ANEXO I
QUESTIONÁRIO PRELIMINAR DE CONFORMIDADE

QUESTIONÁRIO PRELIMINAR DE CONFORMIDADE		
Declaração inicial: Ao subscrever o presente termo, declaro que: (1) sou legitimado a responder ao presente questionário em nome da empresa avaliada; (2) as respostas que serão conferidas ao presente questionário expressam a verdade; (3) estou ciente de que poderão ser exigidas evidências a respeito das respostas que serão conferidas ao presente questionário; (4) eventual constatação de que foram prestadas informações falsas, incompletas ou contraditórias constituirá justa causa para *(i)* a ruptura da negociação preliminar iniciada; ou *(ii)* a resolução de eventual contrato/convênio celebrado com a Cagece _____ ASSINATURA DO DECLARANTE NOME:		
	QUESTÕES REFERENTES À INSTITUIÇÃO	SIM/NÃO/ PARCIALMENTE
1	Nomeou um Encarregado de Proteção de Dados.	
2	Mantém política de privacidade.	
3	Mantém política de segurança da informação.	
4	Mantém plano de resposta a incidentes.	
5	Mantém plano de resposta a demandas de titulares.	
6	Mantém processo de notificação de incidentes de segurança.	
7	Em relação à notificação mencionada no item anterior, a notificação indica: (i) data e hora do incidente; (ii) data e hora da ciência pelo controlador responsável; (iii) descrição dos dados pessoais afetados; (iv) número de titulares afetados; (v) relação dos titulares envolvidos; (vi); riscos relacionados ao incidente; (vii) indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados; (viii) motivos da demora, no caso de a comunicação não haver sido imediata; (ix) medidas que foram ou que	

	serão adotadas para reverter ou mitigar os efeitos do prejuízo; (x) o contato do encarregado de proteção de dados ou de outra pessoa junto à qual seja possível obter maiores informações sobre o ocorrido.	
8	Submete sócios, funcionário, parceiros, prestadores de serviços ao dever de confidencialidade.	
9	Observa regras de governança sugeridos por normas técnicas, tais como ISO e ABNT.	
10	É capaz de manter procedimentos de segurança de dados que assegurem a sua confidencialidade, integridade e disponibilidade e que atendam aos padrões mínimos sugeridos em normas técnicas como ISO e ABNT.	
11	É capaz de manter relatórios que indiquem, no mínimo: (i) os sistemas em que os dados são tratados; (ii) as medidas de segurança que tais sistemas oferecem; (iii) o tempo registrado de eventual inatividade das medidas técnicas de segurança; (iv) a conformidade/inconformidade do sistema com relação às medidas de segurança e governança de dados especificadas neste contrato; v) as eventuais ameaças ou efetivas violações de dados e/ou incidentes de segurança; e (vi) as contramedidas ou salvaguardas recomendadas, exigidas e implementadas.	
12	Assegura meios para que seja fiscalizada e auditada relativamente às obrigações de proteção de dados pessoais presencial e remotamente.	
	REQUISITOS MÍNIMOS DA FERRAMENTA (SOFTWARE/SISTEMA/APLICAÇÃO/SOLUÇÃO)	SIM/NÃO
1	Possui comunicação segura (aplicações web com certificado válido e protocolo HTTPS em comunicação com o padrão de criptografia SSL/TLS)?	
2	Funciona em alta disponibilidade, possuindo mais de uma instância?	
3	Possui rotinas de backup?	
4	As credenciais de acesso do usuário devem ter nível de complexidade alto?	
5	Possui trilha de auditoria?	
6	Dispões de opção para informar ao usuário quais dados está retendo do usuário e permitir que o usuário exclua esses dados?	
7	Baseia-se em tecnologias atualizadas?	
8	O sistema operacional é mantido atualizado?	
9	Possui um firewall de aplicação?	
10	Conta com sistema de *captcha* para páginas web (quando for o caso)?	
11	Possui sistema para evitar ataque de negação de serviço?	

12	Possui autenticação de múltiplo fator (importante para plataformas SaaS)	