# CARTILHA DE **SEGURANÇA**

Dicas valiosas para você proteger seus dados.

Rech®
INFORMÁTICA
SISTEMAS DE GESTÃO **ERP BI Mobile**

# A importância do backup para a segurança da suas informações.

A perda de dados em consequência de um dano no servidor ou no próprio computador é hoje uma das principais preocupações de uma empresa. Devido a isso, o backup de todas as informações é de fundamental importância e tem se tornado uma opção valiosíssima para empresas que dependem de sistemas informatizados para o faturamento e produtividade de seus negócios.

**O backup é a única forma de recuperar informações em caso de pane. Talvez você nunca precise utilizá-lo, porém é melhor prevenir.**

Confira 5 práticas recomendadas para a realização de backups e proteger os dados da empresa:

**1) Defina a estratégia de backup**
Com uma estratégia bem definida a recuperação dos dados será rápida e eficaz.

**2) Defina os responsáveis e capacite os mesmos**
De acordo com o nível de segurança necessário para as informações, defina os responsáveis pela realização e restauração do backup, atribua acesso às informações e capacite os mesmos para realização dos processos.

**3) Faça backup de todos os dados importantes para a empresa, do ERP SIGER®, arquivos, e-mails e demais sistemas.**
A periodicidade do backup pode ser planejada conforme a demanda de atualização das informações, podendo ser diários, semanais, mensais, etc.

**4) Faça cópias em diferentes mídias**
Mantenha cópias das informações em diferentes mídias e locais. Guarde pelo menos uma cópia em ambiente seguro. As mídias podem ser pendrives, HDs externos, servidores em outros locais ou na nuvem, DVDs, etc.

**5) Execute testes de restaurações**
Periodicamente faça tentativas de restauração para verificar se os arquivos foram copiados da forma correta e descobrir possíveis problemas de hardware.

**LEMBRE-SE!**

A Rech Informática não tem acesso a sua base de dados **a realização do backup é de total responsabilidade da empresa.**

**DICA:** no ERP SIGER®, existe um recurso que auxilia você na realização do backup, basta acessar o menu 94A - BACKUP DA BASE DE DADOS.

# Apresentação

A Cartilha de Segurança tem como objetivo fornecer dicas de segurança da informação para os usuários da internet, principalmente para aqueles que desconhecem ou não tomam todas as precauções necessárias na hora de acessar a internet.

Mesmo sendo a internet uma tecnologia altamente presente em nosso dia-a-dia, devemos sempre nos precaver e evitar que nossos dados, imagens, senhas e outras informações postadas ou utilizadas na rede estejam desprotegidos.

# Conceitos

## O que é Segurança da Informação?

Denomina-se Segurança da Informação a proteção existente sobre as informações de uma determinada empresa ou pessoa. Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa.

## Cuidado com os vírus de computador

1. Eles são instalados e funcionam sem que o usuário perceba;

2. Estão por todos os lados na Internet;

3. Podem roubar senhas e apagar informações preciosas de seu computador;

Ao perceber que foi infectado por um vírus, desligue seu computador e acione a equipe de informática da sua empresa ou procure ajuda de um profissional da sua confiança;

Vírus e outros malwares se disseminam de diversas formas, tais como:

- acessando sites suspeitos;
- embutidos em arquivos ou programas baixados pela Internet, anexados a e-mails ou recebidos por meio de sites de relacionamento e redes sociais;
- utilizando dispositivos infectados: CD, pen-drives ou cartões de memória.

## Dicas para manter seu computador seguro

Instale um bom programa de antivírus e, pelo menos uma vez por semana, faça uma verificação completa do computador;

Use sempre cópia original do programa de antivírus, pois as cópias "piratas" geralmente já estão infectadas e não funcionam corretamente;

Configure seu antivírus para procurar por atualizações diariamente;

Use seu antivírus para verificar todo arquivo baixado antes de abrí-lo ou executá-lo pela primeira vez;

Cópias originais do Windows são mais seguras e são atualizadas periodicamente pela Microsoft;

Mantenha o sistema operacional do seu computador e seus programas sempre atualizados para protegê-los contra as falhas de segurança, que são descobertas todos os dias;

Somente instale programas de fontes confiáveis. Evite os serviços de compartilhamento (por exemplo: Kazaa, Bittorrent, Limeware, Emule, etc.). Eles são uma das principais fontes de disseminação de programas nocivos;

Não abra e-mails e arquivos enviados por desconhecidos;

Não abra programas ou fotos que dizem oferecer prêmios;

Cuidado com os e-mails falsos de bancos, lojas e cartões de crédito;

Jamais abra arquivos que terminem com PIF, SCR, BAT, VBS e, principalmente, os terminados com EXE e COM;

Se você desconfiar de um e-mail recebido, mesmo quando enviado por pessoa conhecida, cuidado, pois pode ser um e-mail falso: não abra. Apague-o e não utilize o contato.


# Senhas

Sua senha é pessoal e intransferível. Compartilhar sua senha é como assinar um cheque em branco;

Não escreva a senha em local público ou de fácil acesso como, por exemplo, em sua agenda, em um pedaço de papel pregado no seu monitor ou guardado na sua gaveta;

Troque a senha regularmente ou sempre que suspeitar de quebra de sigilo;

Não utilize números fáceis de serem descobertos, tais como o número da carteira de identidade, do CPF e de outros documentos ou datas de qualquer espécie, como sua senha bancária.

# Navegando na Internet com Segurança

## Fique atento aos endereços acessados no seu navegador

Verifique se o endereço que está aparecendo em seu navegador é realmente o que você queria acessar;

Não confie em tudo o que vê ou lê; O navegador não garante sozinho a segurança de informações pessoais, senhas e dados bancários;

Não autorize instalação de software de desconhecidos ou de sites estranhos;

Antes de clicar em um link, veja na barra de status do navegador se o endereço de destino do link está de acordo com a descrição do mesmo;

Sempre desconfie de ofertas e sorteios dos quais não tenha prévio conhecimento.

## Compras e Pagamentos

Ao realizar compras pela Internet procure por sites reconhecidamente seguros;

Se for utilizar o seu cartão de crédito ou tiver que fornecer dados bancários, verifique se a página acessada utiliza tecnologia de criptografia: o endereço da página acessada deve começar com "https"; verifique se aparece o ícone do cadeado na barra de status (parte inferior) ou à direita da caixa do endereço, dependendo do navegador;

Confie em seus instintos. Se você desconfiar de um site de compra, deixe-o de lado e compre em outro lugar.

# Utilização do E-mail e programas de mensagens

## Nunca abra e-mails ou execute arquivos enviados por desconhecidos

Pode haver muitas informações falsas e golpes nas mensagens. E-mail é o método mais utilizado para a disseminação de vírus;

Não clique em links recebidos por email e, caso seja necessário clicar, fique atento para ver onde ele irá levar;

Atenção com cartões virtuais. Não abra quando o nome do arquivo tiver a extensão "exe" no final, pois podem ser programas de invasão;

Não acredite em todos os e-mails sobre vírus, principalmente aqueles de origem duvidosa que trazem anexo arquivo para ser executado, prometendo solucionar o problema;

Jamais acredite em pedidos de pagamento, correção de senhas ou solicitação de qualquer dado pessoal por e-mail. Comunique-se por telefone com a instituição que supostamente enviou o e-mail e confira o assunto.

## Bancos não enviam e-mails não solicitados a seus clientes

Fraudadores bancários geralmente enviam e-mails falsos solicitando que você informe seus dados ou senhas bancárias;

Muitas vezes falsos e-mails de bancos levam você a clicar em links que podem causar situações perigosas, como: levá-lo a um site falso do seu banco para capturar o número da sua conta e senha;

Utilização do E-mail e programas de mensagem instantânea com segurança instalar um programa malicioso em sua máquina para roubar suas informações, monitorar suas atividades ou mesmo obter o controle de seu computador.

## Fique atento ao utilizar programas como Google Talk, Skype, etc.

Esses programas estão sempre conectados a um servidor central e podem ser atacados por pessoas mal-intencionadas;

Nunca aceite arquivos de pessoas desconhecidas, principalmente se tiverem a extensão "exe" e "doc", pois podem conter vírus ou outro malware;

Caso haja necessidade, tenha um antivírus atualizado e certeza da pessoa que está enviando.

# Engenharia Social

Consiste da obtenção de informações importantes por meio de uma conversa informal, aproveitando da ingenuidade das pessoas, explorando sua confiança ou a vontade de ajudar;

Geralmente o golpista se faz passar por outra pessoa ou finge ser um profissional de determinada empresa ou área;

O indivíduo mal intencionado usa o telefone, e-mail, salas de bate-papo, sites de relacionamento e mesmo o contato pessoal para conseguir as informações que procura;

Desconfie de abordagens de pessoas que ligam e se identificam como técnicos ou funcionários de determinada firma, solicitando dados sobre sua empresa, sobre o ambiente, sobre você etc;

Evite fazer cadastros pela Internet, especialmente fornecendo seus dados pessoais. Se necessário, somente o faça se confiar no site;

Nunca forneça informações sensíveis, pessoais ou da empresa, por telefone ou outros meios, quando a iniciativa do contato não seja sua;

Nunca forneça sua senha por telefone, e-mails ou outros meios que não sejam o acesso normal aos aplicativos utilizados, ao site do seu banco ou às máquinas de auto-atendimento;

O lixo pode ser uma fonte de informações para pessoas mal-intencionadas. Destrua os documentos que contenham informações sensíveis, pessoais ou corporativas antes de descartá-los no lixo.

Rech®
INFORMÁTICA

SIGER®
SISTEMAS DE GESTÃO ERP BI Mobile

INDÚSTRIAS
DISTRIBUIDORES
COMÉRCIO
SERVIÇOS

(51) 3582-4001
www.rech.com.br

comercial@rech.com.br
/SistemaSIGER

Rua Tupanciretã, 460 - Bairro: Ideal
Novo Hamburgo - RS - CEP 93.334-480
CNPJ 93.419.380/0001-84 - IE 086/0284336