Comunicar para Educar
Maio/2023 - Ano 4 - nº 39

BIM

Boletim Informativo Mensal

DIC

As ações de Segurança da Informação objetivam viabilizar e assegurar a Disponibilidade, a Integridade e a Confidencialidade das informações (DIC). Essas propriedades podem ser definidas resumidamente como:

1. **disponibilidade:** propriedade pela qual se assegura que a informação esteja acessível e utilizável para quem tem permissão;
2. **integridade:** propriedade pela qual se assegura que a informação não seja modificada ou destruída de maneira não-autorizada ou acidental;
3. **confidencialidade:** propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada a quem não está autorizado; e

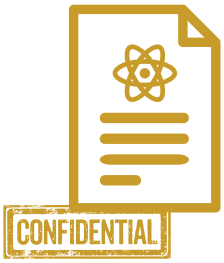
Promulgada a Convenção sobre o Crime Cibernético

- A Convenção sobre o Crime Cibernético, também conhecida como Convenção de Budapeste, foi promulgada pelo Brasil por meio do Decreto Nº 11.491, de 12 de abril de 2023. Ela é um instrumento essencial para facilitar a cooperação internacional em assuntos penais com o objetivo de combater o crime cibernético.
- Os países aderentes entendem que a Convenção é necessária para impedir ações conduzidas contra a confidencialidade, a integridade e a disponibilidade de sistemas informáticos, redes e dados de computador, bem como para impedir o abuso de tais sistemas, redes e dados, ao prever a criminalização de tais condutas.
- Ademais, ao prever a criação de competências suficientes para combater efetivamente tais crimes e estabelecer mecanismos para uma cooperação internacional rápida e confiável, facilita a descoberta, a investigação e o julgamento dessas infrações penais em instâncias domésticas e internacionais.
- Com a adesão à Convenção, o Brasil assume o compromisso de cooperar, o máximo possível, com as outras partes por meio da aplicação de instrumentos internacionais pertinentes de cooperação internacional em assuntos penais, de ajustes firmados com base em legislação uniforme, do princípio da reciprocidade e da legislação doméstica para a realização das investigações ou procedimentos acerca de crimes de computador, ou para a coleta de provas eletrônicas desses crimes.



Restrição de acesso à informação sobre pesquisa e desenvolvimento

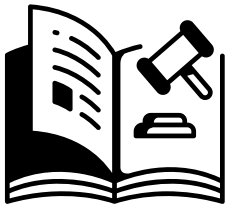
Você sabia que Lei de Acesso à informação (LAI) resguarda informações sobre determinados tipos de pesquisas e desenvolvimento tecnológico?



A LAI, em seu artigo 7º, apresenta, em sete incisos, os tipos de informações que o Estado é obrigado a disponibilizar à sociedade. Entretanto, logo em seu parágrafo 1º, o referido artigo apresenta uma exceção à regra de divulgação: "informações referentes a projetos de pesquisa e desenvolvimento científicos ou tecnológicos cujo sigilo seja imprescindível à segurança da sociedade e do Estado".

Dessa forma, determinados tipos de desenvolvimentos tecnológicos, considerados essenciais para proteção de nossa sociedade e Estado, devem ter seu acesso restrito aos pesquisadores e às pessoas que tenham a necessidade funcional de conhecê-los.

Cabe destacar a relevância dada pela legislação à salvaguarda de informações sobre pesquisas científicas e tecnologia. A LAI, além de abordar o assunto em seu artigo 7º, apresenta, no inciso VI de seu artigo 23, a possibilidade de classificação em grau de sigilo para este tipo de informação, o que aumenta sua proteção:



"Art. 23. São consideradas imprescindíveis à segurança da sociedade ou do Estado e, portanto, passíveis de classificação as informações cuja divulgação ou acesso irrestrito possam:
(...)
VI - prejudicar ou causar risco a projetos de pesquisa e desenvolvimento científico ou tecnológico, assim como a sistemas, bens, instalações ou áreas de interesse estratégico nacional; (...)"

Para saber mais sobre este assunto e outros relacionados à segurança da informação acesse: https://www.gov.br/gsi/dsic.

Postura de Segurança Cibernética

A segurança cibernética é uma das principais preocupações das organizações em todo o mundo. As ameaças cibernéticas são cada vez mais frequentes e sofisticadas, exigindo que as organizações adotem medidas de segurança cibernética eficazes para proteger seus dados e informações confidenciais. A disseminação da cultura de segurança cibernética entre os colaboradores de uma organização é fundamental para garantir que as políticas de segurança sejam seguidas e respeitadas.

Um colaborador consciente contribui para uma segurança cibernética mais forte, pois entende a importância da segurança de dados e está comprometido com o processo de manutenção da integridade das informações organizacionais. Eles reconhecem que sua conduta e ações podem ter um impacto significativo na segurança da organização e estão dispostos a seguir as políticas e práticas de segurança da empresa para proteger suas informações. Colaboradores com uma postura de segurança cibernética forte também são proativos na identificação e relato de possíveis ameaças cibernéticas, o que ajuda a organização a mitigar rapidamente esses problemas.

Adotar uma postura de segurança cibernética entre os colaboradores é fundamental para manter a reputação e a confiança da organização. Se ocorrer uma violação de dados, sérias consequências podem ser enfrentadas, além de abalar a confiança do público. A adoção de medidas de segurança cibernética robustas e a conscientização dos colaboradores contribuem para minimizar o risco de violações de dados e demonstram o compromisso da organização em proteger as informações confidenciais de seus parceiros e público alvo.

Dentre as posturas proativas mais indicadas, podem ser citadas:

o cuidado com ataques de *phishing* - esta ameaça representa 90% de todas as violações que as organizações enfrentam, tendo crescido 65% no último ano;

a preocupação com a qualidade e a utilização de senhas - em torno de 19% dos usuários usam senhas facilmente adivinháveis ou compartilham senhas entre diferentes contas. Evite este comportamento e use multifator de autenticação sempre que possível; e

o comprometimento com a organização - muitas vezes, graves incidentes são causados por funcionários mal-intencionados ou descuidados. Ao se tornarem aliados na prevenção de ameaças internas, usuários com postura de segurança cibernética podem ajudar a garantir a segurança dos dados e informações confidenciais da organização.

E você, cultiva uma postura de segurança cibernética proativa? Pense nisso!

Dicas de Segurança da Informação e Cibernética. Fique atento!

- Se os usuários não souberem os riscos que correm, podem acabar, sem intenção, infectando toda a rede do órgão com vírus ou programas maliciosos.
- Os técnicos do DSIC (Departamento de Segurança da Informação e Cibernética) recomendam que as organizações criem regras de segurança (políticas de segurança da informação e cibernética) e ensinem os funcionários a seguirem essas regras. É importante ficar de olho em sinais de campanhas maliciosas com *e-mails* de *phishing* ou spam, golpes ou distribuição de programas maliciosos feitos pelos *hackers*.

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