BIM
Comunicar para Educar

Boletim Informativo Mensal – Março/2021 – Ano 2 – Nº 14

A instituição onde você trabalha está preparada para garantir a segurança da informação e manter os dados seguros?

Na **Instrução Normativa nº 01/GSI-PR**, de 27 de maio de 2020, o art. 9º diz que **todos os órgãos e as entidades da administração pública federal devem possuir uma Política de Segurança da Informação.**

A Política deve ser implementada, partindo da formalização e da aprovação por parte da autoridade máxima da instituição, com o objetivo de estabelecer diretrizes, responsabilidades, competências e subsídios para a gestão da segurança da informação.

É preciso priorizar recursos para a estrutura de segurança da informação. O recurso, quando direcionado, limita-se, muitas vezes, a equipamentos e não contempla o processo de segurança.

Ações simples, como capacitação da força de trabalho, ou uma campanha de conscientização do pessoal, são, em muitos casos, tão efetivas - do ponto de vista da segurança - quanto um grande investimento em equipamentos.

A **segurança da informação** de um órgão ou instituição **extrapola** o escopo abrangido pelas **áreas de sistemas de informação e recursos computacionais**. **Deve estar diretamente relacionada ao comprometimento e à efetiva atuação da alta administração.**

Monitoramento De Dados Financeiros

Com os recentes vazamentos de dados, (a exemplo, o recente vazamento de aproximadamente 223 milhões de cadastros, entre CPFs e CNPJs) surge a dúvida: **Como se proteger?** Posto que o dado, possivelmente, foi vazado.

Para essa questão, o cidadão possui uma boa prática a seu dispor, porém pouco utilizada: **o monitoramento de seus dados financeiros.**

Ao obter os dados da vítima, o criminoso almeja ganho financeiro por meio de saque e compra indevida em cartão de débito e/ou crédito fraudado, como também por abertura de conta bancária e pedido de empréstimo.

O Banco Central do Brasil disponibiliza para as pessoas físicas e jurídicas brasileiras, a consulta gratuita a relatórios de chave PIX, empréstimos, financiamentos, contas em banco e outros serviços, através do Sistema **REGISTRATO**. Existem também serviços de monitoramento do CPF, oferecidos por instituições de análises e proteção ao crédito.

Tenha sempre em mente: **seus dados são seu maior patrimônio no mundo digital.** E você é o principal responsável pela salvaguarda deles. Por tanto, **evite fornecer de maneira indiscriminada seus dados**, seja seletivo ao preencher cadastros, **se questione: é realmente necessário fornecer todas as informações solicitadas?**

Para saber mais sobre o tema, acesse os *links* abaixo:

https://www.bcb.gov.br/cidadaniafinanceira/registrato
https://www.serasa.com.br/antifraude/
https://credenciamento.bcb.gov.br/soupf
https://www.youtube.com/watch?v=vimRcOSzqTY&feature=emb_logo
https://loja.spcbrasil.org.br/pessoa-fisica/monitorar-cpf-spc-avisa.html

BIM
Comunicar para Educar

Boletim Informativo Mensal – Março/2021 – Ano 2 – Nº 14

Em 9 de dezembro de 2020, foi publicado o **Decreto nº 10.569**, que aprovou a **Estratégia Nacional de Segurança de Infraestruturas Críticas** (**Ensic**), que é um instrumento de orientação estratégica e de referência para a implementação da Política Nacional de Segurança de Infraestruturas Críticas.

Já a **Estratégia Nacional de Segurança Cibernética** (**E-Ciber**), publicada por meio do **Decreto 10.222**, de 5 de fevereiro de 2020, é a orientação manifesta do Governo federal à sociedade brasileira sobre as principais ações por ele pretendidas, em termos nacionais e internacionais, na área da segurança cibernética e tem validade no quadriênio 2020-2023.

Importante destacar **que a Estratégia Nacional de Segurança de Infraestruturas Críticas e a Estratégia Nacional de Segurança Cibernética, são instrumentos de ação conjunta**.

No Brasil, as infraestruturas de comunicações, de energia, de transportes, de finanças, de águas, e de biossegurança, entre outras, possuem dimensão estratégica, uma vez que desempenham papel essencial tanto para a segurança e soberania nacionais, como para a integração e o desenvolvimento econômico sustentável do País. Caso algum fator prejudique o adequado fornecimento dos serviços provenientes dessas infraestruturas, podem ocorrer grandes transtornos e prejuízos ao Estado, à sociedade e ao meio ambiente.

De maneira geral, os países buscam se preparar para possíveis imprevistos que possam afetar tais infraestruturas, identificando ações e procedimentos que permitam garantir o seu funcionamento. Assim, torna-se imperativa a atividade denominada segurança de infraestruturas críticas, cuja implementação necessita do esforço conjunto do Estado e da sociedade.

A Ensic aprovada traz orientações para a definição das principais ações a serem adotadas no sentido de assegurar a integridade e aumentar a resiliência a prestação de serviços indispensáveis ao Estado e à sociedade brasileira. Estabelece os princípios para a atividade de segurança de infraestruturas críticas e identifica os desafios a serem enfrentados, assim como os eixos estruturantes para a efetividade da atividade. Além disso, define objetivos e iniciativas estratégicas que orientarão a elaboração do Plano Nacional de Segurança de Infraestruturas Críticas.

O tratamento **da informação classificada em grau de sigilo**, no âmbito do Poder Executivo federal, **deve utilizar estritamente sistemas de informação e canais de comunicação seguros**, que atendam aos padrões mínimos de segurança definidos pelo Gabinete de Segurança Institucional da Presidência da República.

Dessa forma, ressalta-se que **é vedado qualquer tipo de transmissão, veiculação, encaminhamento, armazenamento ou outra forma de tratamento da informação classificada em grau de sigilo utilizando aplicativos para dispositivos móveis de troca de mensagens como *WhatsApp*, Telegram ou Signal, entre outros**, que não estejam em conformidade com a legislação em vigor.

Para saber mais sobre esse assunto, acesse:
http://gov.br/gsi/dsi

Fonte: https://www.gov.br/gsi/dsi
Editorial/redação/diagramação: ASSESI
https://www.ctir.gov.br/
Sugestões: asscom.dsi@presidencia.gov.br