Política de Segurança da Informação e Comunicação

IN 004/2025 - IEMA

Cartilha

iema
INSTITUTO ESTADUAL DE MEIO AMBIENTE E RECURSOS HÍDRICOS

Este documento baseia-se na INSTRUÇÃO NORMATIVA N. º 004 DE 19 DE FEVEREIRO DE 2025 do Instituto Estadual de Meio Ambiente e Recursos Hídricos do Estados do Espírito Santo – IEMA.

POLÍTICA DE SEGURANÇA DE INFORMAÇÃO

E COMUNICAÇÃO

SUMÁRIO

1. INTRODUÇÃO

O Instituto Estadual de Meio Ambiente e Recurso Hídricos (IEMA) estabeleceu diretrizes essenciais para garantir a segurança da informação e o uso responsável dos recursos de tecnologia da informação e comunicação. Esta cartilha tem como objetivo conscientizar os usuários sobre boas práticas e regras que devem ser seguidas para assegurar a integridade dos sistemas institucionais.

2. OBJETIVOS

- Garantir a proteção de dados e informações institucionais.
- Promover o uso eficiente, ético e seguro dos recursos de Tecnologia da Informação e Comunicação (TIC).
- Estabelecer normas e procedimentos claros para o uso da rede corporativa.
- Criar o Comitê de Governança de Tecnologia da Informação e Comunicação (CGTIC) para fiscalização e orientação.
- Assegurar conformidade com normas e legislações vigentes, como a Lei Geral de Proteção de Dados (LGPD).

3. USUÁRIOS AUTORIZADOS

Os seguintes grupos têm permissão para acessar e utilizar os recursos de tecnologia do IEMA:

- Servidores efetivos e comissionados.
- Empregados terceirizados designados para funções institucionais.
- Estagiários e demais colaboradores com vínculo formal ao IEMA.
- Outros profissionais devidamente autorizados.

4. RESPONSABILIDADES INDIVIDUAIS

Cada usuário deve:

- Respeitar os direitos autorais e a propriedade intelectual de informações e softwares.
- Utilizar a rede e os sistemas de forma adequada e dentro das diretrizes institucionais.
- Manter sigilo sobre informações confidenciais e institucionais.
- Utilizar senhas seguras, alterá-las periodicamente e evitar compartilhamento.
- Realizar backups regulares para evitar perda de dados.

5. PROIBIÇÕES

É expressamente proibido:

- Utilizar a rede para difamação, assédio ou ameaças.

- Compartilhar credenciais de acesso com terceiros.
- Instalar softwares sem autorização do setor de TI.
- Utilizar os recursos de TI para atividades particulares, como propaganda política ou promoção comercial.
- Propagar vírus, malware ou qualquer forma de software prejudicial.
- Violar normas de proteção de dados e segurança da informação.

6. POLÍTICA DE ACESSO E AUDITORIA

- O setor de Tecnologia da Informação e Comunicação (TIC) realizará monitoramento contínuo da rede.
- Auditorias periódicas serão conduzidas para garantir conformidade e segurança.
- A concessão de acessos deve ser feita com base na necessidade funcional de cada usuário.

7. PENALIDADES

Infrações serão analisadas e podem resultar em:

- Advertência formal.
- Suspensão de acesso por períodos de 7 dias a 1 ano.
- Abertura de processos disciplinares para casos graves.
- Demissão e aplicação de sanções legais.

8. COMITÊ DE GOVERNANÇA DE TI (CGTIC)

- Composto por membros do IEMA e um representante da sociedade civil.
- Responsável por definir estratégias e diretrizes de TIC.
- Fiscalização periódica do cumprimento das normas de segurança.
- Reuniões trimestrais para revisão de políticas e melhorias.

9. PROCEDIMENTOS GERAIS

- Todos os usuários devem assinar um termo de compromisso para utilizar recursos de TIC do IEMA.
- Denúncias sobre infrações devem ser reportadas ao setor responsável.
- Em casos de ameaças à segurança da informação, medidas emergenciais serão adotadas.

10. CONSIDERAÇÕES FINAIS

- O desconhecimento das regras não isenta os usuários de suas responsabilidades.
- Casos omissos serão tratados pelo setor de Tecnologia da Informação e Comunicação do IEMA.
- A colaboração de todos é fundamental para garantir um ambiente digital seguro e eficiente dentro do IEMA.

11. CASOS OMISSOS A ESTE REGULAMENTO

Casos omissos a este regulamento serão tratados pelo Setor de Tecnologia da Informação e Comunicação (TIC).