

Conscientização em Segurança da Informação

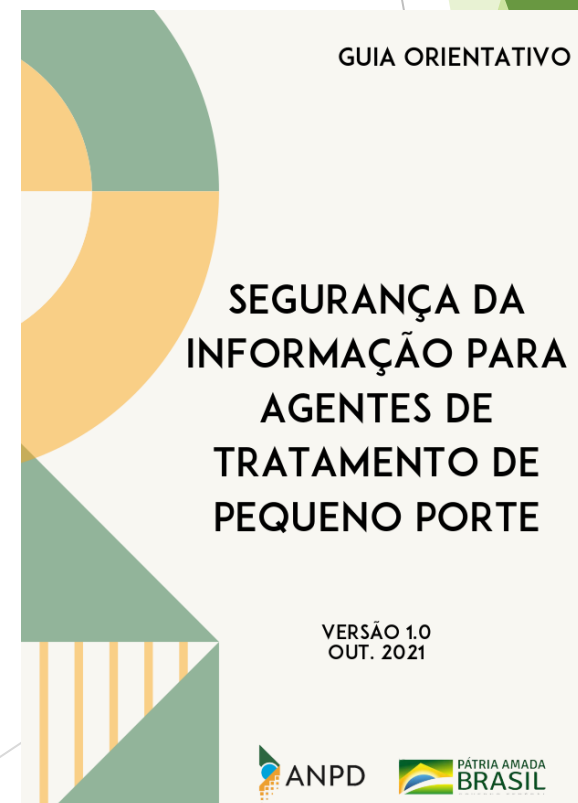
Fevereiro/2022

Objetivo

Sensibilizar todos os funcionários da cooperativa, especialmente aqueles diretamente envolvidos na atividade de tratamento de dados, sobre a execução de suas atividades observando as orientações de Segurança da Informação.

28. Algumas informações úteis que podem ser passadas aos funcionários são:

- como utilizar controles de segurança dos sistemas de TI relacionados ao trabalho diário;
- como evitar de se tornarem vítimas de incidentes de segurança corriqueiros, tais como contaminação por vírus ou ataques de phishing, que podem ocorrer, por exemplo, ao clicar em links recebidos na forma de pop-up de ofertas promocionais ou em links desconhecidos que chegam por e-mail;
- manter documentos físicos que contenham dados pessoais dentro de gavetas, e não sobre as mesas;
- não compartilhar logins e senhas de acesso das estações de trabalho;
- bloquear os computadores quando se afastar das estações de trabalho, para evitar o acesso indevido de terceiros;
- seguir as orientações da política de segurança da informação.



"Os recursos humanos de uma organização são o fator preponderante para o sucesso das medidas que se referem à segurança da informação e à proteção de dados pessoais, já que efetivamente são as pessoas que trabalham para os agentes de tratamento de pequeno porte que realizarão o tratamento dos dados pessoais."

ANPD

Política de Segurança da Informação



Documento mais importante para uma organização quando se trata de proteger seus ativos.

Nela estão contidas a visão e as diretrizes gerais da organização quanto a Segurança da Informação.

Não detalha os controles de segurança, esses são detalhados através de normativos específicos (ex: norma de senhas, norma de backup, etc).

Controles?



- usuário e senha para acesso a rede, dispositivos e sistemas;
- cópia de segurança dos arquivos críticos;
- antivírus atualizado;
- gerenciamento da atualização dos programas;
- firewall de rede;
- autenticação multi fator nos dispositivos e sistemas;
- criptografia de dados sensíveis;

Como utilizar controles de segurança dos sistemas de TI relacionados ao trabalho diário?

Protegendo informações na web



Não publique na Internet documento contendo credencial de acesso a sistemas internos ou de terceiros.

Utilize um provedor de site que possibilite auditoria nos acessos ao site.

Somente forneça acesso a partes mais específicas do site através de área restrita.

Adeque seu processo de publicação de documentos e informações na web.

Notificações



Observe se alguma notificação do seu computador fica aparecendo de forma insistente para você.

Diversos programas são configurados para exibir notificação em caso necessidade de ações adicionais.

Pode ser que seu computador esteja com algum problema, como vírus não eliminado, programa necessitando de atualização, etc.

Multi Fator de Autenticação



Sempre habilite o Multi Fator de Autenticação (MFA) em qualquer dispositivo, sistema ou aplicativo que você usa.

Somente as senhas hoje em dia não garantem proteção adequada.

Senhas



Sempre utilize senhas fortes (mais de 8 caracteres contendo letras maiúsculas e minúsculas, números, caracteres especiais).

Nunca utilize para trabalho as senhas que são usadas em seus acessos particulares.

Não compartilhe seus logins e senhas de acesso das estações de trabalho.

Como evitar de se tornar vítima de incidentes de segurança corriqueiros?

Ataque de Phishing

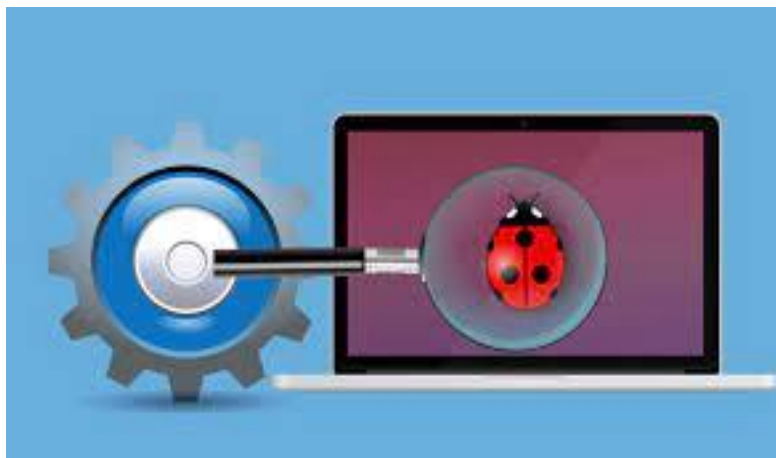


Sempre desconfie de e-mail que solicite clique em algum link ou download de algum anexo.

Observe a ortografia e a identificação visual do remetente.

Se não for um e-mail esperado mas que aparenta ser legítimo, entre em contato diretamente com o remetente verdadeiro por outro canal de comunicação.

Antivírus



Não desative o antivírus de sua estação de trabalho e mantenha-o atualizado.

Normalmente o antivírus não pede intervenção, mas se seu antivírus notificar alguma detecção de ameaça, sempre execute a ação mais restritiva (excluir, quarentena, etc).

Postura segura no dia a dia



- ▶ Sempre bloqueie sua estação de trabalho ao se ausentar;
- ▶ Não mantenha senhas e outras informações importantes expostas na sua mesa;
- ▶ Desconfie sempre de qualquer pedido de informação por telefone;
- ▶ Marque os e-mails suspeitos como Spam;
- ▶ Reporte qualquer não conformidade à Política de Segurança.