Diretor-Geral

ATOS DA PRESIDÊNCIA

PORTARIAS

PORTARIA PRES Nº 440, DE 16 DE DEZEMBRO DE 2025

PUBLICAÇÃO EM : 19/12/2025

Disciplina os modelos de formulários de comunicação de incidentes de segurança envolvendo dados pessoais sensíveis, conforme definidos nos termos da Lei Geral de Proteção de Dados, a serem utilizados pelas unidades administrativas do Tribunal Regional Eleitoral de Goiás.

O Presidente do Tribunal Regional Eleitoral de Goiás, no uso de suas atribuições legais e regimentais e considerando a instrução do Processo SEI nº 25.0.000009515-2, resolve:

Art. 1º Aprovar os modelos de formulários previstos nos Anexos I e II desta Portaria, destinados, respectivamente, à comunicação de incidentes de segurança à Autoridade Nacional de Proteção de Dados (ANPD) e ao titular dos dados pessoais.

Art. 2º Esta Portaria entra em vigor na data de sua publicação.

Desembargador Luiz Cláudio Veiga Braga

Presidente

ANEXO I

	Formulário de Comunicação de Incidente de Segurança com Dados Pessoais

Dados do Controlador				
Razão Social / Nome:				
CNPJ/CPF:				
Endereço:				
Cidade:		Estado:		
CEP:				
Telefone:		E-mail:		
Declara ser Microempresa ou Empresa de Pequeno Porte:			¿ Sim	¿ Não
Declara ser Agente de Tratamento de Pequeno Porte[1]:			¿ Sim	¿ Não
Informe o número aproximado de titulares cujos dados são tratados por sua organização:				
Dados do Encarregado				
Possui um encarregado pela proteção de dados pessoais?			¿ Sim	¿ Não
Nome:				
CNPJ/CPF:				
Telefone:		E-mail:		
Dados do Notificante / Representante Legal				
¿ O próprio encarregado pela proteção de dados.				
¿ Outros (especifique):				

Nome:	
CNPJ/CPF:	
Telefone:	
E-mail:	
A documentação comprobatória da legitimidade para representação do controlador junto à ANPD deve ser protocolada em conjunto com o formulário de comunicação de incidente. · *Encarregado*: ato de designação/nomeação/procuração. · *Representante*: contrato social e procuração, se cabível.	

Tipo de Comunicação	
¿ Completa	*Todas as informações a respeito do incidente estão disponíveis e a comunicação aos titulares já foi realizada.*
¿ Preliminar	*Nem todas as informações sobre o incidente estão disponíveis, justificadamente, ou a comunicação aos titulares ainda não foi realizada.* *A complementação deverá ser encaminhada em até 30 dias corridos da comunicação preliminar.*
¿ Complementar	*Complementação de informações prestadas em comunicação preliminar.*

A comunicação complementar deve ser protocolada no mesmo processo que a comunicação preliminar.

Ø A comunicação preliminar é insuficiente para o cumprimento da obrigação estabelecida pelo art. 48 da LGPD e deve ser complementada pelo controlador no prazo estabelecido.

Avaliação do Risco do Incidente

¿ O incidente de segurança pode acarretar risco ou dano relevante aos titulares.

¿ O incidente não acarretou risco ou dano relevante aos titulares. (Comunicação Complementar)

¿ O risco do incidente aos titulares ainda está sendo apurado. (Comunicação Preliminar)

Justifique, se cabível, a avaliação do risco do incidente:

Da Ciência da Ocorrência do Incidente

Por qual meio se tomou conhecimento do incidente?

¿ Identificado pelo próprio controlador.	¿ Notificação do operador de dados.	¿ Denúncia de titulares/terceiros.
¿ Notícias ou redes sociais.	¿ Notificação da ANPD.	¿ Outros. (especifique)

Descreva, resumidamente, de que forma a ocorrência do incidente foi conhecida:

Caso o incidente tenha sido comunicado ao controlador por um operador, informe:

Dados do Operador

Razão Social / Nome:	
CNPJ/CPF:	
E-mail:	

Cabe ao controlador solicitar ao operador as informações necessárias à comunicação do incidente.

Da Tempestividade da Comunicação do Incidente

Informe as seguintes datas, sobre o incidente:	
Quando ocorreu	
Quando tomou ciência	
Quando comunicou à ANPD	
Quando comunicou aos titulares	
Justifique, se cabível, a não realização da comunicação completa à ANPD e aos titulares de dados afetados no prazo sugerido de 2 (dois) dias úteis após a ciência do incidente:	
Se cabível, informe quando e a quais outras autoridades o incidente foi comunicado:	
Da Comunicação do Incidente aos Titulares dos Dados	
Os titulares dos dados afetados foram comunicados sobre o incidente?	
¿ Sim.	¿ Não, por não haver risco ou dano relevante a eles.
¿ Não, mas o processo de comunicação está em andamento.	¿ Não, vez que o risco do incidente ainda está sendo apurado. (comunicação preliminar)
Se cabível, quando os titulares serão comunicados sobre o incidente?	
De que forma a ocorrência do incidente foi comunicada aos titulares?	
¿ Comunicado individual por escrito. *(mensagem eletrônica / carta / e-mail / etc.)*	¿ Anúncio público no sítio eletrônico, mídias sociais ou aplicativos do controlador.
¿ Comunicado individual por escrito com confirmação de recebimento. *(mensagem eletrônica / carta / e-mail / etc.)*	¿ Ampla divulgação do fato em meios de comunicação, por iniciativa do controlador. (*especifique abaixo*)
¿ Outros. (*especifique abaixo*)	¿ Não se aplica.
Descreva como ocorreu a comunicação:	
Quantos titulares foram comunicados individualmente sobre o incidente?	
Justifique, se cabível, o que motivou a não realização da comunicação individual aos titulares:	
O comunicado aos titulares deve utilizar linguagem clara e conter, ao menos, as seguintes informações: 1. resumo e data de ocorrência do incidente; 2. descrição dos dados pessoais afetados; 3. riscos e consequências aos titulares de dados; 4. medidas tomadas e recomendadas par mitigar seus efeitos, se cabíveis; 5. dados de contato do controlador para obtenção de informações adicionais sobre o incidente.	
O comunicado aos titulares atendeu os requisitos acima?	
¿ Sim	¿ Não
Ø Se não atendidos os requisitos, o comunicado aos titulares deverá ser devidamente retificado. Ø Poderá ser solicitada pela ANPD, a qualquer tempo, cópia do comunicado aos titulares para fins de fiscalização.	

Descrição do Incidente	
Qual o tipo de incidente? (Informe o tipo mais específico)	
¿ Sequestro de Dados (*ransomware*) sem transferência de informações.	¿ Sequestro de dados (*ransomware*) com transferência e/ou publicação de informações.
¿ Exploração de vulnerabilidade em sistemas de informação.	¿ Vírus de Computador / *Malware*.
¿ Roubo de credenciais / Engenharia Social.	¿ Violação de credencial por força bruta.
¿ Publicação não intencional de dados pessoais.	¿ Divulgação indevida de dados pessoais.
¿ Envio de dados a destinatário incorreto.	¿ Acesso não autorizado a sistemas de informação.
¿ Negação de Serviço (DoS).	¿ Alteração/exclusão não autorizada de dados.
¿ Perda/roubo de documentos ou dispositivos eletrônicos.	¿ Descarte incorreto de documentos ou dispositivos eletrônicos.
¿ Falha em equipamento (hardware).	¿ Falha em sistema de informação (*software*).
¿ Outro tipo de incidente cibernético. (especifique abaixo)	¿ Outro tipo de incidente não cibernético. (especifique abaixo)
Descreva, resumidamente, como ocorreu o incidente:	
Explique, resumidamente, por que o incidente ocorreu (identifique a causa raiz, se conhecida):	
Que medidas foram adotadas para corrigir as causas do incidente?	
Impactos do Incidente Sobre os Dados Pessoais	
De que forma o incidente afetou os dados pessoais (admite mais de uma marcação):	
¿ Confidencialidade	Houve acesso não autorizado aos dados, violando seu sigilo.
¿ Integridade	Houve alteração ou destruição de dados de maneira não autorizada ou acidental.
¿ Disponibilidade	Houve perda ou dificuldade de acesso aos dados por período significativo.
Se aplicável, quais os tipos de dados pessoais sensíveis foram violados? (admite mais de uma marcação)	

¿Origem racial ou étnica.	¿Convicção religiosa.	¿Opinião política.
¿Referente à saúde.	¿Biométrico.	¿Genético.
¿Referente à vida sexual.	¿Filiação a organização sindical, religiosa, filosófica ou política.	

Se aplicável, descreva os tipos de dados pessoais sensíveis violados:		
Quais os demais tipos de dados pessoais violados? (admite mais de uma marcação)		
¿ Dados básicos de identificação *(ex: nome, sobrenome, data de nascimento, matrícula)*	¿ Número de documentos de identificação oficial. *(ex: RG, CPF, CNH, passaporte)*	¿ Dados de contato. (*ex: telefone, endereço, e-mail*)

¿ Dados de meios de pagamento. *(ex: cartão de crédito/débito)*	¿ Cópias de documentos de identificação oficial.	¿ Dados protegidos por sigilo profissional/legal.
¿ Dado financeiro ou econômico.	¿ Nomes de usuário de sistemas de informação.	¿ Dado de autenticação de sistema. (*ex: senhas, PIN ou tokens)*
¿ Imagens / Áudio / Vídeo	¿ Dado de geolocalização. *(ex: coordenadas geográficas)*	¿ Outros (especifique abaixo)

Descreva os tipos de dados pessoais não sensíveis violados:

Riscos e Consequências aos Titulares dos Dados

Foi elaborado um Relatório de Impacto à Proteção de Dados Pessoais (RIPD) das atividades de tratamento afetadas pelo incidente?

¿ Sim	¿ Não

Qual o número total de titulares cujos dados são tratados nas atividades afetadas pelo incidente?

Qual a quantidade aproximada de titulares afetados[2] pelo incidente?

Total de titulares afetados	
Crianças e/ou adolescentes	
Outros titulares vulneráveis	

Se aplicável, descreva as categorias de titulares vulneráveis afetados:

Quais a categorias de titulares foram afetadas pelo incidente? (admite mais de uma marcação)

¿ Funcionários.	¿Prestadores de serviços.	¿ Estudantes/Alunos.
¿ Clientes/Cidadãos.	¿ Usuários.	¿ Inscritos/Filiados.
¿ Pacientes de serviço de saúde.	¿Ainda não identificadas.	¿ Outros. (especifique abaixo)

Informe o quantitativo de titulares afetados, por categoria:

Quais as prováveis consequências do incidente para os titulares? (admite mais de uma marcação)

¿ Danos morais.	¿ Danos materiais.	¿ Violação à integridade física
¿ Discriminação social.	¿ Danos reputacionais.	¿ Roubo de identidade.
¿ Engenharia social / Fraudes.	¿ Limitação de acesso a um serviço.	¿ Exposição de dados protegidos por sigilo profissional/legal.
¿ Restrições de direitos.	¿ Perda de acesso a dados pessoais.	¿ Outros (especifique abaixo).

Se cabível, descreva as prováveis consequências do incidente para cada grupo de titulares:

Qual o provável impacto do incidente sobre os titulares? (admite só uma marcação)

¿ Podem não sofrer danos, sofrer danos negligenciáveis ou superáveis sem dificuldade.

¿ Podem sofrer danos, superáveis com certa dificuldade.		
¿ Podem sofrer danos importantes, superáveis com muita dificuldade.		
¿ Podem sofrer lesão ou ofensa a direitos ou interesses difusos, coletivos ou individuais, que, dadas as circunstâncias, ocasionam ou tem potencial para ocasionar dano significativo ou irreversível.		
Se cabível, quais medidas foram adotadas para mitigação dos riscos causados pelo incidente aos titulares?		
Medidas de Segurança Técnicas e Administrativas para a Proteção dos Dados Pessoais		
Os dados violados estavam protegidos de forma a impossibilitar a identificação de seus titulares?		
¿ Sim, integralmente protegidos por criptografia / pseudonimização.	¿ Sim, parcialmente protegidos por criptografia / pseudonimização.	¿ Não.
Descreva os meios utilizados para proteger a identidade dos titulares, e a quais tipos dados foram aplicados:		
Antes do incidente, quais das seguintes medidas de segurança eram adotadas? (admite mais de uma marcação)		
¿ Políticas de segurança da informação e privacidade.	¿ Processo de Gestão de Riscos.	¿ Registro de incidentes.
¿ Controle de acesso físico.	¿ Controle de acesso lógico.	¿ Segregação de rede.
¿ Criptografia/Anonimização.	¿ Cópias de segurança. (*backups*)	¿ Gestão de ativos.
¿ Antivírus.	¿ Firewall.	¿ Atualização de Sistemas.
¿ Registros de acesso (logs).	¿ Monitoramento de uso de rede e sistemas.	¿ Múltiplos fatores de autenticação.
¿ Testes de invasão.	¿ Plano de resposta a incidentes.	¿ Outras (especifique).
Descreva as demais medidas de segurança técnicas e administrativas adotadas antes do incidente:		
Após o incidente, foi adotada alguma nova medida de segurança? (admite mais de uma marcação)		
¿ Políticas de segurança da informação e privacidade.	¿ Processo de Gestão de Riscos.	¿ Registro de incidentes.
¿ Controle de acesso físico.	¿ Controle de acesso lógico.	¿ Segregação de rede.
¿ Criptografia/Anonimização.	¿ Cópias de segurança. (*backups*)	¿ Gestão de ativos.
¿ Antivírus.	¿ Firewall.	¿ Atualização de Sistemas.
¿ Registros de acesso (logs).	¿ Monitoramento de uso de rede e sistemas.	¿ Múltiplos fatores de autenticação.
¿ Testes de invasão.	¿ Plano de resposta a incidentes.	¿ Outras (especifique).
Se cabível, descreva as medidas de segurança adicionais adotadas após o incidente:		
As atividades de tratamento de dados afetadas estão submetidas a regulações de segurança setoriais?		
¿ Sim	¿ Não	

Se cabível, indique as regulamentações setoriais de segurança aplicáveis às atividades de tratamento de dados afetadas pelo incidente:

Declaro, sob as penas da lei, serem verdadeiras as informações prestadas acima.
<ASSINATURA>
[1] Nos termos do REGULAMENTO DE APLICAÇÃO DA LEI Nº 13.709, DE 14 DE AGOSTO DE 2018, aprovado pela RESOLUÇÃO CD/ANPD Nº 2, DE 27 DE JANEIRO DE 2022. (https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019)
[2] Titular afetado é aquele cujos dados podem ter tido a confidencialidade, integridade ou disponibilidade violadas e que ficará exposto a novos riscos relevantes em razão do incidente.
ANEXO II
ASSUNTO: Informação Importante: Incidente de Segurança com Seus Dados Pessoais
PARA: (Nome Completo do Cidadão(ã))
CONTATO: Endereço residencial, E-mail ou Telefone
Prezado(a) (Nome do Cidadão(ã)),
¿¿ Identificamos um incidente de segurança que pode ter afetado seus dados pessoais. Nossa prioridade é proteger a sua privacidade, e por isso estamos avisando você e adotando medidas imediatas para conter o ocorrido.
¿ O que aconteceu?
No dia XX/XX/XXXX, detectamos um(a) (descrever o tipo de incidente). Assim que identificamos o problema:
- ¿¿ bloqueamos o acesso indevido
- ¿¿¿ reforçamos a segurança dos sistemas
- ¿¿ iniciamos investigação detalhada
- ¿¿ notificamos as autoridades competentes
¿¿ Quais dados foram afetados?
As informações que podem ter sido expostas incluem:
- nome completo
- CPF
- e-mail
- telefone
- endereço
- (outras categorias)
¿¿ Quais são os riscos para você?
Existe a possibilidade de:
- tentativas de golpes
- contatos indesejados
- uso indevido da identidade
¿¿ Importante: O Tribunal Regional Eleitoral de Goiás nunca solicita seus dados pessoais por telefone, e-mail ou redes sociais.
O que estamos fazendo?
¿¿¿ O que estamos fazendo para resolver?
Além das medidas já existentes, adotamos providências adicionais:
- ¿¿ reforçamos a segurança dos sistemas
- ¿¿ seguimos monitorando eventuais tentativas de acesso
- ¿¿ cumprimos protocolos legais
¿¿ O que você pode fazer?

Recomendamos que você:
- tenha atenção a contatos suspeitos
- não compartilhe dados sem confirmar a origem
- relate qualquer situação incomum
¿¿ Onde obter mais informações?
A Ouvidoria Regional Eleitoral do TRE-GO, que atua como Unidade Encarregada de Proteção de Dados Pessoais, está à disposição para esclarecer dúvidas sobre este incidente e sobre seus direitos:
¿¿ ouvidoria@tre-go.jus.br
¿¿ (62) 3920-4340 / 3920-4341
¿¿ https://www.tre-go.jus.br/institucional/ouvidoria/ouvidoria
Informamos, ainda, que notificamos a Autoridade Nacional de Proteção de Dados (ANPD) sobre o incidente. Saiba mais sobre seus direitos: http://www.gov.br/anpd/pt-br.
(Se houve atraso na comunicação, incluir este parágrafo, explicando de forma simples:) Atenção: Se esta mensagem não chegou imediatamente, foi porque (explicar o motivo de forma simples, por exemplo: "precisamos de tempo para investigar a fundo o que aconteceu e ter certeza das informações antes de avisar você").
Agradecemos sua compreensão e mantemos nosso compromisso com a segurança e a proteção de seus dados.
Atenciosamente,
Tribunal Regional Eleitoral de Goiás, xx/xx/xxxx

PORTARIA PRES Nº 443, DE 18 DE DEZEMBRO DE 2025

PUBLICAÇÃO EM : 19/12/2025

Fixa o expediente da Justiça Eleitoral em Goiás no mês de janeiro de 2026.
O PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DE GOIÁS, no uso das atribuições legais e regimentais, e, considerando o dispostos nos artigos 220, *caput* (CPC), 3º, *caput* (Resolução CNJ nº 244/2016) e 10 (Resolução TSE nº 23.478/2016),
RESOLVE:
Art. 1º DETERMINAR que o expediente na Secretaria do Tribunal e nos Cartórios Eleitorais, durante o período de 7 a 20 de janeiro de 2026, seja das 13h às 18h.
Art. 2º Caberão à Secretaria de Comunicação Social e Cerimonial, às Juízas e aos Juízes Eleitorais divulgar o contido no artigo 1º.
Art. 3º Esta Portaria entra em vigor na data da publicação.
Desembargador Luiz Cláudio Veiga Braga
Presidente do TRE-GO

ATOS DA SECRETARIA DE ADMINISTRAÇÃO E ORÇAMENTO

EXTRATO

DOAÇÃO DE VEÍCULOS

PUBLICAÇÃO EM : 19/12/2025

EXTRATOS DE TERMO DE TRANSFERÊNCIA DE BENS - TRE/GO - Espécie: Termo de Transferência de Bens. N.º Processo SEI 25.0.000016433-2. Termo de Transferência de Bens celebrado pela União, por intermédio do TRIBUNAL REGIONAL ELEITORAL DE GOIÁS (TRE/GO)