O que é dado pessoal?

Dado pessoal é a informação relacionada à pessoa natural identificada ou identificável.

≠ entre pessoa identificada e identificável?

IDENTIFICADA:

Quando você fornece seu nome, CPF, RG, habilitação.

IDENTIFICÁVEL:

Quando informações aparentemente não relacionadas permitem, em conjunto, identificar o indivíduo.

...e o dado pessoal sensível?

Dado pessoal sensível é toda informação que envolve aspectos mais íntimos da vida de um indivíduo, como origem racial ou étnica, convicções religiosas, opiniões políticas, filiação a sindicatos ou organizações de cunho religioso, filosófico ou político, dados genéticos, biométricos, sobre a saúde ou vida sexual, orientação sexual, dados relativos a menores de idade, entre outros, que merecem uma proteção especial devido ao seu potencial impacto na esfera privada do titular dos dados.

EXEMPLO

Em uma comunidade indígena existe um senhor de 80 anos com uma doença sexualmente transmissível (DST). Nessa comunidade existe apenas uma pessoa com 80 anos. Portanto, esse senhor será identificado através de informações indiretas.

INFORMAÇÕES

Comitê de Segurança da Informação

csi.chc-ufpr@ebserh.gov.br

Encarregado de Dados Pessoais

lgdp.chc-ufpr@ebserh.gov.br

Quem é o titular do dado pessoal?

O titular do dado é o “dono” da informação, ou seja, a pessoa natural a quem se referem os dados que serão objeto de tratamento.

E o que é pessoa natural?

É a pessoa viva.
A LGPD não trata de dados de pessoas falecidas.

Quem ou o que é protegido pela LGPD?

Apesar de usarmos o termo “proteção de dados”, na verdade a proteção não é do dado, mas da pessoa titular dele. O critério de dado pessoal não é de privacidade, mas de identificabilidade.

O espaço de privacidade é aquele que você escolhe com quem compartilhar algo seu. Existe uma diferença entre dados pessoais e dados privados. Saber exatamente o que está sendo feito com os seus dados é autodeterminação informativa: para que, desde quando, até quando, etc.

INFORMAÇÕES

Comitê de Segurança da Informação

csi.chc-ufpr@ebserh.gov.br

Encarregado de Dados Pessoais

lgdp.chc-ufpr@ebserh.gov.br

Medidas de segurança para proteção de dados pessoais

Incluem medidas técnicas, como a criptografia, anonimização e pseudonimização, medidas organizacionais, como quem tem permissão para acessar o dado e jurídicas, como normas de sigilo.

O que é criptografia?

É um método de proteção de dados que envolve a codificação das informações para que apenas pessoas autorizadas possam acessá-las.
Isso é feito através de conjuntos de operações matemáticas que embaralham os dados, tornando-os ilegíveis para quem não possui a chave de decodificação.

O que é anonimização?

É uma técnica de processamento de dados que remove ou modifica informações que possam identificar uma pessoa, ou seja, que não podem ser associados a nenhum indivíduo específico (a pessoa passa a ser anônima).

O que é pseudonimização?

É o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

EXEMPLO

Numa lista “numerada” consta nome completo, CPF, sexo, raça e profissão. Para pseudonimizar seria necessário refazer a lista “numerada” apenas com o CPF descaracterizado, sexo, raça e profissão. Quem consultar a lista desidentificada não saberá quem são as pessoas, porém seria possível a reidentificação comparando uma lista com a outra devido à numeração.

INFORMAÇÕES

Comitê de Segurança da Informação
csi.chc-ufpr@ebserh.gov.br

Encarregado de Dados Pessoais
lgdp.chc-ufpr@ebserh.gov.br

O que é um vazamento de dados?

Um vazamento de dados ocorre quando informações confidenciais são expostas, geralmente de forma não autorizada, podendo envolver dados pessoais, financeiros, médicos, entre outros.

O que é possível fazer com dados vazados?

Com dados vazados os criminosos podem realizar diversas atividades maliciosas, como roubo de identidade,, fraude financeira, chantagem, phishing, entre outros golpes cibernéticos.

Quais são os principais tipos de ataques cibernéticos?

Os principais tipos de ataques cibernéticos incluem:

- doxing (exposição de informações pessoais online)
- vazamento de dados (exposição não autorizada de informações confidenciais)
- defacement (alteração não autorizada de websites)
- ataques de negação de serviço - DoS (torna um serviço indisponível sobrecarregando-o com tráfego)

INFORMAÇÕES

Comitê de Segurança da Informação

csi.chc-ufpr@ebserh.gov.br

Encarregado de Dados Pessoais

lgdp.chc-ufpr@ebserh.gov.br

Quais as principais ameaças a proteção de dados?

As principais ameaças à proteção de dados incluem ataques de engenharia social, vazamento de credenciais, ataques de malware, entre outros.

Quem se beneficia do roubo de credenciais (login/senha)?

O roubo de credenciais beneficia principalmente os crackers, que são indivíduos especializados em invadir sistemas e redes de computadores para obter informações sensíveis ou causar danos.

O que é engenharia social?

É uma técnica utilizada por indivíduos mal-intencionados para manipular pessoas e obter informações confidenciais. Isso pode ser feito através de falsas identidades, persuasão psicológica ou manipulação emocional.

INFORMAÇÕES

Comitê de Segurança da Informação
csi.chc-ufpr@ebserh.gov.br

Encarregado de Dados Pessoais
lgdp.chc-ufpr@ebserh.gov.br

Quais os principais cuidados com as credenciais de acesso (login/senha)?

Os principais cuidados com as credenciais de acesso incluem:

- criação de senhas fortes e únicas para cada conta
- não compartilhamento de senhas com terceiros
- ativação da autenticação de dois fatores (2FA)
- evitar o armazenamento de senhas em locais inseguros, como post-its ou documentos não protegidos.

Considere também utilizar mais de um perfil do navegador para separar as utilizações: por exemplo, possuir um perfil apenas para acessar páginas bancárias.

Ao acessar um site, devo aceitar todos os cookies?

Não necessariamente. É importante revisar as políticas de privacidade e cookies de cada site antes de aceitá-los, pois alguns cookies podem ser invasivos ou comprometer a privacidade do usuário.

O que são cookies?

Cookies são pequenos arquivos de texto que os sites armazenam no navegador do usuário. Eles são usados para rastrear informações sobre a atividade do usuário online, como preferências de navegação e histórico de compras, a fim de oferecer uma experiência personalizada.

No entanto, alguns cookies podem ser utilizados para fins de rastreamento invasivo, daí a importância de revisar suas configurações de cookies e optar por um controle mais rigoroso sobre eles.

INFORMAÇÕES

Comitê de Segurança da Informação

csi.chc-ufpr@ebserh.gov.br

Encarregado de Dados Pessoais

lgdp.chc-ufpr@ebserh.gov.br

≠ entre segurança da informação e privacidade?

SEGURANÇA DA INFORMAÇÃO

Refere-se à proteção dos dados contra acessos não autorizados, uso indevido, divulgação, alteração ou destruição.

PRIVACIDADE

Refere-se ao controle que o indivíduo possui sobre suas informações pessoais e como essas informações são coletadas, utilizadas e compartilhadas. O próprio titular do dado pode optar por expor informações, por exemplo, por meio de postagens em redes sociais, que diminuam sua privacidade.

Como garantir a privacidade?

Para garantir a privacidade, é importante adotar medidas como:

- revisar e entender as políticas de privacidade dos serviços utilizados
- limitar o compartilhamento de informações pessoais
- utilizar configurações de privacidade mais restritivas em dispositivos e aplicativos
- estar ciente dos direitos de proteção de dados

Estes cuidados precisam ser redobrados quando se trata da exposição de menores.

INFORMAÇÕES

Comitê de Segurança da Informação
csi.chc-ufpr@ebserh.gov.br

Encarregado de Dados Pessoais
lgdp.chc-ufpr@ebserh.gov.br

O que fazer em caso de suspeita de violação de credenciais (login/senha)?

Em caso de suspeita de violação de credenciais é recomendado alterar imediatamente as senhas das contas afetadas, verificar a atividade recente nessas contas em busca de atividades suspeitas e notificar o provedor de serviços sobre a possível violação.

Quais as medidas a serem tomadas em caso de crimes envolvendo segurança da informação ou de dados, na esfera pessoal?

Em caso de crimes envolvendo segurança da informação ou dados, é importante contatar as autoridades policiais competentes e cooperar com as investigações. Além disso, é essencial manter registros detalhados de todas as atividades relacionadas ao incidente para fins de investigação e possível responsabilização legal. No Paraná, crimes cibernéticos e relacionado a exploração sexual de menores através de meios eletrônicos devem ser denunciados ao Núcleo de Combate aos Cibercrimes da Polícia Civil.

DICAS DE COMO MELHORAR A SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

- Não compartilhe suas senhas, crachás ou outras credenciais de acesso;
- Não deixe post it colados no computador com a sua senha;
- Utilize sempre múltiplo fator de autenticação. Os e-mails @ebserh e @hc dão suporte a eles;
- Ao se ausentar da sua estação de trabalho, bloqueie a tela do seu computador (tecla Windows + L);
- Apanhe sempre as impressões o mais rápido possível, especialmente se contiver dados pessoais ou assistenciais;
- Não clique em links recebidos por meio de mensagens eletrônicas (SMS, e-mails, redes sociais, etc desconhecidos e/ou não solicitados);
- Evite acessar seu webmail, internet banking ou outros serviços importantes em computadores de terceiros e, caso seja realmente necessário, ative o modo de navegação anônima;
- Nunca forneça informações sensíveis em sites sem que você tenha solicitado o serviço que o exige, e o faça somente se confiar no site e se o mesmo estiver utilizando criptografia (procure pelo cadeado no navegador e um informativo de certificado digital

DICAS DE COMO MELHORAR A SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

- Evite fazer cadastros em sites de venda desconhecidos pela Internet, especialmente fornecendo seus dados pessoais, pois muitas empresas possuem pouco ou nenhum tipo de segurança para armazenar e proteger seus dados;
- Cuidado ao disponibilizar informações pessoais em sites de relacionamento (telefones móveis, endereços residenciais etc). Reduza dados sobre você na internet;
- Pense bem antes de postar algo, porque depois de postado, dificilmente poderá ser excluído;
- Limite a coleta de dados por cookies. Aceite apenas cookies necessários e configure o navegador para não aceitar cookies de terceiros;
- Ao instalar e usar um aplicativo, autorize apenas acessos essenciais a seu funcionamento e operação.
- Só leia códigos QR se tiver certeza de que a fonte é confiável;
- Use sempre conexão segura (https);
- Não deixe mídias (como HD externo de backup) conectadas o tempo todo. Conecte-as apenas quando for realmente usá-las.