Comunicar para Educar
abril/2023 - Ano 4 - nº 38

BIM

Boletim Informativo Mensal

Política de Segurança da Informação

A Política de Segurança da Informação é um documento muito importante para qualquer organização, pois fornece diretrizes, critérios e suporte administrativo para a implementação de ações de segurança da informação. Assim, a elaboração desse documento é obrigatória para os órgãos e as entidades da administração pública federal. As ações de segurança da informação objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.

Para respaldar ainda mais o uso dessa e de outras ferramentas de segurança da informação no âmbito da administração pública federal, o Gabinete de Segurança Institucional da Presidência da República elaborou a Política Nacional de Segurança da Informação, também conhecida como PNSI.

Recomendamos a todos os servidores públicos federais que procurem conhecer mais a PNSI – seus princípios, seus instrumentos e as competências dos órgãos e das entidades – por meio da leitura do Decreto nº 9.637, de 2018, que a instituiu.

Uso de mídias sociais em dispositivos funcionais

O uso de aplicativos de mídias sociais com perfis pessoais em dispositivos funcionais disponibilizados pelas organizações, além de poder ferir políticas de segurança e de uso dos ativos de informação destas, não é recomendado devido aos riscos de segurança que isso pode representar.

Muitos desses aplicativos podem ter acesso a informações sensíveis do dispositivo e do usuário, como, por exemplo, dados de contatos, localização, câmera e microfone. Essa é uma vulnerabilidade que pode ser explorada por *hackers* mal-intencionados ou cibercriminosos.

Alguns dos aplicativos de mídias sociais mais utilizados no Brasil, que possuem na ordem de milhões de usuários, são *WhatsApp*, *YouTube*, *Instagram*, *Facebook*, *TikTok*, *Twitter* e *LinkedIn*.

Vale destacar que, para o uso seguro de mídias sociais com perfis institucionais, de modo geral, foram estabelecidas diretrizes de segurança da informação pela Instrução Normativa nº 6, de 23 de dezembro de 2021, que é uma norma de cumprimento obrigatório para os órgãos e as entidades da administração pública federal e foi tratada no BIM nº 25, de fevereiro de 2022

Importante saber que muitos dos aplicativos de mídias sociais podem exigir permissões de acesso que vão além do necessário para seu funcionamento. Assim, aumentam os riscos à privacidade e à segurança das informações do usuário, pois essas permissões podem viabilizar que os aplicativos acessem diversos dados do dispositivo, como registros de chamadas, mensagens de texto e até mesmo dados de outras contas conectadas.

Além das questões já expostas, outro aspecto que torna o uso de aplicativos de mídias sociais arriscado é o fato de que eles podem ser grandes consumidores de recursos do dispositivo, como bateria, processamento e memória. Isso pode afetar negativamente o desempenho do equipamento, comprometendo seu funcionamento.

Finalmente, por todos esses motivos, é recomendado que o uso de aplicativos de mídias sociais com perfis pessoais seja restrito a dispositivos pessoais particulares e que medidas de segurança sejam adotadas para proteger as informações do usuário. Entre essas medidas, destacamos a utilização de senhas seguras, o uso de *antimalware*, a implementação de autenticação multifator (MFA, na sigla em inglês) e a atualização regular dos aplicativos e do sistema operacional do dispositivo.

Documentos preparatórios

Você sabia que determinados documentos, produzidos para fundamentar a tomada de decisão, podem ter seu acesso restrito ao público?

- São os chamados documentos preparatórios, comumente vistos em processos administrativos que contenham pareceres ou notas técnicas que, caso fossem de acesso público, colocariam em risco a lisura do processo.
- Essa modalidade de restrição de acesso está descrita no §3º do art. 7º da Lei de Acesso à Informação e no art. 20 do Decreto 7.724/2012
- Uma característica importante do documento preparatório é o momento do fim da sua restrição de acesso público, que se dá no momento da tomada de decisão da autoridade que utilizou o documento como subsídio.
- Cabe destacar que diversas decisões podem ser orientadas por documentos preparatórios, o que inclui a classificação em grau de sigilo do próprio documento.
- Para saber mais sobre esse assunto e outras questões relacionados à segurança da informação, acesse https://www.gov.br/gsi/dsic.

Ataques de *phishing* usando a temática IRPF 2023

Com a chegada do período para a entrega da declaração do Imposto sobre a Renda das Pessoas Físicas (IRPF) 2023, os criminosos têm criado armadilhas para que os usuários sejam direcionados a *sites* fraudulentos. Esses *sites* oferecem supostos *softwares* da Receita Federal para *download*, mas, na verdade, trata-se de programas maliciosos que podem comprometer a segurança do seu computador e roubar suas informações pessoais.

Para evitar cair em golpes como esse, é fundamental baixar o *software* exclusivamente pelo *site* oficial da Receita Federal, que é seguro e confiável, disponível em https://www.gov.br/receitafederal/pt-br/centrais-de-conteudo/download/pgd/dirpf.

Aqui estão algumas precauções que você pode tomar para evitar ser vítima de um ataque de *phishing*:

é importante ter cuidado com mensagens enviadas por torpedos (SMS, na sigla em inglês) ou aplicativos que se passam por comunicações oficiais sobre o IRPF. Essas mensagens podem ser golpes de *phishing*, que visam roubar informações pessoais e financeiras;

antes de clicar em um *link*, sempre verifique o endereço *web* (URL, na sigla em inglês) do *site* para garantir que está digitando suas informações em uma página legítima. *Sites* fraudulentos podem parecer idênticos aos oficiais, mas geralmente têm pequenas diferenças em seu URL, como letras ou números adicionais;

não forneça informações pessoais, financeiras, senhas ou números de cartão de crédito por *e-mail* ou em um *site* que não seja seguro;

mantenha os *softwares* atualizados! Todos os programas e sistemas operacionais devem ser atualizados com as últimas correções de segurança e *patches* para evitar que haja vulnerabilidades que podem ser exploradas por *hackers* mal-intencionados;

use um *software* antivírus confiável;

não clique em *links* suspeitos! Ao receber um *e-mail* de um desconhecido ou com conteúdo suspeito, não clique em nenhum *link*. Se você tiver dúvidas sobre a autenticidade de um *e-mail*, encaminhe ao administrador da rede para verificar se ele é legítimo;

use autenticação multifator! Sempre que possível, use a autenticação multifator para fazer *login*. Isso adiciona uma camada extra de segurança, como um código enviado por SMS ou um *token* de segurança.

Lembre-se, a temporada de elaboração e envio de declaração de imposto de renda é um período de risco para ataques de *phishing*, mas, seguindo essas orientações simples de precaução, você pode proteger suas informações pessoais e financeiras contra *hackers* mal-intencionados.

Dicas e Recomendações de Segurança da Informação e Cibernética

- Mantenha instalado um *software* antivírus para cuidar da segurança cibernética durante as atividades de navegação e de utilização de computadores, em casa ou no trabalho. Lembre-se: é necessário manter o programa sempre atualizado, com a versão mais recente instalada.
- Não deixe em local visível ou de fácil acesso informações confidenciais ou de acesso restrito. Cuidado com portas e janelas abertas! Lembre-se de fechá-las e de bloquear a tela do computador ao se ausentar da sala ou da estação de trabalho.

Fonte: https://www.gov.br/gsi/dsi/
Editorial/redação/diagramação: SSIC Sugestões: educa.si@presidencia.gov.br