

Os Pilares da Segurança da Informação nas Empresas

Edição nº25
Julho/2022

A segurança da informação é a área do conhecimento dedicada à proteção dos ativos de informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade. A infraestrutura de segurança da informação é composta por medidas de segurança física, lógica e de recursos humanos. Práticas que permitem o acesso não autorizado a dados, lugares ou objetos fragilizam a segurança da informação, uma vez que as pessoas ou programas maliciosos acabam tendo acesso a informações indevidas, colocando em risco informações valiosas das organizações para as quais trabalham e até mesmo dados pessoais.



A questão comportamental pode afetar significativamente as demais medidas de segurança, por mais modernas que elas sejam. Por maiores que sejam os investimentos em tecnologia e processos, a corrente pode se romper com:

- Servidores, colaboradores ou estagiários descontentes, que conhecem muito bem o que estão fazendo e se propõem a sabotar a organização em que trabalham;
- Colaboradores demitidos, que tiram proveito de seu conhecimento acerca da tecnologia e dos processos internos da organização para lesá-la;
- Colaboradores mal treinados, que não conhecendo as tecnologias, os processos e os perigos aos quais estão expostos colocam em risco involuntariamente os ativos da organização;
- Servidores, colaboradores ou estagiários relapsos, que por mais que saibam lidar com os vários aspectos da segurança da informação, de forma irresponsável negligenciam este conhecimento e derrubam, de dentro, todas as barreiras levantadas para proteção dos ativos da organização.

Pessoas mal intencionadas podem conseguir obter acesso aos mais diversos ambientes da organização ou a senha de acesso aos sistemas da organização, através de uma das técnicas utilizadas pela Engenharia Social (boletim no 16 Outubro/2021).

Um ambiente de trabalho propício à boa segurança da informação deve levar em consideração alguns fatores:

- Manter mesas limpas, sem papéis com informações sensíveis expostas (como, por exemplo, senhas anotadas);
- Observar se alguém está olhando sua senha enquanto a digita no computador;
- Evitar beber ou comer próximo aos computadores, evitando danos graves a eles;
- Bloquear a estação de trabalho ao se ausentar da sala.

Algumas dicas para um ambiente de trabalho seguro:

- Adote práticas de mesa e tela limpas: evite que informações sensíveis – senhas, relatórios, informações pessoais ou funcionais – sejam deixadas desprotegidas em sua mesa ou na tela do computador, *smartphone* ou *tablet*.
- Use áreas com trancas: gavetas, armários, cofres, salas para armazenar CDs, DVDs, *pendrives*, documentos, *notebooks*, *tablets*, *smartphones*, que possuam informações sensíveis e quando não estiverem em uso.
- Computadores e dispositivos similares (boletim no 23 Maio/2022) devem estar dispostos de forma a evitar que transeuntes tenham a oportunidade de olhar as telas. Use protetores de tela temporizados e protegidos por senha.
- Desligue os equipamentos ao final do dia, principalmente os que estiverem conectados em rede.
- Restrinja o uso de celulares, câmeras, e notebooks em ambientes nos quais se manipulem informações sensíveis.
- Adote uma cultura sem papel, não imprima documentos desnecessariamente, evite deixar lembretes em monitores, teclados ou na mesa. O descarte adequado das informações armazenadas em meio físico deve ser realizado de forma segura como, por exemplo, fragmentadoras.

Além da proteção contra acesso não autorizado, estas medidas também podem proteger a informação e os ativos contra desastres tais como incêndios, inundações ou explosões.

Fique ligado: no próximo mês, falaremos sobre **Gestão de Riscos de Segurança da Informação**