



Privacidade e
Proteção de Dados

SAÚDE  BRB



LEI GERAL DE PROTEÇÃO DE DADOS

ESSE ASSUNTO É DO SEU INTERESSE!

SAÚDE
 BRB

Clínica
SAÚDE  BRB

LEI GERAL DE PROTEÇÃO DE DADOS (LEI N. 13.709/18)

A **LGPD** dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (física).

A Lei dá ao Titular o poder de **controlar os seus dados pessoais**, tendo como fundamentos:

- I - o respeito à privacidade;
- II - a autodeterminação informativa;
- III - a liberdade de expressão, de informação, de comunicação e de opinião;
- IV - a inviolabilidade da intimidade, da honra e da imagem;
- V - o desenvolvimento econômico e tecnológico e a inovação;
- VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
- VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

DADOS **PESSOAIS**

É qualquer informação relacionada a pessoa natural (física) identificada ou identificável. Pode ser um CPF, RG, o nome, dentre outras informações que identificam uma pessoa física.

DADOS **SENSÍVEIS**

São uma categoria especial de dados, capazes de gerar discriminação contra o seu titular. A Lei traz uma categoria fechada composta por: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. Uma doença, por exemplo, é um dado pessoal sensível.



A CULTURA ORGANIZACIONAL NA ERA LGPD

A LGPD chega com a proposta de mudar a cultura de tratamento de dados no país, em razão disso, se faz necessário a alteração no comportamento dos profissionais. Segundo **Thomaz Côrte Real**, a maioria dos incidentes em segurança de dados são causados por pessoas.

COMO A SAÚDE BRB PROTEGE A **SEGURANÇA E A PRIVACIDADE?**

A **Saúde BRB** protege a segurança da informação e a privacidade dos seus titulares por meio do seu programa de governança em privacidade, que possui a seguinte estruturação:



**DENTRE
OUTROS
PONTOS,
CONTÊM:**

• Políticas e salvaguardas com base na avaliação de privacidade.

• Controle sobre todo o conjunto de dados pessoais em seus processos.

• Mecanismos para o titular exercer os seus direitos.

• Monitoramento contínuo.

Infelizmente, há situações em que seus dados podem ser perdidos, indevidamente acessados ou até mesmo coletados e vendidos sem que você tenha ciência disso. Por isso, de nada adianta ter a estrutura acima se não houver o cuidado do próprio usuário.

Para tentar evitar essas situações, é importante **proteger seus dados** e assegurar que eles sejam tratados de forma adequada, e para isso há um conjunto de mecanismos de segurança que você pode usar. Outra medida fundamental é tentar limitar a quantidade de dados fornecida por você e compartilhar apenas aquilo que é estritamente necessário.

A seguir, abordaremos os principais pontos a serem adotados para que o próprio usuário possa **evitar invasões, furtos e vazamentos de dados**.

TOME AS SEGUINTE MEDIDAS

- Cuide de suas contas e senhas.
- Nunca forneça códigos de verificação a terceiros.
- Monitore sua vida virtual, principalmente a sua identidade.
- Preste atenção a movimentações “estranhas”, seja em sites de compras, bancários, no próprio portal da Saúde BRB, dentre outros locais.
- Ative notificações e monitore tentativas de login, de recuperação ou troca de senhas.
- Verifique no “**Cadastro Pré**”, mantido por empresas do Setor de Telecomunicações, se alguma linha pré-paga de celular foi ativada usando seu CPF.
- Se receber notificações de instituições de proteção ao crédito, procure o contato destas instituições fora do *e-mail*, e faça uma ligação para saber a veracidade.

- Se ao tentar se cadastrar em algum serviço ou benefício, for informado que seu cadastro já existe, busque o contato e faça uma ligação para entender a situação.
- Caso constate que alguma conta foi invadida (como *e-mail* ou até mesmo o Portal da Saúde BRB) ou que criaram um perfil em seu nome:
 - a) Caso a situação envolva a Saúde BRB, entre em contato imediato com o e-mail *seguranca@saudebrb.com.br* ou *lgpd@saudebrb.com.br*
 - b) Efetue os procedimentos disponíveis nas plataformas para recuperação do acesso ou denúncia do perfil falso.
 - c) Informe seus contatos para que não caiam em golpes.

PREVINA-SE CONTRA GOLPES:

- a) Não clique em *links* recebidos por *e-mail* ou mensagens de texto, mesmo que pareçam enviados por alguém que você conhece (pode ser um *spear phishing*).
- b) Não efetive transações financeiras sem antes confirmar a identidade das partes envolvidas.
- c) Não passe dados pessoais e sensíveis sem ter certeza da identidade do interlocutor.

VULNERABILIDADES MAIS COMUNS

A seguir algumas vulnerabilidades mais comuns que podem ser evitadas:

WHATSAPP PESSOAL

O **Whatsapp** é uma empresa terceirizada que não pertence ou presta serviços diretos à Saúde BRB. Há muita controvérsia sobre a garantia que o *Whatsapp* possui em relação a privacidade nas suas conversas.

Logo, a utilização do *WhatsApp* pessoal em grupos de trabalho, com beneficiários, ou com profissionais de saúde, sempre representa um risco à segurança.

Internamente, a Saúde BRB não permite a utilização de *Whatsapp* pessoal, e as exceções se aplicam apenas para casos específicos previamente autorizados.

Além disso, nos casos de clonagem ou engenharia social, há o risco de acesso indevido e de vazamentos de dados pessoais de empregados/beneficiários/profissionais de saúde.

Por isso é importantíssimo que dados pessoais não sejam compartilhados pelo *Whatsapp*, evitando-se vazamentos.

GUARDA DE DADOS NO COMPUTADOR

Quando os dados relativos ao trabalho ficam salvos na máquina do(a) colaborador(a) e não na rede interna, ficam fora do controle da SETIN/ASTEC. Logo, é imprescindível que os dados/arquivos fiquem armazenados na rede para que a Saúde BRB possa ter o controle e aplicar as medidas de segurança cabíveis.

FALTA DE CONHECIMENTO DAS MEDIDAS DE SEGURANÇA DA SAÚDE BRB

Há ainda o risco de vazamentos e acessos indevidos pela não utilização de medidas de segurança ante a falta de conhecimento sobre a sua existência. Por isso, busque se informar sobre as medidas de segurança em seu setor e as aplique, evitando-se uma omissão causadora de danos.

COMPARTILHAMENTO EXCESSIVO DE DADOS

Outra questão importante é que boa parte dos vazamentos são causados pelo compartilhamento desnecessário ou excessivo de dados pessoais na saúde suplementar. Por isso, evite repassar ou acessar dados desnecessários, verificando efetivamente o que será utilizado.



MEDIDAS A SEREM TOMADAS PARA **ME PREVENIR**

SENHAS FORTES E TROCA PERIÓDICA

Use senhas fortes e não as repita. Se possível, habilite a verificação em duas etapas, notificações de login, para ser mais fácil perceber se outras pessoas estiverem usando suas contas.

A Saúde BRB possui como padrão interno a troca periódica de senhas justamente para evitar vazamentos e invasões.

Quando sair de suas contas faça *logout*, principalmente caso esteja usando equipamentos compartilhados.

Caso haja vazamento, troque imediatamente as senhas expostas.

E-MAILS

Não confie em *links* ou pedidos de pagamentos recebidos via mensagens eletrônicas, mesmo que vindos de pessoas conhecidas. Principalmente após um vazamento, é esperado um aumento nas tentativas de golpes por diferentes meios, como *e-mails*, mensagens de texto e ligações telefônicas. Estamos também em um período de alto índice de tentativas de golpes pela *internet*.

Ao acessar o seu e-mail por meio de uma plataforma, *web*, digite a URL diretamente no navegador.

Finalmente, armazene *e-mails* confidenciais em formato criptografado.

ENGENHARIA SOCIAL

A **Engenharia Social** é uma técnica empregada por criminosos virtuais para induzir usuários desavisados a enviar dados confidenciais, infectar seus computadores com *malware* ou abrir *links* para *sites* infectados. Além disso, os *hackers* podem tentar explorar a falta de conhecimento do usuário.

É importante destacar que os seus dados podem ser indevidamente acessados: por aplicativos e sites que processem seus dados além das finalidades informadas, e/ou por atacantes ou códigos maliciosos que consigam acesso às suas contas, aos seus equipamentos ou mídias.

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. Além disso, ative as configurações de criptografia em seus discos e mídias, como *pen drives* e discos externos. Use conexões seguras, sempre que possível.

COMPARTILHAMENTO DE 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.

APLICATIVOS

- Limite quais aplicativos podem acessar o microfone, a câmera, seus contatos e sua localização.
- Apague os aplicativos que você não usa mais.
- 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 e forneça apenas aquelas que considerar necessárias.
- 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

- Faça *backup* regularmente e mantenha pelo menos um *backup off-line*. Mantenha seus equipamentos seguros, com o sistema e os aplicativos atualizados e utilize mecanismos de segurança.
- Verifique no monitor de atividades de seu equipamento a lista de programas em execução e desconfie de processos “estranhos”.
- Evite colocar na nuvem arquivos contendo dados pessoais que considere confidenciais, como fotos e cópias de documentos. Use criptografia, sempre que possível, para proteger os dados armazenados em seus equipamentos
- Atualize o sistema e os aplicativos e 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.

REFERÊNCIAS

BRASIL. Presidência da República. Governo Digital. **Guias operacionais para adequação à LGPD**. Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias-operacionais-para-adequacao-a-lei-geral-de-protecao-de-dados-pessoais-lgpd> Acesso em: 08 nov. 2021.

CERT.br - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, et. al. **Cartilha de Segurança para Internet**: Fascículo Proteção de Dados. Disponível em: <https://cartilha.cert.br/fasciculos/protecao-de-dados/fasciculo-protecao-de-dados.pdf>. Acesso em : 08 nov. 2021.

CERT.br - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, et. al. **Cartilha de Segurança para Internet**: Fascículo Vazamento de Dados. Disponível em: <https://cartilha.cert.br/fasciculos/vazamento-de-dados/fasciculo-vazamento-de-dados.pdf>. Acesso em : 08 nov. 2021.

KAPERSKY. **Engenharia social**: definição. Disponível em: <https://www.kaspersky.com.br/resource-center/definitions/what-is-social-engineering>. Acesso em: 08 nov. 2021.

Saúde BRB

Central de Atendimento

(61) 3029-8057 - Distrito Federal
0800 061 0466 - Outras Localidades

Fale Conosco

faleconosco@saudebrb.com.br

Ouvidoria - Saúde BRB

ouvidoria@saudebrb.com.br

Encarregado de Dados

Canal de Denúncias

Clínica Saúde BRB

Diretrizes de Atendimento

SGAS Quadra 902, Conjunto B, Entrada A, 2º Andar
Edifício Athenas - Asa Sul
Brasília - DF, CEP 70.297-400

Horário de Funcionamento:

2ª a 6ª feira - 7h30 às 21h
Sábados, domingos e feriados - 8h às 13h

Telefone (61) 3029-6363

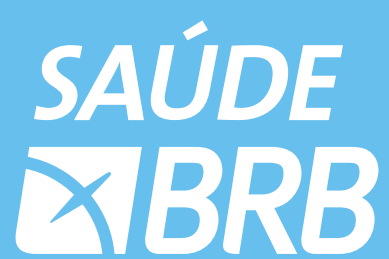
Whatsapp (61) 99981-4501

clinica@clnicasaudebrb.com.br

Saiba mais:

Sobre a Saúde BRB e o seu plano
www.saudebrb.com.br

Clique nos
links para
acessar



www.saudebrb.com.br

Clínica
SAÚDE  BRB

(61) 3029-6363

SGAS Quadra 902, Conjunto B, Entrada A, Sala 215, Ed. Athenas
clinica@clinicasaudebrb.com.br