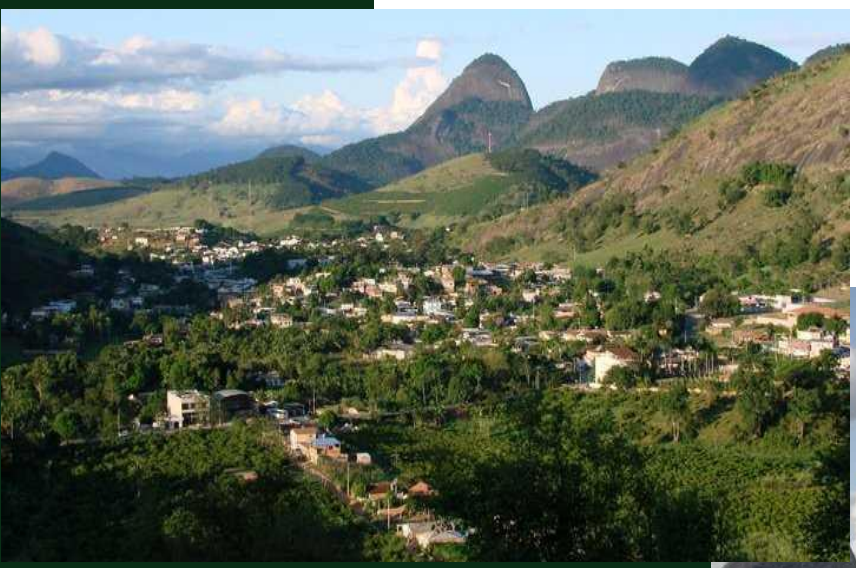
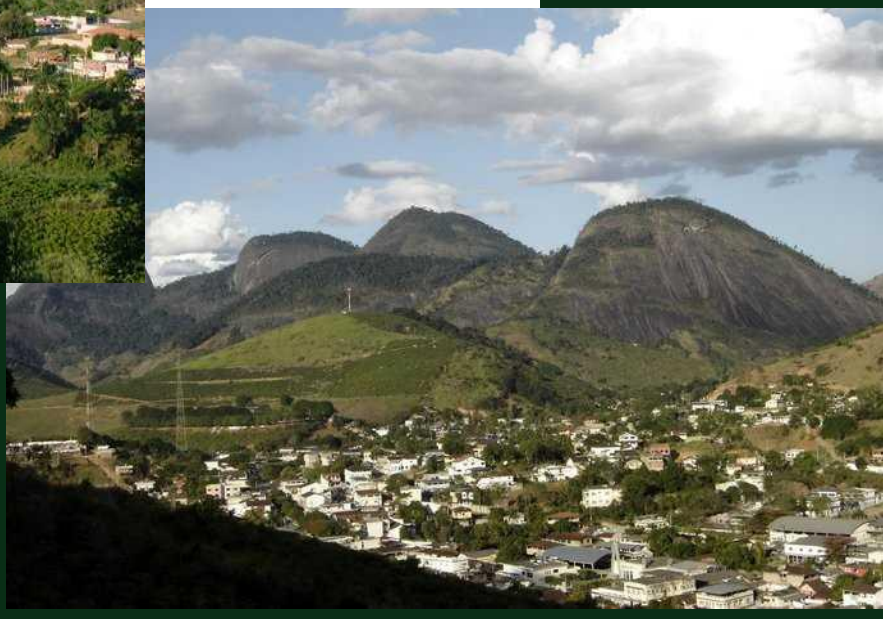
CARTILHA DA SEGURANÇA DA INFORMAÇÃO.





PREFEITURA MUNICIPAL DE JERÔNIMO MONTEIRO

SÉRGIO FARIAS FONSECA
PREFEITO MUNICIPAL

GENALDO RESENDE RIBEIRO
VICE PREFEITO

ELABORAÇÃO

CONTROLADORIA GERAL MUNICIPAL

DAYANI BITTENCOURT
CONTROLADORA PÚBLICA

Versão
1.1 Abril/2024

2024

SUMÁRIO

Sumário

OBJETIVO:

Esta cartilha tem como objetivo fornecer informações essenciais sobre segurança da informação, destacando sua importância e fornecendo orientações sobre como proteger as informações importantes.

POR QUE É IMPORTANTE GARANTIR A SEGURANÇA DAS INFORMAÇÕES?

- As informações são um dos ativos mais valiosos de uma organização, e sua perda, roubo ou divulgação indevida pode ter consequências graves, como danos à reputação, perda financeira e violações de privacidade.

- Garantir a segurança das informações é fundamental para proteger os interesses da organização, seus clientes e colaboradores, além de cumprir requisitos legais e regulatórios.

O QUE É SEGURANÇA DA INFORMAÇÃO?

Segurança da Informação é o conjunto de medidas e práticas adotadas para proteger as informações contra ameaças como acesso não autorizado, uso indevido, divulgação inadequada, alteração não autorizada, destruição acidental ou intencional, entre outros.

POR QUE SE PREOCUPAR COM SEGURANÇA DA INFORMAÇÃO?

- A segurança da informação é essencial para garantir a confidencialidade, integridade e disponibilidade das informações, preservando sua qualidade e valor.

- A preocupação com a segurança da informação ajuda a reduzir os riscos de exposição a ameaças cibernéticas, como ataques de hackers, malware e phishing, que podem comprometer os sistemas e dados da organização.

OS CINCO PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO:

- ✓ Confidencialidade: Garantir que as informações sejam acessadas apenas por pessoas autorizadas.

- ✓ Integridade: Assegurar que as informações não sejam alteradas ou corrompidas de forma não autorizada.

- ✓ Disponibilidade: Garantir que as informações estejam disponíveis quando necessárias para os usuários autorizados.

- ✓ Autenticidade: Verificar a identidade dos usuários e garantir que apenas pessoas autorizadas tenham acesso aos sistemas e informações.

- ✓ Não repúdio: Garantir que as ações realizadas pelos usuários possam ser rastreadas e atribuídas a eles, evitando que neguem a autoria de suas ações.

PRINCIPAIS AMEAÇAS À SEGURANÇA DA INFORMAÇÃO:

- Ataques de hackers e criminosos cibernéticos.
- Malware (vírus, worms, trojans, ransomware, etc.).
- Phishing e engenharia social.
- Roubo ou perda de dispositivos (computadores, smartphones, pen drives, etc.).
- Falhas de segurança em sistemas e aplicativos.
- Erros humanos, como compartilhar informações confidenciais por engano.

BOAS PRÁTICAS DE SEGURANÇA DA INFORMAÇÃO:

- Utilize senhas fortes e únicas para cada conta e sistema.
- Mantenha seus sistemas e programas sempre atualizados.
- Evite clicar em links ou baixar anexos de fontes desconhecidas.
- Faça backup regularmente dos seus dados importantes.
- Esteja atento a solicitações de informações pessoais ou confidenciais por e-mail ou telefone.
- Proteja seus dispositivos com antivírus e firewall.

- Não compartilhe suas credenciais de acesso com outras pessoas.
- Utilize uma conexão segura (HTTPS) ao acessar sites sensíveis ou realizar transações online.
- Esteja ciente das políticas de segurança da informação da sua organização e siga-as rigorosamente.
- Mantenha-se atualizado sobre as últimas ameaças e técnicas de segurança.

Lembre-se de que a segurança da informação é responsabilidade de todos. Adote essas práticas em sua rotina para proteger seus dados e informações contra ameaças cibernéticas.