BIM
Boletim Informativo Mensal
Comunicar para Educar
Nº 20– Setembro/2021

"Formas de proteger sua carteira no século XXI. O seu celular".

Algum tempo atrás, se um cidadão tivesse seu celular furtado ou roubado, basicamente, o prejuízo seria apenas a perda do aparelho. Todavia, com o advento dos *smartphones*, e a disponibilidade de aplicativos bancários e financeiros serem instaláveis nos mais diversos tipos de sistemas operacionais dos celulares, o criminoso pode causar prejuízos consideráveis à vítima.

Diante desse cenário, sugerimos algumas formas de como proteger sua carteira no século XXI, o seu celular.

Dica nº 1: Proteja seu *chip*

Configure uma senha no seu SIM *card (chip*) da operadora de telefonia que você utiliza, para que o criminoso não coloque o seu *chip*, ora roubado, em outro aparelho e com isso tenha acesso a sua linha telefônica.

- No Sistema *Android*, **entre em configurações, segurança, bloqueio/alterar PIN do *chip* (Exigir PIN para usar o telefone).** No Sistema do *iPhone*, entre em **ajustes, celular e PIN do SIM**. Nestas configurações você poderá definir uma senha de 4 números para o *chip*. É provável que você precise do código PUK, que veio junto com o *chip* da operadora; e caso você não tenha, terá que obter essa informação em sua operadora de telefonia celular.

Dica nº 2: Proteja seu SMS

Configure o seu aplicativo de SMS para que uma senha ou sua impressão digital seja requerida, mesmo que o seu celular esteja com a tela ativa. Algumas marcas de celulares têm essa função integrada, bastando **pesquisar por bloqueio de *Apps* ou Pasta Segura e escolher o aplicativo de SMS que geralmente é denominado Mensagens**.

Uma outra forma é instalar um aplicativo de segurança (um aplicativo de antivírus) que possua a funcionalidade do tipo *App Lock* ou Antirroubo.

Dica nº 3: Proteja os Aplicativos críticos

Configure uma segunda camada de proteção para os aplicativos considerados críticos, tais como o *Play Store*, Gmail, a área de configuração do aparelho, entre outros. Agindo assim, você evitará que o criminoso acesse seus *e-mails* e aplicativos importantes.

Como na dica anterior, utilize o bloqueio de *Apps*/Pasta Segura ou um aplicativo de segurança que possua a funcionalidade do tipo *App Lock* ou Antirroubo.

Dica nº 4: Guarde o IMEI do aparelho

O *International Mobile Equipment Identity* (IMEI) é um número contendo 15 dígitos que identifica o seu celular. Caso o seu dispositivo seja roubado, a operadora pedirá o IMEI do aparelho para realizar o bloqueio. Anote o IMEI em lugar seguro e de fácil acesso.

Tanto para *iPhone*, quanto para *Android*, o procedimento é o mesmo: basta **abrir o *app* de ligações telefônicas e digitar *#06# no teclado. O IMEI será exibido na tela.**

Dica nº 5: Utilize o apagamento remoto

É possível utilizar o recurso de apagamento remoto do celular. Em aparelhos *Android*, basta **abrir o seu computador** (ou se logar na sua conta do *Google* em qualquer outro computador), **acessar a pesquisa do *Google* e digitar *"find my phone".*** Ato contínuo aparecerá um mapa mostrando a localização aproximada do seu *smartphone*. **Permita o monitoramento remoto do *smartphone*, e configure a proteção e limpeza do seu aparelho.**

Para o caso de ser *iPhone*, **acesse o *iCloud* (*icloud.com*) com o seu *login* e senha da *Apple* e clique em Buscar *iPhone*.**

Dica nº 6: Evite armazenar informações sensíveis no seu aparelho

As dicas acima tornam o seu aparelho celular mais seguro e dificultam o acesso do criminoso a informações sensíveis. Todavia, dificultar não significa impossibilitar o acesso, por isso, evite armazenar informações sensíveis, documentos pessoais, e manter aplicativos que raramente são utilizados.

Tenha em mente que o celular facilita, em muitos casos, o acesso aos seus recursos financeiros e, sem as efetivas camadas de proteção, ele poderá representar um grande transtorno em caso de perda ou roubo.

BIM
Boletim Informativo Mensal
Comunicar para Educar
Nº 20– Setembro/2021

O que é CGSI?

Em edição anterior, escrevemos sobre as alterações no decreto que institui a Política Nacional de Segurança da Informação (PNSI). Entre essas alterações, ressalta-se que algumas novas regras são relacionadas diretamente ao CGSI; mas o que significa essa sigla?

CGSI significa **Comitê Gestor de Segurança da Informação**, o qual foi instituído para assessorar o Gabinete de Segurança Institucional da Presidência da República (GSI/PR) nas atividades relacionadas à segurança da informação. Esse comitê é composto de representantes de cada órgão da administração pública federal (APF) com status de Ministério, sendo coordenado pelo GSI/PR, tendo em vista a transversalidade do tema, e a importância da discussão de questões relacionadas à segurança da informação.

Conforme previsto em seu regimento interno, suas reuniões ordinárias ocorrem semestralmente, sendo que reuniões extraordinárias também podem ser realizadas a critério de seu coordenador. A primeira reunião ordinária de 2021 foi realizada em 29 de junho e contou com a presença de membros do comitê, convidados, e autoridades, incluindo o Sr. Ministro de Estado Chefe do Gabinete de Segurança Institucional da Presidência da República, General Augusto Heleno.

Entre os assuntos tratados nessa primeira reunião, vale destacar a apresentação:

- do resultado dos trabalhos produzidos sobre segurança cibernética dos sistemas estruturantes da APF;
- das informações sobre a revisão do Glossário de Segurança da Informação; e
- da proposta de metodologia para avaliação periódica do cumprimento do Decreto nº 7.845, de 14 de novembro de 2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo e que dispõe sobre o Núcleo de Segurança e Credenciamento.

Para compreender um pouco mais sobre esse comitê, acesse seu regimento interno em: https://www.in.gov.br/en/web/dou/-/resolucao-n-1-de-11-de-setembro-de-2019-217042776.

Credenciamento de Segurança

No âmbito da Administração Pública federal, os órgãos e entidades públicas e privadas que recebem, produzem, guardam ou enviam documentos que contêm **informações classificadas**, bem como as pessoas que manuseiam esse tipo de informação, devem ser submetidos ao processo de habilitação e de credenciamento de segurança.

O processo de credenciamento de segurança visa a subsidiar o órgão ou entidade do Poder Executivo federal, a fim de conhecer, valorizar, proteger e manter seus ativos de informação classificada em conformidade com os requisitos legais e do negócio.

Para saber mais sobre esse assunto, consulte as normas do Gabinete de Segurança Institucional da Presidência da República – Instrução Normativa nº 02, de 5 de fevereiro de 2013 e Norma Complementar nº 01, de 27 de junho de 2013, por meio do link: http://dsic.planalto.gov.br/assuntos/publicacoes-1

Foi publicada, no Diário Oficial da União, a Instrução Normativa Nº 5, de 30 de agosto de 2021, que dispõe sobre os **requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem,** pelos órgãos e pelas entidades da administração pública federal.

Esse importante normativo entra em vigor na data publicação e revoga a Norma Complementar Nº 14.