**Cibersegurança: saiba como proteger seus dados e quais as obrigações de empresas e clientes**

*No Dia Internacional de Proteção de Dados, especialista dá dicas para ampliar a segurança da informação no ambiente digital; Brasil é o país com maior volume de vazamentos do mundo*

O Dia Internacional da Proteção de Dados, celebrado em 28 de janeiro, alerta a sociedade sobre os cuidados que pessoas físicas e jurídicas devem ter no compartilhamento, tratamento e armazenamento de informações sigilosas, principalmente no ambiente digital. “A proteção de dados é uma responsabilidade que deve ser compartilhada entre os clientes e as empresas. Por isso, além das medidas que as organizações têm que adotar para manter o sigilo de informações, os usuários também devem ter atitudes preventivas no dia a dia”, destaca Fábio Fukushima, especialista em cibersegurança e diretor da L8 Security, empresa especializada em segurança da informação.

O Brasil é o país que registra o maior volume de vazamentos do mundo, com mais de 2 bilhões de dados sigilosos vazados somente em 2023, segundo levantamento mais recente da NordVPN, empresa global de cibersegurança. As informações pessoais como nome, e-mail, cidade, senha e endereço residencial estão entre os dados mais expostos.

Fábio Fukushima lembra que a Lei Geral de Proteção de Dados (LGPD), em vigor no Brasil desde 2020, prevê uma série de penalidades e determina as obrigações das empresas no tratamento das informações sensíveis de clientes e colaboradores. Ele destaca cinco medidas que podem ajudar as corporações a ampliarem a segurança da informação, evitando ataques cibernéticos:

1 – Treinamento de colaboradores em segurança cibernética: a conscientização é o primeiro passo para um ambiente digital seguro. Realizar treinamentos regulares com os colaboradores para que conheçam as melhores práticas de segurança é fundamental para evitar que caiam em golpes de engenharia social como o phishing, por exemplo.

2 – Implementação de um protocolo de crise: ter um sistema de detecção e resposta a incidentes de segurança é um dos principais pilares da segurança da informação. Assim, caso uma ameaça seja identificada é possível agir de forma rápida para investigar e responder às violações de dados;

3 – Criptografia e controle de acesso: criptografar dados sensíveis, tanto em repouso quanto em trânsito e implementar um sistema de controle de acesso baseado em papéis, garantindo que apenas usuários autorizados tenham acesso aos dados necessários para suas funções, também são medidas necessárias para uma boa gestão de redes corporativas;

4 – Gestão de vulnerabilidades: realizar auditorias regulares e testes de intrusão (pentests) para avaliar a segurança dos sistemas e identificar as vulnerabilidades também auxilia a manter a proteção de dados das empresas. “Em cibersegurança, a prevenção é sempre o caminho mais indicado. Isso porque ao identificar as possíveis vulnerabilidades é possível corrigir as falhas antes que alguém mal-intencionado acesse a rede e sequestre os dados, tornando o ambiente mais seguro”, explica Fábio Fukushima.

5 – Uso de soluções de segurança: utilizar firewalls, antivírus, sistemas de detecção de intrusão e outras ferramentas de segurança para proteger os sistemas e dados da empresa é importante para todas as empresas, independentemente do tamanho ou ramo de atuação.

Fábio Fukushima ressalta, no entanto, que os usuários também têm um papel fundamental na proteção de suas informações na internet. Entre os cuidados que devem ser tomados estão o acesso somente a redes Wi-Fi seguras, o uso de anti-vírus atualizados e ter muita cautela no momento de acessar promoções ou fazer cadastros online.

“Antes de fornecer os dados a qualquer empresa, site ou aplicativo, é indispensável ler atentamente a política de privacidade. Desta forma o usuário saberá como os seus dados serão coletados, armazenados e compartilhados. Se tiver alguma dúvida, procure outras opções ou entre em contato com a empresa”, alerta Fábio Fukushima. “Vale lembrar que a LGPD garante alguns direitos aos titulares dos dados, como acesso, retificação anonimização, bloqueio e eliminação de dados sempre que for solicitado”, complementa.

Outra medida que ajuda a proteger os dados na internet é evitar compartilhar informações desnecessárias em perfis online ou nas redes sociais e utilizar senhas fortes e únicas para cada conta, ativando, sempre que possível, a autenticação em duas etapas.

**Sobre a L8**

Fundado em 2014, o Grupo L8 é formado pela L8 Security, especializada em soluções para segurança da informação; pela L8 Energy, que atua na industrialização e distribuição de sistemas fotovoltaicos; e pela L8 GROUP, holding operacional do grupo que atua com foco em Telecomunicações e Segurança Eletrônica. Com a missão de facilitar e otimizar a utilização de tecnologias diferenciadas, oferecendo soluções com valor agregado aos clientes, o grupo preza por inovação e materiais de qualidade, tornando-se referência no mercado brasileiro. [www.l8group.net](http://www.l8group.net/)