MANUAL SOBRE
LGPD

Descubra como proteger as suas informações,
na era dos ataques cibernéticos.

PGE·RO

ELABORAÇÃO - CONTEÚDO

Maxwel Mota de Andrade
Procurador-Geral do Estado

Fábio Sousa Santos
Secretário-Geral da Procuradoria Geral do Estado

Rod Daniel Gomes Sussuarana do Nascimento
Encarregado pelo Tratamento de Dados Pessoais

DIAGRAMAÇÃO

Coordenação de Relações Públicas da
Procuradoria Geral do Estado

SUMÁRIO

GLOSSÁRIO

Antimalware: Ferramenta de detecção que procura anular ou remover os códigos maliciosos de um computador.

Antivírus: Ferramenta desenvolvida para detectar, anular e eliminar de um computador vírus e outros tipos de códigos maliciosos;

ANPD: É a autoridade máxima no Brasil sobre LGPD e sua missão é prestar orientações quanto à Lei e fazer com que suas regras sejam observadas por todos, estando autorizada a fiscalizar o seu efetivo e adequado cumprimento e a aplicar penalidades em caso de transgressão;

Backup: Cópias de segurança dos dados de um dispositivo ou local de armazenamento para outro. Tornando o dado redundante;

Dados pessoais sensíveis: Informações relacionadas à pessoa física/pessoa natural que podem causar discriminação e que, por isso, merecem proteção especial. Exemplos: 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.

GLOSSÁRIO

Filtro Antispam: Ferramenta que permite separar e-mails de acordo com regras pré-definidas. Utilizado tanto para o gerenciamento das caixas postais como para a seleção de e-mails válidos dentre os diversos spams recebidos.

Finalidade: Propósito, objetivo do tratamento de dados pessoais, previamente informado ao seu respectivo titular para efeito de obtenção de seu consentimento.

Firewall: Dispositivo de segurança usado para dividir e controlar o acesso entre redes de computadores.

Phishing: Tática de enganar as pessoas com o objetivo de obter informações pessoais como números de conta, senhas de acesso, de cartões, são os mais comuns.

Pseudoanonimização: É uma espécie de anonimização reversível. Exemplo: as informações obtidas do titular são mantidas em arquivos separados e somente sua junção permitirá identificar o indivíduo a quem pertencem.

Spam: Palavra comumente utilizada para se referir aos e-mails não solicitados, que normalmente são enviados em larga escala.

SOBRE A LGPD
(LEI GERAL DE PROTEÇÃO DE DADOS)

1. Afinal, o que é a LGPD?

A LGPD, Lei Geral de Proteção de Dados (Lei 13.709 de 14 de agosto de 2018), estabelece regras para tratamento dos dados pessoais (coleta, produção, armazenamento, utilização, acesso, etc), garantindo mais direitos aos titulares dos dados, bem como limitações e penalidades ao controlador de dados que trabalham com essas informações.

2. Para que foi criada a LGPD?

O objetivo da lei é dar mais transparência aos titulares dos dados e detalhar obrigações para o controlador de dados. Para isso, a lei é baseada em dez princípios, entre eles transparência, segurança, finalidade, necessidade e adequação.

3. Quais são os direitos dos titulares perante a administração ?

Para o exercício dos direitos dos titulares, a Lei prevê um conjunto de ferramentas, que, no âmbito público, traduzem-se em mecanismos que aprofundam obrigações de transparência ativa e passiva, bem como criam meios processuais para provocar a Administração Pública.

Em todos os casos, o titular do dado tem a faculdade de optar por resposta por meio eletrônico, seguro e idôneo para esse fim ou sob forma impressa.

Art. 1º. Esta Lei 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.

A PGE e a LGPD

A Procuradoria-Geral do Estado através da Portaria nº 345/2022 instituiu o Comitê Gestor de Proteção de Dados no âmbito da Procuradoria-Geral do Estado de Rondônia. Sendo composto pelo:

I. Secretário(a)-Geral da Procuradoria-Geral do Estado de Rondônia;

II. Encarregado(a) de Proteção de Dados Pessoais;

III. Diretor(a) de Tecnologia da Informação;

IV. Controlador(a) Interno(a);

V. Ouvidor(a) da Procuradoria-Geral do Estado de Rondônia;

VI. Assessor(a)de Segurança Institucional;

VII. Coordenador(a) do Escritório de Projetos;

VIII. 1 (um) representante designado pela da Corregedoria da Procuradoria-Geral do Estado de Rondônia;

IX. 1 (um) servidor(a) da carreira de apoio;

X. 1 (um) Procurador(a) do Estado não ocupante do cargo disposto no inciso I.

Por meio do comitê gestor foi aprovado o Programa de Governança da Procuradoria-Geral do Estado por meio da Portaria nº 457/2022 um roteiro de atividades que devem ser implementadas.

O roteiro é baseado em boas práticas sugeridas pela ANPD e em modelos internacionais, mas leva em consideração a estrutura organizacional da Procuradoria-Geral do Estado de Rondônia (PGE-RO).

USO SEGURO DE CREDENCIAIS DE ACESSO

- Sempre que disponível, ative a autenticação em duas etapas.
- A senha é pessoal e intransferível, não a divulgue e nem compartilhe. A senha é sua e de mais ninguém!
- Não escreva sua senha em local público ou de fácil acesso como em papéis, em arquivos sem proteção no computador ou em outro tipo de mídia.
- Feche sua sessão (logout) ao acessar sites que requeiram o uso de senhas, principalmente ao usar equipamentos compartilhados.
- Nunca use dados pessoais ou sequências de teclado como senha. Tente criar senhas fortes contendo letras (maiúsculas e minúsculas), números aleatórios e caracteres especiais, de pelo menos 10 (dez) dígitos.
- Evite usar a mesma senha para cadastro e acesso aos sistemas.
- Tente mudar suas senhas regularmente, principalmente se acessar sistemas em dispositivos que são utilizados por várias pessoas.

- Caso desconfie que sua senha tenha sido descoberta, vazada ou usada em um equipamento invadido ou infectado, altere-a imediatamente.
- Use conexões seguras (https) quando o acesso a um site, envolver o fornecimento de credenciais de acesso.

CUIDADOS COM O USO DO CORREIO ELETRÔNICO 

Sempre verifique a procedência de e-mails em nome de bancos, provedores de serviços, lojas, órgãos públicos, etc. observando o cabeçalho e o conteúdo completo da mensagem. Nunca saia clicando de imediato em links e anexo da mensagem. Verifique se o remetente é mesmo quem diz ser.

Caso desconfie de alguma mensagem, consulte o Catálogo de Fraudes da Rede Nacional de Pesquisa (https://catalogodefraudes.rnp.br/) que tem como objetivo conscientizar a comunidade sobre os principais golpes que estão em circulação na internet, identificando e divulgando fraudes reportadas pela comunidade ou coletadas por seus sensores.

Mesmo que tenha utilizado o antivírus, evite abrir arquivos enviados por fontes não confiáveis.

Desconfie sempre de arquivos executáveis recebidos, mesmo vindos de fontes confiáveis. Eles podem vir mascarados com extensão compactada (.zip, .rar, .gz, ...).

Verifique a veracidade das informações e use sempre seu bom senso antes de repassar a mensagem.

Desconfie de links e arquivos anexados à mensagem mesmo que tenham sido enviados por pessoas ou instituições conhecidas (pode ser uma conta de email invadida que está sendo utilizada para aplicar golpes).

Antes de abrir um arquivo anexado à mensagem tenha certeza de que ele não apresenta riscos, verificando-o com ferramentas antivírus.

Seja cuidadoso ao acessar a página do seu webmail para não ser vítima de golpe (phishing).

NÍVEIS DE ACESSO NO SEI

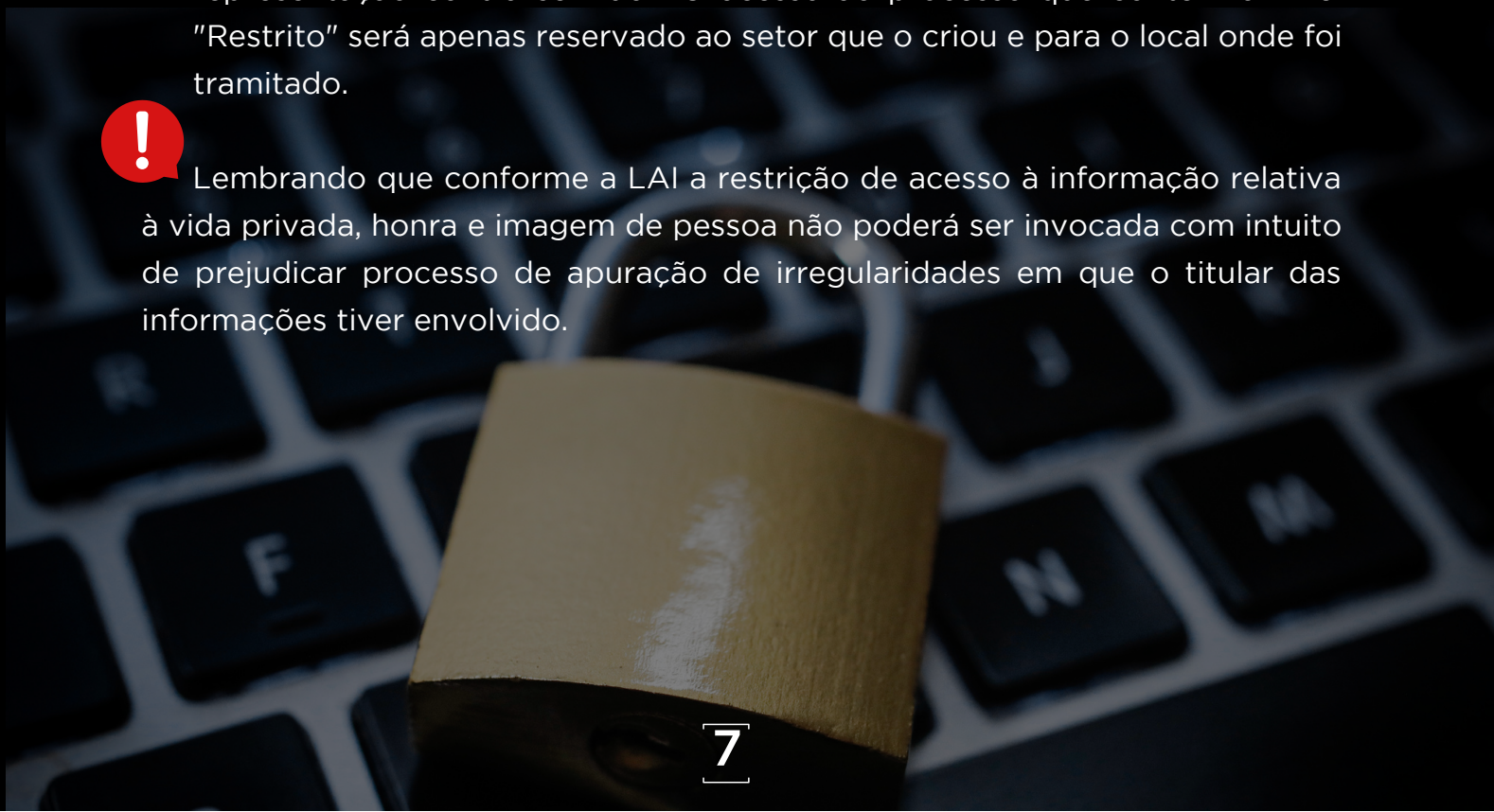
A fim de fazer cumprir a principal diretriz da Lei de Acesso à Informação - LAI 12.527, que é a publicidade e a transparência das informações, orientamos que, em regra, o nível de acesso seja sempre público para o Memorando, Memorando-Circular, Ofícil e Ofício-Circular.

Documentos com caráter informativo devem ter o nível de acesso público. Com o propósito de elucidar quais assuntos possuem restrição de acesso, vejamos:

- Documentos sigilosos: Informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para segurança da sociedade e do Estado, e aquelas abrangidas pelas demais hipóteses legais do sigilo.

- Documentos restritos: São aqueles que contêm informações pessoais e funcionais com respeito à intimidade, vida privada, honra e imagem, prevenção e diagnóstico médico, apuração de responsabilidade e representação contra servidor. O acesso ao processo que contém o nível "Restrito" será apenas reservado ao setor que o criou e para o local onde foi tramitado.

Lembrando que conforme a LAI a restrição de acesso à informação relativa à vida privada, honra e imagem de pessoa não poderá ser invocada com intuito de prejudicar processo de apuração de irregularidades em que o titular das informações tiver envolvido.



QUANDO E COMO ACIONAR O DPO

Qualquer comunicação e solicitação relativa ao tratamento de dados pessoais devem ser encaminhadas pelos titulares dos dados diretamente ao DPO, pelo endereço eletrônico.

epd@pge.ro.gov.br

PROCURADORIA GERAL DO ESTADO
RONDÔNIA

PGE·RO

https://pge.ro.gov.br/