GRUPO

SERVAL®

1970

POLÍTICA DE E-MAILS

Versão001

SUMÁRIO

1. OBJETIVOS 3
2. ABRANGÊNCIA 3
3. DIRETRIZES GERAIS 3
4. MEDIDAS PARA PREVENÇÃO DE SPAM E E-MAILS MALICIOSOS 4
5. TRATAMENTO DE E-MAILS SUSPEITOS 4
6. PROTEÇÃO CONTRA PHISING E ATAQUES CINBERNÉTICOS 4
7. PENALIDADES PARA USO INDEVIDO 5
8. RESPONSABILIDADES 5
9. REVISÃO E ATUALIZAÇÃO 5

1. OBJETIVOS

A presente política tem como objetivo estabelecer diretrizes para o uso adequado do e-mail corporativo do Grupo Serval, garantindo a segurança da informação, a conformidade com normas internas e a eficiência da comunicação eletrônica.

2. ABRANGÊNCIA

Esta política se aplica a todos os colaboradores, prestadores de serviço e terceiros que possuam acesso ao e-mail corporativo do Grupo Serval.

3. DIRETRIZES GERAIS

Estas diretrizes visam as melhores práticas de utilização de e-mail corporativo:

- Ao enviar e-mail para uma lista de distribuição (Grupo de E-mail), o mesmo deve ser enviado como cópia oculta (Cco) e no “Para” o e-mail do próprio remente.
- Os colaboradores devem revisar regularmente sua caixa de e-mails e excluir mensagens fúteis ou desnecessárias, evitando o acúmulo de informações irrelevantes.
- O e-mail corporativo é de uso exclusivo para atividades profissionais relacionadas ao Grupo Serval. O uso do e-mail para fins pessoais ou não autorizados é proibido.
- É proibido o compartilhamento de credenciais de acesso ao e-mail corporativo.
- Evite enviar anexos arquivo com tamanho acima de 10 MB, se os envolvidos possuem acesso a rede, disponibilize na Pasta da Rede/GED (ged.gruposerval.com.br, utilizando os mesmos dados do sistema Tela) e compartilhe apenas o local de armazenamento.
- Todas as comunicações por e-mail devem seguir os padrões de segurança e conduta profissional estabelecidos pela organização.

4. MEDIDAS PARA PREVENÇÃO DE SPAM E E-MAILS MALICIOSOS

- **Filtros de Spam:** E-mails suspeitos serão filtrados automaticamente para evitar a entrega na caixa de entrada dos usuários, caso você receba o mesmo deve marcá-lo como spam para aprimorar os filtros de segurança.

- **Lista de Permissões (Whitelist):** Apenas domínios e remetentes autorizados poderão enviar e-mails diretamente aos destinatários internos.

- **Lista de Bloqueios (Blacklist):** Domínios e remetentes que enviem e-mails considerados maliciosos serão bloqueados.

- **Treinamento de Conscientização:** Os colaboradores receberão capacitação sobre como identificar e-mails de phishing e outras ameaças.

5. TRATAMENTO DE E-MAILS SUSPEITOS

Caso um colaborador receba um e-mail suspeito:

- Não deve clicar em links ou baixar anexos desconhecidos.
- Deve reportar imediatamente ao setor de TI pelo e-mail ti@gruposerval.com.br.
- Se identificar um e-mail malicioso, deve marcá-lo como spam para aprimorar os filtros de segurança.

6. PROTEÇÃO CONTRA PHISING E ATAQUES CIBERNÉTICOS

Foi aplicado a autenticação de E-mails: Implementação de protocolos de segurança como SPF, DKIM e DMARC para reduzir o risco de spoofing. Bloqueio de Arquivos Perigosos: Anexos suspeitos como .exe, .bat, .scr serão bloqueados automaticamente pelo sistema.

7. PENALIDADES PARA USO INDEVIDO

- O uso inadequado do e-mail corporativo poderá resultar em sanções disciplinares, incluindo advertências, suspensões ou desligamento, conforme o Código de Conduta do Grupo Serval.

- A reincidência no descumprimento desta política poderá resultar no bloqueio definitivo do acesso ao e-mail corporativo.

8. RESPONSABILIDADES

- **Colaboradores:** Utilizar o e-mail corporativo conforme esta política e relatar atividades suspeitas.

- **Gestores:** Garantir que suas equipes cumpram as diretrizes estabelecidas.

- **Departamento de Tecnologia da Informação:** Monitorar, proteger e aplicar medidas de segurança para garantir o uso adequado do e-mail corporativo.

9. REVISÃO E ATUALIZAÇÃO

Esta política será revisada periodicamente para garantir sua eficácia e alinhamento com as melhores práticas de segurança da informação.