

POLÍTICA INTERNA DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS



MINISTÉRIO DAS
COMUNICAÇÕES

GOVERNO FEDERAL
BRASIL
UNIÃO E RECONSTRUÇÃO

**Ministério das Comunicações,
2024**

**Equipe de Elaboração da Política Interna
de Privacidade e Proteção de Dados
Pessoais**

**Secretaria Executiva
SÔNIA FAUSTINO MENDES**

**Secretaria Executiva Adjunta
JOÃO ALOISIO VIEIRA**

**Subsecretaria de Planejamento e
Tecnologia da Informação
GUSTAVO HENRIQUE DE SOUTO SILVA**

**Coordenação-Geral de Gestão
da Informação
TARIC DE OLIVEIRA SOUSA**

**Coordenação de Gestão Estratégica
de Dados
DAVI DE OLIVEIRA SANTOS**

**Equipe de Projeto
JALILE OLIVEIRA DERZE
DIOGO MACHADO DE CARVALHO**

**Consultoria e Elaboração
JULIA LOPES FERREIRA**

Sumário

1. Apresentação	4
1.1. Alinhamento Estratégico	4
2. Objetivo	5
3. Escopo	5
4. Princípios	5
5. Definições	6
6. Diretrizes Gerais	8
7. Diretrizes Específicas	9
7.1. Propriedade da Informação e Direitos do Titular	9
7.2. Tratamento de Dados Pessoais	10
7.3. Segurança da Informação	12
7.4. Tratamento de Incidentes	12
7.5. Regime de Sanções	13
7.6. Apoio ao Programa de Governança da Privacidade – PGP-MCom	13
8. Responsabilidades	13
9. Disposições Gerais	14
10. Referências E Normativos	14

1. Apresentação

Este documento apresenta a Política Interna de Privacidade e Proteção de Dados Pessoais do Ministério das Comunicações (MCom). Nela, o Ministério fortalece o compromisso da instituição com a Lei Geral de Proteção de Dados Pessoais (LGPD 13.709/2018).

Busca-se proporcionar diretrizes para que agentes públicos possam amparar a adequação do MCom à LGPD, apoiando sua execução e orientando a implementação do Programa de Governança da Privacidade – PGP MCom.

Esta Política deverá servir como documento de consulta, e, portanto, deve estar disponível aos servidores em suas atividades rotineiras de tratamento de dados pessoais. Ela orienta brevemente os curadores, sem, no entanto, esgotar as medidas necessárias para a proteção da privacidade e dos direitos do titular de dados.

1.1. Alinhamento Estratégico

Lei Geral de Proteção de Dados Pessoais (LGPD)

Este documento apresenta, de forma sucinta e sistemática, as diretrizes determinadas para o Ministério das Comunicações apoiar agentes de tratamento, servidores e quaisquer curadores de dados pessoais na adequação da instituição à LGPD.

Programa em Governança da Privacidade

O Programa em Governança da Privacidade do Ministério das Comunicações, (PGP-MCom) aprovado pelo Comitê Gestor de Proteção de Dados Pessoais em 18 de dezembro de 2020 estabelece a estratégia e os critérios para o tratamento de dados pessoais conforme a Lei Geral de Proteção de Dados Pessoais (LGPD 13.709, de 14 de agosto de 2018). Ainda, determina a criação desta política interna de privacidade e proteção de dados pessoais. Nesse sentido, a política estabelece, em conformidade com a LGPD, que o tratamento de dados pessoais deverá seguir a estratégia do programa de modo a evitar violações de privacidade, ao mesmo tempo que preza pelos controles democráticos e pela transparência. Em especial, a política se alinha às atividades de treinamento e conscientização, definição da estratégia, elaboração dos documentos de privacidade, implementação e monitoramento do PGP-MCom.

Orientação Conjunta nº 1//2021/ME/CGU

Esta orientação discorre sobre a transparência no processo administrativo eletrônico e o equilíbrio entre a Lei de Acesso à Informação – LAI nº 12.527, de 18 de novembro de 2011 e a LGPD. De maneira congruente, esta política visa orientar sobre a proteção da privacidade e dos direitos do titular de dados pessoais sem, no entanto, a adoção de medidas antidemocráticas e extremas que possam ferir a transparência, a ética, o acesso à informação e os mecanismos de controle do serviço público.

Política de Segurança da Informação e Comunicação – PoSIC

A PoSIC institui diretrizes e princípios de Segurança da Informação e Comunicação no âmbito do MCom com o propósito de limitar a exposição ao risco a níveis aceitáveis e buscar continuamente a disponibilidade, a integridade, a confidencialidade, a autenticidade, a irretroatividade e o não repúdio das informações que suportam os objetivos estratégicos da instituição. A Política Interna de Privacidade e Proteção de Dados Pessoais, por sua vez, foi desenvolvida de modo a seguir as diretrizes e princípios da PoSIC, de maneira específica para apoiar a segurança das informações pessoais tratadas pelo Ministério.



Portaria nº 462 de 12 de novembro de 2012

A Portaria nº 462 de 12 de novembro de 2012 regulamenta os procedimentos relativos à disponibilização, à classificação, ao tratamento e à gestão da informação de natureza restrita e sigilosa no âmbito do Ministério das Comunicações. Esta Política está em consonância com as determinações da Portaria, sobretudo no tratamento de dados pessoais em sua finalidade, restrição de acesso àqueles cujo conhecimento dos dados seja motivado, na responsabilização pelas informações acessadas e na responsabilidade pelo resguardo da informação.

Portaria MCOM nº 3.857, de 14 de outubro de 2021

Aprova a norma Complementar para Tratamento de Incidentes Cibernéticos.

2. Objetivos

Este documento busca estruturar e definir práticas de governança em privacidade e proteção de dados, apresentando uma visão clara do ciclo de vida dos dados e limitando riscos de violações à LGPD. Pretende alcançar estes objetivos definindo diretrizes e responsabilidades do programa em privacidade de dados do Ministério das Comunicações.

3. Escopo

Esta política se aplica aos servidores, colaboradores, terceirizados, estagiários, fornecedores, parceiros, todos que realizem atividades que envolvam, de forma direta ou indireta, o tratamento de dados pessoais custodiados pelo Ministério das Comunicações. No eventual tratamento de dados realizado por decisões automatizadas, ou pelo uso de inteligência artificial, também deverão ser aplicadas as diretrizes desta política.

Esta política se aplica a quaisquer órgãos de assistência direta e imediata ao Ministro de Estado, aos órgãos específicos singulares, órgãos colegiados e unidades descentralizadas, não se aplicando às entidades vinculadas ao MCom.

A política deverá ser fielmente observada por todos os atores acima (definidos como agentes públicos do Ministério das Comunicações), sob pena de responsabilidade, na forma da lei.

4. Escopo

As atividades de tratamento de dados pessoais deverão observar a boa-fé e os demais princípios que integram a Lei Geral de Proteção de Dados Pessoais (LGPD 13.709/2018), sendo integralmente incorporados à Política de Privacidade do Ministério das Comunicações.

4.1. Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

4.2. Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

4.3. Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

4.4. Livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

4.5. Qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade

de seu tratamento;

4.6. Transparéncia: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

4.7. Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

4.8. Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

4.9. Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; e,

4.10. Responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

São ainda princípios que devem ser adotados pela organização:

4.11. Segurança e privacidade by design: adoção de medidas em quaisquer processos e projetos de modo que a privacidade e a proteção dos dados pessoais sejam mantidas em todas as etapas de seu ciclo de vida. Na prática, a segurança da informação deve ser incorporada à organização de ponta a ponta.

4.12. Privacidade by default: aplicação-padrão das condições mais seguras de proteção da privacidade de dados pessoais em quaisquer processos ou serviços lançados pelo Ministério das Comunicações. Ainda, apenas os dados mínimos necessários devem ser mantidos para execução do serviço, pelo menor tempo possível.

4.13. Cultura da privacidade: processo contínuo de conscientização, capacitação, para criação de uma cultura de proteção da privacidade e dos direitos do titular de dados e do desenvolvimento da pessoa física.

Ademais, prezam-se os princípios em comum com a Política da Segurança da Informação e Comunicações – PoSIC MCom: celeridade, autenticidade da informação, clareza, confidencialidade, disponibilidade equanimidade, ética, finalidade, integridade, menor privilégio, privacidade, publicidade, responsabilidade.

5. Definições

Esta política faz referência ao Glossário de Segurança da Informação, disponível na Portaria nº 93, de 26 de setembro de 2019 e pelo link a seguir:

<https://www.in.gov.br/en/web/dou/-/portaria-n-93-de-26-de-setembro-de-2019-219115663>

Cabe, no entanto, ressaltar alguns dos conceitos primordiais ao entendimento e observância desta política:

Agentes de tratamento: O controlador e o operador.

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: acrônimo de Autoridade Nacional de Proteção de Dados, órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da Lei Geral de

Proteção de Dados Pessoais (LGPD nº 13.709 de 14 de agosto de 2018) em todo o território nacional.

Aviso de Privacidade: extrato desta Política de Privacidade que comunica aos titulares de dados os termos pelos quais o Ministério das Comunicações trata e compartilha seus dados pessoais em uma determinada prestação de serviço. Ao fazer uso deste serviço, os usuários recebem o aviso e concordam com seus termos.

Compartilhamento de Dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

Controlador de dados: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. O controlador define a finalidade e os meios pelo qual os dados pessoais serão tratados e é o principal responsável pelas operações de tratamento de dados.

Curadoria de dados: coordenações incumbidas da captação de dados e da garantia de sua autenticidade, atualização, consistência e precisão.

Dado anonimizado: dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

Dado pessoal: informação relacionada a pessoa natural identificada ou identificável. Seu escopo é amplo e pode se referir tanto a dados que identificam diretamente o indivíduo (ex. nome, CPF, e-mail, etc.), como também atributos do indivíduo que, quando correlacionados permitem a sua identificação (ex. gênero, idade, altura, formação acadêmica, endereço físico, endereço IP, etc.).

Dado (pessoal) sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. Devido à sua natureza mais sensível possui maiores restrições para seu tratamento, de acordo com o estipulado na LGPD.

Encarregado: pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados. A/o Encarregado Substituto, pessoa também nomeada pelo controlador, assume funções em caso de afastamento.

LGPD: Lei Geral de Proteção de Dados Pessoais, Nº 13.709, de 14 de agosto de 2018. Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Pseudoanonymização: tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional

mantida separadamente pelo controlador em ambiente controlado e seguro.

RIPD: relatório de impacto à proteção de dados pessoais. Documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

Termos de Uso: contrato de adesão firmado entre o usuário e o Ministério das Comunicações, enquanto fornecedor de serviços. O uso dos diversos serviços fica condicionado à aceitação dos termos e das políticas associadas, os quais o usuário deverá ler e certificar-se de havê-los entendido, concordar com todas as condições estabelecidas e se comprometer a cumpri-las. Deste modo, ao utilizar o serviço, o usuário manifesta sua livre, expressa e inequivoca concordância com relação ao conteúdo do Termo de Uso e fica legalmente vinculado a todas as condições nele previstas.

Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento. Transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro.

Tratamento: Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

6. Diretrizes Gerais

Cabe aos servidores e demais curadores de dados pessoais aos quais a política se aplica, enumerados anteriormente, conhecer, aderir, cumprir e fazer cumprir a Política de Privacidade do Ministério das Comunicações, conforme as diretrizes gerais a seguir.

- Conhecer, aderir, cumprir e fazer cumprir o Programa de Governança em Privacidade do Ministério das Comunicações.
- Compreender os riscos relacionados ao tratamento de dados pessoais e sua relação com os benefícios ao titular de dados e à sociedade resultantes dos serviços prestados. Adotar os processos de gestão de risco determinados pelo Ministério das Comunicações em sua Política de Gestão de Riscos e Controle Interno - RESOLUÇÃO N° CTIR nº 1/2021/SEI-MCTIC.
- Conhecer e seguir diretrizes gerais da PoSIC, tanto para ambientes informatizados quanto para meios convencionais de tratamento, processamento, armazenamento e comunicação da informação. Compreender e colocar em prática as orientações de gestão de ativos, uso de correio eletrônico, acesso à internet, redes sociais, computação em nuvem e controles de acesso. Adotar e adequar atividades aos processos de gestão da continuidade, auditoria e conformidade dispostos na PoSIC.



- Compreender e implementar os processos de proteção da informação, mecanismos de segurança e recursos disponíveis.
- Adotar processos de tratamento de incidentes dispostos no Plano de Resposta a Incidentes do PGP-MCom e na PoSIC.
- Apoiar processos de auditoria, fornecendo informação completa e adequada.
- Planejar processos conforme os princípios de Privacidade by Design: identificar necessidade de tratamento de dados pessoais e planejar todo o ciclo de vida dos dados priorizando a proteção dos direitos do titular, sobretudo no tratamento de dados pessoais sensíveis, dados pessoais de crianças e adolescentes e na transferência internacional de dados.

7. Diretrizes Específicas

7.1. Propriedade da Informação e Direitos do Titular

Cabe a todos os agentes de tratamento e curadores de dados pessoais:

- Certificar-se da obtenção de consentimento livre, manifesto e inequívoco do titular para o tratamento dos dados; ou, em caso de hipótese de dispensa de consentimento, identificar a base legal que permite o tratamento de dados pessoais conforme lei específica.

Cabe ressaltar que o tratamento de dados no Ministério das Comunicações se dá em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD), utilizando como bases legais, na maioria de seus processos:

"Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I - mediante o fornecimento de consentimento pelo titular;

(...)

III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;" (grifo nosso).

Quaisquer outros casos deverão ser analisados de forma cautelosa e criteriosa, de modo a identificar a base legal que legitima o tratamento de dados pessoais. Ainda:

- Os aplicativos, websites e sistemas do Ministério das Comunicações deverão obter concordância do titular para o tratamento de dados pessoais por meio da aceitação dos Termos de Uso e Aviso de Privacidade, que deverão ser mantidos atualizados à luz da legislação específica.
- Nestes Termos de Uso, os titulares deverão ser informados de forma clara e precisa sobre os dados que serão coletados, a finalidade do tratamento, a natureza obrigatória ou facultativa do fornecimento e as consequências da negativa em fornecê-los.
- O Aviso de Privacidade consiste em um extrato desta Política de Privacidade e Proteção de Dados Pessoais e está em anexo.
- Assegurar que estejam garantidos os direitos do titular, sobretudo no que tange



a confirmação da existência e finalidade do tratamento, o acesso, correção, compartilhamentos, portabilidade, automatização de decisões, anonimização, eliminação; possibilidade e impactos da revogação do consentimento, além da própria revogação.

- Aderir às determinações de propriedade da informação, cessão e obtenção de direitos, conforme a PoSIC, a LGPD e demais regulamentações em vigor.

- Responsabilizar-se por toda informação criada, manuseada, armazenada, transportada, descartada ou custodiada pelo MCom. Neste sentido, ela deve ser classificada e protegida adequadamente quanto aos aspectos de confidencialidade, integridade, autenticidade e disponibilidade, de forma explícita ou implícita conforme o Decreto nº 7.845, de 14 de novembro de 2012, a Lei Nº 13.709, de 14 de agosto de 2018 e a Política de Segurança da Informação e Comunicação – POSIC.

- Resguardar o sigilo das informações pessoais acessadas, sob pena de responsabilização, sem as revelar ou divulgar mesmo após o desligamento de suas funções.

7.2. Tratamento de Dados Pessoais

No tratamento de dados pessoais, cabem aos curadores de dados pessoais:

- Compreender o ciclo de vida dos dados pessoais a serem tratados:

Coleta: refere-se à coleta, produção e recepção de dados pessoais, independentemente do método utilizado.

Retenção: corresponde ao arquivamento ou armazenamento de dados pessoais.

Processamento: Qualquer operação que envolva classificação, utilização, reprodução, processamento, avaliação ou controle da informação, além de extração e modificação de dados pessoais retidos pelo controlador.

Compartilhamento: qualquer operação de transmissão, distribuição, comunicação, transferência, difusão e uso compartilhado de dados pessoais.

Eliminação: operação que visa excluir um dado ou conjunto de dados pessoais.

- Planejar todo o ciclo de vida dos dados priorizando a segurança da informação, a privacidade e a proteção dos direitos do titular, conforme princípios da privacidade *by design* e privacidade *by default* de ponta-a-ponta do processo.

- Comunicar novos e atuais processos de tratamento de dados pessoais à área regimentalmente responsável pela gestão de dados pessoais (atualmente determinada à Coordenação de Gestão Estratégica de Dados – COGED), para inclusão e atualização do inventário de dados pessoais. A comunicação deverá ser feita pelo preenchimento do formulário a seguir:

Mapeamento de Dados Pessoais:
<https://forms.office.com/r/9e2QWQgfRE>

- Limitar os processos, serviços, acesso de pessoas e compartilhamentos ao mínimo necessário para a finalidade dos tratamentos.
- Executar apenas os tratamentos relacionados à finalidade declarada.

- Registrar os compartilhamentos de dados pessoais, justificando a finalidade e necessidade de compartilhamento e assegurando a limitação do acesso ao mínimo necessário. Os compartilhamentos deverão ser registrados nos formulários a seguir:

Formulário de Compartilhamento Interno de Dados Pessoais:
<https://forms.office.com/r/1QdmF8Jrwm>

Formulário de Compartilhamento Externo de Dados Pessoais:
<https://forms.office.com/r/CUtj5Wz2TP>

Cabe ressaltar que o compartilhamento de dados pessoais configura um tratamento, e deverá ser também registrado e/ou atualizado no inventário de dados pessoais pelo formulário do Mapeamento de Dados Pessoais.

- Respaldar todo e qualquer compartilhamento internacional de dados pessoais conforme hipóteses legais permitidas pela LGPD.
- Atualizar contratos, acordos, convênios e congêneres relacionados ao tratamento de dados pessoais, inclusive em caso de necessidade de acordo de processamento de dados pessoais, de modo a adequá-los à lei específica.
- Respeitar mecanismos de proteção contra uso indevido, tentativas de acesso não autorizado, fraudes, sabotagens, danos e roubo de dados, assim como fazê-los cumprir por aqueles que se relacionam com o Ministério das Comunicações ou em seu nome.
- Compreender a necessidade de restrição de processos eletrônicos quando forem tratados dados pessoais, priorizando as técnicas e tecnologias disponíveis para anonimização ou pseudoanonimização, de modo a proteger os dados pessoais e ao mesmo tempo assegurar os princípios de transparência e a observância da Lei de Acesso à Informação. Para tal, deverão ser observadas as medidas de proteção dispostas na PosIC e a Orientação Conjunta nº 1//2021/ME/CGU, que orienta sobre a transparência no processo administrativo eletrônico e discorre sobre o equilíbrio entre a Lei de Acesso à Informação – LAI nº 12.527, de 18 de novembro de 2011 e a LGPD.
- Observar, concomitantemente, as disposições constantes da Lei nº 9.507, de 12 de novembro de 1997 (Lei do Habeas Data), da Lei nº 9.784, de 29 de janeiro de 1999 (Lei Geral do Processo Administrativo), e da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).
- Observar as hipóteses de destinação final dos dados pessoais a seguir.

A destinação final inclui qualquer operação que envolva ações referentes ao ato de decidir quais documentos devem ser eliminados (mediante autorização, conforme legislação vigente), bem como quais documentos devem ser mantidos por razões administrativas, legais ou fiscais. Para tal, envolve as atividades de análise, seleção e fixação de prazos de guarda dos documentos.

- 1) Guarda permanente: a guarda deverá ser realizada apenas em caso de obrigação legal. Caberá a cada área responsável pela curadoria dos dados compreender a temporalidade do tratamento de dados.
- 2) Eliminação: a exclusão dos dados pessoais deverá ocorrer nas seguintes situações
 - a. Quando os dados pessoais deixarem de cumprir a finalidade definida para o tratamento. Caberá a cada área responsável pela curadoria propor ao SGD o



- término desta finalidade; ou
- b. Quando o titular dos dados solicitar exclusão cabível.

Quando do descarte de informações institucionais, deverão ser observadas as políticas, as normas, os procedimentos internos, a classificação que a informação possui, bem como a temporalidade prevista na legislação.

- Observar as determinações e orientações da Comissão Permanente de Avaliação de Documentos Sigilosos – CPADS quanto aos procedimentos de descarte e eliminação de dados sigilosos, classificados, reclassificados e desclassificados conforme determinação da Portaria MCom nº 8.490, de 24 fevereiro de 2023 e regulamentos da Portaria nº 462 de 12 de novembro de 2012.

7.3. Segurança da Informação

É de responsabilidade do agente público do Ministério das Comunicações:

- Garantir segurança dos ativos de informação sob sua responsabilidade (senha, login, usuário de rede, crachá, carimbo, assinatura digital, token, entre outros);
- Utilizar dos ativos de segurança dentro do propósito adequado;
- Adotar medidas e seguir determinações para garantir segurança física do ambiente, inclusive em relação aos controles de acesso e identificação;
- Seguir as determinações para o adequado tratamento da informação dispostas na PoSIC, além das diretrizes específicas voltadas ao tratamento de dados pessoais supracitadas;
- Conhecer e aderir às normas de classificação e reclassificação do Ministério das Comunicações, de acordo com determinações da PoSIC, da Comissão Permanente de Avaliação de Documentos – CPAD e da Comissão Permanente de Avaliação de Documentos Sigilosos - CPADS (Portaria nº 8.490, de 24 fevereiro de 2023).

A informação classificada conforme a legislação vigente que for produzida, armazenada e transportada em meios eletrônicos deverá utilizar criptografia compatível com o grau de sigilo, em especial as informações de autenticação dos usuários das aplicações e os dados pessoais.

7.4. Tratamento de Incidentes

É de responsabilidade do agente público do Ministério das Comunicações:

- Notificar, imediatamente, incidentes que afetem a segurança dos dados pessoais, casos de violação de direitos do titular, infrações da LGPD ou o descumprimento da PoSIC, ao Encarregado pela Proteção de Dados Pessoais e à Equipe de Tratamento de Incidentes de Rede (ETIR), para que as providências necessárias sejam adotadas a fim de sanar as causas. Após a referida notificação, todos procedimentos, atribuições e diretrizes referentes ao Tratamento de Incidentes Cibernéticos seguirão a Norma Específica – Portaria MCom nº 3.857, de 14 de outubro de 2021.
- Conhecer, compreender e seguir as orientações da Norma Complementar para Tratamento de Incidentes Cibernéticos (Plano de Resposta a Incidentes) do Ministério das Comunicações, de modo a garantir o sigilo de informações sensíveis quanto à violação, as funções e responsabilidades organizacionais, o escalonamento de possíveis



problemas e relato de atividades suspeitas, as classificações de gravidade de incidentes e as orientações para comunicações externas.

- Conhecer e seguir o plano de resposta a incidentes em rede determinado pela PoSIC.
- Seguir as orientações e processos determinados para a gestão de riscos do Ministério das Comunicações.
- Entender a necessidade de elaboração de Relatório de Impacto à Proteção de Dados (RIPD), conforme checklist constante do Mapeamento de Dados Pessoais. Caso necessário, o RIPD deverá ser preenchido pelo formulário a seguir:

Relatório de Impacto à Proteção de Dados Pessoais – RIPD:
<https://forms.office.com/r/gBBjqQEg38>

7.5. Regime de Sanções

- Sanções externas: conhecer e compreender o [Regulamento de Dosimetria e Aplicação de Sanções Administrativas da Autoridade Nacional de Proteção de Dados](#), que regulamenta os artigos 52 e 53 da LGPD, estabelece parâmetros e critérios para aplicação de sanções administrativas pela ANPD, bem como as formas e dosimetrias para o cálculo do valor-base das sanções de multa.
- Sanções internas: por ocasião de violação da LGPD e descumprimento desta política de privacidade, caberá ao Ministério das Comunicações avaliar e estabelecer o regime de sanções disciplinares conforme legislação específica.

7.6. Apoio ao Programa de Governança da Privacidade – PGP-MCom

- Conhecer e compreender as etapas do Programa de Governança da Privacidade – PGP-MCom, suas etapas e atividades: treinamento e conscientização; composição do Comitê de Proteção de Dados Pessoais e da Equipe de Proteção de Dados Pessoais; definição da Estratégia de Proteção de Dados Pessoais, avaliação da Realidade Organizacional, elaboração dos Documentos de Privacidade; implementação do Programa de Governança em Privacidade; monitoramento do Programa de Governança em Privacidade.
- Apoiar o Encarregado/a, os comitês, equipes e quaisquer eventuais servidores designados na implementação do PGP-MCom na instituição, sua estrutura de governança e mecanismos de supervisão internos e externos.

8. Responsabilidades

A atuação do Encarregado/a deverá se pautar no fato de que, na maioria dos casos, o Ministério das Comunicações age no papel de operador para a maioria de seus tratamentos de dados pessoais, mas também como controlador em nível corporativo-institucional. Os casos em que o tratamento dos dados for realizado por terceiros deverão ser analisados individualmente.

Esteja o MCom atuando como operador ou controlador, deverão ser observadas cláusulas contratuais, acordos de processamento de dados, políticas de privacidade, segurança e classificação da informação. Quando necessário, diferentes agentes de tratamento deverão trabalhar de forma colaborativa para o atendimento da LGPD.



O Subcomitê de Governança de Dados – SGD, colegiado subordinado ao Comitê de Governança Digital, Segurança da Informação e Proteção de Dados Pessoais – CGSP, é a instância interna de apoio à governança e ao Comitê de Governança Ministerial.

Os demais órgãos, agentes de tratamento, agentes públicos, servidores e curadores de dados pessoais em nome do Ministério das Comunicações são responsáveis pela observância da Política Interna de Privacidade e Proteção de Dados Pessoais; do Programa de Governança da Privacidade -PGP MCom; da Política de Governança; da Política de Segurança da Informação e Comunicação – PoSIC; da Política de Classificação da Informação e de quaisquer normativos relacionados à proteção da privacidade e dados pessoais.

9. Disposições Gerais

Esta política deverá ser revista a cada dois anos para atualização de seus termos e adequação aos normativos e programas com os quais interage.

10. Referências e Normativos

- [Lei nº 13.709, de 14 de agosto de 2018](#) - Lei Geral de Proteção de Dados Pessoais.
- [Lei nº 14.460, de 25 de outubro de 2022](#) - Transforma a Autoridade Nacional de Proteção de Dados (ANPD) em autarquia de natureza especial e transforma cargos comissionados; altera as Leis nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), e nº 13.844, de 18 de junho de 2019; e revoga dispositivos da Lei nº 13.853, de 8 de julho de 2019.
- [Instrução Normativa SGD nº 117, de 19 de novembro de 2020](#) - Dispõe sobre a indicação do Encarregado pelo Tratamento dos Dados Pessoais no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional.
- [Portaria MCom nº 374, de 19 de outubro de 2023](#) – Nomeação do Encarregado Titular e Substituto do Ministério das Comunicações.
- [Decreto nº 10.046, de 9 de outubro de 2019](#) - Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados.
- [ADI 6.649](#) – Dispõe sobre o compartilhamento de dados pela administração pública e a criação do Cadastro Base do Cidadão e do Comitê Central de Governança de Dados.
- [Guias e Modelos](#) do Departamento de Privacidade e Segurança da Informação, da Secretaria de Governo Digital.
- [Repositório](#) de publicações da ANPD.
- [Resolução N° CTIR nº 1/2021/SEI-MCTIC](#) - Dispõe sobre a Política de Gestão de Riscos e Controle Interno do Ministério das Comunicações.
- [Orientação Conjunta nº 1//2021/ME/CGU](#) – Transparência no processo administrativo eletrônico.
- [Portaria MCom nº 8.490, de 24 fevereiro de 2023](#) - Dispõe sobre a Política de Governança do Ministério das Comunicações.

- [Portaria MCom nº 10.290, de 23 de agosto de 2023](#) - Designa o Gestor de Segurança da Informação do Ministério das Comunicações.
- [Portaria MCom nº 8.374, de 6 de fevereiro de 2023](#) - Aprova o Regimento Interno do Ministério das Comunicações e divulga o quadro demonstrativo de cargos em comissão e de funções de confiança do órgão.



**MINISTÉRIO DAS
COMUNICAÇÕES**



gov.br/mcom

 [mincomunicacoes](https://mincomunicacoes.com.br)