da Ouvidoria em ferramentas de inteligência artificial ou outros serviços não autorizados pelo MAPA;
10. comunicar imediatamente à chefia qualquer erro, suspeita ou ocorrência com potencial de comprometer informações e, quando se tratar de incidente ou suspeita de incidente de segurança da informação, comunicar também à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos — ETIR/MAPA, pelo canal institucional definido; e
11. cumprir as orientações do Manual de Segurança da Informação da Ouvidoria e buscar orientação da chefia antes de prosseguir quando houver dúvida ou risco de exposição indevida.

4 - Responsabilidade e consequências

Estou ciente de que a inobservância da PoSIC/MAPA e de seus atos normativos complementares poderá acarretar responsabilização administrativa, civil e penal, nos termos da Portaria MAPA nº 136, de 25 de maio de 2021, ou norma que venha a substituí-la, sem prejuízo das medidas previstas na legislação aplicável e nas regras próprias do meu vínculo com a Administração.

A assinatura deste Termo não implica reconhecimento antecipado de responsabilidade nem substitui o devido processo de apuração. A aplicação de qualquer medida dependerá da natureza da conduta, do dano ou risco produzido, do elemento subjetivo exigido pela norma, do vínculo do agente e da observância do contraditório e da ampla defesa.

5 - Vigência do compromisso

Os deveres previstos neste Termo vigoram durante todo o período de atuação na Ouvidoria e permanecem aplicáveis, quanto às informações protegidas conhecidas em razão da atividade, após a alteração das atribuições, a revogação do acesso, o afastamento ou o encerramento do vínculo.

6 - Guarda e renovação do Termo

O Termo de Ciência e Responsabilidade assinado será autuado em processo próprio no Sistema Eletrônico de Informações — SEI, sob guarda da Ouvidoria, com nível de acesso restrito, em razão dos dados pessoais nele constantes.

A Ouvidoria manterá controle nominal dos Termos assinados, de modo a assegurar que a ciência seja formalizada antes da concessão dos acessos necessários ao exercício das atividades.

Nova ciência será colhida na hipótese de revisão relevante do Manual de Segurança da Informação da Ouvidoria ou de alteração do vínculo ou das atribuições do agente público.

7. Declaração

Declaro que li e compreendi o conteúdo deste Termo, que tive oportunidade de esclarecer dúvidas e que estou ciente dos deveres e das consequências decorrentes do descumprimento das normas de segurança da informação aplicáveis às atividades da Ouvidoria do MAPA.

Brasília, _____ de _____ de _____.

Assinatura do agente

Nome completo

Chefia imediata ou responsável pela ciência

Data da ciência

REFERÊNCIAS

BRASIL. Lei nº12.527, de 18 de novembro de 2011. Regula o acesso a informações.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil.

BRASIL. Lei nº 13.608, de 10 de janeiro de 2018. Dispõe sobre o serviço telefônico de recebimento de denúncias e sobre recompensa por informações que auxiliem nas investigações policiais.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais.

BRASIL. Decreto nº 7.845, de 14 de novembro de 2012. Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada.

BRASIL. Decreto nº 10.153, de 3 de dezembro de 2019. Dispõe sobre as salvaguardas de proteção à identidade dos denunciantes.

BRASIL. Ministério da Agricultura, Pecuária e Abastecimento. Portaria MAPA nº 136, de 25 de maio de 2021. Aprova a Política de Segurança da Informação do MAPA — PoSIC/MAPA.

BRASIL. Ministério da Agricultura, Pecuária e Abastecimento. Portaria MAPA nº 491, de 21 de setembro de 2022. Aprova a Política de Gestão de Controle de Acesso Lógico e Físico.

BRASIL. Ministério da Agricultura, Pecuária e Abastecimento. Portaria MAPA nº 528, de 8 de dezembro de 2022. Aprova a Política do Uso Seguro de Computação em Nuvem.

BRASIL. Controladoria-Geral da União. Portaria Normativa CGU nº 116, de 18 de março de 2024. Estabelece orientações para o exercício das competências das unidades do Sistema de Ouvidoria do Poder Executivo Federal.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Secretaria de Governo Digital. Guia de IA generativa para o serviço público.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Guia unificado de IA: metodologia, implementação e acompanhamento de projetos de IA. Brasília, DF: MGI, 2026.

CONSELHO NACIONAL DE JUSTIÇA; PROGRAMA DAS NAÇÕES UNIDAS PARA O DESENVOLVIMENTO. Cartilha de segurança da informação. Série Fazendo Justiça. Brasília, DF: CNJ; PNUD, 2023.

MINISTÉRIO DA
AGRICULTURA
E PECUÁRIA

GOVERNO DO
BRASIL
DO LADO DO POVO BRASILEIRO