
6 PRÁTICAS
RECOMENDADAS PARA
PROTEGER SUA REDE!
MANTENHA SEUS DADOS PROTEGIDOS

QUAL A IMPORTÂNCIA DE MANTER SEUS DADOS SEGUROS?

Dentre outras coisas, a segurança de rede tem como objetivo: garantir que o acesso de dados compartilhados por uma instituição seja feito apenas para quem possui autorização, além de proteger a usabilidade e integridade das conexões e informações.

Grupo Dunamys

É fato que nenhuma organização está 100% segura, mesmo porque os responsáveis por crimes cibernéticos estão cada vez mais se aprimorando e encontrando alternativas para burlar qualquer tipo de proteção.

Mesmo assim, as tecnologias e os mecanismos de segurança de dados acompanham o ritmo das ameaças para conter esse avanço.

Lei de Proteção de Dados e os direitos do indivíduo

Toda nova legislação prevê uma adequação de conduta ao grupo que será implicado na lei. A partir de 2021, a proteção de dados pessoais passou a configurar como direito fundamental pela Constituição Federal. A Lei de Proteção de Dados, no entanto, não atua diretamente no direito da pessoa. No entanto cria-se mecanismos para proteger dados pessoais a partir de quem faz o tratamento deles.

1º Autenticação de dois fatores:

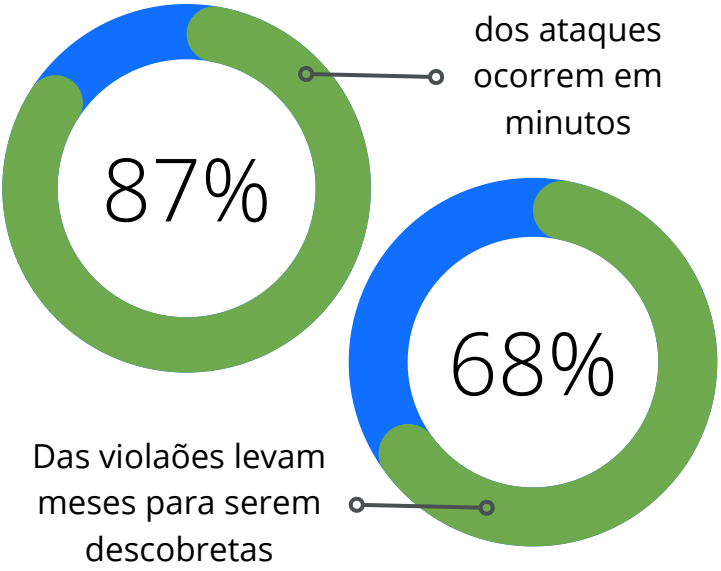
A utilização dessa ferramenta costuma ser mais comum por instituições financeiras. Já que reduz bem os riscos de uma senha roubada ser utilizada para acessar os dados do cliente. Pode parecer algo simples, mas com a autenticação de dois fatores são duas informações para serem descobertas e não apenas uma, o que dificulta o crime.

2º Nuvem como ambiente seguro:

Utilizar a nuvem como lugar seguro para salvar os dados é algo possível. Porém, alguns fatores são necessários: uso de firewalls básicos e avançados que avaliam ameaças, registros de eventos, que identificam todas as ações da rede e podem ajudar a prevenir violações e criptografia de dados, que os mantém protegidos contra usuários não autorizados,

3º Treinamento para colaboradores para segurança de dados:

Não está claro para todas as pessoas como é importante manter seus dados seguros. Por isso, cursos sobre segurança da informação podem ser uma alternativa para quem deseja que os colaboradores protejam os sistemas da empresa – e seus próprios dados de tabela! Cursos práticos, por exemplo, podem reunir simulações de armadilhas e ataques para que todos estejam atentos caso haja uma tentativa de invasão por cibercriminosos.



4º A importância do backup:

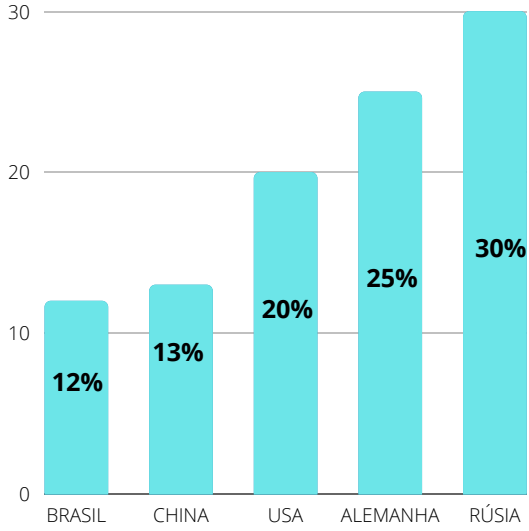
Só quem já perdeu dados importantes sabe como é fundamental ter uma cópia de segurança. Para proteger os dados e evitar prejuízos, é recomendado que a empresa faça backups recorrentes.
Atualmente, contratar um servidor em nuvem é a forma mais segura, confiável e econômica para armazenar dados. O backup no ambiente cloud reduz riscos de violação da informação, é flexível para atender qualquer porte de empresa e garante maior proteção para todas as suas informações.
Fale com a Plus-IT sobre ecossistemas cloud e aplicações customizáveis com segurança de dados, conectividade e integração.

5º Invista em softwares e de proteção:

Uma das principais medidas preventivas a serem adotadas nas empresas é a instalação de um bom antivírus que previne, detecta e elimina ameaças do computador.

Invista também em um programa de Firewall eficiente e ative filtros anti-spam que servem para evitar riscos e golpes que ocorrem por meio da internet.

Outra dica importante é manter sempre os seus softwares e programas atualizados. O motivo é simples: atualizações corrigem falhas de segurança e diminuem os riscos de ataques na rede.



FONTE:ESTATÍSTICAS | Mapa em tempo real de ameaças cibernéticas da Kaspersky

6º Invista em FIREWALLS e de proteção:

Um firewall é uma solução de segurança de rede que protege sua rede contra tráfego indesejado. Os firewalls bloqueiam o malware de entrada com base em um conjunto de regras pré-programadas. Essas regras também podem impedir que os usuários na rede acessem determinados sites e programas.

Os firewalls são baseados na ideia simples de que o tráfego de rede de ambientes menos seguros deve ser autenticado e inspecionado antes de passar para um ambiente mais seguro. Isso evita que usuários, dispositivos e aplicativos não autorizados entrem em um ambiente ou segmento de rede protegido. Sem firewalls, os computadores e dispositivos em sua rede ficam suscetíveis a ataques e tornam você um alvo fácil para ataques.

ORÇAMENTO FIREWALL

ACESSAR PÁGINA