MANUAL DE BOAS PRÁTICAS PARA

PROTEÇÃO DE DADOS PESSOAIS

Unimed
Mato Grosso

ANS - nº 32803-1

DIRETORIA EXECUTIVA

Unimed Mato Grosso
Gestão 2019 – 2022

Dr. Rubens Carlos de Oliveira Júnior
Diretor Presidente

Dr. Quidinho Tolentino de Queiroz
Diretor Administrativo

Dr. Ricardo Antônio Gonsales
Diretor Financeiro

Dr. Ricardo Rohde
Diretor de Intercâmbio

ÍNDICE

PALAVRA DO PRESIDENTE

Neste universo cada vez mais *smart*, onde a informação ganhou e continua ganhando mais relevância e valor, é fundamental a existência de regras bem claras para que os dados sejam manipulados e armazenados com seriedade e segurança.

A criação da **Lei Geral de Proteção de Dados,** popularmente conhecida pela sigla **LGPD**, é um grande avanço, pois coloca o Brasil na vanguarda do assunto, proporcionando mais critério e transparência nas relações entre as entidades e os donos dos dados.

Para nós, enquanto cidadãos, a lei permite controle sobre quais e como nossas informações serão utilizadas por organizações, empresas e pelo governo, garantindo privacidade e protagonismo nas decisões quanto aos nossos dados pessoais.

Como uma entidade prestadora de serviços, cuja função coleta, armazena e usa diariamente inúmeros dados pessoais, a existência de uma lei com diretrizes bem definidas dá um norte seguro para trabalharmos com a tranquilidade de que tudo está sendo feito da maneira correta.

Com a ideia de facilitar o entendimento e a aplicação da lei em seu dia a dia, desenvolvemos este manual para ajudar você a seguir todas as normas da LGPD em seu trabalho. Afinal, é nosso papel como Federação estar sempre ao seu lado, cuidando de você e da marca Unimed em todo Mato Grosso.

Dr. Rubens Carlos de Oliveira Júnior
Diretor Presidente da Unimed Mato Grosso

INTRODUÇÃO

A Lei nº 13.709, de 14 de agosto de 2018, intitulada **Lei Geral de Proteção de Dados Pessoais – LGPD**, dispõe sobre o tratamento de dados pessoais da pessoa natural, inclusive nos meios digitais, e tem como objetivo principal, proteger os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade do indivíduo.

Lidando com um volume imenso de dados pessoais, a Saúde é um dos setores mais impactados pela LGPD.

Em nosso Estado somos mais de **439 mil** beneficiários, **2.273** cooperados e **2.276** colaboradores, o que nos dá a dimensão da quantidade de dados pessoais e dados pessoais sensíveis que são tratados regularmente.

Com a LGPD, todos nós assumimos um grande desafio de tratar estes dados de forma legal, sempre considerando o melhor interesse do titular de dados, e proteger as informações pessoais que nos são confiadas em razão das nossas atividades.

Para respaldar nossas equipes, parceiros e terceiros, lançamos este Manual, que além de orientativo, reforça o nosso compromisso com a execução das melhores práticas de proteção e privacidade de dados pessoais.

POR DENTRO DA LGPD

A **LGPD** foi inspirada na **GDPR *(General Data Protection Regulation)***, aprovada na União Europeia desde 2016, que objetiva justamente a proteção e a privacidade dos dados pessoais.

Você pode então estar se perguntando, **"afinal, o que são dados pessoais?"**
Além de dado pessoal, outros conceitos sobre dados são fundamentais para o entendimento da LGPD, então veja a seguir:

Dado Pessoal

é toda informação que identifique ou permita identificar uma pessoa natural (física), como por exemplo: nome, CPF, RG, endereço, dados de localização, e-mail, número de telefone, data de nascimento, número do cartão do beneficiário ou uma foto.

Dado pessoal sensível

leva esse nome por estar relacionado a situações de vulnerabilidade e discriminação, exigindo um regime jurídico diferenciado e mais reforçado, como a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico.

Dado pessoal anonimizado

é quando o dado pessoal é convertido à um modo não identificável, como por exemplo, quando encobrimos caracteres através de símbolos:
Telefone (65) 9XXXX – 3567 ou CPF ***. ***. ***457- 06.

OS FUNDAMENTOS DA LGPD

É importante que você também conheça os fundamentos, ou seja, o que dá embasamento, alicerce para a LGPD.

- respeito à privacidade;
- inviolabilidade da intimidade, da honra e da imagem;
- autodeterminação informativa, ou seja, o poder que cada cidadão tem sobre seus próprios dados pessoais;
- liberdade de expressão, de informação, de comunicação e de opinião;
- desenvolvimento econômico e tecnológico e inovação;
- livre-iniciativa, livre concorrência e defesa do consumidor;
- Direitos Humanos, livre desenvolvimento da personalidade, dignidade e exercício da cidadania pelas pessoas naturais.

OS AGENTES DA LGPD

Agora que você já conhece a definição de dados estabelecida pela lei e seus fundamentos, é a hora de entender quem são os envolvidos na aplicação da LGPD.

Titular:

pessoa natural a quem se referem os dados pessoais que são objeto de tratamento, como, por exemplo, você!

Controlador:

pessoa natural ou jurídica, de direito público ou privado, a quem compete decidir sobre a utilização e o tratamento de dados pessoais, como por exemplo, a Unimed Mato Grosso.

Operador:

pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador, como por exemplo, colaboradores, fornecedores e/ou terceiros contratados que tratem dados pessoais em nome da Unimed Mato Grosso.

Encarregado de dados:

pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Autoridade Nacional de Proteção de Dados (ANPD):

órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da lei em todo o território nacional.

Tratamento é qualquer ação realizada durante todo ciclo de vida dos dados pessoais.

O CICLO DE VIDA DOS DADOS PESSOAIS

IMPORTANTE: É nossa responsabilidade assegurar os direitos do titular durante todo ciclo de vida dos dados pessoais.

Já que falamos sobre a importância de cumprir com a LGPD durante todo o ciclo de vida dos dados pessoais, vamos entender um pouco mais sobre cada uma das etapas deste ciclo.

1. **COLETA:** Obtenção, recepção ou produção de dados pessoais, independentemente do meio utilizado (papel, documento eletrônico, sistema de informação etc.).

2. **RETENÇÃO:** Arquivamento ou armazenamento de dados pessoais, independentemente do meio utilizado (papel, pastas suspensas, documento eletrônico, banco de dados etc.).

3. **PROCESSAMENTO:** Qualquer operação que envolva classificação, utilização, reprodução, processamento, avaliação ou controle da informação, extração e modificação de dados pessoais.

4. **COMPARTILHAMENTO:** Qualquer operação que envolva transmissão, distribuição, comunicação, transferência, difusão e compartilhamento de dados pessoais.

5. **ELIMINAÇÃO:** Qualquer operação que visa apagar ou eliminar dados pessoais, contemplando também o descarte dos ativos organizacionais, nos casos necessários ao negócio da instituição.

Os principais ativos organizacionais envolvidos no ciclo de vida dos dados pessoais são:

E QUAIS SÃO OS DIREITOS DO TITULAR DE DADOS?

- conhecer o processo de tratamento dos dados pessoais;
- ter acesso aos dados pessoais sob custódia do controlador;
- contar com meios para correção e atualização dos dados pessoais;
- solicitar anonimização, bloqueio ou eliminação de dados pessoais que sejam considerados excessivos ou que estejam em desconformidade com a LGPD;
- solicitar a portabilidade dos seus dados para outras empresas;
- ser informado sobre como e com quem o controlador realiza o compartilhamento de seus dados;
- revogar qualquer consentimento, a qualquer tempo.

A **LGPD** também determina em quais hipóteses os dados pessoais e dados pessoais sensíveis poderão ser tratados, ou seja, qualquer ação que seja aplicada a qualquer dado pessoal, em qualquer etapa do seu ciclo de vida, deve se enquadrar em alguma das justificativas legalmente previstas.

As hipóteses de tratamento estão detalhadamente descritas nos **artigos 7º e 11º da LGPD** e podem ser resumidas conforme abaixo:

Dados pessoais (Art. 7º)

1. mediante o consentimento do titular;
2. cumprimento de obrigação legal ou regulatória;
3. execução de políticas públicas;
4. realização de estudos de órgãos de pesquisa;
5. Execução de contrato/diligência pré-contratual;
6. exercício regular de direitos em processo judicial, administrativo ou arbitral;
7. proteção à vida ou incolumidade física do titular;
8. garantia à tutela da saúde, exclusivamente em procedimento realizado por profissional de saúde, serviços de saúde ou autoridade sanitária;
9. proteção ao crédito;
10. legítimo interesse do controlador.

Dados pessoais sensíveis (Art. 11º]

1. mediante o consentimento do titular;
2. cumprimento de obrigação legal ou regulatória;
3. execução de políticas públicas;
4. realização de estudos de órgãos de pesquisa;
5. exercício regular de direitos em processo judicial, administrativo ou arbitral;
6. proteção à vida ou incolumidade física do titular;
7. garantia à tutela da saúde, exclusivamente em procedimento realizado por profissional de saúde, serviços de saúde ou autoridade sanitária;
8. garantia da prevenção à fraude e à segurança do titular.

As CRIANÇAS E ADOLESCENTES ganharam destaque diferenciado no tratamento de seus dados pessoais, que poderão ser realizados somente mediante consentimento específico dado por, pelo menos, um dos pais ou pelo responsável legal. Somente poderão ser coletados dados pessoais de crianças sem o consentimento específico dos pais e/ou responsável legal quando a coleta for necessária para contatar os pais ou o responsável legal, uma única vez e sem seu armazenamento, ou para a proteção da criança.

Para ajudar você a gerenciar o consentimento do titular conforme as melhores práticas da LGPD, temos dicas importantes!

FIQUE ATENTO!

Quando for executar qualquer tratamento a um dado pessoal ou dado pessoal sensível, questione-se sobre a sua hipótese legal, mesmo que seja solicitado por algum superior.

Por exemplo: o gerente do departamento que você trabalha solicita que encaminhe um banco de dados de clientes para o e-mail pessoal dele. Você sabe que essa atividade não está prevista em nenhum processo e os riscos não estão mapeados. Antes de encaminhar os dados pessoais, questione a finalidade desse tratamento!

Na dúvida, converse com o nosso encarregado de dados:
Thiago Ferreira
RAMAL (65) 3612-3539
encarregado@unimedmt.coop.br

através do Portal da Privacidade no link:
https://www.unimedmt.com.br/site/Home/PrivacidadeIntro

ou acione qualquer membro do Comitê Gestor de Proteção de Dados Pessoais.

CONHEÇA OS PRINCIPAIS RISCOS À PROTEÇÃO E PRIVACIDADE DE DADOS PESSOAIS E SEUS IMPACTOS

Os principais riscos

Os impactos de incidentes com dados pessoais

Segundo o Relatório do Custo de uma Violação de Dados, da IBM Security, versão 2021,

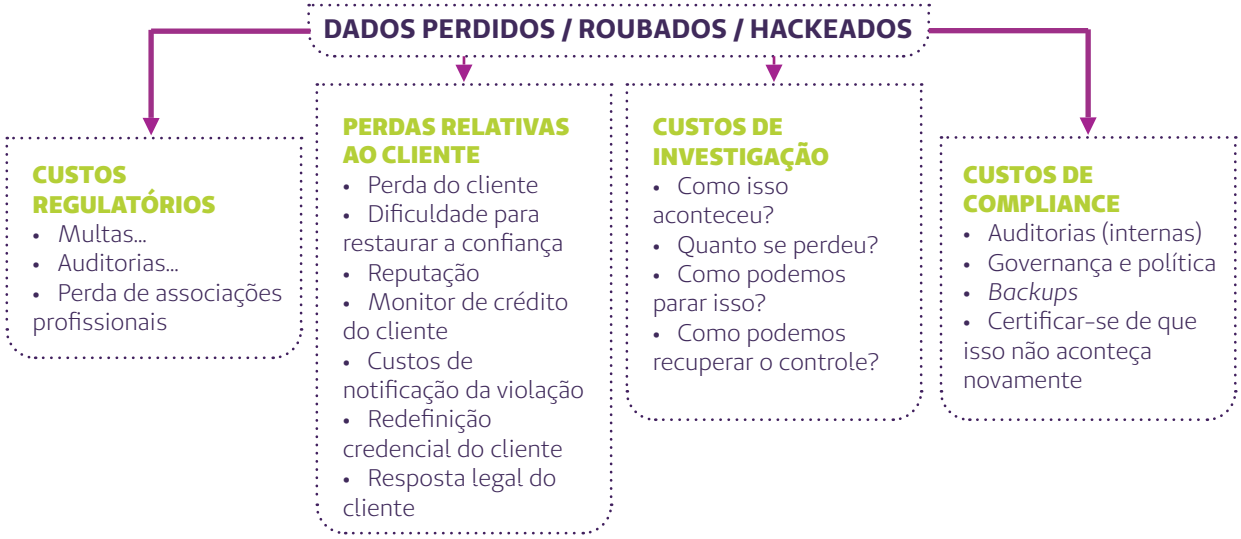
287 Número médio de dias para identificar e conter a violação de dados

US$ 9,23 milhões Custo total médio de uma violação de dados no setor da saúde

US$ 1,07 milhão Diferença do custo onde o trabalho remoto foi um causador ou fator para a violação de dados.

58 dias Tempo a mais que as organizações que tinham mais de 50% da sua força de trabalho em home office, demoraram para identificar e conter violações se comparado àquelas com menos de 50% dos funcionários trabalhando remotamente.

COMO A PERDA DE DADOS TRAZ CUSTOS FINANCEIROS PARA A MINHA ORGANIZAÇÃO?



PENALIDADES DA LGPD

Uma das formas de buscar prever os futuros riscos dos impactos das sanções da LGPD no Brasil reside em analisar cautelosamente a atuação das autoridades de proteção de dados na Europa, onde a lei já está em vigor há alguns anos.

Segundo relatórios sobre a GDPR e sua atuação na proteção de dados pessoais em países da União Europeia, da sua vigência até meados de 2021, teriam sido aplicadas mais de 800 penalidades.

Destas, as multas de maior valor foram aplicadas contra as empresas Amazon Europe Core, no valor de 746 milhões de euros (aproximadamente R$ 4,5 bilhões de reais) e a WhatsApp Ireland Ltd, no valor de 225 milhões de euros (cerca de R$ 1,3 bilhão de reais).

No Brasil, o Capítulo VIII da LGPD trata sobre as Sanções Administrativas e prevê a aplicação das seguintes penalidades:

1. Advertência, com indicação de prazo para adoção de medidas corretivas;
2. Multa simples, de até R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
3. Multa diária, observado o limite total;
4. Publicização da infração após devidamente apurada e confirmada a sua ocorrência;
5. Bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
6. Eliminação dos dados pessoais a que se refere a infração;
7. Suspensão parcial do funcionamento do banco de dados ou do exercício da atividade a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização pelo controlador;
8. Proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

BOAS PRÁTICAS PARA TORNAR SUA ROTINA MAIS SEGURA

Conheça e aplique as Políticas de Privacidade e de Proteção de Dados Pessoais, e demais normas, procedimentos e/ou orientações de segurança de dados.

Não fotografe seu ambiente de trabalho, pois dados podem estar expostos em documentos ou telas de computadores.

Não deixe documentos expostos em cima da mesa. Mantenha sua mesa limpa e organizada.

Não solicite dados pessoais, a menos que sejam estritamente necessários. Nada de coletá-los pensando "vai que eu precise".

Quando não estiver utilizando o computador, lembre-se de bloquear a tela do seu monitor. Utilize o atalho das teclas Windows + L, simultaneamente.

Não instale sistemas, softwares e/ou aplicativos em seu computador sem a autorização/conhecimento da TI.

Fique atento caso seu computador desligue sozinho ou sem motivo aparente, fique lento para ligar ou executar programas, apareçam mensagens em excesso e/ou sinta falta de arquivos que você certamente não deletou. Comunique a TI!

Execute todos os alertas de atualização para o seu computador.

Não compartilhe nenhum de seus dados de login e senhas.

Crie senhas fortes, que incluam letras maiúsculas e minúsculas, caracteres especiais e números. Troque suas senhas com frequência e não utilize a mesma senha para todos os seus acessos.

Não clique em links suspeitos ou abra anexos de remetentes desconhecidos no e-mail.

Ao encaminhar e-mails, certifique-se da necessidade das informações que está encaminhando e se os destinatários estão corretos.

Não divulgue dados ou informações de colaboradores, cooperados, fornecedores, terceiros, beneficiários ou qualquer outra pessoa, sem que tenha uma justificativa legal para fazê-lo.

Cuidado ao conversar com colegas de trabalho sobre assuntos referentes à organização em corredores, elevadores, restaurantes e outros espaços de circulação de pessoas.

Ao descartar documentos contendo dados pessoais, opte por picotar ou rasgar, evite apenas amassá-los. Consulte a forma de descarte padronizada para cada documento.

Não deixe documentos na impressora.

Verifique se o rascunho que vai utilizar não contém dados pessoais ou informações sigilosas da organização.

Não conecte computadores ou dispositivos móveis à rede de Wi-Fi desconhecida ou de acesso livre enquanto estiver fora do seu ambiente de trabalho.

Não utilize dispositivos de armazenamentos (pendrive, hd externo) de origem desconhecida que possam colocar em risco o seu computador.

Comunique o Encarregado de Dados Pessoais sempre que houver um incidente com dados pessoais ou até mesmo um quase erro de tratamento, assim você ajudará a manter nossa Unimed segura.

Qualquer dúvida, conte sempre com nosso Encarregado de Proteção de Dados Pessoais.

Atenção:

para ajudá-lo a reconhecer se a decisão que irá tomar sobre o tratamento de um dado pessoal é a melhor, faça uma reflexão:

Este tratamento é realmente necessário?

A finalidade desse tratamento está fundamentada na LGPD?

Para este tratamento, os dados pessoais podem ser minimizados ou anonimizados?

Para este tratamento, os riscos de um possível incidente ou violação de segurança, e seus impactos, são conhecidos e monitorados?

Se não estiver seguro, fale com o Encarregado de Proteção de Dados Pessoais.

GLOSSÁRIO

ACESSO: ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique.

ARMAZENAMENTO: ação ou resultado de manter ou conservar em repositório um dado.

ARQUIVAMENTO: ato ou efeito de manter registrado um dado em qualquer das fases do ciclo da informação, compreendendo os arquivos corrente, intermediário e permanente, ainda que tal informação já tenha perdido a validade ou esgotado a sua vigência.

AVALIAÇÃO: analisar o dado com o objetivo de produzir informação.

BACKUPS: "cópia de segurança", e corresponde a criação e armazenamento de cópias de arquivos digitais importantes, de modo que seja possível realizar sua restauração em caso de perda dos arquivos originais.

CLASSIFICAÇÃO: maneira de ordenar os dados conforme algum critério estabelecido.

COLETA: recolhimento de dados com finalidade específica.

COMUNICAÇÃO: transmitir informações pertinentes a políticas de ação sobre os dados.

CONSENTIMENTO: manifestação livre em que se aprova algo.

CONTROLE: ação ou poder de regular, determinar ou monitorar as ações sobre o dado.

DIFUSÃO: ato ou efeito de divulgação, propagação, multiplicação dos dados.

DISTRIBUIÇÃO: ato ou efeito de dispor de dados de acordo com algum critério estabelecido.

ELIMINAÇÃO: ato ou efeito de excluir ou destruir dado do repositório.

EXTRAÇÃO: ato de copiar ou retirar dados do repositório em que se encontrava.

HARDWARE: partes físicas de um computador, necessárias para o seu funcionamento.

GLOSSÁRIO

INCIDENTE DE SEGURANÇA ou VIOLAÇÃO DE DADOS: acontecimento indesejado ou inesperado, hábil a comprometer a segurança dos dados pessoais, de modo a expô-los a acessos não autorizados e a situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

LOGS: registro de atividades gerado por programas e serviços de um computador.

MODIFICAÇÃO: ato ou efeito de alteração do dado.

PHISHING: o phishing ocorre por meio do envio de mensagens eletrônicas que tenta obter dados pessoais e/ou financeiros de um usuário.

PROCESSAMENTO: ato ou efeito de processar dados visando organizá-los para obtenção de um resultado determinado.

PRODUÇÃO: criação de bens e de serviços a partir do tratamento de dados.

RANSOMWARE: ataque malicioso que bloqueia o acesso do usuário aos seus arquivos ou ao dispositivo, exigindo um pagamento online anônimo para que o acesso seja restaurado.

RECEPÇÃO: ato de receber os dados ao final da transmissão.

REPRODUÇÃO: cópia de dado preexistente obtido por meio de qualquer processo.

SOFTWARE: conjunto de componentes lógicos de um computador ou sistema de processamento de dados, ou seja, todo programa presente em diversos dispositivos, como computadores, celulares, televisores, etc.

TI: Tecnologia da Informação.

TRANSFERÊNCIA: mudança de dados de uma área de armazenamento para outra, ou para terceiro.

TRANSMISSÃO: movimentação de dados entre dois pontos por meio de dispositivos elétricos, eletrônicos, telegráficos, telefônicos, radioelétricos, pneumáticos, etc.

UTILIZAÇÃO: ato ou efeito do aproveitamento dos dados.

VULNERABILIDADE: condição que, quando explorada por um atacante, pode resultar em uma violação de segurança.

REFERÊNCIAS

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 de janeiro de 2022.

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Cartilha de Segurança para Internet – Fascículo de Proteção de Dados, versão 2021/ CERT.br – São Paulo: Comitê Gestor da Internet no Brasil, 2021. Disponível em: https://cartilha.cert.br/fasciculos/protecao-de-dados/fasciculo-protecao-de-dados.pdf. Acesso em: 10 de janeiro de 2022.

CNSAUDE. Código de Boas Práticas – Proteção de Dados para Prestadores Privados em Saúde. Confederação Nacional de Saúde, 2021. Disponível em: http://cnsaude.org.br/baixe-aqui-o-codigo-de-boas-praticas-protecao-de-dados-para-prestadores-privados-de-saude/. Acesso em: 10 de janeiro de 2022.

Comitê Central de Governança de Dados. Guia de Boas Práticas - Lei Geral de Proteção de Dados (LGPD), versão 2.0 de 2020. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf. Acesso em: 10 de janeiro de 2022.

GET PRIVACY. Ebook: LGPD no Setor da Saúde, 2021. Disponível em: https://getprivacy.com.br/ebook-lgpd-saude/. Acesso em: 08 de outubro de 2021.

IBM. Relatório do Custo de uma Violação de Dados. IBM Security, versão 2021. Disponível em: https://www.ibm.com/br-pt/security/data-breach. Acesso em: 10 de janeiro de 2022.

Núcleo de Segurança Informação e Coordenação do Ponto BR. Segurança digital: uma análise da gestão de riscos em empresas brasileiras [livro eletrônico] / [editor] Núcleo de Informação e Coordenação do Ponto BR. -- 1. ed. – São Paulo: Comitê Gestor da Internet no Brasil, 2020. Disponível em: https://cetic.br/media/docs/publicacoes/7/20210514123130/estudos-setoriais-seguranca-digital.pdf. Acesso em: 11 de outubro de 2021.

Unimed
Mato Grosso

WWW.UNIMEDMT.COOP.BR