BIM

Boletim Informativo Mensal

Comunicar para Educar

Nº 02 – Fevereiro/2020

O **Departamento de Segurança da Informação (DSI)** é o órgão do Governo Federal responsável por elaborar normativos e requisitos metodológicos relativos à atividade nacional de segurança da informação, no âmbito da administração pública federal, nela inclusos a segurança cibernética, a gestão de incidentes computacionais, a proteção de dados, o credenciamento de segurança e o tratamento de informações sigilosas, conforme o Decreto nº 9.669, de 2 de janeiro de 2019.

O DSI foi responsável pela elaboração de 3 Instruções Normativas e 22 Normas Complementares sobre diversos assuntos de Segurança Cibernética e de Segurança da Informação desde 2008. Esses normativos foram publicados por meio de Portaria do Gabinete de Segurança Institucional (GSI) e são de cumprimento obrigatório para a Administração Pública Federal. Eles podem ser encontrados no site do Departamento:

- Instruções Normativas em: http://dsic.planalto.gov.br/assuntos/editoria-c/instrucoes-normativas
- Normas Complementares em: http://dsic.planalto.gov.br/assuntos/editoria-c/normas-complementares

Você Sabia?

Você sabia que, no âmbito da Administração Pública Federal, todos os órgãos e entidades públicas e privadas que recebem, produzem, guardam ou enviam documentos que contêm informações classificadas devem possuir um ***Gestor de Segurança e Credenciamento Titular e um Suplente?***

O Gestor de Segurança e Credenciamento é a pessoa responsável pela segurança da informação classificada em qualquer grau de sigilo (reservado, secreto, ultrassecreto) no âmbito da sua organização e deverá observar os procedimentos de segurança necessários a esse tipo de informação.

Para saber mais sobre este 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

Acompanhe: E-Ciber

A Estratégia Nacional de Segurança Cibernética (E-Ciber), aprovada pelo Decreto nº 10.222, de 5 de fevereiro de 2020, foi elaborada com o objetivo principal de apresentar, para a sociedade brasileira, os rumos que o governo federal considera essenciais para que o País, sua sociedade e suas instituições, se tornem seguros e resilientes no uso do espaço cibernético.

Atendendo ao clamor público por uma legislação mais efetiva, o GSI já trabalha no projeto de lei da POLÍTICA NACIONAL DE SEGURANÇA CIBERNÉTICA, a fim de proporcionar uma governança colaborativa de âmbito nacional.

Saiba mais:
http://dsic.planalto.gov.br/noticias/estrategia-nacional-de-seguranca-cibernetica-e-ciber/view

Phishing

É uma tentativa de fraude pela internet que utiliza "iscas", isto é, artifícios para atrair a atenção de uma pessoa e fazê-la realizar alguma ação, na tentativa de obter dados pessoais e financeiros do indivíduo.

Dicas de como evitar o "*phishing*":

- não abra e-mails de remetentes com os quais você não esteja familiarizado;
- para melhorar a proteção, se você receber um e-mail, mesmo que seja de uma pessoa conhecida, acesse o link inserindo manualmente o endereço do website em seu navegador. Em muitos casos de golpe, o endereço ao qual você é direcionado contêm erro de grafia;
- se pedirem algum dado confidencial, verifique se o endereço do *site* da página começa com "HTTPS" e não apenas como "HTTP." O \"S\" significa \"seguro\". Isso não é uma garantia de que ele seja seguro, mas os *sites* originais usam HTTPS porque é mais resguardado. Os *sites* HTTP, mesmo que sejam legítimos, são mais vulneráveis a *hackers;*
- se você suspeitar que um e-mail é falso, anote o nome ou um trecho da mensagem e faça uma busca na internet para verificar se existe algum registro de ataque de *phishing* que utilize o mesmo método; e
- revise suas contas regularmente e verifique atividade não autorizada.

Fonte: http://dsic.planalto.gov.br/ https://www.ctir.gov.br/
Editorial/redação/diagramação: DSI Sugestões: asscom.dsi@presidencia.gov.br