

Privacidade no mundo digital

O mundo está ao alcance de um clique. Nessa imensidão virtual, é fundamental estabelecermos uma prioridade essencial: a privacidade. À medida que exploramos a *Internet*, devemos estar conscientes dos perigos e proteger nossos dados pessoais.



No ambiente digital em constante expansão, a proteção da privacidade torna-se um aspecto de extrema importância. À medida que navegamos na *Internet* e utilizamos os serviços *on-line*, é imperativo estarmos cientes das ameaças existentes e adotarmos medidas para salvaguardar nossos dados pessoais.

Ao priorizarmos a privacidade, estamos fortalecendo nossa proteção no mundo virtual. Veja algumas formas de se proteger:

a. Controle a privacidade nas redes sociais

As redes sociais são como janelas para nossas vidas, permitindo que nos conectemos com o mundo. No entanto, é crucial estabelecer limites para proteger nossas informações pessoais. Descubra como ajustar as configurações de privacidade em suas contas, garantindo que apenas as pessoas certas tenham acesso aos seus dados. Aprenda a identificar e evitar perfis falsos e a compartilhar conteúdo com cuidado, protegendo sua privacidade enquanto interage em um ambiente social digital;



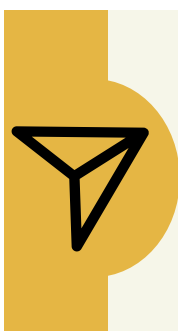
b. Uso de Redes Virtuais Privadas (VPN)

Ao navegar na *internet*, os rastros que deixamos podem revelar muito sobre nós. Explore como uma VPN pode proteger seus dados, criptografando sua conexão e mantendo suas atividades *on-line* em sigilo. Aprenda sobre os benefícios de usar uma VPN ao se conectar a redes *Wi-Fi* públicas, como escolher o provedor certo para garantir sua privacidade e sobre a importância de usar *firewalls* pessoais;



c. Cuidado com o compartilhamento de dados

Em um mundo cada vez mais interconectado, compartilhar informações pessoais é comum. No entanto, é crucial ser seletivo e cauteloso ao compartilhar dados sensíveis. Fique atento sobre como identificar situações em que é apropriado compartilhar informações pessoais e como evitar fornecer dados desnecessários. Aprenda a navegar por *e-mails* suspeitos, *links* duvidosos e a proteger-se contra esquemas de *phishing* que visam roubar suas informações pessoais.



Esperamos que você compreenda a importância da privacidade em primeiro lugar em seu mundo digital. Proteger seus dados pessoais permite que você aproveite ao máximo os recursos da *internet*, mas com segurança e tranquilidade. Lembre-se sempre de controlar suas configurações de privacidade, considerar o uso de uma VPN confiável e compartilhar informações com cautela.



Tratamento de informações sigilosas

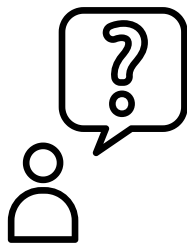
A Lei de Acesso à Informação (LAI) regulamentou o preceito constitucional da transparência na relação entre o Estado e o cidadão. O capítulo II da lei aborda a temática do acesso à informação e o capítulo III apresenta os procedimentos que devem ser adotados.



Apesar de ser vocacionada para a transparência, a LAI também trata de sigilo. Em seu capítulo IV, intitulado “das restrições de acesso à informação”, a lei regulamenta a classificação de informações e a proteção de dados pessoais tratados pelo serviço público.





Nesse contexto, cabe destacar que a referida norma não exclui as demais hipóteses legais de sigilo e de segredo de justiça nem as hipóteses de segredo industrial. Além disso, embora o foco do sigilo abordado pela LAI seja a informação pessoal e a classificada, a lei trata sobre restrição de acesso a documentos preparatórios e a determinados projetos de pesquisa e desenvolvimento.



Sobre o assunto, constata-se que há previsão legal de sigilo para diversos tipos de informação. Diante disso, uma dúvida pode surgir: para que classificar uma informação que já tem seu sigilo previsto em lei ou norma infralegal? Para essa questão, a resposta é simples e direta: a imprescindibilidade para a segurança da sociedade e do Estado de determinada informação, fator principal de motivação para sua classificação, requer que ela receba um tratamento especial para a garantia de sua inviolabilidade.

Respondida a dúvida descrita acima, outra pergunta pode surgir: o que há de especial no trato da informação classificada, já que há vários tipos de informações com restrição de acesso e para todas elas devem ser tomadas medidas que garantam seu sigilo? Essa segunda pergunta é importante e nos permite apresentar a figura abaixo, que apresenta a resposta de maneira ainda mais simples e direta do que na questão anterior.

Informações Classificadas	Demais informações com restrição de acesso
	
OBRIGATÓRIO:	OBRIGATÓRIO:
<input checked="" type="checkbox"/> Necessidade funcional de conhecer	<input checked="" type="checkbox"/> Necessidade funcional de conhecer
<input checked="" type="checkbox"/> Tratamento em área de acesso restrito	<input type="checkbox"/> Tratamento em área de acesso restrito
<input checked="" type="checkbox"/> Guarda em instalação certificada	<input type="checkbox"/> Guarda em instalação certificada
<input checked="" type="checkbox"/> Medidas especiais para expedição	<input type="checkbox"/> Medidas especiais para expedição
<input checked="" type="checkbox"/> Utilização de Criptografia de Estado	<input type="checkbox"/> Utilização de Criptografia de Estado
<input checked="" type="checkbox"/> Credencial de Segurança	<input type="checkbox"/> Credencial de Segurança

Por fim, vale destacar que o tratamento da informação classificada é regulamentado pelo Decreto nº 7.845, de 14 de novembro de 2012, e por Instruções Normativas do Gabinete de Segurança Institucional da Presidência da República.

Para saber mais sobre este assunto e outros relacionados à segurança da informação acesse:

<https://www.gov.br/gsi/pt-br/composicao/SSIC/dsic>

Primeira Reunião Ordinária do Comitê Gestor da Segurança da Informação (CGSI)

- A primeira Reunião Ordinária do Comitê Gestor da Segurança da Informação (CGSI) de 2023 foi realizada em 31/05. Como já escrevemos em edição anterior, esse comitê é composto por representantes dos órgãos da Presidência da República, dos Ministérios, do Banco Central do Brasil (BACEN), da Controladoria-Geral da União (CGU), da Advocacia Geral da União (AGU) e da Autoridade Nacional de Proteção de Dados (ANPD).
- O CGSI se reúne semestralmente com a atribuição de assessorar o Gabinete de Segurança Institucional da Presidência da República (GSI/PR) nas atividades relacionadas à segurança da informação, conforme determinado pelo Decreto nº 9.637, de 26 de dezembro de 2018, que instituiu a Política Nacional de Segurança da Informação.
- Essa primeira reunião de 2023 contou com a presença do Ministro de Estado Chefe do GSI/PR, General Marcos Antonio Amaro Dos Santos, do Secretário-Executivo do GSI/PR e Coordenador do CGSI, General Ivan de Sousa Corrêa Filho, do Secretário de Segurança da Informação e Cibernética e Secretário-Executivo do CGSI, Sr. Luiz Fernando Moraes da Silva, além de representantes dos órgãos integrantes do Comitê.
- Os membros do comitê e seus respectivos suplentes são indicados pelos titulares dos órgãos que representam dentre os agentes públicos que possuam atribuição para definir políticas ou normas relacionadas à tecnologia da informação ou à segurança da informação nos respectivos órgãos.
- Essa reunião não foi deliberativa e teve como objetivo o nivelamento dos novos representantes dos órgãos que já eram membros e dos representantes dos novos ministérios, bem como uma reciclagem dos representantes mantidos. O CGSI teve uma renovação de cerca da metade dos representantes, o que concilia a manutenção da memória dos trabalhos anteriores com a adição de novas perspectivas.
- Houve apresentações do Departamento de Segurança da Informação e Cibernética (DSIC) sobre o trabalho que vem sendo realizado pelo GSI/PR na área de segurança da informação e cibernética e os presentes tiveram a oportunidade de esclarecer dúvidas e expor suas preocupações, necessidades e sugestões sobre a segurança cibernética na administração pública federal.

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>

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



• Tenha um antivírus

- Instalar um software antivírus é o item inicial para cuidar da segurança cibernética durante as atividades de navegação e de utilização de computadores, em casa ou no trabalho.
- É necessário manter o programa sempre atualizado, com a versão mais recente instalada.

Fonte: <https://www.gov.br/gsi/dsic/>

Editorial/redação/diagramação: SSIC

Sugestões: educa.si@presidencia.gov.br