

Anexo IV do Termo de Referência – Gestão da Segurança e Privacidade - Requisitos e Obrigações

Em atenção aos tópicos “Requisitos gerais de estruturação de segurança e privacidade” e “Requisitos de Segurança da Informação e Privacidade – SIP” do Termo de Referência, a Contratada deverá cumprir as regras mencionadas a seguir, estão sujeita às sanções indicadas, no caso da inobservância dos procedimentos requeridos.

1. No que diz respeito ao acesso e tratamento de informações disponibilizadas pela ANEEL por força dos procedimentos necessários para a execução do contrato, o Contratado deverá atuar de acordo com o que dispõem a Lei nº 12.527, de 18 de novembro de 2011, Lei nº 13.709, de 14 de agosto de 2018, Lei nº 14.133, de 1º de abril de 2021, Decreto nº 7.724, de 16 de maio de 2012, Decreto nº 7.845, de 14 de novembro de 2012, Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, normas da ANEEL (Norma de Organização nº 01/2006-ANEEL/ANP/CPRM e outras, disponíveis em <https://www.gov.br/aneel/pt-br/centrais-de-conteudos/normas-internas-de-organizacao>), e demais normativos relativos à segurança da informação e privacidade, vigentes ou que venham a ser implantados, tanto no âmbito da Contratante quanto da Administração Pública Federal.
2. O Contratado deverá implementar e manter controles e procedimentos específicos para assegurar completo e absoluto sigilo quanto a todos os dados e informações de que o preposto, seus empregados e outros profissionais sob sua direção e/ou controle venham a tomar conhecimento em razão da execução do contrato, de forma a assegurar o uso dos dados somente para as finalidades previstas em contrato e as restrições de uso dos ativos utilizados para desenvolvimento e/ou operação da Solução de TIC, cumprindo e fazendo cumprir o disposto no Termo de Compromisso e Manutenção de Sigilo firmado conforme o respectivo anexo do Termo de Referência.
3. O Contratado se compromete a manter sigilo e confidencialidade de todas as informações – em especial os dados pessoais e os dados pessoais sensíveis eventualmente repassados em decorrência da execução contratual, em consonância com o disposto na Lei nº 13.709/2018, sendo vedado o repasse das informações a outras empresas ou pessoas, salvo aquelas decorrentes de obrigações legais ou para viabilizar o cumprimento do edital/instrumento contratual.
 - 3.1. A coleta de dados pessoais indispensáveis à própria prestação do serviço, se houver, será realizada mediante prévia e fundamentada aprovação da Contratante, responsabilizando-se o Contratado por obter o consentimento dos titulares (salvo nos casos em que opere outra hipótese legal de tratamento);
 - 3.2. Os dados assim coletados só poderão ser utilizados na execução dos serviços especificados neste contrato, e em hipótese alguma poderão ser compartilhados ou utilizados para outros fins, nos termos da Lei Federal nº 13.709/18.
 - 3.3. Fica vedado o tratamento de dados pessoais e/ou dados pessoais sensíveis de pessoas físicas vinculadas à Contratante, com o objetivo de obter vantagem econômica de qualquer espécie.
4. Em consonância com as demais especificações do Termo de Referência e da legislação, o Contratado deverá cumprir os requisitos listados abaixo; no caso de seu descumprimento, será aplicada multa, conforme especificado:

REQUISITOS GERAIS DE ESTRUTURAÇÃO DE SEGURANÇA E PRIVACIDADE		INFRAÇÃO	MULTA
Escala, natureza e finalidade do processamento contratado	Executar os serviços observando as seguintes especificações quanto à escala, natureza e finalidade do processamento contratado, conforme objeto desse termo de referência.	Não executar os serviços observando as especificações quanto à escala, natureza e finalidade do processamento contratado	Mensal de 5% (cinco por cento), sobre o valor da fatura mensal.

Segurança das Redes Corporativas	Implementar e manter controles e procedimentos específicos para assegurar o nível adequado de segurança da informação às redes corporativas da Contratante e da Contratada, de forma a reduzir o nível de risco ao qual a Solução de TIC e a contratante estão expostos, considerando os critérios de aceitabilidade de riscos definidos pela contratante; Implementar e manter, controles e procedimentos específicos de Segurança Web, nos servidores da aplicação, ou na própria aplicação, para garantir o nível adequado de segurança da informação e privacidade.	Não apresentar documentação que comprove estar em conformidade com nível adequado de segurança da informação às redes corporativas da Contratante e da Contratada.	Mensal de 1% (um por cento), sobre o valor da fatura mensal.
Política de Backup	Possuir e implementar, política de backup das informações e dos registros de log da solução contratada, em conformidade com os dispositivos legais aplicáveis, a ser homologada pela contratante, que assegure a manutenção de cópias de segurança de todos os componentes de software dos sistemas, de suas bases de dados e da documentação associada, observando a técnica, os cuidados requeridos para cada caso, de modo a ser possível a plena recuperação de versões dos sistemas e dados salvaguardados em caso de falha ou por solicitação da contratante, reduzindo o nível de risco ao qual o objeto do contrato e/ou a contratante está exposta, considerando os critérios de aceitabilidade de riscos definidos pela contratante.	Não apresentar documentação referente a política de backup.	Mensal de 1% (um por cento), sobre o valor da fatura mensal.
REQUISITOS DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE ESPECÍFICOS DA SOLUÇÃO DE TIC		INFRAÇÃO	MULTA
Controle de Acesso	Implementar controles de acesso baseados em uma política de controle de acesso para o objeto contratado, elaborada pela contratante em conjunto com a contratada, tendo em vista o princípio do menor privilégio, a segurança da informação e a privacidade, de forma a reduzir o nível de risco ao qual o objeto e a contratante estão expostos, considerando os critérios de aceitabilidade de riscos definidos pela contratante. A política deve estabelecer, dentre outros	Não apresentar documento probatório que evidencie as políticas e controles de acesso.	Mensal de 1% (um por cento), sobre o valor da fatura mensal

	critérios, que se deve conceder autorizações de acesso apenas quando realmente sejam necessárias para o desempenho de uma atividade específica, definindo também protocolos para cadastramento, mecanismo de controle de acesso (como, por exemplo, validação de formulário), habilitação, inabilitação, atualização de direitos de acesso e exclusão de usuário, além de revisões periódicas da política. A política também deve definir situações e protocolos para acesso à informações sensíveis, necessidades de não repúdio, situações que requerem autenticação via duplo fator e acesso via certificado digital, nos casos em que a contratante julgar necessário.		
Registro de Eventos e Incidentes de Segurança	Implementar os controles necessários para o registro de eventos e incidentes de segurança da informação e privacidade.	Não apresentar documentos de comprovação de registros de eventos e incidentes.	Mensal de 1% (um por cento), sobre o valor da fatura mensal
Registro de Eventos e Rastreabilidade	Implementar e manter controles específicos para registro de eventos e rastreabilidade de forma a manter trilha de auditoria de segurança da informação e privacidade, aderente a disposto em dispositivo legal correlato publicado pelo GSI/PR, de forma a assegurar a rastreabilidade das ações de usuário por meio de logs de transações e de acesso aos sistemas, conforme especificação de requisitos, e gerá-los e disponibilizá-los à contratante para fins de auditorias e inspeções.	Não apresentar documentos de comprovação de registros de eventos e rastreabilidade.	Mensal de 1% (um por cento), sobre o valor da fatura mensal
Identificação da operação	Implementar dispositivo que possibilite todas as operações de processamento realizadas com dados pessoais serem registradas de modo a identificar a operação realizada, quem realizou, data e hora.	Não apresentar documentos de comprovação de registro de identificação, data e hora de operação.	Mensal de 1% (um por cento), sobre o valor da fatura mensal
Salvaguarda de Logs	Implementar medidas de salvaguarda para os logs descritos, bem como controles específicos para registro das atividades dos administradores e operadores dos sistemas relacionados ao objeto do contrato, de forma que esses não tenham permissão de exclusão ou desativação dos registros (log) de suas próprias atividades.	Não apresentar comprovação de salvaguarda de logs e registro das atividades de administradores e operadores.	Mensal de 1% (um por cento), sobre o valor da fatura mensal

Compartilhamento, uso e proteção da Informação	Implementar procedimentos e controles adequados para compartilhamento, uso e proteção da informação; os casos de compartilhamento de informações com terceiro devem ser avaliados pela contratante, por intermédio da autoridade competente, a qual caberá autorizar a divulgação do mínimo de informações necessárias para cada compartilhamento, caso julgue apropriado, preservados os casos de sigilo previstos na legislação aplicável e de proteção de dados pessoais disposto pela Lei nº 13.709/2018.	Não apresentar documentos de comprovação de procedimentos e controles adequados para compartilhamento, uso e proteção da informação.	Mensal de 1% (um por cento), sobre o valor da fatura mensal
Análise de Vulnerabilidades	Executar periodicamente análise de vulnerabilidades na Solução de TIC, para detecção de vulnerabilidades técnicas e execução de medidas para seu saneamento ou contenção.	Não apresentar documentos de comprovação de procedimentos periódicos de análise de vulnerabilidades	Mensal de 5% (cinco por cento), sobre o valor da fatura mensal.
DEMAIS OBRIGAÇÕES DE RESPONSABILIDADE DA CONTRATADA		INFRAÇÃO	MULTA
Recursos em Versões Comprovadamente Seguras e Atualizadas	Utilizar recursos de segurança da informação e de tecnologia da informação de qualidade, eficiência e eficácia reconhecidas e em versões comprovadamente seguras e atualizadas, de forma reduzir o nível de risco ao qual o objeto do contrato e/ou a contratante está exposta, considerando os critérios de aceitabilidade de riscos definidos pela contratante.	Não utilizar recursos de segurança da informação e de tecnologia da informação nos moldes exigidos.	Mensal de 5% (cinco por cento), sobre o valor da fatura mensal.
Reportar Incidentes	Reportar de imediato à contratante incidentes que envolvam vazamento de dados, indisponibilidade ou comprometimento da informação relacionados à Solução de TIC.	Não reportar incidentes que envolvam vazamento de dados, indisponibilidade ou comprometimento da informação relacionados à Solução de TIC.	Mensal de 1% (um por cento), sobre o valor da fatura mensal
Termo de Compromisso e Ciência	Cumprir e fazer cumprir o disposto nos Termo de Compromisso e Termo(s) de Ciência firmados pelo representante legal e pelo(s) empregado(s) da contratada	Não apresentar Termos de Compromisso e Ciência firmados	Mensal de 1% (um por cento), sobre o valor da fatura mensal
Notificar violação	Notificar o Controlador em caso de ocorrência de violação de dados pessoais, processamento não autorizado ou outro não cumprimento dos termos e condições contratuais.	Não notificar o Controlador nos casos estabelecidos.	Mensal de 1% (um por cento), sobre o valor da fatura mensal
Descarte Seguro	Definir e executar procedimento de descarte seguro dos dados pessoais ou	Não apresentar documentação de que a	Mensal de 1% (um por cento),

	sigilosos da contratante ao encerrar a execução do contrato.	Solução de TIC possui processamento que garante descarte seguro.	sobre o valor da fatura mensal
Revogação de Privilégios	Comunicar à contratante, de imediato, a ocorrência de transferência, remanejamento ou demissão de funcionário, para que seja providenciada a revogação de todos os privilégios de acesso aos sistemas, informações e recursos da contratante, porventura colocados à disposição para realização dos serviços contratados.	Não apresentar documentação sobre as providências de revogação de privilégios	Mensal de 1% (um por cento), sobre o valor da fatura mensal
Utilização de Serviços de Terceiros	Informar e obter a anuência do contratante sobre a utilização de serviços de terceiros (como Content Delivery Network, Youtube, Flickr etc.) para sustentar ou viabilizar o funcionamento da Solução de TIC. Impedir o tratamento de dados pessoais por subcontratados, exceto por aprovação do controlador	Não obter anuência da CONTRATANTE sobre a utilização de serviços de terceiros (como Content Delivery Network, Youtube, Flickr, etc.) para sustentar ou viabilizar o funcionamento da Solução de TIC.	Mensal de 1% (um por cento), sobre o valor da fatura mensal
Segurança Física e do Ambiente	Implementar e manter, em conjunto com a contratante, controles e procedimentos específicos para assegurar a segurança física e do ambiente de acesso às bases, informações, sistemas e demais ativos que compõem a Solução de TIC, de forma a prevenir qualquer tipo de ocorrência de evento de efeitos danosos ou prejudiciais ao funcionamento dos recursos de processamento das informações relacionadas à Solução de TIC, reduzindo assim o nível de risco ao qual o objeto do contrato e/ou a contratante estão expostos, considerando os critérios de aceitabilidade de riscos definidos pela contratante.	Não apresentar documentos que comprovem procedimentos de segurança física e do ambiente.	Mensal de 1% (um por cento), sobre o valor da fatura mensal
Auditabilidade	Apresentar à contratante, sempre que solicitado, toda e qualquer informação e documentação que comprovem a implementação dos requisitos de segurança da informação e privacidade especificados na contratação, de forma a assegurar a auditabilidade do objeto contratado, bem como demais dispositivos legais aplicáveis.	Não apresentar documentação que comprovem a implementação dos requisitos de segurança da informação e privacidade especificados na contratação.	Mensal de 1% (um por cento), sobre o valor da fatura mensal

Auditoria de segurança da informação e privacidade	Disponibilizar todos os recursos necessários para que a contratante, ou outra entidade por ela indicada, realize atividade continuada de auditoria de segurança da informação e privacidade relacionadas ao objeto do contrato.	Não disponibilizar recursos para auditoria de segurança da informação e privacidade relacionadas ao objeto do contrato.	Mensal de 1% (um por cento), sobre o valor da fatura mensal
Tratamento de incidentes de segurança da informação e privacidade	Realizar em conjunto com a contratante, ou com outros órgãos por ela indicados, ações de tratamento de incidentes de segurança da informação e privacidade relacionados ao objeto do contrato, bem como apoiar essas ações com o monitoramento e o envio de informações tempestivos.	Não realizar em conjunto com a contratante, ou com outros órgãos por ela indicados, ações de tratamento de incidentes de segurança da informação e privacidade relacionados ao objeto do contrato.	Mensal de 1% (um por cento), sobre o valor da fatura mensal
	Dispositivo que garanta uma política ou norma de proteção de dados pessoais que aborde a finalidade da contratada perante o processamento de dados; a transparência com Escala, natureza e finalidade do processamento Norma de proteção de dados pessoais Monitorar e auditar dados pessoais Treinamento e conscientização Requisitos de conformidade Atendimento de finalidade pública Dados limitados ao mínimo para tratamento Notificar violação Precisão dos dados Controle de Integridade Identificar operação Canal de comunicação Sanções administrativas relação à coleta e processamento; a estrutura estabelecida para a proteção; regras para tomar decisões relacionadas a dados pessoais; critérios de aceitação de risco e compromisso de satisfazer os requisitos aplicáveis de proteção à privacidade.	Não apresentar documentação que garanta política ou norma de proteção de dados pessoais que aborde a finalidade da contratada perante o processamento de dados.	Mensal de 1% (um por cento), sobre o valor da fatura mensal
	Realizar o tratamento de dados pessoais para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais da contratante	Não apresentar documentação que comprove que o tratamento de dados pessoais é realizado para o atendimento de sua finalidade pública	Mensal de 1% (um por cento), sobre o valor da fatura mensal

	Coletar e processar dados limitados ao mínimo necessário para atendimento da finalidade do tratamento	Não apresentar documentação que comprove que o tratamento de dados está limitado ao mínimo necessário para atendimento da finalidade do tratamento	Mensal de 1% (um por cento), sobre o valor da fatura mensal
	Implementar medidas que garantam e maximizem a precisão dos dados pessoais coletados, antes de qualquer armazenamento ou processamento de dados pessoais	Não apresentar documentação que comprove que foram implementadas medidas que garantem e maximizam a precisão dos dados pessoais coletados	Mensal de 1% (um por cento), sobre o valor da fatura mensal
	Realizar o processamento com dados pessoais de modo a identificar a operação realizada, quem realizou, data e hora;	Não apresentar documentação que define que as operações de processamento realizadas com dados pessoais são registradas identificando a operação realizada, quem realizou, data e hora	Mensal de 1% (um por cento), sobre o valor da fatura mensal