Diario Oficial - DODP
Publicada 05/07/2025

DPMG
DEFENSORIA PÚBLICA DE MINAS GERAIS

Rua dos Guajajáras, 1707 - Bairro Barro Preto - CEP 30180-099 - Belo Horizonte - MG - www.defensoria.mg.def.br
7º andar

RESOLUÇÃO

Nº 3762/2025

Aprova a Política de Uso do E-mail Institucional da Defensoria Pública do Estado de Minas Gerais.

A DEFENSORA PÚBLICA-GERAL DO ESTADO DE MINAS GERAIS em exercício, no uso de suas atribuições estabelecidas no art. 9º, I, III e VII c/c art. 11º da Lei Complementar nº 65, de 16 de janeiro de 2003, e tendo em vista o disposto no inciso LXXIX do art. 5º da Constituição Federal, na Lei Federal 13.709, de 14 de agosto de 2018, na Deliberação 397/2024 e na Resolução 2970/2024,

RESOLVE:

Art. 1º – Fica aprovada a Política de Uso do E-mail Institucional da Defensoria Pública do Estado de Minas Gerais, nos termos do Anexo.

Art. 2º – Esta Resolução entra em vigor na data de sua publicação.

Belo Horizonte, 03 de julho de 2025.

Karina Rodrigues Maldonado
Defensora Pública-Geral do Estado de Minas Gerais em exercício

ANEXO

(a que se refere o art. 1º da Resolução nº 3762/2025)

POLÍTICA DE USO DO E-MAIL INSTITUCIONAL DA DEFENSORIA PÚBLICA DO ESTADO DE MINAS GERAIS (DPMG)

1. OBJETIVO

1.1 O objetivo da Política de uso do e-mail institucional é regulamentar a utilização, para o envio e recebimento de documentos, acompanhamento regular das contas de e-mail institucional por parte dos usuários, e estabelecimento de padrões de conduta relacionados à segurança da informação, à privacidade, à proteção de dados pessoais e estratégicos no âmbito da instituição.

2. PRINCÍPIOS

2.1 Esta Política observará os princípios estabelecidos na Deliberação nº 397/2024, na Resolução nº 2970/2024 e os seguintes:

2.1.2 Rastreabilidade: Capacidade de identificar, auditar e registrar o histórico de uso e de comunicações realizadas por meio do e-mail institucional, possibilitando a apuração de responsabilidades em eventuais incidentes.

2.1.3 Finalidade: Utilização do e-mail institucional exclusivamente para fins relacionados ao exercício das atividades funcionais, respeitando os objetivos institucionais da Defensoria Pública e vedando seu uso para interesses particulares ou alheios à atuação institucional.

3. DEFINIÇÕES

3.1 Para fins deste documento devem ser consideradas as definições da Deliberação nº 397/2024, da Resolução nº 2970/2024 e as seguintes:

3.1.1. Malware: Software malicioso criado para danificar, invadir ou obter acesso não autorizado a dispositivos ou sistemas, como *vírus, worms, trojans, ransomware,* entre outros.

3.1.2 Phishing: Técnica fraudulenta utilizada para enganar o usuário e induzi-lo a fornecer dados pessoais, financeiros ou credenciais de acesso, geralmente por meio de mensagens de e-mail que simulam comunicações legítimas.

3.1.3 Spam: Mensagem eletrônica não solicitada, frequentemente de cunho publicitário ou fraudulento, enviada em massa e sem o consentimento do destinatário.

4. E-MAIL INSTITUCIONAL

4.1 Considera-se e-mail institucional a conta de correio eletrônico de titularidade da DPMG, disponibilizada nominalmente, fornecida e destinada exclusivamente à realização de comunicações de natureza oficial, interna ou externa, no âmbito das atividades institucionais.

4.2 O e-mail institucional de uso individual corresponde à caixa de correio eletrônico atribuída nominalmente a servidor, colaborador ou membro da instituição, para utilização pessoal e intransferível durante a vigência do vínculo formal com a DPMG, sendo seu uso restrito aos fins relacionados ao estrito cumprimento das atividades funcionais atribuídas ao usuário de e-mail.

5. TITULARIDADE DE CONTAS DE E-MAIL INSTITUCIONAL

5.1 O fornecimento de contas de e-mail institucional pela DPMG é destinado exclusivamente a pessoas que mantenham vínculo formal com a instituição, conforme as seguintes categorias:

5.1.2 **E-mail institucional de uso individual:** Poderá ser concedido a membros, servidores, estagiários e prestadores de serviços terceirizados, desde que a utilização da conta seja necessária para o desempenho de suas atribuições funcionais no âmbito da DPMG.

5.1.3 **E-mail institucional de uso setorial:** Poderá ser disponibilizado aos órgãos de atuação e órgãos ou serviços administrativos, projetos institucionais, eventos oficiais, dentre outros, enquanto estiverem em vigor ou em execução, visando à comunicação e à operacionalização de atividades específicas de interesse institucional.

6. GRUPO DE E-MAIL

6.1 Considera-se grupo de e-mail o conjunto de e-mails reunidos em uma lista de distribuição, de modo a possibilitar o envio simultâneo de mensagens a todos os seus integrantes.

6.2 Antes de utilizar um grupo de e-mail, o remetente deve avaliar cuidadosamente a pertinência da mensagem e o grau de sensibilidade das informações a serem compartilhadas, restringindo o envio apenas quando for estritamente necessário e compatível com o interesse funcional do grupo.

7. RECOMENDAÇÕES DE SEGURANÇA NO USO DO E-MAIL INSTITUCIONAL

7.1 O e-mail institucional é ferramenta destinada exclusivamente ao exercício das atividades funcionais. É vedado utilizá-lo para cadastros em sites de compras, promoções, redes sociais, estabelecimentos comerciais ou quaisquer outras finalidades não institucionais, a fim de evitar a exposição indevida do endereço eletrônico.

7.2 É desaconselhável a abertura de mensagens de origem ou autenticidade duvidosa.

7.3 O usuário deve verificar cuidadosamente os campos Remetente (De) e Destinatário (Para), atentando-se à grafia dos nomes. A mesma cautela se aplica aos campos CC (Com Cópia), CCO (Com Cópia Oculta) ou BCC (Blind Carbon Copy).

7.4 Mensagens alarmistas, sensacionalistas ou que apresentem conteúdos chamativos, como promessas de prêmios, alertas urgentes de expiração de senhas ou ofertas excessivamente vantajosas, devem ser consideradas suspeitas.

7.4.1 Nestes casos, recomenda-se que a mensagem seja apagada ou marcada como spam.

7.4.2 Mensagens identificadas como spam não devem ser respondidas.

7.4.3 Recomenda-se utilizar a funcionalidade de marcação como spam da plataforma de e-mail, o que contribuirá para o aprimoramento dos filtros de segurança do provedor.

7.5 Não se deve abrir arquivos anexos com extensões potencialmente perigosas (tais como .exe, .scr, .com, .bat, entre outras), especialmente quando provenientes de fontes não confiáveis, por apresentarem risco de infecção por malwares.

7.6 Cada usuário de e-mail é responsável pelo uso individual de sua conta institucional.

7.6.1 É proibido o compartilhamento de credenciais (usuário e senha) com terceiros, inclusive colegas de trabalho, estagiários ou prestadores de serviço.

7.7 O e-mail institucional não deve ser utilizado para fins políticos, partidários, religiosos, promocionais, ou para envio de correntes, mensagens de cunho pessoal, ofensivo, discriminatório, difamatório ou que atentem contra a moral, os bons costumes ou a imagem da DPMG.

7.8 Deve-se ter especial atenção com mensagens fraudulentas conhecidas como *phishing*, que tentam induzir o usuário a fornecer informações sensíveis, como senhas, dados bancários ou credenciais de acesso, geralmente por meio de mensagens que simulam comunicações oficiais. Essas mensagens podem conter links maliciosos ou redirecionar para páginas falsas.

7.8.1 Em caso de dúvida, recomenda-se não clicar em links, não fornecer informações e encaminhar a mensagem à equipe de segurança da informação da DPMG.

7.9 É vedado o uso do e-mail institucional para o envio de grandes volumes de mensagens não solicitadas (spam).

7.10 A conta de e-mail institucional deve ser acessada, preferencialmente, em dispositivos que estejam atualizados, protegidos por antivírus e com sistema operacional legítimo**.**

7.11 É responsabilidade do usuário manter seus dados de recuperação atualizados, especialmente o número de telefone e o e-mail secundário vinculado à conta institucional.

7.12 A utilização de equipamentos de terceiros deve ser evitada. Quando inevitável, recomenda-se o uso de modo de navegação anônima, com a finalidade de impedir o armazenamento de senhas, cookies ou histórico de navegação.

7.13 Deve ser evitado, sempre que possível, o acesso à conta institucional por meio de redes públicas ou desprotegidas, como aquelas disponíveis em aeroportos, estabelecimentos comerciais e locais públicos. Caso seja imprescindível o uso, devem ser evitadas atividades sensíveis, como envio de e-mails institucionais, acesso à nuvem ou a sistemas sob responsabilidade da DPMG.

7.14 A conta de e-mail institucional está sujeita a monitoramento e auditoria por parte da área de Segurança da Informação da DPMG, exclusivamente para fins de segurança em conformidade com os normativos vigentes e prevenção de incidentes, sendo resguardado o sigilo profissional.

7.15 Em caso de perda, roubo ou acesso indevido à conta institucional, o usuário de e-mail deverá comunicar imediatamente à equipe de Segurança da Informação da DPMG, para adoção das medidas cabíveis.

7.16 É responsabilidade do usuário encerrar corretamente a sessão ao utilizar computadores compartilhados ou públicos, garantindo que nenhum dado fique acessível a terceiros.

8. ADMINISTRAÇÃO SEGURA DE SENHAS DE ACESSO

8.1 Recomenda-se que o usuário não utilize a mesma senha para múltiplas finalidades, como acesso a e-mail institucional, e-mail pessoal, contas bancárias, dispositivos móveis e sites diversos, para não gerar vulnerabilidade.

8.2 Ao criar uma senha, recomenda-se utilizar ao menos três (03) dos seguintes critérios de complexidade: letras minúsculas, letras maiúsculas, números e caracteres especiais.

8.2.1 Sugere-se a não reutilização da senha anterior.

8.3 Evite registrar senhas em locais visíveis ou de fácil acesso, como papéis, notas adesivas no computador, estações de trabalho ou arquivos eletrônicos não protegidos. Essa prática compromete a segurança das informações e deve ser evitada.

8.4 Recomenda-se evitar senhas óbvias ou de fácil dedução, tais como datas de nascimento, nomes próprios, sequências numéricas simples ou palavras comuns.

8.5 Recomenda-se a troca de senhas periodicamente, num prazo não superior a seis (06) meses.

8.6 Os usuários devem trocar suas senhas imediatamente após suspeitarem que foram violadas.

9. COMUNICAÇÃO E TREINAMENTOS

9.1 As regras e diretrizes definidas nesta Política serão divulgadas, por meios oficiais de divulgação da DPMG, de maneira que seu conteúdo possa ser consultado a qualquer momento.

9.2 Cabe a cada usuário de e-mail manter-se atualizado em relação a esta Política e às normas relacionadas, buscando orientação junto ao responsável pela Segurança da Informação, sempre que não estiver seguro quanto ao uso ou descarte do e-mail institucional.

10. CONTROLE DAS REVISÕES

10.1 A revisão desta Política será realizada anualmente, em conformidade com as melhores práticas globais de segurança da informação e as normas ISO aplicáveis ao nosso negócio.

Documento assinado eletronicamente por **Karina Rodrigues Maldonado**, **Defensora Pública-Geral em exercício**, em 03/07/2025, às 19:00, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://defensoria.mg.def.br/portal-sei informando o código verificador **0601571** e o código CRC **9F66ABAF**.