GOVERNO DO ESTADO DE RONDÔNIA
Controladoria Geral do Estado - CGE

Ofício nº 1684/2023/CGE-CGPD

Aos Órgãos e Entidades do Poder Executivo Estadual

Assunto: **Renovação do acesso às Normas ABNT NBR ISO/IEC para a Rede de Encarregados.**

Senhores Encarregados/DPOs,

1. Com nossos cordiais cumprimentos, **considerando** o disposto na **Lei Federal nº 13.709, de 14 de agosto de 2018**, Lei Geral de Proteção de Dados Pessoais - LGPD, bem como no **Decreto Estadual nº 26.451, de 4 de outubro de 2021**, que dispõe sobre a adoção de medidas para aplicação da LGPD e criação do CGPD no âmbito da Administração Pública Estadual Direta, Autárquica e Fundacional no Poder Executivo do Estado de Rondônia.

2. **Considerando** que este Comitê LGPD tem por objetivo estabelecer o conjunto de regras de boas práticas e de governança, diretrizes, políticas, projetos, ações e metas estratégicas a serem observadas pelos órgãos do Poder Executivo Estadual às disposições da LGPD, inteligência do *caput* do art. 14 do Decreto Estadual nº 26.451/2021.

3. Considerando o Ofício ID SEI nº 0033890222 deste CGPD que informou sobre a disponibilização do acesso para a Rede de Encarregados das Normas ABNT NBR ISO/IEC, ação promovida pela Superintendência Estadual de Tecnologia da Informação e Comunicação - SETIC.

4. Neste expediente, trazemos a informação de que **a SETIC renovou a licença para acesso às Normas ABNT NBR ISO/IEC**, por meio de Termo Aditivo ao Contrato nº 0385/SETIC/PGE/2022 (ID SEI nº 0037875924), disponível por intermédio da Plataforma Target GedWeb (https://www.gedweb.com.br/setic/), e a pedido deste Comitê LGPD, disponibilizou **para a Rede de Encarregados do Governo do Estado**.

5. As referidas normas trazem orientações quanto a requisitos e aplicação de boas práticas sobre diversas temáticas, incluindo segurança e privacidade, temas importantes para a adequação dos órgãos e entidades à LGPD, sendo indicada para a Rede de Encarregados a leitura e aplicação, no que couber, das seguintes:

Norma	Título	Descrição
NBR ISO/IEC 27001	Tecnologia da Informação - Técnicas de Segurança - Sistemas de gestão da segurança da informação - Requisitos.	Especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização. Também inclui requisitos para a avaliação e tratamento de riscos de segurança da informação voltados para as necessidades da organização.
NBR ISO/IEC 27002	Tecnologia da Informação - Técnicas de Segurança - Código de prática para controles de segurança da informação.	Fornece um conjunto de referência de controles genéricos de segurança da informação, incluindo orientação para implementação.

NBR ISO/IEC 27005	Segurança da informação, segurança cibernética e proteção à privacidade — Orientações para gestão de riscos de segurança da informação.	Este documento fornece orientações para ajudar as organizações a: cumprir os requisitos da NBRISO/IEC27001 em relação às ações para abordar riscos de segurança da informação; realizar atividades de gestão de riscos de segurança da informação, especificamente avaliação e tratamento de riscos de segurança da informação.
NBR ISO/IEC 27007	Segurança da Informação, segurança cibernética e proteção da privacidade - Diretrizes para auditoria de sistemas de gestão da segurança da informação	Fornece orientações sobre como gerenciar um programa de auditoria de sistemas de gestão da segurança da informação (SGSI), como executar as auditorias e a competência dos auditores de SGSI, em complemento às orientações descritas na NBRISO19011.
NBR ISO/IEC 27701	Técnicas de Segurança - Extensão da NBR ISO/IEC 27001 e NBR ISO/IEC 27002 para gestão da privacidade da informação - Requisitos e diretrizes.	Especifica os requisitos e fornece as diretrizes para o estabelecimento, implementação, manutenção e melhoria contínua de um Sistema de Gestão de Privacidade da Informação (SGPI) na forma de uma extensão das NBRISO/IEC27001 e NBRISO/IEC27002 para a gestão da privacidade dentro do contexto da organização.
NBR ISO/IEC 29100	Tecnologia da Informação - Técnicas de Segurança - Estrutura de Privacidade.	Fornece uma estrutura de privacidade que: especifica uma terminologia comum de privacidade; especifica os atores e os seus papéis no tratamento de dados pessoais (DP); descreve considerações de salvaguarda de privacidade; e fornece referências para princípios conhecidos de privacidade para tecnologia da informação.
NBR ISO/IEC 29134	Tecnologia da Informação - Técnicas de segurança - Avaliação de impacto de privacidade - Diretrizes.	Fornece diretrizes para: processos de avaliação de impacto de privacidade, e estrutura e conteúdo de relatório de PIA.
NBR ISO/IEC 29151	Tecnologia da Informação - Técnicas de Segurança - Código de prática para proteção de dados pessoais.	Estabelece objetivos de controle, controles e diretrizes para implementar controles, para atender aos requisitos identificados por uma avaliação de risco e impacto relacionado à proteção de dados pessoais (DP).
NBR ISO/IEC 29184	Aviso de privacidade *online* e consentimento.	Especifica os controles que formatam o conteúdo e a estrutura dos avisos de privacidade on-line, bem como o processo de solicitação de consentimento para coletar e tratar dados pessoais (DP) de titulares de DP.

6. **No mais, esclarecemos que:**

a) as normas elencadas no quadro acima são apenas referências indicativas, devendo os Encarregados/DPOs se aterem a outras que forem pertinentes;

b) o acesso à Plataforma somente será concedido aos Encarregados/DPOs formalmente designados/nomeados por meio de instrumento oficial;

c) tal acesso depende de prévio credenciamento, cuja solicitação deverá ser realizada pelo próprio Encarregado/DPO por meio da Central de Atendimento da SETIC (https://atendimento.setic.ro.gov.br/plugins/formcreator/front/formdisplay.php?id=493), devendo, o próprio Encarregado/DPO, apresentar o ato normativo de nomeação/indicação e indicar seu *e-mail* institucional, cujo domínio deverá ser **<sigla_orgao>@lgpd.ro.gov.br** (caso não possua, deverá providenciar por meio da Central de Atendimento), conforme art. 5º da Instrução Normativa nº 3/2022/CGPD;

d) o contrato do serviço de acesso às normas ficará **disponível até 23/06/2024**; e

e) as credenciais de acesso são de inteira responsabilidade do Encarregado/DPO, não podendo divulgá-las, emprestá-las ou fornecê-las a terceiros.

7. **Considerando os apontamentos alhures, solicitamos que este expediente seja levado ao conhecimento dos encarregados pelo tratamento de dados pessoais/DPOs.**

Sem mais,

Cordialmente.

TIAGO LOPES DE AGUIAR
Coordenador do Comitê Gestor de Privacidade e Proteção de Dados Pessoais - CGPD
Decreto nº 27.032/2022/RO

Documento assinado eletronicamente por **TIAGO LOPES DE AGUIAR**, **Coordenador(a)**, em 27/06/2023, às 14:05, conforme horário oficial de Brasília, com fundamento no artigo 18 caput e seus §§ 1º e 2º, do Decreto nº 21.794, de 5 Abril de 2017.

A autenticidade deste documento pode ser conferida no site portal do SEI, informando o código verificador **0039134266** e o código CRC **9352EFF9**.

Referência: Caso responda este Ofício, indicar expressamente o Processo nº 0007.000735/2023-78 SEI nº 0039134266