

**PESQUISA DE SEGURANÇA
DA INFORMAÇÃO
E COMUNICAÇÃO NA CAPES**

BOLETIM DTI N. 2



Resultado da Pesquisa de Segurança Informação e Comunicação na CAPES

Um dos principais desafios da Administração Pública nos últimos anos é o de proporcionar ações e políticas de segurança da informação e comunicação, que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, no contexto de todos os órgãos e entidades governamentais.

Em conformidade com as melhores práticas, a CAPES promove medidas para garantir a devida proteção ao seu ambiente tecnológico, incluindo seus ativos de informação (equipamentos, softwares, sistemas etc.), que possuem um valor incalculável para esta Fundação, não só pelo seu patrimônio material histórico, como pela criticidade das informações inerentes ao seu negócio e à sua Missão Institucional em prol da sociedade brasileira.

Uma das iniciativas adotadas é a realização de uma pesquisa, que objetiva avaliar o conhecimento e a conscientização do público interno da CAPES em relação à Segurança da Informação e Comunicação no contexto da Fundação. A análise dos resultados obtidos possibilitará o desenvolvimento e aplicação de medidas de segurança, bem como o aprimoramento das ações atualmente em execução.



Responsabilidade e Normas de Segurança

A pesquisa verificou que **70%** das pessoas confirmaram saber da existência de um comitê responsável pela segurança da informação. Todavia, **22%** não sabem se existe uma Política de Segurança da Informação na CAPES.

Estimulados por outra questão, **88%** declararam entender que a responsabilidade de manter os dados da CAPES seguros não é somente de equipes ou grupos de segurança, mas sim de todos aqueles que acessam tais informações.

Tendo em vista que **36%** declararam não saber se há informações de regulamentação sobre segurança, reforçamos os locais e meios em que tais portarias são publicadas: [PoSIC](#), [Normas de Acesso à Internet](#), correio eletrônico, [site institucional da CAPES](#), [Intranet](#), entre outras.



Percepção da Segurança

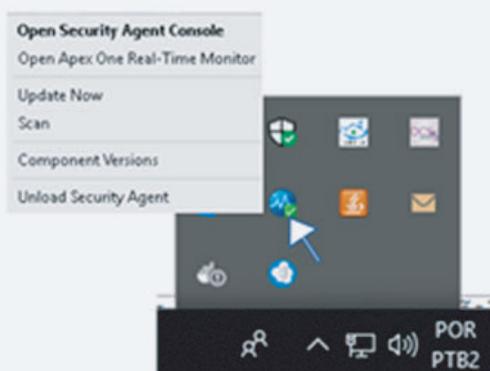
Em tempos de trabalho remoto, avaliamos a percepção da segurança dos computadores pessoais, sendo que **66%** consideram que tomam as devidas precauções.

Já **26%** dos usuários não sabem informar, desconhecem a existência do antivírus ou não sabem se está instalado e/ou atualizado no computador da CAPES. Além disso, **68%** sabem que os computadores de seu uso na sede da Fundação estão configurados para receber atualizações do sistema operacional diariamente.

Infelizmente, **16%** acreditam que a sua conta da CAPES (usuário/senha) não é de interesse dos hackers, não obstante as notícias atuais sobre ataques indiscriminados a órgãos do governo. Apesar disso, **92%** consideraram o computador da CAPES muito/suficientemente seguro. Para melhorar essa percepção, seguem algumas dicas para manter o computador seguro:

Percepção da Segurança

- Usar/Atualizar antivírus
 - No caso da CAPES, clique com botão direito no ícone azul (Trend Micro) para detalhes



- Utilizar um firewall, como por exemplo o nativo do próprio Windows;
- Bloquear a tela do computador, quando se ausentar de seu lugar;
- Utilizar usuários individualizados na família, com senhas distintas;
- Reiniciar o computador, quando for solicitado pelas atualizações.



Conhecimento sobre Ameaças

Apesar de 80% terem respondido que são cuidadosos ao prevenir o golpe de phishing, para esse tipo de ameaça basta um usuário ser “fisgado”, enviando usuário/senha para que um atacante possa fazer estragos no ambiente computacional. Por conta disso, a DTI tem feito campanhas para treinar a atenção contra este tipo de ataque, cada vez mais comum em nosso cotidiano.

Além disso, 14% não souberam afirmar que SPAM é uma mensagem não solicitada; 16% não consideraram arquivos executáveis como vetores de vírus; 40% desconhecem as ameaças de negação de serviço (DDoS) que derrubam sites, causando sua indisponibilidade, e 12% desconhecem que um ransomware criptografa arquivos e exige pagamento (resgate), sendo umas das piores ameaças do mundo digital atualmente. Vale destacar que, em média, a CAPES sofre mais de 9 milhões de ataques por mês aos seus sistemas, detectados pelos mecanismos de segurança implantados em seu ambiente. Sem mencionar que, do total de e-mails recebidos mensalmente, em torno de 65% são SPAMS/phishing. Já a média de infecções das estações de trabalho dos usuários está na casa de quase 3 mil, afetando aproximadamente 85 máquinas infectadas/mês.

Detalhes e dicas sobre [como se prevenir de phishing](#).



Melhores Práticas

A partir das respostas, observa-se que **6%** dos usuários já compartilharam suas senhas da rede CAPES com outras pessoas, e **8%** costumam utilizar a mesma senha dos sistemas da CAPES em sistemas externos ao órgão, sendo ambas as práticas temerárias para quem preza ou possui um mínimo de conhecimento acerca de segurança.

Além disso, um outro dado ruim obtido na pesquisa foi de que apenas **30%** dos usuários trocam suas senhas entre 3 e 6 meses.

Recomendações:

- Nunca compartilhe senhas, elas são pessoais;
- Utilize as senhas da CAPES somente no ambiente da CAPES;
- Troque suas senhas com certa frequência;
- Opte por senhas complexas, utilizando números, letras e caracteres, como por exemplo, C@P&\$.

Veja aqui o [resultado completo da pesquisa!](#)