

# **CONSULTA PÚBLICA PARA CONTRATAÇÃO DE SERVIÇO DE SOLUÇÃO DE SOFTWARE DE GOVERNANÇA, RISCO E CONFORMIDADE**

## **1.0 Objeto**

Contratação de Serviço de Solução de Software de Governança, Riscos, Conformidade e Continuidade.

## **2.0 Especificação do Objeto**

2.1. O Serviço de Solução de Software de Governança, Riscos, Conformidade e Continuidade com fornecimento mediante assinatura básica inicial, deve ser fornecido na forma de uma plataforma de tecnologia para dar suporte a todas as iniciativas do SERPRO que envolvam a implementação de gestão de riscos corporativos e de ativos de TI, gestão de conformidade a normativos de mercado e internos, gestão da continuidade dos negócios, permitir a criação de fluxos de trabalho, notificações, integrações com produtos de terceiros via acesso a dados estruturados e customização de *layout*, campos, fórmulas, painéis de indicadores e relatórios, bem como subsidiar a Governança Corporativa de TI e de Segurança da Informação.

2.1.1. Entende-se por Assinatura Básica Inicial os serviços compostos por todos os requisitos básicos de negócios para disponibilizar, configurar e parametrizar o Serviço de Solução de Software de Governança, Riscos, Conformidade e Continuidade.

### **2.1.2. Requisitos Gerais do Serviço:**

2.1.2.1. Dever ser baseada em plataforma Web, sem a necessidade de instalação de aplicações cliente (modelo *client/server*).

2.1.2.2. O serviço deve estar licenciado para um mínimo de 200 usuários e permitir o uso simultâneo de, no mínimo, 100 usuários.

2.1.1.4. A CONTRATADA deve disponibilizar para o SERPRO, quando disponível, todas as atualizações de versões e releases e efetuar a atualização do serviço.

2.1.2.5. Para a instalação do serviço, o SERPRO disponibilizara a infraestrutura de hardware e softwares básicos (sistema operacional e sistema gerenciador de banco de dados) em umas das seguintes plataformas:

2.1.2.5.1. Sistemas Operacional:

2.1.2.5.1.1. Red Hat Enterprise Linux;

2.1.2.5.1.2. CentOS Linux;

2.1.2.5.1.3. Windows Server.

2.1.2.5.2. Sistema gerenciador de banco de dados:

2.1.2.5.2.1. SQLServer;

2.1.2.5.2.2. PostgreSQL;

2.1.2.5.2.3. Oracle.

2.1.2.6. No caso do serviço de solução ser composta por módulos, os mesmos devem

ser integrados entre si e serem do mesmo fabricante.

2.1.2.7. Todas as características abrangidas na solução devem ser funcionalidades do software ofertado, não havendo necessidade de instalação de outros produtos para criação de relatórios, *dashboard*, conectores, mobile, dentre outras características.

2.1.2.8. Suportar o idioma Português do Brasil.

2.1.2.9. Possibilitar a criação de um painel executivo de indicadores que permita a visualização completa de todas as soluções abrangidas pela plataforma (exemplo: Risco, Conformidade, Auditoria, etc), e que permita a definição de controles de acesso diferenciados a este painel.

2.1.2.10. Permitir a criação de usuários na própria plataforma, incluindo a possibilidade de especificar informações de contatos (e-mails, telefones, cargo, endereço, etc), time zone, língua padrão (Português), e definir a quais grupos e papéis estes usuários pertencem.

2.1.2.11. Permitir a criação de grupos de usuários de tal forma a utilizá-los em outras funções dentro da plataforma, tais como envio de notificações, fluxos de trabalho, controle de acesso, entre outros.

2.1.2.12. Possibilitar a definição de papéis de acesso, incluindo granularidade que permita definir, para cada aplicação que a plataforma possui, os direitos de criar, ler, atualizar e apagar.

2.1.2.13. Permitir a definição de parâmetros de segurança de senhas incluindo, no mínimo, as seguintes opções:

2.1.2.13.1. Tamanho mínimo de senha;

2.1.2.13.2. Obrigatoriedade de uso de caracteres numéricos, letras maiúsculas e caracteres especiais;

2.1.2.13.3. Intervalo para a troca das senhas;

2.1.2.13.4. Definição da quantidade de senhas anteriores que não poderão ser reutilizadas;

2.1.2.13.5. Definição do prazo para envio de lembretes da proximidade da troca das senhas;

2.1.2.13.6. Quantidades de tentativas de senhas erradas;

2.1.2.13.7. Período de bloqueio após sucessivos erros de autenticação;

2.1.2.13.8. Tempo de expiração de sessões;

2.1.2.13.9. Desativação automática de usuários após longo período de inatividade.

2.1.2.14. Permitir a sincronização com bases LDAP genéricas e Microsoft Active Directory, para possibilitar o login na plataforma utilizando usuário/senha da rede e adicionalmente, deverá permitir os seguintes requisitos:

2.1.2.14.1. Definição do domínio e endereço IP do servidor LDAP;

2.1.2.14.2. Definição das credenciais que permitem o acesso às bases LDAP;

2.1.2.14.3. Definição da base DN e do mapeamento de campos, tais como: usuário, primeiro nome, sobrenome, e-mail, telefone, entre outros;

2.1.2.14.4. Definição da frequência de atualização (diária ou semanal), incluindo horário de início e *timezone*;

2.1.2.14.5. Sincronização de usuários específicos de acordo com um critério de seleção de atributo LDAP;

2.1.2.14.6. Criação automática de usuários que pertençam à fonte LDAP, porém não estejam cadastrados na plataforma contratada;

2.1.2.14.7. Desativação automática de usuários que existam na plataforma contratada, porém não existam na fonte LDAP;

2.1.2.14.8. Replicação da estrutura de grupos na plataforma contratada, de acordo com fonte LDAP;

2.1.2.14.9. Histórico do processo de sincronização, incluindo a data de execução e quantidades de contas e grupos criados/desativados/reactivados, além do total de falhas e detalhamento destas.

2.1.2.15. Permitir gerar relatórios referentes a controle de acesso à plataforma contratada, com no mínimo os seguintes requisitos:

2.1.2.15.1. Relação de direitos de acesso, filtrados por papéis por aplicações específicas da plataforma;

2.1.2.15.2. Relação de falhas de login;

2.1.2.15.3. Relação de logins de usuários bloqueados;

2.1.2.15.4. Relação de eventos de segurança relativos à plataforma, incluindo, no mínimo:

2.1.2.15.4.1. Importação de dados;

2.1.2.15.4.2. Login/logout, criação/deleção/modificação de perfis de acesso, usuários, grupos;

2.1.2.15.4.3. Modificação de parâmetros de segurança de senhas;

2.1.2.15.4.4. Modificação de parâmetros LDAP, deleção dos próprios eventos de segurança, entre outras atividades administrativas, de tal forma a manter uma trilha de auditoria da administração da plataforma.

2.1.2.15.5. Permitir a exportação dos relatórios nos seguintes formatos (no mínimo): RTF, PDF, Excel, CSV, HTML.

2.1.2.16. Possibilitar a customização da identidade visual da plataforma através das seguintes requisitos:

2.1.2.16.1. Customização do cabeçalho da página, permitindo a utilização de cores sólidas, degradê ou imagens;

2.1.2.16.2. Utilização de logotipo personalizado;

2.1.2.16.3. Possibilidade de customização de quaisquer aspectos como cores das abas, fontes, botões, menus na plataforma contratada;

2.1.2.16.4. Esta customização deverá ser realizada através de interface intuitiva, sem a necessidade de desenvolvimento.

2.1.2.17. Possibilitar a customização de telas, funcionalidades e consultas parametrizáveis sem necessidade de programação e custos adicionais, com as seguintes requisitos:

2.1.2.17.1. Fórmulas e cálculos personalizáveis;

2.1.2.17.2. Matriz de risco;

2.1.2.17.3. Criação de objetos de layout tais como: abas, sessões, campo texto pré-formatado, objetos customizáveis e gráficos de tendências;

2.1.2.17.4. Aplicação de *layouts* condicionais, isto é, dependendo do valor de um campo específico, pode-se exibir ou esconder uma determinada porção do *layout* (sessão ou campos específicos), de acordo com a necessidade;

2.1.2.17.5. Possibilidade de filtragem da exibição de valores constantes nos campos (qualquer campo), de acordo com um critério específico;

2.1.2.17.6. Possibilidade de gerar uma notificação a partir da seleção de um determinado valor de um campo.

2.1.2.18. Permitir a especificação de fluxos de trabalho, de forma independente, entre as diversas aplicações que compõem a plataforma selecionada. A definição do fluxo de trabalho deverá permitir criar vários estágios, sem limite de quantidade, com a

possibilidade de criação de regras de avaliação de campos e associação de usuários ou grupos dependendo do resultado da avaliação destas regras.

2.1.2.19. Permitir criar campos calculados que apresentem resultados a partir de fórmulas personalizadas. O editor de fórmulas deverá permitir a utilização de quaisquer campos preexistentes (incluindo aqueles criados pelo administrador) e deverá validar as fórmulas à procura de inconsistências. Adicionalmente, o editor de fórmulas deverá ter uma seção de ajuda que mostre o descritivo e exemplos para cada função utilizada.

2.1.2.20. Prover motor para cálculo de indicadores com no mínimo funções matemáticas, lógicas e de texto;

2.1.2.21. Possibilitar a exibição dos resultados das fórmulas aplicadas em formato texto ou através da utilização de imagens (arquivos GIF, BMP, JPG ou PNG) permitindo, desta forma, apresentar os resultados de forma mais intuitiva. Exemplos: semáforos coloridos de cores vermelha, laranja e verde, ao invés do uso de textos simples como "Alta", "Média" e "Baixa". Adicionalmente, deverá permitir a inclusão de novas imagens (arquivos GIF, BMP, JPG ou PNG) para utilização na exibição dos resultados de campos calculados.

2.1.2.22. Permitir a criação de questionários dentro da plataforma contratada. Estes questionários deverão possuir, no mínimo, as seguintes requisitos:

2.1.2.22.1. Definição do texto da questão;

2.1.2.22.2. Definição do peso da questão;

2.1.2.22.3. Definição da categoria;

2.1.2.22.4. Definição das respostas possíveis;

2.1.2.22.5. Vínculo da questão a documentos de referência;

2.1.2.22.6. Permitir o envio para pessoas que não são necessariamente usuários da aplicação;

2.1.2.22.7. Permitir customização de identidade visual;

2.1.2.22.8. Exibição das alternativas das respostas através do uso de campos *dropdown* (escolha de somente uma opção), *radio buttons* (escolha de somente uma opção), *check boxes* (uma ou mais opções) ou *listbox* (uma ou mais opções);

2.1.2.22.9. Permitir anexação de documentos em diversos formatos;

2.1.2.22.10. Controlar o acompanhamento das respostas incluindo prazos, quantidade de pessoas que responderam, identificação dos respondentes;

2.1.2.22.11. Possibilitar configuração de lembretes, alertas e alarmes;

2.1.2.22.12. Permitir respostas on-line e off-line.

2.1.2.23. Possibilitar o empacotamento da aplicação para permitir o uso em outra infraestrutura da plataforma contratada, caso seja necessário.

2.1.2.24. Permitir a integração com outros sistemas através da importação e exportação de dados estruturados, através dos seguintes métodos:

2.1.2.24.1. Arquivos CSV;

2.1.2.24.2. Arquivos XML.

2.1.2.25. Permitir a criação de relatórios customizados a partir de *templates* de arquivos.

2.1.2.25.1. Estes *templates* deverão permitir a definição de rodapés, logotipo, identidade visual, e conteúdo variável (tabelas ou gráficos), em layouts 100% customizáveis.

- 2.1.2.26. Permitir a disponibilização de relatórios por via de serviços Web para incorporação em outras páginas Web.
- 2.1.2.27. Permitir a criação de relatórios customizados, a partir da execução de consultas nas bases de dados com exibição em formato de tabela, gráfico, *dashboards* customizáveis, etc.
- 2.1.2.28. Permitir a consulta e emissão de relatórios a partir de um determinado ativo e seu histórico de utilizações nos módulos da solução.
- 2.1.2.29. Possibilitar a criação de *dashboards* diferentes de acordo com as funcionalidades contratadas.
- 2.1.2.30. Possibilitar o controle de acesso aos relatórios e *dashboards* através da definição de grupos/usuários.
- 2.1.2.31. Possibilitar a criação de campanhas de treinamento e conscientização dentro da plataforma contratada com, no mínimo, as seguintes características:
- 2.1.2.31.1. Definição de um texto explicativo a respeito da campanha em questão e inclusão de questionários para verificação do entendimento dos usuários;
  - 2.1.2.31.2. Definição do período de aplicação da campanha de conscientização, incluindo a possibilidade de envio de lembretes e permissão para pular perguntas do questionário;
  - 2.1.2.31.3. Definição dos destinatários das campanhas de conscientização.
- 2.1.2.32. Permitir acompanhar os resultados das campanhas de conscientização através da geração de relatórios que mostrem o controle das respostas por usuários, incluindo o tipo e data das respostas.
- 2.1.2.33. Permitir criar *dashboards* customizados, com possibilidade de ajustar tamanho dos gráficos de indicadores, incluindo o rearranjo destes gráficos, de acordo com a necessidade.
- 2.1.2.34. Possibilitar a criação de vários *dashboards* diferentes de acordo com as funcionalidades contratadas. Exemplo: Risco, Conformidade, Políticas, Incidentes, etc, cada um com seu próprio *dashboard*.
- 2.1.2.35. Permitir a visualização gráfica do relacionamento entre os diversos objetos que compõem uma determinada informação. Exemplo: A partir de um incidente, deverá ser possível observar o relacionamento deste incidente com unidades de negócio, investigações, tarefas, planos de remediação, registros de risco, etc, de maneira visual (diagrama).
- 2.1.2.36. A ferramenta de visualização gráfica do relacionamento entre os objetos deverá permitir a escolha de trechos do diagrama através de uma janela minimizada de visualização. Esta mesma janela também deverá permitir o zoom para aumentar ou diminuir detalhes sobre os objetos que compõem o diagrama.
- 2.1.2.37. Permitir a inclusão, manutenção e exclusão de objetos e seus atributos/características com pelo menos 5 (cinco) níveis hierárquicos, assim como a vinculação de objetos a outros objetos, como, por exemplo, unidades, processos, produtos, serviços, objetivos corporativos, indicadores, ativos de TI, vulnerabilidades, ameaças, riscos, controles, e seus atributos.

2.1.2.38. A ferramenta de visualização gráfica do relacionamento entre os objetos deverá permitir o *drill down* em cada um dos objetos que compõem o diagrama. Ao clicar em um objeto, deverá ser possível expandir a visualização de tal a forma a permitir a inclusão de novos subitens (objetos do diagrama).

2.1.2.39. Em relação à visualização gráfica do relacionamento entre os objetos, deve-se permitir a visualização dos objetos da seguinte forma:

2.1.2.39.1. Hierárquica;

2.1.2.39.2. Circular;

2.1.2.39.3. Dirigida.

2.1.2.40. Possuir logs (eventos), possibilitando a auditoria em todas as partes da Solução, armazenando as credenciais dos usuários responsáveis por modificação e/ou ação realizada na solução (inclusive, mas não limitado à emissão de relatórios, análises, modificação de normas e processos).

### **2.1.3. Módulo de Gestão de Governança e Conformidade**

#### **2.1.3.1. Estrutura Organizacional**

2.1.3.1.1. Permitir a inclusão de informações relativas a Perfil da Empresa.

2.1.3.1.1.1. Deve permitir a inclusão de informações relativas a identificação da Empresa, sua estrutura organizacional, processos, instalações, ativos, produtos, serviços e aplicações.

2.1.3.1.1.2. As informações de estrutura devem servir para garantir a segmentação do acesso à informação bem como para agrupamento de informações, emissão de relatórios, consultas, etc.

2.1.3.1.2. Permitir a inclusão de informações relativas a Processos de Negócios. Deve-se incluir, no mínimo, as seguintes características: tipo de processo, objetivo de negócio, descrição, *rating* de criticidade, gestores do processo de negócios, e ligação com Análise de Impacto de Negócios (BIA), contexto de negócios e infraestrutura (aplicações e dispositivos).

2.1.3.1.3. Permitir a inclusão de informações relativas a Contatos. Deve-se incluir, no mínimo, as seguintes características: nome completo, primeiro nome, sobrenome, título, departamento, unidade de negócios, hierarquia, tipo, endereço completo (incluindo possibilidade de especificar coordenadas para georreferenciamento), e papel em BIA (*Business Impact Analysis*), gestão de riscos e continuidade de negócios.

2.1.3.1.4. Permitir a inclusão de informações relativas a Objetivos Corporativos incluindo, no mínimo, as seguintes informações:

2.1.3.1.4.1. Nome do objetivo;

2.1.3.1.4.2. Categoria (exemplo: operacional, estratégico, etc);

2.1.3.1.4.3. Usuário que criou o objetivo;

2.1.3.1.4.4. Status deste objetivo (ativo, inativo, etc);

2.1.3.1.4.5. Associação do objetivo corporativo com políticas específicas;

2.1.3.1.4.6. Associação do objetivo corporativo com riscos identificados e cadastrados;

2.1.3.1.4.7. Associação do objetivo corporativo com indicadores de *performance* (KPI).

2.1.3.1.5. Permitir a inclusão de informações relativas a Produtos e Serviços, com no mínimo, as seguintes características: descrição, *rating* de conformidade, informações sobre impacto para clientes, relação de gestores, contatos e ligação com processos de negócios, infraestrutura (aplicações e dispositivos).

2.1.3.1.6. Permitir a inclusão de informações relativas a Instalações, com no mínimo, as seguintes características: descrição, *rating* de criticidade, tipo de localidade, gestores, localização (incluindo possibilidade de especificar coordenadas para georreferenciamento), contatos e contexto de negócios e infraestrutura (processos de negócios, dispositivos, fornecedores).

2.1.3.1.7. Permitir a inclusão de informações relativas a Dispositivos, com no mínimo, as seguintes características: descrição, categoria, departamento, *rating* de risco/conformidade/criticidade, gestores, detalhes tecnológicos (ex.: número serial, modelo, fabricante, entre outros), e ligação com contexto de negócios e infraestrutura (processos de negócios, aplicações, localidades).

2.1.3.1.8. Permitir a inclusão de informações relativas a Aplicações, com no mínimo, as seguintes características: descrição, tipo de aplicação, tempo esperado de recuperação (RTO), objetivo de ponto de recuperação (RPO), *rating* de criticidade, gestores, detalhes de licenciamento, contatos e contexto de negócios e infraestrutura (processos de negócios, localidades).

### **2.1.3.2. Documentos de Referência (Normas, Padrões, Políticas Corporativas)**

2.1.3.2.1. Fornecer conteúdo de, no mínimo, os seguintes documentos de referência: ISO22301, ISO 22313, Cloud Security Alliance, Cobit 4.1 e 5, família ISO 27000, ITIL, NIST SP 800, PCI, Sarbanes-Oxley, SABSA, GDPR, ISO19.600, normas complementares DSIC/GSI/PR, ABNT 14276, ABNT 15219, NR20.

2.1.3.2.1. Possibilitar a inclusão de novos documentos de referência manualmente ou através da importação de arquivos.

2.1.3.2.2. Permitir referência cruzada entre itens e subitens de documentos de referência.

2.1.3.2.3. Documentos nativos devem ser mantidos atualizados sem custo adicional.

### **2.1.3.3. Planos de Ação**

2.1.3.3.1. A solução deve possibilitar a criação e gestão de Planos de Ação, de tal forma a permitir o acompanhamento de tarefas necessárias para mitigação dos apontamentos descobertos e a documentação das ações.

2.1.3.3.2. Os Planos de Ação deverão possibilitar o acompanhamento de correções para as seguintes funcionalidades, dentro da mesma aplicação: controles, recomendações e sugestões.

2.1.3.3.3. As ações devem possuir responsável, prazo e permitir o envio de alertas e alarmes configuráveis.

2.1.3.3.4. A solução deve emitir notificação de ação para o responsável.

2.1.3.3.5. A solução deve permitir a priorização das ações.

## **2.1.4. Módulo de Gestão de Riscos e Vulnerabilidades**

### **2.1.4.1. Gestão de Riscos**

2.1.4.1.1. Permitir implementar as fases ou etapas de Gestão de Riscos definidas na Norma ISO 27005.

2.1.4.1.2. Permitir a criação de projetos de Risco com, no mínimo, os seguintes requisitos:

2.1.4.1.2.1. Nome e descrição do projeto, datas esperadas e reais de início e término, além de definição dos profissionais envolvidos no projeto;

2.1.4.1.2.2. Definição do escopo do projeto de Risco (aplicações, processos de negócios, dispositivos, localidades, terceiros, etc);

2.1.4.1.2.3. Levantar nível de probabilidade, nível de impacto e nível de risco;

2.1.4.1.2.4. Suportar a criação de Plano de Ações, permitindo a definição de controles, ações, prazos e responsáveis por ação;

2.1.4.1.2.5. Permitir a priorização das ações do plano;

2.1.4.1.2.6. Permitir o acompanhamento do progresso das ações com identificação do seu status;

2.1.4.1.2.7. Permitir que a etapa de tratamento seja feita em ferramenta externa de gestão de projetos por meio da importação e exportação das ações nos formatos .CSV e .XLS;

2.1.4.1.2.8. Definição do nível de risco geral final, incluindo as seguintes informações: participantes, *overview* do risco, data de finalização da análise de risco, status da análise, atribuição final de probabilidade e impacto e nível final geral de risco;

2.1.4.1.2.9. Estabelecimento de uma ligação entre o projeto de risco e Planos de Ação.

2.1.4.1.3. Possibilitar a criação de Análises de Risco que incluam, no mínimo, os seguintes requisitos:

2.1.4.1.3.1. Definição do nome do projeto, aplicações envolvidas, processos de negócios, unidades de negócios, dispositivos e localidades. Ao atrelar qualquer um destes itens, a plataforma deverá, automaticamente, selecionar um conjunto de questionários focados, que poderão ser parametrizáveis caso seja necessário, sem necessidade de desenvolvimento de código;

2.1.4.1.3.2. Status, responsável pela análise, data limite para término, informações de revisão, além de um resumo do nível geral de risco e mapa de calor;

2.1.4.1.3.3. Definição de perguntas, parametrizáveis e sem a necessidade de desenvolvimento de código;

2.1.4.1.3.4. Questionário pré-definido para avaliação de risco em aplicações;

2.1.4.1.3.5. Questionário pré-definido para análise de impacto ao negócio;

2.1.4.1.3.6. Questionário pré-definido para avaliação de risco em Processos de Negócio;

2.1.4.1.3.7. Questionário pré-definido para avaliação de risco em Unidades de Negócio;

2.1.4.1.3.8. Questionário pré-definido para avaliação de risco em Dispositivos;

2.1.4.1.3.9. Questionário pré-definido para avaliação da Gestão de Riscos da Empresa;

2.1.4.1.3.10. Questionário pré-definido para avaliação de risco em Questões Ambientais;

2.1.4.1.3.11. Questionário pré-definido para avaliação de risco em Localidade Física;

2.1.4.1.3.12. Questionário pré-definido para avaliação de risco das Informações;

2.1.4.1.3.13. Questionário pré-definido para avaliação de risco da Segurança da



Informação;

2.1.4.1.3.14. Questionário pré-definido para avaliação de riscos associados a Privacidade;

2.1.4.1.3.15. Questionário pré-definido para avaliação de risco em Projetos.

2.1.4.1.4. Análise e avaliação com uso de questionários com conexão a documentos de referência, envio aos respondentes definidos e consolidação das respostas recebidas.

2.1.4.1.5. Análise e avaliação sem uso de questionários com identificação de riscos de forma livre, sem obrigatoriedade de vinculação a controles cadastrados, permitindo a avaliação qualitativa para a estimativa do risco.

2.1.4.1.6. Possibilitar a inclusão de novas perguntas manualmente ou através da importação de arquivos em formato texto (CSV, XML).

2.1.4.1.6.1. O conteúdo de cada questão deverá ser composto no mínimo por Nome da pergunta, status, categoria, texto descritivo da pergunta, tipo de questão, formato de exibição, texto de ajuda.

2.1.4.1.7. Permitir definir a ordem de exibição das opções das perguntas, peso, layout de exibição, quantidades mínimas e máxima de seleções, associações com Fontes Autoritativas e Padrões de Controle, definição de respostas certas e erradas, além de permitir identificar a quais questionários a questão está associada.

2.1.4.1.8. Enviar um lembrete e notificações de escalonamento conforme a data final de uma avaliação se aproxima;

2.1.4.1.9. Aceitar anexos obrigatórios e opcionais;

2.1.4.1.10. Suportar ajuda on-line para os participantes da avaliação/pesquisa;

2.1.4.1.11. Suportar pesquisas dinâmicas (perguntas seguintes são determinadas pela resposta anterior);

2.1.4.1.12. Disponibilizar um *dashboard* que permita a visualização da aderência às diversas normativas.

#### **2.1.4.2. Gestão de Vulnerabilidades**

2.1.4.2.1. Permitir cadastrar requisições de *scans* de vulnerabilidades, com no mínimo, as seguintes informações:

2.1.4.2.1.1. Requisitante;

2.1.4.2.1.2. Data de Criação da requisição;

2.1.4.2.1.4. Gestor do requisitante;

2.1.4.2.1.4. *e-mail* do requisitante;

2.1.4.2.1.5. Departamento;

2.1.4.2.1.6. Informações sobre a requisição como Data limite para realização do *scan*;

2.1.4.2.1.7. Prioridade;

2.1.4.2.1.8. Endereço IP ou faixa de endereços IP;

2.1.4.2.1.9. Data de início e término dos *scans*;

2.1.4.2.1.10. Tipo do *scan* (ex.: teste de invasão, *network scanner*, etc).

2.1.4.2.2. Permitir cadastrar informações sobre os *scans* de vulnerabilidades com, no mínimo, as seguintes informações:

- 2.1.4.2.2.1. Nome do *scan*;
- 2.1.4.2.2.2. Descrição;
- 2.1.4.2.2.3. Gestor responsável pelos testes;
- 2.1.4.2.2.4. Recorrência do *scan*;
- 2.1.4.2.2.5. Ferramenta a ser utilizada (ex.: Qualys, Retina, etc);
- 2.1.4.2.2.6. Data de início e término do *scan*;
- 2.1.4.2.2.7. Escopo do *scan*: dispositivos afetados, aplicações, localidade, unidades de negócio, faixa de endereços IP e equipamentos envolvidos.

2.1.4.2.3. Fornecer um conjunto de relatórios predefinidos (por exemplo, vulnerabilidades por nível de severidade ou tipo, código malicioso por tipo, tarefas de correção por status etc.).

2.1.4.2.4. Oferecer a capacidade para produzir relatórios específicos para visualizar ameaças por tecnologia, severidade, tipo e impacto na organização.

2.1.4.2.5. Permitir a criação de indicadores relacionados a vulnerabilidades, atrelando-os a contexto corporativo ou de negócios.

2.1.4.2.6. Permitir a criação de planos de ação, a partir de vulnerabilidades específicas identificadas no ambiente, com no mínimo, as seguintes informações:

- 2.1.4.2.6.1. Responsável(eis) pela ação;
- 2.1.4.2.6.2. Informações sobre as vulnerabilidades;
- 2.1.4.2.6.3. Informações sobre as correções;
- 2.1.4.2.6.4. Prazo de correção.

2.1.4.2.7. Ser agnóstico em relação a *scanners* de vulnerabilidades e permitir a importação de resultados de *scans* tais como: Qualys, Foundstone, AVDS, Rapid7, etc, sem a necessidade de programação.

2.1.4.2.8. Suportar nativamente, no mínimo, as seguintes tecnologias de *scans* de vulnerabilidades:

- 2.1.4.2.8.1. Qualys Vulnerability Management;
- 2.1.4.2.8.2. McAfee Vulnerability Manager;
- 2.1.4.2.8.3. Security Sentinel;
- 2.1.4.2.8.4. Rapid7 Nexpose;
- 2.1.4.2.8.5. Veracode SecurityReview;
- 2.1.4.2.8.6. Core Security;
- 2.1.4.2.8.7. BeyoundTrust Retina CS;
- 2.1.4.2.8.8. AVDS.

2.1.4.2.9. Em relação às informações de vulnerabilidades importadas das ferramentas de *scan*, deve-se permitir a coleta, no mínimo, das seguintes informações:

- 2.1.4.2.9.1. Origem da informação (associada à ferramenta de *scan* utilizada);
- 2.1.4.2.9.2. Nome do dispositivo afetado;
- 2.1.4.2.9.3. Endereço IP;
- 2.1.4.2.9.4. *Hostname*;
- 2.1.4.2.9.5. Sistema operacional;
- 2.1.4.2.9.6. NETBIOS;
- 2.1.4.2.9.7. Datas nas quais a vulnerabilidade foi encontrada pela primeira e última vezes;
- 2.1.4.2.9.8. Tipo de resposta associada (aceitar risco ou remediar);
- 2.1.4.2.9.9. ID da vulnerabilidade;
- 2.1.4.2.9.10. Severidade;

- 2.1.4.2.9.11. Categoria;
- 2.1.4.2.9.12. ID Bugtraq;
- 2.1.4.2.9.13. CVSS score;
- 2.1.4.2.9.14. CVE ID;
- 2.1.4.2.9.15. Nome da vulnerabilidade;
- 2.1.4.2.9.16. Descrição;
- 2.1.4.2.9.17. Impacto e solução.

2.1.4.2.10. Permitir integração com outras ferramentas de *scan* de vulnerabilidades que não sejam nativamente suportadas, através da importação de dados estruturados gerados por elas. A Solução deverá permitir a importação de dados, no mínimo, através dos seguintes métodos:

2.1.4.2.10.1. Arquivos CSV - Deve permitir a importação de arquivos delimitados (CSV). Também deverá permitir a definição dos delimitadores de registros, de campos, de listas, além da possibilidade de definir sequências de "escapes". A plataforma deverá permitir a definição da sequência numérica de registros que poderão ser ignorados durante a importação;

2.1.4.2.10.2. Arquivos XML – Deve permitir a importação de arquivos XML e deverá permitir a utilização de definições XSLT, que possibilitam realizar transformações no arquivo XML original;

2.1.4.2.10.3. Obtenção de arquivos, no mínimo, através dos protocolos HTTP, FTP, Consultas diretas a Bancos de Dados (exemplo: Oracle, SQL Server, etc).

## **2.1.5. Módulo de Gestão de Continuidade de Negócios**

### **2.1.5.1. Gestão de Continuidade**

2.1.5.1.1. As funcionalidades de Gestão de Continuidade de Negócio devem permitir implementar as fases ou etapas definidas nas Normas ISO 22313 e ISO 22301;

2.1.5.1.2. Possibilitar a exportação dos documentos gerados neste módulo em formatos .CSV, .DOC e .PDF;

2.1.5.1.3. Possibilitar a anexação de arquivos de qualquer tipo aos documentos gerados neste módulo.

### **2.1.5.2. Gestão de BIA (Business Impact Analysis)**

2.1.5.2.1. Permitir a criação, revisão e acompanhamento de Documentos de Análise de Impacto (BIA) com as seguintes informações:

2.1.5.2.1.1. Nome e descrição do projeto, datas esperadas e reais de início e término, além de definição dos profissionais envolvidos no projeto;

2.1.5.2.1.2. Possibilidade de definição do escopo do projeto incluindo quais aplicações, objetivos corporativos, processos de negócio, dispositivos, localidades, terceiros, etc., podem ser incluídos no projeto;

2.1.5.2.1.3. Estabelecer a conexão entre o projeto e os questionários de BIA.

2.1.5.2.2. Permitir criar questionário de BIA customizável.

2.1.5.2.3. Permitir o envio, notificação de envio, acompanhamento e consolidação das respostas ao questionário.

2.1.5.2.4. Permitir consultas e emissão de relatórios individuais de BIA dos serviços e processos.

2.1.5.2.5. Permitir a priorização dos serviços e processos com base nos questionários do BIA.

2.1.5.2.6. Permitir o registro da estratégia de continuidade para cada serviço ou processo com base no resultado do BIA e Análise de Riscos.

### **2.1.5.3. Planos de Continuidade de Negócios**

2.1.5.3.1. Permitir cadastrar os Riscos associados a Continuidade de Negócios com, no mínimo, as seguintes informações:

2.1.5.3.1.1. Nome do risco, categoria, proprietário, descrição, além da definição de Processos de Negócios, Produtos e Serviços, Localidades, Aplicações e Dispositivos afetados pelo risco;

2.1.5.3.1.2. Avaliação de Impacto/Probabilidade e impacto ao longo do tempo (parametrizável);

2.1.5.3.1.3. Definição de Controles Mitigatórios;

2.1.5.3.1.4. Estabelecimento de conexão entre os riscos identificados e os Planos de Continuidade;

2.1.5.3.1.5. Estabelecimento de conexão entre os riscos identificados e eventos de crise;

2.1.5.3.1.6. Possibilitar a criação, revisão e acompanhamento de Documentos de Plano de Continuidade de Negócios, com as seguintes características:

2.1.5.3.1.7. Nome do Plano, tipo, processos de negócios afetados;

2.1.5.3.1.8. Definição de Escopo e Objetivo;

2.1.5.3.1.9. Sequência de atividades e duração estimada;

2.1.5.3.1.10. Definição da equipe de recuperação, incluindo nome, título, telefones, e-mail, etc, além da sequência a ser seguida no acionamento dos profissionais (*Call Tree*).

2.1.5.3.2. Possibilitar a criação e acompanhamento de Testes e Exercícios, que permitam a avaliação da efetividade dos Planos de Continuidade. Dentre as características necessárias, destacam-se:

2.1.5.3.2.1. Armazenamento do histórico de testes realizados para cada Plano de Continuidade com o intuito de avaliar a sua adequação;

2.1.5.3.2.2. Definição de notificações a serem enviadas aos envolvidos. As notificações deverão ser compostas pelo iniciador, pessoas envolvidas (incluindo nome, telefone e e-mail) e a mensagem. Adicionalmente, a plataforma deverá manter um histórico de envio de notificações.

2.1.5.3.2.3. Acompanhar o percentual de execução das atividades do Plano;

2.1.5.3.2.4. O acompanhamento das atividades de um Plano deverá permitir a visualização por Estratégias de Recuperação, de tal forma a permitir identificar em qual ponto o processo está adiantado/atrasado;

2.1.5.3.2.5. Atestação da efetividade do plano.

2.1.5.3.3. Deverá permitir o uso de aplicativo mobile para acesso aos planos de forma *off-line* por todos os empregados sem a necessidade de compra de licenças mobile para esse fim.

## **2.2. Prazo para início da prestação de serviço.**

2.2.1. A CONTRATADA deve disponibilizar, instalar, Configurar e Parametrizar o serviço na infraestrutura do SERPRO em até 60 (sessenta) dias corridos após a data de início da vigência do contrato.

2.2.2. A CONTRATADA deverá prover todos os serviços necessários para a instalação, configuração e testes dos serviços na infraestrutura do SERPRO, de forma a propiciar seu pleno funcionamento.

2.2.2.3. O serviço engloba a instalação, configuração e parametrização de todos os módulos do serviço da solução, internalização do serviço e operação assistida por até 30 (dias) após a disponibilização dos serviços.

2.2.3. A emissão do termo de recebimento definitivo por parte do SERPRO para o início da prestação dos serviços será efetuado em até 10 (deis) dias corridos após o serviço estar integralmente implementado e atendendo a todos os requisitos especificados neste documento.

## **2.3. O serviço deve ser prestado no seguinte endereço:**

2.3.1. Regional Brasília/DF

Endereço: SGAN AV. L2 NORTE, QUADRA 601 MÓDULO "G" - Brasília/DF

CEP: 70.836-900

CNPJ: 33.683.111/0002-80

Inscrição Estadual: 07334743/002-94

Inscrição Municipal: 07334743/002-94

## **3.0 Níveis de serviço e sancionamentos**

3.1. Possuir suporte técnico inerente ao serviço para solução de problemas, resolução de dúvidas e apoio nas atualizações de software, com os seguintes requisitos:

3.1.1. Os atendimentos devem ser prestado de segunda-feira a sexta-feira (exceto feriados), das 08h00 às 18h00 (horário de Brasília).

3.1.2. O atendimento aos chamados deverá obedecer às seguintes classificações quanto ao nível de severidade:

Severidade	Descrição	Tipo de atendimento	Tempo de Atendimento	Tempo de Solução ou Solução de Contorno	Penalidades
1 – Crítica	Chamados referentes a	Remoto	No máximo 2	No máximo 12 (doze) horas úteis	Multa no valor de 1% (um por cento do

	situações de emergência ou problema crítico, caracterizados pela existência de ambiente paralisado e/ou interrupção da solução		(duas) horas úteis após abertura do chamado	após o início do atendimento.	valor total anual dos serviços de solução de software, por hora ou fração de hora de atraso.
2 – Alta	Chamados associados a situações de alto impacto, incluindo os casos de degradação severa de desempenho.	Remoto	No máximo 4 (quatro) horas úteis após abertura do chamado	No máximo 24 (vinte e quatro) horas úteis após o início do atendimento.	Multa no valor de 0,8% (zero vírgula oito por cento) do valor total anual dos serviços de solução de software, por hora ou fração de hora de atraso.
3 – Média	Chamados referentes a situações de baixo impacto ou para aqueles problemas que se apresentem de forma intermitente.	Remoto	No máximo 12 (doze) horas úteis após abertura do chamado	No máximo 48 (quarenta e oito) horas úteis após o início do atendimento.	Multa no valor de 0,6% (zero vírgula seis por cento) do valor total anual dos serviços de solução de software, por hora ou fração de hora de atraso.
4 – Baixa	Chamados com objetivo de sanar dúvidas ao uso.	Remoto	No máximo 24 (vinte e quatro) horas úteis após abertura do chamado	No máximo 72 (setenta e duas) horas úteis após o início do atendimento.	Multa no valor de 0,4% (zero vírgula quatro por cento) do valor total anual dos serviços de solução de software, por hora ou fração de hora de atraso.

3.1.3.1. Tempo de Atendimento é o prazo máximo para início do atendimento a partir da abertura do chamado na CONTRATADA.

3.1.3.2. Tempo de Solução ou Solução de Contorno é o prazo máximo para que a CONTRATADA aplique uma correção definitiva ou solução de contorno após o início do atendimento.

3.1.3.3. A CONTRATADA deverá fornecer informações sobre as correções a serem aplicadas ou a própria correção.

3.1.3.4. A CONTRATADA deverá prover todas as correções e atualizações dos softwares do serviço, que permitam melhorar as funcionalidades dos equipamentos, sem ônus adicional para o SERPRO.

#### 3.1.4. Chamados, Registros e Início de Prazos

3.1.4.1. Será aberto um chamado para cada problema reportado.

3.1.4.2. A abertura do chamado na CONTRATADA pelo SERPRO poderá ser realizado por meio de telefone 0800 e/ou portal na internet.

3.1.4.3. Os prazos para atendimento de chamados de qualquer severidade serão considerados a partir da hora em que o chamado é aberto, isto é, registrado na CONTRATADA, recebendo dela uma identificação para acompanhamento, controle e histórico.

3.1.4.4. Todos os chamados serão controlados por sistema de informação da CONTRATADA.

3.1.4.5. Antes do fechamento de cada chamado a CONTRATADA consultará o SERPRO para validar o fechamento do chamado.

3.1.4.5.1. Um chamado fechado sem anuência do SERPRO ou sem que o problema tenha sido de fato resolvido, será reaberto e os prazos serão contados a partir da abertura original do chamado, inclusive para efeito de aplicação das sanções previstas.

#### 3.1.5. Relatórios sobre a prestação dos serviços

3.1.5.1. A CONTRATADA deverá emitir mensalmente até o 10º (décimo) dia útil, do mês subsequente, um relatório constando os acionamentos técnicos abertos, em andamento e encerrados no período, com no mínimo as seguintes informações: número do contrato, número de acionamento, descrição da ocorrência, severidade, nome do responsável do SERPRO pela abertura do chamado, data e hora de abertura do chamado, data e hora do início do atendimento, data e hora do atendimento local, se for o caso, data e hora de solução ou medida de contorno, e descrição da resolução adotada. O relatório deverá ser entregue mesmo quando não houver chamados no período.

3.1.5.2. A entrega dos relatórios mensais será condição necessária para o SERPRO realizar o recebimento definitivo, para fins de pagamento dos serviços executados.

### **4.0 Especificações de Valores e forma de pagamentos**

4.1. O valor total estimado para esta contratação é de R\$ 0,00 (x reais), assim distribuídos:

4.1.1. O valor estimado para a Assinatura Básica Inicial é de R\$ 0,00 (x reais), conforme tabela abaixo:

<b>Grupo</b>	<b>Item</b>	<b>Descrição</b>	<b>Métrica</b>	<b>Quantidade</b>	<b>Valor Unitário (R\$)</b>	<b>Valor Total (R\$)</b>
1	1	Assinatura Básica Inicial	Única	1		

4.1.2. O valor estimado para Serviço de solução de software é de R\$ 0,00 (x reais), conforme tabela abaixo:

<b>Grupo</b>	<b>Item</b>	<b>Descrição do Módulo</b>	<b>Métrica</b>	<b>Quantidade</b>	<b>Valor Total Mensal (R\$)</b>	<b>Valor Total Anual (R\$)</b>	<b>Valor Total por 36 meses (R\$)</b>
1	2	Módulo de Gestão de Governança e Conformidade	Mensal	1			
	3	Módulo de Gestão de Riscos e Vulnerabilidades	Mensal	1			
	4	Módulo de Gestão de Continuidade de Negócios	Mensal	1			

#### 4.2. Forma e Condições de Pagamento

4.2.1. O pagamento da Assinatura Básica Inicial será em parcela única, no primeiro dia útil após o 20º (vigésimo) dia corrido da data do recebimento definitivo, referente às notas fiscais entregues no protocolo geral do SERPRO ou por meio do endereço eletrônico a ser informado pelo gestor do contrato.

4.2.2. Os pagamentos dos Serviço de Gestão Integrada serão efetuados mensalmente no 1º (primeiro) dia útil, após o 20º (vigésimo) dia corrido da data do recebimento definitivo dos serviços prestados, referente a Nota Fiscal/Fatura entregue no Protocolo Geral do SERPRO ou através do endereço eletrônico a ser informado pelo Gestor do Contrato, condicionado à apresentação de relatório mensal de serviços pela CONTRATADA.

4.2.2.1. O prazo para emissão do recebimento definitivo por parte do Serpro é de 5 (cinco) dias úteis a partir do recebimento da nota fiscal e/ou fatura e da apresentação de relatório mensal de serviços pela CONTRATADA.

4.2.2.2. No primeiro mês de faturamento, o valor deverá ser rateado à base de 1/30 (um trinta avos) do valor da contraprestação mensal, por dia, considerando-se o mês de 30 dias.



4.2.2.3. Nos meses subsequentes, os serviços serão cobrados com base no período de 1 a 30 do mês da efetiva execução dos serviços.

4.2.2.4. No último mês de vigência do contrato o valor deverá ser rateado à base de 1/30 (um trinta avos) do valor da contraprestação mensal, por dia, considerando-se o mês de 30 dias.

5.1. < INTERNO>

## **6.0 Seleção do fornecedor**

6.1. A contratação será na Modalidade de Pregão na forma eletrônica com fulcro no Art. 32, inciso IV, da Lei 13.303/2016 c/c Lei nº 10.520/2002, por se tratar de bens e serviços comuns e ter os padrões de desempenho e qualidade objetivamente definidos, por meio de especificações usuais de mercado.

7.1 <INTERNO>

## **8.0 Gerenciamento contratual**

8.1. A consulta pública eletrônica será acompanhada pelos empregados:

8.1.1. Charles Moraes Magalhães, telefone (61) 2021-7259, e-mail charles.magalhaes@SERPRO.gov.br.

8.1.2. Aparecida Pessoa Coutinho, telefone (61) 2021-8708, e-mail aparecida-pessoa.coutinho@SERPRO.gov.br.

**8.2. As empresas deverão encaminhar para o SERPRO o anexo "A" da consulta pública preenchido, sugestões de melhorias e proposta comercial conforme tabelas dos itens 4.1.1 e 4.1.2.**

8.3. O prazo de vigência inicial do contrato será de 36 (trinta e seis) meses, a partir da data de início da vigência contratual, podendo ser prorrogado até o limite de 60 (sessenta) meses.

8.4. Obrigações da CONTRATADA.

8.4.1. Ao término do contrato a CONTRATADA se obriga a prestar todas as informações que se fizerem necessárias à migração dos dados de seu software do serviço para outro software que porventura venha a ser adotado pelo SERPRO.

8.4.2. A CONTRATADA deve disponibilizar as atualizações de manutenção corretiva e evolutiva que venham a ser implementadas para o serviço contratado.

8.4.3. A CONTRATADA deverá realizar repasse de conhecimento, sem ônus para o SERPRO, inerente a instalar, configuração, parametrizar e uso do serviço, conforme descrito a seguir:

8.4.3.1. O repasse deverá ser realizado em dependência providenciada pela CONTRATADA na localidade de Brasília/DF e São Paulo/SP.

8.4.3.2. Para até 40 (quarenta) empregados do SERPRO, com carga horária de até 40 (quarenta) horas por turma, sendo 02 (duas) turmas por localidade.

8.4.3.3. A CONTRATADA deverá prover toda a logística e todo o material didático necessário à execução do repasse de conhecimento teórico e prático, ou seja, instalações adequadas, equipamentos, manuais e apostilas.

8.4.3.4. O repasse de conhecimento deverá ser realizado utilizando conteúdo teórico e prático, através de laboratório preparado com o serviço contratado, onde estarão disponíveis as mesmas funcionalidades solicitadas nas especificações técnicas.

8.4.3.5. Todas as despesas com material, equipamentos, instrutores, deslocamento de instrutores e demais itens serão de responsabilidade da CONTRATADA.

8.4.3.6. O Repasse de Conhecimento deverá ser ministrado exclusivamente em Língua Portuguesa do Brasil devendo a CONTRATADA enviar cronograma de execução até o décimo dia corrido após a reunião de Kick-off do contrato, para ser aprovado pelo Serpro.

8.4.3.7. O repasse de conhecimento para o SERPRO deverá ser iniciado em até 30 (trinta) dias corridos após a data de vigência do contrato, podendo ser prorrogado por conveniência do SERPRO, quando então, em comum acordo com a CONTRATADA, será definida uma nova data.

8.4.3.8. A CONTRATADA deverá encaminhar a UniSerpro, até o décimo dia útil após assinatura do contrato, uma ementa do repasse de conhecimento, contendo: nome, objetivo, conteúdo programático e carga horaria.

8.4.3.9. O repasse de conhecimento deverá ser ministrados por instrutores certificados no serviço contratado.

8.4.3.10. Deverá ser emitido certificado para cada empregado que obtiver presença mínima de 75% (setenta e cinco por cento).

8.4.3.10.1. Os certificados de repasse de conhecimento dos empregados do SERPRO deverão ser encaminhados aos Responsáveis da Universidade do Serpro em Brasília, no seguinte endereço: SGAN QUADRA 601 MÓDULO "V" - BRASÍLIA/DF, CEP: 70.836-900, em até 10 (dez) dias corridos após o seu término.

8.4.3.11. Ao final de cada turma, os participantes do SERPRO, farão avaliação do repasse de conhecimento. Caso não seja atingida a média 70% (setenta por cento) de conceitos "bom" e/ou "ótimo", haverá a necessidade de realização de outro repasse de conhecimento.

8.4.3.11.1. Somente poderão fazer a avaliação os empregados que obtiver presença mínima de 75% (setenta e cinco por cento).

8.4.7.12. Ao final do repasse de conhecimento, se a CONTRATADA atendeu todos os requisitos, a UniSERPRO emitirá a Declaração de Aceite de Repasse de Conhecimento.