Comunicar para Educar
Junho/2023 - Ano 4 - nº 40

BIM

Boletim Informativo Mensal

Audiência Pública sobre a PNCiber

- O Gabinete de Segurança Institucional da Presidência da República (GSI/PR) realizou dia 15 de junho, a audiência pública para tratar da proposta de Projeto de Lei para a criação da Política Nacional de Cibersegurança (PNCiber).
- A proposta da PNCiber tem como objetivo principal a criação do Sistema Nacional de Cibersegurança, que irá centralizar a segurança cibernética na estrutura do governo federal. A proposta prevê a criação de órgãos como o Comitê Nacional de Cibersegurança (CNCiber), a Agência Nacional de Cibersegurança (ANCiber), o Gabinete de Gerenciamento de Cibercrises (GGCiber) e o Complexo Nacional de Cibersegurança.
- As informações específicas preliminares sobre o projeto encontram-se no site: https://www.gov.br/gsi/pt-br/composicao/SSIC/dsic/audiencia-publica/01-2023.

A Secretaria de Segurança da Informação e Cibernética do GSI/PR trabalhando em prol de um ambiente virtual seguro, confiável, inclusivo e resiliente!

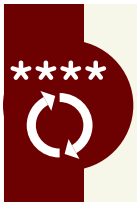
Proteja suas senhas contra os perigos do mundo virtual!

A cada dia, indivíduos mal-intencionados dedicam tempo e esforço para invadir sistemas e roubar informações pessoais valiosas. As senhas são a chave que protege sua privacidade, suas contas bancárias, suas redes sociais e muito mais. É hora de agir e proteger-se contra essas ameaças!

Fique atento aos ataques descritos abaixo!

Phishing: Você já recebeu um *e-mail* ou mensagem solicitando que você clique em um *link* e insira suas informações de *login*? Cuidado! Essa é uma tática comum na qual os *hackers* se passam por empresas ou serviços legítimos para obter acesso às suas senhas;

Ataques de força bruta: Os *hackers* podem usar programas para testar todas as combinações possíveis de senhas até encontrar a correta. Senhas fracas e previsíveis são vulneráveis a esse tipo de ataque. Evite usar senhas óbvias, como datas de aniversário ou sequências numéricas simples;



Reutilização de senhas: É compreensível que seja difícil lembrar de senhas exclusivas para cada conta, mas reutilizá-las é um convite para os criminosos cibernéticos. Se um serviço for comprometido e você usar a mesma senha em outros lugares, todas as suas contas correm risco;

Malwares: Esses programas maliciosos são projetados para se infiltrar em seu dispositivo e capturar suas senhas enquanto você as digita. Eles podem ser encontrados em *links* suspeitos, *downloads* não verificados ou anexos de *e-mail*. Mantenha seu antivírus atualizado e evite clicar em *links* desconhecidos; e

Engenharia social: Nessa técnica, os *hackers* usam truques psicológicos para enganar você e obter suas informações. Eles podem fingir ser um amigo ou colega confiável, pedir ajuda ou usar informações pessoais que encontraram *on-line* para ganhar sua confiança. Fique atento a solicitações suspeitas e verifique a autenticidade antes de fornecer qualquer informação pessoal.

Agora que você está ciente dessas ameaças, é hora de proteger-se e manter suas senhas seguras:

tenha cuidado ao compartilhar informações pessoais - Evite enviar informações pessoais confidenciais por *e-mail*, mensagens ou em *sites* não confiáveis. As empresas legítimas nunca solicitarão suas senhas ou informações confidenciais dessa forma

ative a autenticação de dois fatores - muitos serviços oferecem a opção de adicionar uma camada extra de segurança, exigindo um código adicional além da senha para fazer *login*. Aproveite essa opção sempre que possível

fique de olho em atividades suspeitas em suas contas, como *logins* desconhecidos, alterações não autorizadas de informações pessoais ou atividade incomum. Se você notar algo fora do comum, entre em contato imediatamente com o suporte do serviço em questão

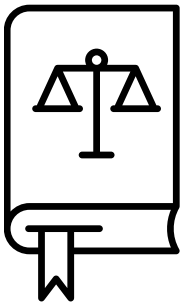
mantenha seu *software* atualizado – geralmente as atualizações incluem correções de segurança importantes que podem proteger suas informações

use senhas fortes - crie senhas longas e complexas, com uma combinação de letras maiúsculas e minúsculas, números e caracteres especiais. Evite informações pessoais óbvias e não use a mesma senha para várias contas.

Você é profissional de segurança cibernética ou gosta do tema? Acompanhe os Alertas e Recomendações do CTIR Gov disponíveis em: https://www.gov.br/ctir/pt-br.

Sigilo das informações pessoais tratadas no serviço público

A Lei de Acesso à Informação (LAI) trouxe à tona a temática da proteção dos dados pessoais tratados no âmbito do serviço público. Segundo a LAI, independente da atribuição de grau de sigilo, o acesso a esse tipo de informação só será permitido a agentes públicos que tenham a "necessidade de conhecer" e à pessoa a quem ela se refere, pelo prazo máximo de 100 (cem) anos, a contar da data de sua produção.



Porém, essa regra não vale para qualquer informação pessoal. O mesmo artigo 31 da LAI estabelece que a restrição de acesso às informações pessoais relativas à "intimidade, vida privada, honra e imagem das pessoas", que são bens imateriais protegidos pelo inciso X do art. 5º da Constituição Federal de 1988. Cabe ressaltar, ainda, que o referido dispositivo da LAI não poderá ser invocado com intuito de prejudicar o processo de apuração de irregularidades da pessoa envolvida ou a recuperação de fatos históricos de maior relevância.

É importante dizer que o prazo de restrição de acesso é automaticamente imposto e quem detiver o dado pessoal não poderá divulgá-lo antes dos cem anos previstos na legislação. A **divulgação das informações** ou o **acesso a terceiros** se dará somente por **consentimento expresso da pessoa a quem a informação se referir,** diante de previsão legal para tal ou por término do prazo de sigilo.

Por fim, vale destacar que as pessoas autorizadas a acessar esse tipo de informação serão responsabilizadas por seu uso indevido.

Para saber mais sobre este assunto acesse:
https://www.gov.br/gsi/pt-br/composicao/SSIC/dsic/nucleo/tratamento-de-informacao-classificada.

Dicas de Segurança da Secretaria de Informação e Cibernética. Fique atento!

Para se prevenir contra golpes, é importante adotar alguns cuidados básicos. Siga as dicas abaixo!

1. Sempre desconfie de promoções muito vantajosas ou pedidos de informações pessoais, como senhas ou dados bancários.
2. Não clique em *links* suspeitos ou compartilhe informações confidenciais em conversas privadas com desconhecidos.
3. Habilite a autenticação em duas etapas para reforçar a segurança da suas contas e perfis.
4. Atenção aos perfis falsos e mensagens automáticas com erros de português ou que parecem "forçadas" demais.

Comprometa-se com a proteção, pratique a prevenção!

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