

POLÍTICA DE USO DO E-MAIL CORPORATIVO

Código: POL-TI-001

Versão: 1.0

Data de aprovação: 05/10/2026

Área responsável: Tecnologia da Informação

1. Objetivo

Estabelecer diretrizes para o uso adequado, seguro e responsável do e-mail corporativo, visando proteger as informações da organização, reduzir riscos de segurança e garantir o uso adequado dos recursos tecnológicos disponibilizados aos colaboradores.

2. Abrangência

Esta política aplica-se a todos os colaboradores, prestadores de serviços, terceiros e demais usuários que possuam uma conta de e-mail corporativo disponibilizada pela organização.

3. Diretrizes de utilização

O e-mail corporativo deve ser utilizado prioritariamente para atividades relacionadas às funções profissionais do usuário e aos interesses legítimos da organização.

É responsabilidade de cada usuário:

- manter suas credenciais de acesso em sigilo;
- utilizar somente sua própria conta de e-mail;
- verificar cuidadosamente remetentes e destinatários antes do envio de mensagens;
- comunicar imediatamente situações suspeitas, como mensagens de phishing, tentativas de fraude ou acesso indevido;
- utilizar linguagem profissional e adequada nas comunicações corporativas;
- observar as normas internas de segurança da informação e proteção de dados pessoais.

4. Usos não permitidos

É vedada a utilização do e-mail corporativo para:

- envio ou armazenamento de conteúdo ilícito, ofensivo, discriminatório ou que viole direitos de terceiros;
- disseminação de mensagens maliciosas, spam ou conteúdo fraudulento;

- compartilhamento indevido de informações confidenciais ou dados pessoais;
- tentativa de obtenção de credenciais, senhas ou informações de outros usuários;
- cadastro em serviços externos que possam representar risco à segurança da organização, quando não autorizado;
- realização de atividades comerciais ou pessoais incompatíveis com as funções profissionais do usuário;
- qualquer atividade que possa comprometer a segurança, a reputação ou os recursos tecnológicos da organização.

5. Proteção de informações

Informações confidenciais, estratégicas ou que contenham dados pessoais devem ser compartilhadas por e-mail somente quando houver necessidade relacionada à atividade profissional e observando-se os controles de segurança estabelecidos pela organização.

Quando aplicável, devem ser utilizados mecanismos adicionais de proteção, como criptografia, proteção por senha ou ferramentas corporativas autorizadas para compartilhamento de arquivos.

6. Segurança das credenciais

As credenciais de acesso são pessoais e intransferíveis.

O usuário não deve compartilhar sua senha, permitir que terceiros utilizem sua conta ou armazenar credenciais em locais inadequados.

Sempre que houver suspeita de comprometimento da conta, o usuário deverá comunicar imediatamente a área responsável pela Tecnologia da Informação.

7. Monitoramento e auditoria

A organização poderá realizar registros, monitoramento e auditorias relacionados ao uso dos recursos corporativos, respeitando a legislação aplicável, as políticas internas e os princípios de segurança da informação e proteção de dados.

O monitoramento poderá ser utilizado para identificar incidentes de segurança, utilização inadequada dos recursos, cumprimento desta política e atendimento a requisitos legais ou regulatórios.

8. Responsabilidades

Usuários: utilizar o e-mail de forma adequada e segura, observando esta política e as demais normas internas.

Tecnologia da Informação: administrar o serviço de e-mail, implementar controles de segurança e apoiar os usuários na prevenção e tratamento de incidentes.

Gestores: orientar suas equipes quanto ao cumprimento desta política e comunicar situações de uso inadequado.

9. Descumprimento

O descumprimento desta política poderá resultar na adoção de medidas administrativas e disciplinares cabíveis, sem prejuízo das responsabilidades civis, administrativas ou legais eventualmente aplicáveis.

10. Vigência e revisão

Esta política entra em vigor na data de sua aprovação e deverá ser revisada periodicamente ou sempre que ocorrerem alterações relevantes nos processos, tecnologias, riscos ou requisitos legais aplicáveis.