

Requisitos	Forma de Atendimento		Observações
	Nativo (N) / Nativo por Parametrização (NP) / Customizado (C) / Não Atende (NA)		
2.Descrição do Objeto			
2.1. Contratação de Solução Integrada de Gestão de Auditoria, com serviços de implantação e serviços técnicos especializados, conforme especificações a seguir:			
2.1.1. Visão Geral da Solução			
2.1.1.1. A solução deve prover a gestão da auditoria com informações sobre todo o processo de auditoria interna, apresentando os principais resultados e indicadores do processo de auditoria, alinhada aos órgãos reguladores e normas internacionais do IIA, no que tange ao planejamento anual e customização dos fatores de riscos considerados, planejamento dos trabalhos individuais, aprovação do programa de auditoria, amostragens probabilísticas e não probabilísticas auditáveis, execução e testes de controles, supervisão e revisão dos resultados, planos de ação para as não conformidades, monitoramento de planos de ação, geração e emissão de relatórios de auditoria, relatório anual de atividades e suporte à consolidação de opinião geral sobre os controles partindo dos trabalhos individuais, principais resultados e indicadores de desempenho da auditoria interna, gestão de papéis de trabalho permanentes (base de			
2.1.1.2. A solução deve possuir integração nativa entre todos os módulos e manter logs de todas as alterações realizadas pelos usuários, indicando no mínimo usuário, campo alterado, valor anterior, valor alterado e data.			
2.1.1.3. A solução deve proporcionar benefícios para Auditoria Interna com a utilização de ferramentas sistêmicas para Gestão de Auditoria alinhada as melhores práticas do mercado.			
2.1.1.4. A solução deve permitir planejamento baseado em riscos, alinhados aos riscos corporativos da empresa e customização dos fatores de riscos e dos objetos auditáveis, hierarquização e priorização pelo nível de risco deles.			
2.1.1.5. A solução deve permitir biblioteca nativa atualizada de testes de controle de normas de mercado tais como ISO 19011, ISO 27001, ISO 27002, ISO 27701, COBIT 2019 dentre outros relacionados aos objetos de auditoria.			
2.1.1.6. Gerenciar as atividades de auditoria em sua totalidade, permitindo a gestão de auditoria por tarefas, painéis gerenciais para gestão de projetos de auditoria.			
2.1.1.7. Gerenciamento da atividade de auditoria por meio da produção de indicadores de desempenho e indicadores de produtividade individuais.			
2.1.1.8. Tratamento de demandas externas - TCU/CGU/demais Órgãos Fiscalização.			
2.1.1.9 Integração por API, banco de conhecimento (papéis de trabalho permanente) dos objetos auditáveis, sendo desejável ferramenta de amostragem estatística.			

2.1.1.10. A solução deve atender ao disposto nas Normas Internacionais para a Prática da Atividade de Auditoria Interna – IPPF/IIA.		
2.1.1.11. A solução deve atender ao disposto na legislação que rege a atividade de auditoria interna governamental do Poder Executivo Federal:		
2.1.1.11.1. Referencial Técnico da Atividade de Auditoria Interna Governamental do Poder Executivo Federal.		
2.1.1.11.1.1. Instrução Normativa SFC nº 3, de 9 de junho de 2017.		
2.1.1.11.1.2. Manual de Orientações Técnicas da Atividade de Auditoria Interna Governamental do Executivo Federal.		
2.1.1.11.2.1. Instrução Normativa SFC nº 8, de 6 de dezembro de 2017.		
2.1.1.11.3. Plano Anual (PAINT) e Relatório Anual (RAINT) das UAIG do Poder Executivo Federal.		
2.1.1.11.3.1. Instrução Normativa SFC nº 5, de 27 de agosto de 2021.		
2.1.1.11.4. Sistemática de Quantificação e Registro dos Resultados e Benefícios da Atividade de Auditoria Interna		
2.1.1.11.4.1. Instrução Normativa SFC nº 10, de 28 de abril de 2020.		
2.1.1.11.4.2. Portaria SFC nº 1.976, de 20 de agosto de 2021		
2.1.1.11.4.3. Manual de Contabilização de Benefícios.		
2.1.1.11.5. Orientação Prática: Relatório de Auditoria.		
2.1.1.11.5.1. Portaria SFC nº 1037, de 07 de março 2019.		
2.1.1.11.6. Orientação Prática: Plano de Auditoria Interna Baseado em Risco.		
2.1.1.11.6.1. Anexo Portaria SFC nº 1055, de 30 de abril de 2020.		
2.1.1.12. Atender aos requisitos do Programa de Gestão e Melhoria da Qualidade dos Trabalhos da Auditoria Interna –		
2.1.1.13. Suportar a Política Corporativa de Segurança da Informação do SERPRO, disponível no endereço: https://www.transparencia.serpro.gov.br/acesso-a-informacao/licitacoes-e-contratos/documentos/sg-018-2019.pdf		
2.1.1.14. Permitir gerenciar as atividades de auditoria em sua totalidade.		
2.1.2. Requisitos Funcionais		
2.1.2.1. Análise Preliminar de Riscos		
2.1.2.1.1. Cadastrar riscos no modelo horizontal ou vertical de processos de negócio e de projetos.		
2.1.2.1.2. Para cada risco deve ser possível informar detalhes que permitam avaliar a relevância de cada risco através de campos como: impacto, probabilidade, risco inerentes e risco residual criando uma matriz de riscos para administração, mitigação, controle dos mesmos, hierarquização e priorização de riscos, com o registro do racional adotado.		
2.1.2.1.3. Visualizar quais riscos da organização estão cobertos, onde estão os GAPs dentro do processo.		
2.1.2.1.4. Permitir aos auditores e gestores de riscos a catalogar, avaliar, priorizar e comunicar os riscos estratégicos.		
2.1.2.1.5. Capturar e manter uma visão completa dos riscos da organização.		
2.1.2.1.6. Comunicar efetivamente a posição atual e histórica dos riscos, riscos emergentes e resultados de projetos.		
2.1.2.1.7. A categorização e rastreamento dos riscos por características e planos de ação.		

2.1.2.1.8. Integração com pontos de projetos, resultados e atividades de remediação.		
2.1.2.1.9. Suportar a implementação de frameworks tais como: COSO ICF, COSO ERM, ISO 31000, COBIT 2019, GTAG 11, dentre outras e quadros genéricos de gestão de riscos.		
2.1.2.1.10. Emitir relatório de Matriz de Risco com rastreabilidade.		
2.1.2.2. Planejamento Anual de Auditoria		
2.1.2.2.1. Permitir personalizar o processo de planejamento anual com o cadastramento de fatores e critérios de		
2.1.2.2.2. Cadastrar a Matriz de Riscos da Auditoria para embasar o plano anual.		
2.1.2.2.3. Cadastrar categoria da auditoria, a exemplo de avaliação, consultoria, apuração, permitindo subcategorias como conformidade e operacional.		
2.1.2.2.4. Cadastrar e obter do sistema corporativo de processo, objeto (processo ou tema ou questão) a ser auditado. Permitir estabelecer o objeto como padrão para aproveitar em outro planejamento.		
2.1.2.2.5. Permitir recuperar o objeto (processo ou tema ou questão) padrão para elencá-lo na elaboração do PAINT (Plano Anual de Atividades de Auditoria Interna).		
2.1.2.2.6. Cadastrar descrição do contexto e do escopo do objeto a auditar.		
2.1.2.2.7. Cadastrar e obter do sistema corporativo de riscos, os riscos associados ao objeto auditado.		
2.1.2.2.8. Cadastrar processo da área de negócio que será associado ao item do PAINT.		
2.1.2.2.9. Cadastrar tipo da auditoria (Operacional, Desempenho, Sistema, Especial, Controles Internos, Contínua etc.).		
2.1.2.2.10. Cadastrar data prevista (início e fim) de cada item do PAINT.		
2.1.2.2.11. Cadastrar e calcular quantidade de recursos utilizados na auditoria e horas previstas a cada item do PAINT.		
2.1.2.2.12. Associar o objeto ao risco relacionado na Matriz de Risco da Auditoria.		
2.1.2.2.13. Emitir relatório com distribuição de horas.		
2.1.2.2.14. Emitir Plano Anual de Auditoria (PAINT) com as atividades programadas, discriminando atividade, área auditada, objetivo, escopo, riscos, nível de risco (probabilidade vs. Impacto), origem da demanda, cronograma, recursos utilizados, e representatividade em relação ao total (%).		
2.1.2.2.15 Permitir registro de log do histórico de supervisão e aprovação da etapa do planejamento incluindo o cronograma e programa de trabalho da auditoria.		
2.1.2.2.16 Permitir envio de questionário aos gestores.		
2.1.2.3. Execução do trabalho de auditoria.		
2.1.2.3.1. A partir do planejamento anual de auditoria, elencar o objeto a ser auditado.		
2.1.2.3.2. Alocar os participantes da auditoria (auditores, gerentes, revisor, órgão auditado).		
2.1.2.3.3. Permitir registrar a data de início e término previstos da auditoria e data de início e término reais.		
2.1.2.3.4. Permitir cadastrar e utilizar programa de auditoria padrão.		

2.1.2.3.5.	Permitir cadastrar e utilizar riscos na auditoria padrão.			
2.1.2.3.6.	Permitir cadastrar e utilizar não-conformidades na auditoria padrão.			
2.1.2.3.7.	Permitir cadastrar e utilizar recomendações da auditoria padrão.			
2.1.2.3.8.	A partir do programa de auditoria padrão elencar os itens que farão parte do roteiro de verificação.			
2.1.2.3.9.	Permitir a emissão de relatório referente ao planejamento do trabalho.			
2.1.2.3.10.	Permitir o registro e armazenamento de arquivos coletados nas áreas de negócio, incluindo a definição de tabela de temporalidade de informações marcadas como dados pessoais e dados pessoais sensíveis.			
2.1.2.3.11.	Registrar, anexar informações dos testes realizados e das condições observadas, assim como do critério de auditoria, causas e consequências identificadas.			
2.1.2.3.12.	Facilitar a documentação da execução dos trabalhos de auditoria e registro de evidências identificadas durante a realização da auditoria, permitindo referência cruzada entre planejamento, testes realizados, achados, evidências, plano de ação.			
2.1.2.3.13.	Possibilitar anexar diferentes tipos de documentos (textos, planilhas, apresentações, gráficos e imagens).			
2.1.2.3.14.	Permitir cadastro das não-conformidades com os respectivos riscos, testes de controle, fundamentações, achados, recomendações, plano de ação e situação atual.			
2.1.2.3.15.	Permitir a confecção de Relatório de Auditoria com as não-conformidades, riscos, testes realizados, achados, fundamentações, recomendações e planos de ação.			
2.1.2.3.16.	Permitir a edição compartilhada do resultado dos testes e registro de revisão dos itens considerados no trabalho, registrando o responsável pela revisão, aprovação e data.			
2.1.2.3.17.	Apropriar horas trabalhadas e custos incorridos nos trabalhos (registro de tempos e despesas).			
2.1.2.3.18.	Permitir registro de log do histórico de supervisão e aprovação da etapa de execução incluindo atribuição dos testes de controle, execução dos testes, registro dos resultados, registro de achados e aprovações.			
2.1.2.3.19.	Permitir envio de solicitações ou comunicados em geral para área e gestor responsável com cópia para demais interessados.			
2.1.2.3.20.	Permitir por no mínimo dois (02) remetentes habilitados e designados no trabalho para envio de solicitações em geral referente ao trabalho.			
2.1.2.4. Não Conformidades e Planos de Ação				
2.1.2.4.1.	Para cada não conformidade identificada no trabalho de auditoria, permitir cadastramento do plano de ação, explicações, prazo da área auditada, responsável pela ação e pelo acompanhamento.			
2.1.2.4.2.	Permitir ao auditado executar esta tarefa, não sendo permitido o acesso e nem visualização do papel de trabalho. Permitir edição do plano de ação, explicações, prazo e responsável pelo plano de ação.			
2.1.2.4.3.	Permitir reprogramar o plano de ação e cadastrar as justificativas.			
2.1.2.4.5.	Permitir a configuração de alertas de cobrança com vencimento.			

2.1.2.4.6.	Emitir relatório das não conformidades, planos de ação, prazos por área e responsável pela não conformidade.		
2.1.2.4.7.	Permitir associar status nos planos de ação.		
2.1.2.4.8.	Permitir dar aceite nos planos de ação pelo auditor responsável e aprovação pela gerência.		
2.1.2.4.9.	Envio automático de e-mail para os interessados nas principais ações.		
2.1.2.4.10.	Controle automatizado e customizável dos processos de trabalhos (Workflow).		
2.1.2.4.11	Permitir registro de log do histórico de supervisão, aprovação e alteração do plano de ação.		
2.1.2.4.12	Permitir geração de indicadores das não-conformidades em acompanhamento e encerradas.		
2.1.2.5. Monitoramento			
2.1.2.5.1.	Permitir rastreabilidade entre o PAINT e os trabalhos de auditoria.		
2.1.2.5.2.	Emitir relatório comparativo das auditorias previstas no PAINT e realizadas.		
2.1.2.5.3.	Permitir criar indicadores de desempenho.		
2.1.2.5.4.	Permitir acompanhamento através de relatórios customizados, gráficos e dashboards.		
2.1.2.6. Atendimentos a órgãos de fiscalização			
2.1.2.6.1.	Permitir registro de ofícios de solicitações recebidas dos órgãos de fiscalização e controle.		
2.1.2.6.2.	Permitir cadastramento de demandas de órgãos de fiscalização e prazo de atendimento (previsto, adiamento autorizado e realizado).		
2.1.2.6.3.	Permitir envio de solicitação de informações e documentos relacionados aos documentos recebidos dos órgãos de fiscalização e controle para as áreas internas do Serpro.		
2.1.2.6.4.	Permitir o registro pelas áreas internas de informações e de documentos para atender à demanda dos órgãos de fiscalização e controle.		
2.1.2.6.5.	Gerar relatório de Ofícios/demandas recebidas, em atendimento e em atraso.		
2.1.2.6.6.	Emitir alerta de prazo vencido e a vencer aos usuários. 2.1.2.4.5. Permitir a configuração de alertas de cobrança com vencimento.		
2.1.2.6.7.	Permitir geração de indicadores quanto demandas externas tramitadas.		
2.1.2.7. Elaboração do Relatório Anual de Atividades da Auditoria (RAINT)			
2.1.2.7.1.	Consolidar os resultados das auditorias realizadas.		
2.1.2.7.2.	Consolidar as não conformidades e planos de ação finalizadas e pendentes, por ano.		
2.1.2.7.3.	Consolidar horas trabalhadas incorridos nos trabalhos de auditoria em comparação com as horas planejadas no PAINT.		
2.1.2.7.4.	Permitir elaboração do Relatório Anual de Atividades da Auditoria (RAINT) a partir de <i>template</i> customizável.		

2.1.3. Requisitos Não Funcionais		
2.1.3.1. A solução deve ser disponibilizada nas modalidades:		
2.1.3.1.1. Licenciamento Perpetuo.		
2.1.3.1.2. Software como Serviço ("Software as a Service - SaaS").		
2.1.3.2. A CONTRATADA deve fornecer, no mínimo, licenças para os ambientes de produção e homologação.		
2.1.3.3. [SE NA MODALIDADE SAAS] A CONTRATADA será responsável pela definição, dimensionamento e parametrização dos ambientes na plataforma Software como Serviço, necessários e com recursos suficientes para suportar a Solução com a estrutura de dados e usuários do SERPRO.		
2.1.3.4. [SE NA MODALIDADE SAAS] A CONTRATADA será responsável por manter durante a vigência do contrato os ambientes em funcionamento, e fazer qualquer ajuste de dimensionamento em recursos de processamento e armazenamento que forem necessários para a boa performance da Solução.		
2.1.3.5. [SE NA MODALIDADE SAAS] A CONTRATADA deve garantir que os dados e backups da Solução estejam		
2.1.3.6. [SE NA MODALIDADE SAAS] A CONTRATADA comprometer-se-á a preservar os dados do SERPRO contra acessos indevidos e abster-se-á de replicar ou realizar cópias de segurança (backups) destes dados fora do território brasileiro, devendo informar imediatamente e formalmente o SERPRO qualquer tentativa, inclusive por meios judiciais, de acesso por		
2.1.3.7. Requisitos relacionados a Acesso.		
2.1.3.7.1. A CONTRATADA deve ofertar licenças de acesso a solução, conforme tabela abaixo:		
Tipo de Perfil / Métrica/ Quantidade Estimada		
Perfil Administrador / Usuário nominal / 3		
Perfil Auditor / Usuário nominal / 32		
Perfil Consulta / Usuário nominal / 12		
Perfil Auditado / Usuários concorrentes / 60		
2.1.3.7.1.1. A solução deve permitir o cadastro de até 6.009 (seis mil e nove) usuários concorrentes ativos.		
2.1.3.7.2. A solução deverá diferenciar níveis de acesso de usuários através de perfil e suas funcionalidades, respeitando as características dos perfis abaixo:		
2.1.3.7.2.1. Perfil Administrador - Acesso a todos os módulos e funcionalidades da solução.		
2.1.3.7.2.2. Perfil Auditor - Acesso aos diversos módulos da solução, porém com limitações que se restringem a acessos somente leitura e/ou às informações e projetos que estão envolvidos; Permitir visualização e acesso as exceções, independentemente a quem eles são designados e adicionar comentários e anexos; não podem alterar o status/prioridade/prazo; permitir acesso à leitura aos relatórios.		
2.1.3.7.2.3. Perfil Consulta - Acesso de consulta destinado a áreas de assessoramento de diferentes unidades selecionadas; O acesso é destinado para acompanhar o atendimento a pendências e demandas solicitadas.		

2.1.3.7.2.4. Perfil Auditado - Acesso destinado às áreas auditadas e/ou acionadas pelos auditores para responder aos workflows enviados pela solução; O acesso é destinado para responder à demanda solicitada.		
2.1.3.7.3. Permitir customização de perfis e níveis de acesso.		
2.1.3.7.4. Suportar o protocolo OpenIDConnect 1.0 (https://openid.net/connect/) para integração com Autenticador e Autorizador externo do Serpro.		
2.1.3.8. Requisitos Relacionados à Interface.		
2.1.3.8.1. Disponibilizar todas as funcionalidades em arquitetura 100% Web permitindo acesso via browser, mantendo compatibilidade com os navegadores Microsoft Edge, Mozilla Firefox, Google Chrome e Apple Safari, sem necessidade de instalação de software adicional no computador dos usuários.		
2.1.3.8.2. A solução deve ser responsiva, se adaptando aos diversos meios de acessos web, inclusive mobile.		
2.1.3.9. Requisitos Relacionados a Log de Atividades.		
2.1.3.9.1. Registrar e exibir log contendo todas as ações (inclusão, alteração, exclusão e consulta) dos usuários em todas as operações executadas.		
2.1.3.9.2. Registrar e exibir, aos usuários de perfis para auditoria, os acessos efetuados por todos os usuários para efeito de trilha de auditoria, log e elaboração de relatórios gerenciais, constando no mínimo: operação realizada, usuário, data, hora, ação realizada, dado alterado/incluído/excluído.		
2.1.3.9.3. Permitir consultas das trilhas de auditoria para perfis especificados, tendo como parâmetro qualquer de seus elementos ou a combinação desses elementos. O resultado dessas consultas deve ser exibido na própria interface web da solução, via funcionalidade específica da solução, tendo ainda a possibilidade de exportação e emissão de relatório técnico e executivo.		
2.1.3.9.4. Realizar a gravação de histórico de todos os eventos ocorridos (inclusão, exclusão, alteração e outros), nas trilhas de auditoria.		
2.1.3.9.5. Reter dados durante o período de tempo determinado pelo SERPRO para fins de auditoria.		
2.1.3.9.6. A gravação e armazenamento das informações de auditoria não podem sofrer descontinuidade, interrupção ou anomalias em função de problemas humanos, técnicos ou qualquer outra razão que pudesse ser evitada pelos		
2.1.3.9.7. Criar e manter logs para consulta online com as atividades do usuário como ação realizada, data, hora, evento, entre outros enquanto aquele registro se encontrar disponível para consultas e auditorias.		
2.1.3.10. Requisitos Relacionados a Manutenção e Evolução da Solução		

2.1.3.10.1. Garantir a atualização legal e tecnológica com novas versões, pelo prazo de vigência do contrato, para todos os produtos fornecidos e instalados, de acordo com o objeto, contados a partir da data de aceite da solução. Durante esse período, deverá ser assegurada a atualização de versões dos itens que compõem a solução ofertada, na medida em que novas versões forem disponibilizadas pelo fabricante.		
2.1.3.10.1.1. A manutenção de caráter legal é aquela necessária para ajustar a solução CONTRATADA a alterações de dispositivos legais que afetem o sistema.		
2.1.3.10.1.2. A manutenção de caráter legal está inclusa no suporte do software contratado, abrangendo toda e qualquer alteração no sistema que porventura venha a ser exigida por órgãos regulamentadores e demande adequação no sistema, devendo ser executada pela CONTRATADA sem qualquer ônus adicional para o SERPRO.		
2.1.3.10.2. A infraestrutura disponibilizada deve ser facilmente escalável para atender as necessidades de crescimento da solução, e deve ser possível sem a necessidade de alteração em código-fonte.		
2.1.3.10.3. Garantir a correção de erros e inconsistências durante a vigência do contrato.		
2.1.3.10.4. Prover atualizações de versões, correções de bugs, funcionalidades e suporte técnico, garantindo desta forma ao SERPRO, os benefícios de novas versões disponibilizadas pelo fabricante da solução.		
2.1.3.11. Requisitos Relacionados à Segurança.		
2.1.3.11.1. A arquitetura deverá possuir todos os componentes necessários à garantia da segurança (integridade, acessibilidade, disponibilidade) da plataforma dos dados.		
2.1.3.11.2. Utilizar criptografia para enviar informações sensíveis, seja através da Internet ou outra rede pública.		
2.1.3.11.3. A Solução deve permitir a criptografia automática de dados e objetos armazenados usando AES (Advanced Encryption Standard) de, no mínimo, 256 bits ou outro algoritmo com força de chave equivalente ou superior, neste último caso desde que aprovado pelo SERPRO.		
2.1.3.11.4. [SE NA MODALIDADE SAAS] Fornecer mecanismo de criptografia padrão NIST (National Institute of Standard Technology) para o tráfego de informações entre suas camadas e armazenamento em SGBD.		
2.1.3.11.5. Suportar no mínimo o protocolo SSL 128 bits para criptografia.		
2.1.3.11.6. O uso dos dados de indivíduos no contexto da solução deve seguir os requisitos de privacidade estabelecidos na Lei Geral de Proteção de Dados Pessoais (Lei 13709/2018 - http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm).		
2.1.3.11.7. [SE NA MODALIDADE SAAS] O Sistema deverá garantir a confidencialidade dos dados armazenados através do uso de criptografia.		
2.1.3.11.8. [SE NA MODALIDADE SAAS] Possuir mecanismos de segurança para garantir que dados sensíveis não sejam copiados de um ambiente para outro, porém mantendo a integridade das informações na base de dados de destino.		
2.1.3.11.9. Garantir o uso de criptografia SSL/TLS 128 bits nas páginas autenticadas.		

2.1.3.12. [SE NA MODALIDADE SAAS] Requisitos Relacionados a Disponibilidade da Solução			
2.1.3.12.1. Possuir disponibilidade de 7 (sete) dias na semana, 24 (vinte e quatro) horas por dia.			
2.1.3.12.2. Disponibilidade do serviço será de no mínimo de 96% (noventa e seis por cento) do tempo durante cada mês.			
2.1.3.12.3. Tempo médio das funcionalidades da solução deve ser menor que 3 segundos.			
2.1.3.13. Requisitos Relacionados a Usabilidade.			
2.1.3.13.1. Toda a solução deve estar disponível no idioma português (PT-BR).			
2.1.3.13.2. Fornecer, em português (PT-BR), manuais do usuário, tutoriais e bases de exemplo, em meio digital (on-line ou arquivos), referentes a todos os módulos da solução.			
2.1.3.13.3. Permitir que uma única transação executada pelo usuário desencadeie todas as ações a ela pertinentes, ou seja, processos totalmente integrados entre si em processamento online, ainda que tais processos tenham desdobramentos que exijam interface com outras soluções.			
2.1.3.13.4. Ter possibilidade de imprimir, enviar e exportar dados nos formatos PDF, XLS e CSV.			
2.1.3.13.5. Permitir anexar arquivos no mínimo, mas não limitado a estes, nos formatos: PDF, TXT, XLS, ODS, DOCX, ODT, PPTX, ODP, JPG, PNG, ZIP, RAR e TXT.			
2.1.3.13.6. A Solução deve ter capacidade de realizar download de arquivos previamente anexados.			
2.1.3.13.7. Permitir a personalização do layout do relatório (ex.: inserção de tabelas, imagens, etc.).			
2.1.3.13.8. Disponibilizar exportação de dados dos relatórios em padrões compatíveis com mercado, no mínimo .xls, .pdf e			
2.1.3.14. [SE NA MODALIDADE SAAS] Requisitos de Backup			
2.1.3.14.1. Deverá ser realizado backup diário, semanal e mensal da solução de forma incremental e completa.			
2.1.3.14.2. Possuir mecanismo de Backup e Restore de todos os dados e metadados contidos na Solução, independentemente da tecnologia utilizada para armazenamento (SGBD, Filesystem, entre outros).			