RAZÃO SOCIAL:	

AVALIAÇÃO

+ Aplicabilidade	0%
+ Aderência	0%
+ Justificativa	0%

DAE S/A					FORNECEDOR		Progresso de Coleta de Evidências			
#	Grupo	Requisito de fornecedor, prestador ou terceiroproteção de dados de fornecedores da DAE S/A	Perguntas	Aplicabilidade	Avaliação de aderência ao requisito	Justificativa e comentários.	Proposta de Evidência	Status - Evidência	Referência da Evidência (Arquivo Anexo/Link)	Observações
A.1	A - Gestão	O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, independentemente da base legal escolhida.	O Fornecedor, prestador ou terceiro adota um inventário contendo o registro de suas operações de tratamento de dados pessoais com informações sobre a categoria de titulares, finalidade de tratamento, base legal e outros?	Selecione..	Selecione..	Por favor, insira a justificativa referênte a aplicabilidade e aderência definida	Evidência de registro.	Pendente		
A.2	A - Gestão	O controlador deverá indicar o encarregado pelo tratamento de dados pessoais.	O Fornecedor, prestador ou terceiro nomeou um Encarregado pelo tratamento de dados pessoais?	Selecione..	Selecione..	Por favor, insira a justificativa referênte a aplicabilidade e aderência definida	As informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador	Pendente		
A.3	A - Gestão	Estabelecer, manter registros do compromisso de confidencialidade com colaboradores que terão acesso às informações pessoais e/ou sensíveis de titulares	O Fornecedor, prestador ou terceiro celebra Acordo de Confidencialidade com os seus colaboradores na prestação de serviços relacionados ao tratamento de dados pessoais?	Selecione..	Selecione..	Por favor, insira a justificativa referênte a aplicabilidade e aderência definida	NDA	Pendente		
A.4	A - Gestão	Realizar formação em proteção de dados e segurança da informação periódica para colaboradores que terão acesso às informações pessoais e/ou sensíveis de titulares	O Fornecedor, prestador ou terceiro fornece treinamento periódico sobre proteção de dados para sua equipe?	Selecione..	Selecione..	Por favor, insira a justificativa referênte a aplicabilidade e aderência definida	Evidência de treinamentos LGPD e Segurança da Informação	Pendente		
A.5	A - Gestão	Desenvolver produtos e serviços já com um grau adequado de proteção ao titular segundo a Lei Geral de Proteção de Dados Pessoais.	O Fornecedor, prestador ou terceiro adota mecanismos sobre análise de privacidade e proteção de dados pessoais, desde a concepção (Privacy by Design), de seus produtos, serviços ou projetos, e realiza avaliações constantes, inclusive antes da implementação daqueles? Em caso positivo, detalhar como é realizado.	Selecione..	Selecione..	Por favor, insira a justificativa referênte a aplicabilidade e aderência definida	Evidência de análises de Privacy by Design	Pendente		
A.6	A - Gestão	Propiciar um grau de conscientização dentro da empresa sobre as práticas adequadas, bem como alocar as responsabilidades dos colaboradores, salvaguardando os titulares de eventuais práticas ilegais.	O Fornecedor, prestador ou terceiro possui política ou norma de proteção de dados que aborde as formas adequadas de tratamento de dados pelos seus colaboradores e terceiros, bem como alocando responsabilidades sobre os tratamentos?	Selecione..	Selecione..	Por favor, insira a justificativa referênte a aplicabilidade e aderência definida	Evidência de Política ou Norma que aborde as formas adequadas de tratamento.	Pendente		
B.1	B - Retenção	Garantir que as informações de titulares, sejam elas de qualquer categorias, sejam devolvidas ou destruída após o fim dos serviços ou mediante pedido da DAE S/A	As práticas de descarte ou destruição segura das informações garantem que esses dados não sejam recuperados?	Selecione..	Selecione..	Por favor, insira a justificativa referênte a aplicabilidade e aderência definida	Política de descarte e destruição (LGPD Art. 16)	Pendente		
B.2	B - Retenção	Os requisitos de retenção para cada tipo de informação deve ser documentada no registro de ativos de informações e apoiados por um planejamento abrangente que especifique o período de retenção.	Há algum registro ou tabela que detenha/centralize as informações de tempo de retenção dos dados pessoais estabelecidas pela DAE S/A e/ou pela legislação vigente aplicável?	Selecione..	Selecione..	Por favor, insira a justificativa referênte a aplicabilidade e aderência definida	Política de descarte e destruição ou uma Tabela de Temporalidade (LGPD Art. 16)	Pendente		
C.1	C - Acesso	Apoiar a DAE S/A, através de medidas técnicas e organizacionais adequadas para cumprir as suas obrigações de responder aos pedidos dos titulares dos dados que solicitam exercer os seus direitos de acordo com a LGPD.	O fornecedor, prestador ou terceiro possui procedimentos/mecanismos para garantir que as solicitações de requisição dos titulares sejam atendidas de forma segura e comunicadas, se necessário, para a DAE S/A ?	Selecione..	Selecione..	Por favor, insira a justificativa referênte a aplicabilidade e aderência definida	Procedimento , normativo ou evidência de etapas que comprovem a possibilidade de cumprir tal interação com o titular.	Pendente		
D.1	D - Divulgação a Terceiros	Notifique a DAE S/A imediatamente ao saber que um subcontratado tratou dados pessoais e/ou sensíveis de titulares para qualquer finalidade diferente das relacionadas aos serviços adquiridos.	O fornecedor, prestador ou terceiro possui mecanismos/procedimentos que requeiram a comunicação/notificação da DAE S/A caso haja um tratamento indevido por parte de um subcontratado?	Selecione..	Selecione..	Por favor, insira a justificativa referênte a aplicabilidade e aderência definida	Procedimento, normativo ou evidência que comprove a possibilidade de interação quando da ocorrência de um tratamento indevido.	Pendente		
E.1	E - Monitoramento e Imposição	O Fornecedor, prestador ou terceiro tem um plano de resposta a incidentes que exige que a DAE S/A seja notificada rapidamente ao tomar conhecimento de uma violação de dados ou vulnerabilidade de segurança relacionada à manipulação dos dados pessoais ou confidenciais	Há um plano de contingência que inclui notificar a DAE S/A sobre incidentes com violação de dados pessoais?	Selecione..	Selecione..	Por favor, insira a justificativa referênte a aplicabilidade e aderência definida	Evidência de ferramenta/processo de DLP em funcionamento no ambiente; Procedimentos de gestão de incidentes (framework corporativo); Evidência de teste para Disaster Recovery.	Pendente		
F.1	F - Segurança	O Fornecedor, prestador ou terceiro deve ter definido, comunicado e implementado políticas que protejam e limitem o acesso a dados pessoais e/ou sensíveis de titulares	Possui controles que protejam e limitem o acesso a dados pessoais e/ou sensíveis de clientes ou colaboradores da DAE S/A?	Selecione..	Selecione..	Por favor, insira a justificativa referênte a aplicabilidade e aderência definida	Código de Ética/Conduta; Documento com políticas para Gestão de acessos (Prints de telas explicando como os acessos aos sistemas e aplicações são concedidos, alterados e revogados tempestivamente.); Política de revisão de acessos formalizada + última revisão de acessos realizada	Pendente		
F.2	F - Segurança	Realizar avaliações periódocas de segurança de rede que incluam: • Revisão das principais alterações no ambiente, como um novo componente do sistema, topologia de rede, regra de firewall, etc; • Realizar análises de vulnerabilidade; • Manter os registos de alterações, informações sobre o motivo da alteração, incluir um revisor e aprovador das mudanças.	O Fornecedor, prestador ou terceiro realiza avaliações periódicas de segurança de rede? São aplicadas regras de firewall para conter o acesso a sites e códigos maliciosos?	Selecione..	Selecione..	Por favor, insira a justificativa referênte a aplicabilidade e aderência definida	Evidência de teste para Disaster Recovery; Política de Segurança da Informação (última versão); Certificações Corporativas Segurança da Informação CISM/CEH/ECSA/CHFI/ISFS; Último teste de vulnerabilidade realizado (PenTest)	Pendente		
F.3	F - Segurança	Todos os ativos de tecnologia utilizados devem ser contabilizados e ter um gestor identificado. O fornecedor, prestador ou terceiro é responsável por manter um inventário desses ativos, estabelecer o uso aceitável e autorizado dos ativos, e fornecer um nível adequado de proteção para os ativos ao longo de seu ciclo de vida.	O terceiro mantém um inventário atualizado dos ativos utilizados para dar suporte no processamento/armazenamento de dados?	Selecione..	Selecione..	Por favor, insira a justificativa referênte a aplicabilidade e aderência definida	Evidência de inventário de ativos de TI	Pendente		
F.4	F - Segurança	Estabelecer e manter controles de acesso lógico definindo perfis e grupos de acessos de acordo com a necessidade, para impedir o acesso não autorizado a qualquer dado pessoal e/ou sensível de titulares	O Fornecedor, prestador ou terceiro adota acesso restrito e com controles de autenticação no ambiente onde se armazenam e tratam dados pessoais?	Selecione..	Selecione..	Por favor, insira a justificativa referênte a aplicabilidade e aderência definida	Evidência de controle (prints de tela de sistemas, política de segurança e fluxos de aprovação); Política de Controle de Acesso	Pendente		
F.5	F - Segurança	Definir e implementar procedimentos de gerenciamento de patches que priorizem a segurança dos sistemas utilizados para processar dados pessoais e/ou sensíveis de c. Esses procedimentos devem incluir: • Abordagem de risco definido para priorizar patches de segurança; • Capacidade de lidar com e implementar correções de emergência; • Aplicabilidade ao sistema operacional e software de servidor, como servidor de aplicativos e software de banco de dados; • Documentar o risco que o patch mitiga e rastrear quaisquer exceções;	O Fornecedor, prestador ou terceiro promove patchs para garantir a segurança nos sistemas utilizados no processamento de dados pessoais e/ou sensíveis de clientes ou colaboradores da DAE S/A?	Selecione..	Selecione..	Por favor, insira a justificativa referênte a aplicabilidade e aderência definida	Documento/Evidências com Procedimentos de gerenciamento de patches e como são aplicados.	Pendente		
F.6	F - Segurança	Instalar software antivírus e antimalware em equipamentos ligados à rede utilizada para processar informações de titulares, incluindo, entre outros, servidores, computadores de produção e de formação para proteger de vírus potencialmente nocivos e de aplicações de software malicioso. Atualizar as definições de antimalware diariamente ou de acordo com as instruções do fornecedor de antivírus/antimalware.	O terceiro possui antivírus e antimalware, atualizados e licenciados, em todos os equipamentos que processam dados pessoais e/ou sensíveis de clientes ou colaboradores da DAE S/A?	Selecione..	Selecione..	Por favor, insira a justificativa referênte a aplicabilidade e aderência definida	Tela de gerenciamento do antivírus e antimalware	Pendente		
F.7	F - Segurança	O fornecedor, prestador ou terceiro tem de garantir a existência de processos de planejamento de cópia de segurança que protejam os dados da DAE S/A contra a utilização, acesso, divulgação, alteração e destruição não autorizadas.	O Fornecedor, prestador ou terceiro possui documentado um plano para garantir a disponibilidade dos dados, por exmplo um plano de backup e restore implementado?	Selecione..	Selecione..	Por favor, insira a justificativa referênte a aplicabilidade e aderência definida	Política de Retenção e Backup	Pendente		
F.8	F - Segurança	Estabelecer e testar os planos de continuidade do negócio e recuperação após desastres.	O Fornecedor, prestador ou terceiro possui planos de continuidade de negócios e realiza testes de recuperação após incidentes?	Selecione..	Selecione..	Por favor, insira a justificativa referênte a aplicabilidade e aderência definida	Procedimentos de continuidade de negócios (PCN,DRP); Evidência de execução de Teste de DRP	Pendente		

F.9	F - Segurança	As informações quando estão em trafego entre sistemas ou bases de dados utilizam mecanismos de segurança. Por exemplo: protocolo Https ou FTPS.	O Fornecedor, prestador ou terceiro realiza a transmissão segura de dados pessoais, inclusive por e-mails e mensagens instantâneas?	Selecione..	Selecione..	Por favor, insira a justificativa referênte a aplicabilidade e aderência definida	Normativos de criptografia e compartilhamento seguro, por exemplo. Verificação em duas etapas quando do uso de aplicativos de mensagens instantâneas, por exemplo	Pendente		
F.10	F - Segurança	Todos os dispositivos (portáteis, estações de trabalho, etc.) que irão acessar ou processar informações pessoais ou confidenciais de titulares têm aplicado criptografia em disco.	O Fornecedor, prestador ou terceiro possui criptografia nos dispositivos que irão acessar ou processar dados da DAE S/A?	Selecione..	Selecione..	Por favor, insira a justificativa referênte a aplicabilidade e aderência definida	Configurações criptográficas (para os sistemas e dispositivos que possuem criptografia).	Pendente		
F.11	F - Segurança	O fornecedor tem que manter arquivos físicos com dados de titulares em um ambiente de acesso controlado.	O Fornecedor, prestador ou terceiro possui gerenciamento de acesso aos ambientes físicos que são armazenados dados da DAE S/A?	Selecione..	Selecione..	Por favor, insira a justificativa referênte a aplicabilidade e aderência definida	Certificações Corporativas Data Center ISO/PCI/TIER/IEC/SOC	Pendente		
F.12	F - Segurança	Tornar anônimos todos os dados dos titulares usados em um ambiente de desenvolvimento ou teste.	O Fornecedor, prestador ou terceiro mantém anônimos os dados utilizados em ambientes de desenvolvimento ou homologação?	Selecione..	Selecione..	Por favor, insira a justificativa referênte a aplicabilidade e aderência definida	Evidência de procedimento (prints de tela de sistemas, política de segurança e tela de software onde o banco de dados está com criptografia / anonimizado)	Pendente		
F.13	F - Segurança	Os serviços em nuvem devem ser incluídos em um inventário de ativos. Um registro de serviço em nuvem deve estar em vigor. O registro deve: - identificar todos os serviços em nuvem em uso; - detalhar o perfil de segurança das informações do serviço; - detalhar os recursos de proteção de informações do serviço.	O Fornecedor, prestador ou terceiro possui um inventário dos serviços utilizados em nuvem?	Selecione..	Selecione..	Por favor, insira a justificativa referênte a aplicabilidade e aderência definida	Evidência do controle de inventários (prints de tela do software que gerencie o controle)	Pendente		
F.14	F - Segurança	Os requisitos de disponibilidade definidos pelo proprietário da empresa devem ser cumpridos no design da solução em nuvem e aplicados no contrato.	O contrato firmado com o fornecedor de serviços de nuvem atende os requisitos de disponibilidade?	Selecione..	Selecione..	Por favor, insira a justificativa referênte a aplicabilidade e aderência definida	Último Relatório SOC do ambiente hospedado em datacenter de terceiros (quando aplicável)	Pendente		