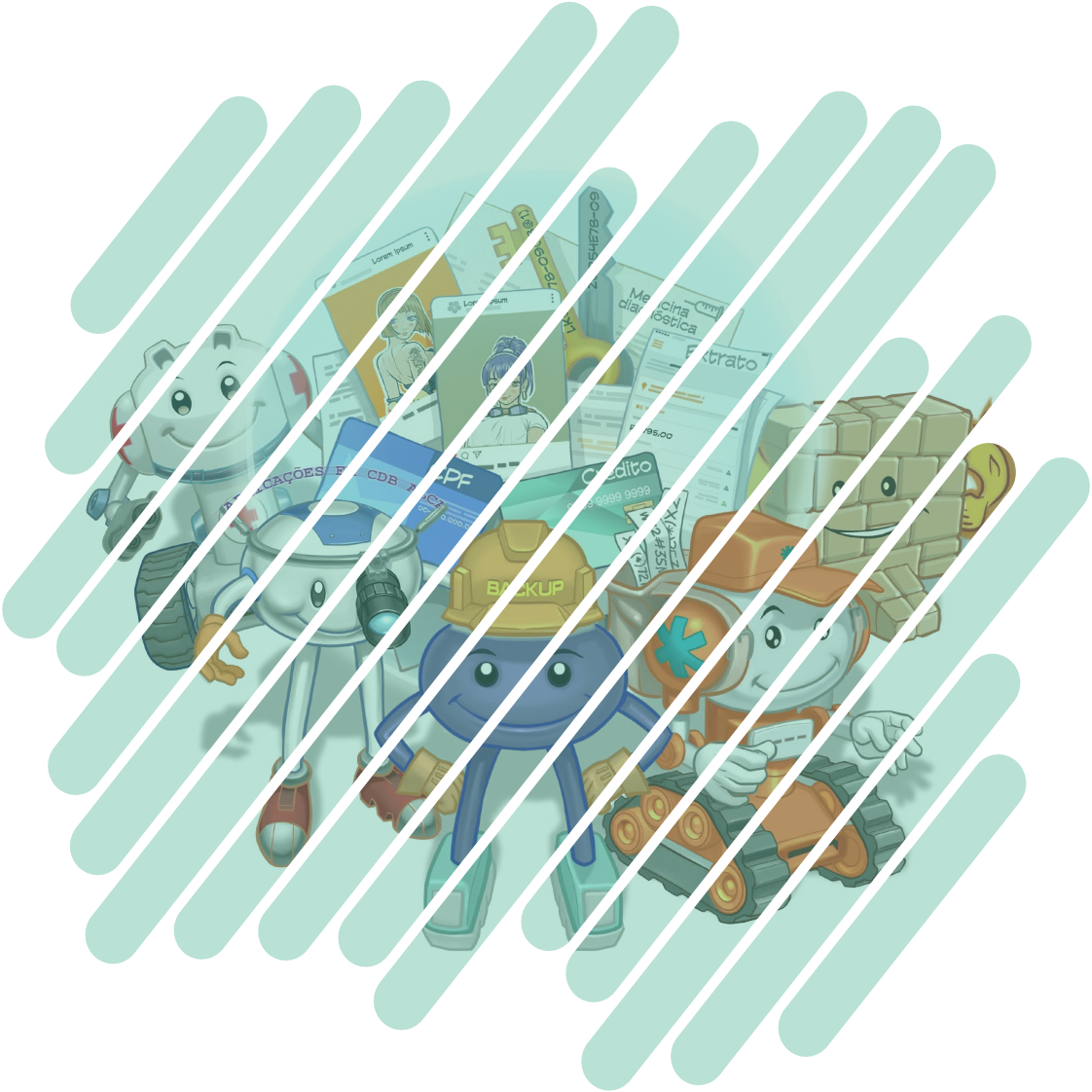
Cartilha de Segurança para Internet

FASCÍCULO

PROTEÇÃO DE DADOS



Com a contribuição da:

ANPD

Produzido por:

cert.br nic.br cgi.br

VOCÊ JÁ REPAROU NA QUANTIDADE DE DADOS QUE POSSUI E PRODUZ?

Dados de cadastros, biográficos, profissionais, financeiros e de navegação são apenas alguns exemplos de dados referentes a você que, diariamente, circulam por diversas redes e são armazenados em diferentes sistemas, dispositivos e mídias.

Infelizmente, há situações em que seus dados podem ser perdidos, indevidamente acessados ou até mesmo coletados e vendidos sem que você tenha ciência disso. Alguns exemplos dessas situações incluem:

- » você perde o celular, computador ou mídia removível
- » seus dados são interceptados ao trafegarem nas redes
- » há um vazamento envolvendo seus dados
- » suas contas de usuário e sistemas onde seus dados estão armazenados são invadidos
- » seus dados de navegação são coletados de forma não transparente e compartilhados sem seu consentimento.

Para tentar evitar essas situações, proteger seus dados e assegurar que eles sejam tratados de forma adequada há um conjunto de mecanismos de segurança que você pode usar. Por exemplo, o uso de senhas fortes impede o acesso indevido às contas e a criptografia dificulta que seus dados sejam acessados e alterados indevidamente.

Há situações, entretanto, em que os mecanismos de segurança sozinhos não protegem seus dados; por exemplo, quando eles são passados deliberadamente a outros sem sua autorização ou são coletados sem necessidade.

Por isso, adotar uma postura preventiva, tentando reduzir a quantidade de dados fornecida por você, é essencial. Para coibir abusos, garantir seus direitos e agir adequadamente quando necessário é importante também que você conheça um pouco da legislação vigente.

SEUS DADOS SÃO VALIOSOS: PROTEJA-OS

COMO SEUS DADOS PODEM SER ABUSADOS

O abuso de seus dados pode acarretar prejuízos financeiros, restrição a direitos ou benefícios e invasão da sua privacidade. Esse abuso pode ocorrer de diversas formas:

ACESSO INDEVIDO

» Seus dados podem ser indevidamente acessados:

- por aplicativos e *sites* que processem seus dados além das finalidades informadas
- por atacantes ou códigos maliciosos que consigam acesso às suas contas, aos seus equipamentos ou mídias
- em casos de vazamentos de dados

COLETA EXCESSIVA

» Muitos aplicativos e *sites* coletam dados extras sem o seu conhecimento e os utilizam para a elaboração de perfis de comportamento (*profiling*)

» Seu perfil pode, então, ser usado, sem o seu consentimento, de forma discriminatória ou para fins como propagandas

PERDA DE DADOS

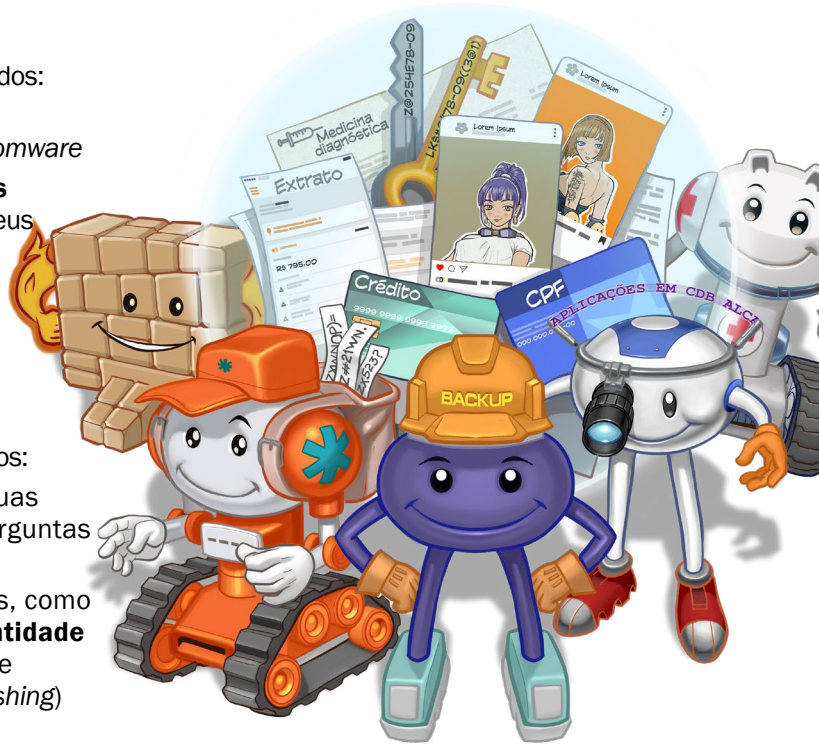
» Seus dados podem ser perdidos:

- pela ação de **códigos maliciosos**, como *ransomware*
- pela ação de **atacantes** que consigam invadir seus equipamentos e mídias e venham a apagá-los

INVASÃO DE CONTAS E GOLPES

» Seus dados podem ser usados:

- para tentar adivinhar suas senhas e responder perguntas de segurança
- em tentativas de golpes, como **extorsão**, **furto de identidade** e ***phishing*** direcionado e personalizado (*spear phishing*)



COMO SE PREVENIR

BACKUPS

Backups **protegem** seus dados **em caso de mau funcionamento** de equipamentos, da **perda de dispositivos** e da ação de **códigos maliciosos**, especialmente *ransomware.*

- Faça *backup* regularmente
- Teste periodicamente
- Mantenha pelo menos um *backup off-line*

ARQUIVOS

- Evite colocar na nuvem arquivos contendo dados confidenciais ou que considere privados
- Crie uma partição criptografada ou use recursos de criptografia para armazená-los
- Seja cuidadoso ao abrir arquivos enviados por terceiros

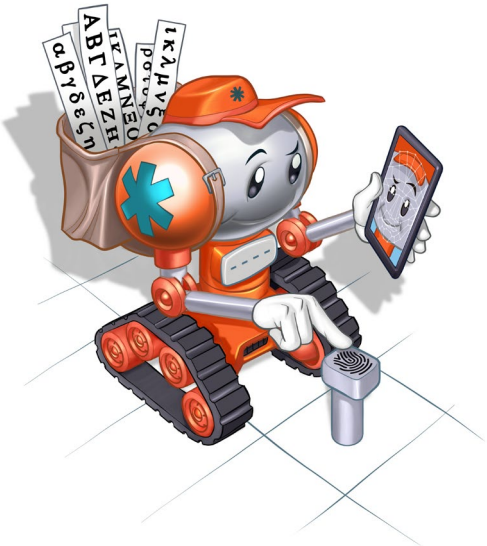
CRIPTOGRAFIA

A criptografia ajuda a tornar as transmissões de dados mais seguras, detectar alterações em seus dados e impedir que sejam lidos indevidamente.

- Use criptografia para **proteger os dados armazenados** em seus equipamentos e mídias
- **Ative** as configurações de **criptografia** em seus **discos** e **mídias**, como *pen drives* e discos externos
- Use conexões seguras, sempre que possível

CONTAS E SENHAS

- Crie **senhas fortes** e não repita senhas
- Habilite a **verificação em duas etapas** em todas as suas contas
- Habilite, quando disponíveis, **notificações de *login***, para ser mais fácil perceber se outras pessoas estiverem usando suas contas
- Tenha certeza de sair de suas contas (*logout*) ao usar equipamentos compartilhados
- Habilite as configurações de privacidade e segurança nos serviços



APLICATIVOS

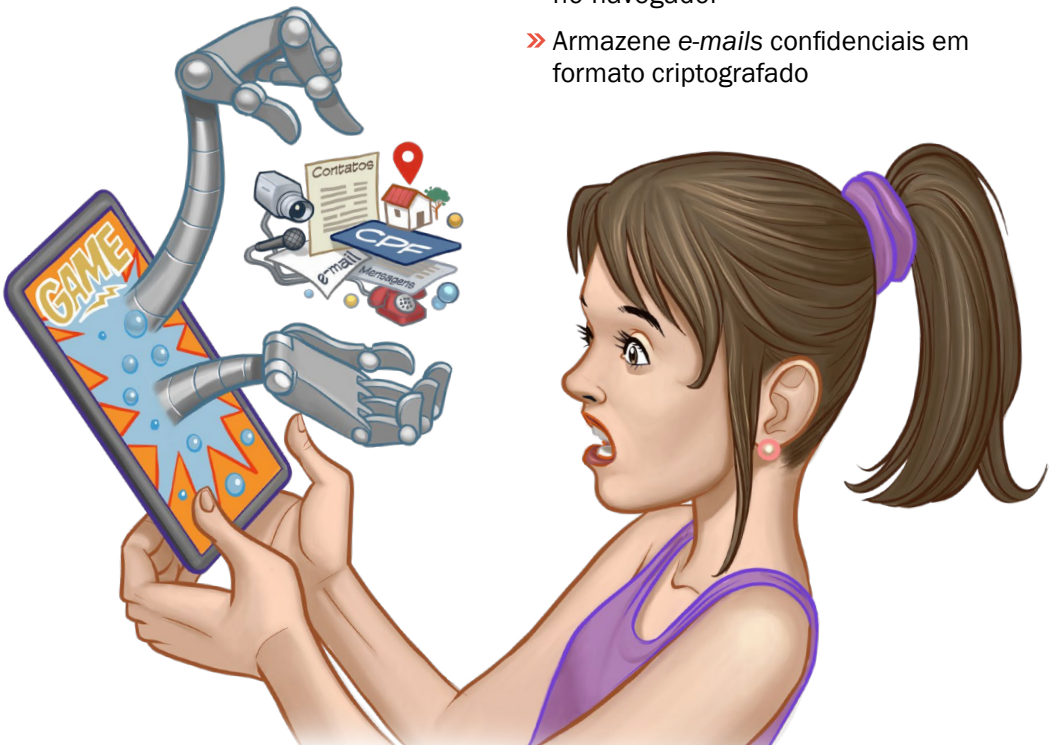
- Instale aplicativos somente de **fontes e lojas oficiais**
- Antes de instalar, verifique as telas e o nome do aplicativo, pois muitos falsos aplicativos se assemelham aos oficiais
- Observe se o **desenvolvedor é confiável**, quantas pessoas instalaram o aplicativo e qual a opinião delas sobre ele
- Durante a instalação, **fique atento às permissões**:
  - forneça apenas aquelas que considerar necessárias
  - por exemplo, um aplicativo de teste de velocidade não precisa ter acesso aos seus contatos para funcionar
- **Limite** quais aplicativos podem acessar o microfone, a câmera, seus contatos e sua localização
- Apague os aplicativos que você não usa mais

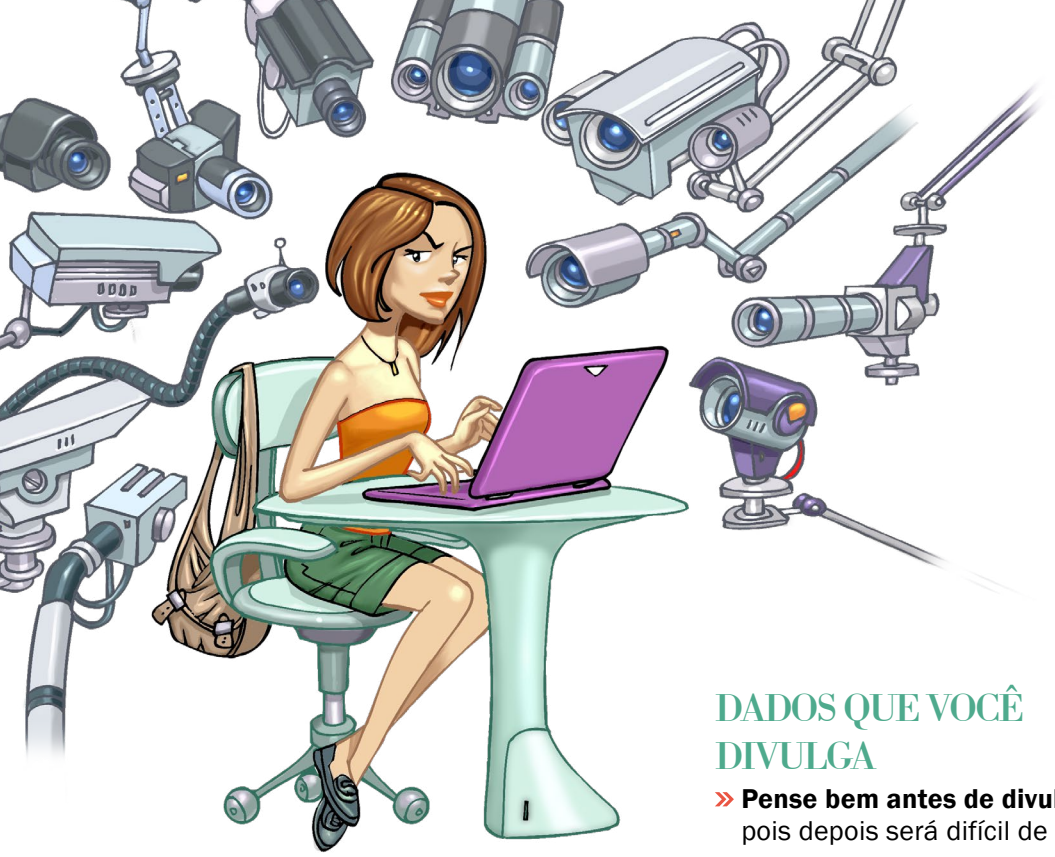
EQUIPAMENTOS E MÍDIAS

- Atualize o **sistema e os aplicativos**
- Utilize **mecanismos de segurança**
- Cuidado para não perder *pen drives* e discos externos
- Antes de se desfazer de seus equipamentos e mídias **apague os dados armazenados**, sobrescrevendo discos ou restaurando opções de fábrica
- Escolha empresas com **boa reputação**, ao enviar seus equipamentos para **manutenção**
- Seja cuidadoso ao usar equipamentos de terceiros

E-MAILS E MENSAGENS ELETRÔNICAS

- **Desconfie** de *links* ou pedidos de pagamentos recebidos via mensagens eletrônicas, **mesmo que vindos de pessoas conhecidas**
- Seja cuidadoso ao acessar seu *webmail*: digite a URL diretamente no navegador
- Armazene *e-mails* confidenciais em formato criptografado





REDUZA A QUANTIDADE DE DADOS SOBRE VOCÊ NA INTERNET

Você sabia que todas as vezes que acessa seus equipamentos e “entra na Internet” alguns de seus dados são de alguma forma fornecidos? Cada vez que acessa um *site*, assiste a um vídeo ou compra algo, deixa marcas de sua passagem. Essas marcas são chamadas **vestígios**, **rastros** ou **pegadas digitais** e podem ser usadas para criar sua reputação *online* e definir seu perfil comportamental.

DADOS QUE VOCÊ DIVULGA

- **Pense bem antes de divulgar algo**, pois depois será difícil de excluir
- Seja **seletivo** ao aceitar seus **contatos** nas redes sociais
- **Ao preencher cadastros questione-se** sobre a real necessidade de fornecer todos os dados, e de a instituição retê-los

DADOS COLETADOS SOBRE VOCÊ

- Use conexões seguras
- Seja **seletivo** ao baixar **aplicativos**
- Observe as **configurações de privacidade** de seus aplicativos e navegadores
- Ao acessar *sites*, procure **limitar a coleta** de dados por ***cookies***
  - preferencialmente, autorize somente aqueles essenciais ao funcionamento da sessão
- **Limpe** frequentemente o **histórico de navegação**

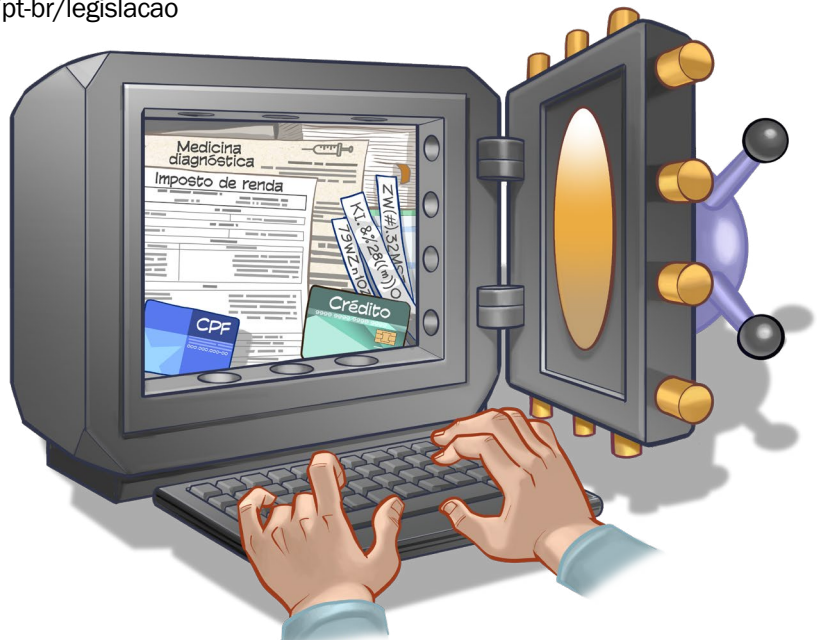
INFORME-SE SOBRE SEUS DIREITOS

A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

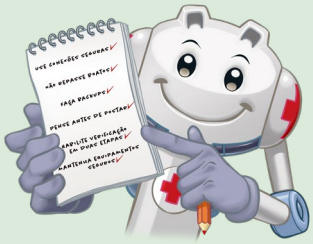
- A LGPD foi criada para que o indivíduo tenha **controle** sobre seus **dados pessoais** e saiba **como** esses dados **são tratados** por organizações públicas, privadas e terceiros
- Segundo a LGPD são considerados dados pessoais as informações relacionadas a pessoa natural identificada ou identificável
- Como titular de dados pessoais você tem diversos direitos garantidos pela LGPD, como os definidos no art. 18
- Informe-se sobre a LGPD, **conheça seus direitos** e saiba como agir de forma adequada: https://www.gov.br/anpd/pt-br/legislacao

BENEFÍCIOS E DIREITOS TRAZIDOS PELA LGPD

- A LGPD dá a você o direito de **saber** exatamente como seus dados **são tratados**, quais dados são **coletados** e o porquê e com quem eles são **compartilhados**
- Organizações públicas e privadas devem disponibilizar informações claras que o ajudem a compreender os termos de consentimento e as bases legais que apoiam o tratamento dos seus dados
- A LGPD traz maior segurança jurídica, ao fornecer mecanismos para que você tenha controle sobre quais dados seus são coletados e como são usados
- **Caso a instituição** responsável pelo tratamento de seus dados pessoais **não atenda a um de seus direitos** de titular sem uma justificativa legal, você tem o direito de peticionar uma **reclamação para a Autoridade Nacional de Proteção de Dados** – ANPD, através deste *link*: https://www.gov.br/anpd/pt-br/canais_atendimento



SAIBA MAIS



» Para mais detalhes sobre este e outros assuntos relacionados com cuidados na Internet, consulte os demais Fascículos da Cartilha de Segurança e o Livro Segurança na Internet, disponíveis em: **cartilha.cert.br**

» Procurando material para conversar sobre segurança com diferentes públicos? O Portal Internet Segura apresenta uma série de materiais focados em crianças, adolescentes, pais, responsáveis e educadores, confira em: **internetsegura.br**

cert.br

O CERT.br é o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Desde 1997, o grupo é responsável por tratar incidentes de segurança envolvendo redes conectadas à Internet no Brasil. O Centro também desenvolve atividades de análise de tendências, treinamento e conscientização, com o objetivo de aumentar os níveis de segurança e de capacidade de tratamento de incidentes no Brasil. Mais informações em **www.cert.br.**

nic.br

O Núcleo de Informação e Coordenação do Ponto BR — NIC.br (**www.nic.br**) é uma entidade civil, de direito privado e sem fins de lucro, que além de implementar as decisões e projetos do Comitê Gestor da Internet no Brasil, tem entre suas atribuições: coordenar o registro de nomes de domínio — Registro.br (**www.registro.br**), estudar, responder e tratar incidentes de segurança no Brasil — CERT.br (**www.cert.br**), estudar e pesquisar tecnologias de redes e operações — Ceptro.br (**www.ceptro.br**), produzir indicadores sobre as tecnologias da informação e da comunicação — Cetic.br (**www.cetic.br**), implementar e operar os Pontos de Troca de Tráfego — IX.br (**www.ix.br**), viabilizar a participação da comunidade brasileira no desenvolvimento global da Web e subsidiar a formulação de políticas públicas — Ceweb.br (**www.ceweb.br**), e abrigar o escritório do W3C no Brasil (**www.w3c.br**).

cgi.br

O Comitê Gestor da Internet no Brasil, responsável por estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil, coordena e integra todas as iniciativas de serviços Internet no País, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados. Com base nos princípios do multissetorialismo e transparência, o CGI.br representa um modelo de governança da Internet democrático, elogiado internacionalmente, em que todos os setores da sociedade são partícipes de forma equânime de suas decisões. Uma de suas formulações são os 10 Princípios para a Governança e Uso da Internet (**www.cgi.br/principios**). Mais informações em **www.cgi.br**.

ANPD

A Autoridade Nacional de Proteção de Dados – ANPD é um órgão vinculado à Presidência da República, dotada de autonomia técnica e decisória, que tem a competência de zelar pela proteção dos dados pessoais com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, conforme disposto na Lei nº 13.709, de 14 de agosto de 2018, a LGPD. Mais informações em **www.gov.br/anpd.**

maio / 2021