Empresa de Tecnologia da Informação do Ceará - Etice
Av. Pontes Vieira 220 - São João do Tauape
CEP: 60.130-240- Fortaleza/CE
Fone: (85) 3108-0900
www.etice.ce.gov.br

Chamada de Oportunidade de Serviços de Nuvem Pública Nº. 006/2022, aderente ao Edital de Pré-qualificação Permanente de Serviços em Nuvem Nº 001/2019 - ETICE

Julho de 2022

1. OBJETO

O presente termo de referência é referente à chamada de oportunidade para prestação de serviços compreendendo uma Central de Privacidade, Segurança e Governança de Riscos, Processos e Dados em nuvem, com serviços técnicos de mapeamento e automação de processos, monitoramento, sustentação, desenvolvimento e atuação integrada à Gestão do CONTRATANTE, visando adequar, proteger e manter o CONTRATANTE aderente às Normas de Privacidade, Governança e Segurança, tais como ISO/IEC 27005, AICPA TSC 2017 (SOC 2), NIST (CSF) Core v1.1, LGPD, ISO/IEC 29100:2011, ISO/IEC 27701:2019 e ISO/IEC 27001:2013, abrangendo todo ciclo de vida do processamento, desde a coleta até o encerramento e exclusão dos dados, por um período mínimo de 12 (doze) meses, além da constante vigilância e pronta atuação contra os possíveis ataques cybernéticos e da disponibilização de EAD em LGPD e CyberSegurança e transferência de conhecimento para equipe interna.

2. OBJETIVOS:

Contribuindo com o aprimoramento tecnológico dos entes da Administração Pública do Estado do Ceará e reforçando sua missão de ser referência nacional como empresa de Tecnologia da Informação e Comunicação – TIC, indutora da inovação e modernização para o desenvolvimento econômico-social no fornecimento de serviços de tecnologia de alta performance em nuvem, a **ETICE** deseja selecionar, dentre as empresas pré-qualificadas, **serviços técnicos especializados para provimento de solução em nuvem**, conforme detalhamento técnico constante neste documento.

Assim, considerando as premissas estabelecidas no Edital de Pré-qualificação 001/2019, a Empresa de Tecnologia da Informação do Ceará – ETICE convoca as empresas pré-qualificadas para **que apresentem propostas para fornecimento dos serviços em nuvem, seguindo as definições técnicas deste documento convocatório**.

Todos os recursos e serviços necessários deverão ser lançados na proposta em modalidade OPEX.

Outrossim, vale destacar que os itens de serviços vencedores de cada chamada de oportunidade já serão trazidos para a composição do Marketplace da ETICE, devendo o(s) contrato(s) serem realizados por demanda; ou seja, SEM comprometimento do Orçamento da ETICE, podendo haver a contratação parcelada do objeto da presente chamada de Oportunidade; tudo consoante ao disposto nos itens 13.11, 17.1.1, 17.1.2 e 17.1.3 do Edital de Préqualificação, *in verbis*:

> "13.11. **Os itens de serviços vencedores de cada chamada de oportunidade serão trazidos para a composição dos serviços do *marketplace* da Etice**, devendo seus preços finais serem mantidos como máximos por um prazo mínimo de 12 (doze) meses a contar da data da homologação do resultado da chamada de oportunidade.
>
> (...)
>
> 17.1.1. Consoante o disposto no art. 140, parágrafos 4º e 5º do Regulamento de Licitações e Contratos da Etice, **fica desde já a ETICE autorizada a celebração de contratos por demanda.**

17.1.2. A ETICE fixará um quantitativo ou valor máximo de fornecimento ou serviço a ser utilizado no prazo de vigência do referido contrato, **SEM comprometimento do Orçamento da Etice.**

17.1.2. Na hipótese do item anterior, a ETICE **demandará o objeto de forma PARCELADA e apenas quando necessitar, nos termos e prazos definidos no Edital e contrato**, remunerando o contratado apenas pelo que for efetivamente executado." (grifou-se)

Este documento descreve as **características funcionais, premissas técnicas e de serviços** que deverão ser consideradas pelas pré-qualificadas, para que, munidos de informações relevantes sobre as necessidades para atendimento ao escopo dos serviços, emitam propostas de acordo com as condições preestabelecidas no Edital de Pré-qualificação supracitado.

3. SOBRE O MODELO DE CONTRATAÇÃO

3.1 Esta chamada de oportunidade obedecerá ao disposto **no Edital de pré-qualificação de nuvem nº 001/2019 da ETICE e seus anexos**, nos **Termos de Pré-Qualificação** e no **Regulamento de Licitações e Contratos da ETICE**; sendo regido, também, pela **Lei Federal 13.303/2016**, pelos **Princípios do Direito Civil** e, no que couber, pelos **Princípios da Administração Pública** e demais legislação correlata.

3.2 A chamada será feita em lote único visto que os itens desta chamada são intrinsicamente interconectados o que impossibilitaria sua divisão.

3.2.1 Considerando que o Edital de Pré-qualificação 0001/2019–ETICE, prevê a possibilidade de chamadas nominadas, nos termos do item 13.5 e 13.5.1 do EDITAL DE PRÉ-QUALIFICAÇÃO PERMANENTE DE SERVIÇOS EM NUVEM N° 0001/2019, nos seguintes termos:

*"13.5. Em chamada de oportunidade envolvendo produto e/ou serviço **nominado**, será obrigatório existir pelo menos 03 (três) propostas de integradores de serviços de nuvem (vendors) pré-qualificados para que seja homologado o resultado da chamada.*

13.5.1. Caso o produto seja oriundo de um CSP, a chamada de oportunidade será realizada somente se existirem, no mínimo, 03 (três) vendors pré-qualificados deste CSP e o resultado somente será homologado caso, no mínimo, 03 (três) vendors deste CSP apresentem proposta."

4. ORIENTAÇÕES GERAIS

4.1 Prazos

Número do Evento	Evento	Prazo limite
1	Recebimento de propostas das empresas pré-qualificadas pela ETICE	Até 8 (oito) dias úteis (*)
2	Pedidos de Esclarecimentos	**Até às 17h:00min do 3º (terceiro) dia útil que antecede o prazo de entrega das propostas.**
3	Resposta aos Pedidos de Esclarecimentos	Até 2 (dois) dias úteis, a contar do término do prazo de pedidos de esclarecimentos (**).
4	Pedidos de Impugnação	**Até às 17h:00min do 3º (terceiro) dia útil que antecede o prazo de entrega das propostas.**
5	Respostas à Impugnação Interposta	Até 2 (dois) dias úteis, a contar do término do prazo de pedidos de esclarecimento.
6	Avaliação e definição da proposta vencedora pela ETICE	Até 5 (cinco) dias úteis, contados a partir do término do prazo de apresentação de propostas.
7	Interposição de Recurso	Até 5 (cinco) dias úteis, contados a partir da divulgação da proposta vencedora.
8	Apresentação de Contrarrazões ao Recurso	Até 5 (cinco) dias úteis, contados a partir do término do prazo de interposição de recurso.

9	Decisão definitiva da Comissão	Até 5 (cinco) dias úteis, contados a partir do término do prazo de apresentação de contrarrazões recursais, podendo variar em razão da complexidade da matéria.
10	Homologação e Adjudicação	Até 5 (cinco) dias úteis, a contar da divulgação da decisão definitiva da Comissão.

(*) O prazo será contado a partir do primeiro dia útil seguinte à publicação deste documento no website da ETICE, no link https://www.etice.ce.gov.br/projeto/pre-qualificacao-permanente/.

(**) O prazo poderá ser alterado conforme disposto no item 5.4.

(***) Caso haja desistência expressa do Prazo Recursal (e consequente Contrarrazões), o Prazo para apresentação da Decisão Definitiva poderá ser reduzido, conforme o caso.

4.1.1 Os Prazos dispostos no item acima poderão variar em conformidade com o caso concreto, podendo inclusive serem mitigados, em razão de não apresentação de recursos ou mesmo que as empresas Pré-qualificadas declinem, formalmente, do direito Recursal (e consequentemente das Contrarrazões).

4.2 Sobre o envio da Proposta Técnicas

4.2.1 Em razão do período delicado de Pandemia mundial que estamos passando, e até mesmo como um mecanismo de evitar o trânsito de papel e aglomeração de pessoas, consoante previsão disposta no item 13.8.2 do Edital nº, 001/2019 de Pré-Qualificação, a proposta deverá ser enviada de **forma eletrônica** e deverá inicialmente ser **CRIPTOGRAFADA** utilizando o algoritmo de criptografia AES-256 (FIPS PUB 197).

4.2.2 O proponente é responsável por gerar uma chave aleatória de 256 bits e **manter completo sigilo desta chave, sem revelá-la a terceiros, nem à Etice**, até que se tenha passado o período de recebimento de propostas estabelecido na tabela do item 6.1.

4.2.3 Antes ou após criptografada utilizando-se o algoritmo AES-256, a proposta deve ser assinada digitalmente, conforme o modelo da Medida Provisória 2.200-2/2001.

4.2.3.1 Com o objetivo de facilitar a submissão de propostas e considerando que vários *softwares* possibilitam a assinatura digital de um documento antes de uma encriptação e não após ela a ETICE aceitará também propostas que tenham sido assinadas digitalmente antes de terem sido encriptadas contanto que o nome do arquivo de proposta possibilite a identificação clara do proponente.

4.2.4 A proposta criptografada e assinada deve ser enviada para o e-mail avaliacao.nuvem@etice.ce.gov.br. **O HORÁRIO DE RECEBIMENTO DAS PROPOSTAS SERÁ ATÉ ÀS 17H (DEZESSETE HORAS) DO ÚLTIMO DIA ÚTIL PARA RECEBIMENTO DAS PROPOSTAS.**

4.2.5 Uma proposta só será considerada entregue no prazo caso a Etice responda com um e-mail para o proponente reconhecendo o recebimento dentro do prazo.

4.2.6 A resposta da Etice será assinada digitalmente ou de outra forma por ela estabelecida.

4.2.7 Proposta enviada para e-mail não correto ou com erro de escrita ou que tenha sido recusado pelo servidor não serão considerados entregues no prazo.

4.2.8 A proponente deverá enviar a chave criptográfica usada para encriptar a proposta com o algoritmo AES-256 para a Etice em até 1 (um) dia útil após encerrado o prazo de recebimento de propostas.

4.2.9 Arquivos corruptos ou chaves que não permitam descriptografar a proposta, farão a proposta nula.

4.2.10 **Todos os recursos e serviços necessários deverão ser lançados na proposta em modalidade OPEX e em moeda nacional (reais).**

4.2.11 Na proposta deverá constar as cotações de todos os itens de serviços especificados neste documento, expressas em reais e em valores mensais e anuais.

4.2.12 Para fins de elaboração de Proposta, as empresas participantes deverão considerar que o prazo contratual será de 12 (doze) meses, prorrogável na forma da lei.

4.2.13 A Etice descriptografará todas as propostas válidas e ordenará tais propostas baseadas em seu valor global.

4.3 Processo de Seleção e Negociação

4.3.1 **A seleção e negociação da melhor proposta só ocorrerá se existirem, no mínimo, 3 (três) propostas válidas para a chamada.**

4.3.2 O processo de seleção e negociação respeitará as regras do edital de pré-qualificação e da presente chamada, com base na proposta mais vantajosa para a Etice; de forma a não comprometer a economicidade.

4.3.3 Serão **DESCLASSIFICADAS** as Propostas que:

4.3.3.1 Contenham vícios insanáveis;

4.3.3.2 Descumpram especificações técnicas constantes da Chamada de Oportunidade;

4.3.3.3 Apresentem preços manifestamente inexequíveis;

4.3.3.4 Não tenham sua exequibilidade demonstrada, quando exigido pela ETICE;

4.3.3.5 Apresentem desconformidade com outras exigências do instrumento convocatório, salvo se for possível a acomodação a seus termos antes da adjudicação do objeto e sem que se prejudique a atribuição de tratamento isonômico entre as licitantes;

4.3.3.6 A ETICE poderá realizar diligências para aferir a exequibilidade das propostas ou exigir das licitantes que ela seja demonstrada;

4.3.3.7 A desclassificação será sempre fundamentada.

5 ESCLARECIMENTOS

5.1 As dúvidas na interpretação do presente documento e anexos, consultas ou pedido de esclarecimentos acerca das informações técnicas porventura existentes, poderão ser feitos via e-mail de forma **expressa**, **clara**, **concisa** e **objetiva**, constando no corpo do texto do e-mail a identificação completa da empresa pré-qualificada participante e do representante que questiona as informações ou solicita esclarecimentos.

5.2 Os pedidos de esclarecimentos deverão ser encaminhados **até às 17h:00min do 3º (terceiro) dia útil que antecede o término do prazo de apresentação das propostas.**

5.3 O endereço de e-mail para os esclarecimentos é: **avaliacao.nuvem@etice.ce.gov.br.**

5.4 A Etice terá um prazo de até 02 (dois) dias úteis para resposta, sendo possível estender esse prazo de acordo com a complexidade dos esclarecimentos e/ou a necessidade de utilização de recursos técnicos externos à Etice.

5.5 Caso a(s) resposta(s) dos esclarecimentos provoquem alterações das definições técnicas do projeto e estas sejam consideradas relevantes pela Etice, será reiniciada a contagem dos prazos estabelecidos no item 6.1 deste documento, cabendo comunicação prévia e única a todas as pré-qualificadas.

5.6 **As quantidades aqui mencionadas são previsões e não implicam em obrigatoriedade de contratação de quaisquer quantidades pela Administração Pública, servindo apenas como referencial para a elaboração das propostas das empresas pré-qualificadas pela ETICE.**

6 ESPECIFICAÇÃO TÉCNICA DOS SERVIÇOS

A Central de Privacidade, Segurança e Governança de Riscos, Processos e Dados será monitorada constantemente por uma equipe especializada onde conjunto de ações de adequação nas áreas de privacidade e segurança da informação serão desenvolvidas dentro do escopo das disciplinas de governança, pessoas, metodologia, tecnologia e gestão de maturidade, implementadas de forma concomitante e incremental. Tais ações são voltadas para aumento do grau de maturidade e de resiliência do CONTRATANTE.

Os itens do objeto são compreendidos conforme tabela abaixo:

TABELA 01

Item	Descrição	Unidade	Quantidade máxima
01	Portal Centralizado de Governança, incluindo suporte técnico, manutenção e atualização tecnológica, implantação, diagnósticos e melhorias nos processos aderentes	Mensal	60
02	Módulo de Governança	Bancos de dados – blocos de 50	750
03	Módulo de Privacidade	Bancos de dados – blocos de 50	750
04	Módulo de Segurança	Bancos de dados – blocos de 50	750
05	Módulo de Gerenciamento Integrado de Riscos	Usuários – blocos de 25	250
06	Módulo de Automação	Usuários – blocos de 25	250
07	Módulo de Gestão de Serviços	Usuários – blocos de 25	250
08	Módulo de Gestão de Atendimento	Usuários – blocos de 25	250
09	Módulo de Gestão de Demandas, Projetos e Novos Desenvolvimentos	Usuários – blocos de 25	250
10	Módulo de Gestão de Operações	Usuários – blocos de 25	250
11	Módulo de Gestão de Ativos	Usuários – blocos de 25	250
12	Módulo de Gestão de Segurança e Incidentes	Usuários – blocos de 25	250
13	Serviço de hospedagem em cloud	Banco de dados – Blocos de 50 (mensal)	1.000
14	Solução de monitoramento contínuo para detecção de possíveis impactos corporativos	Por ativos – blocos de 10	300
15	Solução de monitoramento, detecção e resposta a incidentes de segurança da informação - 1.500 Eventos por segundo (EPS)	Aferição mensal de eventos por segundo	Máximo 6000 mês
16	Serviços de customização e desenvolvimento de integrações com os sistemas da Contratante.	blocos de 100 UST	5.000
17	Serviço especializado para mapeamento e análise dos processos de negócio, serviços de customização e desenvolvimento de integrações com os sistemas da contratante.	blocos de 100 UST	1.000
18	Solução para testes de penetração em acordo com o OWASP (Plataforma WEB aberta para segurança de aplicativos)	500 endpoints 10 domínios	Máximo 5000 endpoints Máximo 1000 domínios
19	Solução de compliance e anti-fraude em ambientes de inteligência artificial com deploy ilimitados	Blocos de 10 usuários	50 usuários

20	Transferência de conhecimento de instalação, configuração e administração da plataforma e componentes	Por turma com 20 alunos	40
21	Serviços de operação assistida (sustentação da plataforma)	blocos de 100 UST	2.000
22	Serviços de monitoramento e suporte à privacidade	blocos de 100 UST	2.000
23	Licença para uso de plataforma de treinamento em Conceitos de Segurança da Informação em formado EAD	Por Aluno – mínimo 50	5.000

A quantidade mínima para 12 meses será solicitada na assinatura do contrato de acordo com a coluna quantidade mínima garantida.

A quantidade máxima de licenças é uma estimativa de consumo para os 60 meses da prestação de serviços.

6.1 ESCOPO DOS SERVIÇOS E FUNCIONALIDADES DA SOLUÇÃO

6.1.1 As soluções sistêmicas deverão ter plataformas únicas ou a possibilidade de integração entre elas, com backup automático, com resiliência operacional, que opere em ambiente de nuvem (Cloud Computing) e deverá possuir infraestrutura escalável automaticamente (auto scalling).

6.1.2 O licitante é o único responsável pelas informações sobre tributos. Não caberá qualquer reivindicação para majoração de preço em virtude de possíveis equívocos cometidos. Efetuar-se-á a devida correção quando houver alteração da respectiva legislação tributária que rege a operação, após a data estabelecida para apresentação da proposta.

6.1.3 As soluções sistêmicas deverão ser ofertadas via um sistema único ou que possibilite uma integração que automatize fluxos de trabalho e que tenha integração entre processos de negócios da CONTRATANTE. A CONTRATADA deverá prestar todos os serviços especializados de qualquer das soluções partes dessa especificação técnica.

6.2 PORTAL CENTRALIZADO DE GOVERNANÇA, INCLUINDO SUPORTE TÉCNICO, MANUTENÇÃO E ATUALIZAÇÃO TECNOLÓGICA, IMPLANTAÇÃO, DIAGNÓSTICOS E MELHORIAS NOS PROCESSOS ADERENTES

6.2.1 Requisitos técnicos GERAIS

6.2.1.1 A Solução deverá ser fornecida em nuvem para atender os requisitos de privacidade e segurança;

6.2.1.2 Todas as funcionalidades da solução que dependam de interação com CONTRATANTE/usuário devem ser disponibilizadas via interface/aplicação web sem necessidade de instalação de agentes ou conectores nas máquinas dos usuários ou em servidores da CONTRATANTE (Banco de Dados, File Server, etc.). Não serão aceitas

soluções CONTRATANTE/servidor;

6.2.1.3 Não deve haver a necessidade de instalação e nem de utilização de plug-ins nos navegadores para a execução da camada CONTRATANTE da aplicação web;

6.2.1.4 A aplicação/interface web deve rodar nas versões atuais dos principais navegadores de Internet existentes no mercado à época da instalação da solução e deve garantir compatibilidade com as suas novas versões. Por "principais navegadores de Internet" considere-se, no mínimo, os seguintes: Microsoft Edge (clássico e baseado no Chromium), Mozilla Firefox e Google Chrome, independentemente do sistema operacional utilizado (Windows, MAC OS, Linux, etc.);

6.2.1.5 A solução deverá ser compatível com os navegadores das plataformas de dispositivos móveis: Android e iOS - web adaptativo/responsivo. Alternativamente, poderá ser atendido via aplicativo móvel para as plataformas citadas (app);

6.2.1.6 A solução deve fornecer mecanismos para integração síncrona e assíncrona com aplicações da CONTRATANTE incluindo RESTful e SOAP APIs, assim como requisições de API GET, PUSH, PULL etc.;

6.2.1.7 A solução deve fornecer integração com serviço de e-mail, devendo ser utilizado servidor SMTP/POP/IMAP provido pela empresa;

6.2.1.8 A solução deve permitir a capacidade de se personalizar, no mínimo:

6.2.1.8.1 Fundos e banners;

6.2.1.8.2 Menu e ferramentas de navegação;

6.2.1.8.3 Campos, formulários e tabelas;

6.2.1.8.4 Cor do texto, fonte e tamanho;

6.2.1.8.5 Infográficos, Gráficos e painéis;

6.2.1.8.6 Alertas e notificações.

6.2.1.8.7 A solução deve permitir a integração de sistemas de terceiros e recursos de migração de dados. A solução deve fornecer uma variedade de técnicas de integração, incluindo:

6.2.1.8.7.1 Webservices;

6.2.1.8.7.2 JDBC;

6.2.1.8.7.3 LDAP;

6.2.1.8.7.4 Excel;

6.2.1.8.7.5 CSV;

6.2.1.8.7.6 E-mail

6.2.1.9 A solução também deve usar tecnologias padrão da indústria, como SOAP, REST ou WSDL. Além disso, as integrações de API e de linha de comando devem ser possíveis usando um MID Server (Middleware/Barramento). Todo o tráfego de Webservices deve ser encriptado com TLS;

6.2.1.10 A plataforma deve ser baseada em arquitetura orientada a serviços (SOA), na qual todos os objetos de dados podem usar os Webservices para acessar a integração bidirecional de nível de dados;

6.2.1.11 A solução deverá possuir ferramenta de criação de formulários e relatórios, a fim de personalizar a inserção de informações e controles de acordo com a necessidade do CONTRATANTE, sem a necessidade de programação ou alteração do código fonte;

6.2.1.12 A plataforma deve ser baseada em arquitetura orientada a serviços (SOA), na qual todos os objetos de dados podem usar os Webservices para acessar a integração bidirecional de nível de dados;

6.2.1.13 A plataforma deve oferecer uma interface rica (Rich interface) para carregar dados externos usando conjuntos de importação de várias fonts de dados, como HTTPS, FTPS e SCP usando formatos de arquivo, como XML, CSV e Microsoft Excel XLS;

6.2.1.14 A solução deve suportar a governança dos dados pessoais de organização hierárquicas, tais como órgãos de um estado ou empresas de um grupo empresarial, permitindo que a gestão dos dados ;

6.2.1.15 A solução deve suportar a governança dos dados pessoais de organizações hierárquicas, tais como órgãos de um estado ou empresas de um grupo empresarial, permitindo que a gestão dos dados pessoais destas empresas seja: centralizada, parcialmente distribuída, totalmente distribuída ou variações dessas configurações, de acordo com as necessidades do contratante. Deve atender, no mínimo, aos seguintes cenários:

6.2.1.16 Uma organização central pode gerir todos os dados pessoais das organizações do grupo/órgãos de governo;

6.2.1.17 Cada organização pode administrar os dados pessoais do qual é controladora, porém, a organização central tem visibilidade dos processos comuns e pode ter visibilidade sobre os dados pessoais compartilhados entre as organizações do grupo;

6.2.1.18 Deve ser permitindo que uma ou mais organizações tenham uma gestão dos dados pessoal totalmente independente da organização central;

6.2.1.19 Que as organizações controladoras, participantes da hierarquia, possam emitir relatórios de consulta sobre a existência de dados pessoais sob sua responsabilidade e que estejam sob custódia de operadores que façam parte da mesma hierarquia;

6.2.1.20 Por questões de segurança, a solução deverá suportar a instalação dos

componentes que necessitam acessar as bases de dados ou dados não estruturados da contratante, tais como data discovery, no datacenter da contratante (on premises), em servidores com sistemas operacionais Windows em suas versões mais recentes, ou Linux, nas distribuições mais utilizadas no mercado em suas versões mais recentes. A conexão da plataforma em nuvem com estes servidores de data Discovery deverá ser realizada por conexão segura e criptografada.

6.2.1.21 A CONTRATANTE será responsável por fornecer a infraestrutura de rede, processamento, armazenamento, bancos de dados e licenciamento dos sistemas operacionais utilizados. Todas as demais licenças necessárias ao funcionamento da solução deverão ser fornecidas pela contratada. Todas as demais funcionalidades deverão ser SaaS (Software as a Service).

6.2.1.22 O ambiente de nuvem que hospeda a solução deverá atender aos requisitos definidos no item 8.

6.3 INTEGRAÇÃO, INDICADORES E PAINÉIS

6.3.1 A Contratada deverá realizar, para dados estruturados, o data Discovery, integração com portal do titular e gestão jurídica (Data Mapping), seguindo a Política de Gestão e Governança de Dados Corporativo da Contratante, considerando todas as bases de dados utilizados pela Contratante, devendo gerar as seguintes informações.

6.3.2 Dashboard com o resultado do Data Discovery informando quantidade de banco de dados por tecnologia;

6.3.3 Dashboard com o resultado do inventário de servidores analisados (Discos, memória, Ethernet, etc.);

6.3.4 Dashboard com o resultado do Data Discovery por banco de dados, informando quais bancos de dados possuem dados pessoais e/ou sensíveis e a quantidade de colunas que contem cada dado em cada banco de dados.

6.3.5 A Contratada deverá realizar, para dados não estrutuados, o data discovery, data mapping, integração com portal do titular, seguindo a Política de Gestão e Governança de Dados Corporativo da Contratante, considerando todas os repositórios de dados não estruturados utilizados pela Contratante, devendo gerar as seguintes informações.

6.3.6 Dashboard com o resultado do Data Discovery informando quantidade de documentos com dados pessoais e/ou sensíveis;

6.3.7 Permitir criar gráficos e relatórios com o resultado do Data Discovery;

6.3.8 Dashboard com o resultado do Data Discovery por repositório, informando quais diretórios/servidores possuem dados pessoais e/ou sensíveis e a quantidade de dados por

tipo (CFP, RG, NOME, etc.).

6.3.9 As integrações deverão ser sugeridas pela CONTRATADA, permitindo que a CONTRATANTE possa estruturar papéis necessários para gestão de informações; definição da estratégia de dados das áreas de negócio; cesta de indicadores que permita:

6.3.10 Medir objetivamente a maturidade das áreas de negócio e TI quanto a disciplinas de gestão de informações;

6.3.11 Medir qualidade das informações;

6.3.12 Eficiência e eficácia dos processos de governança e gestão dedados;

6.3.13 Engajamento das áreas de negócio e TI.

6.3.14 A solução deverá permitir a criação de painéis gerenciais utilizando técnicas e softwares de B.I. Nativa da própria ferramenta da Contratada para a construção de visões analíticas e gerenciais de todos os módulos previstos na plataforma. Neste caso, a Contratada ficará com a responsabilidade pelo desenvolvimento, sustentação, construção e apresentação dos dados. Além disso, deverá ser fornecido um painel estratégico, onde serão apresentadas e analisadas as informações de acesso.

6.3.15 Considerando que cada usuário da solução possui necessidades de uma visão gerencial de acordo com suas atividades e processos de trabalho são fundamentais que a solução permita ao próprio usuário da solução, sem apoio técnico especializado e de forma intuitiva, criar seus painéis e dashboards de gerenciamento. Para isso, a solução deverá:

6.3.16 Permitir a criação de painéis e dashboards com gráficos de gestão, de forma ágil e intuitiva, sem a necessidade de programação e alteração do código-fonte.

6.3.17 Permitir a criação de painéis e dashboards com gráficos do tipo pizza, linha, colunas, barras e tabelas dinâmicas, sem a necessidade de programação e alteração do código-fonte.

6.3.18 Permitir alterações de atributos de forma dinâmica em gráficos de gestão, contidos em painéis e dashboards da solução, possibilitando a alteração de eixos, titulo do gráfico, legenda, escala, rótulos de dados, tamanho do gráfico, de forma gráfica na solução e sem a necessidade de alterações do código-fonte.

6.3.19 Permitir aos usuários criarem seus próprios painéis e gráficos dentro da solução e compartilharem com grupos ou usuários específicos da solução, permitindo gerenciar as permissões de compartilhamento de acordo com os perfis de usuários da solução.

6.3.20 Permitir a criação de gráficos com informações de diferentes entidades da solução, permitindo a sobreposição e cruzamento de informações e delimitação de linhas de tendência.

6.3.21 Permitir que a partir de qualquer gráfico de gestão, contido em painéis e dashboards da solução, o usuário possa clicar e listar os registros relacionados com os dados contidos no

gráfico (funcionalidade drill down).

6.3.22 Permitir ao usuário organizar os gráficos e informações, em seus painéis e dashboards de gestão, ajustando o layout e conteúdo do painel de acordo com suas necessidades.

6.3.23 Permitir aos usuários a configuração de painéis e dashboards agrupados por assunto e independentes entre si.

6.3.24 Permitir ao usuário organizar seus painéis e dashboards com listas de registros de seu interesse, possibilitando a escolha de colunas, realização de filtros e ordenação da lista.

6.3.25 Permitir a criação de painéis e dashboards com gráficos de gestão a partir de qualquer coluna do banco de dados da solução, sem a necessidade de programação e alteração do código-fonte.

6.3.26 Permitir a geração de relatórios, impressão e exportação para arquivos no mínimo do tipo csv, html, pdf e xml.

6.3.27 Prover informação em "real-time" de maneira gráfica por meio de dashboards.

6.3.28 Permitir configurar o envio automático e agendado de relatórios e gráficos gerenciais para grupos de usuários ou usuários específicos.

6.4 Desenvolvimento de novas Integrações, evoluções e desenvolvimento de novos algoritmos

6.4.1 Como processo vivo, está sujeito a evolução nos processos de arregimentação, atendimento e desenvolvimento, entre outros. Assim o CONTRATANTE necessitará de um processo contínuo de desenvolvimento de algoritmos de conversão, impacto, integração e deployment para produção para o pleno funcionamento de suas ações. Assim, é prudente estimarmos Unidade de Serviços Técnicos (UST) no processo para este tipo de integração, garantindo a plena adequação independente das novas soluções do CONTRATANTE.

6.4.2 A implantação de tais políticas e procedimentos deverá ser promovida via mapeamento de processos e mecanismos de controle ainda desconhecidos, que a consultoria a ser contratada deverá viabilizar, tendo em vista o quadro técnico reduzido do CONTRATANTE.

6.4.3 O desenvolvimento de novas funcionalidades e algoritmos deverá ser contratado sob demanda seguindo a seguinte sequência de procedimentos:

6.4.4 O CONTRATANTE apresentará a necessidade;

6.4.5 A CONTRATADA estimará as horas adequadas (UST) e cronograma para realização da integração e enviará ao CONTRATANTE para aprovação

6.4.6 Caso a demanda seja aprovado, o CONTRATANTE emitirá a ordem de serviço;

6.4.7 A CONTRATADA inicia o desenvolvimento das novas funcionalidades.

6.5 Armazenamento, Suporte e Processamento de modelos de dados

6.5.1 A solução deverá compreender o tratamento de dados estruturados e não estruturados vindos das propriedades digitais, combinando capacidade e desempenho conforme o necessário para o caso de uso de lógica analítica, permitindo que seja possível combinar dados para o provimento de informações gerenciais e oferecendo ferramentas modernas de gerenciamento de dados para análise e identificação de informações que possam ser utilizadas.

6.5.2 A solução de armazenamento deverá ser implementada na infraestrutura do CONTRATANTE em local adequado e o controle sob os procedimentos em nuvem, conforme item 8 (serviços em cloud):

6.5.3 02 (dois) Servidores para Dados Estruturados;

6.5.4 01 (um) Servidor para Dados Não-Estruturados;

6.5.5 01 (um) Servidor para Auditoria de Tratamento de Dados.

6.6 Compliance

6.6.1 A CONTRATADA deverá seguir as normas de Privacidade visando a plena adequação do processo. Assim, alguns procedimentos deverão ser estabelecidos a fim de promover mais transparência. Assim será necessário:

6.6.2 Um relatório mensal da CONTRATANTE e da CONTRATADA, com as informações de todos os servidores que trabalharão no projeto com os níveis de acesso de informações.

6.6.3 Termo de confidencialidade da CONTRATANTE e da CONTRATADA para cada servidor que for trabalhar com os dados do CONTRATANTE.

6.6.4 A ferramenta deverá ter domínio e governança sobre todos os dados utilizados, com a rastreabilidade de dados a partir de qualquer chave de acesso.

6.7 Padrões da Solução

6.7.1 Todos os aplicativos deverão ser criados em uma única plataforma do CONTRATANTE;

6.7.2 Acesso e interface com o CONTRATANTE da Web - sem a necessidade de aplicativo ou agente local;

6.7.3 Base de dados única;

6.7.4 A solução deve fornecer alta disponibilidade avançada (AHA) em clusters. Os recursos de disponibilidade devem incluir:

6.7.4.1 Possibilidade de redundância total;

6.7.4.2 Tolerância ao erro;

6.7.4.3 Balanceamento de cargas nos servidores;

6.7.4.4 Monitoramento de desempenho;

6.7.4.5 Processo de failover;

6.7.4.6 Backup (Full) e recuperação de desastres;

6.7.4.7 Plano de continuidade de negócios.

6.7.5 A solução deve permitir recursos de personalização para a solução proposta. No mínimo, a solução selecionada deve incluir a capacidade de personalizar:

6.7.5.1 Tema geral (cores, logotipos e imagens);

6.7.5.2 Fundos e banners;

6.7.5.3 Menu e ferramentas de navegação;

6.7.5.4 Campos, formulários e tabelas;

6.7.5.5 Cor do texto, fonte e tamanho;

6.7.5.6 Exibir lista;

6.7.5.7 Site completo;

6.7.5.8 UI para login, home ou páginas de pesquisa;

6.7.5.9 Infográficos, Gráficos e painéis;

6.7.5.10 Alertas e notificações;

6.7.5.11 Automação de fluxo de trabalho;

6.7.5.12 Integração do sistema.

6.7.6 A solução deve habilitar e suportar a escalabilidade. No mínimo, a solução selecionada deve incluir:

6.7.6.1 Servidores de aplicativos agrupados em cluster;

6.7.6.2 Balanceamento de carga moderno;

6.7.6.3 Teste de escalabilidade;

6.7.6.4 Tempo de resposta do sub-segundo;

6.7.6.5 Nenhuma interação entre nós de cluster;

6.7.6.6 Ambientes multiprocessador / multi-núcleo

6.7.6.7 Compressão de dados;

6.7.7 A solução deve apresentar controles de segurança e de operações. No mínimo, a solução deve prever:

6.7.7.1 Active Directory / LDAP;

6.7.7.2 Autenticação e início de sessão único;

6.7.7.3 Auditoria e logs do sistema;

6.7.7.4 Segurança das comunicações;

6.7.7.5 Separação de empresas e de domínio;

6.7.7.6 Segurança contextual;

6.7.7.7 Criptografia e integridade de dados;

6.7.7.8 Firewalls e balanceadores de carga;

6.7.7.9 Sistemas de prevenção de intrusão;

6.7.7.10 Segurança e redundância da rede;

6.7.7.11 Controles físicos de segurança;

6.7.7.12 Controles de acesso baseados em funções;

6.7.7.13 Segurança da camada de transporte;

6.7.7.14 Teste de penetração;

6.7.7.15 Vulnerabilidade e gerenciamento de patches;

6.7.7.16 Governança e políticas.

6.7.8 A solução deve permitir a integração de sistemas de terceiros e recursos de migração de dados. A solução deve fornecer uma variedade de técnicas de integração, incluindo:

6.7.8.1 Webservices;

6.7.8.2 JDBC;

6.7.8.3 LDAP;

6.7.8.4 Excel;

6.7.8.5 CSV;

6.7.8.6 E-mail.

6.7.9 A solução deverá usar tecnologias padrão da indústria, como SOAP, REST Ou WSDL. Além disso, as integrações de API e de linha de comando devem ser possíveis usando um MID Server (Middleware/Barramento). Todo o tráfego de Webservices deve ser encriptado com TLS.

6.7.10 A solução deverá ser baseada em arquitetura orientada a serviços (SOA), na qual todos os objetos de dados podem usar os Webservices para acessar a integração bidirecional de nível de dados.

6.7.11 Além disso, a solução deverá oferecer uma interface rica (Rich Interface) para carregar dados externos usando conjuntos de importação de várias fontes de dados, como HTTPS, FTPS e SCP usando formatos de arquivo, como XML, CSV e Microsoft Excel XLS.

6.7.12 A solução deverá possuir processo de atualização de novas versões. No mínimo, a solução selecionada deve incluir:

6.7.13 Atualizações automáticas de novas versões contendo novas funcionalidades para CONTRATANTEs entregues várias vezes por ano com ótima qualidade e estabilidade;

6.7.14 Novas versões e hotfixes/patchs;

6.7.15 Capacidade de confirmar uma atualização e configurar a notificação de atualização;

6.7.16 Atualizar o histórico e as ferramentas de monitoria de progresso da atualização;

6.7.17 Possuir histórico online de notas de versão para todas as versões anteriores do produto.

6.8 Automação de processos e fluxos de trabalho de Governança para as Normas de Privacidade.

6.8.1 A automação de processos e fluxos de trabalho da solução deve ser interativa, prática e de fácil implementação. O desenvolvimento de soluções ágeis e dentro da velocidade que o negócio do CONTRATANTE exige, deve ser suportado pela solução, para tanto, a solução deverá suportar a criação de novas funcionalidades, automações de fluxos de trabalho, processos de TIC e suportar a implementação de rotinas e processamento de funcionalidades com uma programação mínima e básica (Low-Code), usando componentes integrados e nativos da própria plataforma. Neste sentido, a solução deverá:

6.8.1.1 Possuir recursos gráficos de workflow interativos para criação de processos e rotinas operacionais, que permita operações como arrastar-e-soltar para o desenho dos

fluxos de trabalho;

6.8.1.2 Apresentar componente próprio para a modelagem gráfica e a automação de processos e fluxos de trabalho;

6.8.1.3 Permitir a automação de fluxos de automação de forma gráfica, incluindo estágios, tarefas paralelas ou sequenciais, regras de decisão e aprovação, sem a necessidade de programação ou alteração de código-fonte;

6.8.1.4 Possuir ferramenta de criação de formulários com campos específicos de cada processo e fluxo de trabalho, a fim de personalizar a inserção de informações e controles de acordo com a necessidade do CONTRATANTE, sem a necessidade de programação ou alteração do código fonte;

6.8.1.5 Dispensar a necessidade da criação de tabelas, colunas e campos de banco de dados na solução, ou a necessidade de programação ou alteração do código-fonte, tornando estas alterações, quando necessárias, transparentes aos operadores e administradores que implementam os fluxos de trabalho;

6.8.1.6 Dispensar a necessidade a criação, de forma manual (usando scripts e programação), de tabelas, colunas e campos de banco de dados na solução, tornando estas atividades, quando necessárias, transparentes aos administradores da solução;

6.8.1.7 Possuir e disponibilizar em ambiente de nuvem privada no mínimo instâncias de desenvolvimento e de produção;

6.8.1.8 Permitir a criação de campos compartilhados que possam ser utilizados em quaisquer outras entidades, sem a necessidade de programação ou alteração do código-fonte;

6.8.1.9 Disponibilizar recursos tecnológicos de catálogo de serviços que possibilitem a automação de processos de gestão de TIC;

6.8.1.10 Permitir a customização de menus, formulários, labels, automatizações de fluxos de trabalho e processos de TIC do CONTRATANTE, desenvolvidos na solução, permitindo a adequação às necessidades de uso de cada usuário, sem a necessidade de programação ou alteração do código-fonte;

6.8.1.11 Permitir a criação e automação de processos e fluxos de trabalho de forma segregada e independente a fim de permitir a personalização para cada unidade do CONTRATANTE;

6.8.1.12 Permitir que os processos e fluxos de trabalho automatizados na solução possuam as mesmas funcionalidades nativas disponibilizadas na solução, como por exemplo: requisitos de usabilidade da lista de registros, citados nesta especificação técnica, ferramentas de colaboração como chat e notificações, permitindo comunicação entre CONTRATANTEs e provedor de serviços, personalização de menus, regras de aprovação de fluxos, relacionamento entre processos, painéis e dashboards automatizados, etc.

6.9 Portal de Serviços para as Normas de Privacidade

6.9.1 A solução deverá permitir que o CONTRATANTE possa criar portal de serviço e de atendimento para quaisquer unidades administrativas com serviços internos e externos, com visibilidade de ofertas e serviços baseada em perfis de usuário, garantindo que apenas usuários com as devidas permissões de acesso visualizem informações, registrem incidentes e requisições e participem nos fluxos de trabalho automatizados. Para tanto, a solução deverá:

6.9.1.1 Possuir recurso de Portal de Serviços WEB, customizável em recursos gráficos da solução, que permita acesso a todas as funcionalidades e recursos de gerenciamento e utilização disponíveis para o usuário final

6.9.1.2 Deve permitir disponibilizar recursos que possibilitem a criação de múltiplas visibilidades do portal de autoatendimento, para segmentar diferente perfil de usuário ou diferentes serviços, de diferentes departamentos.

6.9.2 O portal de serviços deverá ser personalizável para atender as necessidades da CONTRATANTE permitindo que áreas de inserção de conteúdos sejam criadas e organizadas de acordo com a necessidade da CONTRATANTE.

6.9.3 A partir da página inicial do portal de serviços deve ser possível a pesquisa de itens de catálogo de serviço, artigos de conhecimento, artigos de autosserviço, dentre outros itens.

6.9.4 O portal de serviços deve permitir aos usuários dos serviços a visualização completa da situação atual dos serviços, indicando se existem degradações, indisponibilidades, problemas e manutenções programadas nos serviços.

6.9.5 A solução deverá permitir a interação completa entre provedores de serviço e os usuários dos serviços, devendo no mínimo:

6.9.6 Possuir função de acompanhamento de todas as suas solicitações;

6.9.7 Permitir inserir quantidade ilimitada de informações e anexos em suas solicitações, nova ou já em atendimento;

6.9.8 Permitir visualizar em suas solicitações, informações do atendimento e mensagens do atendente;

6.9.9 Permitir acompanhar em tempo real a situação atual de sua solicitação;

6.9.10 Permitir ao usuário acompanhar e saber o prazo estimado para a conclusão do seu atendimento;

6.9.11 Permitir ao usuário conversar em tempo real, via chat, com o atendente;

6.9.12 Permitir que os usuários tenham uma visão histórica de todas as suas solicitações;

6.9.13 Permitir ao usuário acompanhar os custos envolvidos em sua solicitação.

6.9.14 A solução deverá permitir que os formulários de solicitação, de itens do catálogo de serviço no portal de serviço, sejam totalmente personalizáveis, permitindo a inserção de quantos campos forem necessários, para perguntas e respostas e permitindo ainda, que as respostas e seleções do usuário, no preenchimento do formulário de solicitação, direcione o seu registro para o fluxo de trabalho ou processo correto de atendimento.

6.9.15 A solução deverá possuir a funcionalidade de solicitações em lote, para a realização de mais de uma solicitação ao mesmo tempo.

6.9.16 A solução deverá permitir aos usuários aprovadores, visualizar suas aprovações em local de fácil acesso e visualização no portal de serviços

6.9.17 A solução deverá permitir a criação de ilimitados perfis de acesso ao portal de serviços, conforme necessidades do CONTRATANTE.

6.9.18 O acesso ao portal de autosserviço deve ser garantido mediante autenticação do usuário através de login e senha simples, ou através da integração com fontes externas de autenticação.

6.9.19 A autenticação do usuário deve ser suficiente para a correta identificação do seu grupo de permissões, apresentando a este usuário as informações e funcionalidades as que ele tem acesso.

6.9.20 O portal de autosserviço deve se beneficiar de folhas de estilo para que administradores possam aplicar personalizações adicionais quanto às cores, fontes, imagens e demais elementos visuais do portal, aplicando as alterações a todas as páginas automaticamente.

6.9.21 O portal de autosserviço deverá permitir que o usuário tenha acesso à um conjunto de perguntas frequentes (FAQ) para a elucidação de dúvidas e esforços de auto resolução de incidentes e solicitações de serviço

6.9.22 O portal de autosserviço deverá garantir ao usuário final o acesso ao Catálogo de Serviços, onde estarão dispostas as requisições de serviço passíveis de disparo, de acordo com seu perfil de permissões.

6.9.23 A solução deve permitir ser possível facultar ao usuário final a quantidade de itens solicitados na mesma requisição de serviço (ex. instalação de 02 PCs, ou 03 vagas de treinamento).

6.9.24 A definição dos campos deve permitir a inclusão de críticas quanto à obrigatoriedade do preenchimento do campo.

6.9.25 A requisição de serviços deve ser suportada por fluxos de trabalho estruturados definidos por administradores para o cumprimento da requisição, que incluam, pelo menos, estágios, tarefas e decisões

6.9.26 O portal de autosserviço deve permitir que usuários com as devidas permissões registrem incidentes e solicitações de serviços em nome de outros usuários.

6.9.27 O portal de autosserviço deve informar os tempos previstos de resposta e resolução do incidentes e requisições registrados pelo usuário final, com base nos acordos de nível de serviço firmados e configurados na solução.

6.9.28 O portal de autosserviço deve permitir que qualquer usuário final acompanhe o atendimento às suas requisições de serviço, a resolução de seus incidentes, participe de processos de trabalho para aprovações e autorizações e verifique o histórico de seus atendimentos fechados, através de uma seção para o acompanhamento dos eventos daquele usuário.

6.9.29 O portal de autosserviço deve permitir o encaminhamento e resposta pelo usuário final de pesquisas de satisfação, referentes aos serviços recebidos de prestadores de serviço.

6.10 Gerenciamento de Nível de Serviço para as solicitações e acompanhamentos dos Direitos dos Titulares

6.10.1 A configuração de níveis de serviço adequados para todos os provedores de serviços internos e externos do CONTRATANTE é vital para garantir que a qualidade na prestação de serviços esteja alinhada com as necessidades de negócio. Para isso, a solução deverá:

6.10.1.1 Permitir a definição de parâmetros que são utilizados para definir o Service Level Agreement - SLA, tais como: por CONTRATANTE, por servico, dentro de um calendário a que se aplica O SLA, meta de nível de serviço relacionados ao SLA, escalações automatizadas relacionadas ao SLA

6.10.1.2 Permitir a definição de critérios que possibilitem a associação de SLA a registros de atendimentos, incidentes, problemas, solicitações de mudanças e fluxos de trabalho do CONTRATANTE, automatizados na solução

6.10.1.3 Permitir a definição de alertas com regras que viabilizem a emissão de avisos de registros incidentes, problemas, mudanças, solicitações de serviço, tarefas e atividades de fluxos de trabalho que estejam próximos de limites de SLA estabelecidos.

6.10.1.4 Manter um histórico dos níveis mínimos de serviço para acompanhamento de desempenho dos serviços.

6.10.1.5 Permitir a definição do tempo de duração para os níveis mínimos de serviço ou percentual de disponibilidade de um item de configuração.

6.10.1.6 Indicar quando o nível de serviço não foi cumprido ou está próximo do não cumprimento.

6.10.1.7 Permitir definição de múltiplos SLA.

6.10.1.8 Permitir a criação de modelos de SLA para reutilização e facilidade de configuração de novos serviços.

6.10.1.9 Possuir um repositório único com todos os registros de SLA, consolidando os Acordos de Nível de Serviço e Acordos de Nível Operacional.

6.10.1.10 Permitir o acesso seguro e controlado às informações do processo de gerenciamento de níveis de serviço e de SLA.

6.10.1.11 Permitir gerenciar o ciclo de vida de SLA.

6.10.1.12 Permitir anexar SLA á qualquer processo ou fluxo de trabalho do CONTRATANTE, automatizado na plataforma.

6.10.1.13 Implementar e seguir corretamente o fluxo de Gerenciamento de Níveis de Serviço conforme prescrito na biblioteca ITIL V3.

6.10.1.14 Deverá ser capaz de monitorar automaticamente os tempos de resposta, resolução e escalação relacionados com SLA.

6.10.1.15 Deve permitir a configuração de contabilização de SLA apenas em horários definidos pelo CONTRATANTE, a exemplo da necessidade de contabilização de SLA apenas em horas úteis.

6.10.1.16 Deve garantir o monitoramento dos prazos não apenas do SLA, firmado entre TI e usuários finais, mas também entre equipes (OLA) e prestadores de serviço externos (UC).

6.10.1.17 A medição de prazos deve ser insumo para a composição de indicadores gráficos de performance, exibidos em painéis do tipo dashboards.

6.10.1.18 Permitir que eventos sejam disparados através da integração com ferramentas de monitoramento e gerenciamento de eventos e a contagem de seus prazos iniciados, para acompanhamento do atingimento dos limites definidos

6.10.1.19 Permitir emitir relatórios das métricas de SLA sem a necessidade de outra solução.

6.10.1.20 Deve permitir a automação da escalação e notificação, baseado nos tempos de resposta e resolução

6.10.1.21 Garantir a integração nativa entre o Gerenciamento de Níveis de Serviço com o Gerenciamento de Incidentes, Problemas e Mudanças, garantindo que a execução de ações siga tempos pré-definidos.

6.10.1.22 Deve ser capaz de alertar ao time e à gestão, caso um evento exceda um número específico de atribuições e escalações

6.11 Base de conhecimento sobre NORMAS DE PRIVACIDADE, Políticas, Termos e Normas

6.11.1 O gerenciamento do conhecimento de uma organização é fundamental não só para sua agilidade na entrega de serviço, mas também para a continuidade de seus serviços. Com isso, a solução deverá:

6.11.1.1 Possuir uma base de dados para armazenamento de artigos de conhecimento da organização.

6.11.1.2 Permitir configurar e gerenciar o ciclo de vida de registros de artigos de conhecimento.

6.11.1.3 Possuir recursos de pesquisa de soluções aos usuários enquanto registram as solicitações;

6.11.1.4 Possuir recurso para busca indexada, apresentando soluções para os atendentes;

6.11.1.5 Permitir classificar e atribuir categorias e pesos para o conhecimento;

6.11.1.6 Permitir a pesquisa de artigos de conhecimento nas telas de atendimento de registros dos processos de gerenciamento de incidente, mudança, problema, requisições.

6.11.1.7 Possuir campos de pesquisa de conhecimento, integrados com a base de conhecimento da solução, nas interfaces de solicitação e operação de aplicações, processos e fluxos de trabalho do CONTRATANTE.

6.11.1.8 Permitir gerenciar documentos de conhecimento estabelecendo prazos de validade e de revisão.

6.11.1.9 Permitir o gerenciamento de acesso de usuários aos artigos de conhecimento.

6.11.1.10 Permitir inserir ou anexar imagens, vídeos e textos em documentos de conhecimento.

6.11.1.11 Permitir a criação, adição, manutenção e remoção de artigos de conhecimento em uma estrutura definida e hierárquica de conhecimento.

6.11.1.12 Permitir pesquisar através de palavras-chave ou frases inteiras.

6.11.1.13 Deve controlar o processo de aprovação de um documento, antes do mesmo ser publicado na base de conhecimento.

6.11.1.14 Deve permitir o ranking de uso das informações de conhecimento e identificar as necessidades não atendidas por conhecimento, de forma que o próprio usuário final possa classificar a utilidade (ou não) do artigo de conhecimento.

6.11.1.15 Deve possuir uma interface fácil e iterativa para a consulta a base de conhecimento, tanto para o analista quanto para o usuário final.

6.11.1.16 Possuir lista de perguntas frequentes (FAQS) para cadastrar informações sobre problemas conhecidos, erros comuns, rotinas e procedimentos, permitindo a categorização das informações inseridas.

6.11.1.17 Deve possibilitar rastrear, automaticamente, quantas vezes um artigo ou informação de conhecimento foi utilizado.

6.11.1.18 Deve apresentar a integração nativa do Gerenciamento do Conhecimento com os demais processos (nativos da solução ou implementados para atendimento de processos de trabalho), permitindo, por exemplo, mas não limitado, a associação de documentos e artigos de conhecimento a eventos de Incidentes, Problemas e Mudanças.

6.12 Banco de Dados de Gerenciamento de Configuração - BDGC.

6.12.1 Quanto ao inventário de ativos de tecnologia, gerenciamento de ativos e itens de configuração, mapeamento de modelos de configuração de serviços e definição de linhas de base de configuração, a solução deverá:

6.12.1.1 Prover a descoberta de toda a infraestrutura, Itens de Configuração e seus respectivos relacionamentos de forma automática sem agentes instalados em ambiente on-premises ou em nuvem, para a população do BDGC.

6.12.1.2 Prover a descoberta dos serviços de negócio "top down" e criar um mapa abrangendo todos os dispositivos, aplicações e perfis de configuração referente a estes serviços de negócio.

6.12.1.3 Possuir uma base única de gerenciamento de ativos e itens de configuração podendo gerenciar tais itens independentemente da metodologia ou processo e que permita sua população de forma automatizada e manual.

6.12.1.4 Permitir inventariar e mapear serviços de negócio hospedados em nuvem privada, pública, híbrida ou em recursos locais.

6.12.1.5 Permitir a configuração de informações de cada tipo de ativo, permitindo adicionar e remover campos de informações de gestão do ativo.

6.12.1.6 Permitir o acesso seguro e controlado à base de dados do gerenciamento da configuração.

6.12.2 Deve implementar e seguir corretamente o fluxo de Gerenciamento de Configuração e Ativos de Serviço conforme prescrito na biblioteca ITIL V3 e deve permitir no mínimo:

6.12.2.1 Manter atualizadas características da configuração de ativos;

6.12.2.2 Manter atualizadas características da configuração de componentes de ativos;

6.12.2.3 Manter atualizados os relacionamentos entre ativos com possibilidade de

representação gráfica destes relacionamentos;

6.12.2.4 A representação gráfica do relacionamento entre ativos deve permitir o drilldown de informações, para obter detalhes do ativo, seus relacionamentos, seus usuários, ou seus componentes.

6.12.2.5 Permitir a criação manual de itens de configuração a partir de modelos pré-definidos (templates), para agilizar o preenchimento de informações e criação de relacionamentos entre ativos.

6.12.2.6 Permitir a criação livre de itens de configuração, para o registro e controle de itens que não se aplicam sob um padrão.

6.12.2.7 Permitir a criação manual de itens de configuração para aqueles tipos de ativos que não sejam eletronicamente inventariáveis.

6.12.2.8 Permitir o complemento de informações de um ativo, que não puderam ser eletronicamente inventariadas ou que não estavam disponíveis.

6.12.2.9 Permitir também o cadastro de itens não técnicos, como mobiliário, equipamentos que não pertençam à TI, dentre outros, sem prejuízo à capacidade de relacioná-los com outros itens, técnicos ou não, para a representação gráfica dos relacionamentos

6.12.2.10 Permitir o gerenciamento de todo o ciclo de vida do ativo, de acordo com as definições da biblioteca ITIL V3 ou conforme necessidades do CONTRATANTE.

6.12.2.11 Deve prover uma hierarquia de produtos que possua, pelo menos, uma classe, uma categoria, um tipo e seus itens. Exemplo: Software > Aplicações de Escritório > MS Office > Licença XYZ do MS Office 2010. Ou conforme necessidades de personalização do CONTRATANTE

6.12.2.12 Deve permitir a definição de atributos personalizáveis para itens de configuração, tais como, mas não limitado, a número de série, patrimônio, versão, localização, carga e taxa de depreciação.

6.12.2.13 Deve suportar a federação e reconciliação de dados com fontes de dados externas, para permitir manter as informações de ativos em bases de dados distintas do BDGC.

6.12.2.14 Oferecer um conjunto mínimo de relatórios gerenciais sobre itens de configuração, ativos e informações financeiras, para facilitar os processos de auditoria do Gerenciamento da Configuração e permitir a criação de relatórios e dashboards conforme as necessidades do CONTRATANTE.

6.12.2.15 Deve permitir a rápida identificação, recuperação e análise de todas as Requisições de Mudança associadas a um mesmo item de configuração.

6.12.2.16 Deve permitir a rápida identificação, recuperação e análise de todas os registros

de incidentes e problemas associados um item de configuração.

6.12.2.17 Prover o inventário das informações de hardware de estações de trabalho e servidores tais como: processador(es), memória, placa mãe, interface(s) de rede, protocolos de rede, System BIOS, System Slots, portas de 1/0, Devices, Discos (físicos e lógicos), file systems, recursos do sistema operacional, settings de região, controladoras (IDE, SCSI, USB) e outros, além de permitir a coleta e inserção de dados de inventário a partir do uso de arquivos externos.

6.12.2.18 Possibilitar a coleta, em plataforma Windows e Linux (servidores de rede), dos serviços existentes e as informações associadas a estes (Status, descrição etc.).

6.12.2.19 Deve ter um BDGC centralizado, para acesso a partir de qualquer processo nativo da solução ou fluxo de trabalho que tenha sido automatizado na solução.

6.13 Requisitos de usabilidade para a Equipe de Privacidade

6.13.1 A interface de uso e facilidades de manuseio da solução são essenciais para que a experiência dos usuários e sua produtividade sejam as melhores possíveis e para que as pessoas consigam extrair da plataforma os recursos e benefícios esperados para facilitar seu trabalho, executar atividades do dia a dia e gerenciar suas atribuições de forma integrada com outros processos e procedimentos de gestão do CONTRATANTE , Neste sentido, sem a necessidade de programação, a solução deverá:

6.13.1.1 Possuir uma mesma interface (Ex.: estilos de menus, listas e telas de registros, gráficos, dashboards, relacionamento de registros etc.) de navegação e uso em todos os fluxos de trabalho, processos e aplicações que sejam automatizadas dentro da solução.

6.13.1.2 Permitir inserir quantidade ilimitada de anexos em registros de trabalho, fluxos de trabalho e processos automatizados na solução.

6.13.1.3 Opcionalmente, admite-se a utilização de aplicações não nativamente WEB unicamente do lado dos operadores, não sendo admitido do lado do usuário final, para funcionalidades como desenvolvimento de modelos (formulários, relatórios, diagramas de fluxos, calendários, catálogo), exclusivamente para aquelas que dependem de tecnologias que deixaram de ser suportadas por navegadores, devendo-se, ainda assim, serem invocadas pela WEB sem necessidade de instalação prévia de qualquer aplicativo, mantendo-se toda a operação restante possível através de ambiente WEB.

6.13.1.4 A solução deverá possuir interface de acesso totalmente WEB para todas as funcionalidades (administração e uso).

6.13.1.5 A solução deverá possuir interface de acesso e todas suas telas de administração e uso em idioma português padrão Brasil.

6.13.1.6 A solução deverá possuir interface amigável e intuitiva para os usuários e administradores.

6.13.1.7 A solução deverá permitir ser operada em navegadores Internet Explorer, Microsoft Edge, Mozilla Firefox, Google Chrome e Safari.

6.13.1.8 A solução deverá permitir acesso controlado à solução por meio de usuário e senha e com autenticação utilizando serviços de Diretórios LDAP e Microsoft Active Directory-AD.

6.13.1.9 A solução deverá permitir a adequação de menus da interface de atendimento para cada operador, permitindo que o operador organize seus menus com os principais links que utiliza dentro da solução.

6.13.1.10 A solução deverá permitir a criação de menus específicos paras as aplicações e automatizações de fluxos de trabalho e processo do CONTRATANTE, desenvolvidos na solução.

6.13.1.11 A solução deverá permitir o desenvolvimento de formulários, sem a necessidade de programação e diagramação, para a inclusão, exclusão e alteração de campos escolhidos.

6.13.1.12 A solução deverá possuir interface de lista de registros de qualquer processo ou fluxo de trabalho da solução, seja nativo ou criado para O CONTRATANTE, totalmente customizável, permitindo adicionar, remover ou alterar a ordem das colunas no grid de visualização de registros.

6.13.1.13 A solução deve permitir a consulta global por texto livre, pesquisando em textos de eventos, registros e ações.

6.13.1.14 A solução deve permitir a criação de pesquisas e listas de registro sem a necessidade de programação e alteração de código fonte, inclusive por operadores não administradores da solução, a partir da definição dos critérios de pesquisa que devem ser aplicados sobre qualquer campo de um registro de evento.

6.13.1.15 A solução deverá permitir que consultas personalizadas à base de dados podem ser criadas e gravadas para uso posterior pelos times de suporte e gestão, fazendo uso das listas e grids para a apresentação dos resultados.

6.13.1.16 A solução deverá permitir aos usuários inserir e remover quantas colunas forem necessárias em sua lista e grids, desde que estas estejam na tabela de banco de dados ao qual estão sendo listados os registros.

6.13.1.17 A solução deverá permitir ordenar a lista de registros por qualquer das colunas do grid de visualização, de A a Ze de maior para menor, ou vice-versa.

6.13.1.18 A solução deverá permitir que as listas e grids de registros devem ser separados da janela de registro, permitindo consultar dados de outros registros enquanto realizando um novo cadastro em outra janela, sem consumir mais de uma licença de

uso por usuário conectado para este fim,

6.13.1.19 A solução deve permitir ser possível atualizar manualmente as consultas exibidas nas listas e grids (Refresh) sem fechar ou atualizar toda a janela atual do navegador.

6.13.1.20 A solução deve permitir abrir múltiplas listas e grids em janelas diferentes e facilmente alternar entre elas, utilizando apenas uma licença de uso por usuário.

6.13.1.21 O acesso às listas e grids, assim como às informações disponíveis, deve ser controlado por permissões de acesso e perfis de usuário, garantindo que cada usuário somente visualize as informações as quais tem acesso.

6.13.1.22 A solução deverá permitir criar filtros, inclusive com a combinação de mais de um parâmetro de filtro, na lista de registros em qualquer das colunas disponíveis na tela.

6.13.1.23 A solução deverá permitir que usuários realizem pesquisas e filtros avançados.

6.13.1.24 A solução deverá permitir que os usuários exportem para arquivos formato Excel, CSV e XML.

6.13.1.25 A personalização de listas e grids não devem depender de um usuário administrador, sendo facultado a qualquer outro operador a criação de suas próprias listas e grids, não estando restrito às listas e grids originalmente disponíveis na aplicação ou disponibilizadas pelos administradores.

6.13.1.26 A solução deverá permitir a alteração de registros, inclusive alterações em lote (vários registros), na própria tela de visualização de registros e grid da solução.

6.13.1.27 A solução deve possuir recurso que permita aos operadores fazer a listagem de todos os registros em sua fila ou fila de grupos de solução a que pertence, combinando registros de incidentes, requisições, mudanças e tarefas de processos.

6.13.1.28 A solução deverá permitir o relacionamento de tabelas de bancos de dados criadas para automação de aplicações, processos e fluxos de trabalho do CONTRATANTE, com tabelas e bancos de dados nativos da solução, sem a necessidade de programação ou alterações do código-fonte.

6.13.1.29 A solução deverá permitir o relacionamento entre registros de processos, projetos, aplicações e fluxos de trabalho automatizados na solução, sem a necessidade de programação ou alterações do código-fonte.

6.13.1.30 A solução deverá prover recursos que possibilitem a parametrização de regras para aprovações de fluxos de trabalho, processos, requisições e outros registros da solução, com base nas regras de negócio do CONTRATANTE, sem a necessidade de alteração do código-fonte.

6.13.1.31 A solução deverá permitir configurar aprovação em fluxos trabalho no mínimo com as seguintes regras para andamento do fluxo, sem necessidade de programação ou alterações do código-fonte:

6.13.1.31.1 Aprovação por um usuário específico;

6.13.1.31.2 Aprovação por conjuntos de usuários e regras específicas para sequência de aprovação;

6.13.1.31.3 Aprovação pelo gerente de um grupo solucionador;

6.13.1.31.4 Aprovação pelo gerente do solicitante;

6.13.1.31.5 Aprovação de acordo com o cargo e a estrutura de cargos da organização de forma recursiva (independentemente da quantidade de níveis ascendentes) e dinâmica (não atrelado à usuário específico);

6.13.1.31.6 Aprovação por quantidade definida de pessoas em um grupo de solução;

6.13.1.31.7 Aprovação por vários grupos de solução;

6.13.1.31.8 Aprovação por grupos de solução juntamente com usuário específico.

6.13.1.31.9 A solução deverá permitir a configuração, sem alteração de código-fonte, para aprovações que não se enquadram no subitem anterior.

6.13.1.31.10 A solução deverá permitir atribuir a um usuário ou grupo de usuários específico, o acesso à abertura, modificação e fechamento de registros.

6.13.1.31.11 A solução deverá permitir a delegação de responsabilidades, papéis e funções dentro da solução, para fins de substituição temporária do usuário principal.

6.14 Gerenciamento de Serviços, Tarefas e Incidentes de NORMAS DE PRIVACIDADE

6.14.1 A solução deve possuir nativamente suporte para os processos de gerenciamento de serviços de TIC a seguir. Para tanto, a solução deverá:

6.14.1.1 Permitir o registro de solicitações de serviços, por meio do portal de serviços ou de tela própria de requisições de serviço.

6.14.1.2 Permitir gerenciar o ciclo de vida de requisições de serviço.

6.14.1.3 Permitir vinculação de várias tarefas para o atendimento de em um mesmo registro de solicitação, inclusive para grupos de atendimento diferentes,

6.14.1.4 Permitir configurar fluxos de trabalho diferentes para cada solicitação, conforme necessidade da CONTRATANTE.

6.14.1.5 Permitir aos atendentes a visualização do fluxo de trabalho, a partir da tela do registro da solicitação.

6.14.1.6 Atender aos requisitos de aprovação de fluxos de trabalho descritos neste documento técnico.

6.14.1.7 Permitir a realização de atendimento da solicitação por fases, permitindo ainda a visualização gráfica das fases de atendimento e situação atual.

6.14.1.8 Permitir a criação de modelos de requisições de serviço permitindo a reutilização para configuração de outras requisições.

6.14.1.9 Deve possuir uma visão baseada em permissões do requisitante dos serviços no catálogo que o usuário tem direito a requisitar.

6.14.1.10 Deve automatizar o roteamento de requisições para a coleta das autorizações apropriadas.

6.14.1.11 Deve permitir que o usuário submeta requisições de serviço, mantenha a visibilidade detalhada do cumprimento da requisição e acompanhe todo o ciclo de vida do cumprimento de sua requisição, sem a necessidade de entrar em contato com a central de serviços para acompanhamento.

6.14.1.12 Deve permitir que indicadores de impacto, prioridade e urgência sejam atribuídos ao registro da Requisição de Serviço.

6.14.1.13 Deve orquestrar os processos de trabalho de requisições complexas através de tarefas sequenciais e paralelas.

6.14.1.14 Deve facilitar a geração de relatórios de requisições de serviço pelo próprio usuário sem a necessidade de intervenção de administradores.

6.14.1.15 Permitir Integração com sistemas de e-mail padrão de mercado, para envio de e-mails (alertas, notificações) de forma automática, ou manual (pelo operador), bem como troca de mensagens entre os profissionais da TI ou outros usuários da solução.

6.14.1.16 Deve permitir a criação de regras de negócio para requisições específicas ou grupos de requisições, para automatizar processos, tarefas e notificações.

6.14.1.17 Deve suportar a criação de Requisições, a partir de registros de incidentes.

6.15 Gerenciamento de Incidente relacionados à Não-Conformidade / Segurança das NORMAS DE PRIVACIDADE.

6.15.1 A solução deverá permitir o registro, a modificação, tratamento e o encerramento de incidentes.

6.15.2 A solução deverá permitir configurar e gerenciar o ciclo de vida de registros de incidentes de acordo com o processo do CONTRATANTE .

6.15.3 A solução deverá permitir consultar a Base de Conhecimento a partir da tela do registro do incidente.

6.15.4 Sugerir resoluções e apresentar informações, para resolução de incidentes, na tela do

registro de incidente, sem a necessidade de realizar pesquisa, oferecendo sugestões de resolução do incidente ao operador, apenas com a digitação ou preenchimento de campos básicos do registro de incidente.

6.15.5 A solução deverá permitir a integração com o Banco de Dados de Gerenciamento de Configuração – BDGC, para relacionamento de incidentes com serviços de negócio e outros itens de configuração.

6.15.6 A solução deverá permitir acessar mapas de serviço, para consulta ao relacionamento de itens de configuração, a partir da tela do registro do incidente.

6.15.7 A solução deverá permitir consultar, ou apresentar automaticamente, sem a necessidade de realizar pesquisa, outros registros de incidentes relacionados com o mesmo usuário solicitante.

6.15.8 A solução deverá permitir criar um registro de problema ou de mudança a partir da tela do registro de incidente.

6.15.9 A solução deverá permitir a associação e a manutenção de relacionamentos entre registros de incidentes e de problemas e outros tipos de registros da solução (Ex.: registros de riscos, registros de aplicações e fluxos de trabalho automatizados para o CONTRATANTE, registros de projetos, dentre outros), sem a necessidade de alteração do código-fonte.

6.15.10 A solução deverá permitir a priorização, atribuição e escalação automática dos incidentes baseados na categorização do registro.

6.15.11 A solução deverá permitir a escalação automática dos incidentes baseados em usuários afetados e intervalos de tempo pré-determinados.

6.15.12 A solução deverá permitir a integração com ferramentas de monitoração viabilizando a abertura e fechamento de registros de incidentes de forma automática conforme estado de eventos em ferramentas de monitoração.

6.15.13 A solução deverá permitir a integração com ferramentas de Application Performance Management - APM.

6.15.14 Apresentar automaticamente, sem a necessidade de realizar pesquisa, outros registros de incidentes relacionados com o mesmo usuário solicitante.

6.16 Gerenciamento de Evento relacionados à Não-conformidade/Segurança das Normas de Privacidade

6.16.1 A solução deverá permitir o registro, a modificação, tratamento e o encerramento de eventos de infraestrutura provenientes de ferramenta de monitoramento.

6.16.2 Permitir configurar e gerenciar o ciclo de vida de registros de eventos de acordo com o processo do CONTRATANTE .

6.16.3 A solução deverá permitir a integração com ferramentas de monitoração viabilizando a abertura e fechamento de registros de eventos de forma automática conforme estado de eventos em ferramentas de monitoração.

6.16.4 A solução deverá permitir a integração com o Banco de Dados de Gerenciamento de Configuração - BDGC da solução, permitindo a visualização, no próprio BDGC, de alertas gerados em serviços e outros itens de configuração.

6.16.5 A solução deverá permitir receber eventos de diversas fontes externas como os sistemas de monitoração: SCOM, Nagios, Zabbix, Zen, OSS, System Center, etc.

6.17 Gerenciamento de Mudança relacionados à Não-Conformidade/Segurança

6.17.1 A solução deverá permitir o registro, a modificação, tratamento e o encerramento de mudanças.

6.17.2 A solução deverá permitir configurar e gerenciar o ciclo de vida de registros de mudanças de acordo com o processo do CONTRATANTE.

6.17.3 A solução deverá permitir a configuração de "n" aprovações em fluxos de registros de mudança e atender aos requisitos de aprovações em fluxos de trabalho descritos neste documento técnico.

6.17.4 A solução deverá permitir o relacionamento de registros de mudanças com registros de incidente, problemas, riscos e outros registros da solução.

6.17.5 A solução deverá permitir o registro de novos incidentes, problemas e requisições de serviço a partir de um registro de mudança.

6.17.6 A solução deverá permitir o relacionamento de registros de mudança com serviços de negócio e outros itens de configuração, inclusive com "n" itens de configuração.

6.17.7 A solução deverá permitir identificar visualmente o conflito de calendário (data/hora) com outros registros de mudança programados ou em andamento.

6.17.8 A solução deverá permitir a criação de modelos de mudança para utilizar e facilitar o preenchimento de outros registros de mudança.

6.17.9 A solução deverá permitir aos operadores visualizar o fluxo de trabalho da mudança a partir da tela do registro de mudança.

6.17.10 A solução deverá permitir o encerramento de erros conhecidos, de problemas e de incidentes quando uma mudança relacionada a estes é implementada com sucesso.

6.17.11 A solução deve exibir alertas baseados em dados preenchidos para informar, por exemplo, conflitos de janelas de manutenção e impossibilidade de parada do IC.

6.17.12 A solução deve ser capaz de exibir a programação futura de mudanças, baseado

nas requisições de mudança registradas.

6.17.13 Dever ser possível alterar os valores da requisição de mudança durante o seu ciclo de vida, tais como, mas não limitado a prioridade, categoria, ICs e SLA, baseado em permissões.

6.17.14 A solução deve facilitar a produção do calendário de mudanças em suas diversas fases, tais como estágios de construção, implementação, testes e implantação.

6.17.15 Deve ser possível disparar consultas à base de conhecimento a partir do Gerenciamento de Mudanças.

6.17.16 Processos de trabalho (workflow) graficamente definidos devem poder ser associados à registros de mudança para automatizar tipos particulares de mudanças.

6.18 Requisitos de Interoperabilidade e Integração

6.18.1 Quanto a integração e interoperabilidade a solução deve:

6.18.1.1 A solução deverá permitir autenticação integrada com o serviço de Diretórios LDAP ou Microsoft Active Directory-AD.

6.18.1.2 A solução deverá permitir receber eventos de diversas fontes externas como os sistemas de monitoração: SCOM, Nagios, Zabbix, Zen, OSS, System Center etc.

6.18.1.3 A solução deverá permitir a integração com ferramentas de monitoramento de performance de aplicações (Application Performance Management - APM) do CONTRATANTE.

6.18.1.4 A solução deverá permitir a integração, importação e atualização em árvores de serviço (modelos de configuração) refletindo em tempo real, conforme alterações percebidas por ferramentas de APM do CONTRATANTE.

6.18.1.5 A solução deverá possuir conectores e tecnologias para se integrar com sistemas e Bancos de Dados do CONTRATANTE.

6.18.1.6 A solução deverá permitir a replicação programada (Ex. D-1) dos dados, metadados, informações e conhecimentos gerados pelo CONTRATANTE e hospedados em ambiente de nuvem da CONTRATADA.

6.19 Auditoria de Segurança das Normas de Privacidade

6.19.1 Auditoria automatizada das fontes abaixo e com as seguintes funcionalidades:

6.19.1.1 A solução deverá permitir a auditoria automatizada do Active Directory (incluindo Group Policy e Logon Activity; listagem de usuários inativos, notificação de expiração de senha) e uso de escala de privilégios.

6.19.1.2 A solução deverá permitir a auditoria automatizada de Políticas do Active Directory.

6.19.1.3 A solução deverá permitir a auditoria automatizada do Azure Active Directory utilizado no Microsoft Office 365.

6.19.1.4 A solução deverá permitir a auditoria automatizada do Exchange.

6.19.1.5 Microsoft Exchange Server 2016

6.19.1.6 Microsoft Exchange Server 2013

6.19.1.7 Microsoft Exchange Server 2010 SP1 e superior

6.19.1.8 A solução deverá permitir a auditoria automatizada do Exchange Online utilizado no Microsoft Office 365.

6.19.1.9 A solução deverá permitir a auditoria automatizada do Servidor de Arquivos Windows.

6.19.1.10 Windows Server - Sistema Operacional;

6.19.1.11 Windows Server 2019 6.25.1.6.3. Windows Server 2016

6.19.1.12 Windows Server 2012/2012 R2

6.19.1.13 Windows Server 2008 R2

6.19.1.14 Windows Server 2008 SP2 (32 e 64-bit)

6.19.1.15 Windows Desktop OS (32 e 64-bit):

6.19.1.16 Windows 10

6.19.1.17 Windows 8.1

6.19.1.18 Windows 7

6.19.1.19 A solução deverá permitir a auditoria automatizada do EMC

6.19.1.20 EMC VNX/VNXe/Família Celerra (CIFS configuração somente)

6.19.1.21 EMC Isilon 7.2.0.0- 7.2.0.4, 7.2.1.0- 7.2.1.2, 8.0.0.0, 8.1.0.0 (CIFS configuração somente)

6.19.1.22 A solução deverá permitir a auditoria automatizada do NetApp

6.19.1.23 NetApp ONTAP 9.0-9.6 (CIFS configuração somente)

6.19.1.24 NetApp Clustered Data ONTAP 8.2.1-8.2.3, 8.3, 8.3.1, 8.3.2 (CIFS configuração

somente)

6.19.1.25 NetApp Data ONTAP 8 em modo 7 (CIFS configuração somente)

6.19.1.26 NetApp Data ONTAP 7 (CIFS configuração somente)

6.19.1.27 6.25.1.9. A solução deverá permitir a auditoria automatizada do Nutanix e Nutanix Files 3.6

6.19.1.28 A solução deverá permitir a auditoria automatizada de Dispositivos de Rede:

6.19.1.29 Dispositivos Cisco:

6.19.1.30 Cisco ASA (Adaptive Security Appliance) 8 e superior

6.19.1.31 Cisco IOS (Internetwork Operating System) 12 e 15

6.19.1.32 Fortinet - FortiGate:

6.19.1.33 FortiOS 5, 6

6.19.1.34 SonicWall

6.19.1.35 SonicWall Web Application Firewall 2.0.X.X

6.19.1.36 SonicWall NSV 6.5.x.x with Sonicos 6.5.x

6.19.1.37 SonicWall SMA 11.4.x

6.19.1.38 Juniper Networks

6.19.1.39 VSRX com Junos OS 12.1, Junos OS 18.1

6.19.1.40 VMX com Junos OS 17.1

6.19.1.41 Palo Alto

6.19.1.42 Palo Alto com PAN-OS 8.0.0

6.19.1.43 A solução deverá permitir a auditoria automatizada do ambiente Oracle - Banco de Dados

6.19.1.44 Oracle Database 11g

6.19.1.45 Oracle Database 12c On-Premise (todas as edições)

6.19.1.46 Oracle Database 18c On-Premise

6.19.1.47 Oracle Database 19c On-Premise

6.19.1.48 Oracle Database Cloud Service (edição Enterprise)

6.19.1.49 A solução deverá permitir a auditoria automatizada do ambiente SharePoint

6.19.1.50 Microsoft SharePoint Server 2019

6.19.1.51 Microsoft SharePoint Server 2016

6.19.1.52 Microsoft SharePoint Foundation 2013 e SharePoint Server 2013

6.19.1.53 Microsoft SharePoint Foundation 2010 e SharePoint Server 2010

6.19.1.54 A solução deverá permitir a auditoria automatizada do SharePoint Online utilizada no Microsoft Office 365

6.19.1.55 A solução deverá permitir a auditoria automatizada do SQL Server

6.19.1.56 Microsoft SQL Server 2017

6.19.1.57 Microsoft SQL Server 2016

6.19.1.58 Microsoft SQL Server 2014

6.19.1.59 Microsoft SQL Server 2012

6.19.1.60 Microsoft SQL Server 2008 R2

6.19.1.61 Microsoft SQL Server 2008

6.19.1.62 A solução deverá permitir a auditoria automatizada do ambiente VMware.

6.19.1.63 VMware vSphere (ESX) 6.0-6.7

6.19.1.64 VMware vSphere Hypervisor (ESXI) 6.0-6.7

6.19.1.65 VMware vCenter Server 6.0-6.7

6.19.1.66 A solução deverá permitir a auditoria automatizada de Log de Eventos

6.19.1.67 Windows Server - Sistema Operacional:

6.19.1.68 Windows Server 2019 6.25.1.13.7. Windows Server 2016

6.19.1.69 Windows Server 2012/2012 R2

6.19.1.70 Windows Server 2008 R2

6.19.1.71 Windows Server 2008 SP2 (32 e 64-bit)

6.19.1.72 Windows Desktop OS (32 e 64-bit):

6.19.1.73 Windows 10

6.19.1.74 Windows 8.1

6.19.1.75 Windows 7

6.19.1.76 A solução deverá permitir a auditoria automatizada do Windows - Servidor

6.19.1.77 Windows Server - Sistema Operacional:

6.19.1.78 Windows Server 2019

6.19.1.79 Windows Server 2016

6.19.1.80 Windows Server 2012/2012 R2

6.19.1.81 Windows Server 2008 R2

6.19.1.82 Windows Server 2008 SP2 (32 e 64-bit)

6.19.1.83 Windows Desktop OS (32 e 64-bit):

6.19.1.84 Windows 10

6.19.1.85 Windows 8.1

6.19.1.86 Windows 7

6.19.1.87 A solução deverá permitir a auditoria automatizada do DNS

6.19.1.88 Windows Server - Sistema Operacional:

6.19.1.89 Windows Server 2019

6.19.1.90 Windows Server 2016

6.19.1.91 Windows Server 2012 R2

6.19.1.92 Windows Server 2012

6.19.1.93 Windows Server 2008 SP2 (32 e 64-bit)

6.19.1.94 A solução deverá permitir a auditoria automatizada do DHCP

6.19.1.95 Windows Server - Sistema Operacional:

6.19.1.96 Windows Server 2019

6.19.1.97 Windows Server 2016

6.19.1.98 Windows Server 2012 R2

6.19.1.99 Windows Server 2012

6.19.1.100 Windows Server 2008 R2

6.19.1.101 A solução deverá permitir a auditoria automatizada do IIS 7.0 e superior

6.19.1.102 A solução deverá permitir a auditoria automatizada do Oracle - Banco de Dados

6.19.1.103 Oracle Database 11g

6.19.1.104 Oracle Database 12c On-Premise (todas as edições)

6.19.1.105 Oracle Database 18c On-Premise

6.19.1.106 Oracle Database 19c On-Premise

6.19.1.107 Oracle Database Cloud Service (edição Enterprise)

6.19.2 A solução deverá permitir a auditoria automatizada do SharePoint:

6.19.2.1 Microsoft SharePoint Server 2019

6.19.2.2 Microsoft SharePoint Server 2016

6.19.2.3 Microsoft SharePoint Foundation 2013 e SharePoint Server 2013

6.19.2.4 Microsoft SharePoint Foundation 2010 e SharePoint Server 2010

6.19.2.5 A solução deverá permitir a auditoria automatizada do SharePoint Online utilizada no Microsoft Office 365

6.19.3 A solução deverá permitir a auditoria automatizada do SQL Server:

6.19.3.1 Microsoft SQL Server 2017

6.19.3.2 Microsoft SQL Server 2016

6.19.3.3 Microsoft SQL Server 2014

6.19.3.4 Microsoft SQL Server 2012

6.19.3.5 Microsoft SQL Server 2008 R2

6.19.3.6 Microsoft SQL Server 2008

6.19.3.7 A solução deverá permitir a auditoria automatizada de Atividade de Usuários

6.19.3.8 Windows Server - Sistema Operacional:

6.19.3.9 Windows Server 2019

6.19.3.10 Windows Server 2016

6.19.3.11 Windows Server 2012/2012 R2

6.19.3.12 A solução deverá permitir a auditoria automatizada do VMware

6.19.3.13 VMware vSphere (ESX) 6.0-6.7

6.19.3.14 VMware vSphere Hypervisor (ESXI) 6.0 - 6.7

6.19.3.15 VMware vCenter Server 6.0-6.7

6.19.3.16 A solução deverá permitir a auditoria automatizada de Atividade de Usuários

6.19.4 Windows Server - Sistema Operacional:

6.19.4.1 Windows Server 2019

6.19.4.2 Windows Server 2016

6.19.4.3 Windows Server 2012/2012 R2

6.19.4.4 Windows Server 2008 R2

6.19.4.5 Windows Server 2008 SP2 (32 e 64-bit)

6.19.4.6 Windows Desktop OS (32 e 64-bit):

6.19.4.7 Windows 10

6.19.4.8 Windows 8.1

6.19.4.9 Windows 7

6.20 Integrações de tecnologias

6.20.1 Além das fontes de dados monitoradas no produto, suporta integrações de tecnologia, através do uso de API de integração Integrar as trilhas de auditoria com a atividade dos seguintes sistemas e aplicativos:

6.20.1.1 A solução deverá permitir integrações com RADIUS - Servidor

6.20.1.2 Windows Server 2008/2008 R2

6.20.1.3 Windows Server 2012/2012 R2

6.20.1.4 Windows Server 2016

6.20.1.5 A solução deverá permitir integrações com Amazon Web Services

6.20.2 A solução deverá permitir integrações com Syslog - Genérico - baseado em sistemas operacionais Linux:

6.20.2.1 Red Hat Enterprise Linux 7 e 6

6.20.2.2 SUSE Linux Enterprise Server 12

6.20.2.3 openSUSE 42

6.20.2.4 Ubuntu 16

6.20.2.5 E outros dispositivos que suportem mensagens do tipo rsyslog.

6.21 Pesquisa (busca) Interativa

6.21.1 A solução deverá permitir a visibilidade completa da infraestrutura de TI do CONTRATANTE. Com uma conveniente interface de pesquisa interativa, permitindo investigar incidentes e navegar pelos dados coletados em toda a infraestrutura de TI. Ao executar uma pesquisa, o administrador não deverá estar limitado a uma determinada fonte de dados, tipo de alteração ou nome do objeto. A solução deverá permitir a criação de pesquisas flexíveis que forneçam resultados precisos sobre quem mudou o quê, quando e onde cada alteração foi feita.

6.21.2 A solução deverá permitir que as customizações de buscas com esses detalhamentos deverão funcionar nas seguintes fontes de dados:

6.21.2.1 Active Directory

6.21.2.2 Azure AD

6.21.2.3 Exchange

6.21.2.4 Exchange Online

6.21.2.5 File Servers (Servidor de Arquivos Windows, EMC, e NetApp)

6.21.2.6 Dispositivos de Rede

6.21.2.7 Oracle - Banco de Dados

6.21.2.8 SharePoint

6.21.2.9 SharePoint Online

6.21.2.10 SQL Server

6.21.2.11 VMware

6.21.2.12 Windows Serverfluxo

6.21.2.13 Group Policy

6.21.2.14 Logon Activity

6.21.2.15 User Activity (Video)

6.21.2.16 A solução deverá mostrar todas as entradas principais nos resultados da pesquisa.

6.21.2.17 A solução deverá permitir rastrear todas as alterações no plano de monitoramento, fonte de dados e escopo da auditoria e mostrar detalhes sobre ele (valores originais e alterados). Permitindo identificar o que foi alterado e por qual usuário.

6.22 Anomalias de comportamento

6.22.1 A solução deverá detectar anomalias de comportamento no seu ambiente de TI, como picos de atividade ou exclusões em massa de dados arquivados, permitindo análise e detecção de violação das políticas de segurança.

6.22.2 A solução deverá permitir a avaliação de anomalias de comportamento deve possuir emissão de alerta e fornecer uma visualização de alto nível com histórico detalhado da atividade. A solução deve manter o histórico de anomalias e fornecer a visão panorâmica dos padrões de atividade.

6.23 Gerenciar fontes e processar dados

6.23.1 A solução deverá permitir que na tela principal de gerenciamento, o usuário deverá poder executar as seguintes ações:

6.23.1.1 Excluir - remove a fonte do processamento; isso será removido dos resultados da pesquisa no devido tempo.

6.23.1.2 Recolher novamente - enfileira a origem para reprocessamento.

6.23.1.3 Reindexar - enfileira uma fonte ou item a ser reprocessado, com a verificação de alterações. Se forem encontradas alterações, o item será atualizado e reclassificado.

6.23.1.4 Reclassificar - enfileira uma origem ou item a ser reclassificado de acordo com as regras de classificação configuradas mais recentes

6.23.1.5 Pausar - pausa temporariamente o processamento de uma fila

6.23.1.6 Retomar - retoma o processamento de uma fila pausada

6.23.1.7 Adicionar ao grupo - permite que uma fonte seja movida para um contêiner lógico (grupo de origem), um grupo existente ou um recém-criado.

6.23.2 A solução deverá permitir, ao clicar no ícone do gráfico, exibir estatísticas específicas da fonte escolhida, de maneira semelhante ao painel principal.

6.23.3 A solução também deverá possibilitar:

6.23.3.1 Alterar a fonte / grupo selecionando o ícone "engrenagem"

6.23.3.2 Ver informações detalhadas selecionando o ícone "i"

6.23.3.3 Navegar até a fonte selecionando o ícone "link"

6.23.3.4 A solução também deverá possibilitar que ao clicar em uma linha de origem exibirá os dados rastreados diretamente abaixo, com opções ligeiramente reduzidas. Cada linha de origem também mostra estatísticas em cache detalhando o número de registros filho (Documentos) e o tamanho do conteúdo rastreado (Tamanho).

6.23.4 A solução também deverá possibilitar que ao clicar nos níveis possíveis na área de fontes, você pode percorrer toda a estrutura do conteúdo rastreado. Como alternativa, você pode usar ícones para alternar entre a exibição estruturada (pai / filho) e uma exibição plana que mostra todo o conteúdo em uma fonte. Também é possível filtrar a grade por:

6.23.4.1 Status da página

6.23.4.2 URL

6.23.4.3 Tipo (dividido entre tipos e arquivos de contêiner)

6.23.4.4 A solução deverá permitir verificar a listagem de documentos encontrados através da listagem em tela e através de relatório, contendo a localização de origem.

6.23.4.5 A solução também deverá possibilitar que cada um dos documentos possua um ícone indicando o tipo de arquivo, além de um link "Informações" que abrirá um pop-up, permitindo que usuário visualize as propriedades, o texto e as classificações do documento.

6.23.4.6 A solução também deverá possibilitar que cada documento também possua um status associado, mostrado em formato numérico. Ao clicar no número, será exibida uma representação textual do status.

6.23.4.7 A solução deve permitir a gravação de informações de classificações no sistema, com o campo de metadados gerenciados do SharePoint. Deverá conter um indicador se a gravação foi bem-sucedida ou se a gravação falhar, com descrição em texto identificando a falha.

6.23.4.8 A solução também deverá possibilitar que ao adicionar / gerenciar configurações de origem, as configurações mais usadas são exibidas por padrão. Possibilitar configurações adicionais dependendo da fonte.

6.24 Capacidades de Geração de Relatórios

6.24.1 A solução deve possuir uma área de gestão da ferramenta possibilitando a emissão de relatórios. O painel principal deverá possuir três gráficos de alto nivel, destacando o estado atual do processamento:

6.24.1.1 Progresso do documento - Uma exibição gráfica da exibição principal de estatísticas, assim que o processamento estiver concluído, os documentos serão alocados para totalmente processado ou erros;

6.24.1.2 Tamanho do índice - mostra a porcentagem de cada tipo de fonte sendo processada: arquivos, SharePoint, SQL e fontes da Web;

6.24.1.3 Cobertura de classificação - mostra a porcentagem de conteúdo classificado, discriminada por tipo, e a porcentagem de conteúdo que não recebeu nenhuma classificação automática.

6.24.2 A solução deve possibilitar filtrar e refinar a exibição, procurar as áreas que contêm a maior quantidade de documentos marcados com um termo específico ou revisar apenas conteúdo específico.

6.25 Visão geral das taxonomias incorporadas

6.25.1 A solução também deverá possibilitar a classificação de dados que vem com cerca de oito taxonomias, com centenas de regras de classificação prontas para uso. As quatro taxonomias principais cobrem uma ampla gama de informações pessoais, financeiras e de saúde sensíveis. As quatro taxonomias restantes derivam do conjunto principal. Eles são adaptados para atender aos requisitos de regulamentos específicos de proteção de dados (LGPD, GDPR, GLBA e HIPAA).

6.25.2 A solução também deverá possibilitar visualizar Registros Financeiros.

6.25.3 A solução deverá visualizar números de roteamento ABA, códigos IBAN / SWIFT, números de contas bancárias.

6.25.4 A solução deverá visualizar informações de identificação pessoal (PMI).

6.25.5 A solução deverá visualizar informações pessoais (nome completo, endereço residencial, data de nascimento), no mínimo, nos seguintes idiomas:

6.25.5.1 Inglês

6.25.5.2 Francês

6.25.5.3 Alemão

6.25.5.4 Italiano

6.25.5.5 Português

6.25.5.6 Espanhol

6.25.6 A solução também deverá possibilitar visualizar IDs nacionais, números de passaporte, carteiras de motorista, documentos de contribuinte etc. para, no mínimo, paises como:

6.25.6.1 Brasil

6.25.6.2 Canadá

6.25.6.3 França

6.25.6.4 Finlândia

6.25.6.5 Alemanha

6.25.6.6 Índia

6.25.6.7 Irlanda

6.25.6.8 Itália

6.25.6.9 Portugal

6.25.6.10 África do Sul

6.25.6.11 Espanha

6.25.6.12 Reino Unido

6.25.6.13 EUA

6.25.7 A solução também deverá possibilitar visualizar Informações de Saúde do Paciente (PHI), formulários médicos, registros de tratamento, medicamentos prescritos, nomes / códigos de falecimentos, alergias, números sociais e de seguros.

6.25.8 A solução também deverá possibilitar visualizar Taxonomias Derivadas, Regulamento Geral de Proteção de Dados (GDPR) Um subconjunto da taxonomia de PII relacionada às informações pessoais dos residentes da União Européia.

6.25.9 A solução deve estar Restrito ao GDPR, dados pessoais (iguais aos da PII) acompanhados pelas seguintes categorias especiais de informações pessoais (artigo 9 do GDPR):

6.25.9.1 Etnia

6.25.9.2 Ideologia política

6.25.9.3 Crenças religiosas

6.25.10 A solução deverá contemplar algumas taxonomias para detecção de dados pertinentes às Normas de Privacidade.

6.25.11 A solução deve permitir a criação e customização de outras taxonomias.

6.26 INTERFACE MOBILE PARA A EQUIPE DE PRIVACIDADE

6.26.1 A velocidade exigida pelo negócio, tanto em operações de Privacidade, quanto em operações de negócio do CONTRATANTE, também exige que Gestores, Técnicos e outros atores em processos e procedimentos, tenham a facilidade de uso e mobilidade para interagir com os processos da organização. Para tanto, é fundamental que a solução disponibilize meios práticos e modernos de interação das pessoas com suas funcionalidades por meio de dispositivos móveis. Com isso, sema necessidade de programação, a solução deverá:

6.26.1.1 Ser responsiva para dispositivos móveis podendo ser operada por meio de aplicativos mobile que opere nos sistemas operacionais Android, IOS e Windows Phone.

6.26.1.2 Possuir funcionalidades, para usuários e operadores solucionadores, que permitam interações com aplicações, processos e fluxos de trabalho automatizados;

6.26.1.3 Poder tomar decisões e realizar ações que possam afetar o fluxo de um workflow;

6.26.1.4 Poder visualizar e adicionar anexos;

6.26.1.5 Poder acessar menus configurados e personalizados na solução WEB;

6.26.1.6 Possuir chat e mensagens instantâneas entre usuários da solução;

6.26.1.7 Possuir notificações do tipo push.

6.27 ATUALIZAÇÕES, DESENVOLVIMENTOS E NOVAS INTEGRAÇÕES

6.27.1 Como a Privacidade é um processo vivo, está sujeito a evolução nos processos seguindo as diretrizes da ANPD, a Contratante necessitará de um processo continuo de sustentação para ajustes, definições, integrações, Q&A e deployment para produção, visando o pleno funcionamento de suas ações. Assim, é prudente estimarmos Unidade de Serviços Técnicos (UST) no processo para este tipo de serviço, garantindo a plena adequação independente das novas soluções do CONTRATANTE.

6.27.2 A implantação de tais políticas e procedimentos deverá ser promovida via mapeamento de processos e mecanismos de controle ainda desconhecidos, que a consultoria a ser contratada deverá viabilizar, tendo em vista o quadro técnico reduzido do CONTRATANTE.

6.28 REQUISITOS DO MÓDULO DE MAPEAMENTO DE DADOS PESSOAIS E DADOS PESSOAIS SENSÍVEIS (Questionário de inventário de Dados).

6.28.1 O módulo de mapeamento dos fluxos de dados pessoais (questionário de inventário) deve ser integrado aos demais módulos do sistema;

6.28.2 O módulo de mapeamento dos fluxos de dados (questionário de inventário) pessoais deve permitir o registro, atualização e consulta dos critérios utilizados para decisões automatizadas;

6.28.3 Deve possuir modelos de questionários pré-definidos que mapeiam especificamente os requisitos legais em regulamentos de privacidade brasileira;

6.28.4 Deve ter a capacidade de adicionar comentários por pergunta ao revisar o questionário preenchido;

6.28.5 Deve ter a capacidade permitir o envio de mensagens rápidas e interativas com os usuários preenchedores da plataforma, para dúvidas, registro de informações adicionais ou anexos.

6.28.6 Deve ter a capacidade de fazer upload de processos de negócios já analisados, sendo: Questionários de inventários, planos de ação, bases legais, etc.;

6.28.7 Deve possuir a funcionalidade de apoiar iniciativas de mapeamento de dados, incluindo mapeamento e análise de ativos e atividades de tratamento;

6.28.8 Deve ser capaz de armazenar informações sobre todos os itens acima, tais como classificação de atributos para cada ativo e atividade de processamento; Deve possuir recurso para suportar diferentes elementos de dados que se aplicam a indivíduos específicos, tais como funcionários internos, CONTRATANTEs externos e fornecedores;

6.28.9 Deve ser capaz de atualizar o inventário de dados quando houver qualquer alteração nas quantidades, finalidades e demais características de ativos, processos ou atividades de tratamento de dados pessoais;

6.28.10 Deve possuir recursos para visualizações de mapeamento de dados, como mapas de calor e gráficos de dados pessoais pro processo;

6.28.11 Deve possuir a capacidade de gerar relatórios de acordo com o Artigo 37 de Privacidade;

6.28.12 Deve possuir recurso que permita personalização dos relatórios de acordo com as necessidades da CONTRATANTE;

6.28.13 Deve possuir recuso para fazer reavaliação programada das atividades de mapeamento de dados;

6.28.14 Deve possuir recurso, como um painel de controle central, ou semelhante, com capacidade de classificação e filtragem;

6.28.15 Deve ter a capacidade de definir diferentes elementos de dados a serem associados a cada atividade de tratamento;

6.28.16 Deve permitir anexar documentos a um ativo ou atividade de tratamento individual;

6.28.17 Deve permitir o disparo de questionários para diversos respondentes via e-mail a partir da aplicação;

6.28.18 Deve permitir o envio de lembretes, via sistema e por e-mail, para os respondentes que receberam questionários para responder;

6.28.19 Deve permitir o envio de lembretes, via sistema e por e-mail, para os usuários cadastrados que tenham ações pendentes no sistema a serem executadas;

6.28.20 Deve registrar os riscos e controles aplicados a cada item do inventário (ativos, atividades de tratamento, fornecedores etc.);

6.28.21 Deve permitir a análise jurídica, definindo planos de ação, riscos, bases legais, teste de proporcionalidade do Legítimo Interesse, politicas, termos, normas e emissão do DPIA/LIA/ROPA;

6.28.22 A frequência e quantidade de lembretes deve ser, preferencialmente, personalizável.

6.29 REQUISITOS DE SEGURANÇA

6.29.1 A solução deve permitir a autenticação através do AD ou LDAP local da organização;

6.29.2 A solução deve permitir a criação de um login interno apenas se a conta existir no AD ou LDAP da organização;

6.29.3 A solução deve possuir mecanismo parametrizável de bloqueio da sessão e/ou logout automático por tempo de inatividade;

6.29.4 A solução deve prover mecanismo de segundo fator de autenticação;

6.29.5 Todas as funcionalidades da solução devem ser acessíveis através de um único login, sem necessidade de criação de logins adicionais;

6.29.6 A solução deve realizar o registro (logs) de todas as atividades ou tentativas de

login/logout, registrando, no mínimo, a identificação do usuário, computador, data, hora e endereço IP utilizados;

6.29.7 A solução deve ter a funcionalidade de criação de perfis de Controlador, Jurídico, TI (usuários administradores/aprovadores) e de usuário da plataforma, permitindo a criação desses papéis de acordo com as necessidades da contratante. Não poderá existir limitações de usuários preenchedores na plataforma.

6.29.8 Um perfil de acesso deverá ser composto de uma ou mais funcionalidades e/ou de um ou mais grupos;

6.29.9 A solução deve permitir a geração dos logs das atividades de administração da ferramenta e logs das atividades dos usuários, para fins de auditoria;

6.29.10 A solução deve permitir a consulta, pesquisa e geração de relatórios a partir dos logs de auditorias, conforme os itens de logs de auditoria especificados nesta seção;

6.29.11 A solução deve oferecer suporte para acesso de usuários externos, tais como fornecedores;

6.29.12 A criação de acesso para usuários externos deve ser controlada pelos administradores da solução, de forma que a identidade do usuário externo possa ser verificada antes da liberação do acesso;

6.29.13 A plataforma da solução deve possuir recursos para garantir a segurança das informações em trânsito e em repouso;

6.29.14 Quanto aos requisitos de segurança da aplicação, a solução deve atender, no mínimo, aos requisitos de segurança do framework OWASP;

6.29.15 Pré-requisitos para o ambiente SaaS:

6.29.16 O fabricante deve possuir em seu site evidências de que possui a certificação ISO/IEC 27017:2015;

6.29.17 O fabricante deve possuir em seu site evidências de que possui a certificação ISO/IEC 27001:2013;

6.29.18 O fabricante deve possuir em seu site evidências de que possui a certificação ISO/IEC 27018:2019;

6.29.19 O fabricante deve possuir em seu site evidências de que possui a certificação ISO/IEC 27701:2019;

6.29.20 O fabricante deve possuir em seu site evidências de que possui o relatório SSAE 18 SOC 1 e SOC 2;

6.29.21 A solução deve fornecer alta disponibilidade avançada (AHA) em clusters;

6.29.22 O fabricante deve atender ao Padrão BSI Cloud Computing Compliance Controls Catalog (C5);

6.29.23 O fabricante deve possuir em seu site evidências de que possui a Certificação Cyber Essentials Plus;

6.29.24 O fabricante deve possuir reconhecimento de Privacidade da APEC para Processadores (PRP)

6.29.25 O fabricante deve possuir ASD IRAP avaliado para serviços em nuvem OFICIAIS E PROTEGIDOS

6.29.26 O fabricante deve possuir deve ter Relatório SOC 2 + HITRUST

6.29.27 O fabricante deve possuir deve ter Certificação Cyber Essentials Plus

6.29.28 Os recursos de alta disponibilidade devem incluir, mas não se limitar a:

6.29.28.1 99,8% de disponibilidade ou mais;

6.29.28.2 Centros de dados (Datacenters) espelhados localizados em território nacional;

6.29.28.3 Redundância total;

6.29.28.4 Tolerância ao erro;

6.29.28.5 Balanceamento de cargas nos servidores;

6.29.28.6 Monitoramento de desempenho;

6.29.28.7 Processo de failover – RTO de 2 horas e RPO de 1 hora, no máximo;

6.29.28.8 Backup (Full) e recuperação de desastres;

6.29.28.9 Plano de Continuidade de Negócios.

6.30 REQUISITOS DO TREINAMENTO ONLINE NA SOLUÇAO.

6.30.1 A solução deverá disponibilizar em sua plataforma recursos de treinamento online para uso e administração da solução, tais como vídeo aulas, tutoriais etc.

6.30.2 Os cursos devem fazer referências e disponibilizar manuais de instalação, manuais de administração, manual do usuário, FAQs (Frequently Asked Questions), troubleshooting, etc., que devem ser acessíveis a partir da Internet ou da plataforma e obrigatoriamente 100% (cem por cento) em Português.

6.31 REQUISITOS DO MÓDULO DE ATENDIMENTO AOS DIREITOS DOS TITULARES

6.31.1 A solução deve ter capacidade para receber, processar e registrar uma solicitação de acesso dos titulares de dados;

6.31.2 A solução deve permitir fluxos de atendimento distintos e configuráveis para cada tipo de solicitação;

6.31.3 A solução deve permitir alterar ou definir outro fluxo de atendimento durante a execução de uma solicitação;

6.31.4 A solução deve possuir um portal seguro onde o titular de dados pode entrar e visualizar o status do(s) seu(s) pedido(s) submetido(s), validando a identidade do titular;

6.31.5 A solução deve fornecer recursos de atribuição automática e retribuição conforme necessário para cada ticket de solicitação de titulares;

6.31.6 A solução deve dispor de funcionalidade para selecionar e estender a solicitação do titular de dados;

6.31.7 A solução deve possuir fluxos de trabalho personalizáveis para processar todos as solicitações de titulares recebidos;

6.31.8 A solução deve possuir a funcionalidade de atribuir subtarefas dentro de uma solicitação de titulares;

6.31.9 A solução deve possuir formulários web personalizáveis onde os titulares de dados podem enviar seus pedidos;

6.31.10 A solução deve permitir que os titulares de dados possam enviar anexos nos formulários de solicitações, objetivando ajudar na verificação de sua identidade;

6.31.11 A solução deve possuir um painel de controle central para mostrar todas as solicitações recebidos em uma fila fácil de gerenciar;

6.31.12 A solução deve registrar através de um numero de protocolo todas as atividades realizadas, permitindo rastrear o titular em cada solicitação;

6.31.13 A solução deve gerenciar e monitorar o tempo restante para cada solicitação ser atendida, além dos SLA definidos no workflow de aprovação da solicitação, notificando o Controlador sempre que um SLA não for cumprido;

6.31.14 A solução deve fornecer protocolos de comunicação seguros com o titular de dados em relação ao seu pedido;

6.31.15 A solução deve fornecer modelos pré-definidos a serem usados para comunicação com um titular de dados referentes ao seu pedido, conforme os requisitos de

Privacidade;

6.31.16 A solução deve possuir recursos de geração de relatórios personalizados;

6.31.17 A solução deve registrar a entrega e o resultado de cada solicitação do titular de dados;

6.31.18 A solução deve registrar o fluxo, tempo e os fatores associados para cumprir o atendimento de cada solicitação.

6.31.19 A solução deverá permitir a integração do portal do titular com os processos de Data Discovery de dados estruturados e não estruturados, gerando as informações dos titulares de forma automática. Deverá permitir também a integração com os processos de negócio para busca de bases legais relacionadas ao titular.

6.31.20 A solução deverá permitir definir no portal do titular o Controlador que será responsável pelo atendimento das solicitações realizadas neste portal, sendo que um Controlador deverá poder ser cadastrado em mais de um portal. No registro da solicitação deverá ser identificado de qual portal veio a solicitação para o Controlador.

6.32 REQUISITOS DO MÓDULO DE GESTÃO DE CONSENTIMENTOS.

6.32.1 A Solução deve possuir um módulo para gestão de consentimento para o tratamento de dados pessoais;

6.32.2 A gestão do consentimento deve ser integrada aos demais módulos da solução, de forma a permitir o controle de quais processos/tratamentos usam consentimento, a finalidade do tratamento, quais dados e/ou dados sensíveis são tratados, o prazo de validade do tratamento.

6.32.3 A solução deverá possuir API's para integração dos processos de negócio da CONTRATANTE com o portal de consentimento da plataforma, devendo ser via portal Web e Smartphone.

6.32.4 Em complemento ao item anterior, a solução deve registrar os tratamentos de dados sensíveis e outras permissões realizadas através de consentimento;

6.32.5 Quando houver revogação de consentimento pelo titular, a solução deve notificar a necessidade de eliminação dos dados, exceto nas exceções previstas no art. 16 (o titular deve ter sido informado quanto às exceções de exclusão antes de fornecer o consentimento);

6.32.6 A Solução deve ser capaz de identificar os titulares que estão com o consentimento ativo e os titulares que solicitaram a revogação do consentimento;

6.32.7 A Solução deve controlar a validade do consentimento e solicitar novo consentimento ao usuário em caso de expiração;

6.32.8 A solução deve permitir a solicitação de novo consentimento caso uma nova finalidade de tratamento ou compartilhamento venham a ocorrer para os dados já coletados;

6.32.9 A Solução deve permitir que aplicações da contratante possam consultar o prazo de validade do consentimento, conforme técnicas especificadas no item 7.36.1;

6.32.10 A Solução deve permitir a consulta do histórico do consentimento concedido, por titular, data do consentimento, data da revogação do consentimento e sua finalidade. A consulta deve também ser disponibilizada ao titular pelo portal;

6.32.11 A Solução deve permitir realizar, no mínimo, as seguintes consultas: quais processos ou atividades possuem consentimento para uso de dados pessoais, quais são os sistemas que tratam esses dados, quais processo de negócio possuem consentimento para uso de dados pessoais, quantos titulares concederam o consentimento, e quantos titulares revogaram o consentimento;

6.32.12 A Solução deve fornecer um painel de controle central e recursos de relatórios que permitam ao Controlador avaliar o status, histórico, estatísticas e informações relacionadas de forma a verificar e comprovar a conformidade com o uso do consentimento para tratamento de dados pessoais e dados pessoais sensíveis realizados pela organização;

6.32.13 A solução deve permitir a integração do módulo de consentimento com as aplicações da contratante através de API, consolidando todos os consentimentos no portal da plataforma. A integração deve operar de forma bidirecional, permitindo que a aplicação seja informada quando o titular revogar o consentimento através do portal;

6.32.14 A solução deve possuir versão de aplicativo mobile para acesso e gestão dos consentimentos (opt-in e opt-out);

6.32.15 A solução deve gerar QR Code para redirecionamento para Plugin de site ou aplicativo de celular

6.33 REQUISITOS DO MÓDULO DE GESTÃO DE TERCEIROS

6.33.1 A solução deve permitir a avaliação de fornecedores e de terceiros;

6.33.2 A solução deve suportar a gestão de contratos e termos aditivos de fornecedores;

6.33.3 A solução deve permitir que os fornecedores acessem a aplicação usando um portal de autoatendimento;

6.33.4 A solução deve permitir que fornecedores respondam as avaliações via portal dentro da plataforma;

6.33.5 A solução deve possuir modelos pré-definidos de questionário de avaliação de fornecedores e permitir a customização desses modelos para criação de formulários de acordo com as necessidades da contratante;

6.33.6 A solução deve permitir a criação de questionários customizados a partir dos modelos existentes;

6.33.7 A solução deve prover a capacidade de auditar fornecedores externos de maneira personalizável;

6.33.8 O módulo de gestão de fornecedores deve permitir a geração de relatórios de gestão dos fornecedores;

6.33.9 A solução deve possuir um painel de controle para gestão dos fornecedores;

6.33.10 A solução deve permitir aos fornecedores que atuam como controladores conjuntos, registrar informações relativas às operações de tratamento sob sua responsabilidade;

6.33.11 O painel de controle de gestão de fornecedores deve permitir a criação de novos atributos para cada fornecedor de acordo com as necessidades da contratante;

6.33.12 A solução deve permitir aos fornecedores que atuam como operadores ou controladores conjuntos, consultar as informações relativas às operações de tratamento sob sua responsabilidade;

6.34 REQUISITOS DO MÓDULO DE GESTÃO DE RISCOS.

6.34.1 O sistema deve identificar os impactos para cada fluxo de dados de acordo com os critérios estabelecidos;

6.34.2 O sistema deve permitir o registro dos controles, das medidas, salvaguardas e mecanismos de mitigação de riscos identificados;

6.34.3 O sistema deve permitir o registro dos eventos e ameaças para o titular de dados, analisando a probabilidade de violação aos princípios de Privacidade, o impacto que as violações podem causar ao titular em relação ao processamento dos dados pessoais;

6.34.4 O sistema deve emitir o relatório de impacto de proteção de dados (RIPD/DPIA);

6.34.5 O sistema deve permitir a criação de workflow e acompanhamento das atividades subsequentes relacionadas aos riscos, a fim de garantir execução dos controles corretivos;

6.34.6 A solução deve permitir o registro e a consulta de todas as atividades relacionadas às recomendações para mitigação dos impactos identificados no RIPD/DPIA (tratativas e recomendações com sucessos e sem sucessos), com a guarda do histórico;

6.34.7 O módulo de riscos deve possuir integração com o módulo de mapeamento de fluxo de dados para que as atualizações deste sejam refletidas na análise de impacto do fluxo de dados em questão;

6.34.8 O módulo de riscos deve possuir modelos de questionários/avaliações predefinidos que mapeiam especificamente os requisitos legais de Privacidade, bem como deve permitir a importação de questionários criados pela CONTRATANTE;

6.34.9 Os questionários/avaliações devem suportar lógica condicional para o preenchimento;

6.34.10 A solução deve suportar pontuações de risco customizáveis;

6.34.11 A solução deve suportar a visualização dos riscos em um mapa de calor;

6.34.12 A solução deve suportar a avaliação quanto a eficácia dos controles aplicados aos riscos;

6.34.13 A solução deve suportar rastreamento de risco, sinalização e passos de mitigação de risco associados a cada incidente documentado.

6.34.14 A solução deve permitir filtros por criticidade e/ou nível de riscos para emissão do DPIA/RIPD.

6.35 REQUISITOS DO MÓDULO DE GESTÃO DE INCIDENTES

6.35.1 A solução deve permitir o registro dos incidentes relativos à violação de dados pessoais, seja por acesso não autorizado ou por perda de informação como também outros tipos de incidentes;

6.35.2 A solução deve permitir o registro das identificações do incidente e seus atores, como a descrição, data de registro, identificação do relator, o período da ocorrência, os processos, documentos, aplicativos de negócios envolvidos, áreas envolvidas e empregados envolvidos;

6.35.3 A solução deve permitir o registro das informações referentes ao local do incidente; natureza da violação de dados (acesso não autorizado, perda acidental de dados pessoais etc.); quantidade de titulares envolvidos; quais os dados pessoais envolvidos, impacto para os titulares dos dados, para quem o incidente já foi reportado;

6.35.4 O sistema deve permitir a integração de API nativa com aplicações ITSM, tais como: ServiceNow, JIRA e BMC;

6.35.5 O sistema deve permitir o registro das consequências prováveis da violação de dados, todas as evidências do incidente, seja descritivo ou através de documentos anexados;

6.35.6 O sistema deve permitir o registro das ações tomadas para resolver o incidente e plano de tratamento do incidente;

6.35.7 O sistema deve armazenar o registro do fato que resultou a perda, indisponibilidade, divulgação ou alteração de dados pessoais;

6.35.8 O sistema deve registrar e permitir o acompanhamento e situação do incidente até o seu encerramento;

6.35.9 O sistema deve possuir um workflow em que o Controlador faça a análise de todo o processo e realize a aprovação de encerramento do incidente;

6.35.10 O sistema deve permitir realizar as seguintes consultas: quantos incidentes foram abertos, concluídos em determinado período, quais os incidentes estão abertos, concluídos ou em andamento. Consulta detalhada do incidente com apresentação de todos os registros realizados (causa, impacto, ações tomadas, melhorias propostas, titulares envolvidos entre outros);

6.35.11 A solução deve gerar notificações automáticas por e-mail para as atividades dentro dos fluxos de trabalho;

6.35.12 A solução deve possuir fluxos de trabalho automatizados e customizáveis com subtarefas atribuíveis para cada incidente;

6.35.13 A solução deve suportar o rastreamento de risco, sinalização e passos de mitigação de risco associados a cada incidente documentado;

6.35.14 O módulo de incidentes da solução deve possuir formulário para comunicação do incidente à ANPD, conforme padrão https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca, nativamente na solução, a fim de permitir rastreabilidade e acompanhamento do andamento do caso.

6.36 REQUISITOS DO MÓDULO DE GESTÃO DE AVISOS DE PRIVACIDADE E GESTÃO DE COOKIES.

6.36.1 O sistema deve possuir um módulo para criação, revisão, aprovação e publicação de políticas e avisos em websites e aplicativos, bem como controle do versionamento das políticas;

6.36.2 Deve atualizar as Políticas de Privacidade e Segurança de Dados Pessoais de todos os websites;

6.36.3 Deve fazer varreduras nos websites para verificar inconsistências nas Políticas de Privacidade e Segurança de Dados Pessoais;

6.36.4 Deve manter as versões antigas das Políticas de Privacidade e Segurança de Dados Pessoais;

6.36.5 Deve integrar as Políticas de Privacidade e Segurança de Dados Pessoais em aplicativos móveis através de SDK;

6.36.6 Deve permitir a criação das Políticas de Privacidade e Segurança de Dados Pessoais usando modelos pré-definidos, em conformidade com a norma e voltados para governo e empresas públicas;

6.36.7 Deve permitir a importação da Política de Privacidade e Segurança de Dados Pessoais atuais;

6.36.8 O sistema deve possuir um módulo para gestão de consentimento de uso de dados pessoais e de Cookies;

6.36.9 O sistema deve prever a gestão de consentimento para uso de cookies nos domínios da organização, através de varredura de páginas dos websites e coleta de consentimento para cada situação específica;

6.36.10 O sistema deve executar uma varredura para identificar todos os cookies e outras tecnologias de coleta de dados que estão sendo utilizadas nos websites;

6.36.11 Deve ser capaz de coletar recibos de ciência das Políticas para colaboradores e parceiros;

6.36.12 Deve ter capacidade de associar Políticas de Privacidade e Segurança da Informação aos controles existentes em seu programa de privacidade;

6.36.13 Deve permitir verificar o histórico de versões e fornecer notificações quando são feitas alterações nas políticas;

6.36.14 Deve ter capacidade de expor as Políticas associadas a um usuário num portal de autoatendimento;

6.36.15 Deve permitir a integração com sistemas de gestão de conteúdo já existentes;

6.36.16 Deve possuir recurso par bloquear automaticamente os cookies sem necessitar de "tag Managers";

6.36.17 Deve de capacidade de automatizar e realizar uma auditoria completa de todos os domínios do site de nossa organização;

6.36.18 Deve fornecer relatório ou descrição de uso para cada um dos cookies de terceiros e outras tecnologias de coleta de dados do site identificadas na varredura;

6.36.19 Deve fornecer relatório detalhando os resultados da auditoria de cookies, devendo incluir, mas não se limitar a:

6.36.20 Todos os cookies e instâncias de outras tecnologias de dados do site encontrados;

6.36.21 identificar as tecnologias de captura de dados de cookies/site não declaradas nas políticas de cookies.

6.36.22 Deve ter capacidade de produzir uma política de cookies atualizada para cada domínio com base nos resultados da auditoria de cookies;

6.36.23 Deve ter a capacidade de criar um banner de cookie personalizado para cada site

verificado;

6.36.24 Deve suportar diferentes idiomas para os banners de cookies;

6.36.25 Deve ter a capacidade de detectar automaticamente o idioma de preferência do visitante do site;

6.36.26 Deve de possuir recurso para suportar diferentes modelos de consentimento de cookies para que possamos escolher;

6.36.27 Deve ser capaz de registrar o consentimento de cookies dos visitantes do nosso site;

6.36.28 Deve permitir o agendamento periódicos de auditorias;

6.36.29 Deve notificar através de e-mail quando novos cookies forem identificados após uma varredura agendada e/ou iniciada manualmente;

6.36.30 Deve ter capacidade de reter relatórios de cookies para cada página verificada e rastrear as mudanças.

6.37 REQUISITOS DO MÓDULO DE DATA DISCOVERY E DATA MAPPING PARA DADOS ESTRUTURADOS E NÃO ESTRUTURADOS - PESSOAIS E/OU SENSÍVEIS.

6.37.1 A solução/módulo de data discovery deve funcionar de forma totalmente integrada ao módulo de mapeamento de fluxos de dados pessoais, de maneira que o resultado do data discovery seja utilizado diretamente pelo mapeamento, permitindo seu relacionamento com os demais itens do mapeamento, permitindo relacionar os processos de negócio aos ativos de informação e dados obtidos pelo data discovery;

6.37.2 Deve possuir recurso para permitir classificadores personalizáveis;

6.37.3 Deve ter a capacidade de identificar dados pessoais e/ou sensíveis em bases estruturadas e não estruturadas;

6.37.4 Deve ser capaz de realizar varredura e identificação de dados pessoais sem a necessidade de instalação de agentes ou plugins no ambiente;

6.37.5 Deve permitir realizar varredura por amostragem;

6.37.6 Deve possuir recurso para realizar a varredura e descoberta, localmente e na nuvem;

6.37.7 Deve ter a capacidade de fazer a descoberta de dados pessoais e dados pessoais sensíveis através de OCR (reconhecimento ótico de caracteres) tanto em arquivos do tipo imagem (no mínimo JPG, JPEG, JFIF, PNG, BMP, GIF, SVG, WEBP, TIFF, PSD) quanto em PDFs salvos no formato PDF/Imagem;

6.37.8 Deve possuir recursos para avaliar e comparar as execuções do data Discovery, tais como: identificar novos itens ou itens que que deixaram de aparecer entre as execuções, dentre outros;

6.37.9 Apresentar a taxonomia para os dados pessoais e/ou sensíveis encontrados nos bancos de dados e repositórios analisados;

6.37.10 Destacar a presença de dados pessoais sensíveis dentre os resultados das análises;

6.37.11 Deve informar a origem dos dados pessoais descobertos (servidor, pasta, arquivo, banco de dados etc.);

6.37.12 A solução deve suportar a descoberta em banco de dados estruturados de forma nativa, no mínimo, nas plataformas de bancos de dados SQL/Server, Oracle, Mysql, Postgres, Progress e DB2 e de banco de dados não estruturados como Mongodb e MARIADB. Para os bancos de dados não suportados nativamente, a solução deve permitir a descoberta através de conectores JDBC;

6.37.13 A solução deve possuir recursos que permitam o desenvolvimento de conectores para bancos de dados Adabas ou a integração com ferramenta de terceiros que permitam a conexão com Adabas em ambiente Mainframe e baixa plataforma. No segundo caso, o fornecedor deverá prover as licenças necessárias para o conector;

6.37.14 A solução deve suportar a descoberta de dados não estruturados de forma nativa, no mínimo, nas plataformas servidores de arquivos Windows e Linux (PDF, XLS*, DOC*,PPT*, TXT, CSV, ODT, PST, MSG, SMB/NFS (File Server), imagem (boa resolução), etc.) e plataformas em nuvem Office 365, Google Drive, S3 Amazon, OneDrive, Hadoop HDFS.

6.37.15 A solução deverá permitir realizar auditoria e alertas em tempo real nos dados pessoais e sensíveis, identificando quem leu, alterou, incluiu ou excluiu documentos que possuem dados pessoais e/ou sensíveis.

6.38 REQUISITO DO MÓDULO DE PRIVACY BY DESIGN/DEFAULT.

6.38.1 A solução deverá possuir portal WEB que permita a avaliação dos itens previstos no PRIVACY BY DESIGN/DEFAULT, sendo:

6.38.1.1 Proativo, e não reativo; preventivo, e não corretivo

6.38.1.2 Privacidade como padrão (Privacy by Default)

6.38.1.3 Privacidade incorporada ao design

6.38.1.4 Funcionalidade total (soma positiva, não soma-zero)

6.38.1.5 Segurança de ponta a ponta

6.38.2 Visibilidade e transparência

6.38.3 Respeito pela privacidade do usuário

6.39 COMUNICAÇÃO INTEGRADA PARA O DPO, Equipe de privacidade, jurídico, ti e titulares de dados.

6.39.1 Todas as atividades de uma organização devem estar ligadas com objetivos institucionais, com projetos, processos de trabalho e consequentemente devem estar vinculados com registros de gestão. A comunicação por meio de serviços de correio eletrônico e aplicativos de mensagens instantâneas externos, impede e dificulta o rastreamento de informações de projetos e processos de trabalho do CONTRATANTE . Com isso, é fundamental que a plataforma permita uma comunicação completa e integrada entre os atores envolvidos nas operações de Privacidade . Para tanto, sem a necessidade de programação, a plataforma deverá:

6.39.1.1 Permitir a comunicação em tempo real entre CONTRATANTEs, usuários e atendentes dos serviços por meio de chat integrado à plataforma

6.39.1.2 Permitir que anotações de trabalho sejam registradas nos registros da solução, dando a opção aos operadores atendentes de publicar e deixar visível ou não para usuários solicitantes.

6.39.2 Manter as partes interessadas e envolvidas nos processos e atendimentos dos serviços do CONTRATANTE informadas, é essencial para manter uma comunicação efetiva e um atendimento ágil. Para atender a essa necessidade, a plataforma deverá:

6.39.2.1 Poder inserir notificações automatizadas em qualquer momento de fluxo de trabalho e processos automatizados na solução.

6.39.2.2 Poder enviar notificações com informações contendo dados de qualquer parte do registro de um fluxo de trabalho ou processo implementado na solução.

6.39.2.3 Poder enviar notificações baseadas em condições e eventos da solução incrementados ou alternados.

6.40 auditoria de políticas do active directory

6.40.1 Auditoria automatizada das fontes abaixo e com as seguintes funcionalidades:

6.40.1.1 A solução deverá permitir a auditoria automatizada do Active Directory (incluindo Group Policy e Logon Activity; listagem de usuários inativos, notificação de expiração de senha) e uso de escala de privilégios.

6.40.1.2 A solução deverá permitir a auditoria automatizada de Políticas do Active Directory.

6.40.1.3 A solução deverá permitir a auditoria automatizada do Azure Active Directory utilizado no Microsoft Office 365.

6.40.1.4 A solução deverá permitir a auditoria automatizada do Exchange.

6.40.1.5 Microsoft Exchange Server 2016

6.40.1.6 Microsoft Exchange Server 2013

6.40.1.7 Microsoft Exchange Server 2010 SP1 e superior

6.40.1.8 A solução deverá permitir a auditoria automatizada do Servidor de Arquivos Windows.

6.40.1.9 Windows Server – Sistema Operacional:

6.40.1.9.1 Windows Server 2019

6.40.1.9.2 Windows Server 2016

6.40.1.9.3 Windows Server 2012/2012 R2 6.25.1.6.5.

6.40.1.9.4 Windows Server 2008 R2

6.40.1.9.5 Windows Server 2008 SP2 (32 e 64-bit)

6.40.1.9.6 Windows Desktop OS (32 e 64-bit)

6.40.1.9.7 Windows 10

6.40.1.9.8 Windows 8.1

6.40.1.9.9 Windows 7

6.40.1.10 A solução deverá permitir a auditoria automatizada do ambiente SharePoint

6.40.1.11 Microsoft SharePoint Server 2019

6.40.1.12 Microsoft SharePoint Server 2016

6.40.1.13 Microsoft SharePoint Foundation 2013 e SharePoint Server 2013

6.40.1.14 Microsoft SharePoint Foundation 2010 e SharePoint Server 2010

6.40.1.15 A solução deverá permitir a auditoria automatizada do SharePoint Online utilizada no Microsoft Office 365

6.41 Serviços de hospedagem cloud

6.41.1 Especificações técnicas e funcionais

6.41.1.1 A Contratante deverá contar com uma disponibilidade de acesso 24 horas por dia, sete dias por semana. As políticas e a modalidade de acesso deverão ser especificadas em um manual de acesso ou documento de boas-vindas do Data Center.

6.41.1.2 O serviço de Colocation deverá prever as seguintes modalidades: mini rack, full rack, e cage. A Contratante poderá optar pela modalidade que melhor se ajuste a suas necessidades de negócio.

6.41.2 Condições de construção predial

6.41.2.1 As instalações dos Data Centers têm características definidas na sua construção para evitar ou minimizar os riscos de origem geológica e/ou meteorológica, contando com instalações em áreas que possam ter terremotos, ou contra furacões em áreas que cuja presença de furacões é freqüente.

6.41.3 Fornecimento de Energia Elétrica Garantida

6.41.3.1 A Contratada deverá ter o sistema de energia projetado de forma a garantir uma alta disponibilidade, tornando quase impossível a interrupção do serviço, ou mesmo a degradação da qualidade do serviço por falha no sistema. Não deverá existir qualquer ponto único de falha que possa interromper o fornecimento de energia para o ambiente dos equipamentos.

6.41.3.2 O Datacenter da Contratada deverá possuir um sistema completo de energia em redundância 3N+1. Toda a infraestruturadeverá ser dimensionada para que não haja nenhuma degradação do serviço, mesmo com a falha de um componente. A Redundância N+1 deverá ser aplicada aos geradores, retificadores, ar condicionado, no-breaks e alimentação elétrica, formando dois sistemas redundantes em paralelo. Entre os geradores e os racks deverão existir no mínimo2 (dois) circuitos elétricos totalmente independentes.

6.41.3.3 Todos os componentes rotativos (motores e geradores) e outras eventuais fontes de interferência eletromagnética deverão estar localizados em um edifício afastado do prédio de equipamentos. A subestação da Contratada deverá ter a energia fornecida pela concessionária em média em 13800 Volts com proteção e seccionada com disjuntores classe 15KV, isolamento SF6, relés de proteção secundária estáticos e transformadores de no mínimo 750 KVA, funcionando em configuração redundante n+1.

6.41.3.4 A infraestrutura de distribuição em baixa tensão deverá ser do tipo TN-C com 5 condutores (3 fases + neutro + terra), possuindo um barramento "não essencial" para as instalações prediais de uso de escritório, um barramento "essencial" ligado ao sistema de geração próprio e um barramento "crítico" (no break) ligado ao Sistema de UPS. A energia em baixa tensão deverá ser fornecida aos racks em 120V AC, podendo também ser fornecida em 220V AC ou 48V DC, conforme especificado pela Contratante.

6.41.3.5 O datacenter da Contratada deverá ter os sistemas de proteção e monitoramento de energia analisam permanentemente o estado de diversos parâmetros, tais como, consumo de corrente, tensões e fator de potência, podendo também ser monitorados remotamente. A automação deve ser realizada por um controle lógico inteligente com análise de demanda.

6.41.3.6 O sistema próprio de geração de energia dispõe de grupos geradores de 450 KVA cada, operando em paralelo e com unidades de supervisão (USCA) micro-processadas, com redundância N+1.

6.41.3.7 O sistema de combustível Diesel é composto por 1 tanque de grande capacidade que bombeia o óleo para tanques intermediários menores, usados para armazenamento de consumo e destes para tanques de pequena capacidade, para armazenamento técnico de cada grupo gerador.

6.41.3.8 O sistema de geradores tem autonomia para aproximadamente 7 dias sem reabastecimento, podendo ser reabastecido em carga. Convênios com distribuidoras de diesel, garantem a continuidade ilimitada da disponibilidade de energia elétrica.

6.41.3.9 O Sistema de "No Break" (UPS) deverá ser composto por no mínimo equipamentos Powerware de última geração em ligação 1+1 e com barramento interligado. Os UPS funcionam em modo "on line" contínuo, de forma a não provocar transientes.

6.41.3.10 A proteção contra descargas eletromagnéticas, descargas atmosféricas e aterramento seguem os padrões ETSI, ITU-T e NBR 113. O aterramento atende às recomendações ITU-T K-27. Todos os "cable trays", "racks" e gabinetes são aterrados.O sistema de administração redundante da energia elétrica dos Data Centers deverá fornecer potência limpa e independente a Contratante e sistemas críticos. O Sistema de No-Breaksdeverá consistir em sistemas múltiplos de No-Breaks. Caso um falhar, os demais podem assumir a carga sem exceder sua capacidade nominal. As baterias do No-Breakdeverão ser carregadas pela rede pública de energia elétrica ou pelos geradores redundantes de reserva nos Data Centers.

6.41.3.11 Os Data Centers deverão ser alimentados por transformadores dedicados e redundantes. O serviço entrante deverá ser respaldado respaldado e sustentado por painéis automáticos de transferência e geradores a diesel redundantes que verificam a qualidade da energia ou interrupções

6.41.3.12 As cargas elétricas deverão ser alimentadas por sistemas de No-Breaks paralelos e redundantes que são configurados como bridge estática automática e com circuitos de derivação manuais. Cada módulo de No-Breakdeverá ter seu próprio grupo de baterias com capacidade suficiente para manter a carga elétrica dos Data Centers por períodos de 30 minutos, tempo suficiente para a entrada em operação dos geradores a diesel, deverão requer até um minuto para a sua estabilização.

6.41.3.13 Em cada um dos Data Centers, deverão ter turbogeradores a diesel capazes de entrar em operação e se acoplarem automaticamente à rede elétrica em um minuto. Esses geradores deverão ter tanques de combustível que permitirão sua

realimentação externa, facilitando uma operação contínua com grande autonomia. Os geradores deverão contar com sistemas automáticos para que, após a inicialização, permaneçam em funcionamento somente o(s) gerador(es) que corresponda(m) à capacidade de energia demandada.

6.41.3.14 Deverão atender os padrões de conexão ao terraconforme especificações e recomendações pelas normas ITU-T K-27 e ETS1.

6.41.3.15 Cada rack ou mini-rack deverá ser alimentado por no mínimo dois PDUs, que são utilizados para melhorar a redundância dos equipamentos que possuem dupla fonte ou entrada de energia.

6.41.4 Sistema anti-incêndio

6.41.4.1 O sistema da supressão de incêndios nos Data Centers da Contratada deverão contar com sistema de detecção antecipada, que detecta a fumaça nas primeiras etapas da combustão por meio de um analisador de gases baseado em um raio laser que inspeciona a composição do ar dentro do Data Center. Este sistema de detecção deverá ser respaldado por sistemas iônicos de detecção de partículas

6.41.4.2 Caso um sistema de detecção de incêndio for acionado, os Data Centers deverão contar com um sistema de extinção redundante contra incêndios por meio da utilização de Gás FM200 ou similar mais moderno.

6.41.4.3 mecanismo de extinção de incêndios do agente FM-200 é ativo. Sua ação principal é esfriar fisicamente o incêndio a um nível molecular. O agente FM-200 (HFC-227) pertence ao mesmo tipo de compostos utilizados na refrigeração e, como tal, é um agente de transferência de calor eficiente.

6.41.4.4 FM-200 extrai literalmente a energia calorífica do incêndio até o ponto em que a reação de combustão não pode ser mantida. Além disso, há uma ação de extinção química atribuível ao agente FM-200. Durante um incêndio, pequenas quantidades de radicais livres são liberadas, que inibem a reação na cadeia de combustão.

6.42 Sistema de Controle Ambiental e Ar-Condicionado

6.42.1 Os Data Centers da Contratada deverão contar com um sistema de refrigeração baseado em equipamentos MCU (Modular CoolingUnits), que recebem o fluido refrigerado e insuflam ar refrigerado por baixo do piso elevado, forçando a saída do mesmo pela parte superior de cada rack. A infraestrutura deverá oferecer diversas unidades de ar-condicionado que irão assegurar uma adequada dissipação de calor. Caso uma unidade de ar-condicionado falhe, as outras unidades deverão compensar a carga térmica completa dos equipamentos alojados.

6.42.2 A Contratada deverá manter sempre múltiplas unidades MCU nos Data Centers, e elas deverão ser alimentadas pela rede de energia garantida para assegurar a continuidade das operações. Estas ainda deverão ser monitoradas por meio de um sistema de gerência – tipo SCADA, que permite a gestão e controles adequados para a detecção de qualquer falha. A temperatura nos Data Centers deverá ser mantida entre 17 a 27ºC. A umidade relativa dos

da Contratada Data Centers deverá ser controlada para que ela se mantenha sempre entre 40-60%, não permitindo desta forma a condensação.

6.42.3 A Contratada deverá ter um processo de verificação permanente do ar na sala de equipamentos, onde deverá ser possível detectar a presença de fumaça, estado dos filtros de pó, diferença de temperatura etc.

6.42.4 A Contratada deverá ter a infraestrutura dos equipamentos de refrigeração e controle configurados para atender ao esquema mínimo de redundância 2N+1.

6.43 Controle de Acessos

6.43.1 A segurança de cada Data Center é mantida por um sistema de vigilância por circuito fechado de televisão digital, alarmes de movimento e pessoal 24 horas por dia.

6.43.2 Existem câmeras montadas dentro e fora de cada edifício. A vigilância é monitorada localmente em cada local. As informações registradas nas câmeras são mantidas em meios magnéticos para posterior análise em caso de necessidade.

6.43.3 Os Data Centers exigem uma identificação biométrica ou cartão de proximidade, que permitem o acesso às diferentes áreas e salas. Estas são habilitadas pelo pessoal da CONTRATADA, utilizando tecnologia de última geração (scanners portáteis, leitores de impressão digital, etc.).

6.43.4 Controle de acesso às áreas de Colocation é realizado de forma rígida, e concedido apenas às pessoas autorizadas pela Contratante para este fim (consultar o processo de autorização no Anexo do Manual do Cliente de Data Center & Segurança).

6.44 Suporte

6.44.1 A CONTRATADA conta com Centros de Operação e monitoramento que funcionam 7X24 horas. Eles são responsáveis pela manutenção da infraestrutura que suporta a operação dos Data Centers, e oferece ajuda imediata frente a qualquer eventualidade.

6.44.2 Ao mesmo tempo, oferece equipamentos e peças redundantes em cada local para suportar substituições de emergência, e acordos com cada fornecedor dos serviços de infraestrutura, visando assegurar a continuidade da operação dos Data Centers.

6.45 Manutenção

6.45.1 Rotinas de manutenção periódicas são realizadas em todas as instalações.

6.45.2 Para o desenvolvimento das tarefas de manutenção, a CONTRATADA considerará as recomendações e procedimentos fornecidos pelos diferentes fornecedores de dispositivos e infraestrutura, visando garantir o cumprimento dos seus respectivos requisitos operacionais.

6.46 Especificação da solução de IaaS – Infraestrutrura como serviço

6.46.1 A infraestrutura básica para contratação deve seguir a tabela a seguir:

Infraestrutrua em nuvem		
TAMANHO DO ESCOPO QUANTIDADE DE BDS	50	
APLICAÇÃO PRINCIPAL	x1	8 vCPU 24 GB RAM 500 GB Disk
SERVIDOR PARA BD	x1	16 vCPU 64 GB RAM 500 GB Disk
SERVIDOR DE CORRELAÇÃO	x1	4 vCPU 16 GB RAM 500 GB Disk
SERVIDOR DE INTEGRAÇÃO	1	

tabela de especificação de servidores em nuvem

6.47 SOLUÇÕES DE GOVERNANÇA DE DADOS, PRIVACIDADE DE DADOS E SEGURANÇA DE DADOS

6.47.1 IMPLANTAÇÃO E INTEGRAÇÃO DE QUALQUER DAS SOLUÇÕES DEVE POSSUIR NO MÍNIMO OS SEGUINTES REQUISITOS:

6.47.1.1 A solução preferencialmente, na modalidade on-premise, deve fornecer a possibilidade de instalação do core da aplicação em sistema operacional open source e que tenha a sua funcionalidade de rodar em contêiner. Caso a solução seja entregue na modalidade nuvem, deve possuir uma nuvem própria ou utilizar de nuvens que atendam aos requisitos da ISO 27017.

6.47.1.2 Deve permitir integração nativa com fontes de dados estruturados

6.47.1.3 Microsoft SQL Server 2008 ou superior;

6.47.1.4 MySQL;

6.47.1.5 PostgreSQL;

6.47.1.6 DB2;

6.47.1.7 DB2 Mainframe;

6.47.1.8 MariaDB;

6.47.1.9 OracleDB;

6.47.1.10 Soluções de NoSQL;

6.47.1.11 Aurora DB;

6.47.1.12 SAS;

6.47.1.13 Vertica;

6.47.1.14 SAP Hana;

6.47.1.15 Deve permitir integração nativa com fontes de dados semi estruturados

6.47.1.16 MongoDB;

6.47.1.17 Deve permitir integração nativa com fontes de dados não estruturados

6.47.1.18 Microsoft Windows DFS;

6.47.1.19 Linux SMB;

6.47.1.20 EMC²;

6.47.1.21 NetAPP;

6.47.1.22 AWS S3;

6.47.1.23 Suite Office 365;

6.47.1.24 Google Workspace;

6.47.1.25 Deve permitir integração nativa com Data Lakes & Data Warehouses

6.47.1.26 Deve permitir integração nativa com Filas e Mensageria

6.47.1.27 Deve permitir integração nativa com bases Big Data & NoSQL

6.47.1.28 Deve permitir integração nativa com Aplicações

6.47.1.29 Deve permitir integração nativa com Sistemas de Arquivos

6.47.1.30 Deve permitir integração nativa com Emails & Mensagens

6.47.1.31 Deve permitir integração nativa com Middleware

6.47.1.32 Deve permitir integração nativa com Cloud SaaS

6.47.1.33 Deve permitir integração nativa com Cloud IaaS

6.47.1.34 Deve permitir integração nativa com Mainframe

6.47.1.35 Deve permitir integração com fontes de dados através do REST API

6.47.1.36 Deve permitir desenvolvimento de Conectores Customizados

6.47.1.37 Deve oferecer um inventario de todos os tipos de dados (tabelas, arquivos, filas, etc.), atualizado de maneira continua e automática, com apoio de Machine Learning

6.47.1.38 Deve contar com filtros (expressões) baseados no conteúdo e contexto (por exemplo, residências dos titulares vs geo-localização dos armazéns dos dados)

6.47.1.39 Deve permitir visualização das informações em mapas geográficos com as localizações dos sistemas e titulares

6.47.1.40 Deve permitir visualização do estilo "mapa de calor" dos sistemas com mais dados pessoais e sensíveis

6.47.1.41 Deve indicar a propriedade do objeto (donos, respectivamente técnicos e de negocio)

6.47.1.42 Deve permitir colaboração, como comentários nos objetos e possibilidade se seguir

6.47.1.43 Deve permitir enfio de notificações de maneira proativa, sobre mudanças nos objetos, aos destinatários interessados (seguidores, donos, stewards, etc.)

6.47.1.44 Deve indicar a correlação entre os dados armazenados em diferentes objetos, e conectá-los, junto com índice de confiança

6.47.1.45 Deve permitir descobrimento de Dark Data (dados obscuros, até então desconhecidos) e Shadow IT

6.47.1.46 Deve permitir realizar vista previa de conteúdo do objeto ou coluna, sem armazenar os dados

6.47.1.47 Deve indicar pontuação de exposição ao risco, em diferentes níveis, como coluna, atributo, objeto, entidade, sistema fonte e organização

6.47.1.48 Deve permitir classificação de objetos de acordo com os níveis de sensibilidade e criticidade do conteúdo

6.47.1.49 Deve permitir classificação de dados PI (informação pessoal) e PII (informação de identificação pessoal)

6.47.1.50 Deve permitir a varredura de informações utilizando algoritmos de aprendizado de máquina em dados não-estruturados

6.47.1.51 Deve permitir configuração das janelas e sistemas em quais especificas varreduras serão executadas

6.47.1.52 Deve permitir iniciar, pausar, e parar uma varredura manualmente

6.47.1.53 Deve permitir, através da interface do usuário, acompanhar o andamento das varreduras

6.47.1.54 Deve permitir visualizar uma lista dos objetos com erro, para os quais a varredura não pôde ser executada.

6.47.1.55 Deve suportar o uso de expressões regulares para encontrar dados pessoais em dados estruturados e não-estruturados

6.47.1.56 Deve suportar o uso da tecnologia OCR para classificar texto nos arquivos JPEG,JPG,BMP,GIF,PNG e PDF e imagens contidas dentro de arquivos Office.

6.47.1.57 Deve permitir manter uma lista de campos excluídos da analise, a serem ignorados pelas varreduras

6.47.1.58 Deve possuir capacidade de aperfeiçoar o tempo de varredura de dados não-estruturados utilizando machine learning, de acordo com seus metadados.

6.47.1.59 Deve fazer a classificação e busca de dados dos titulares sem manter cópias ou índices dos dados

6.47.1.60 Deve contar com, minimamente, as seguintes expressões regulares nativamente: (CPF, PIS, CNH, Titulo de Eleitor, IPv4, IPv6, IMEI, Email, Endereço MAC e Telefone)

6.47.1.61 Deve permitir a inclusão de novas expressões regulares e suportar a busca de termos próximos ao valor encontrado, para reduzir falsos positivos.

6.47.1.62 Deve suportar o treinamento de modelos de rede neural para classificar arquivos do negócio, como currículos, notas fiscais, invoices, etc.

6.47.1.63 Deve ter a capacidade de adicionar tags (etiquetas) nas propriedades dos objetos para que outros sistemas possam identificar sua classificação

6.47.1.64 Deve permitir customização dos tags (etiquetas) e aplicação automática de acordo com os critérios pré-estabelecidos ou padrões identificados através de machine learning

6.47.1.65 Deve suportar a utilização de expressões regulares para classificação de metadados

6.47.1.66 Deve ser possível realizar separadamente, a varredura de metadados, e de dados.

6.47.1.67 Deve construir um catálogo contendo todos os arquivos e tabelas escaneados durante as varreduras

6.47.1.68 Deve permitir a exportação de seus dados em formato CSV

6.47.1.69 Deve permitir a carga e a exportação de seus dados através de REST API

6.47.1.70 Deve possuir capacidade nativa de intercâmbio com ferramentas de catalogação no mercado

6.47.1.71 Deve ser capaz de indicar se um arquivo está duplicado em diversos sistemas

6.47.1.72 Deve permitir agrupamento dos arquivos em grupos lógicos, que contem as mesmas características (fatura, CV, cartão de embarque, etc.)

6.47.1.73 Deve ser capaz de indicar colunas similares, através de análise dos dados armazenados

6.47.1.74 Deve permitir filtrar os resultados por sistemas, tipos de dados, classificação, existência de dados pessoais e duplicados.

6.47.1.75 Ao apresentar tabelas de bancos de dados relacionais, deve exibir suas colunas e o tipo de dados (declarado e inferido na base de conteúdo)

6.47.1.76 Ao apresentar tabelas de bancos de dados relacionais, deve indicar qual coluna é a chave primária, caso exista.

6.47.1.77 Ao apresentar tabelas de bancos de dados relacionais, deve indicar a qualidade de dados por coluna: tipo inferido, % distintos, % nulos, valores min/max etc.

6.47.1.78 Ao apresentar arquivos, o catálogo deve indicar se possui permissões excessivas, como visualização ou edição, grupos Everyone, Domain Users, e Authenticated Users

6.47.1.79 Deve contar com dashboard que permita visualizar de forma prática a quantidade de objetos com permissões excessivas

6.47.1.80 Deve contar com dashboard que permita visualizar de forma prática quais sistemas possuem mais arquivos com permissões excessivas

6.47.1.81 Deve contar com dashboard que permita visualizar de forma prática quais sistemas possuem arquivos compartilhados com usuários externos à organização

6.47.1.82 Deve contar com dashboard que permita visualizar de forma prática quantas políticas de conformidade estão sendo atendidas ou infringidas

6.47.1.83 Deve permitir descobrimento quais dados são afetados por regulamentações com política pré-configuradas prontas para uso

6.47.1.84 Deve permitir criação de novas políticas e customização das existentes

6.47.1.85 Deve permitir configuração de gatilhos e critérios quantitativos (de violações)

6.47.1.86 Deve permitir identificação automática das quais políticas se aplicam as quais dadas confidenciais e sensíveis

6.47.1.87 Deve permitir revalidação das políticas a cada atualização (metadados ativos)

6.47.1.88 Deve permitir aplicação de tags (etiquetas) relacionadas com políticas out-of-the-box

6.47.1.89 Deve permitir aplicação de tags (etiquetas) relacionadas com políticas customizadas

6.47.1.90 Deve permitir auditoria e ações automáticas de acordo com as regras das políticas, e notificações

6.47.1.91 Deve permitir aplicação de novas políticas em escala à medida que as regulamentações mudam ou novas regulamentações são introduzidas

6.47.1.92 Deve possuir mecanismo para acionar APIs de outros sistemas a partir da violação de uma política

6.47.1.93 Deve fornecer relatórios de avaliação das varreduras, a estrutura, e logs

6.47.1.94 Deve permitir avaliação e exportação dos resultados das varreduras em relatórios detalhados

6.47.1.95 Deve permitir integração aberta com aplicações e sistemas do CONTRATANTE

6.47.1.96 Deve permitir integração com outros catálogos de dados e qualquer sistema fonte

6.47.1.97 Deve oferecer bibliotecas SDK para desenvolvimento customizado de novos módulos e conectores

6.47.1.98 Deve permitir disponibilização do conteúdo do catalogo aos cientistas de dados em bibliotecas Python

6.47.1.99 Deve contar com tecnologia de repositório de metadados com opção de replicação e alta disponibilidade nativa

6.47.1.100 Deve possuir opção de comunicação segura entre todos seus componentes, com criptografia SSL e certificados

6.47.1.101 Deve permitir arquitetura distribuída compreendendo ambientes híbridos, multi-cloud, e multi-datacenter

6.47.1.102 Deve permitir escalonamento horizontal sob demanda para atender tarefas computacionais intensas, como scans

6.47.1.103 Deve permitir instalação remota dos scanners para realizar varreduras perto das fontes e minimizar a transferência de dados e custos de data regress (caso aplica)

6.47.1.104 Deve permitir (arquitetura aberta) desenvolvimento customizado, para ampliação das funcionalidades nativas, como criação de novo módula e conectores adicionais

6.47.1.105 Deve possuir integração com o software de gerenciamento de senhas Senha Segura (vault)

6.47.1.106 Deve permitir integração com provedores de identidade IDM através de protocolo SAML ou LDAP para autenticação de usuários

6.47.1.107 Deve utilizar RBAC (com possibilidade de customização) para definir diferentes perfis de acesso às funcionalidades do sistema

6.47.1.108 Deve permitir a criação de escopos para limitar quais sistemas e dados são visíveis aos quais usuários

6.47.1.109 Deve possuir auditoria dos acessos realizados, seja através da interface de usuário ou diretamente através de API

6.47.1.110 Deve possuir a opção de exportar os logs do sistema e de auditoria através da interface de usuário

6.47.1.111 Deve ser disponibilizada através de protocolo web, para acesso através de navegadores

6.47.1.112 Deve ser compatível minimamente com os seguintes navegadores: Google Chrome, Apple Safari e Mozilla Firefox

6.47.1.113 Deve oferecer um dashboard para acompanhamento dos principais indicadores da solução

6.47.1.114 Deve oferecer um dashboard que fornece recursos gráficos como mapas e gráficos para melhor visualização das informações

6.47.1.115 Deve oferecer um dashboard que fornece atalhos para os principais recursos da solução e atividades

6.47.1.116 Deve permitir salvar as consultas e filtros, para que sejam refeitas de maneira prática posteriormente

6.47.1.117 Deve permitir envio de notificações por e-mail sobre novas atividades designadas

6.47.1.118 Deve permitir envio de notificações por e-mail sobre o andamento das varreduras

6.47.1.119 Deve permitir envio de notificações por e-mail sobre políticas em não-conformidade

6.48 MÓDULO DE GOVERNANÇA DE DADOS

6.48.1 Deve permitir analise de linhagem de dados, ao nível de objeto, para entender e rastrear a origem e como a informação foi transformado

6.48.2 Deve permitir analise de linhagem de dados, ao nível de coluna, para entender e rastrear a origem e como a informação foi transformado

6.48.3 Deve permitir realizar a analise de impacto, ao nível de objeto, para evolução proativa de impactos diretos e indiretos das mudanças planejadas

6.48.4 Deve permitir realizar a analise de impacto, ao nível de coluna, para evolução proativa de impactos diretos e indiretos das mudanças planejadas

6.48.5 Deve permitir integração com ferramentas terceiras especializadas em linhagem dedada, como por exemplo, Manta

6.48.6 Deve permitir geração de linhagem derivada dos dados e correlações e não somente dos metadados de integração e transformação

6.48.7 Deve permitir acompanhamento da mudança dos indicadores de qualidade de dados ao longo do processo de transformação

6.48.8 Deve permitir diferentes níveis de visão, desde linhagem detalhada até visão agregada e simplificada para melhor entendimento

6.48.9 Deve permitir exportação da linhagem de dados e relatórios da analise de impacto

6.48.10 Deve permitir criação manual de linhagem de dados, além das integrações com ferramentas terceiras

6.48.11 Deve oferecer um gerenciador de tarefas para que os Stewards possam priorizar e organizar o trabalho

6.48.12 Devem permitir colaboração entre Stewards, proprietários de negócios e proprietários técnicos

6.48.13 Deve permitir agrupamento de tarefas de administração semelhantes para processamento em lote

6.48.14 Deve usar Machine Learning para recomendar invés de selecionar manualmente os glossários de negócios

6.48.15 Deve permitir associação automática dos termos lógicos do glossário com ativos físicos em escala

6.48.16 Deve permitir pesquisa de glossário comercial para que os usuários encontrem termos e atributos

6.48.17 Deve permitir criação de hierarquias de domínios, atributos, termos para estrutura e compreensão

6.48.18 Deve permitir importação dos termos do glossário comercial de fontes de terceiros

6.48.19 Deve permitir enriquecer os catálogos de terceiros com termos do glossário

6.48.20 Deve permitir enriquecer os catálogos de terceiros associando termos lógicos do glossário a dados físicos

6.48.21 Deve permitir identificar automaticamente as informações pessoais e confidenciais em todos os ativos de dados

6.48.22 Deve permitir captura da finalidade de uso para justificação de armazenamento destes dados

6.48.23 Deve permitir mapeamento dos termos lógicos do glossário de negócios para ativos físicos

6.48.24 Devem permitir definição de regras personalizadas de qualidade de dados

6.48.25 Deve permitir gestão de regras de qualidade de dados em linguagem natural

6.48.26 Deve permitir tomar ações para os dados que não cumprem esperados níveis de qualidade

6.48.27 Deve permitir notificar aos proprietários dos dados sobre eventos de avaliação e resultados

6.48.28 Deve permitir avaliação com o Machine Learning para obter orientação sobre valores discrepantes

6.48.29 Deve permitir avaliação de regras de qualidade dos dados por colunas

6.48.30 Deve permitir avaliação de regras de qualidade dos dados por atributos (por exemplo CPF, e-mail, RG, etc.)

6.48.31 Deve permitir avaliação de regras de qualidade dos dados por objeto (tabela, coluna, etc.)

6.48.32 Deve permitir gerenciamento proativo de qualidade de dados

6.48.33 Deve permitir definição de regras reutilizável no nível organizacional, para gerenciar qualidade em fontes de dados, projetos e iniciativas

6.48.34 Deve permitir acompanhamento das tendências da qualidade na linha de tempo

6.48.35 Deve permitir gerenciamento de qualidade dos dados a partir de um único ponto de controle

6.48.36 Deve integrar para o catálogo as pontuações de níveis de qualidade de dados

6.48.37 Deve permitir integração com as tecnologias de fluxo de trabalho como Jira, ServiceNow, etc.

6.48.38 Deve permitir definição de políticas para gerenciamento do ciclo de vida dos dados

6.48.39 Deve permitir definição de políticas para retenção legal (ex. dados dos ex-funcionários, ações na justiça)

6.48.40 Deve permitir criação de políticas em critério de tempo (filtro de data)

6.48.41 Deve permitir criação de políticas em critério de metadados (ex. data de criação do documento, modificação, etc.)

6.48.42 Deve permitir criação de políticas em critério de classificação (atributos, sensibilidade, etc.)

6.48.43 Deve permitir analise automática de todos os dados para identificar quaisquer dados que violem as políticas

6.48.44 Deve permitir ações sobre os dados que precisam ser arquivados ou excluídos (remediação)

6.48.45 Deve permitir exportação e importação de políticas

6.49 MÓDULO DE PRIVACIDADE DE DADOS

6.49.1 Deve permitir a emissão de relatório de acesso aos dados do titular (dossiê), personalizado, com todas as informações relacionadas ao titular

6.49.2 Deve permitir a busca de dados pessoais iniciadas através do nome ou código único de identificação, como o CPF

6.49.3 Deve permitir rastreamento dos dados pessoais retornados pelo inventário na busca de um titular até a tabela onde foram encontrados

6.49.4 Deve permitir rastreamento dos dados pessoais retornados pelo inventário na busca de um titular até o arquivo onde foram encontrados

6.49.5 Deve permitir a requisição e obtenção do dossiê através de API

6.49.6 Deve permitir inclusão no dossiê também dos registros de consentimento coletados do titular

6.49.7 Deve permitir deleção de dados sobre solicitação do titular ou gestão de fluxo de trabalho com controle de tarefas manuais

6.49.8 Deve permitir emissão do dossiê em formato PDF ou CSV

6.49.9 Deve fazer a busca de dados do titular automaticamente (sem intervenção) e sob demanda, buscando sempre os dados mais atuais nas fontes de dados

6.49.10 Deve permitir solicitações em lotes, por mais que um titular numa solicitação

6.49.11 Deve permitir diferentes perfis de dossiê, de acordo com o relacionamento com o titular, exemplos: funcionário, ex-funcionário, CONTRATANTE, fornecedor, etc.

6.49.12 Deve contar com um mecanismo que garanta que os dados foram de fato excluídos e que permaneçam excluídos, mesmo em caso de restauração de backup, por exemplo.

6.49.13 Deve prover um portal de autoatendimento para que o próprio titular possa realizar suas solicitações

6.49.14 Deve permitir, no mínimo, solicitações de acesso, retificação e remoção dos dados, bem como alteração das preferências de consentimento.

6.49.15 Deve possuir integração com protocolo OAUTH para autenticação dos solicitantes

6.49.16 Deve permitir controles de segurança como confirmação positiva de e-mail e telefone para validação dos dados

6.49.17 Deve permitir customização do questionário de solicitação

6.49.18 Deve permitir envio de imagens e documentos para comprovação da identidade do solicitante

6.49.19 Deve permitir a configuração de fluxos de trabalho, possibilitando inclusive a entrega completamente automatizada do relatório final para o titular.

6.49.20 Deve fornecer dashboard para que o gestor de privacidade possa ter uma visão agrupada das requisições, minimamente: data, tipo da solicitação, e prazo/em atraso.

6.49.21 Deve fornecer ao titular uma interface com os dados originais e permiti-lo alterar estes dados

6.49.22 Deve permitir ao gestor a revisão das informações antes de serem enviadas ao solicitante

6.49.23 Deve possuir auditoria das solicitações, dos revisores e dos aprovadores

6.49.24 Deve ser capaz de ler diversas fontes de consentimento para identificar quais consentimentos foram dados por cada titular

6.49.25 Deve permitir documentação dos termos de privacidade disponíveis, com sua localização (URL), versão e tempo de validade, relacionando-os às bases legais

6.49.26 Deve permitir emissão de um relatório das bases legais, e quais dados estão relacionados a elas

6.49.27 Deve permitir emissão de um relatório de propósitos de utilização, e quais dados estão relacionados a eles

6.49.28 Deve permitir registro de consentimento do titular

6.49.29 Deve permitir gestão de consentimento do titular

6.49.30 Deve permitir validação do consentimento e violações

6.49.31 Deve permitir integração de base externa com registros de consentimento

6.49.32 Deve permitir documentação dos termos legais de consentimento

6.49.33 Deve permitir documentação do propósito de armazenamento dos dados

6.49.34 Deve permitir documentação da base legal para armazenamento de dados

6.49.35 Dever permitir múltiplos canais de consentimento (CONTRATANTE, fornecedores, funcionário, etc.)

6.49.36 Devem permitir customização de acordos, baseados em regulamentações ou políticas internas

6.49.37 Deve oferecer ao titular centro de gestão de preferências

6.49.38 Devem correlacionar automaticamente os consentimentos e preferências

6.49.39 Deve identificar todos os cookies e outras tecnologias de coleta de dados estão sendo utilizadas nos sites

6.49.40 Deve incluir a auditoria de páginas web onde a autenticação do usuário é necessária

6.49.41 Deve fornecer uma descrição de uso para cada um dos cookies de terceiros e outras tecnologias de coleta de dados do site identificadas na varredura

6.49.42 Deve possuir a capacidade de gerar relatórios: todos os cookies e instâncias de outras tecnologias de dados do site encontrados

6.49.43 Deve possuir a capacidade de gerar relatórios: identificar as tecnologias de captura de dados de cookies/site não declaradas nas políticas de cookies

6.49.44 Deve possuir a capacidade de produzir uma política de cookies atualizada para cada domínio com base nos resultados da auditoria de cookies

6.49.45 Deve possuir a capacidade de criar um banner de cookies personalizado para cada site verificado

6.49.46 Deve possuir a capacidade de que o banner de cookies para cada domínio seja "estilizado" de forma diferente de acordo com as orientações da marca desse domínio

6.49.47 Deve registrar o consentimento de cookies dos visitantes dos sites

6.49.48 Deve possuir a capacidade de adicionar uma descrição de cookies novos/desconhecidos antes da política de cookies ser publicada

6.49.49 Deve permitir que realização das auditorias automatizadas não degrade ou prejudica o desempenho em tempo real dos sites auditados

6.49.50 Deve permitir auditorias automatizadas realizadas pelo menos a cada trimestre

6.49.51 Deve possuir a capacidade de reter relatórios de cookies para cada página verificada e rastrear as mudanças

6.49.52 Deve possuir a capacidade de bloquear automaticamente os cookies das categorias as quais o visitante não deu consentimento

6.49.53 Deve permitir mapeamento de processos de negócios, atores, bases de dados e aplicações envolvidas

6.49.54 Deve permitir gestão e visibilidade de atividades de processamento de dados

6.49.55 Deve permitir monitoramento das atividades de processamento de dados

6.49.56 Deve permitir sinalizar riscos relacionados com envolvimento de dados confidenciais e sensíveis

6.49.57 Deve permitir criação de modelos padrão de processamento de dados a partir das descobertas realizadas

6.49.58 Deve permitir carregamento manual dos modelos de processamento de dados

6.49.59 Deve permitir descobrimentos de compartilhamento de dados com terceiros

6.49.60 Deve permitir documentação de compartilhamento de dados com terceiros

6.49.61 Deve permitir geração de relatórios de processamento de dados

6.49.62 Deve permitir geração de relatórios de compartilhamento de dados com terceiros

6.49.63 Deve permitir avaliação de risco dos processos de negócios

6.49.64 Deve permitir gestão da conformidade com regulamentações

6.49.65 Deve permitir revisão e aplicação das recomendações sobre processos de negocio para agilizar a documentação

6.49.66 Deve permitir exportação da documentação dos processos em formato PDF, ou semelhante

6.49.67 Deve permitir mapear e documentar fluxos de risco de privacidade

6.49.68 Deve permitir mapear e documentar a estrutura organizacional de privacidade

6.49.69 Deve permitir avaliação de risco relacionado aos terceiros

6.49.70 Deve permitir colaboração na avaliação de risco

6.49.71 Deve permitir medição níveis de acessos e exposição publica

6.49.72 Deve permitir documentação das transferências de dados

6.49.73 Deve alterar em função de acionamento dos gatilhos de nível de risco

6.49.74 Deve permitir gestão de fluxos de trabalho de correção de dados (remediação)

6.49.75 Deve oferecer as trilhas de auditoria e relatórios

6.50 MÓDULO DE SEGURANÇA DE DADOS

6.50.1 Deve permitir identificação dos usuários e contas com privilégios excessivos

6.50.2 Deve permitir identificação dos dados super expostos por sensibilidade

6.50.3 Deve fornecer a visibilidade de acessos no nível interno e externo, por sensibilidade

6.50.4 Deve sinalizar e permitir investigação dos problemas de alto risco

6.50.5 Deve integrar para o catálogo os objetos com acessos ou permissões excessivas

6.50.6 Deve permitir integração com ferramentas como MIP e DLP para reforçar o cumprimento

6.50.7 Deve permitir correção dos conjuntos de dados com violações e problemas de risco, com orquestração de fluxo de trabalho

6.50.8 Deve priorizar as descobertas por sensibilidade e nível de risco de exposição

6.50.9 Deve permitir atribuir atividade de correção relacionada com conjuntos de dados

6.50.10 Deve permitir delegar as atividades de correção por função, escopo e usuário

6.50.11 Deve permitir automação de ações de remediação como deleção, quarentena

6.50.12 Deve permitir coleção de informações para trilha de auditoria das ações tomadas

6.50.13 Deve permitir colaboração entre as equipes e comentários

6.50.14 Deve permitir integração com ferramentas terceiras para anonimização, criptografia, aposentadoria, etc.

6.50.15 Deve permitir integração com ferramentas como MIP e DLP para reforçar o cumprimento

6.50.16 Deve permitir carregamento de amostra de dados vazados para análise do conteúdo e identificação dos titulares envolvidos

6.50.17 Deve permitir carregamento de amostra de dados vazados para identificação (pela sua semelhança) qual dos sistemas monitorados foi possivelmente comprometido

6.50.18 Deve permitir evolução e pontuação de risco de exposição de acordo com os dados vazados

6.50.19 Deve permitir identificação de dados regulamentados super expostos

6.50.20 Deve permitir identificação e monitoramento continuo de dados confidenciais super expostos

6.50.21 Deve permitir identificação dos usuários com privilégios excessivos

6.50.22 Deve permitir identifique de dados confidenciais e sensíveis duplicados (superfície de ataque)

6.50.23 Deve permitir atribuição de pontuações de risco com base na fonte de dados

6.50.24 Deve permitir atribuição de pontuações de risco por tipo de dados (classificação de atributos)

6.50.25 Deve permitir atribuição de pontuações de risco por país de residência do titular

6.51 Integração dos Módulos

6.51.1 Os módulos de Privacidade, Governança e Segurança devem conter nativamente os seguintes conectores:

6.51.1.1 Deve permitir integração com as tecnologias de fluxo de trabalho como Jira, ServiceNow, e outros soluções de ITSM, ITOM e Projetos.

6.51.1.2 Deve permitir integração nativa com ferramentas de risco dos terceiros, com RSA Archer, ServiceNow, Collibra, Alation, etc.

6.51.1.3 Deve contar com integração nativa com ferramentas como Salesforce, ServiceNow, Jira, SAP, etc.

6.51.1.4 Deve permitir autodescobrimento de dados nos ecossistemas GCP, Azure e AWS

6.51.1.5 Deve contar com integração nativa com ferramentas Vault como CyberArk e HashiCorp.

6.52 SOLUÇÃO EM NUVEM COMPUTACIONAL PARA GERENCIAMENTO DE SERVIÇOS, GESTÃO DE RISCO E CONFORMIDADE, DEVOPS E INTEGRAÇÃO

6.52.1 REQUISITOS FUNCIONAIS GERAIS DA SOLUÇÃO

6.52.1.1 A automação de processos e fluxos de trabalho da solução deve ser interativa, prática e de fácil implementação. O desenvolvimento de soluções ágeis e dentro da velocidade que o negócio da CONTRATANTE exige, deve ser suportado pela solução, para tanto, a solução deve suportar a criação de soluções, automações de fluxos de trabalho, processos de TI e de negócio e suportar a implementação de rotinas e processamento de funcionalidades com uma programação mínima e básica (Low-Code), usando componentes integrados e nativos da própria plataforma.

6.52.1.2 A solução deverá ser ofertada na modalidade Software como Serviço - SaaS, em nuvem com Data Centers localizados exclusivamente em território nacional, sem qualquer replicação de dados no exterior.

6.52.1.3 Deve ser assegurado que dados, metadados, informações e conhecimento, produzidos ou custodiados em decorrência da prestação de serviços, bem como suas cópias de segurança, residam em território brasileiro, para tanto, a empresa contratada deve garantir a territorialidade única na prestação do serviço, em vez de um ambiente tecnológico multinacional, não sendo admitida nenhum tipo de replicação para fora do país, tão pouco o fornecimento de informações.

6.52.1.4 Deverão ser garantidos a disponibilidade, a integridade, a confidencialidade, o não-repúdio e a autenticidade dos conhecimentos, informações e dados hospedados em ambiente tecnológico sob custódia do prestador de serviços.

6.52.1.5 Garantia de foro brasileiro;

6.52.1.6 Garantia de aplicabilidade da legislação brasileira;

6.52.1.7 Garantia de que o acesso aos dados, metadados, informações e conhecimentos utilizados e/ou armazenados na solução, ferramentas, softwares, infraestrutura ou em qualquer outro recurso que a empresa contratada utilize para a prestação de serviços somente serão acessados pela CONTRATANTE e serão protegidos de acessos de outros CONTRATANTEs e de colaboradores da empresa contratada;

6.52.1.8 Garantia que, em qualquer hipótese, a CONTRATANTE tem a tutela absoluta sobre os conhecimentos, informações e dados produzidos pelos serviços;

6.52.1.9 Vedado o uso não corporativo dos conhecimentos, informações e dados pelo prestador de serviço, bem como a replicação não autorizada.

6.52.1.10 A empresa contratada deve executar os serviços em conformidade com a legislação brasileira aplicável, em especial as certificações sobre segurança da

informação solicitadas para Qualificação Técnico-Operacional, sem prejuízo de outras exigências, objetivando mitigar riscos relativos à segurança da informação.

6.52.1.11 A empresa contratada deve disponibilizar canais de atendimento para o registro e abertura de chamados, com no mínimo um canal de atendimento via WEB e um canal telefônico, do tipo 0800 junto ao fabricante da solução.

6.52.2 DISPONIBILIDADE E ACORDO DE NÍVEIS DE SERVIÇO

6.52.2.1 A solução deve estar disponível em regime 24x7 (24 horas por dia, 7 dias por semana) com disponibilidade mínima de 99.8%.

6.52.2.2 Quando houver a custódia de conhecimentos, informações e dados pelo prestador de serviços, a empresa contratada deverá cumprir as seguintes diretivas:

6.52.2.3 A solução deve fazer uso de criptografia nas camadas e protocolos de redes de ativos computacionais para os dados em trânsito e/ou armazenados;

6.52.2.4 O prestador de serviços deve disponibilizar mecanismos para auditoria, como log de atividades dos usuários, ferramenta integrada a estes logs e painéis para os gestores. A ferramenta deve permitir diversos tipos de consulta aos logs, gerando relatórios customizados. Deve ser possível, ainda, a triagem de eventos relacionados à segurança que garantam um gerenciamento de incidentes completo e ágil;

6.52.2.5 Possuir procedimentos para triagem de eventos e incidentes de segurança da informação e garantir um tratamento de incidentes de segurança de forma completa e ágil;

6.52.2.6 Eventos e incidentes de segurança de informação devem ser comunicados através de canais predefinidos de comunicação, disponibilizados pela empresa contratada, de maneira rápida e eficiente e de acordo com os requisitos legais, regulatórios e contratuais;

6.52.2.7 Logs de auditoria do provedor que registram atividades de acesso de usuários privilegiados, tentativas de acesso autorizados e não autorizados, exceções do sistema e eventos de segurança da informação devem ser mantidos em conformidade com as políticas e regulamentos aplicáveis e serem comunicados para a CONTRATANTE;

6.52.2.8 O acesso e uso de ferramentas de auditoria que interajam com os sistemas de informação da CONTRATANTE deverão estar devidamente segmentados e restritos para evitar comprometimentos e uso indevido de dados de log;

6.52.2.9 Disponibilizar meios de replicação de logs de auditoria para que a CONTRATANTE possa armazenar cópias de segurança destas informações para futuras consultas e auditorias.

6.52.3 SEGURANÇA

6.52.3.1 Deverão ser observados os regulamentos, normas e instruções de segurança da

informação e comunicações adotadas pela CONTRATANTE, incluindo as Políticas e Diretrizes de Governo, normativos associados ou específicos de Tecnologia da Informação, Política de Segurança da Informação e Comunicações – POSIC e Normas Complementares – NC do Gabinete de Segurança Institucional – GSI da Presidência da República – PR.

6.52.3.2 Prover a criptografia de arquivos em repouso utilizando chave simétrica usando, no mínimo, algoritmo AES com 128 bits ou 3DES com 168 bits;

6.52.3.3 Possuir nas instâncias da plataforma proteção antivírus para proteger contra upload ou download de conteúdo malicioso. Os anexos de arquivos devem ser verificados por servidores dedicados em cada data center regional para proteção.

6.52.3.4 Manter uma política de backup dos dados, de pelo menos 20 (vinte) dias, dos metadados, dados, informações e conhecimento, produzidos ou custodiados pela CONTRATANTE e hospedados em ambiente de nuvem da empresa contratada, a fim de garantir tempo de replicação pela CONTRATANTE.

6.52.3.5 Estar em conformidade com a ISO/IEC 27001- padrão para sistema de gestão da segurança da informação (ISMS – Information Security Management System). Esta norma foi elaborada para prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI). Uma solução em nuvem tem que adotar um SGSI e ser certificado nessa norma. A especificação e implementação do SGSI de uma organização são influenciadas pelas suas necessidades e objetivos, exigências de segurança, os processos empregados e o tamanho e estrutura da organização.

6.52.3.6 Estar em conformidade com a ISO/IEC 27017:2015 que fornece orientações quanto aos aspectos de segurança de informações de computação em nuvem, recomendando a implementação de controles de segurança de informações específicas da nuvem que complementam a orientação das normas ISO/IEC 27001. Esse código de práticas disponibiliza instruções de implementação de controles adicionais de segurança da informação específicos para provedores de serviços de nuvem.

6.52.3.7 Estar em conformidade com a ISO/IEC 27018:2014 que é um código de práticas concentrado na proteção de dados pessoais na nuvem. Ela é baseada no padrão de segurança da informação e fornece orientação sobre a implementação dos controles aplicáveis às Informações de Identificação Pessoal (PII) de nuvens públicas. Esta Norma estabelece objetivos de controle, controles e diretrizes comumente aceitos para implementação de medidas para proteger as Informações de Identificação Pessoal (PII) de acordo com os princípios de privacidade.

6.52.3.8 Estar em conformidade com a SSAE 18 (SOC 1 – TYPE 2 E SOC 2 – TYPE2) - Statement on Standards for Attestation Engagements - A SSAE18 norma padrão de auditoria que obriga as empresas prestadoras de serviços possuírem mais controle e propriedade sobre a identificação e classificação de riscos, e gerenciamento adequado de suas subcontratadas. A grande vantagem dessa norma é o controle e a confiança nos negócios firmados. SOC 1 – TYPE 2 – Relatório que trata de controles internos

relevantes para uma auditoria das demonstrações financeira de uma subcontratada, por um período e o SOC 2 – TYPE 2, relatório que detalha os controles de uma organização de serviços que são relevantes para suas operações e conformidade, conforme descrito pelos Critérios de serviços de confiança (Segurança, disponibilidade, Integridade no processamento, confidencialidade e privacidade) TSC da AICPA.

6.52.3.9 Possuir e disponibilizar em ambiente de nuvem no mínimo um ambiente não-produtivo, por exemplo, ambientes de Desenvolvimento - DEV, Quality Assurance – QA e um ambiente Produção – PROD e, possuir funcionalidades de desenvolvimento em ambiente de Dev e publicação em outros ambientes, com controle de versionamento e publicação;

6.52.3.10 Permitir a criação de campos compartilhados nos formulários da aplicação e que possam ser utilizados em quaisquer outras entidades, sem a necessidade de programação ou alteração do código-fonte;

6.52.3.11 Consolidar vários recursos de automação em um único ambiente para que os proprietários e desenvolvedores de processos possam construir e visualizar processos de negócios a partir de uma única interface;

6.52.3.12 Incluir fluxos e ações acionadas por eventos, como por exemplo itens do catálogo de serviço;

6.52.3.13 Consolidar as informações de configuração e tempo de execução em uma única interface para que os proprietários e desenvolvedores de processos possam criar, operar e solucionar problemas de fluxos a partir desta interface;

6.52.3.14 Permitir que sejam criados processos automatizados em um único ambiente utilizando linguagem natural para automatizar ações, tarefas, notificações e operações de registro sem codificação;

6.52.3.15 Fornecer descrições em linguagem natural da lógica de fluxo para ajudar usuários não técnicos a entender gatilhos, ações, entradas e saídas;

6.52.3.16 Promover a automação de processos, permitindo que especialistas no assunto desenvolvam e compartilhem ações reutilizáveis com designers de fluxo;

6.52.3.17 Fornecer uma biblioteca de ações reutilizáveis, reduzindo os custos de desenvolvimento de novos fluxos para o CONTRATANTE.

6.52.4 PORTAL WEB

6.52.4.1 Disponibilizar um portal web de serviços onde os usuários finais possam encontrar soluções para seus problemas e registrar solicitações de serviço através de um catálogo de serviços, conforme permissões pré-estabelecidas;

6.52.4.2 Fornecer um portal de autoatendimento ao CONTRATANTE, no qual um CONTRATANTE pode acessar artigos da base de conhecimento e perguntas

frequentes, enviar e atualizar solicitações e monitorar o status de suas solicitações;

6.52.4.3 Fornecer funcionalidade para pesquisa de soluções na base de conhecimento por meio de palavras-chave, operadores booleanos e pesquisa de texto completo;

6.52.4.4 Associar usuários finais a grupos específicos, linhas de negócios etc., e adaptar o conteúdo apresentado, informações e opções de autoatendimento de acordo com assinaturas baseadas em regras para funções ou grupos;

6.52.4.5 Deve possuir recurso de Portal de Serviços WEB, parametrizável em recursos gráficos da solução que permita acesso a todas as funcionalidades e recursos de gerenciamento e utilização disponíveis para o usuário final;

6.52.4.6 O portal de serviços deve ser personalizável para atender as necessidades da CONTRATANTE permitindo que áreas de inserção de conteúdos sejam criadas e organizadas de acordo com a necessidade da CONTRATANTE;

6.52.4.7 A partir da página inicial do portal de serviços deve ser possível a pesquisa de itens de catálogo de serviço, artigos de conhecimento e artigos de autos serviço;

6.52.4.8 Deve disponibilizar recursos que possibilitem a criação de múltiplas visibilidades do portal de autoatendimento, para segmentar diferentes perfis de usuário ou diferentes serviços, de diferentes departamentos;

6.52.4.9 O portal de serviços deve permitir aos usuários dos serviços a visualização completa da situação atual dos serviços, indicando se existem degradações, indisponibilidades, problemas e manutenções programadas nos serviços;

6.52.4.10 A solução deve prover, automaticamente, que os itens cadastrados no catálogo de serviço web estejam também disponíveis no mesmo Catálogo de Serviços acessado por meio de aplicativo móvel; e

6.52.4.11 Deve fornecer ao atendente informações sobre os registros pendentes para determinado usuário (ex. requisição de serviço, resolução de incidente, problema, liberação e mudança, etc) facilitando as ações de atendimento.

6.52.4.12 Permitir o detalhamento de diversas informações, tais como: serviço solicitado, solicitante, data de criação e de modificação, prioridades, descrição, status e notas nas solicitações.

6.52.4.13 Permitir que os atendentes e analistas da contratante ou de empresas terceirizadas registrem as ações tomadas durante o atendimento dos Incidentes, Problemas, Requisições de Serviço, Requisições de Mudança e Tarefas, mantendo um histórico completo das ações tomadas, a data e o profissional que realizou a ação.

6.52.4.14 Permitir que os atendentes e analistas da contratante ou de empresas terceirizadas possam registrar o tempo gasto e os custos associados com cada ação tomada durante o atendimento dos Incidentes, Problemas, Requisições de Serviço, Requisições de Mudança.

6.52.4.15 Permitir a atribuição automática de requisições para profissionais ou equipes de atendimento em específico, com o uso de regras e parâmetros definidos pelo administrador. Estas regras e parâmetros poderão se utilizar, no mínimo, das seguintes informações: especialidade da equipe de serviço; item de configuração afetado; criticidade ou impacto do incidente; e carga de trabalho, agenda e habilidades de cada profissional.

6.52.4.16 Deve possuir recursos para a condução de enquetes ou pesquisas de satisfação.

6.52.4.17 Permitir que CONTRATANTEs e usuários finais respondessem a pesquisas de satisfação - associadas ou não a uma solicitação específica - que auxiliem a área de tecnologia da contratante a conhecer a percepção de seus CONTRATANTEs e permitam melhorar continuamente seus serviços.

6.52.4.18 Permitir pesquisas elaboradas conforme a metodologia NPS (Net Promoter Score), questionários elaborados conforme escalas de Likert, entre outros métodos de avaliação de satisfação consagrados no mercado.

6.52.4.19 Permitir a realização das perguntas das enquetes ou pesquisas no formato sim/não ou verdadeiro/falso por meio de "check box", de forma que os pesquisados respondam, no formato lista de alternativas por meio de "option button", todas as respostas que se aplicam, garantindo assim uma única resposta válida.

6.52.4.20 Deve armazenar em banco de dados as respostas dos usuários às enquetes ou pesquisas a fim de que seja possível a confecção de relatórios estatísticos.

6.52.4.21 Permitir que as enquetes ou pesquisas também sejam enviadas de forma periódica, bem como, também permitir que sejam enviadas toda vez que ocorra uma atividade associada.

6.52.4.22 Deve possuir recurso que garanta uma única resposta por usuário de determinada pesquisa ou enquete, prevenindo que usuários enviem repetidamente a mesma resposta.

6.52.4.23 Deve possibilitar o envio de enquetes ou pesquisas para um determinado grupo de usuários, para que respondam quando puderem, dentro de um determinado período de tempo.

6.52.4.24 Deve oferecer funcionalidade que facilite a disseminação de informação para a comunidade de usuários através do uso de recursos, tais como: envio automático de mensagens de correio eletrônico e quadro de avisos.

6.52.4.25 Permitir a busca nos registros de chamados (requisições de serviço, incidentes, problemas e requisições de mudança) com critérios de data, tipo de atividade, descrição e nome da pessoa que abriu o chamado.

6.52.4.26 Deve possuir um mecanismo automático para as escaladas funcionais e hierárquicas, ou seja, deve ser capaz de direcionar um atendimento para outra equipe e enviar alertas para os gerentes da organização em seus diversos níveis hierárquicos,

com base na categoria, na prioridade e no tempo transcorrido do atendimento.

6.52.4.27 Permitir o envio de alertas por e-mail, SMS, Microsoft Teams e WhatsApp.

6.52.4.28 Permitir ao administrador configurar as regras de notificação e escalação.

6.52.4.29 Permitir rastreabilidade completa do fluxo do chamado que está sendo tratado por diversas equipes de serviço.

6.52.4.30 Deve ter incorporada ferramentas de comunicação e colaboração dos atendedores com os usuários e CONTRATANTEs, tais como, bate-papo (chat), as quais deverão estar disponíveis em todas as plataformas de execução da aplicação.

6.52.4.31 O sistema deve permitir um recurso de rastreamento de solicitação visual (por exemplo, breadcrumbs, linha do tempo, Chevron process flow, etc.).

6.52.4.32 Deve ser possível aos atendentes transferir solicitações para outras equipes / times de serviço.

6.52.4.33 O aplicativo móvel deve ser disponível, de forma gratuita, para as plataformas iOS e Android.

6.52.5 PAINÉIS, GRÁFICOS, RELATÓRIOS E DASHBOARDS

6.52.5.1 Deve oferecer formulários, painéis e relatórios inerentes aos processos de gerenciamento de serviços disponíveis na solução que sejam usuais de mercado (conforme biblioteca ITIL v3 e outras referências) e Out-of-the-Box (OOTB), ou seja, prontos para uso imediatamente a instalação sem qualquer configuração, customização ou modificação especial.

6.52.5.2 Permitir a criação de painéis e dashboards com gráficos de gestão, de forma ágil e intuitiva, sem a necessidade de programação e alteração do código fonte;

6.52.5.3 Permitir a criação de painéis e dashboards com gráficos do tipo pizza, linha, colunas, barras, mapa de calor e tabelas dinâmicas, sem a necessidade de programação e alteração do código-fonte;

6.52.5.4 Permitir alterações de atributos de forma dinâmica em gráficos de gestão, contidos em painéis e dashboards da solução, possibilitando a alteração de eixos, título do gráfico, legenda, escala, rótulos de dados, tamanho do gráfico, de forma gráfica na solução e sem a necessidade de alterações do código fonte;

6.52.5.5 Permitir aos atendentes e solucionadores de chamados criarem seus próprios painéis e gráficos dentro da solução e compartilharem com grupos de usuários ou usuários específicos da solução, permitindo gerenciar as permissões de compartilhamento de acordo com os perfis de usuários da solução;

6.52.5.6 Suportar a definição de indicadores de desempenho (KPIs);

6.52.5.7 Prover visão da central de serviços em tempo real;

6.52.5.8 Permitir exportar ou agendar a exportação dos dashboards em formato PDF;

6.52.5.9 Permitir o detalhamento de informações contidas em gráficos de dashboards em gráficos detalhados;

6.52.5.10 Permitir ao usuário organizar os gráficos e informações, em seus painéis e dashboards de gestão, ajustando o layout e conteúdo do painel de acordo com suas necessidades;

6.52.5.11 Permitir aos usuários a configuração de painéis e dashboards agrupados por assunto e independentes entre si;

6.52.5.12 Permitir o gerenciamento de permissões por usuários e grupos para acesso aos painéis e dashboards da solução;

6.52.5.13 Permitir ao usuário organizar seus painéis e dashboards com listas de registros de seu interesse, possibilitando a escolha de colunas, realização de filtros e ordenação da lista;

6.52.5.14 Permitir configurar o envio automático e agendado de relatórios e gráficos gerenciais para grupos de usuários ou usuários específicos.

6.52.5.15 Permitir a cópia e a personalização dos objetos mencionados no item anterior de forma não programática ("codeless" ou "lowcode").

6.52.5.16 Deve prover um mecanismo de desenvolvimento de formulários, painéis e relatórios básicos ou avançados, de forma gráfica, por meio de recursos de arrastar e soltar (drag and drop), para a inclusão dos campos escolhidos e separadores. Esta funcionalidade deverá ser do tipo WYSIWYG (What You See Is What You Get), ou seja, deverá permitir a visualização do resultado final durante o desenvolvimento do mesmo.

6.52.5.17 Permitir o desenvolvimento de painéis de controle (dashboards) capazes de apresentar relatórios e gráficos operacionais e gerenciais em tempo real, e de acordo com o papel do usuário.

6.52.5.18 Devem os painéis de controle ter capacidade de navegação (drill down) até o nível do registro de atendimento.

6.52.5.19 Deve prover recursos para explorar tendências, padrões, anomalias e correlações em dados, permitindo, ao usuário, realizar análises complexas (slice and disse), reorganizar dinamicamente (pivot), filtrar, fazer análises detalhadas (drill-down) e representar graficamente os dados, em tempo real.

6.52.5.20 Devem prover recursos que permitam o cálculo e exibição do tempo de resolução

de diferentes alvos SLA - tempo de resposta e tempo de solução - e exibição de informações resumidas sobre a quebra do SLA em incidentes, problemas, mudanças e serviços.

6.52.5.21 Permitir a geração de relatórios com base em qualquer combinação dos atributos (campos) contidos no âmbito da infraestrutura de dados.

6.52.5.22 Permitir a produção de relatórios customizados avançados, integradamente a outros processos ITSM.

6.52.5.23 Permitir a geração de relatórios, no mínimo, nos seguintes formatos: Adobe Reader® (PDF), Comma-separated values (CSV), Microsoft Office e HTML.

6.52.5.24 Permitir a integração com, no mínimo, as seguintes fontes de dados: XML, CSV, Web Services SOAP, Web Services Rest e Bancos de Dados relacionais através de ODBC e JDBC.

6.52.5.25 Deve ser possível criar relatórios gerenciais específicos para uma ou mais unidades de negócios ou grupos de usuários.

6.52.5.26 Permitir a distribuição automatizada de relatórios diretamente por e-mail para destinatários únicos ou listas de distribuição.

6.52.5.27 Deve prover a emissão de relatórios comparativos entre os níveis de serviço acordados e os níveis de serviço efetivamente realizados.

6.52.5.28 Deve prover a emissão de gráficos gerenciais consolidados por período, contendo os KPIs.

6.52.5.29 Deve prover recursos para o Gerenciamento dos SLAs, contemplando um Dashboard para aferição dos objetivos de níveis de serviço.

6.52.5.30 Permitir a geração, no mínimo, de relatórios tais como os listados a seguir: Relatório de serviços registrados no Catálogo de Serviços, com indicadores de número de serviços em transição, em produção e total.

6.52.6 CATÁLOGO DE SERVIÇOS

6.52.6.1 O catálogo de serviços deve ser acessível via web, mostrar os serviços conforme a permissão de acesso dos usuários;

6.52.6.2 Permitir a personalização da apresentação do catálogo nos canais de Autoatendimento.

6.52.6.3 Permitir a criação de múltiplos catálogos de serviços.

6.52.6.4 Deve possuir uma interface gráfica para o desenho da estrutura do Catálogo de Serviços em níveis e subníveis, sem a necessidade de usar qualquer tipo de linguagem de programação ("codeless" ou "lowcode"), de forma que não seja necessária a

intervenção de um programador para manter o Catálogo de Serviços atualizado.

6.52.6.5 Permitir a organização do Catálogo de Serviços em uma visão de CONTRATANTEs, usuários ou tipos ou categorias de usuários dos serviços de TI. Os itens do catálogo de serviços deverão ser distintos das categorias de serviços de TI, contudo, deverá ser garantido o relacionamento entre eles.

6.52.6.6 Permitir o cadastro e manutenção de Serviços de Negócio e Serviços de TI.

6.52.6.7 Permitir relacionar cada Serviço de TI aos itens de configuração que o compõem, às suas janelas de manutenção e seus períodos de congelamento.

6.52.6.8 Permitir a definição de quais Grupos de Usuários podem acessar cada serviço e item do catálogo, de forma que seja possível manter um único Catálogo de Serviços, sem duplicação de informações.

6.52.6.9 Permitir a definição de quais Grupos de Usuários podem acessar cada serviço e item do catálogo, de forma que seja possível manter um único Catálogo de Serviços, sem duplicação de informações.

6.52.6.10 Permitir o registro da descrição detalhada do item e da categoria de serviço, bem como, associar esses registros à artigos da base de conhecimento.

6.52.6.11 Deve exibir os itens de configuração componentes técnicos utilizados para entregar cada serviço em específico.

6.52.6.12 Permitir a vinculação de cada oferta de serviço com a respectiva instância de processo, seja o processo de incidentes, requisições de serviços ou qualquer outro.

6.52.6.13 Permitir a visualização do catálogo nos canais de autoatendimento e console de servicedesk para os usuários de acordo com as políticas de acesso pré-estabelecidas.

6.52.6.14 Permitir o cadastro de documentação detalhada aos usuários associada a cada oferta de serviço.

6.52.6.15 Deve oferecer suporte ao gerenciamento do ciclo de vida do catálogo de serviços, incluindo as seguintes funcionalidades:

6.52.6.16 Criar, modificar e excluir categorias / modelos de serviços.

6.52.6.17 Criar, modificar e excluir serviços.

6.52.6.18 Criar, modificar e excluir componentes de serviço.

6.52.6.19 Rastrear o status de implementação dos serviços.

6.52.6.20 Definir métricas, KPIs e SLAs / OLAs para modelos de serviço, serviços e componentes de serviço.

6.52.6.21 Permitir a definição do catálogo de serviços e o cadastro e manutenção de

descrição de serviços, assim como de seus atributos;

6.52.6.22 Permitir a customização da estrutura do catálogo de serviços, devendo esta parametrização ser realizada através da própria interface da ferramenta pelos administradores da ferramenta;

6.52.6.23 Permitir que, para cada serviço e/ou item de configuração, seja possível informar o seu grau de prioridade (importância) para o negócio de forma a estabelecer a priorização no atendimento;

6.52.6.24 Permitir a criação e configuração de catálogos de serviços negociais e catálogos de serviços técnicos;

6.52.6.25 Permitir a criação de ilimitadas categorias de navegação nos catálogos de serviços, permi ndo a organização do catálogo em quantos níveis forem necessários;

6.52.6.26 O Catálogo de Serviços deve permitir o agrupamento de serviços conforme a necessidade da Contratante, a qual definirá seus próprios grupos e ofertas;

6.52.6.27 Permitir a criação de múltiplos catálogos de serviços ou perfis de visibilidade para oferta de serviços dos departamentos do CONTRATANTE como uma central de serviços compartilhados;

6.52.6.28 Todos os catálogos, níveis e agrupamentos criados para a interface web deve estar, da mesma maneira, disponíveis e agrupados no aplicativo móvel disponibilizado;

6.52.6.29 A solução deve implementar e seguir corretamente o fluxo de Gerenciamento de Catálogo de Serviços;

6.52.6.30 Para a automação dos serviços, o Gerenciamento do Catálogo de Serviços deve permitir associar à oferta de serviço os formulários personalizados para entrada de dados pelo usuário final e fluxos de trabalho automatizados e estruturados para o cumprimento das requisições;

6.52.6.31 Deve ser possível criar serviços técnicos e serviços de negócio de forma gráfica e sem a necessidade de programação ou alterações do código-fonte;

6.52.6.32 Deve ser possível associar Service Level Agreement – SLA aos serviços;

6.52.6.33 Deve ser permitido copiar as ofertas de serviço para rapidamente publicar novas ofertas semelhantes, herdando as informações de configuração, parâmetros, SLA, custos, demanda e visibilidade; e

6.52.6.34 Deve ser possível carregar valores automáticos com base em respostas anteriores do formulário de serviços e com isso o item de catálogo pode seguir fluxos de trabalho específicos.

6.52.7 GERENCIAMENTO DE NÍVEL DE SERVIÇO

6.52.7.1 Permitir a definição de parâmetros que são utilizados para definir o Service Level Agreement - SLA, tais como: por CONTRATANTE, por serviço, dentro de um calendário a que se aplica o SLA, meta de nível de serviço relacionados ao SLA, escalações automatizadas relacionadas ao SLA;

6.52.7.2 Permitir a definição de critérios que possibilitem a associação de SLA a registros de atendimentos, incidentes, problemas, solicitações de mudanças e fluxos de trabalho do CONTRATANTE, automatizados na solução;

6.52.7.3 Permitir a definição de alertas com regras que viabilizem a emissão de avisos de registros incidentes, problemas, mudanças, solicitações de serviço, tarefas e atividades de fluxos de trabalho que estejam próximos de limites de SLA estabelecidos;

6.52.7.4 Manter um histórico dos níveis mínimos de serviço para acompanhamento de desempenho dos serviços;

6.52.7.5 Permitir a definição do tempo de duração para os níveis mínimos de serviço ou percentual de disponibilidade de um item de configuração;

6.52.7.6 Indicar quando o nível de serviço não foi cumprido ou está próximo do não cumprimento;

6.52.7.7 Permitir definição de múltiplos SLA;

6.52.7.8 Permitir a criação de modelos de SLA para reutilização e facilidade de configuração de novos serviços;

6.52.7.9 Possuir um repositório único com todos os registros de SLA, consolidando os Acordos de Nível de Serviço e Acordos de Nível Operacional;

6.52.7.10 Permitir o acesso seguro e controlado às informações do processo de gerenciamento de níveis de serviço e de SLA;

6.52.7.11 Permitir gerenciar o ciclo de vida de SLA;

6.52.7.12 Permitir anexar SLA a qualquer processo ou fluxo de trabalho do CONTRATANTE, automatizado na plataforma;

6.52.7.13 Permitir monitorar automaticamente os tempos de resposta, resolução e escalação relacionados com SLA;

6.52.7.14 Permitir a configuração de contabilização de SLA apenas em horários definidos pelo CONTRATANTE, a exemplo da necessidade de contabilização de

6.52.7.15 SLA apenas em horas úteis;

6.52.7.16 A solução deve garantir o monitoramento dos prazos não apenas do SLA, firmado

entre TI e usuários finais, mas também entre equipes (OLA) e prestadores de serviço externos (UC);

6.52.7.17 A medição de prazos deve ser insumo para a composição de indicadores gráficos de performance, exibidos em painéis do tipo dashboards;

6.52.7.18 A solução deve permitir que eventos sejam disparados através da integração com ferramentas de monitoramento e gerenciamento de eventos e a contagem de seus prazos iniciados, para acompanhamento do atingimento dos limites definidos;

6.52.7.19 A solução deve permitir emitir relatórios das métricas de SLA;

6.52.7.20 A solução deve permitir a automação da escalação e notificação, baseado nos tempos de resposta e resolução;

6.52.7.21 A solução deve garantir a integração nativa entre o Gerenciamento de Níveis de Serviço com o Gerenciamento de Incidentes, Problemas e Mudanças, garantindo que a execução de ações siga tempos pré-definidos; e

6.52.7.22 Permitir alertar ao me e à gestão, caso um evento exceda um número específico de atribuições e escalações.

6.52.7.23 Permitir a criação de SLAs, OLAs e KPIs definidos pelo administrador de uma forma não programática ("codeless" ou "lowcode").

6.52.7.24 Permitir a definição, gerenciamento, revisão, monitoramento e divulgação dos Acordos de Nível de Serviço (SLAs), Acordos de Níveis Operacionais (OLAs) e Contratos de Apoio (UCs).

6.52.7.25 Deve prover calendário com datas, feriados e horários de trabalho, parametrizáveis por Acordo em seus diversos escopos (SLA, OLA, UC), permitindo a aferição dos níveis de serviço oferecidos pelas áreas ou equipes de atendimento da Sefa-PR.

6.52.7.26 Permitir a definição de níveis de serviço para os processos de Gerenciamento de Incidentes, Gerenciamento de Problemas, Gerenciamento de Mudanças e Cumprimento de Requisições de Serviços.

6.52.7.27 Permitir a definição e ser capaz de medir e monitorar prazos de resposta e prazos de resolução tanto para o atendimento como um todo ("nível de serviço") quanto para as atividades que compõem o atendimento ("nível operacional") de forma que seja possível avaliar o desempenho de cada equipe envolvida no atendimento, em comparação com o seu nível de serviço acordado.

6.52.7.28 Permitir, no mínimo, a definição dos níveis de serviço para:

6.52.7.28.1 Tempo de início do atendimento.

6.52.7.28.2 Tempo de solução do atendimento.

6.52.7.28.3 Tempo de resposta do chamado.

6.52.7.28.4 Disponibilidade do serviço.

6.52.7.29 Permitir a diferenciação dos níveis de serviço estabelecidos para um chamado, associando automaticamente o acordo apropriado, de acordo com o usuário, item de configuração, setor (ex.: seção, departamento ou divisão.) ou serviço. Se nenhum destes tiver um SLA associado, o SLA padrão deve ser utilizado.

6.52.7.30 Permitir a definição de paradas programadas e janelas de manutenção para os serviços de TIC, de modo que interrupções durante esses intervalos não influenciem o cálculo dos níveis de serviço correspondentes.

6.52.7.31 Deve auxiliar na monitoração de OLAs, UCs, do mesmo modo que trata um SLA.

6.52.7.32 Permitir a programação de revisão SLAs, OLAs e UCs.

6.52.7.33 Permitir a configuração e a emissão de alertas automáticos, por exemplo, via correio eletrônico ou SMS, quando um nível de serviço estiver próximo de seu limite acordado.

6.52.7.34 Permitir a integração do processo de Gerenciamento de Níveis de Serviço com os processos de Gerenciamento de Incidentes, Gerenciamento de Problemas e Cumprimento de Requisições de Serviço.

6.52.7.35 Deve prover, ao processo de Gerenciamento de Mudanças, o acesso a informações de SLAs, para tratar requerimentos de disponibilidade, janelas para implementações, detalhes acordados e assuntos correlatos.

6.52.7.36 Deve prover mecanismos de relacionamento entre SLAs, OLAs e UCs.

6.52.7.37 Permitir a associação de incidentes a serviços e SLAs, possibilitando a visualização dos incidentes que impactaram serviços e SLAs.

6.52.7.38 Permitir a associação de problemas a serviços e SLAs, possibilitando a visualização dos problemas que impactaram cada serviço.

6.52.7.39 Permitir a associação de mudanças a serviços e SLAs, possibilitando a visualização das mudanças que impactaram cada serviço.

6.52.7.40 Permitir a associação de SLAs a serviços.

6.52.7.41 Permitir a definição de penalidades nos seguintes acordos: SLA, OLA e UC.

6.52.7.42 Deve implementar aferição e monitoração de níveis de serviço para cada IC.

6.52.7.43 Deve prover a correlação entre os parâmetros dos SLAs com os UCs.

6.52.7.44 Permitir o desenvolvimento e monitoração de UCs com fornecedores externos, da mesma forma como são desenvolvidos e monitorados os OLAs.

6.52.7.45 Deve possibilitar a monitoração automática dos limites de níveis de serviço, entregues com base nos SLAs.

6.52.7.46 Permitir o cadastramento de detalhes do fornecedor, incluindo dados do contato: nome, e-mail, telefone, data de assinatura, datas de efetivação, renegociação e encerramento do contrato, objeto do contrato, periodicidade (mensal, trimestral, anual), etc.

6.52.7.47 Permitir o rastreamento e alteração de detalhes de manutenção por fornecedor e por ICs.

6.52.8 BASE DE CONHECIMENTO

6.52.8.1 Possuir uma base de dados para armazenamento de artigos de conhecimento da organização;

6.52.8.2 Permitir configurar e gerenciar o ciclo de vida de registros de artigos de conhecimento;

6.52.8.3 Possuir recurso para busca indexada, apresentando soluções para os atendentes;

6.52.8.4 Permitir classificar e atribuir categorias para os artigos de conhecimento;

6.52.8.5 Permitir a pesquisa de artigos de conhecimento nas telas de atendimento de registros dos processos de gerenciamento de incidente, mudança, problema, requisições;

6.52.8.6 Possuir campos de pesquisa de conhecimento, integrados com a base de conhecimento da solução, nas interfaces de solicitação e operação de aplicações, processos e fluxos de trabalho do CONTRATANTE;

6.52.8.7 Permitir gerenciar documentos de conhecimento estabelecendo prazos de validade e de revisão;

6.52.8.8 Permitir o gerenciamento de acesso de usuários aos artigos de conhecimento;

6.52.8.9 Permitir inserir ou anexar imagens, vídeos e textos artigos de conhecimento;

6.52.8.10 Permitir pesquisar através de palavras-chave ou frases inteiras;

6.52.8.11 Permitir controlar o processo de aprovação de um documento, antes do mesmo ser publicado na base de conhecimento;

6.52.8.12 Permitir o ranking de uso das informações de conhecimento e identificar as necessidades não atendidas por conhecimento, de forma que o próprio usuário final possa classificar a utilidade (ou não) do artigo de conhecimento;

6.52.8.13 Deve permitir o cadastro, alteração, revisão, desativação, publicação de procedimentos para a base de conhecimento (perguntas frequentes, erros

conhecidos, soluções de contorno, entre outros.) e o público para o qual deve ser disponibilizado (equipes de TI, usuários finais, etc.), de forma que incidentes e problemas já diagnosticados ou resolvidos possam ser registrados e pesquisados para facilitar e aumentar a velocidade de solução de futuras ocorrências.

6.52.8.14 Deve integrar nativamente o processo de Gerenciamento de Conhecimento aos processos de Gerenciamento de Incidentes, Gerenciamento de Problemas e Gerenciamento de Configurações.

6.52.8.15 Permitir o recebimento de propostas de ativos de conhecimento, sua posterior análise e sua aceitação ou rejeição. Esse recebimento de propostas deve ter origem no Gerenciamento de Incidentes, no Gerenciamento de Problemas, no Gerenciamento de Configuração ou em uma solicitação direta de um usuário.

6.52.8.16 Deve permitir revisões para cada ativo de conhecimento.

6.52.8.17 Deve implementar recursos comuns de gerenciamento de documentos, incluindo: captura, classificação, marcação e indexação, pesquisa e recuperação, controle de versão, segurança e gerenciamento de acesso.

6.52.8.18 Deve permitir a estruturação do conteúdo da KB (Knowledge Base) na forma "Wiki", sem depender de codificação.

6.52.8.19 Deve fornecer uma plataforma de gerenciamento de KB (Knowledge Base) exclusiva para todos os usuários de diferentes equipes e departamentos.

6.52.8.20 Deve controlar as permissões de acesso à plataforma KB (Knowledge Base) com base em papeis, equipe do usuário ou com base em grupos.

6.52.8.21 Deve obter automaticamente itens relevantes da base de conhecimento com base nas pesquisas dos usuários ou contextualmente, para resolução de incidentes de autoatendimento

6.52.8.22 Deve oferecer funcionalidade semelhante blogs para permitir a pesquisa, postagem e acompanhamento de tópicos de resolução de problemas.

6.52.8.23 Permitir uma variedade de mídias, incluindo arquivos de áudio e vídeo internos ou externos (por exemplo, vídeos do YouTube), links, arquivos, etc.

6.52.8.24 Deve fornecer recursos de colaboração social, incluindo: perfis e funções dos usuários, postagens dos usuários, curtidas e comentários, bate-papos e mensagens (internos à solução).

6.52.8.25 Possuir uma interface fácil e iterativa para a consulta a base de conhecimento, tanto para o analista quanto para o usuário final;

6.52.8.26 Possuir a integração nativa do Gerenciamento do Conhecimento com os demais processos (nativos da solução ou implementados para atendimento de processos de trabalho), permitindo, por exemplo, mas não limitado a tal, a associação de

documentos e artigos de conhecimento a eventos, incidentes, problemas, mudanças e registros de fluxos de trabalho automatizados na solução;

6.52.8.27 Possuir recursos de pesquisa de soluções aos usuários enquanto registram as solicitações;

6.52.8.28 Rastrear, automaticamente, quantas vezes um artigo ou informação de conhecimento foi utilizado.

6.52.8.29 Deve possuir uma base de conhecimento onde serão registradas soluções para os problemas e erros conhecidos, possibilitando relacionar os problemas e suas respectivas soluções a mudanças e a incidentes específicos.

6.52.8.30 Permitir consulta rápida, por palavras-chave, das informações que se encontram na base de conhecimento e possibilitar a navegação na hierarquia de tópicos ou assuntos.

6.52.8.31 Deve possibilitar, aos usuários administrativos, ou outros usuários, com nível de autorização suficiente, o gerenciamento (inclusão, alteração, consulta e exclusão) das informações armazenadas na base de conhecimento.

6.52.9 REGISTRO DE COMUNICAÇÃO

6.52.9.1 Possuir funcionalidade de chat;

6.52.9.2 Permitir a interação em tempo real entre o atendente do chamado e o CONTRATANTE solicitando, mantendo o registro da solicitação atualizado e visível para ambas as partes;

6.52.9.3 Permitir a utilização dos seguintes meios para abertura e resolução de chamados:

6.52.9.4 telefone;

6.52.9.5 e-mail;

6.52.9.6 whatsapp;

6.52.9.7 chatbot;

6.52.9.8 ferramentas de gestão de infraestrutura (monitoração);

6.52.9.9 portal web;

6.52.9.10 Permitir que o atendente faça anotações nos registros de trabalho podendo escolher entre a mensagem estar visível para o CONTRATANTE solicitante ou somente para o time de atendimento.

6.52.9.11 Permitir que solicitantes abram requisições consultem bases de conhecimento utilizando agentes ativos (funcionários), agentes virtuais (chatbots) ou ambos usando

as interfaces de conversação

6.52.9.12 Permitir explorar, implementar e manter as interfaces de conversação com mais rapidez e facilidade com uma experiência guiada no Portal, Intranet e/ou pagina dos católogos disponibilizados na plataforma.

6.52.9.13 Todas as parametrizações, fluxos, treinamentos e configurações que seja preciso para configurar e iniciar as interfaces, como Agente Virtual e Chat de devem ser realizadas na mesma interface da plataforma.

6.52.9.14 A interface de criação das conversas do agente virtual deve permitir desenvolver, testar e implantar conversas automatizadas que auxiliam usuários com problemas comuns ou tarefas de autoatendimento;

6.52.9.15 Possuir nativamente o entendimento para linguagem natural (NLU - Natural Language Understand);

6.52.9.16 A interface de conversação do chatbot deve oferecer aos seus usuários várias opções para gerenciar a conversa;

6.52.9.17 Deverá permitir interação com o Assistente Virtual Inteligente utilizando "linguagem natural ou coloquial", em língua Portuguesa Brasileira, como se es vesse falando com um humano, tornando mais fácil e produtiva sua interação, devendo tratar neologismos, gírias e regionalismos, de forma a entender a real intenção dos usuários ao efetuarem uma pergunta ou busca por conteúdo;

6.52.9.18 Deverá oferecer um Modelo de Linguagem Natural parametrizável que contemple vocabulário, conceitos e termos específicos para emular (intent) a atividade humana de atendimento ao usuário e permita a customização de vocabulário específico;

6.52.9.19 A interface de criação deve ser uma ferramenta gráfica para construir os fluxos de diálogo das conversas (tópicos)., devendo cada fluxo ou tópico capaz de definir o diálogo trocado entre um agente virtual e um usuário para atingir um objetivo específico ou resolver um problema.

6.52.9.20 Permitir desviar os problemas mais comuns e fáceis de resolver do usuário para um bot de agente virtual disponível 24 horas por dia, 7 dias por semana.

6.52.9.21 Permitir configurar, gerenciar e monitorar os agentes virtuais e ao vivo na página inicial em uma interface integrada e graficamente intuitiva.

6.52.9.22 Permitir criar tópicos de Agente Virtual para desviar solicitações comuns de usuários.

6.52.9.23 Permitir chat assíncrono, ou seja, os agentes e usuários finais podem participar de conversas de longa duração sem estarem online simultaneamente, podendo o agente entrar em contato proativamente com os usuários sempre que houver informações úteis para compartilhar, como alertas ou atualizações importantes.

6.52.9.24 Para o chat assíncrono, a interface de conversação deve ser a mesma que no chat online, devendo essas conversas sejam executadas em canais de mensagens que permitem que seus usuários e agentes se comuniquem em momentos diferentes e retomem as conversas de onde pararam.

6.52.9.25 O chat assíncrono deve permitir indicadores de mensagens que informam os usuários sobre mensagens novas e não lidas recebidas quando estão fora da janela de bate-papo ou offline.

6.52.9.26 O chat assíncrono deve permitir mensagens do sistema, exibidas para usuários e agentes, que são personalizadas para canais de mensagens ou bate-papo.

6.52.9.27 Deve ser possível configurar para o chat assíncrono com um período de tempo limite de conversa ociosa, onde administradores possam ajustar o valor para canais de mensagens, conforme necessário.

6.52.9.28 Deve possuir recurso proativo de mensagens que permite que os agentes iniciem a comunicação com os usuários

6.52.9.29 O sistema deve possuir configuração como expressões regulares para cada tipo de dados confidenciais (por exemplo CPF, cartão de credito, OAB etc), onde manipulador de dados confidenciais detecta e mascara os dados confidenciais para que não sejam visualizados pelo agente ou solicitante.

6.52.9.30 Deve ser possível configurar o mascaramento de dados no chat do agente de modo que a manipulação de dados confidenciais funcione apenas para mensagens de entrada (do solicitante), mensagens de saída (do agente ativo) ou ambas.

6.52.9.31 O sistema deve validar os dados sensíveis e caso o solicitante envie uma mensagem contendo dados confidenciais para um agente, uma mensagem do sistema será enviada ao solicitante e ao agente notificando que a mensagem continha dados confidenciais. Os dados confidenciais devem ser mascarados na transcrição e marcados como confidenciais na transcrição interna.

6.52.9.32 Deverá ser possível a criação de fluxos de atendimento, por meio de programação de árvores de decisões e perguntas de esclarecimento e de direcionamento dos usuários;

6.52.9.33 Permitir que os usuários recebam alertas de áudio e visuais automaticamente quando recebem uma mensagem de um agente ao vivo ou bot virtual;

6.52.9.34 Permitir que usuários autenticados possam a var ou desativar alertas audíveis e de notificações de bate-papos por meio do botão de alternância no menu de bate-papo ou em configuração própria;

6.52.9.35 Possuir mecanismo que disponibilize para o desenvolvedor facilidade na criação de fluxos de conversação;

6.52.9.36 Permitir dentro da plataforma inserir em qualquer portal a função chat virtual

robotizado, com atendimento virtual por meio de chatbot;

6.52.9.37 Possuir mecanismos diversos para automação como: árvore de decisões gráficas, looping, conteúdos e serviços de localização;

6.52.9.38 A interface de conversação deve oferecer aos seus usuários várias opções para gerenciar a conversa, podendo os usuários interromperem a conversa atual e iniciar uma nova ou entrar em contato com o suporte para acessar um agente ao vivo e obter assistência imediata;

6.52.9.39 Quando os usuários são transferidos para um agente ativo, analista da CONTRATANTE, o cabeçalho da janela de bate-papo deve mudar para indicar que agora eles estão interagindo com um agente ativo;

6.52.9.40 Deve ser possível na janela de bate-papo efetuar o upload de uma imagem, texto ou arquivo PDF e enviá-lo ao agente; e Ser nativo da solução, sem a necessidade de integração com ferramentas de terceiros.

6.52.9.41 Possuir, na mesma interface/sistema, a possibilidade de construir fluxos de conversação de forma gráfica (inicio-> iterações-> fim) com o virtual agente (chatbot), utilizando recursos como: entradas do usuário, respostas de bot e utilitários (ler um registro da base, executar uma ação de script, decisão de fluxo etc) para definir o fluxo;

6.52.9.42 Possuir a capacidade sobre as construções dos fluxos de conversação para inserir utilitário de Decisão em um tópico do Agente Virtual para adicionar duas ou mais ramificações que representam caminhos diferentes em uma conversa. Por exemplo: um controle de escolha estático solicita que o usuário selecione entre três cores disponíveis e a seleção é armazenada em uma variável. O controle do utilitário de decisão é configurado com uma ramificação para cada seleção possível. Cada ramificação contém um script na propriedade/condição que identifica quando uma cor específica é selecionada.

6.52.9.43 O sistema deve validar caso um agente tente enviar uma mensagem contendo dados confidenciais a um solicitante, a mensagem não deverá ser enviada ao solicitante. Em vez disso, um erro deve ser exibido para o agente e a mensagem deve ser marcada como confidencial na transcrição interna.

6.52.9.44 Deve permitir configurar o agente virtual em interface do Portal de Serviços e em aplicativos disponibilizados nas plataformas Apple iOS e Google Android.

6.52.9.45 Deve permitir, de forma nativa, integrações com aplicativos de mensagens corporativas de terceiros, no mínimo: Slack , Microsoft Teams, Workplace do Facebook e facebook Messenger para usuário externo.

6.52.9.46 Permitir criar integrações de bate-papo personalizado de conversação com outros provedores de bate-papo, como Whatsapp por exemplo;

6.52.9.47 Deve possuir capacidade de criar conversas baseadas em palavras-chave que os usuários inserem ou aplicar modelos de compreensão de linguagem natural (NLU), que

permitam que o agente virtual entenda, processe e responda ao que os usuários estão dizendo durante uma conversa.

6.52.9.48 Permitir que quando os usuários iniciem uma conversa com o bot, eles possam inserir uma solicitação ou ver uma lista de tudo o que o bot pode ajudar. Caso eles optem por ver tudo, a janela de bate-papo exibirá todos os tópicos disponíveis para o usuário.

6.52.9.49 Deverá utilizar NLU para processar a linguagem humana com base no contexto e nos dados da organização.

6.52.9.50 Deverá o NLU possuir a capacidade de aprender a sintaxe, a semântica e o vocabulário de organização usando um construtor de modelo NLU e o serviço de inferência NLU para permitir que o sistema aprenda e responda à intenção do usuário.

6.52.9.51 Na parametrização de intenções (Intent) NLU deve permitir criar palavras-chave de backup caso uma intent não seja correspondida. Se houver várias correspondências, o agente virtual retornará no mínimo três intents por padrão. O administrador deve poder alterar o número de tópicos retornados usando a propriedade do sistema.

6.52.9.52 Permitir que o sistema identifique e gere automaticamente variável de contexto identificando se o usuário está em uma conversa web ou usando um dispositivo móvel, para fornecer experiências de conversação personalizadas e relevantes com base no dispositivo que está sendo usado

6.52.9.53 Permitir que administradores criem scripts para personalizar o comportamento dos tópicos do Agente Virtual e fornecer contexto para tópicos, como reter informações sobre um usuário ou a entrada de um usuário permitindo usar essas informações para personalizar uma conversa, como para apresentar uma saudação ou confirmação com script. Os scripts também podem especificar determinadas ações a serem executadas em informações obtidas durante uma conversa.

6.52.9.54 Caso o agente virtual não encontre nenhuma correspondência/intenção/intent correspondente no NLU, ele deve usar a pesquisa de IA (Inteligência Artificial) para gerar resultados de pesquisa que exibam links relevantes para artigos de conhecimento de perguntas e respostas, itens do catálogo de serviços ou registros de pessoa (usuário).

6.52.9.55 As pesquisas de IA devem ser controladas pelo tópico de configuração de pesquisa AI exclusivo e parametrizável,

6.52.9.56 Possuir solução de análise e relatório de agente virtual contendo painel de análise de conversação pré-configurado para ajudar a melhorar as interações do agente virtual.

6.52.9.57 Para compor os gráficos e painéis o Agente Virtual deverá manter registros das interações com os usuários. O painel deve conter informações sobre essas interações para que possa visualizar como o Virtual Agent entendeu e resolveu os problemas do

usuário, com métricas como: Qual porcentagem de usuários transfere do Agente Virtual para um agente ativo, Tópicos mais e menos usados, detalhes da conversa (interface web, mobile, id do usuários, inicio e fim da conversa, duração), mostrar o número de vezes que o modelo de previsão NLU entendeu com precisão a intenção da conversa do usuário ou selecionou um tópico automaticamente, exibir informações sobre o número de problemas do usuário interceptados pelo serviço de resolução automática e resolvidos pelo Agente Virtual

6.52.9.58 Possuir API de integração API Rest ou Soap para o chatbot/virtual agent.

6.52.10 NOTIFICAÇÕES

6.52.10.1 Poder inserir notificações automatizadas em qualquer momento de fluxo de trabalho e processos automatizados na solução;

6.52.10.2 Permitir configurar notificações automáticas de alertas, para reiteração de chamados técnicos abertos;

6.52.10.3 Enviar notificações com informações contendo dados de qualquer parte do registro de um fluxo de trabalho ou processo implementado na solução;

6.52.10.4 Enviar notificações baseadas em condições e eventos da solução incrementados ou alternados.

6.52.11 USABILIDADE

6.52.11.1 Possuir uma mesma interface (Ex.: estilos de menus, listas e telas de registros, gráficos, dashboards, relacionamento de registros, etc.) de navegação e uso em todos os fluxos de trabalho, processos e aplicações que sejam automatizadas dentro da solução;

6.52.11.2 Permitir inserir quantidade ilimitada de anexos em registros de trabalho, fluxos de trabalho e processos automatizados na solução;

6.52.11.3 Possuir interface de acesso totalmente WEB para todas as funcionalidades (administração e uso);

6.52.11.4 Possuir interface de acesso e todas suas telas de administração e uso em idioma português padrão Brasil;

6.52.11.5 Possuir interface amigável e intuitiva para os usuários e administradores;

6.52.11.6 Permitir acesso controlado à solução por meio de usuário e senha e com autenticação utilizando serviços de Diretórios LDAP e Microsoft Active Directory – AD;

6.52.11.7 Permitir a adequação de menus da interface de atendimento para cada operador, permitindo que o operador organize seus menus com os principais links que utiliza dentro da solução;

6.52.11.8 Permitir a criação de menus específicos paras as aplicações e automatizações de fluxos de trabalho e processo do CONTRATANTE, desenvolvidos na solução;

6.52.11.9 Permitir o desenvolvimento de formulários, sem a necessidade de programação e diagramação, para a inclusão, exclusão e alteração de campos escolhidos.

6.52.12 RELACIONAMENTO DE REGISTROS

6.52.12.1 Possuir interface de lista de registros de qualquer processo ou fluxo de trabalho da solução, seja nativo ou criado para o CONTRATANTE, totalmente customizável, permitindo adicionar, remover ou alterar a ordem das colunas no grid de visualização de registros;

6.52.12.2 Permitir filtros e consultas a partir de qualquer coluna listada no grid de registros;

6.52.12.3 Permitir que usuários refinem a pesquisa com consultas avançadas, podendo inserir vários critérios de consulta e filtros no grid de registros;

6.52.12.4 Permitir que consultas personalizadas possam ser gravadas e compartilhadas com outros usuários da solução;

6.52.12.5 Permitir aos usuários inserir e remover quantas colunas forem necessárias em sua lista e grids, desde que estas estejam na tabela de banco de dados ao qual estão sendo listados os registros;

6.52.12.6 Permitir a alteração da ordem de apresentação das colunas no grid de registros;

6.52.12.7 Permitir ordenar a lista de registros por qualquer das colunas do grid de visualização, de A a Z e de maior para menor, ou vice-versa;

6.52.12.8 Permitir atualizar manualmente as consultas exibidas nas listas e grids (refresh) sem fechar ou atualizar toda a janela atual do navegador;

6.52.12.9 Permitir que usuários salvem seus filtros / pesquisas;

6.52.12.10 Permitir que usuários compartilhem os filtros entre usuários e grupos;

6.52.12.11 Permitir que usuários realizem pesquisas e filtros avançados;

6.52.12.12 Permitir que os usuários exportem para arquivos formato Excel, CSV e XML;

6.52.12.13 Permitir que usuários importem dados para criação e alteração de registros com base em modelo no formato Excel, CSV e XML;

6.52.12.14 A personalização de listas e grids não devem depender de um usuário

administrador, sendo facultado a qualquer outro operador a criação de suas próprias listas e grids, não estando restrito às listas e grids originalmente disponíveis na aplicação ou disponibilizadas pelos administradores;

6.52.12.15 Permitir a alteração de registros, inclusive alterações em lote (vários registros), na própria tela de visualização de registros e grid da solução;

6.52.12.16 A solução deve possuir recurso que permita aos operadores fazer a listagem de todos os registros em sua fila ou fila de grupos de solução a que pertence, combinando registros de incidentes, requisições, mudanças e tarefas de processos e fluxos de trabalho;

6.52.12.17 Permitir a criação de novos registros ou exclusão de registros, a par r da lista de registros;

6.52.12.18 Prover recursos que possibilitem a parametrização de regras para aprovações de fluxos de trabalho, processos, requisições e outros registros da solução, com base nas regras de negócio do CONTRATANTE, sem a necessidade de alteração do código-fonte; e

6.52.12.19 Permitir o relacionamento de tabelas de bancos de dados criadas para automação de aplicações, processos e fluxos de trabalho do CONTRATANTE, com tabelas e bancos de dados nativos da solução, sem a necessidade de programação ou alterações do código-fonte.

6.52.13 FUNCIONALIDADES DE APROVAÇÕES EM FLUXOS DE TRABALHO

6.52.13.1 Prover recursos que possibilitem a parametrização de regras para aprovações de fluxos de trabalho, processos, requisições e outros registros da solução, com base nas regras de negócio do CONTRATANTE, sem a necessidade de alteração do código-fonte;

6.52.13.2 Permitir configurar aprovação em fluxos trabalho no mínimo com as seguintes regras para andamento do fluxo, sem necessidade de programação ou alterações do código-fonte:

6.52.13.3 Aprovação por um usuário específico;

6.52.13.4 Aprovação por conjuntos de usuários e regras específicas para sequência de aprovação;

6.52.13.5 Aprovação pelo gerente de um grupo solucionador;

6.52.13.6 Aprovação pelo gerente do solicitante;

6.52.13.7 Aprovação de acordo com o cargo e a estrutura de cargos da organização de forma recursiva (independentemente da quantidade de níveis ascendentes) e dinâmica (não atrelado à usuário específico);

6.52.13.8 Aprovação por quantidade definida de pessoas em um grupo de solução;

6.52.13.9 Aprovação por vários grupos de solução;

6.52.13.10 Aprovação por grupos de solução juntamente com usuário específico.

6.52.14 RELACIONAMENTO DE REGISTROS

6.52.14.1 Prover recursos que possibilitem a parametrização de regras para aprovações de fluxos de trabalho, processos, requisições e outros registros da solução, com base nas regras de negócio do CONTRATANTE, sem a necessidade de alteração do código-fonte;

6.52.14.2 Permitir o relacionamento de tabelas de bancos de dados criadas para automação de aplicações, processos e fluxos de trabalho do CONTRATANTE, com tabelas e bancos de dados nativos da solução, sem a necessidade de programação ou alterações do código-fonte.

6.52.15 GERENCIAMENTO DE USUÁRIOS E PERMISSÕES DE ACESSO

6.52.15.1 Permitir atribuir a um usuário ou grupo de usuários específico, o acesso à abertura, modificação e fechamento de registros;

6.52.15.2 Permitir a delegação de responsabilidades, papéis e funções dentro da solução, para fins de substituição temporária do usuário principal;

6.52.15.3 Permitir configurar a aprovação em fluxos de trabalho no mínimo com as seguintes regras para andamento do fluxo, sem necessidade de programação ou alterações do código-fonte:

6.52.15.4 Permitir aprovação por um usuário específico;

6.52.15.5 Permitir aprovação por conjuntos de usuários e regras específicas para sequência de aprovação;

6.52.15.6 Permitir aprovação pelo gerente de um grupo solucionador;

6.52.15.7 Permitir aprovação pelo gerente do solicitante;

6.52.15.8 Permitir aprovação de acordo com o cargo e a estrutura de cargos da organização de forma recursiva (independentemente da quantidade de níveis ascendentes) e dinâmica (não atrelado à usuário específico);

6.52.15.9 Permitir aprovação por quantidade definida de pessoas em um grupo de solução;

6.52.15.10 Permitir aprovação por vários grupos de solução;

6.52.15.11 Permitir aprovação por grupos de solução juntamente com usuário específico.

6.52.15.12 Permitir a configuração, sem alteração de código-fonte, para aprovações que não se enquadram no subitem anterior;

6.52.15.13 Permitir atribuir a um usuário ou grupo de usuários específico, o acesso à

abertura, modificação e fechamento de registros;

6.52.15.14 Permitir a delegação de responsabilidades, papéis e funções dentro da solução, para fins de substituição temporária do usuário principal.

6.52.16 INTELIGÊNCIA OPERACIONAL

6.52.16.1 Possui a habilidade de capturar, explorar e analisar métricas operacionais que podem promover alertas, fazendo o mesmo aparecer na console de alertas e no dashboard de saúde dos serviços;

6.52.16.2 Possuir mecanismo de análise de métricas para identificar desvios/eventos baseados em estatísticas de comportamento (Ex. Faixa de uso comum de CPU, faixa de uso comum de memória), cada desvio do comportamento padrão deverá ser classificado como um evento anômalo;

6.52.16.3 O mecanismo estatístico deve ser baseado em dados histórico, e para cada métrica irá identificar o limiar superior e inferior;

6.52.16.4 Cada evento anômalo deverá receber uma classificação (score) para saber o grau de desvio;

6.52.16.5 Possuir inteligência para identificar eventos anômalos e alertas anômalos, promovendo para alertas de TI caso esteja fora de um comportamento normal;

6.52.16.6 Possuir um mapa de anomalias que mostra uma visão geral de anomalias por IC, apresentando o histórico de anomalias por item de configuração, e cores desse histórico por score (grau de anomalia);

6.52.16.7 Poder navegar por cada IC onde será apresentado a métrica coletada, o gráfico de comportamento do IC frente a métrica, as anomalias detectadas e o score (grau da anomalia) durante o tempo;

6.52.16.8 Realizar a exclusão dos dados de métricas quando o IC estiver no modo de manutenção

6.52.16.9 Possuir uma funcionalidade para testar/avaliar a detecção de anomalias, podendo comparar os resultados do teste aos resultados esperados e permitir fazer ajustes até que fique ajustado.

6.52.17 MANIPULAÇÃO DE DADOS E FORMULÁRIOS EXISTENTES E/OU NOVOS

6.52.17.1 Possuir recursos gráficos de workflow interativos para criação de processos e rotinas operacionais, que permita operações como arrastar-e-soltar para o desenho dos fluxos de trabalho;

6.52.17.2 Apresentar componente próprio para a modelagem gráfica e a automação de

processos e fluxos de trabalho na solução;

6.52.17.3 Permitir a criação dessas aplicações sem uso de código, para que toda a empresa possa desenvolver e u lizar novas aplicações integradas a plataforma;

6.52.17.4 Possuir um Estúdio IDE Integrado para desenvolvimento de aplicações integradas a plataforma;

6.52.17.5 O IDE deve possuir wizard que automaticamente crie as aplicações web e para o aplicativo mobile;

6.52.17.6 As novas aplicações deverão gerar tabelas independentes das outras aplicações. Isto é, independente de outros módulos da solução;

6.52.17.7 Uma nova aplicação deverá conter no mínimo:

6.52.17.8 Tabelas;

6.52.17.9 Elementos gráficos de interface do usuário: Menus, Módulos, Listas e Formulários;

6.52.17.10 Arquivos da Aplicação: Regras de Negócio, Workflows, Ações gráficas (UIs);

6.52.17.11 Integrações: Rest Web Services, JSON Data Format, SOAP, e outras possíveis integrações dessa aplicação;

6.52.17.12 Dependências: Tabelas de tarefas, Gerenciamento de SLA, Base de Usuários e seus respectivos acessos;

6.52.17.13 Permitir a construção independente, de menus, telas, módulos para a mesma aplicação em dispositivo móvel (iOS e Android) em aplicativo fornecido nativamente pela solução;

6.52.17.14 Integrar com gerenciador de código fontes (git).

6.52.17.15 Permitir que os desenvolvedores de aplicativos se integrem a um repositório de controle de origem (GIT), salve e gerencie várias versões de um aplicativo em ambiente desenvolvimento e/ou homologação;

6.52.17.16 O sistema deve gerar um arquivo controle de integridade (checksum) no repositório GIT para determinar se algum arquivo do aplicativo foi alterado fora da IDE de desenvolvimento. Quando o valor da soma de verificação do arquivo corresponde ao valor da soma de verificação atual, a integração ignora o processo de validação e sanitização. Quando os valores da soma de verificação não correspondem, a integração valida e limpa os arquivos do aplicativo como parte da operação de controle de origem;

6.52.17.17 Permitir a automação de fluxos de trabalho de forma gráfica, incluindo estágios, tarefas paralelas ou sequenciais, regras de decisão e aprovação, sem a necessidade de

programação ou alteração de código-fonte;

6.52.17.18 Possuir ferramenta de criação de formulários com campos específicos de cada processo e fluxo de trabalho, a fim de personalizar a inserção de informações e controles de acordo com a necessidade do CONTRATANTE, sem a necessidade de programação ou alteração do código-fonte;

6.52.17.19 Dispensar a necessidade a criação, de forma manual (usando scripts e programação), de tabelas, colunas e campos de banco de dados na solução, tornando estas atividades, quando necessárias, transparentes aos administradores da solução;

6.52.17.20 Permitir a customização de menus, formulários, labels, de automações de fluxos de trabalho e processos do CONTRATANTE, desenvolvidos e

6.52.17.21 implementados na solução, permitindo a adequação às necessidades de uso de cada usuário, sem a necessidade de programação ou alteração do código fonte;

6.52.17.22 Permitir a configuração de ciclos de vida específicos para fluxos de trabalho ou processo automatizados na solução;

6.52.17.23 Permitir que os processos e fluxos de trabalho automatizados na solução possuam as mesmas funcionalidades nativas disponibilizadas na solução, como por exemplo: requisitos de usabilidade da lista de registros, citados nesta especificação técnica, ferramentas de colaboração como chat e notificações, permitindo comunicação entre CONTRATANTEs e provedor de serviços, personalização de menus, regras de aprovação de fluxos, relacionamento entre processos, painéis e dashboards automatizados;

6.52.17.24 Deve possuir o conceito de segregação de aplicações, escopo de aplicações, funções dentro do escopo só poderão ser acessadas ou manipuladas por aqueles que possuem acesso. Ex. Escopo de aplicações do Jurídico, Escopo de Aplicações do RH, etc;

6.52.17.25 Possuir o conceito de hierarquia de escopo de aplicações;

6.52.17.26 Possuir controle de dependências entre aplicações e privilégios de acesso;

6.52.17.27 Permitir o compartilhamento de aplicações entre outras instâncias, sejam de desenvolvimento, teste ou em produção;

6.52.17.28 Possuir mecanismo de teste automatizado de versões de aplicações, dentro da própria solução, o qual permite criar e executar testes automatizados para confirmar se a instância funciona após fazer uma alteração. Por exemplo, após uma atualização, durante o desenvolvimento do aplicativo ou ao implementar configurações de instância com conjuntos de atualização. Revise os resultados do teste com falha para identificar as mudanças que causaram a falha e as mudanças que você deve revisar;

6.52.17.29 Permitir que sejam criados vários testes e fiquem disponíveis para futuros testes de upgrade ou mudanças nas aplicações, podendo ser reutilizados;

6.52.17.30 Permitir pelo menos os seguintes testes:

6.52.17.31 Testar operações básicas de um formulário;

6.52.17.32 Fazer referência a um valor de uma etapa anterior em um workflow. Ex.: Testar atribuição a um campo de formulário do valor de uma variável de saída de uma etapa anterior;

6.52.17.33 Testar uma regra de negócio que deva ser aplicado em alguma etapa;

6.52.17.34 Testar o workflow de um processo.

6.52.17.35 Após a configuração de uma aplicação permitir visualizar como a aplicação funcionaria no Tablet, em um computador ou em um dispositivo celular;

6.52.17.36 Permitir que possa utilizar/estender as tabelas de uma determinada aplicação para criar outras aplicações;

6.52.17.37 Permitir a comunicação em tempo real entre CONTRATANTEs, usuários e atendentes dos serviços;

6.52.17.38 Incluir anotações nos registros da solução, possibilitando aos operadores atendentes publicar e tornar visível ou não para os usuários;

6.52.17.39 Registrar toda comunicação entre usuários e atendentes dos serviços nos registros da plataforma;

6.52.17.40 Permitir comunicação entre as partes interessadas e envolvidas nos processos e em atendimentos dos serviços, a plataforma deve;

6.52.17.41 Possibilitar a inserção de notificações automatizadas em qualquer momento de fluxo de trabalho e processos automatizados na solução;

6.52.17.42 Configurar as notificações automáticas de alertas para reiterar chamados técnicos abertos;

6.52.17.43 Enviar notificações com informações contendo dados de qualquer parte do registro de um fluxo de trabalho ou processo implementado na solução;

6.52.17.44 Enviar notificações baseadas em condições e eventos da solução.

6.52.18 GESTÃO DE SERVIÇOS DE TI

6.52.18.1 GERENCIAMENTO DE MUDANÇA

6.52.18.1.1 Permitir o registro, a modificação, tratamento e o encerramento de mudanças;

6.52.18.1.2 Permitir configurar e gerenciar o ciclo de vida de registros de mudanças de acordo com o processo do CONTRATANTE;

6.52.18.1.3 Permitir a configuração de "n" aprovações em fluxos de registros de mudança e atender aos requisitos de aprovações em fluxos de trabalho descritos neste documento técnico;

6.52.18.1.4 Permitir o relacionamento de registros de mudanças com registros de incidente, problemas, riscos e outros registros da solução;

6.52.18.1.5 Permitir o relacionamento de registros de mudança com serviços de negócio e outros itens de configuração, inclusive com "n" itens de configuração;

6.52.18.1.6 Permitir identificar visualmente o conflito de calendário (data/hora) com outros registros de mudança programados ou em andamento;

6.52.18.1.7 Permitir a criação de modelos de mudança para utilizar e facilitar o preenchimento de outros registros de mudança;

6.52.18.1.8 Permitir o encerramento de erros conhecidos, de problemas e de incidentes quando uma mudança relacionada a estes é implementada com sucesso;

6.52.18.1.9 Dever ser possível alterar os valores da requisição de mudança durante o seu ciclo de vida, tais como, mas não limitado a prioridade, categoria, ICs e SLA, baseado em permissões;

6.52.18.1.10 A solução deve facilitar a produção do calendário de mudanças em suas diversas fases, tais como estágios de construção, implementação, testes e implantação;

6.52.18.1.11 Deve ser possível disparar consultas à base de conhecimento a partir do Gerenciamento de Mudanças;

6.52.18.1.12 Possuir funcionalidade de realização de reuniões de Comitês Consultivos de Mudanças em sala virtual online, possibilitando a reunião remota e a votação por integrantes do Comitê em tempo real, inclusive via aplicativo mobile;

6.52.18.1.13 Disponibilizar recursos para criar, avaliar, aprovar e executar mudanças e ainda gerar procedimentos de reversão de mudança;

6.52.18.1.14 Permitir a configuração de várias etapas de aprovação em fluxos de registros de mudança, conforme critérios de aprovação pré-definidos, comunicando as informações de Mudanças e PM (Programação de Mudanças) que possam ser distribuídas para a Central de Serviços e grupos de usuários;

6.52.18.1.15 Permitir a criação, de forma gráfica, de fluxos de trabalho associados a tipos específico de mudança, conforme a necessidade do CONTRATANTE, sem necessidade de alteração do código-fonte;

6.52.18.1.16 Exibir alertas quando no preenchimento de solicitações de mudanças baseados no calendário de mudanças programadas para serviços que podem causar impacto em um mesmo IC (Ex.: conflitos de janelas das mudanças que envolvem um mesmo IC);

6.52.18.1.17 Criar relacionamentos entre problemas, mudanças, incidentes, riscos e outros registros de solução;

6.52.18.1.18 Suportar a tarefa de atualização de informações de IC no CMDB quando ocorrer uma mudança bem-sucedida no mesmo.

6.52.18.1.19 Permitir o gerenciamento de todo o processo de mudanças, controlando o planejamento, as requisições, os registros, o andamento, as aprovações, a autorização da implementação, a implementação, a avaliação, e monitoramento do trâmite da Requisição de Mudança.

6.52.18.1.20 Permitir a definição de relacionamentos do tipo "resolvido por" entre incidentes e mudanças, e entre problemas e mudanças.

6.52.18.1.21 Permitir a inserção de dados em texto livre e em arquivos, assim como o uso de códigos, para a classificação de requisições de mudança (categoria e prioridade).

6.52.18.1.22 Deve permitir que mudanças não autorizadas sejam devidamente justificadas e notificadas para a Central de Serviços e para os usuários.

6.52.18.1.23 Deve permitir o registro de um ou mais itens de configuração associados à mudança.

6.52.18.1.24 Permitir o cadastramento, dentro do registro de mudança, de informações sobre a avaliação de impacto, para subsidiar o processo de autorização de mudanças (ex: relatórios técnicos anexos).

6.52.18.1.25 Permitir a elaboração de programação de mudanças, assim como a definição de janelas (dias e horários) para a execução de mudanças, em função dos itens de configuração envolvidos, do tipo e da criticidade da mudança.

6.52.18.1.26 Permitir os seguintes tipos de mudanças definidos no ITIL V3:

6.52.18.1.27 Mudanças padrão (Standard Changes).

6.52.18.1.28 Mudanças normais (Normal Changes).

6.52.18.1.29 Mudanças emergenciais (Emergency Changes).

6.52.18.1.30 Deve permitir o registro dos procedimentos para se desfazer uma mudança malsucedida (Planos de Retorno de Mudanças).

6.52.18.1.31 Permitir a identificação dos erros conhecidos, problemas e incidentes

associados a uma mudança implementada com sucesso, com o objetivo de permitir a sua revisão e o seu fechamento.

6.52.18.1.32 Permitir a divulgação de comunicados para grupos de usuários sobre informações e programações de mudanças, via correio eletrônico e quadro de avisos.

6.52.18.1.33 Permitir a tarefa de atualização automática de informações de itens de configuração no CMS, quando uma mudança for bem-sucedida.

6.52.18.1.34 Permitir o acesso aos relacionamentos entre vários itens de configuração para analisar o impacto e respaldar a avaliação de uma autorização de mudança. Esses relacionamentos devem ser visualizados em gráfico construído automaticamente, com o objetivo de apoiar a tomada de decisões pelo gerente do processo.

6.52.18.1.35 Permitir o gerenciamento de mudanças encadeadas, controlando o seu tempo de execução e o seu fluxo, incluindo mudanças predecessoras e sucessoras.

6.52.18.1.36 Deve prover acesso às informações do processo Gerenciamento de Mudanças, como a programação e o histórico de mudanças, de acordo com o nível de autorização do perfil do usuário.

6.52.18.1.37 Permitir a solicitação de autorização a grupos de usuários ou a usuários individuais, de acordo com o nível de autorização de seu perfil, com o impacto e criticidade da mudança.

6.52.18.1.38 Deve permitir que os usuários envolvidos ou impactados pela mudança possam acompanhar a sua realização.

6.52.18.1.39 Deve ser capaz de solicitar autorização, caso uma mudança necessite ser cancelada.

6.52.18.1.40 Deve o processo de Gerenciamento de Mudanças ser nativamente integrado com os seguintes processos:

6.52.18.1.41 Gerenciamento de Configuração e de Ativo de Serviço, com a possibilidade de associação de itens de configuração e pessoas a mudanças, e de auditar alterações no CMS, para as quais não há mudança registrada.

6.52.18.1.42 Gerenciamento de Incidentes, com a possibilidade de associação de Incidentes a uma mudança, com relacionamentos tipo, "causado por" ou "resolvido por".

6.52.18.1.43 Cumprimento de Requisições de Serviço.

6.52.18.1.44 Gerenciamento de Liberações e Implantações.

6.52.18.1.45 Gerenciamento de Níveis de Serviço, com a possibilidade de associar a mudança sendo gerenciada ao serviço impactado por ela.

6.52.18.1.46 Permitir o controle de acesso e as modificações realizadas nas Requisições de Mudanças, em diferentes estágios do processo, mantendo histórico sobre as alterações realizadas.

6.52.18.1.47 Deve prover facilidades de notificação, através de e-mail, quadro de aviso ou SMS aos envolvidos com uma mudança, durante todo o ciclo de vida da Requisição de Mudança, com disparo manual ou automático por gatilhos de tempo ou eventos operacionais.

6.52.18.1.48 Permitir a solução automática de incidentes e problemas, quando uma determinada Requisição de Mudança tiver sido fechada com sucesso.

6.52.18.1.49 Permitir a comunicação das informações de mudanças e programação de mudança que possam ser distribuídas para a Central de Serviços e grupos de usuários, através de e-mail ou painéis dinâmicos de monitoramento.

6.52.18.1.50 Permitir o cálculo de janelas de trabalho para a execução de atividades que indisponibilizem um item de configuração e que possam causar impacto ao serviço prestado, sugerindo períodos de menor impacto. Esses períodos devem ser calculados considerando:

6.52.18.1.51 Os horários permitidos constantes em SLA dos serviços que usam o IC a ser indisponibilizado.

6.52.18.1.52 Os horários dos "CONTRATANTEs" dos serviços.

6.52.18.1.53 Os horários que o Item de Configuração deve estar operacional para não causar impacto ao serviço.

6.52.18.1.54 Deve o calendário de mudanças alertar para mudanças que estejam planejadas fora da janela de manutenção de um item, dentro de uma janela de congelamento, ou quando conflitarem sobre o mesmo item de configuração.

6.52.18.1.55 Deve permitir a criação e armazenamento de pesquisas para Requisições de Mudança, facilitando o acesso às informações. Tais pesquisas devem definir tanto o critério de seleção dos registros (filtros) quanto o formato de apresentação (colunas que devem aparecer na lista de resultados da pesquisa).

6.52.18.1.56 Deve permitir a configuração e armazenamento de filtros de pesquisa padrão para Requisições de Mudança, facilitando o acesso às informações.

6.52.19 GERENCIAMENTO DE LIBERAÇÃO E IMPLANTAÇÃO

6.52.19.1 Permitir o registro e o gerenciamento de liberações e implantação em serviços de TIC;

6.52.19.2 Permitir configurar e gerenciar o ciclo de vida de registros de liberações e implantações de acordo com o processo do CONTRATANTE;

6.52.19.3 Permitir o relacionamento de registros de liberações e implantações com registros de mudança, registros de projetos e outros registros de processos e fluxos de trabalho automatizados na solução;

6.52.19.4 Permitir a automação da mudança de estado em registros de mudança, de acordo com a mudança de estado de registros de liberações e implantações;

6.52.19.5 Permitir o agendamento das atividades de distribuição e entrega de liberações;

6.52.19.6 Facilitar o processo de autorização e agendamento de liberação de pacotes de forma integrada ao processo de Gerenciamento de Mudanças;

6.52.19.7 Garantir que uma Liberação passe por processos de agendamento da distribuição e todas as aprovações requeridas pelo processo de Gerenciamento de Mudanças.

6.52.19.8 Deve ser possível executar funcionalidades comuns de gerenciamento de liberação, como documentar, planejar, aprovar e rastrear liberações em uma variedade de classes de ativos e ICs.

6.52.19.9 Deve ser possível realizar o gerenciamento de bugs e integrar este processo com os de gerenciamento de incidentes e problemas.

6.52.19.10 Deve ser possível realizar a rastreabilidade e gerenciamento de requisitos e integrá-los aos processos de gerenciamento de bugs, incidentes, problemas, solicitações, demandas, projetos e liberações.

6.52.19.11 Permitir processo de gerenciamento de requisitos que permita estimar e planejar os custos e esforços de implementação.

6.52.19.12 Deve ser capaz de auxiliar na geração de scripts de teste (semi-) automatizados e oferecer suporte a testes automatizados e funcionais.

6.52.19.13 Deve ser capaz de produzir relatórios de testes incluindo informações agregadas e granulares (detalhamento).

6.52.19.14 Permitir o acesso ao Banco de Dados de Gerenciamento de Configurações (CMS), possibilitando a extração de informações sobre liberações, configurações, distribuições e implementações.

6.52.19.15 Permitir a associação entre a entrega da liberação (release) com o processo de Gerenciamento de Mudanças, no que concerne o agendamento e autorização.

6.52.19.16 Deve permitir a utilização de um fluxo de Gerenciamento de Mudanças para o planejamento e gerenciamento dos rollouts (disponibilização para uso) de software, o hardware associado e sua documentação.

6.52.19.17 O fluxo deve incluir todas as fases de Gerenciamento de Liberação, e respectivas tarefas/alçadas de aprovação.

6.52.19.18 Permitir a especificação de prazos, tanto para o projeto como um todo, quanto para cada fase e para cada tarefa.

6.52.19.19 Permitir a liberação de componentes e produtos de software baseada no critério de tipo de versão (completa ou pacote).

6.52.19.20 Deve permitir que planejamentos específicos de mudança sejam associados para garantir o sucesso da implementação.

6.52.19.21 Permitir a integração nativa e na mesma plataforma entre a disciplina de Gerenciamento de Liberação e as de Gerenciamento de Configuração e de Ativo de Serviço e de Gerenciamento de Mudanças.

6.52.19.22 Permitir a definição de linha de base (baseline) para a implantação (disponibilização para uso) bem-sucedida de software e ou hardware, através de uma metodologia sistêmica, segura e autorizada.

6.52.19.23 Permitir a especificação de prazos para uma liberação, de forma integrada ao módulo de Gerenciamento de Mudanças, considerando cada fase e cada tarefa de uma liberação.

6.52.20 GERENCIAMENTO DE INCIDENTES

6.52.20.1 Permitir o registro, a modificação, tratamento e o encerramento de incidentes;

6.52.20.2 Permitir consultar a Base de Conhecimento a partir da tela do registro do incidente;

6.52.20.3 Sugerir resoluções e apresentar informações, para resolução de incidentes, na tela do registro de incidente, sem a necessidade de realizar pesquisa, oferecendo sugestões de resolução do incidente ao operador, apenas com a digitação ou preenchimento de campos básicos do registro de incidente;

6.52.20.4 Integrar com o Banco de Dados de Gerenciamento de Configuração – BDGC (do inglês CMDB), para relacionamento de incidentes com serviços de negócio e outros itens de configuração;

6.52.20.5 Deve oferecer todas as funcionalidades comuns de gerenciamento do ciclo de vida de incidentes, incluindo criação, priorização, atribuição, transferência, documentos e anexo de notas, fechamento e verificação.

6.52.20.6 Permitir a inserção de dados em texto livre e a inclusão de arquivos anexados para a descrição de incidentes e atividades ligadas à sua resolução.

6.52.20.7 Permitir, no registro de incidentes, o preenchimento automático de atributos

(campos), tais como data, hora e identificador do incidente.

6.52.20.8 Deve permitir o registro de um ou mais itens de configuração associados ao Incidente.

6.52.20.9 Deve permitir a definição dos níveis de impacto e de urgência automaticamente, a partir do serviço impactado.

6.52.20.10 Deve permitir o registro de um código de prioridade para os incidentes.

6.52.20.11 Deve definir o código de prioridade dos incidentes a partir de cálculo que se baseie no código de impacto, no código de urgência do atendimento e no marcador de CONTRATANTE ou usuário VIP.

6.52.20.12 Deve possuir um mecanismo automático para as escaladas funcionais e hierárquicas, ou seja, deve ser capaz de direcionar um atendimento para outra equipe e enviar alertas para os gerentes da organização, com base na categoria, na prioridade, no tipo de usuário afetado, na importância dos ICs afetados e no tempo transcorrido do atendimento.

6.52.20.13 Deve permitir que o incidente seja escalado manualmente, de forma funcional e hierárquica.

6.52.20.14 Permitir o redirecionamento de incidentes, entre atendentes de um ou mais grupos de suporte (equipe de serviço) técnico.

6.52.20.15 Deve ser possível a um determinado atendente ou grupo (equipe de serviço), repassar o incidente ou o problema para outro atendente ou outro grupo, sempre mantendo o histórico desses repasses.

6.52.20.16 Permitir a notificação do(s) grupos(s) de atendentes de suporte técnico, quando houver chamados recém-abertos, atrasados, escalados ou concluídos, devendo esta notificação ser encaminhada, no mínimo, através de correio eletrônico.

6.52.20.17 Permitir a associação de determinado incidente a um registro de problema.

6.52.20.18 Permitir a associação de determinado incidente ao serviço impactado.

6.52.20.19 Permitir, através de regras configuráveis, o envio de alertas de incidentes para grupos de usuários pré-definidos.

6.52.20.20 Deve fornecer consultas ou relatórios que suportem a análise de incidentes com o objetivo de identificar padrões e tendências.

6.52.20.21 Permitir a geração de relatórios de incidentes por estado, como por exemplo: resolvidos, não resolvidos ou cancelados.

6.52.20.22 Deve permitir a criação e armazenamento de pesquisas para Incidentes, facilitando o acesso às informações. Tais pesquisas devem definir tanto o critério de

seleção dos registros (filtros) quanto o formato de apresentação (colunas que devem aparecer na lista de resultados da pesquisa).

6.52.20.23 Deve permitir a configuração e armazenamento de filtros de pesquisa padrão para Incidentes, facilitando o acesso às informações.

6.52.20.24 Deve disponibilizar um registro histórico para auditoria de todos os incidentes registrados, bem como das atividades realizadas para resolução desses incidentes.

6.52.20.25 Deve possuir um mecanismo que facilite a comparação de incidentes ("incident matching") inteligente, pesquisando automaticamente registros de atendimentos anteriores com características semelhantes ao incidente que está sendo reportado (mesmos sintomas, mesmo usuário, mesmo serviço, mesmo item de configuração, mesma localidade, entre outros) e listando os problemas possíveis que podem estar associados ao incidente.

6.52.20.26 Deve permitir a configuração, pelo administrador, dos critérios de similaridade sem a necessidade de codificação ("codeless" ou "lowcode").

6.52.20.27 Deve prover acesso seguro e controlado ao CMS (Configuration Management System), permitindo a navegação, modificação e extração de informações relacionadas a incidentes, como por exemplo, indicadores de criticidade de um item de configuração.

6.52.20.28 Permitir a associação de incidentes a mudanças, provendo acesso seguro e controlado às informações do processo de Gerenciamento de Mudanças, tais como a programação e histórico de mudanças.

6.52.20.29 Permitir a associação de incidentes a problemas, provendo acesso seguro e controlado às informações do processo de Gerenciamento de Problemas.

6.52.20.30 Permitir a busca de mudanças programadas, permitindo, ao gestor de incidentes e problemas, verificar se alguma delas proverá a solução para incidentes existentes.

6.52.20.31 Permitir a especificação de determinado incidente como sendo uma pergunta frequente (FAQ) e assim, disponibilizá-lo facilmente, via os canais de autoatendimento e e-mail, para outros usuários.

6.52.20.32 Permitir a definição de roteiros de apoio ao diagnóstico e resolução de incidentes, que deverão ser automaticamente apresentados ao analista durante o preenchimento do formulário de incidente no contato com o usuário, com base em, pelo menos, o item de configuração afetado e a categoria do incidente reportado.

6.52.20.33 Deve fornecer as seguintes informações, em tempo real ou em intervalo de tempo ajustável, relativas ao processo de Gerenciamento de Incidentes:

6.52.20.34 Número total de incidentes.

6.52.20.35 Situação do incidente em cada fase da busca da solução.

6.52.20.36 Relação de incidentes pendentes.

6.52.20.37 Quantidade e percentual de incidentes classificados como graves.

6.52.20.38 Tempo médio para resolução de incidentes.

6.52.20.39 Percentual de incidentes que foram resolvidos no tempo acordado.

6.52.20.40 Deve integrar o processo de Gerenciamento de Incidentes nativamente com os seguintes processos: Gerenciamento de Mudanças, Gerenciamento de Problemas, Gerenciamento de Conhecimento, Gerenciamento de Configuração e de Ativo de Serviço.

6.52.20.41 Deve prover recurso de monitoramento e rastreamento dos registros de incidentes para que eles possam ser acompanhados pelos usuários responsáveis pelo registro/abertura e pela equipe responsável pela sua solução.

6.52.20.42 Permitir, em cada fase do ciclo de vida do incidente, o registro, a categorização e priorização desse incidente, de acordo com os padrões de SLA e OLA previamente definidos.

6.52.20.43 Deve permitir o registro de um código de fechamento distinto do código da categorização inicial do incidente, a fim de permitir-se a verificação da classificação original do chamado e a ocorrência de ajustes na classificação do chamado por parte do Service Desk.

6.52.20.44 Deve permitir tomar ações em lote, como por exemplo, registrar uma ação ou resolver diversos registros de incidente ao mesmo tempo.

6.52.20.45 Permitir pesquisas de satisfação online no seu encerramento, através da interface com o usuário.

6.52.20.46 Permitir acessar mapas de serviço, para consulta ao relacionamento de itens de configuração, a partir da tela do registro do incidente;

6.52.20.47 Permitir consultar, ou apresentar automaticamente, sem a necessidade de realizar pesquisa, outros registros de incidentes relacionados com o mesmo usuário solicitante;

6.52.20.48 Permitir criar um registro de problema ou de mudança a partir da tela do registro de incidente;

6.52.20.49 Permitir a associação e a manutenção de relacionamentos entre registros de incidentes e de problemas e outros tipos de registros da solução;

6.52.20.50 Permitir a associação entre incidentes, com a possibilidade de gestão de comunicação entre incidente pai e filho;

6.52.20.51 Permitir a gestão de comunicação para incidentes principais ou críticos, podendo

definir tarefas pré-definidas de comunicação;

6.52.20.52 Permitir a priorização, atribuição e escalação automática dos incidentes baseados na categorização do registro;

6.52.20.53 Permitir a escalação automática dos incidentes baseados em usuários afetados e intervalos de tempo pré-determinados;

6.52.20.54 Permitir a integração com ferramentas de monitoração viabilizando a abertura e fechamento de registros de incidentes de forma automática conforme estado de eventos em ferramentas de monitoração;

6.52.20.55 Apresentar automaticamente, sem a necessidade de realizar pesquisa, outros registros de incidentes relacionados com o mesmo usuário solicitante.

6.52.21 GERENCIAMENTO DE PROBLEMA

6.52.21.1 Permitir o registro, a modificação, o tratamento e o encerramento de problemas;

6.52.21.2 Permitir configurar e gerenciar o ciclo de vida de registros de problemas de acordo com o processo do CONTRATANTE;

6.52.21.3 Permitir consultar a Base de Conhecimento a partir da tela do registro do problema;

6.52.21.4 Permitir a integração com o Banco de Dados de Gerenciamento de Configuração – BDGC com o gerenciamento de problema;

6.52.21.5 Permitir acessar mapas de serviço, para consulta ao relacionamento de itens de configuração, a partir da tela do registro de problema;

6.52.21.6 Permitir o fechamento de todos os incidentes relacionados quando o problema associado ou o erro conhecido é resolvido;

6.52.21.7 Permitir a associação e a manutenção de relacionamentos entre registros de problemas e de incidentes e outros tipos de registros da solução (Ex.: registros de projetos); e

6.52.21.8 Permitir procedimentos de escalamento do gerenciamento de incidente para o gerenciamento de problema.

6.52.21.9 Deve oferecer todas as funcionalidades comuns de gerenciamento do ciclo de vida de problemas, incluindo a identificação, o registro, a classificação, a designação, a investigação, a identificação da causa raiz e a resolução de problemas.

6.52.21.10 Deve ser possível realizar análise de causa raiz, integradamente a CMDB e ao Gerenciamento de Mudanças.

6.52.21.11 Deve ser possível calcular ou prever impactos de problemas em termos de estimativas de número de incidentes para um problema especificado e usar essas informações para triagem dos problemas.

6.52.21.12 Deve ser possível gerenciar a comunicação relacionada à identificação de problemas, a fim de evitar o acúmulo de solicitações (por exemplo: a partir da descrição da solicitação já correlacioná-la com problemas em aberto e informar algo ao usuário como "estamos trabalhando nisso, deseja prosseguir ao registro dessa solicitação").

6.52.21.13 Permitir a apropriação de horas por serviço contratado objetivando gerar informações para o faturamento, através do registro das horas estimadas (planejadas) e as horas técnicas realmente utilizadas para a solução de problemas.

6.52.21.14 Permitir a definição de associação (relacionamentos) do tipo "causado por" entre problemas e incidentes.

6.52.21.15 Permitir o controle de erros conhecidos de acordo com as definições do ITIL V3, permitindo sua identificação, avaliação, registro e fechamento.

6.52.21.16 Permitir a associação e manutenção do relacionamento entre incidentes, problemas e erros conhecidos. Esta associação deverá ser feita a partir do item de configuração afetado ou pela sua categoria, bem como por outros atributos que caracterizam os problemas e incidentes envolvidos.

6.52.21.17 Deve permitir o registro de um ou mais itens de configuração associados ao Problema.

6.52.21.18 Deve prover indicadores de prioridade, de impacto e de urgência para os problemas, através de regras configuráveis, podendo levar em consideração, entre outras variáveis, o impacto e a urgência do problema cadastrado.

6.52.21.19 Deve disponibilizar um histórico de problemas e erros conhecidos para auxiliar na investigação e solução de um novo problema.

6.52.21.20 Permitir a inserção de dados em texto livre ou provenientes de arquivos, para a descrição de problemas e atividades ligadas à sua resolução.

6.52.21.21 Deve prover a integração com o processo de Gerenciamento de Mudanças, suportando, para isso, a abertura de uma requisição de mudanças a partir de um ou mais registros de problemas existentes.

6.52.21.22 Deve prover facilidade de identificação dos erros conhecidos e associados a uma mudança implementada com sucesso, permitindo a revisão e o fechamento desses erros.

6.52.21.23 Deve permitir que as alterações no estado de determinado problema sejam informadas à Central de Serviços, bem como os progressos alcançados e as soluções temporárias.

6.52.21.24 Permitir o aumento automático do grau de severidade ou de impacto, em razão do número de incidentes associados, do número de usuários finais afetados ou de acordo com outras regras configuráveis.

6.52.21.25 Deve disponibilizar, no mínimo, os indicadores chave de desempenho (KPIs) para o processo de gerenciamento de problemas.

6.52.21.26 Permitir a associação do tipo "causado por" ou "resolvido por" de um problema a uma mudança anteriormente efetuada.

6.52.21.27 Permitir a associação de requisições de serviço a problemas.

6.52.21.28 Permitir a associação de determinado problema a um (ou mais) serviço impactado.

6.52.21.29 Deve o processo de Gerenciamento de Problemas ser integrado, de forma nativa, com o processo de Gerenciamento de Conhecimento.

6.52.21.30 Deve identificar e informar, aos usuários do grupo gestor do processo de Gerenciamento de Problemas, as tendências de ocorrência de problemas, provenientes de análise dos volumes e tendências dos registros de incidentes, viabilizando o Gerenciamento Proativo de Problemas.

6.52.21.31 Permitir a associação entre um problema a outro, a mudanças, a incidentes, a requisições de serviços, sendo que os registros dependentes ("filhos") serão encerrados automaticamente quando o registro "pai" for encerrado.

6.52.21.32 Permitir a escalada funcional (direcionamento) de problemas entre grupos de atendentes (equipes de serviço), ou seja, deverá ser possível a um atendente ou a uma equipe repassar o problema para outra, sempre armazenando esse histórico.

6.52.21.33 Deve permitir o registro de um código de fechamento distinto do código da categorização inicial do problema.

6.52.22 GERENCIAMENTO DE REQUISIÇÕES DE SERVIÇO

6.52.22.1 Permitir o registro de solicitações de serviços, por meio do portal de serviços ou de tela própria de requisições de serviço;

6.52.22.2 Permitir gerenciar o ciclo de vida de requisições de serviço;

6.52.22.3 Permitir vinculação de várias tarefas para o atendimento de em um mesmo registro de solicitação, inclusive para grupos de atendimento diferentes;

6.52.22.4 Permitir configurar fluxos de trabalho diferentes para cada solicitação, conforme necessidade da CONTRATANTE;

6.52.22.5 Permitir aos atendentes a visualização do fluxo de trabalho, a partir da tela do

registro da solicitação;

6.52.22.6 Atender aos requisitos de aprovação de fluxos de trabalho descritos neste documento técnico;

6.52.22.7 Permitir a realização de atendimento da solicitação por fases, permitindo ainda a visualização gráfica das fases de atendimento e situação atual;

6.52.22.8 Permitir a criação de modelos de requisições de serviço permitindo a reutilização para configuração de outras requisições;

6.52.22.9 A solução deve possuir uma visão baseada em permissões do requisitante dos serviços no catálogo que o usuário tem direito a requisitar;

6.52.22.10 A solução deve automatizar o roteamento de requisições para a coleta das autorizações apropriadas;

6.52.22.11 A solução deve permitir que o usuário submeta requisições de serviço, mantenha a visibilidade detalhada do cumprimento da requisição e acompanhe todo o ciclo de vida do cumprimento de sua requisição, sem a necessidade de entrar em contato com a central de serviços para acompanhamento;

6.52.22.12 A solução deve permitir que indicadores de impacto, prioridade e urgência sejam atribuídos ao registro da Requisição de Serviço;

6.52.22.13 A solução deve orquestrar os processos de trabalho de requisições complexas através de tarefas sequenciais e paralelas;

6.52.22.14 A solução deve facilitar a geração de relatórios de requisições de serviço pelo próprio usuário sem a necessidade de intervenção de administradores;

6.52.22.15 Integração com sistemas de e-mail padrão de mercado, para envio de e-mails (alertas, notificações) de forma automática, ou manual (pelo operador), bem como troca de mensagens entre os profissionais da TI ou outros usuários da solução;

6.52.22.16 A solução deve permitir a criação de regras de negócio para requisições específicas ou grupos de requisições, para automatizar processos, tarefas e notificações;

6.52.22.17 A solução deve suportar a criação de Requisições, a partir de registros de incidentes; e

6.52.22.18 O Gerenciamento de Requisições de Serviço deve ser nativamente integrado ao CMDB, para permitir associar um IC à Requisição de Serviço.

6.52.23 GESTÃO DE ATENDIMENTO:

6.52.23.1 A solução deve possuir em sua plataforma uma aplicação de Gerenciamento de

Serviços a CONTRATANTEs internos e externos do CONTRATANTE, a qual possui como foco atender aos usuários de uma forma avançada e com qualidade. Neste ponto, a solução deve:

6.52.23.2 Possuir funcionalidade que permita construir (customizar) de forma no code/low code portais customizados por tipo de CONTRATANTE ou cidadão;

6.52.23.3 Possuir um modelo de dados centralizado e integrado baseado em nuvem com CMDB nativo;

6.52.23.4 Permitir suporte para desenvolvedores no-code, low-code e pro-code;

6.52.23.5 Possuir ambiente, permitindo que os atendentes do telefone, o portal, o chat e a interação por e-mail sejam feitos pela mesma aplicação;

6.52.23.6 Permitir automatizar tarefas redundantes para o CONTRATANTE, por meio do Chatbot;

6.52.23.7 Possuir regras de roteamento sofisticado, utilizando regras baseado em perfil do agente e da solicitação, geografia do agente, compromisso contratual, disponibilidade do agente, carga de trabalho do agente e outras prioridades customizáveis;

6.52.23.8 Possuir a funcionalidade de forçar perfis mandatório para atendimento de casos que exigem esse tipo de perfil profissional;

6.52.23.9 Possuir funcionalidade de Inteligência Artificial, Machine Learning para automaticamente assinalar quem irá atender, categorizar e priorizar automaticamente. Essa inteligência deve aprender baseada nos dados históricos;

6.52.23.10 Fornecer alertas aos agentes e fazer a linha de tempo de interação com o CONTRATANTE/solicitante;

6.52.23.11 Deve ter uma camada de colaboração avançada para suportar as comunicações da equipe;

6.52.23.12 Deve fornecer notificações proativas de suporte via e-mail, SMS e portal para os CONTRATANTEs afetados;

6.52.23.13 Deve ter um recurso de serviço de atendimento em campo totalmente integrado na mesma plataforma, por meio de aplicativo móvel, que deve funcionar on-line e off-line para atividades, permitindo a sincronização quando estiver conectado;

6.52.23.14 Deve fornecer autoatendimento personalizado por meio de um portal de serviços configurável que incorpora uma base de conhecimento, catálogo de serviços e comunidades;

6.52.23.15 Deve ser capaz de conectar outros departamentos aos processos de atendimento ao CONTRATANTE em uma única plataforma com aderência interna aos níveis mínimos de serviços;

6.52.23.16 Deve ser capaz de suportar diferentes SLA's para diferentes produtos pertencentes a um CONTRATANTE;

6.52.23.17 Permitir totalmente SLA's para objetos diferentes do objeto "caso", como em tarefas, incidentes, problemas, alterações e solicitações associados a um caso;

6.52.23.18 Deve fornecer gerenciamento de solicitações com várias camadas e permitir o relacionamento com registros de incidente, problemas e outras solicitações de serviço;

6.52.23.19 Deve fornecer escalonamento automático sem intervenção manual;

6.52.23.20 Deve fornecer chatbot ou agente virtual que permita o desenvolvimento de diálogos conversacionais;

6.52.23.21 Deve fornecer um espaço de trabalho eficiente do agente que permita que os agentes executem várias tarefas no trabalho em vários canais, como telefone, bate-papo, e-mail e web;

6.52.23.22 O espaço de trabalho do agente deve exibir informações contextuais automaticamente para oferecer suporte à resolução rápida de casos. Isso inclui artigos de conhecimento contextualizado, publicações na comunidade e itens de catálogo de serviços. Os agentes devem poder anexar artigos aos casos;

6.52.23.23 A solução deve permitir o feedback do CONTRATANTE sobre o artigo da base de conhecimento, por meio de um processo estruturado e automatizado de feedback;

6.52.23.24 Permitir que os agentes sinalizem quando algo está faltando no artigo da base de conhecimento e isso deve alimentar o processo de feedback estruturado de ajuste da base de conhecimento;

6.52.23.25 Na gestão do conhecimento, a solução deve permitir a definição de blocos de conteúdo reutilizáveis que possam ser incorporados em vários artigos de conhecimento, a fim de reduzir a redundância. Os blocos de conhecimento devem poder ser restringidos pelo papel do usuário.

6.52.24 GERENCIAMENTO DE PORTFÓLIO

6.52.24.1 Possuir um Portal de ideias que permita que os usuários finais visualizem, enviem, filtrem, classifiquem, comentem e votem em ideias;

6.52.24.2 Permitir que os gestores de ideias usem o Portal de ideias para revisar, avaliar, colaborar e gerenciar ideias;

6.52.24.3 Permitir que os usuários que enviam, comentam ou assinam uma ideia recebem uma notificação para qualquer mudança de estado, comentário ou resposta a essa ideia, mantendo-os informados sobre seu status e progresso;

6.52.24.4 Permitir visualizar os detalhes de uma ideia e faça ou responda perguntas e troque informações sobre uma ideia usando comentários;

6.52.24.5 Permitir que essa ideia criada no Portal de Ideias possa ser convertida diretamente para uma nova Demanda, Projeto ou itens específicos como tarefas ou histórias de usuário (user stories);

6.52.24.6 Permitir que novas demandas das áreas de negócio sejam cadastradas e um fluxo específico para o Gerenciamento Demandas e de Portfólio de Serviços;

6.52.24.7 Permitir que registros de novas demandas sejam desdobrados e permaneçam relacionados em novos registros de projetos (tradicionais ou ágeis) permitindo ao CONTRATANTE escolher como a demanda será atendida e em que tipo de projeto;

6.52.24.8 Permitir o relacionamento do Serviços de TI e registros de processos de Gerenciamento de Serviços de TI com registros de demandas no Portfólio de Serviço;

6.52.24.9 Permitir o relacionamento de uma nova necessidade de negócio com um serviço existente;

6.52.24.10 Permitir o tratamento de uma nova necessidade de negócio mesmo sem estar atrelado a um serviço de TIC;

6.52.24.11 Permitir a configuração de comitês de aprovação para investimentos em serviços e aprovações nos fluxos de trabalho do processo de Portfólio de Serviços de TIC;

6.52.24.12 Permitir a configuração e automação do Termo de Serviço para documentação de Serviços de TIC.

6.52.25 GERENCIAMENTO DE DEMANDAS

6.52.25.1 Permitir o registro de novas demandas de negócio para serem atendidas em projetos de TI;

6.52.25.2 Permitir que demandas registradas sejam desdobradas em projetos de TI (projetos tradicionais ou baseados em metodologias ágeis).

6.52.26 GERENCIAMENTO DE PROJETOS

6.52.26.1 Permitir a configuração do ciclo de vida do projeto de acordo com o Modelo de Gerenciamento de Projetos do CONTRATANTE;

6.52.26.2 Permitir relacionar e integrar projetos com registros de processos de gerenciamento de serviços (Ex.: registros de mudança, incidentes, problemas, requisições, eventos e liberações e implantações);

6.52.26.3 Permitir relacionar e integrar projetos com tabelas de banco de dados da solução,

criados especificamente para aplicações do CONTRATANTE;

6.52.26.4 Permitir relacionar e integrar projetos e tarefas de projetos com registros de qualquer processo, fluxo de trabalho, sistema ou aplicações criadas ou automatizadas dentro da solução para o CONTRATANTE;

6.52.26.5 Possuir funcionalidades de gerenciamento de projetos tradicionais, híbridos e ágeis. Por exemplo baseadas em PMI/Prince2 e SCRUM;

6.52.26.6 Prover a capacidade de gerenciar carteiras de projetos com seus respectivos indicadores de acompanhamento (no mínimo prazos e custos);

6.52.26.7 Prover a capacidade de gerenciar programas e monitorar seus indicadores (no mínimo prazos e custos);

6.52.26.8 Permitir importar e exportar projetos da ferramenta MS-Project (Microsoft);

6.52.26.9 Permitir controlar o apontamento de horas dentro das atividades do projeto com processos de revisão e aprovação destas;sim

6.52.26.10 Prover fluxos de trabalho prontos com o processo de gestão de projetos, com funcionalidades de aprovações, paralelismo de atividades, alertas e controles de prazo;

6.52.26.11 Permitir a criação de campos adicionais nos formulários que (buscam) carregam informações de programas e projetos;

6.52.26.12 Permitir relacionar casos de negócio, finanças, subprojetos, requisitos e outros atributos de acordo com as necessidades do CONTRATANTE;

6.52.26.13 Possuir interface para visualização de projetos em gráfico de Gantt;

6.52.26.14 Possuir painéis e dashboards resumidos com informações sobre tarefas de projetos e seus status;

6.52.26.15 Possuir visões de painéis e dashboards específicos para o Escritório de Projetos e para os Gestores (Project Management Office – PMO e para o Chief Information Officer – CIO), permitindo uma completa visão dos programas e projetos do CONTRATANTE;

6.52.26.16 Permitir a revisão do diagnóstico estratégico, com o estabelecimento de indicadores, metas e objetivos estratégicos e a medição das iniciativas x indicadores;

6.52.26.17 Permitir acompanhar a implementação e monitorar o andamento do Plano Estratégico.

6.52.27 GERENCIAMENTO DE DESENVOLVIMENTO ÁGIL

6.52.27.1 Possuir módulo para gerenciamento de projetos baseado em metodologias ágeis;

6.52.27.2 Permitir a criação e cadastramento Produtos, Backlog de Produto, o cadastramento de histórias de usuário e sprints, bem como, a priorização de itens;

6.52.27.3 Permitir o relacionamento de Produtos e Backlog de Produtos com Serviços de TIC, registros processos e projetos;

6.52.27.4 Permitir que as Releases sejam cadastradas e definidas em cronograma para executar histórias priorizadas a partir do backlog.

6.52.27.5 Permitir que as histórias do backlog possam ser categorizadas por temas e épicos.

6.52.27.6 Permitir que Sprints sejam geradas para grupos de atribuições específicos. Grupos diferentes podem usar agendas de sprint diferentes ou todos os grupos podem seguir a mesma agenda.

6.52.27.7 Possuir um Painel para controle Ágil de projetos, onde as tarefas possam ser movidas no modelo Scrum, com recursos de arrastar e soltar (drag-and-drog) as tarefas;

6.52.27.8 Permitir visualizar e atualizar vários registros de tarefas, que aparecem como cartões (cards) que podem ser movidos entre as rotas (fases/situações ou outra cadastrada);

6.52.27.9 Permitir que o fluxo de atividades exiba as atividades recentes para que possa rastrear facilmente as alterações nas tarefas;

6.52.27.10 Permitir o relacionamento de registros da metodologia Scrum com registros de fluxos de trabalho do CONTRATANTE implementados na solução.

6.52.28 GERENCIAMENTO DE OPERAÇÕES DE TECNOLOGIA DA INFOMAÇÃO

6.52.28.1 DESCOBERTA DE ITENS DE CONFIGURAÇÃO

6.52.28.1.1 Prover a descoberta de toda a infraestrutura, Itens de Configuração e seus respectivos relacionamentos de forma automática sem agentes instalados em ambiente on-premises ou em nuvem, para a população do BDGC.

6.52.28.1.2 A descoberta deve permitir encontrar computadores/notebooks, servidores, impressoras, uma variedade de dispositivos habilitados para IP e as aplicações executadas neles, atualizando, se necessário, o BDGC com os dados que coleta

6.52.28.1.3 Prover a descoberta dos serviços de negócio "top down" e criar um mapa abrangendo todos os dispositivos, aplicações e perfis de configuração referente a estes serviços de negócio.

6.52.28.1.4 A descoberta top-down deve permitir que o Mapeamento de serviço usado para localizar e mapear ICs que fazem parte dos serviços de negócios, como um serviço de e-mail. Por exemplo, a descoberta de cima para baixo (top-down) pode mapear um serviço de negócios do site da Web, mostrando os relacionamentos entre um serviço de servidor da web Apache Tomcat, um servidor Windows e o banco de dados MSSQL que armazena os dados para o serviço de negócios

6.52.28.1.5 Possuir uma base única de gerenciamento de ativos e itens de configuração podendo gerenciar tais itens independentemente da metodologia ou processo e que permita sua população de forma automatizada e manual.

6.52.28.1.6 Prover a informação de configuração do serviço na linha do tempo, possibilitando a visualização das diferenças entre o período atual e a data selecionada.

6.52.28.1.7 Permitir a fácil visualização no mapa do impacto causado por eventos e/ou problemas associados que lhe causam impacto, permitindo a rápida visualização dos ICs e seus relacionamentos em estrutura de árvore de serviço.

6.52.28.1.8 Permitir inventariar e mapear serviços de negócio hospedados em nuvem privada, pública, híbrida ou em recursos locais.

6.52.28.1.9 Permitir a configuração de informações de cada tipo de ativo, permitindo adicionar e remover campos de informações de gestão do ativo.

6.52.28.1.10 Permitir o acesso seguro e controlado à base de dados do gerenciamento da configuração.

6.52.28.1.11 Permitir o armazenamento do histórico de mudanças dos IC para fins de auditoria.

6.52.28.1.12 A solução deve implementar e seguir corretamente o fluxo de Gerenciamento de Configuração e Ativos de Serviço conforme prescrito na biblioteca ITIL V3 e deve permitir no mínimo:

6.52.28.1.13 Manter atualizadas características da configuração de ativos;

6.52.28.1.14 Manter atualizadas características da configuração de componentes de ativos;

6.52.28.1.15 Manter atualizados os relacionamentos entre ativos com possibilidade de representação gráfica destes relacionamentos;

6.52.28.1.16 A representação gráfica do relacionamento entre ativos deve permitir o drill down de informações, para obter detalhes do ativo, seus relacionamentos, seus usuários, ou seus componentes;

6.52.28.1.17 A solução deve oferecer a capacidade de carga a partir de fontes externas

e extração por outras aplicações de informações do CMDB, para população de dados e consultas;

6.52.28.1.18 A solução deve permitir a criação manual de itens de configuração a partir de modelos pré-definidos (templates), para agilizar o preenchimento de informações e criação de relacionamentos entre ativos;

6.52.28.1.19 Permitir a criação livre de itens de configuração, para o registro e controle de itens que não se aplicam sob um padrão;

6.52.28.1.20 Permitir a criação manual de itens de configuração para aqueles tipos de ativos que não sejam eletronicamente inventariáveis;

6.52.28.1.21 Permitir o complemento de informações de um ativo, que não puderam ser eletronicamente inventariadas ou que não estavam disponíveis;

6.52.28.1.22 Permitir também o cadastro de itens não técnicos, como mobiliário, equipamentos que não pertençam à TI, dentre outros, sem prejuízo à capacidade de relacioná-los com outros itens, técnicos ou não, para a representação gráfica dos relacionamentos;

6.52.28.1.23 A solução deve permitir o gerenciamento de todo o ciclo de vida do ativo, de acordo com as definições da biblioteca ITIL V3 ou conforme necessidades.

6.52.28.1.24 Cria e manter o mapa de serviço que apresenta os componentes de TI e suas dependências, com uma abordagem de cima para baixo (Top-Down);

6.52.28.1.25 O qual inclui, tráfego de rede, descobertas e mapas de relacionamento entre os componentes, mesmo que dinâmicos, ou ambientes virtualizados.;

6.52.28.1.26 Esse mapeamento fica continuamente monitorando as mudanças no ambiente para atualizar os mapas de serviços em tempo real. Permitindo que se tenha uma fotografia em tempo real do impacto no serviço e possa proativamente identificar problemas.

6.52.28.1.27 Permitir a descoberta, inventário e gerenciar proativamente todos os seus certificados TLS da organização.

6.52.28.1.28 Permitir que o processo de descoberta verifique automaticamente os certificados em portas específicas (portas padrões como 443, 8443, 636 etc e cadastro de outras) por meio de seus agendamentos de descoberta baseados em CI existentes.

6.52.28.1.29 Permitir criar agendamentos de descoberta para verificar URLs específicas.

6.52.28.1.30 Permitir o cadastramento do certificado como um item de configuração no CMDB e manter informado sobre expirações iminentes.

6.52.28.1.31 Deve automaticamente criar tarefas de certificado por meio de fluxos para renovar certificados expirados.

6.52.28.1.32 Deve automaticamente criar incidentes para certificados já expirados.

6.52.28.1.33 Solicitações de certificado e incidentes devem ser criados automaticamente quando certificados próximos a vencer e expirados são descobertos.

6.52.28.1.34 Solicitações e incidentes de renovação de certificados devem ser criadas automaticamente quando os certificados estão prestes a expirar ou expiraram.

6.52.28.1.35 Solicitações podem ser criadas manualmente usando o Catálogo de Serviços no ITSM da plataforma.

6.52.28.1.36 As tarefas para renovações de certificados devem ser geradas automaticamente 60 dias antes da expiração e deve permitir parametrização da quantidade de dias.

6.52.28.1.37 Se já houver uma tarefa de certificado para o certificado atual, nenhuma tarefa adicional deverá ser criada.

6.52.28.1.38 Para tarefas e incidentes de certificado de renovação, vários campos devem ser pré-preenchidos automaticamente com base no IC do certificado (validade, número de série, subject common name etc).

6.52.28.1.39 Permitir que os Itens de Configuração criados a partir dos certificados identificados possam ser priorizados em relação a importância do certificado.

6.52.28.1.40 Permitir descobrir a cadeia de certificados para cada uma das URLs no lote e armazenar as informações da cadeia de certificados para cada certificado.

6.52.28.1.41 Permitir a descoberta diretamente na CA Authority utilizando chamadas de API REST de acordo com o padrão da CA específico (minimamento para GoDaddy, DigiCert, Entrust, Sectigo Certificate Authority).

6.52.28.1.42 Deverá permitir o cadastro das credenciais junto a API da CA (API Key/Secret Key etc).

6.52.28.1.43 Permitir importar os certificados SSL em massa para economizar tempo e recursos utilizando arquivo .xlsx contendo informações como: root issuer, issuer, subject comman name, issuer common name, fingerprint, issuer distinguisged name, validade, algoritimo de assinatura, tamanho da chave e estado (exemplo: instalado, revogado, retired ou outros).

6.52.28.1.44 Permitir a descoberta de certificado por meio da importação de arquivo de certificado armazenado em uma pasta de um servidor na rede Caixa, minimamente nos seguintes formatos: .cert, .pem, .txt e .der.

6.52.28.1.45 Permitir que os certificados descobertos sejam relacionados com servidores, aplicativos ou serviços de negócio existentes no CMDB para identificado todos os locais onde os certificados estão instalados.

6.52.28.1.46 Possuir painéis de gerenciamento de certificados exibindo um resumo de todos os certificados e tarefas de certificados criados.

6.52.28.1.47 Consolida, correlaciona e analisa eventos de todas as ferramentas de monitoração para apresentar em tempo real informações sobre a saúde dos serviços de negócio e sua infraestrutura;

6.52.28.1.48 Possuir separação entre eventos e alertas. Eventos serão as notificações informadas por uma ou mais fonte externa/ferramentas de monitoração (Zabbix, Nagios, Openview, vCenter, Trap SNMP, email, etc) as quais indicam algo que ocorreu no ambiente que necessita ser registrado, como logs, warning ou erro. Alertas serão um ou mais eventos que serão destacados que possuem relevância para ser tratados e gerenciados, pois requerem mais atenção.

6.52.28.1.49 Deve integrar com as ferramentas padrões de Mercado de monitoração nativamente u lizando os seguintes tipos de conexão, REST API, SNMP, ou JavaScript customizado.

6.52.28.1.50 Possuir a função de criar um servidor intermediário para conectar os monitores à aplicação de gerenciamento de eventos, possuindo as formas de pull (coletar os eventos de alguma fonte) ou push (listeners).

6.52.28.1.51 Possuir interface para criar conectores, porém já possuir conectores nativos, formato pull, para: Microsoft SCOM, Nagios, vCenter, vRealize e Zabbix).

6.52.28.1.52 Possuir conectores na vos, formato push (listener) para: AWS, Azure, SNMP Traps, Email.

6.52.28.1.53 Possuir uma arquitetura que permita separar os eventos recebidos, classificar e identificar quais dos eventos serão criados Alertas que realmente necessitam de atenção do time de operação. Evitando excesso de trabalho no volume de eventos das diversas fontes de informação.

6.52.28.1.54 O evento original deve ser mantido, para revisão ou remediação.

6.52.28.1.55 Deve possuir pelo menos os seguintes campos em um evento: Fonte do Evento, Nó que ocorreu o evento (FQDN, endereço IP ou endereço MAC), Tipo do Evento, Recurso relevante (ex. Disco, CPU, processo, serviço, Mensagem chave, Tipo do IC, Severidade, estado do evento (pronto, processado, ignorado ou com erro), estado de resolução (novo ou fechado), hora/minuto e dia que o evento ocorreu, Indicador que um alerta foi criado com o número do alerta, descrição do evento, informações adicionais do evento, log de processamento do evento.

6.52.28.1.56 Possuir mecanismos para ver todos os eventos que estão vindo de fontes

de monitoração ou de outras fontes como Traps SNMP e email.

6.52.28.1.57 Permitir um mapeamento de-para dos campos do evento de origem para a base de evento do sistema, permitindo padronizar diversos tipos de fontes de eventos.

6.52.28.1.58 Possuir mecanismo nativo dentro da solução para gerar eventos e poder realizar testes, sem a necessidade de criar scripts e de forma amigável.

6.52.28.1.59 Permitir criar regras de eventos para gerar alertas. Cada regra de evento de possuir:

6.52.28.1.60 Informações sobre a Regra: Nome, Fonte do evento, Ordem dessa regra frente a todas outras regras e descrição);

6.52.28.1.61 Filtro em que essa Regra do Evento será aplicada (Condições que serão verificadas para que seja aplicada essa regra a esse evento);

6.52.28.1.62 Quais as informações serão utilizadas para transformar esse evento e compor alerta. Deverá permitir alterar e criar novas.

6.52.28.1.63 Possuir mecanismo que gerencie "storm" de eventos e eventos intermitentes, pelo menos com seguintes campos: Tipo de storm, número de ocorrências e duração em segundos.

6.52.28.1.64 Deverá permitir criar uma regra de evento diretamente de um evento já existente, trazendo todas as informações para a criação da regra.

6.52.28.1.65 Por padrão deverá associar um evento a um IC, porém deve permitir ajustar a regra para sobrepor esse padrão para associar um evento a um alerta de um tipo de IC diferente.

6.52.28.1.66 Permitir a configuração de desduplicação de eventos.

6.52.28.1.67 Quando um evento passar por uma regra de evento que deverá gerar um alerta, um alerta deverá ser criado. Cada alerta deverá possuir um número identificador único e um workflow específico para seu ciclo de vida;

6.52.28.1.68 As descobertas devem ser executadas através dos protocolos dos componentes que serão mapeados. Ao menos os seguintes protocolos devem ser contemplados:

6.52.28.1.69 Criar relacionamentos upstream e downstream entre os componentes interdependentes;

6.52.28.1.70 Descobrir e mapear relacionamentos do tipo virtual-virtual e virtual-físico;

6.52.28.1.71 Descobrir e mapear relacionamentos em ambientes virtualizados

instalados, como Vmware;

6.52.28.1.72 Descobrir e mapear relacionamentos onde os componentes estão dentro de um único host virtual ou espalhados por vários hosts virtuais;

6.52.28.1.73 Descobrir e mapear todos os componentes e relacionamentos de TI que suportam um serviço, incluindo aplicativos, middleware, servidores, storage e equipamentos de rede;

6.52.28.1.74 Descobrir e mapear todos os componentes e relacionamentos de TI que suportam uma aplicação, incluindo outras aplicações, servidores, middlewares, storage e equipamentos de rede;

6.52.28.1.75 Descobrir os componentes de TI individualmente, bem como todas as conexões diretas entre componentes adjacentes;

6.52.28.1.76 Descobrir, documentar e mapear dependências de aplicações instaladas em Docker e Kubernetes, suportando as APIs dessas tecnologias;

6.52.28.1.77 Descobrir, documentar e mapear dependências de recursos u lizados pelo INSS nos serviços de nuvem da AWS, Azure, Google, através das APIs desses fornecedores.

6.52.28.1.78 Disponibilizar filtros para cadastros manuais de componentes que devem ser ignorados nos processos de descoberta;

6.52.28.1.79 Disponibilizar graficamente mapas com toda topologia dos serviços identificados;

6.52.28.1.80 Disponibilizar interface para cadastro manual de serviços, componentes e transações;

6.52.28.1.81 Fornecer filtros para seleção das informações que serão coletadas durante as ações de descoberta;

6.52.28.1.82 Fornecer templates customizáveis para realização de descobertas pelos seguintes critérios:

6.52.28.1.83 Gerar mapas atualizados com a identificação dos componentes e os relacionamentos que suportam os serviços;

6.52.28.1.84 Identificar graficamente nos mapas os componentes que impactam na qualidade e disponibilidade dos serviços;

6.52.28.1.85 Identificar portas de entrada e processos utilizados em servidores e que tenham relação com os serviços mapeados; e

6.52.28.1.86 Ignorar de forma proativa componentes e relacionamentos que não fazem parte do serviço.

6.52.28.1.87 Manter os mapas de serviços atualizados periodicamente, bem como as informações das aplicações e de todos os componentes de rede. O período de atualização pode ser customizável;

6.52.28.1.88 Validar periodicamente as relações de dependência das aplicações com componentes de rede e de infraestrutura;

6.52.28.1.89 Montar mapas de dependências e de topologia automaticamente a partir do cadastro de pontos de entrada como URLs, componentes, serviços e transações;

6.52.28.1.90 Permitir a descoberta e obtenção de informações sobre softwares ou outros componentes não suportados nativamente através da customização e extensão de sensores;

6.52.28.1.91 Permitir o mapeamento manual de componentes e serviços;

6.52.28.1.92 Permitir o uso de tags personalizadas para os componentes descobertos;

6.52.28.1.93 Realizar a descoberta de forma híbrida, com e sem o uso de agentes;

6.52.28.1.94 Registrar as seguintes métricas para os relacionamentos entre todos os componentes descobertos e mapeados e registrar informações de IP e subnets associados aos componentes descobertos e mapeados; Usar aprendizado de máquina para detectar automaticamente os componentes e detectar anomalias nos serviços mapeados.

6.52.29 GESTÃO E PROVISIONAMENTO DE NUVEM

6.52.29.1 Permitir o uso em uma única interface para acessar recursos de nuvem, publicar ofertas de nuvem em um catálogo e gerenciar o uso desses recursos.

6.52.29.2 O gerenciamento de serviços em nuvem deve ser integrado a provedores de nuvem privada e pública, minimamente Amazon Web Services, Microsoft Azure e ofertas de VMware.

6.52.29.3 Permitir atribuir funções de provisionamento e governança em nuvem a grupos de usuários e usuários individuais com base nas atividades e responsabilidades do usuário.

6.52.29.4 Disponibilizar capacidade de manter uma conta de serviço como sendo um registro seguro na instância que vai armazenar a credencial e as informações de acesso para a conta de provedor de nuvem.

6.52.29.5 Permitir criar rotinas de trabalho agendado para, regularmente, baixar os dados de faturamento do provedor.

6.52.29.6 Permitir salvar os dados em uma tabela de custos e usar as informações para gerar relatórios.

6.52.29.7 Permitir analisar toda a gama de custos associados aos ativos em nuvem e utilizar os dados para identificar oportunidades, economizar dinheiro e otimizar operações.

6.52.29.8 Permitir chamar uma API do provedor de nuvem, AWS por exemplo, e usar as credenciais permanentes de uma conta mestre (da organização) para assumir a função de uma ou mais contas-membro.

6.52.29.9 Permitir execução de Descoberta de Itens de Configuração, conforme item 7.12 downloads de faturamento, provisionamento de máquinas virtuais e execução de operações de ciclo de vida em máquinas virtuais.

6.52.29.10 Permitir usar os recursos de governança da plataforma para restringir o provisionamento de recursos de nuvem incluindo cotas e políticas.

6.52.29.11 Permitir configurar fluxo de trabalhos de aprovação que deve ser usado depois que um usuário solicita um recurso de nuvem.

6.52.29.12 Possuir Portal com consolidação e visualização de todas as atividades de atividades da nuvem.

6.52.29.13 Disponibilizar no portal monitoramento da cota, custos, orçamento, ciclo de vida de eventos, stack-health e solicitações.

6.52.29.14 Permitir que por meio do portal possa solicitar stacks do catálogo de serviços e rastrear as solicitações.

6.52.29.15 Permitir que por meio do portal possa solicitar operações de ciclo de vida para stacks e recursos (por exemplo, parar, iniciar ou desprovisionar).

6.52.29.16 Permitir que por meio do portal possa criar e rastrear incidentes dos serviços em nuvem.

6.52.29.17 Permitir que ao solicitar um item no catálogo de serviços do Portal do usuário da nuvem o sistema provisione a stack automaticamente ou passe por um processo de aprovação.

6.52.29.18 Permitir o controle do limite de cota e caso exceder para o usuário ou seu grupo de usuários, uma mensagem de erro será exibida ou o sistema acionará um fluxo de trabalho de aprovação com base em políticas.

6.52.29.19 Permitir visualizar os limites de cota para ver quantos recursos foram consumidos pelo usuário e quantos pode provisionar com base nos limites de cota definidos para o usuário ou grupo de usuários.

6.52.29.20 Possuir, minimamente, os seguintes tipos de recursos predefinidos no sistema e que podem ter limites de cota definidos usuário e os grupos de usuários: Contagem

de Stack, Cotagem de VMs, Contagem de vCPUs, Contage do volume de Storage, Contagem de recursos de rede (Network).

6.52.29.21 Permitir que sejam executadas operações como Start/Stop, Deprovision e ExecuteScript nos stacks ou recursos da nuvem.

6.52.29.22 Permitir que por meio do portal sejam visualizadas e gerenciadas as seguintes atividades de ações na nuvem: Solicitações realizadas, pedidos de mudança, incidentes para stack e seus recursos, tarefas de catálogo para quando uma solicitação de stack/recurso falhe, operações de arrendamento (lease) com operações que estão se aproximando das datas de término do aluguel, visualizar as chaves SSH existentes atribuídas ou gerar uma chave.

6.52.29.23 Permitir que para provedores de nuvem que não possuem conexão nativa na plataforma possam ser realizados por meio de chamadas REST, como PUT, GET, POST e DELETE.

6.52.30 GESTÃO/CORRELACIONADOR DE ALERTAS

6.52.30.1 Um Alerta dever possuir, pelo menos, os seguintes campos: Número, Fonte do Evento, Nó que ocorreu o alerta, Tipo, Recurso (Ex. CPU, Disco 1, etc), item de configuração, Atividade (ex. Incidente, Mudança ou Problema), nome da métrica, descrição, Severidade, estado (aberto, reaberto, intermitente ou fechado), Reconhecido (Acknowledged), manutenção, dia/hora que foi atualizado, alerta pai, contagem de eventos, instancia fonte, nome do usuário que fez a última atualização, alertas correlacionados;

6.52.30.2 Para cada alerta dever possuir além dos campos indicados, informações adicionais com as seguintes abas: Serviços impactados, histórico, atividades (registros dos trabalhos realizados);

6.52.30.3 O Alerta deve possuir a função de seguir um alerta (following), para seu acompanhamento e colaboração na sua resolução;

6.52.30.4 Possuir a função de resposta rápida, permitindo abrir uma janela que possua as atividades de executar uma remediação ou abrir alguma aplicação específica;

6.52.30.5 Integração nativa com CMDB, possuindo a capacidade de reduzir os alertas irrelevantes, removendo informações duplicadas, sem perda de contexto ou de criticidade, facilitando, para os analistas, responder primeiro aos alertas de alta prioridade;

6.52.30.6 Possuir painéis intuitivos de saúde devem apresentar o estado de todos os serviços de negócio, e visualizar todos, permitindo a equipe de gerenciamento de eventos realizar o "drill down" em mapas de serviços interativos para determinar a causa raiz do problema;

6.52.30.7 Possuir pesquisa contextual na base de conhecimento para identificar artigos que possam ser utilizados para orientar a resolução ou atividades para um Alerta;

6.52.30.8 Possuir a funcionalidade de responder automaticamente a um alerta, por meio de configuração de regras, para determinar a resposta adequada a um alerta (por exemplo: Abrir um incidente, base de conhecimento, abrir uma tarefa específica, a var ações de remediação, entre outras);

6.52.30.9 As regras devem ser executadas toda vez que um alerta é aberto ou atualizado, baseado em filtro de condições;

6.52.30.10 Deve possuir pelo menos os seguintes subfluxos de remediação: Marcar um Alerta que já está reconhecido, mudar o alerta para "Em manutenção, fechar um alerta, criar um incidente,

6.52.30.11 Permitir criar subfluxos de remediação customizados;

6.52.30.12 Permitir que possa criar separação de domínios de alertas, o qual deve incluir a separação de dados, processos e atividades administrativas em grupos lógicos chamados de domínios;

6.52.30.13 Possuir a capacidade de agregação de alertas e análise de causa raiz (RCA). Com análise de alertas e agregação para serviços técnicos, serviços de aplicativos e grupos de alertas. E fornecer análise de causa raiz (RCA) para serviços de negócios no CMDB;

6.52.30.14 Possuir funcionalidade de Agregação de Alerta, associando alertas similares, mas não necessariamente idênticos, baseado também em quão próximo foram os alertas, possuindo os seguintes componentes;

6.52.30.15 Aprendizado de Agregação de Alerta – um processo que executa uma vez ao dia, avaliando alertas passados identificando padrões de relacionamento e técnicas probabilísticas, para sugerir padrões;

6.52.30.16 Permitir habilitar e desabilitar a identificação de causa raiz;

6.52.30.17 Possuir funcionalidade de validar o gerenciamento de eventos após uma mudança de configuração ou uma atualização;

6.52.30.18 Possuir pelo menos os seguintes papeis de operação de eventos: Administrador, Operador, Usuário e Integrador;

6.52.30.19 Possuir SLA integrado que permita monitorar e gerenciar a qualidade dos serviços de negócio, por exemplo contabilizar o tempo que um IC ou um serviço está no estado crítico até o momento que retorna para um estado aceitável;

6.52.30.20 Permitir criar um grupo baseado em serviços técnicos, ou seja, um grupo dinâmico baseado em um critério comum (Ex. Servidores Web de Brasília ou switches do Edifício Sede, etc);

6.52.30.21 Deverá possuir mecanismo para determinar por quanto tempo um alerta ficará ativo, mesmo quando fechado, permitindo que caso um evento ocorra após um alerta fechado ele possa reabrir o alerta ou criar um novo alerta;

6.52.30.22 Possuir funcionalidade de cálculo de impacto mostrando a magnitude de um alerta para um IC, serviços de negócio, serviços de aplicação e grupos de alertas, sendo baseado nos seguintes fatores: regras de impacto, número de alertas a vos relacionados, histórico do IC afetado, relacionamento entre o IC e o Serviço (Aplicação ou de negócio);

6.52.30.23 Deverá ter funcionalidade de excluir a análise de impacto quando a IC sob alerta es ver uma mudança programada de manutenção;

6.52.30.24 Possuir um dashboard com a informação do status dos serviços de negócio e dos grupos de alertas, permitindo de forma rápida navegar de um para outro, de ver apenas os serviços/grupos críticos, e poder pesquisar um serviço específico por meio de um campo de pesquisa. Nesse dashboard o tamanho do quadro que representa o serviço/grupo devera ser de acordo com sua: prioridade (Relacionada ao negócio, Severidade ou Custo);

6.52.30.25 Possuir de forma gráfica, baseado em árvore de serviço, a situação de cada IC do Serviço. Permitindo que ao clicar em um item de configuração na árvore, apresente os alertas referentes ao IC, no mesmo painel. Esse painel deve incluir o histórico de alerta desse serviço;

6.52.30.26 Possuir uma console de alertas, que apresente os alertas e mostre se houve relacionamento entre um alerta e outros alertas, informando se esse agrupamento foi automatizado por uma regra, automaticamente pelo sistema, pelo relacionamento de CMDB ou Manual;

6.52.30.27 Possuir mecanismo para criar regras de correlacionamento de alertas automáticas, definindo qual tipo de alerta será primário que quais serão secundários;

6.52.30.28 Possuir forma de correlacionar manualmente alertas que são relacionados, apresentado os primários e os secundários;

6.52.30.29 Apresentar um relatório de apresente o percentual de alertas que estão sendo correlacionados durante um período de tempo;

6.52.30.30 Possuir abas de inteligência (Insights), para alertas, com pelo menos as seguintes informações: Alerta repetidos e fechados com a mesma chave de mensagem, Alertas similares, Incidentes com o mesmo IC, Problemas com o mesmo IC, Requisições de Mudanças com o mesmo IC;

6.52.30.31 Possuir um ambiente configurado para o Operador.

6.52.31 INTEGRAÇÃO

6.52.31.1 Integrar com ferramentas de monitoração viabilizando a abertura e fechamento de registros de incidentes de forma automática, conforme estado de eventos e integrar com ferramentas de Application Performance Management – APM.

6.52.31.2 Possuir plataforma DevOps que deve fornecer insights de dados, facilitar o processo de mudanças e aumentar a visibilidade em no ambiente DevOps usando um único sistema.

6.52.31.3 Permitir a coleta dados em todo o conjunto de atividades do ciclo de vida para fornecer visibilidade para as equipes DevOps para que possam controlar o processo de ponta a ponta (planejar, desenvolver, construir, testar, implantar e operar), minimamente integrando-se aos seguintes aplicativos DevOps: Azure DevOps Boards, Jira, Azure DevOps Repos, GitHub, Bitbucket Server, GitLab SCM e Azure DevOps Pipelines, Jenkins e GitLab CI/CD

6.52.31.4 Permitir extrair e visualizar a progressão do estágio do pipeline e os detalhes de cada aplicativo (GitLab SCM e Azure DevOps Pipelines, Jenkins e GitLab CI/CD) no Módulo DevOps.

6.52.31.5 Permitir que o Módulo DevOps acesse as ferramentas listada com as credenciais corretas e obter a URL do webhook para retorno de informações, funcionando em duas vias.

6.52.31.6 Permitir que o Módulo DevOps descubra, automaticamente, todas as informações da ferramenta, como: Planos de aplicação da ferramenta de planejamento, repositórios de ferramentas de codificação, tarefas e pipelines de ferramentas de orquestração.

6.52.31.7 Permitir configurar a URL do webhook na ferramenta de origem para que as notificações da aplicação integrada possam ser recebidas pelo Módulo DevOps.

6.52.31.8 Permitir importar todos os dados da ferramenta e permitir o rastreamento, sendo minimamente: dados do item de trabalho do plano de aplicativo da ferramenta de planejamento (e versões do plano, recursos), ramificação do repositório de ferramentas de repositório de códigos e dados de commit, dados de execução de tarefas da ferramenta de orquestração.

6.52.31.9 Permitir criação de política de repetição de requisição HTTP para os aplicativos de integração para repetir automaticamente as solicitações com falha quando uma etapa encontrar um problema de conexão, como uma falha de rede ou limite de taxa de solicitação.

6.52.31.10 Permitir que todas as conexões de ferramentas de planejamento, codificação e orquestração suportem o modo de configuração manual, por exemplo, quando o usuário não tiver privilégios de administrador em uma das ferramentas a serem integradas para configuração do webhook.

6.52.31.11 Permitir que seja feita a associação do Commit na ferramenta de gestão de código por meio de comentários na plataforma de gestão de código Git, informando a história de usuário utilizando por exemplo: Commit da história #STRY00048 em produção.

6.52.31.12 Permitir criar solicitações de mudança no módulo de ITSM automaticamente em qualquer estágio para implantações que requerem controle de mudança no ambiente.

6.52.31.13 Permitir ao Módulo DevOps a criação automática de solicitação de mudança em seu pipeline utilizando políticas de aprovação de mudança para automatizar a aprovação sob certas condições.

6.52.31.14 Permitir a criação de mudanças no Módulo DevOps no mínimo para: Azure, Jenkins e GitLab.

6.52.31.15 Permitir que as solicitações de mudança sejam automaticamente aprovadas para mudanças de baixo risco, quando o risco e o impacto calculados estão abaixo dos valores limite (definido por formulário para o pipeline).

6.52.31.16 Permitir que os valores calculados de risco e impacto quando estiverem nos valores limite ou acima, a mudança normal permaneça no estado Avaliação ou similar até ser aprovada manualmente.

6.52.31.17 Permitir que Políticas de Aprovação de Mudanças sejam mapeada para a Política de Mudanças DevOps integradas ao módulo de chamados.

6.52.31.18 Permitir seja visualizado graficamente o pipeline extraído das ferramentas como Azure, Jenkins etc, em formato semelhante ao da ferramenta de origem.

6.52.31.19 Possuir painéis de análise de performance para obtenção do ambiente DevOps com no mínimo: Total de alterações DevOps enviadas anualmente, tempo médio para fechar as mudanças de DevOps nos últimos 30 dias, Taxa média de sucesso de mudança do DevOps para solicitações de mudança nos últimos 30 dias, volume de solicitações de mudança criadas para DevOps nos últimos 7 dias, Número de solicitações de mudança que não foram fechadas para cada pipeline, Número de alterações DevOps aguardando aprovação por intervalo de datas, Número de alterações não DevOps aguardando aprovação por intervalo de datas, Número de implantações de produção bem-sucedidas em um mês, Tempo médio de resolução para um incidente causado por uma mudança de DevOps nos últimos 30 dias.

6.52.31.20 Permitir visualizar os resultados do teste de compilação para ver quais testes foram aprovados ou reprovados na interface do módulo de DevOps.

6.52.31.21 Permitir obter uma visão rápida de como tudo está conectado para ver exatamente o que está acontecendo com o pipeline e quando, podendo acessar a UI do Pipeline e ver rapidamente os commits, os committers e outros detalhes da solicitação de mudança em um só lugar.

6.52.31.22 Permitir usar políticas de aprovação de mudança para automatizar a aprovação de solicitação de mudança no módulo de chamados para continuar a implantação por

meio do pipeline de execução automaticamente.

6.52.31.23 Permitir que integrações possam ser criadas pelo usuário do Módulo DevOps com ferramentas adicionais de planejamento, codificação e teste não incluídas nas integrações fornecidas com o Módulo DevOps padrão.

6.52.31.24 Permitir criar um subfluxo para coletar e transformar dados da ferramenta que está sendo integrada integrando sem a necessidade de código (no code/low code).

6.52.31.25 Permitir criar configurações de rotação de banco de dados e limpeza de tabela para os dados importados no Módulo Devops, não comprometendo dessa forma a performance.

6.52.31.26 Deverá permitir a coordenação de atividades de backend através da possibilidade de integração com múltiplas ferramentas e processos (ex.: gerenciamento de acesso para solicitações de acesso, sistemas de gerenciamento de portfólio para solicitações de projetos ou melhorias, sistemas externos à TI como ordens de serviço de manutenção e instalações prediais);

6.52.31.27 Plug-ins nativos para as seguintes ferramentas APM (Application Performance Monitoring):

6.52.31.27.1 Datadog.

6.52.31.27.2 Dynatrace.

6.52.31.27.3 Cisco (AppDynamics).

6.52.31.27.4 New Relic.

6.52.31.27.5 Plug-ins nativos para as seguintes ferramentas de monitoramento:

6.52.31.27.6 Zabbix.

6.52.31.27.7 VMware vRealize Operations e Wavefront.

6.52.31.27.8 Splunk.

6.52.31.27.9 Oracle Enterprise Manager.

6.52.31.28 Microsoft System Center Operations Manager (SCOM).

6.52.31.29 Microsoft Azure Monitor.

6.52.31.30 Aruba Airwave.

6.52.31.31 Deve possuir conector ou gateway que permita a integração a redes de telefonia PSTN (Public Switched Telephone Network) e VoIP por computador, permitindo que o aplicativo de atendimento aos usuários ofereça suporte a chamadas telefônicas de entrada e saída (inbound and outbound telephone calls). Uma vez configurada esta

integração, é possível aos atendentes:

6.52.31.32 Realizar chamadas para algum dos números telefônicos de contato de usuários CONTRATANTEs, de fornecedores ou pontos focais de equipes de atendimento.

6.52.31.33 Receber uma chamada de qualquer terminal de telefonia convencional, celular ou VoIP (SIP).

6.52.31.34 Transferir uma chamada para outro atendente dentro do sistema.

6.52.31.35 Ativar ou desativar, na chamada, o modo mudo.

6.52.31.36 Definir se está disponível para contatos telefônicos ou não.

6.52.31.37 Deve permitir a integração com as seguintes fontes ou protocolos de identidades e diretórios:

6.52.31.37.1 Microsoft Active Directory.

6.52.31.37.2 Azure Active Directory.

6.52.31.37.3 Bancos de dados via ODBC ou JDBC.

6.52.31.37.4 Open Lightweight Directory Access Protocol (Open LDAP).

6.52.31.37.5 Secure Lightweight Directory Access Protocol (SLDAP).

6.52.31.37.6 Security Assertion Markup Language (SAML) 2 e superiores.

6.52.31.37.7 Provedores OAuth 2.0 e superiores.

6.52.31.38 Deve suportar a integração com servidores de e-mail via protocolo SMTP e IMAP, tanto para leitura como para o envio de mensagens.

6.52.31.39 Deve permitir integrações com outras ferramentas por meio de execução de comandos em CLI, scripts e macros.

6.52.31.40 Deve integrar-se nativamente, no mínimo, às seguintes ferramentas e protocolos de comunicação e colaboração:

6.52.31.41 Microsoft Teams.

6.52.31.42 SMS gateway.

6.52.31.43 WhatsApp for Business.

6.52.31.44 Deve permitir a migração de registros de solicitações mantidas nas ferramentas em uso pelo contratante por meio de um processo não manual (ou seja, lote, script, arquivo texto etc.).

6.52.31.45 Deve ser possível a integração com sistemas ITSM de terceiros para abrir tickets automaticamente, rastrear seu status e gerenciar seu ciclo de vida.

6.52.32 GESTÃO DE ATIVOS:

6.52.32.1 Deverão ser fornecidos e instalados todos os módulos e/ou ferramentas para atender aos requisitos de Gestão de Ativos, que estará sempre associado ao processo de GERENCIAR CONFIGURAÇÃO E ATIVOS DE SERVIÇO. As informações dos ativos devem ser integradas ao CMDB (Configuration Management Database, Base de Dados do Gerenciamento de Configuração);

6.52.32.2 A solução deve permitir a gestão do inventário e licenciamento de software de forma integrada com os demais processos ITIL, suportando automação de workflows para a instalação de software mediante fluxo prévio de autorização e gerando relatórios de consumo que permitam a gestão e controle do uso das licenças;

6.52.32.3 Deverá fornecer identificação única do Item de Configuração - IC;

6.52.32.4 Deverá possibilitar o registro e atualização, de forma manual e automática, dos ICs e de seus atributos, permitindo o ajuste e adaptação (personalização) das informações do IC;

6.52.32.5 Deverá permitir copiar um IC e seus atributos para criar um IC com uma identificação distinta;

6.52.32.6 Deverá fornecer modelos de ativos e itens de configuração predefinidos e permitir a criação de modelos customizados, contendo campos pré-populados desses itens, como classificação, descrição, local, usuários, CONTRATANTEs, etc.;

6.52.32.7 Deverá fornecer funcionalidades de inventário dos ativos de TIC;

6.52.32.8 Deverá permitir a associação e visualização da dependência lógica e física entre ativos e itens de configuração;

6.52.32.9 Deverá permitir o controle de licenciamento de software, fornecendo uma visão do número total de licenças, o número de licenças em uso e a localização das licenças em uso de cada software;

6.52.32.10 Deverá controlar o fim de vida de suporte das principais aplicações de mercado;

6.52.32.11 Deverá permitir o gerenciamento de contratos e ordens de compra dos ativos e itens de configuração;

6.52.32.12 Deverá permitir inventário de todas as estações de trabalho do CONTRATANTE, coletando informações parametrizáveis pelos administradores da solução. Após esse passo, deve possibilitar a abertura de ticket para qualquer alteração no ativo;

6.52.32.13 Deverá permitir consulta das informações das estações com os parâmetros pretendidos;

6.52.32.14 Deverá permitir associação de cada item de configuração a um grupo de usuários responsáveis, com permissão para editar seus atributos e relacionamentos;

6.52.32.15 Deverá permitir a definição de permissões para cada campo do IC com, no mínimo, as seguintes opções: nenhum acesso, somente visualização e alteração;

6.52.32.16 Deverá permitir o gerenciamento dos fornecedores dos ativos e itens de configuração;

6.52.32.17 Deverá permitir visualizar facilmente a quantidade de requisições, incidentes, problemas e solicitações de mudanças relacionadas ao ativo ou item de configuração;

6.52.32.18 Permitir que os dados podem ser compartilhados de forma nativa e inteligente com outros aplicativos da plataforma;

6.52.32.19 Permitir monitorar o pico de uso e definir parâmetros para evitar ajustes dispendiosos;

6.52.32.20 Permitir que usuários consigam reservar ativos temporários, e rastrear os estágios de atendimento e ajuda para prever os níveis de estoque;

6.52.32.21 Suporte para gerenciamento de dispositivos móveis e tablets;

6.52.32.22 Permitir suporte à autorização de devolução de mercadoria (RMA) com fluxos de trabalho automatizados;

6.52.32.23 Permitir integração nativa com fluxos da solução de GRC, também objeto deste edital.

6.52.33 GERENCIAMENTO INTEGRADO PARA GOVERNANÇA DE RISCOS E CONFORMIDADE

6.52.33.1 Solução integrada para Processos, Governança, Riscos e Compliance, que deverá permitir controle e gestão do cumprimento às normas internas da DTI/INSS de regulamentações ou instruções normativas externas, visão integrada dos riscos da DTI/INSS vinculados a processos, produtos, serviços ou canais, gestão de riscos operacionais e seus planos de ação;

6.52.33.2 Solução que forneça aos usuários acessar qualquer legislação, normas, políticas e padrões e repositório de controles;

6.52.33.3 A solução deverá possuir taxonomia comum e estruturada para identificar, medir e monitorar riscos, vulnerabilidades e ameaças mantendo em repositório centralizado;

6.52.33.4 A solução deverá possuir taxonomia para processos de conformidade e para conteúdo de governança (políticas, padrões, controles);

6.52.33.5 A solução deverá possuir workflow para governança das informações de controles associados aos processos;

6.52.33.6 Permitir a gestão de riscos com a possibilidade de identificação, análise, avaliação, monitoração, proposição de controles e acompanhamento do tratamento dos riscos;

6.52.33.7 Todas as características abrangidas na solução devem ser funcionalidades da solução ofertada, não havendo necessidade de instalação de outros produtos para criação de relatórios, painel, conectores, mobile, dentre outras características;

6.52.33.8 Possibilitar a criação de painéis de indicadores que permitam a visualização completa de todas as soluções abrangidas pela plataforma (exemplo: Risco, Conformidade, etc.), e que permita a definição de controles de acesso diferenciados a cada painel;

6.52.33.9 Possibilidade de registro em hierarquia para gerenciamento de estrutura organizacional;

6.52.33.10 Possuir log completo de atividade de usuários dentro da plataforma com armazenamento irrestrito dessas informações;

6.52.33.11 Manter trilha de auditoria referente às transações realizadas na solução;

6.52.33.12 Permitir a inclusão, vinculação e parametrização para classificação de controles; marcação de controles-chave, tipo de controle, execução do controle; frequência do controle; dono do controle; resposta do controle; adequação do desenho do controle; registro de avaliação de efetividade; marcação de controles anticorrupção; marcação de controle preventivo de conflito de interesses;

6.52.33.13 Permitir catalogar riscos;

6.52.33.14 Permitir identificar, analisar, avaliar, monitorar, gerenciar e reportar riscos de maneira integrada com todos os demais módulos da solução adequada a diversas categorias de riscos, como por exemplo: Capital, Compliance, Contágio, Crédito, Estratégia, Liquidez, Mercado, Reputação ou de Imagem, Legal ou Jurídico, Operacional, Cibernético e Socioambiental;

6.52.33.15 Permitir a busca de informações em banco de dados externos;

6.52.33.16 Permitir a avaliação periódica do risco, monitorando a sua evolução analiticamente e graficamente – emissão de relatórios, mantendo histórico das avaliações de cada processo;

6.52.33.17 Manter o cadastro histórico e acompanhamento das alterações (revisionamento) dos mapas de risco;

6.52.33.18 Permitir a elaboração e parametrização de mapas de riscos;

6.52.33.19 Possibilitar a aprovação dos mapas de riscos ao final do planejamento e a revalidação dentro de frequência preestabelecida;

6.52.33.20 Descrever e associar controles existentes (processos e normas internas) aos riscos identificados, fatores de riscos, causa ou origem, consequências ou impactos;

6.52.33.21 Permitir a classificação do controle (ex.: manual ou automático; implementado, parcialmente implementado, não implementado; adequado ou não adequado);

6.52.33.22 Permitir associar eventos ao controle como Incidentes, Problemas ou Workflows;

6.52.33.23 Permitir alimentar atributos e informações adicionais ao controle, conforme a necessidade da organização;

6.52.33.24 Permitir a visualização global de todos os riscos cadastrados, independente do componente ao qual estão relacionados;

6.52.33.25 Permitir classificação de impacto e vulnerabilidade dos riscos mapeados, com agrupamentos por classificação por processos, tipo de risco, unidade responsável, dentre outros;

6.52.33.26 (Permitir pesquisar no repositório de riscos usando filtros como categoria, impacto, probabilidade, vulnerabilidade, classificação do risco; componente associado etc.);

6.52.33.27 Permitir a atribuição de pesos para cada aspecto de risco avaliado;

6.52.33.28 Permitir a elaboração de matriz de riscos (da companhia, por unidade, por processo);

6.52.33.29 Permitir visualização da Matriz de Risco, de forma a agrupar quantitativamente as avaliações, bem como de identificar os riscos dentro dos quadrantes utilizados no método de avaliação;

6.52.33.30 Selecionar a natureza e categoria do risco identificado;

6.52.33.31 Identificar responsável pela identificação e análise do risco;

6.52.33.32 Permitir a definição de responsáveis por processos, riscos, controles e planos de ação;

6.52.33.33 Definir medidas saneadoras ou de mitigação de fragilidades (Planos de Ação) de acordo com padrão estabelecido;

6.52.33.34 Permitir o acompanhamento da execução dos planos de ação;

6.52.33.35 Identificar data de cadastro das informações data de início e de conclusão das ações propostas;

6.52.33.36 Permitir visualização do status da ação proposta de acordo com padrão estabelecido;

6.52.33.37 Permitir o estabelecimento de alçadas para assunção a riscos e/ou autorização para prorrogações de prazos de planos de ação;

6.52.33.38 Oferecer um painel customizável aos donos dos riscos e controles (1ª linha de defesa) com a situação dos riscos sob sua responsabilidade, bem como dos apontamentos e obrigações a ele imputadas;

6.52.33.39 Permitir a criação de painel interativo e extração de relatório em que seja possível que os usuários vejam os controles sob sua responsabilidade e possam executar ações sobre eles (avaliações, testes e revisões);

6.52.33.40 Definir prazos dos planos de ação em função da classificação do risco e/ou da assunção de Risco pela Alta Administração, com registro para cada caso;

6.52.33.41 Permitir a criação de painéis dos indicadores de risco, de compliance e de controles internos;

6.52.33.42 Permitir inclusão de novos eventos de risco pelos usuários;

6.52.33.43 Permitir selecionar os eventos de risco para cada atividade do processo;

6.52.33.44 Permitir que os eventos de risco pudessem ser associados a mais de um processo, mas que sejam analisados e documentados individualmente para cada processo;

6.52.33.45 Permitir descrever as causas para cada evento de risco;

6.52.33.46 Permitir descrever os efeitos/consequências para cada evento de risco;

6.52.33.47 Permitir selecionar a categoria do risco identificado/selecionado;

6.52.33.48 Permitir selecionar a natureza do risco identificado, a partir da categoria do risco;

6.52.33.49 Medir o grau de exposição aos riscos e permitir acompanhar sua evolução;

6.52.33.50 Permitir a notificação parametrizável para pessoa ou grupos no cadastramento de eventos;

6.52.33.51 Permitir a identificação e cadastramento de riscos e ausência/deficiência de controles por todos os usuários com restrição de acesso por perfil, inclusive anonimamente;

6.52.33.52 Permitir agendar avaliações periódicas dos riscos e controles, com notificação controlada pela solução e painel de visualização dos riscos e controles a serem revisitados.

6.52.34 COMPLIANCE E INTEGRIDADE

6.52.34.1 Identificar, a partir da norma capturada, quais as normas que sofreram alteração em todo ou em parte;

6.52.34.2 Rastrear nas normas internas aquelas que fazem referência às normas que estão sofrendo alteração, gerando relatório para a área de compliance com o resultado do rastreamento;

6.52.34.3 Distribuir automaticamente as normas aos gestores de produtos, serviços e canais de forma a permitir o acesso ao conteúdo completo da mesma, permitir o registo de sua análise bem como o registro da manifestação de impacto;

6.52.34.4 Oferecer um repositório legislativo de fácil acesso aos usuários;

6.52.34.5 Permitir a integração da legislação aplicável aos negócios e dos instrumentos de controles vinculados (Normas Internas e Processos);

6.52.34.6 Permitir a criação de obrigações de compliance (requisitos e compromissos);

6.52.34.7 Permitir que a área de compliance tenha acesso as informações prestadas pelos gestores e possa questionar eventuais manifestações das áreas;

6.52.34.8 Permitir programar em plataforma única, indicadores do Programa de Compliance e Integridade, por meio de módulos interativos e de fácil

6.52.34.9 Compreensão, adequando os elementos e as ações correlatas estabelecidas no programa;

6.52.34.10 Permitir a análise e diagnóstico de processos críticos a par r da sua relação com riscos e eventos de perda associados, podendo ser realizado ainda o envio de notificações;

6.52.34.11 Permitir mapear os riscos de compliance e de integridade (riscos de fraude e corrupção) aos quais a empresa está sujeita;

6.52.34.12 Permitir a avaliação periódica do risco de integridade, mantendo histórico das avaliações de cada processo;

6.52.34.13 Enviar alertas e notificações periodicamente ou em casos de mudanças de cenários (novas legislações);

6.52.34.14 Apresentar interface gráfica que permita a rápida visualização de vínculos diretos e indiretos entre administradores, colaboradores e fornecedores.

6.52.35 MONITORAMENTO DE ATIVIDADES DE COMPLIANCE EM TEMPO REAL

6.52.35.1 Verificar cumprimento das recomendações / determinações de auditorias internas e externas, fiscalizações de órgãos reguladores apresentando Relatório de Pendências.

6.52.35.2 Mapeamento de violações de integridade com integração das denúncias e correição (canal de denúncias, investigações e punições).

6.52.36 GERENCIAMENTO DE DEMANDAS DE OUVIDORIA E CORREGEDORIA

6.52.36.1 Executar testes de auditoria em cada elemento (pilar) do Programa de Compliance e Integridade;

6.52.36.2 Permitir a criação/edição de normas corporativas;

6.52.36.3 Permitir a inclusão de texto, controles e recomendações de normas internas;

6.52.36.4 Permitir a aprovação da norma com alçada compartilhada;

6.52.36.5 Permitir atualização das normas com envolvimento dos responsáveis.

6.52.37 SEGURANÇA DA INFORMAÇÃO

6.52.37.1 Permitir implementar as fases ou etapas de Gestão de Segurança da Informação definidas na Norma ISO27001;

6.52.37.2 Prover ferramentas de segurança e integridades dos dados armazenados na nuvem fornecida para armazenamento da solução;

6.52.37.3 Permitir detecção e reporte tempestivo de incidentes de TI;

6.52.37.4 Permitir suporte a gestão de incidentes e continuidade de negócios de TI;

6.52.37.5 A solução deve oferecer suporte à criptografia de campos específicos de forma que seja garantida a confidencialidade das informações neles presentes, incluindo o acesso aos administradores do banco de dados;

6.52.37.6 Permitir a extração de relatórios que comprovem a segurança da informação da ferramenta com evidências de testes de segurança, por exemplo, teste de intrusão;

6.52.37.7 Permitir resguardo dos dados e entrega da base de dados dos processos e atividades com informações da Companhia quando do fim da vigência contratual, sem possibilidade de utilização das mesmas pela empresa contratada.

6.52.38 GESTÃO DE AUDITORIA

6.52.38.1 A solução deverá possuir mecanismos que envolvam um conjunto de atividades relacionadas ao planejamento de trabalhos de auditoria, execução de trabalhos e relato dos resultados;

6.52.38.2 O relatório de auditoria deve permitir que às principais partes interessadas que a estratégia de gestão de risco e conformidade da organização é eficaz;

6.52.38.3 A solução deve permitir que o administrador ou gerente de auditoria, crie compromissos para gerenciar informações de auditoria e incluir entidades, controles e testes de controle que sejam relevantes para a auditoria;

6.52.38.4 Os formulários devem ter minimamente a capacidade de identificar:

6.52.38.4.1 Estado da auditoria, exemplos: Novo, Analisado, Respondido, em revisão, fechado;

6.52.38.4.2 Tipo, exemplos: Auditoria de TI, SOX, Auditoria Financeira, Auditoria de Operações, Auditoria de Certificações, Auditoria de Projetos etc.;

6.52.38.4.3 Percentual de Completude;

6.52.38.4.4 Responsáveis;

6.52.38.4.5 Auditores;

6.52.38.4.6 Agendamento com:

6.52.38.4.7 Início planejado;

6.52.38.4.8 Fim planejado;

6.52.38.4.9 Início efetivo;

6.52.38.4.10 Fim efetivo;

6.52.38.4.11 Duração

6.52.38.4.12 Resultados, por exemplo: Satisfatório, Adequado, Inadequado;

6.52.38.5 Relatório, com minimamente:

6.52.38.5.1 Base de conhecimento utilizada;

6.52.38.5.2 Modelo a ser usado para gerar o artigo da base de conhecimento

relatando os resultados do engajamento;

6.52.38.5.3 Artigo da base de conhecimento gerado recentemente contendo os resultados do engajamento.

6.52.38.6 Permitir que depois de adicionar uma entidade a um engajamento, possa gerar testes de controle automaticamente.

6.52.38.7 Permitir que o administrador de auditoria ou gerente de auditoria, depois de criar trabalhos, defina quais entidades têm escopo no trabalho de auditoria;

6.52.38.8 Permitir que gere relatórios de auditoria e mantenha diferentes versões de relatórios de auditoria.

6.52.38.9 Permitir que os gerentes de auditoria possam criar novos Compromissos de auditoria de compromissos anteriores para reduzir a necessidade de redefinir o escopo, auditores e aprovadores para compromissos semelhantes que são realizados ao longo do ano;

6.52.38.10 Permitir que depois de definir um controle, os gerentes de auditoria criem testes de controle que são executados periodicamente e forneçam evidências

6.52.38.11 Documentadas de se o controle associado está operando corretamente;

6.52.38.12 Permitir que gerentes de auditoria criem entrevistas com os proprietários de controle para discutir e fornecer evidências documentadas de se o controle associado está operando corretamente;

6.52.38.13 Permitir que os gerentes de auditoria possam gerar um artigo da base de conhecimento (KB) que resume as descobertas de uma auditoria para que as descobertas do relatório possam ser comunicadas aos executivos.

6.52.39 MÓDULO DE SEGURANÇA E GESTÃO DE INCIDENTES

6.52.39.1 A solução deve permitir a criação de um incidente de segurança na lista de Incidentes de segurança

6.52.39.2 A solução deve fornecer uma interface gráfica para o gestor de segurança consiga identificar áreas de preocupação alto nível.

6.52.39.3 A solução deve possuir inteligência sobre a ameaças para permite encontrar indicadores de comprometimento (IoC) e enriquecer incidentes de segurança com dados ameaças.

6.52.39.4 A solução de resposta a incidentes de segurança deve permitir rastrear o progresso dos incidentes de segurança desde a descoberta e análise inicial, passando pela contenção, erradicação e recuperação, até a revisão final pós-incidente, criação

do artigo da base de conhecimento e encerramento.

6.52.39.5 A solução precisa possuir integração com soluções de segurança que permita usar resposta em tempo real e contenção de rede para realizar ações de correção nos endpoints, implementar perfis para reunir detalhes específicos sobre o host e realizar consultas ou ações específicas no endpoint.

6.52.39.6 Deve ser capaz de identificar incidentes em endpoints e traçar uma linha de ações diretamente da plataforma, mesmo que tenha integração com outras soluções.

6.52.39.7 Deve possuir a capacidade de sandbox ou ter integração com soluções para identificação e análise de malware de formar a isolar o malware em um ambiente virtual para tratativas e testes.

6.52.39.8 A solução deve possuir o recurso de inteligência preditiva para phishing para triagem e priorização pelo usuário.

6.52.39.9 A solução deve possuir integração com soluções de vulnerabilidade e segurança, no mínimo com as ferramentas:

6.52.39.10 Qualys

6.52.39.11 Rapid7

6.52.39.12 InsightVM

6.52.39.13 Tenable

6.52.39.14 Microsoft Defender.

6.52.39.15 A solução deve possuir a capacidade de importar e agrupar automaticamente itens vulneráveis de acordo com as regras de grupo, para correção das vulnerabilidades rapidamente.

6.52.39.16 Deve permitir a extração de dados de vulnerabilidade de fontes internas e externas, como o National Vulnerability Database (NVD) ou integrações de terceiros.

6.52.39.17 A solução deve possuir a capacidade de comparar dados de vulnerabilidade extraídos de fontes internas e externas e criar solicitações de alteração e incidentes de segurança usando grupos de vulnerabilidade para corrigir problemas e mitigar riscos.

6.52.39.18 A solução deve permitir acessar e fornecer um ponto de referência para os dados do Structured Threat Information Expression (STIX™) da sua empresa.

6.52.39.19 A solução deve fornece um meio para analisar as ameaças à sua organização apresentadas por parceiros ou ferramentas externas.

6.53 SOLUÇÃO DE MONITORAMENTO CONTÍNUO PARA DETECÇÃO DE POSSÍVEIS IMPACTOS

CORPORATIVOS

6.53.1 CANAIS DE SUPORTE

6.53.1.1 Para abertura de solicitações a CONTRATADA deverá formulário dentro da própria plataforma de SPRD.

6.53.1.2 O sistema deverá apresentar o histórico dos chamados de suporte permitindo visualizar informações relevantes de sua abertura, tais como solicitante, data de abertura, data de cada interação com o chamado e conteúdo das interações.

6.53.1.3 O sistema deve permitir a reabertura de chamados que tenham sido fechados, retornando estes ao status de aberto, reiniciando o atendimento.

6.53.1.4 Caso a CONTRATADA tenha um sistema de ITSM, ela poderá utiliza-lo para fazer o acompanhamento dos chamados internamente, desde que seja permitido ao CONTRATANTE acompanhar estes chamados e interagir com estes através da console de gerência do SPRDao invés de apenas por e-mail, visando manter todas as informações do contrato na console do produto.

6.53.2 MAPEAMENTO

6.53.2.1 A CONTRATADA entregará a CONTRATANTE a lista dos ativos digitais a serem monitorados, que devem ser cadastrados dentro da plataforma.

6.53.2.2 O SPRD deve ser capaz de contextualizar o tipo de ativo, afim de que seja possível criar regras especificas para cada caso ou tipo de ativo.

6.53.2.3 O SPRD deve possuir capacidade para entender no mínimo as seguintes classes de ativos:

6.53.2.3.1 **Domínios:** é um nome que serve para localizar e identificar conjuntos de computadores na internet. O nome de domínio foi concebido com o objetivo de facilitar a memorização dos endereços de computadores na Internet.

6.53.2.3.2 **Marcas:** é a marca registrada, nome fantasia, nome do produto, nome de fachada, razão social, termo ou expressão que identifique o CONTRATANTE.

6.53.2.3.3 **BIN:** Números do cartão de crédito para identificar o banco emissor e a conta do CONTRATANTE. Os primeiros seis dígitos, liderados pelo primeiro dígito que identifica a bandeira do cartão, são coletivamente conhecidos como o número de identificação do emissor e denominados números de identificação bancária.

6.53.2.3.4 **Endereço IP:** Endereço de Protocolo da Internet, do inglês Internet Protocol address, é um rótulo numérico atribuído a cada dispositivo conectado a uma rede de computadores que utiliza o Protocolo de Internet para

comunicação.

6.53.2.3.5 **Pessoa:** Informação de identificação pessoal de empregado ou pessoa de interesse para monitoramento de riscos digitais dirigidos a pessoa física.

6.53.3 MONITORAMENTO

6.53.3.1 Seguindo um processo de monitoramento contínuo em regime 24x7 a CONTRATADA deve entregar à CONTRATADA em forma de relatórios e notificações.

6.53.3.2 Deverá identificar, reconhecer, coletar, analisar, processar, organizar e apresentar informações disponíveis e acessíveis, de forma automatizada e personalizada, em conversas, mídias e redes sociais, demais páginas da internet de superfície, profunda e oculta, fóruns, redes de compartilhamento de textos e códigos-fonte, aplicativos de mensageria, lojas de aplicativos, feeds RSS, páginas de comércio eletrônico, bem como monitorar outros serviços de descoberta e monitoração e quaisquer outras fontes de informação disponíveis e acessíveis.

6.53.3.3 Correlacionar as informações coletadas, utilizando plataforma de big data para processamento visando normalizar informações, gerando listas acionáveis de inteligência contra ameaças.

6.53.3.4 A plataforma deve, por exemplo, ter a capacidade de ao encontrar um dump de senhas que cite credenciais da CONTRATADA, apresentar evidência referente apenas à contratada, ao invés de apresentar o dump completo para que a CONTRATADA o pesquise manualmente.

6.53.3.5 Deverá fornecer coleta de informações para realização de pesquisas em redes sociais e aplicativos, para, no mínimo: Twitter, Facebook, Youtube, Instagram, TikTok, LinkedIn, WhatsApp, Discord, Telegram, IRC, Pastebin, Scribd, ReclameAQUI, Apple Store, 4Shared, Google Play, Vimeo e Github.

6.53.3.6 Informar anomalias nos registros de nomes dos domínios monitorados ("whois", registros DNS, etc).

6.53.3.7 Deve ter capacidade para análise de áudio de no mínimo 1 plataforma de mensageria, paraque, caso identifique correspondência com os critérios pesquisados, fazer a transcrição de áudio em questão e transformá-lo em evento indicando no mesmo a transcrição do áudio em questão.

6.53.3.8 Na transcrição dos áudios analisados nos vídeos, deverá ser possível destacar informações relevantes de acordo com os ativos digitais definidos pela CONTRATANTE.

6.53.3.9 O áudio (completo), bem como seus metadados, onde foi encontrado algum resultado, deve ser capturado, identificado e disponibilizado para análise.

6.53.3.10 Realizar análise de conteúdo de imagens (OCR) permitindo que um screenshot

contendo uma ameaça a algum dos ativos digitais da CONTRATADA seja detectada e notificada.

6.53.3.11 Por exemplo, um screenshot de uma credencial de acesso da CONTRATANTE.

6.53.3.12 Todos os incidentes reportados devem conter informações de log sendo possível determinar:

6.53.3.13 O ativo digital ao qual aquele determinado incidente se refere;

6.53.3.14 A data e hora em que houve a coleta da informação;

6.53.3.15 A data e hora em que a informação foi analisada;

6.53.3.16 A data e hora em que a informação se transformou em um risco exibido na console do CONTRATANTE;

6.53.3.17 A prioridade do risco determinada pelo SPRD;

6.53.3.18 O tipo do incidente e a sua fonte.

6.53.3.19 O SPRD deve disponibilizar as informações das pesquisas por, no mínimo: intervalo de data, contexto, metadados e tipo da fonte.

6.53.3.20 Para as quantidades de ativos digitais presentes neste termo de referência, não poderá haver limitação da quantidade de alertas gerados pelo serviço da CONTRATADA.

6.53.3.21 As ocorrências devem possuir um campo de descrição em que os analistas possam contextualizar as informações associadas.

6.53.3.22 O serviço deverá realizar a detecção de domínios registrados que possam oferecer riscosde serem utilizados de forma maliciosa, através do registro de domínios com variações comuns de nome, permutações de caracteres e outros (typosquatting, nomes de domínios similares).

6.53.3.23 Deve possibilitar a descoberta de páginas de phishing ativas utilizando o nome, a marca e a identidade visual da CONTRATADA.

6.53.3.24 Deve possibilitar a descoberta de páginas de phishing ativamente, a partir da detecção de clones das aplicações da CONTRATANTE, independente de onde estes estejam sendo executados.

6.53.3.25 Deve possuir pelo menos 150 regras pré-definidas.

6.53.3.26 Permitir a criação e acompanhamento de Incidentes de segurança, de forma manual ou automática.

6.53.3.27 Possuir a capacidade de criação de interpretadores (coletores) para aplicaçõesproprietárias e/ou não conhecidas. Caso a CONTRATANTE solicite a criação

de coletores exclusivos para seu uso, o custo de desenvolvimento será negociado à parte.

6.53.3.28 Deve possuir foco no sistema financeiro brasileiro com fontes relevantes relacionadas a grupos de fraudadores.

6.53.3.29 Deve permitir a inclusão e o monitoramento de novos grupos dos aplicativos de mensageria, incluindo grupos que eventualmente sejam solicitados pela CONTRATANTE.

6.53.3.30 Extrair, no mínimo, os seguintes metadados de cada mensagem: autor, aplicativo de origem e data e hora, com precisão de segundos, dos momentos de envio e coleta.

6.53.3.31 Monitorar, redes de compartilhamento de textos e a plataforma de compartilhamento de códigos.

6.53.3.32 O SPRD deverá possuir a capacidade de análise de até 500 ativos digitais.

6.53.3.33 O módulo de monitoramento deve permitir o uso de regras YARA, inclusive, permitindo o cadastro de regras por solicitação da CONTRATANTE.

6.53.3.34 Para eventos do tipo "informação", não deve ser requerida qualquer tipo de ação, podendo estes serem apenas mantidos temporariamente na solução para posteriormente serem descartados.

6.53.3.35 Para eventos de criticidade superior ao tipo "informação", deve existir a garantia por parte da CONTRATADA, que uma interface humana, ou seja, um(a) analista dedicado ao SPRD, esteja validando e impedindo o envio de falsos positivos para a CONTRATANTE.

6.53.3.36 Deve oferecer canais de comunicação integrados para colaboradores da CONTRATANTE requisitarem e receberem devolutivas de incidentes detectados pela solução.

6.53.4 MITIGAÇÃO

6.53.4.1 Possibilitar a realização do serviço de TAKEDOWN para retirada do ar de sites maliciosos, sites que contenham phishing ou sites/domínios que disparem phishing que utilizem o nome, a marca ou a imagem, mesmo que similar (com intuito de confundir), os CONTRATANTEs da CONTRATANTE.

6.53.4.2 Possibilitar a realização do serviço de TAKEDOWN para retirada do ar de perfis falsos de funcionários (executivos) e da própria empresa em redes sociais;

6.53.4.3 Possibilitar a realização do serviço de TAKEDOWN para retirada do ar de

quaisquer tipos de informação disponíveis e acessíveis que violem os direitos de uso da CONTRATANTE ou que permitam burlar os meios de proteção desses direitos;

6.53.4.4 Possibilitar a realização do serviço de TAKEDOWN para retirada do ar de quaisquer tipos de informação disponíveis e acessíveis quando for identificada a tentativa de ataque à reputação da CONTRATANTE,ou ainda, a tentativa de captura de credenciais da CONTRATANTE.

6.53.4.5 Possibilitar a realização do serviço de TAKEDOWN para retirada do ar de quaisquer informações em redes sociais (Facebook, Twittter, Linkedin, Instagram, YouTube, entre outros) que tenham relação com a CONTRATANTE e não sejam autorizadas ela mesma.

6.53.4.6 Possibilitar a realização do serviço de TAKEDOWN para retirar das principais lojas de aplicativos para mobile (Google Play Store, Apple Store, etc.) os aplicativos falsos e maliciosos distribuídos fora das lojas oficiais comumente conhecidas.

6.53.4.7 Possibilitar a realização do serviço de TAKEDOWN para retirar conteúdo com documentos, informações confidenciais, informações de cartões de crédito, divulgações relacionadas a produtos e sistemas da CONTRATANTE, divulgações relacionadas a CONTRATANTEs e empregados da CONTRATANTE, além do monitoramento de sites de compartilhamento de arquivos e informações, sites de compartilhamento de textos (Pastebin, Ghostbin, entre outros) presentes na internet superficial.

6.53.4.8 A CONTRATADA deverá emitir um alerta, atualizado conforme andamento, para acompanhamento do processo de TAKEDOWN de cada ocorrência.

6.53.4.9 A CONTRATADA deverá disponibilizar um painel para consulta e análise de ocorrências (em andamento e finalizadas) do serviço de TAKEDOWN. Deve permitir consultas por intervalo de tempo, tipos de ocorrências e demais critérios relevantes na análise das ocorrências.

6.53.4.10 O serviço de TAKEDOWN deverá ser disponível em pacotes mensais de 50 em 50.

6.53.5 CARACTERÍSTICAS GERAIS E CONFIDENCIALIDADE.

6.53.5.1 A CONTRATADA deverá manter total sigilo e confidencialidade dos serviços prestados à CONTRATANTE no que se refere a não divulgação, por qualquer forma, de toda ou parte das informações ou documentos a ele relativos, e aos quais venha a ter acesso, em decorrência da prestação dos serviços executados.

6.53.5.2 Eventualmente a CONTRATANTE poderá solicitar uma reunião técnica, a ser realizada remotamente, para que um atendimento qualquer possa ser realizado e/ou acompanhado por um analista, quando a gravidade de um incidente reportado pelo SPRD for classificada como crítica.

6.53.5.3 A plataforma disponibilizada pela CONTRATADA deve oferecer conexão segura

através do protocolo HTTPS.

6.53.5.4 O acesso ao SPRD deve possuir métodos de autenticação de múltiplos fatores.

6.53.5.5 A solução deverá:

6.53.5.5.1 Ser obrigatoriamente de propriedade da CONTRATADA, não podendo ser do tipo open source (software livre), OU

6.53.5.5.2 A CONTRATADA deverá ser representante oficial do fabricante no Brasil.

6.53.5.5.3 Deverá ser obrigatoriamente de propriedade da CONTRATADA ou licenciado para uso pela CONTRATADA, e não poderá ser do tipo open source (software livre).

6.53.5.5.4 O serviço deverá ser prestado por meio de solução provida através da nuvem do fabricante. Nenhum componente da solução poderá ser hospedado ou estar sob responsabilidade da CONTRATANTE.

6.53.5.5.5 O fabricante deverá possuir equipe de suporte em português brasileiro.

6.53.5.5.6 Deve permitir extração de relatórios completos dos eventos em no mínimo formatos PDF e CSV.

6.54 SERVIÇO GERENCIADO DE MONITORAMENTO, DETECÇÃO E RESPOSTA A INCIDENTES DE SEGURANÇA

6.54.1 SERVIÇO DE MONITORAMENTO, DETECÇÃO E RESPOSTA A INCIDENTES DE SEGURANÇA

6.54.1.1 Visa o monitoramento contínuo e ininterrupto de ataques cibernéticos direcionados ao CONTRATANTE, através de fornecimento de serviços com capacidade de correlacionamento de eventos, que possam gerar eventos de segurança da informação, aos quais devem ser analisados, podendo estes serem transformados em um incidente de segurança da informação, obedecendo um processo cíclico e rigoroso de gestão de eventos.

6.54.2 SOBRE AS FERRAMENTAS A SEREM UTILIZADAS

6.54.2.1 Para execução deste serviço, a CONTRATADA deverá utilizar e ser capaz de fornecer, operar, sustentar e suportar soluções de monitoramento que atendam o descritivo técnico a seguir.

6.54.2.2 A plataforma utilizada deverá ser baseada em "Big Data" com capacidade de analisar eventos de segurança (logs).

6.54.2.3 A plataforma utilizada deverá possuir capacidade de operar com volumes massivos de dados em tempo real processando no mínimo 10000 casos de uso padrão da ferramenta, possibilitando ao CONTRATANTE criar casos de uso adicionais quando

necessário.

6.54.2.4 A plataforma deve permitir habilitar ou desabilitar os casos de uso padrão dela.

6.54.2.5 A plataforma deve suportar uma quantidade de picos, ou tráfego sustentado de até um milhão de EPSs sem penalidade de processamento ou cobranças adicionais.

6.54.2.6 A plataforma deverá possuir processo de atualização automática de novos casos de uso que o fabricante disponibilize com base nas ameaças que forem descobertas após a ativação do serviço.

6.54.2.7 A plataforma deverá possuir as características a seguir:

6.54.2.7.1 Extremamente escalável e tolerante a falhas, capaz de ingerir centenas de terabytes por dia e suportar a retenção de eventos de segurança por longo período de tempo;

6.54.2.7.2 Junte-se a eventos ao longo do tempo usando modelos Kill Chain para a análise de eventos de maior risco. Ao gerar um alerta, a plataforma deverá informar com base na metodologia MITRE o que é a ameaça em específico.

6.54.2.7.3 Permitir o hunting rápido de ameaças por meio da pesquisa em todo o banco de dados de eventos, permitindo fazer o detalhamento da pesquisa usando qualquer campo.

6.54.2.7.4 Deve suportar a retenção de todos os eventos (logs) brutos e processados durante o período de 12 meses.

6.54.2.7.5 Deve ter alta disponibilidade e mecanismos de recuperação de desastres;

6.54.2.7.6 Deve permitir a filtragem e compressão de dados seletivos em até 90% no ponto de coleta quando for utilizado um mecanismo de centralização de logs localmente.

6.54.2.7.7 Deve permitir o envio de logs de servidores do CONTRATANTE diretamente para a solução através da instalação de agentes.

6.54.2.7.8 Deve executar o armazenamento em cache local e/ou em buffer nos coletores para garantir que nenhum dado seja perdido em trânsito no caso de um problema de rede ou um pico no volume do evento;

6.54.2.7.9 Deve oferecer suporte a controles de acesso granulares baseados em funções.

6.54.2.7.10 Deve suportar fatores múltiplos de autenticação.

6.54.2.7.11 Deve incluir uma ferramenta de Security Datalake baseada em bigdata em uma arquitetura aberta e escalável e com capacidade de coletar a reter dados por períodos estabelecidos para fins de conformidade e investigação;

6.54.2.7.12 Deve ter uma instância de homologação para testes que permita isolar, do ambiente de produção, novas integrações, novos desenvolvimentos de conteúdos e novos analisadores;

6.54.2.7.13 O banco de dados de eventos deve estar em banco de dados exclusivo para este ambiente.

6.54.2.8 A solução deve atender as seguintes características:

6.54.2.8.1 Deve oferecer suporte a integração através de métodos de syslog, formatos de log estruturados (CEF, LEEF, MEF, JSON, XML), arquivos, bancos de dados (conexão JDBC), conexão API (AWS, Azure, Box, Crowdstrike, Google Report, Netskope, SVN, Salesforce, Splunk, QRadar, Netwitness, Office 365, Okta, Proofpoint, Sumologic, Workday, entre outros), WMI, consultas LDAP/LDAPS, dados e fluxo (Netflow, sFlow, jFlow), Hadoop, Registros não estruturados (Regex), agentes de terceiros (snare);

6.54.2.8.2 Deve permitir a integração com diferentes tipos de fontes de dados, como dados de identidade, logs de atividades / transações, logs de eventos de segurança, fluxos de rede, log de aplicativos / plataformas de nuvem, permissões de acesso, fontes de inteligência de ameaças, dados não estruturados e metadados de ativos;

6.54.2.8.3 Deve permitir conexão a sistemas externos de gerenciamento de identidade, como Active Directory / LDAP ou soluções de IAM (gestão de identidade), como Aveksa/Sailpoint, sistemas de RH, como Peoplesoft/Workday, para realizar o enriquecimento contextual de eventos adicionando identidade do usuário;

6.54.2.8.4 Deve ter conectores, analisadores (parsers) pré-configurados, prontos para uso, mas que possam ser modificados conforme necessário. A análise, normalização e categorização dos coletores devem ser totalmente personalizáveis na interface do usuário.

6.54.2.8.5 Deve ter uma API RESTful de serviços para integração bidirecional com outras tecnologias;

6.54.2.8.6 Deve fornecer integração com pelo menos 10 fontes de inteligência de ameaças inclusas no valor do serviço ofertado;

6.54.2.8.7 Deve realizar o enriquecimento dos eventos com dados contextuais sobre eventos no momento da captura e ingestão de dados adicionando aos eventos:

6.54.2.8.8 Identidade do usuário;

6.54.2.8.9 Contexto de negócios;

6.54.2.8.10 Metadados de ativos;

6.54.2.8.11 Informações de rede;

6.54.2.8.12 Localização Geográfica;

6.54.2.8.13 Dados de inteligência de ameaças;

6.54.2.9 Deve enriquecer eventos em tempo real com contexto de usuário e entidade. Os dados ricos podem fornecer atributos de contexto que podem ser usados para perfis comportamentais, comparações de pares, pesquisas e investigações;

6.54.2.10 Deve enriquecer e analisar dados em tempo real no momento da ingestão, bem como aplicar algoritmos comportamentais no modelo "online" para identificar ameaças;

6.54.2.11 Deve detectar ameaças cibernéticas e internas avançadas (insiderthreat) usando aprendizado de máquina para criar perfis e linhas de base de comportamento de usuários e entidades;

6.54.2.12 Deve ter conteúdo pré-empacotado de casos de uso e modelos de ameaças prontos para uso para detecção avançada de ameaças, como:

6.54.2.13 Detecção de ameaças internas (insiderthreat);

6.54.2.14 Detecção de ameaças cibernéticas (cyber threat);

6.54.2.15 Detecção de ameaças na nuvem (cloud threat);

6.54.2.16 Deve fornecer recursos abrangentes para modelar e ajustar a pontuação de risco com base no perfil do usuário e/ou entidade, gravidade da ameaça e sequência/combinação de eventos que ocorrem durante um período de tempo;

6.54.2.17 Deve permitir a modelagem de risco a partir da interface do usuário de acordo com as prioridades da organização;

6.54.2.18 Deve ter modelos de ameaças que permitam agrupar eventos realizados por um usuário ou entidade que duram dias, semanas, meses e assim por diante. Essas atividades devem ser exibidas como uma cadeia de eliminação com cada evento categorizado em estágios predefinidos.

6.54.2.19 Deve fornecer análises para diferentes tipos de anomalias, como relacionadas ao tempo, volume de transferência de dados, origem do evento relacionado, destino do evento relacionado, anomalias por usuário e grupo de pares, anomalias relacionadas a localização geográfica / velocidade terrestre, bem como rastrear usuários ou outras entidades nas listas de observação;

6.54.2.20 Os filtros para investigação devem permitir selecionar todos os campos possíveis da plataforma, bem como filtrar estes campos para facilitar encontrar a informação desejada.

6.54.2.21 Deve ter algoritmos de aprendizagem não supervisionados para analisar eventos atuais e históricos e determinar associações, para estabelecer padrões de comportamento da atividade do usuário em cada fonte de evento por dia, semana, mês, hora do dia e dia da semana. Qualquer desfio do padrão regular deve ser marcado como uma anomalia;

6.54.2.22 Deve ter algoritmos de aprendizagem supervisionados para detectar ameaças de malware avançadas, como DGA, ataques de phishing/spam e muito mais;

6.54.2.23 Deve ter técnicas de análise baseadas pares para detectar usuários que estão começando a se comportar de maneira diferente dos pares, traçando o perfil do comportamento de diferentes usuários no grupo de pares e, em seguida, comparando as transações do usuário com a dos pares;

6.54.2.24 Deve haver técnicas de análise de raridade de eventos pelas quais atividades suspeitas que não foram vistas antes possam ser identificadas;

6.54.2.25 Deve ter técnicas de análise de comportamento por enumeração que permita criar linhas de base de eventos do mesmo tipo e procurar qualquer desvio do normal;

6.54.2.26 Deve ter técnicas de análise de tráfego para identificar padrões de beaconing, agentes de usuários incomuns, conexões com URLs incomuns, conexões com domínios DGA, etc;

6.54.2.27 Deve ter técnicas de análise de dados de geolocalização para procurar padrões de login que indiquem o possível compartilhamento/comprometimento da identidade do usuário. Por exemplo, diferentes logins de um usuário de diferentes países em um período muito curto de tempo;

6.54.2.28 Deve fornecer a capacidade de definir políticas baseadas em regras para detectar ameaças conhecidas. Essas ameaças conhecidas devem ser usadas como intensificadores de risco e combinadas com as verificações "não assinadas" nos modelos de ameaças;

6.54.2.29 Deve haver modelagem de ameaças que permita a identificação de ameaças compostas, que se observadas isoladamente podem ser de baixo risco, porém, quando combinadas, são indicativas de um evento de alto risco;

6.54.2.30 Deve ter relatórios de ameaças que forneçam visibilidade da postura de segurança cibernética. Por exemplo: usuários de alto risco, ativos de alto risco, principais ameaças, principais IPs maliciosos, etc;

6.54.2.31 Deve ter relatórios que forneçam visibilidade sobre as operações de segurança. Por exemplo, para dispositivos VPN, os relatórios devem incluir as melhores sessões de VPN por duração, os principais eventos de saída de dados, a distribuição dos eventos de login por geografia, as principais tentativas de login com falha e assim por diante;

6.54.2.32 Deve ter relatórios de resumo executivo de violações, incidentes e operações;

6.54.2.33 Deve permitir que os dados sejam exibidos com diferentes tipos de gráficos: gráfico de linhas, gráfico de barras, gráfico de pizza, mapa geográfico, tabelas, gráfico empilhados, gráfico N principais, gráficos de bolhas, gráficos de relacionamento de origem e destino;

6.54.2.34 Deve possuir um painel resumo indicando os principais eventos, alertas gerados nas últimas horas, volume de eventos por segundo sendo processados, eventos processados nas últimas 24 horas.

6.54.2.35 Deve permitir a visualização de dados através de links que permitam vincular qualquer conjunto de atributos e visualização a relação entre eles;

6.54.2.36 O serviço deve possuir solução para análise de artefatos maliciosos que minimamente contemple as funcionalidades a seguir:

6.54.2.37 Analisar mais de 1000 indicadores comportamentais de um artefato;

6.54.2.38 Realizar análise estatística e dinâmica para avaliar se o artefato é malicioso ou não;

6.54.2.39 Deve suportar a análise dos artefatos BAT, CHM, DLL, ISO, HTA, HWP, JAR, JS, JSE, JTD, LNK, MSI, MHTML, documentos do Microsoft Office, EXE, PE32, PDF, VBE, URLs, WSF, XML e ZIP;

6.54.2.40 A plataforma utilizada deverá ser baseada em "Big Data" com capacidade de analisar eventos de segurança (logs);

6.54.2.41 A plataforma utilizada deverá possuir capacidade de operar com volumes massivos de dados em tempo real utilizando algoritmos de aprendizagem de automático de máquina "Machine Learning" e deve contar com casos de uso para detectar ameaças avançadas;

6.54.2.42 A plataforma deverá possuir as características a seguir:

6.54.2.42.1 Extremamente escalável e tolerante a falhas, capaz de ingerir centenas de terabytes por dia e suportar a retenção de eventos de segurança por longo período;

6.54.2.42.2 Deve suportar algoritmos de aprendizado de máquina para detectar com precisão ameaças internas e avançadas com o uso de análise de comportamento de usuários e entidades incorporada (User and Entity Behavior Analysis (UEBA));

6.54.2.42.3 Junte-se a eventos ao longo do tempo usando modelos Kill Chain para a análise de eventos de maior risco;

6.54.2.42.4 Permitir o hunting rápido de ameaças por meio da pesquisa em linguagem natural.

6.54.2.42.5 A solução deve estar classificada como líder no quadrante mágico de

"Security Information and Event Management"do Gartner em 2021;

6.54.2.42.6 A solução deve ter recursos de "Multi-tenant";

6.54.2.42.7 Deve ser do tipo Nuvem em Software como um modo de Serviço e ter as certificações SOC 2 TYPE II e ISO 27001

6.54.2.42.8 Deve garantir retenção dos logs conforme arquitetura abaixo:

6.54.2.42.8.1 7 dias hots retention;

6.54.2.42.8.2 90 dias warm retention;

6.54.2.42.8.3 365 dias cold retention;

6.54.2.42.8.4 O CONTRATANTE proverá espaço ou servidor para armazenamento dos logs;

6.54.2.42.8.5 Deve ter alta disponibilidade e mecanismos de recuperação de desastres;

6.54.2.42.8.6 Deve permitir a filtragem e compressão de dados seletivos em até 90% no ponto de coleta;

6.54.2.42.8.7 Deve permitir o gerenciamento da largura de banda para a transmissão de dados entre os coletores e os servidores de gerenciamento;

6.54.2.42.8.8 Deve executar o armazenamento em cache local e/ou em buffer nos coletores para garantir que nenhum dado seja perdido em trânsito no caso de um problema de rede ou um pico no volume do evento;

6.54.2.42.8.9 Deve oferecer suporte ao mascaramento de dados por meio de controles de acesso granulares baseados em funções, para ofuscar qualquer informação de usuário potencialmente sensível na camada de interface do usuário;

6.54.2.42.8.10 Deve suportar controle de acesso baseado em função granular (RBAC) com suporte a administração delegada, tanto para as funcionalidades na interface do usuário quanto acesso aos dados e configurações;

6.54.2.42.8.11 Deve incluir uma ferramenta de Security Datalake baseada em bigdata em uma arquitetura aberta e escalável e com capacidade de coletar a reter dados por períodos estabelecidos para fins de conformidade e investigação;

6.54.2.42.8.12 Deve ter uma instância de homologação para testes que permita isolar, do ambiente de produção, novas integrações, novos desenvolvimentos de conteúdos e novos analisadores;

6.54.2.43 A solução deve atender as seguintes características:

6.54.2.43.1 Deve oferecer suporte a integração com mais de 500 fontes de eventos usando métodos de syslog, formatos de log estruturados (CEF, LEEF, MEF, JSON, XML), arquivos, bancos de dados (conexão JDBC), conexão API (AWS, Azure, Box, Crowdstrike, Google Report, Netskope, SVN, Salesforce, Splunk, QRadar, Netwitness, Office 365, Okta, Proofpoint, Sumologic, Workday, entre outros), WMI, consultas LDAP/LDAPS, dados e fluxo (Netflow, sFlow, jFlow), Hadoop, Registros não estruturados (Regex), agentes de terceiros (snare);

6.54.2.43.2 Deve permitir a integração com diferentes tipos de fontes de dados, como dados de identidade, logs de atividades / transações, logs de eventos de segurança, fluxos de rede, log de aplicativos / plataformas de nuvem, permissões de acesso, fontes de inteligência de ameaças, dados não estruturados e metadados de ativos;

6.54.2.43.3 Deve permitir conexão a sistemas externos de gerenciamento de identidade, como Active Directory / LDAP ou soluções de IAM (gestão de identidade), como Aveksa/Sailpoint, sistemas de RH, como Peoplesoft/Workday, para realizar o enriquecimento contextual de eventos adicionando identidade do usuário;

6.54.2.43.4 Deve ser capaz de se conectar nativamente através de APIs ou outros meios com serviços em nuvem como Salesforce, Amazon Web Services S3 e Cloudtrail, BOX, Microsoft Azure, Office 365, Google Apps, Google Cloud, Netskop, ServiceNow, entre outros.

6.54.2.43.5 Deve ter uma interface de usuário que permita modificar conectores, analisadores (parsers) existentes ou construir novos analisadores (parsers) na mesma interface de usuário;

6.54.2.43.6 Deve ter conectores, analisadores (parsers) pré-configurados, prontos para uso, mas que possam ser modificados conforme necessário. A análise, normalização e categorização dos coletores devem ser totalmente personalizáveis na interface do usuário.

6.54.2.43.7 Deve ter uma API RESTful de serviços para integração bidirecional com outras tecnologias;

6.54.2.43.8 Deve fornecer integração com pelo menos 5 fontes de inteligência de ameaças inclusas no valor do serviço ofertado;

6.54.2.43.9 Deve realizar o enriquecimento dos eventos com dados contextuais sobre eventos no momento da captura e ingestão de dados adicionando aos eventos:

6.54.2.43.9.1 Identidade do usuário;

6.54.2.43.9.2 Contexto de negócios;

6.54.2.43.9.3 Metadados de ativos;

6.54.2.43.9.4 Informações de rede;

6.54.2.43.9.5 Localização Geográfica;

6.54.2.43.9.6 Dados de inteligência de ameaças;

6.54.2.44 Deve suportar o enriquecimento de eventos em tempo real com contexto de usuário e entidade. Os dados ricos podem fornecer atributos de contexto que podem ser usados para perfis comportamentais, comparações de pares, pesquisas e investigações;

6.54.2.45 Deve suportar enriquecer e analisar dados em tempo real no momento da ingestão, bem como aplicar algoritmos comportamentais no modelo "online" para identificar ameaças;

6.54.2.46 Deve suportar a detecção de ameaças cibernéticas e internas avançadas (insiderthreat) usando aprendizado de máquina para criar perfis e linhas de base de comportamento de usuários e entidades;

6.54.2.47 Deve ter conteúdo pré-empacotado de casos de uso e modelos de ameaças prontos para uso para detecção avançada de ameaças, como:

6.54.2.48 Detecção de ameaças internas (insiderthreat) utilizando técnicas de aprendizagem de máquina;

6.54.2.49 Detecção de ameaças cibernéticas (cyber threat) utilizando técnicas de aprendizagem de máquina;

6.54.2.50 Detecção de ameaças na nuvem (cloud threat) utilizando técnicas de aprendizagem de máquina;

6.54.2.51 Deve fornecer recursos abrangentes para modelar e ajustar a pontuação de risco com base no perfil do usuário e/ou entidade, gravidade da ameaça e sequência/combinação de eventos que ocorrem durante um período;

6.54.2.52 Deve permitir a modelagem de risco a partir da interface do usuário de acordo com as prioridades da organização;

6.54.2.53 Deve ter modelos de ameaças que permitam agrupar eventos realizados por um usuário ou entidade que duram dias, semanas, meses e assim por diante. Essas atividades devem ser exibidas como uma cadeia de eliminação com cada evento categorizado em estágios predefinidos.

6.54.2.54 Deve ter algoritmos preditivos para identificar usuários de risco (por exemplo, usuários prestes a deixar a organização);

6.54.2.55 Deve fornecer análises para diferentes tipos de anomalias, como relacionadas ao

tempo, volume de transferência de dados, origem do evento relacionado, destino do evento relacionado;

6.54.2.56 Dever suportar análise de anomalias por usuário e grupo de pares, anomalias relacionadas a localização geográfica / velocidade terrestre, bem como rastrear usuários ou outras entidades nas listas de observação;

6.54.2.57 Deve suportar algoritmos de aprendizagem não supervisionados para analisar eventos atuais e históricos e determinar associações, para estabelecer padrões de comportamento da atividade do usuário em cada fonte de evento por dia, semana, mês, hora do dia e dia da semana. Qualquer desvio do padrão regular deve ser marcado como uma anomalia;

6.54.2.58 Deve suportar algoritmos de aprendizagem supervisionados para detectar ameaças de malware avançadas, como DGA, ataques de phishing/spam e muito mais;

6.54.2.59 Deve suportar técnicas de análise baseadas pares para detectar usuários que estão começando a se comportar de maneira diferente dos pares, traçando o perfil do comportamento de diferentes usuários no grupo de pares e, em seguida, comparando as transações do usuário com a dos pares;

6.54.2.60 Deve haver técnicas de análise de raridade de eventos pelas quais atividades suspeitas que não foram vistas antes possam ser identificadas;

6.54.2.61 Deve suportar técnicas de análise de comportamento por enumeração que permita criar linhas de base de eventos do mesmo tipo e procurar qualquer desvio do normal;

6.54.2.62 Deve ter técnicas de análise de tráfego para identificar padrões de beaconing, agentes de usuários incomuns, conexões com URLs incomuns, conexões com domínios DGA, etc;

6.54.2.63 Deve suportar técnicas de análise de dados de geolocalização para procurar padrões de login que indiquem o possível compartilhamento/comprometimento da identidade do usuário. Por exemplo, diferentes logins de um usuário de diferentes países em um período muito curto de tempo;

6.54.2.64 Deve fornecer a capacidade de definir políticas baseadas em regras para detectar ameaças conhecidas. Essas ameaças conhecidas devem ser usadas como intensificadores de risco e combinadas com as verificações "não assinadas" nos modelos de ameaças;

6.54.2.65 Deve haver modelagem de ameaças que permita a identificação de ameaças compostas, que se observadas isoladamente podem ser de baixo risco, porém, quando combinadas, são indicativas de um evento de alto risco;

6.54.2.66 Deve suportar recurso para redução do número de falsos positivos aplicando recursos avançados de aprendizado de máquina para aprender o que é normal e o que não é normal no ambiente monitorado;

6.54.2.67 Deve ter relatórios de ameaças que forneçam visibilidade da postura de segurança cibernética. Por exemplo: usuários de alto risco, ativos de alto risco, principais ameaças, principais IPs maliciosos, etc;

6.54.2.68 Deve ter relatórios que forneçam visibilidade sobre as operações de segurança. Por exemplo, para dispositivos VPN, os relatórios devem incluir as melhores sessões de VPN por duração, os principais eventos de saída de dados, a distribuição dos eventos de login por geografia, as principais tentativas de login com falha e assim por diante;

6.54.2.69 Deve ter relatórios de conformidade alinhados com requisitos de conformidade específicos, como PCI, SOX, HIPPA, GDPR, ISO27002, etc;

6.54.2.70 Deve possuir relatórios de resumo executivo de violações, incidentes e operações;

6.54.2.71 Deve ter relatórios sobre a atividade do usuário;

6.54.2.72 Deve permitir que os dados sejam exibidos com diferentes tipos de gráficos: gráfico de linhas, gráfico de barras, gráfico de pizza, mapa geográfico, tabelas, gráfico empilhados, gráfico N principais, gráficos de bolhas, gráficos de relacionamento de origem e destino;

6.54.2.73 Deve permitir a visualização de dados através de links que permitam vincular qualquer conjunto de atributos e visualização a relação entre eles;

6.54.2.74 O serviço deve possuir solução para análise de artefatos maliciosos que minimamente contemple as funcionalidades a seguir:

6.54.2.74.1 Deve suportar analisar mais de 1000 indicadores comportamentais de um artefato;

6.54.2.74.2 Realizar análise estatística e dinâmica para avaliar se o artefato é malicioso ou não;

6.54.2.74.3 Deve suportar a análise dos artefatos BAT, CHM, DLL, ISO, HTA, HWP, JAR, JS, JSE, JTD, LNK, MSI, MHTML, documentos do Microsoft Office, EXE, PE32, PDF, VBE, URLs, WSF, XML e ZIP;

6.54.3 PROCESSO DE MONITORAMENTO, DETECÇÃO E RESPOSTA

6.54.3.1 A CONTRATADA será responsável por implantar, operar e suportar toda a plataforma ofertada;

6.54.3.2 A fim de balizar todo o processo de monitoramento de ataques cibernéticos do CONTRATANTE, e influenciado pelos principais frameworks de boas práticas de serviços de segurança da informação, foi arquitetado o processo que será descrito nos parágrafos que seguem, o qual obrigatoriamente a CONTRATADA deve seguir ipsis

litteris.

6.54.3.3 É sabido que para o sucesso de um monitoramento de ataques cibernético, a primeira definição se deve a que tipo de ocorrência de eventos de segurança, se deseja detectar e tomar algum tipo de ação, logo será de responsabilidade da CONTRATADA como primeiro passo deste processo, a definição de linha de base de eventos monitorados.

6.54.3.4 Tal definição de linha de base de eventos de segurança monitorados, não deve ser tomada de forma unilateral pela CONTRATADA. O CONTRATANTE deverá participar ativamente no processo de construção de forma consultiva. Porém, se ratifica que é de responsabilidade da CONTRATADA a definição, e colocar em operação tal linha de base.

6.54.3.5 Espera-se que a linha de base de eventos de segurança monitorados, seja revista de forma mensal, contudo, não se limitando a este tempo, pois todos os dias novos ataques são projetados no mundo, e se espera que a CONTRATADA tome ciência destes ataques, e por sua vez atualize a linha de base, para que em um cenário onde estes novos ataques sejam direcionados ao CONTRATANTE, sejam detectados através dos serviços em questão.

6.54.3.6 O produto de um evento é a correlação dos logs gerados pelos itens de configurações do parque do CONTRATANTE. Uma vez definida a linha de base de eventos, será também de responsabilidade da CONTRATADA avaliar se todos os insumos para a correta geração do evento, estão sendo enviados corretamente para a ferramenta.

6.54.3.7 Para correto dimensionamento da quantidade de EPS a serem adquiridos, a CONTRATADA deverá realizar um Survey no ambiente para elencar quais as soluções, aplicações, equipamentos deverão gerar telemetria (insumos) para a Solução de Monitoramento de Logs. Com base nesse survey o CONTRATANTE irá realizar a contratação do Item em questão, evitando assim a aquisição de uma quantidade superior à necessária.

6.54.3.8 Durante a execução do serviço, caso seja identificado pela solução de monitoramento uma quantidade de EPS (Eventos por segundo) superior à contratada, a solução deverá ser ajustada para limitar essa quantidade, evitando assim cobranças indevidas no contrato prestado.

6.54.3.9 Caso a CONTRATADA identifique a ausência dos insumos (eventos) a serem gerados por um item de configuração, será de reponsabilidade da CONTRATADA a correção e/ou habilitação de tal insumo dos itens de configuração. Caso o item de configuração não pertencer ao objeto contratado, porém necessário para a correta geração do evento, deverá a CONTRATADA solicitar ao CONTRATANTE a correção e/ou habilitação de tal insumo no item de configuração em questão.

6.54.3.10 Dar-se-á então o passo de classificação do evento, também de responsabilidade da CONTRATADA. O grupo de monitoramento de ataques da CONTRATADA deve focar as ações nos eventos que são significativos. Logo, tal grupo deve analisar todos os

eventos apresentados, classificando-os nos seguintes grupos, a saber:

6.54.3.10.1 Eventos de Informação: Estes eventos não requerem qualquer ação. São usados para fazer verificação de funcionalidade dos itens de configuração de segurança. Ou seja, tem por objetivo puro e simples, identificar se as ferramentas e soluções estão funcionando dentro do esperado. Estes eventos são também úteis para gerar estatísticas como, por exemplo, porcentagem de hosts com a última vacina de antivírus do dia.

6.54.3.10.2 Eventos de Aviso: Este grupo de eventos deve ser utilizado quando existe algum comportamento anômalo, se comparado a linha de base de operação padrão do ambiente (serviço, trafego e/ou solução), porém, ainda não gerou algum tipo de impacto ao ambiente (serviço, trafego e/ou solução) do CONTRATANTE, como por exemplo fictício: É esperado que exista 1.000 (mil) ataques do tipo portscan bloqueados pelo firewall, porém, na última hora, este número passou para 10.000 (dez mil) ataques, todavia, o firewall ainda continua bloqueando sem que haja degradação da performance do ambiente (serviço, trafego e/ou solução).

6.54.3.10.3 Eventos de Exceção: Estes eventos são aqueles que sugere que os pilares de segurança da informação (confidencialidade, integridade e conformidade), foram impactados como, por exemplo: Uma infecção gerada por um malware do tipo ransomware, onde a mesma não tenha sido bloqueada pela solução de antivírus do CONTRATANTE. Este é o único tipo de evento que pode iniciar o processo de resposta a incidente de segurança, descrito no tópico, do presente termo de referência.

6.54.3.11 Uma vez classificado o evento, se inicia o passo de resposta ao mesmo, que também é de responsabilidade da CONTRATADA. As respostas são baseadas nos grupos de classificação de eventos, a saber:

6.54.3.11.1 Para eventos do tipo informação, não é requerido qualquer tipo de ação, porém, como já mencionado no presente termo de referência, tais eventos são utilizados para verificação do perfeito funcionamento das soluções de segurança. Portanto, a CONTRATADA deverá utilizá-los para tal fim.

6.54.3.11.2 Para eventos do tipo Aviso, a CONTRATADA deverá garantir que uma interface humana, ou seja, uma analista que pertence ao grupo de monitoramento de ataques, esteja validando se tal evento pode se transformar em um evento do tipo exceção, e obviamente tomar as ações cabíveis para identificar a causa raiz da mudança de comportamento do ambiente.

6.54.3.11.3 Para eventos do tipo Exceção, a CONTRATADA deverá transformar tal evento em um incidente de segurança, realizando, portanto, a abertura do mesmo na ferramenta de incidente de segurança da informação definida no PROCESSO DE RESPOSTA A INCIDENTE DE SEGURANÇA DA INFORMAÇÃO, descrito no presente termo de referência. Após a abertura do incidente de segurança, obedecendo os critérios estabelecidos para tal, se encerra a participação do grupo de monitoramento de ataques.

6.54.3.12 Como último passo do processo, a CONTRATADA deve encerrar os eventos após as devidas ações tomadas, conforme definido no parágrafo acima. Eventos podem ter apenas dois tipos de status "aberto" ou "encerrado", ou seja, após o correto tratamento, o evento deverá ter seu status alterado na ferramenta de "aberto" para "encerrado".

6.54.3.13 Importante ressaltar que todo o processo de tratamento do evento, independente de qual fase e/ou status, deve ser registrado no módulo de tratamento de eventos da ferramenta. Também é responsabilidade da CONTRATADA a segurança dos eventos, e fica expressamente proibido a remoção de qualquer evento, independentemente de sua classificação e fase de tratamento.

6.54.4 PROCESSO DE CAÇADA CONTINUA A AMEAÇAS

6.54.4.1 Com o aumento do volume e complexidade das ameaças será exigido que a empresa contratada execute processos manuais de caçada de ameaças (threathunting) no ambiente do CONTRATANTE. A fim de balizar todo o processo de caçada de ameaças, e influenciado pelos principais frameworks de boas práticas de serviços de segurança da informação, foi arquitetado o processo que será descrito nos parágrafos que seguem, o qual obrigatoriamente a CONTRATADA deve seguir ipsis litteris.

6.54.4.2 Uma vez ao dia, inclusive nos finais de semana e feriados, a contratada deverá:

6.54.4.3 Definir uma hipótese e uma declaração de uma possibilidade de ameaça, tal hipótese deve ser elaborada utilizando como referência novos vetores de ameaças e novas tendências baseadas em inteligência de ameaças e fontes de riscos digitais, informações relevantes coletadas por processos de aprendizagem de máquina e inteligência artificial e investigações de táticas, técnicas e procedimentos criando desta forma uma hipótese de como ameaças podem existir dentro do ambiente e de como encontrá-las;

6.54.4.4 Uma vez que a hipótese tenha sido definida a CONTRATADA deverá realizar um plano de coleta dos eventos dentro das plataformas relevantes de acordo com a hipótese definida;

6.54.4.5 Uma vez que os eventos relevantes estejam disponíveis, a CONTRATADA deverá avaliar a massa de eventos para buscar anomalias associadas a hipótese definida;

6.54.4.6 Caso sejam encontrados eventos maliciosos, estes entram no processo de resposta a incidentes de segurança da informação, conforme descrito neste documento;

6.54.4.7 Caso não sejam encontrados eventos maliciosos, o processo de caçada é finalizado, sendo repetido no dia seguinte com uma nova hipótese;

6.54.4.8 Todo processo deve ser documentado através da plataforma de ITMS, incluindo

qual hipótese foi utilizada, quais dados foram analisados e o resultado da análise;

6.54.5 GRUPO TÉCNICO DE MONITORAMENTO DE ATAQUES CIBERNÉTICOS

6.54.5.1 Através do seus 02 (dois) centros de operação de segurança, a CONTRATADA deverá manter uma torre de operação denominada GRUPO DE MONITORAMENTO DE ATAQUES, com objetivo e foco de trabalhar no processo de monitoramento de ataques cibernéticos.

6.54.5.2 Este grupo deverá ser exclusivo para trabalhar no serviço em questão, não podem os profissionais pertencentes a este grupo serem compartilhados e/ou atuarem, com os demais serviços descritos no objeto do presente termo de referência.

6.54.5.3 Deverá ser de responsabilidade da CONTRATADA dimensionar o número de profissionais adequado para entrega de tal serviço, sem que haja impacto no acordo de nível de serviço estabelecido no tópico ACORDO DE NÍVEIS DE SERVIÇO do presente termo de referência.

6.54.5.4 A fim de garantir que os profissionais envolvidos tenham conhecimento e habilidade para executar o processo de monitoramento de ataques cibernéticos do CONTRATANTE, a CONTRATADA deverá, obrigatoriamente, compor o GRUPO DE MONITORAMENTO DE ATAQUES, com ao menos 01 (um) perfil de cada profissional que segue descrito abaixo:

TABELA 1 - CERTIFICAÇÕES E QUALIFICAÇÕES DO (GRUPO DE MONITORAMENTO DE ATAQUES)

Perfis	Certificações	Descrição
Analista de Segurança I	ISFS (Information Security Foundation)	Conhecimento avançado em segurança da informação, com experiência em monitoramento de ataques cibernéticos utilizando ferramentas e soluções de SIEM e ATD. Experiência comprovada de no mínimo 12 (doze) meses em segurança da informação.
Analista de Segurança II	Certified Ethical Hacker ou CompTIA Security+ ou CompTIA CySA+	Conhecimento avançado em segurança da informação, com experiência em monitoramento de ataques cibernéticos utilizando ferramentas e soluções de SIEM e ATD. Experiência comprovada de no mínimo 12 (doze) meses em segurança da informação.

6.54.5.5 Não existe restrição ou limite para acúmulo de perfis em um mesmo profissional, uma vez que é de responsabilidade da CONTRATADA definir o quantitativo de profissionais envolvidos no GRUPO DE MONITORAMENTO DE ATAQUES, porém,

conforme já foi mencionado neste termo de referência, este(s) deve(m) compor única e exclusivamente o time denominado GRUPO DE MONITORAMENTO DE ATAQUES.

6.54.5.6 No momento da assinatura do contrato, será exigido da CONTRATADA, as seguintes documentações do(s) profissionais que participarão do GRUPO DE MONITORAMENTO DE ATAQUES, os quais devem comprovar as exigências e obrigações descritas neste termo de referência: carteira de trabalho devidamente assinada pela CONTRATADA, curriculum vitae para comprovação de habilidades, e as devidas certificações técnicas para comprovação do conhecimento exigido no item.

6.54.6 ENTREGAS A SEREM REALIZADAS

6.54.6.1 Para acompanhamento e avaliação do serviço a ser ofertado pela CONTRATADA, o CONTRATANTE definiu os seguintes indicadores chave de desempenho, que reunidos vão compor um único relatório a ser entregue de forma online e em tempo de execução, através do portal de segurança descrito no tópico de condições gerais para prestação do serviço deste termo de referência, a saber:

TABELA 2 - INDICADORES ESTRATÉGICOS DE MONITORAMENTO DE ATAQUES CIBERNÉTICOS

DENOMINAÇÃO	FORMA DE CÁLCULO	FILTRO	AGRUPADOR	DESCRIÇÃO
Quantitativo de eventos correlacionados	Soma de eventos correlacionados	Eventos correlacionados	Eventos correlacionados	Número total de eventos correlacionados
Quantitativo de incidentes abertos	Soma de incidentes abertos	Incidentes abertos	Incidentes	Número total de incidentes abertos
Quantitativo de solicitações por grupo de tecnologia	Soma de solicitações relacionadas aos grupos de tecnologia	Solicitações relacionadas aos grupos de tecnologia	Solicitações	Número total de solicitações relacionadas por grupo de tecnologia
Quantitativo de regras de correlacionamento	Soma do número de regras de correlacionamento	Regras de correlacionamento	Regras de correlacionamento	Número total de regras de correlacionamento
TOP 10 – Regras de correlacionamento	Soma do número de eventos correlacionados por regra de correlacionamento	Eventos correlacionados	Regra de correlacionamento	TOP 10 do número de eventos correlacionados por regra de correlacionamento
TOP 10 – IP de destino de regras de correlacionamento	Soma do número de eventos correlacionados por IP de destino	Eventos correlacionados por IP de destino	IP de destino	TOP do número de eventos correlacionados por IP de destino
TOP 10 – Regras de correlacionamento por país de origem	Soma do número de eventos correlacionados por país de origem	Eventos correlacionados por país de origem	País de origem	TOP do número de eventos correlacionados por país de origem

TOP 10 – Tipos de ataques	Soma do número de ataques correlacionados por tipo de ataque	Eventos correlacionados por ataque	Ataques	TOP 10 por tipo de ataque

6.54.6.2 Tais relatórios e indicadores devem ser apresentados e discutidos em reunião mensal, com a presença de profissional que conheça todos os serviços prestados, e com uma das seguintes certificações: CISSP (Certified Information Systems Security Professional), CISM (Certified Information Security Manager, CIA (Certified Intrusion Analyst), GSEC (GIAC Security Essentials), GCIH (GIAC Incident Handler), COMPTIA SECURITY+ OU COMPTIA CYSA+.

6.54.6.3 Neste contexto, o profissional deve apresentá-lo de forma presencial nas dependências do CONTRATANTE, ou de forma virtual, por meio de solução de videoconferência.

6.55 SOLUÇÃO PARA TESTES DE PENETRAÇÃO EM ACORDO COM O GUIA OWASP

6.55.1 A solução deverá ser capaz de fazer integração com outras ferramentas para replicar detecções de ransomware para que seja possível isolar o ataque, criptografar para gerar um mapa de ataques de ransomware.

6.55.2 A solução deve ser capaz de simular ou emular ransomwares para testar em ambiente Windows.

6.55.3 A ferramenta deverá ser capaz de rodar um escopo de teste em intervalos de endereços IPs e deve permitir a exclusão de um único host ou qualquer serviço dentro do host.

6.55.4 O teste de penetração deve permitir ser parado a qualquer momento para que não ocorra um impacto na infraesrtutura computacional.

6.55.5 O teste de penetração deve possuir níveis diferenciados, com no mínimo 3 níveis de varreduras.

6.55.6 A solução deve ser capaz de realizar varreduras de vulnerabilidades classificadas como críticas para uma ação rápida de resolução.

6.55.7 A solução deve possuir formas de teste direcionado, teste de ação única para uma report rápido sobre determinado host ou serviço.

6.55.8 A ferramenta deve possuir uma função de higienização automática para limpar qualquer resíduo do teste executado.

6.55.9 A solução deve possuir um escopo específico para o Active directory para identificar vulnerabilidades em tempo real, referente a usuários, grupos e contas administrativas.

6.55.10 A ferramenta deve ter a cobertura mínima do OWASP top 10, incluindo JAVA/ASP

e RCE.

6.55.11 A solução deve possuir uma forma de validação por um gestor ou usuário específico, para dar maior visibilidade e transparência no processo de ataque.

6.55.12 A solução deverá ser capaz de identificar uma vulnerabilidade em um escopo de teste e versionar as atualizações para executar um processo completo de controle de qualidade.

6.55.13 A solução deve possuir a funcionalidade de interceptar comunicações entre duas partes e retransmitir os dados para outro dispositivo (de terceiros), incluindo técnicas baseadas em rede MITM.

6.55.14 A solução deve possuir algumas medidas para recuperar senhas em texto simples de usuários, hosts e servidores, quebrando hashes de senhas de dados armazenados ou transportados de um sistema usando uma das seguintes combinações de técnicas de força bruta e dicionário:

6.55.14.1 Uso de senha padrão do fabricante em dispositivos periféricos

6.55.14.2 Validar a existência de senhas fracas

6.55.14.3 Verifique a robustez das senhas mais complexas e teste se elas estão de acordo com a política corporativa

6.55.14.4 Use recursos de cracking baseados em hardware para detectar falhas no ecossistema Kerberos

6.55.14.5 Teste a força da senha de contas privilegiadas em endpoints não gerenciados

6.55.14.6 Aproveite o poder de computação de GPU especializado para técnicas de cracking de alto desempenho

6.55.14.7 Dicionário de senhas onde o sistema aplicará automaticamente as transformações

6.55.14.8 Crie um dicionário personalizado de senhas para caçar

6.56 SOLUÇÃO DE COMPLIANCE E ANTI-FRAUDE EM AMBIENTES DE INTELIGÊNCIA ARTIFICIAL

6.56.1 A solução deverá estar preparada para operar em ambiente híbrido (local, nuvem ou ambos) e multicloud sem necessidade de novas implementações.

6.56.2 A solução deve oferecer segurança refinada baseada em funções, incluindo autenticação de dois fatores, e suporta protocolos Kerberos e LDAP.

6.56.3 54Deve ser possível a instalação da solução em ambiente de containers (docker),

independente de distribuição.

6.56.4 Deve ser possível a instalação da solução em ambiente de cluster Hadoop, independente de distribuição.

6.56.5 Suporte mínimo aos seguintes sistemas operacionais: Windows 10, Windows Server 2016 e superiores; Red Hat Enterprise Linux 7.9 e superiores; SUSE Linux Enterprise Server 12 Service Pack 5 e superiores;.

6.56.6 Suporte mínimo aos seguintes navegadores: Firefox ESR a partir da versão 60, Google Chrome a partir da versão 87 e Microsoft Edge.

6.56.7 Deverá ser possível instalar a solução em servidores virtuais utilizando VMware vSphere/ESXi 6.7 e superiores.

6.56.8 A solução deverá ser compatível com pelo menos um dos seguintes servidores de aplicação: Oracle Weblogic Server 12.2.1.4 e superiores;

6.56.9 IBM WebSphere Liberty 20 e superiores.

6.56.10 A solução deve dar suporte para todos os tipos de problemas de negócios. Deverá analisar seu conjunto de dados de treinamento e recomendar automaticamente o tipo ideal de modelo a ser utitilizado, podendo ser de regressão, classificação ou série temporal.

6.56.11 A solução deverá ter suporte aos algoritmos inovadores de código aberto utilizando no mínimo as bibliotecas de aprendizado de máquina de código aberto:

6.56.11.1 R

6.56.11.2 Python

6.56.11.3 scikit-learn

6.56.11.4 H2O

6.56.11.5 TensorFlow

6.56.11.6 Vowpal Wabbit

6.56.11.7 Spark ML

6.56.11.8 XGBoost.

6.56.12 A solução deve preparar os dados automaticamente, realizando operações como codificação one-hot, imputação de valor ausente, mineração de texto e padronização para transformar recursos para obter resultados ideais.

6.56.13 A solução deve permitir a classificação em alvos com até 100 valores distintos, oferecendo suporte em tempo real e em lote para descobrir a classe preditiva e mostrar sua

probabilidade em todas as classes.

6.56.14 A solução deve ter nativamente técnicas técnicas de ciências de dados avançadas, contendo no mínios as seguintes:

6.56.14.1 Boosting

6.56.14.2 Bagging

6.56.14.3 Random Forest

6.56.14.4 Métodos baseados em kernel

6.56.14.5 Modelos lineares generalizados

6.56.14.6 Deep learning

6.56.15 A solução além de fornecer uma forma automatizada, deverá também oferece suporte ao ajuste manual para que o administrador possa ajustar os algoritmos de aprendizado de máquina para obter resultados em conformidade com alguns pontos da empresa.

6.56.16 A solução deve ser capaz de aplicar uma relação direcional forçada entre os recursos e o destino com base no conhecimento do negócio ou nos requisitos do setor.

6.56.17 A solução deve possuir um portal central e re-treine e substitua modelos para garantir que eles permaneçam precisos e consistentes em todas as condições de mercado em constante mudança.

6.56.18 A solução deve fornecer uma visão do uso da plataforma em toda a organização, incluindo quais usuários e modelos estão consumindo tempo de execução para permitir um planejamento de recursos eficaz.

6.56.19 A solução deve ter tabelas de classificação personalizáveis que permita que os administradores editem e manipulem os coeficientes do modelo de acordo com suas regras de negócios exclusivas, permitindo uma combinação ideal de aprendizado de máquina e experiência humana.

6.57 A QUALIFICAÇÃO TÉCNICA SERÁ COMPROVADA MEDIANTE A APRESENTAÇÃO DOS SEGUINTES DOCUMENTOS

6.57.1 A licitante vencedora deverá apresentar, no ato da assinatura do contrato, no mínimo as certificações abaixo:

6.57.1.1 01 ou mais consultores com as Certificações de DPO emitidas por Certificadoras Nacionais ou Internacionais, descritas nos itens tais certificados podem ser acumulativos por profissionais, sendo que deverá comprovar vínculo com a empresa vencedora através de CLT ou contrato de prestação de serviços. No caso de contrato de prestação de serviços o mesmo deverá constar que o(s) referido(s) profissional (is)

são contratado(s) durante a vigência do contrato, e em caso de substituição durante a vigência contratual, a Licitante Vencedora deverá comunicar em até 30 (trinta dias) a substituição do(s) profissional (ais).

6.57.1.2 Privacy and Data Protection Foundation;

6.57.1.3 Data Protection Officer;

6.57.1.4 Ethical Hacking Essentials Certificate;

6.57.1.5 Computer Forensics Foundation Certificate;

6.57.1.6 Information Security Foundation - ISO/IEC 27001;

6.57.1.7 Information Security Foundation - ISO/IEC 27002;

6.57.1.8 Information Security Specialist;

6.57.1.9 Information Security Policy Foundation;

6.57.1.10 Vulnerability Management Foundation Certificate.

6.57.1.11 CompTIA Security+

6.57.2 Atestado emitido em seu nome de que presta ou prestou serviços de assessoria jurídica para implantação de LGPD e deverá comprovar que os profissional (is) prestador(es) dos serviço(s) tenham habilitação para o exercício das atividades (OAB), conforme previsto na regulamentação da referida atividade profissional.

6.58 TRANSFERÊNCIA DE CONHECIMENTO DE INSTALAÇÃO, CONFIGURAÇÃO E OPERACIONALIZAÇÃO DA SOLUÇÃO

6.58.1 A CONTRATADA deverá oferecer treinamento do fabricante para a equipe de TI da CONTRATANTE englobando, no mínimo, as atividades de instalação, implementação, configuração, monitoramento, diagnóstico de problemas e desempenho da solução;

6.58.2 O treinamento deverá ser composto de parte teórica e parte prática (hands on) e apresentar conteúdo suficiente para que os profissionais designados pela CONTRATANTE sejam capacitados a realizar todas as atividades de instalação, implementação, monitoramento e suporte à solução;

6.58.3 O treinamento deverá ser realizado nas dependências da CONTRATANTE ou através de EAD (Ensino a Distância) com aulas ao vivo, desde que mantenha inalterados o cronograma e conteúdo do treinamento presencial;

6.58.4 Todas as despesas relativas ao treinamento, tais como: contratação, transporte, estadia e alimentação dos instrutores, material, bem como quaisquer outras inerentes à

capacitação contratada, são de exclusiva responsabilidade da CONTRATADA;

6.59 TRANSFERÊNCIA DE CONHECIMENTO DE ADMINITRAÇÃO E USO DA SOLUÇÃO.

6.59.1 A CONTRATADA deverá oferecer treinamento do fabricante para a equipe responsável pela administração e uso da solução, englobando, no mínimo, as atividades de implementação, administração e utilização de todos os módulos da solução;

6.59.2 O treinamento deverá ser composto de parte teórica e parte prática (hands on) e apresentar conteúdo suficiente para que os profissionais designados pela CONTRATANTE sejam capacitados a realizar todas as atividades de administração, implementação e uso pleno da solução;

6.59.3 O treinamento deverá ser realizado nas dependências da CONTRATANTE ou através de EAD (Ensino a Distância) com aulas ao vivo, desde que mantenha inalterados o cronograma e conteúdo do treinamento presencial;

6.59.4 Todas as despesas relativas ao treinamento, tais como: contratação, transporte, estadia e alimentação dos instrutores, material, bem como quaisquer outras inerentes à capacitação contratada, são de exclusiva responsabilidade da CONTRATADA.

6.60 SERVIÇOS DE SUSTENTAÇÃO DA CENTRAL

6.60.1 A sustentação técnica da contratada deve ser composta por profissionais especializados e certificados em todas as disciplinas que permeiam o espectro da solução seja ele técnico, legislativo ou jurídico.

6.60.2 A sustentação técnica da contratada deve possuir metodologia prática, acessível e inovadora, com foco em mitigação dos maiores riscos.

6.60.3 A sustentação técnica da contratada deverá ser multidisciplinar, possuir um suporte técnico altamente especializado para suportar todas as funcionalidades da solução adotada e para temas relacionados a processos de negócios e quiçá apoio jurídico (será considerado um diferencial).

6.60.4 Atividades que deverão ser consideradas:

6.60.4.1 A sustentação técnica da contratada deverá prestar suporte especializado N1, N2 e N3 para todas falhas e dúvidas relativas à solução ofertada para suportar a implantação da conformidade no contratante.

6.60.4.2 A sustentação técnica da contratada deverá executar monitoramento diário das principais funcionalidades e eventuais componentes externos da solução ofertada para implantar a conformidade as Normas de Privacidade no contratante.

6.60.4.3 A sustentação técnica da contratada deverá ser responsável pelo monitoramento

diário da disponibilidade da solução ofertada para implantar a conformidade as Normas de Privacidade no contratante.

6.60.4.4 A sustentação técnica da contratada deverá executar atividades recorrentes para manutenção da operacionalidade da solução sistêmica a fim de validar se todos os módulos estão disponíveis e funcionando adequadamente.

6.60.4.5 A sustentação técnica da contratada deverá enviar regularmente ao contratante materiais específicos relacionados as Normas de Privacidade a fim de reforçar a cultura de proteção de dados dos colaboradores do contratante.

6.60.4.6 A sustentação técnica da contratada deverá apoiar o contratante na execução de testes no Portal no Portal do Titular a fim de evitar falhas que impeçam o atingimento dos SLAs definidos pela ANPD.

6.60.4.7 A sustentação técnica da contratada deverá apoiar a equipe de TI do contratante respondendo dúvidas técnicas sobre a solução ofertada.

6.60.4.8 A sustentação técnica da contratada deverá apoiar o contratante no cadastro de planos de ação e as suas respectivas ações de adequação dentro da solução tecnológica ofertada.

6.60.4.9 A sustentação técnica da contratada deverá apoiar o contratante na execução de testes de operacionais de toda a solução tecnológica adotada e principalmente no portal do titular e na gestão de incidentes de segurança que deve ser um componente obrigatório na solução tecnológica ofertada.

6.60.4.10 A sustentação técnica da contratada deverá apoiar a execução de treinamentos curtos em todos os módulos da solução tecnológica adota e deve no mínimo ter as seguintes funcionalidades e componentes

6.60.4.11 Inventário de Dados/ROPA, DPIA/Relatórios de Impacto, Data Mapping/Data Discovery, Gestão de cookies, Gestão de Planos de Ação, Gestão de Políticas, Gestão de Consentimentos, Portal de Titular, Gestão de Incidentes, Gestão de Terceiros, Gestão da Capacitação, "Privacy by Design and Privacy by Default", Framework de Conformidade, Indicadores de 400 pontos, Maturidade de TI, Auditoria e Monitoramento de Tratamento de Dados não estruturados.

6.60.4.12 A sustentação técnica da contratada deverá apoiar ao contratante o processamento de atividades automatizadas no atendimento às solicitações dos titulares de dados.

6.60.4.13 A sustentação técnica da contratada deverá sempre que solicitado deverá ser capaz de personalizar as notificações e comunicações do Portal do Titular com os titulares.

6.60.4.14 A sustentação técnica da contratada deverá sempre que solicitada participar de reuniões técnicas relativas à solução tecnológica oferta;

6.60.4.15 A sustentação técnica da contratada deverá apoiar o contratante na descoberta de dados pessoais e sensíveis nas bases de dados estruturados e não estruturados sempre que houver mudança na estrutura das bases de dados ou repositórios;

6.60.4.16 A sustentação técnica da contratada deverá apoiar o contratante na execução de auditoria nos diversos repositórios (CRUD) do ambiente tecnológico do contratante a fim de se obter dados pessoais e sensíveis do titular.

6.60.5 A CONTRATADA deverá oferecer pacote de serviços de operação assistida da solução para as atividades de administração, implementação e uso da solução, para ser utilizado pela CONTRATANTE, sob demanda, após a etapa de implantação inicial da solução;

6.60.6 Os serviços de operação assistida deverão ser prestados remotamente ou presencialmente nas dependências da CONTRATANTE, por profissional devidamente qualificado e certificado na solução;

6.60.7 Todas as despesas relativas aos serviços de operação assistida, tais como: transporte, estadia, alimentação e materiais, bem como quaisquer outras inerentes aos serviços de operação assistida, são de exclusiva responsabilidade da CONTRATADA.

6.61 SERVIÇOS DE MONITORAMENTO E SUPORTE À PRIVACIDADE

6.61.1 O Serviço de Monitoramento e Suporte à Privacidade especializado da contratada deverá apoiar o contratante no atendimento aos titulares dos dados pessoais para dúvidas, solicitações.

6.61.2 O Serviço de Monitoramento e Suporte à Privacidade especializado da contratada deverá apoiar o contratante na condução das respostas a eventuais incidentes de segurança ocorridos no controlador.

6.61.3 O Serviço de Monitoramento e Suporte à Privacidade especializado da contratada deverá apoiar o contratante na adequação na conformidade de Privacidade na organização.

6.61.4 O Serviço de Monitoramento e Suporte à Privacidade especializado da contratada deverá apoiar o contratante na criação e manutenção dos controles de gestão complementares para gerir as ações e planos de Privacidade.

6.61.5 O Serviço de Monitoramento e Suporte à Privacidade especializado da contratada deverá apoiar o contratante na criação de uma fonte de conhecimento, políticas normativas vigentes atualizadas e disponíveis para quem couber o acesso.

6.61.6 O Serviço de Monitoramento e Suporte à Privacidade especializado da contratada deverá apoiar o contratante na definição e organização da melhor estrutura de bases de conhecimento, categorias e artigos de conhecimento na solução tecnológica fornecida.

6.61.7 O Serviço de Monitoramento e Suporte à Privacidade especializado da contratada deverá apoiar o contratante na divulgação e difundir conhecimento sobre as políticas e normas da

organização relacionadas as Normas de Privacidade.

6.61.8 O Serviço de Monitoramento e Suporte à Privacidade especializado da contratada deverá apoiar o contratante na governança das evidências sobre ações de capacitação e conscientização de colaboradores da organização sobre as Normas de Privacidade e seus conceitos, políticas e procedimentos.

6.61.9 O Serviço de Monitoramento e Suporte à Privacidade especializado da contratada deverá apoiar o contratante na manutenção de ações consistentes e continuadas de capacitação e conscientização de seus colaboradores sobre as Normas de Privacidade e seus conceitos, políticas e procedimentos.

6.61.10 O Serviço de Monitoramento e Suporte à Privacidade especializado da contratada deverá apoiar o contratante para que todos os sites da organização possuam gestão de cookies que são utilizados durante a navegação de usuários nos sites da organização.

6.61.11 O Serviço de Monitoramento e Suporte à Privacidade especializado da contratada deverá apoiar o contratante nas atualizações de configuração de gestão de cookies no site da organização.

6.61.12 O Serviço de Monitoramento e Suporte à Privacidade especializado da contratada deverá apoiar o contratante na análise dos relatórios de impacto, riscos, conformidade de processos e ações.

6.61.13 O Serviço de Monitoramento e Suporte à Privacidade especializado da contratada deverá apoiar o contratante na geração do relatório de impacto, riscos e planos de ação para que estejam documentados e disponíveis para consulta do Jurídico.

6.61.14 O Serviço de Monitoramento e Suporte à Privacidade especializado da contratada deverá apoiar o contratante na compreensão de forma analítica o resultado do framework de conformidade e apoiar no direcionamento das ações de adequação.

6.61.15 O Serviço de Monitoramento e Suporte à Privacidade especializado da contratada deverá apoiar o contratante na definição de estratégias de atualização do inventário de dados e conformidade de processos.

6.61.16 O Serviço de Monitoramento e Suporte à Privacidade especializado da contratada deverá apoiar o contratante na criação de conteúdo e material orientativo e educacional relacionado as Normas de Privacidade e disponibilizar para conhecimento da organização.

6.61.17 O Serviço de Monitoramento e Suporte à Privacidade especializado da contratada deverá apoiar o contratante na manutenção do indicador de conscientização atualizado nos Indicadores de Adequação.

6.61.18 O Serviço de Monitoramento e Suporte à Privacidade especializado da contratada deverá apoiar o contratante na elaboração de notas técnicas ou pareceres relacionados a aprovação ou não de alterações ou criação de novos serviços, produtos ou processos da organização.

6.61.19 O Serviço de Monitoramento e Suporte à Privacidade especializado da contratada deverá apoiar o contratante na execução do planejamento dos planos de ação identificados durante o projeto.

6.61.20 O Serviço de Monitoramento e Suporte à Privacidade especializado da contratada deverá apoiar o contratante na monitoração e na execução dos planos de ação e suas ações de adequação.

6.61.21 O Serviço de Monitoramento e Suporte à Privacidade especializado da contratada deverá apoiar o contratante na definição de fluxos de trabalho interno, visando o atendimento das solicitações dos titulares de dados.

6.61.22 O Serviço de Monitoramento e Suporte à Privacidade especializado da contratada deverá apoiar o contratante na implementação do "privace by design and privacy by default" em novos processos.

6.61.23 O Serviço de Monitoramento e Suporte à Privacidade especializado da contratada deverá apoiar o contratante na avaliação de alterações ou criação de novos serviços, produtos ou processos na organização, para que estes passem pela validação de assuntos relacionados à privacidade de dados.

6.61.24 O Serviço de Monitoramento e Suporte à Privacidade especializado da contratada deverá apoiar o contratante no controle dos prazos determinados pela ANPD desde que devidamente registrado em nosso portal.

6.61.25 O Serviço de Monitoramento e Suporte à Privacidade especializado da contratada deverá apoiar o contratante na interpretação da Lei através dos nossos especialistas e parceiros jurídicos.

6.61.26 O Serviço de Monitoramento e Suporte à Privacidade especializado da contratada Serviço de sustentação da contratada a deverá apoiar o contratante na elaboração de análise de impactos sobre proteção de dados.

6.61.27 O Serviço de Monitoramento e Suporte à Privacidade especializado da contratada deverá apoiar o contratante na orientação para adequação das políticas de privacidade..

6.61.28 O Serviço de Monitoramento e Suporte à Privacidade especializado da contratada deverá apoiar o contratante na revisão de contrato com fornecedores e prestadores afim de se adequarem as Normas de Privacidade.

6.61.29 O Serviço de Monitoramento e Suporte à Privacidade especializado da contratada deverá apoiar o contratante na revisão de formulários, políticas, e divulgação do Controlador.

6.61.30 O Serviço de Monitoramento e Suporte à Privacidade especializado da contratada deverá apoiar o contratante na manutenção do inventário de dados para coleta de informações do processo de negócio e análise jurídica.

6.61.31 O Serviço de Monitoramento e Suporte à Privacidade especializado da contratada deverá apoiar o contratante na verificação proativa das políticas e termos nos sites do controlador indicando ao controlador eventuais divergências.

6.62 SERVIÇOS DE CUSTOMIZAÇÃO E DESENVOLVIMENTO DE INTEGRAÇÕES COM OS SISTEMAS DA CONTRATANTE

6.62.1 Esse item engloba serviços contratados sob demanda:

6.62.1.1 Serviços de customização da solução para atender a necessidades específicas da Contratante;

6.62.1.2 Serviços de desenvolvimento de integrações de módulos da solução com os sistemas da contratante;

6.62.1.3 A execução dos serviços ocorrerá mediante solicitação da contratante. A partir da solicitação, a contratada deverá apresentar planejamento da atividade e a quantidade de USTs necessárias à execução da atividade;

6.62.1.4 A execução dos serviços ocorrerá somente após a avaliação e aprovação da contratante.

6.63 SERVIÇOS DE AVALIAÇÃO DOS PROCESSOS DE NEGÓCIO QUE TRATAM DADOS PESSOAIS

6.63.1 Os serviços descritos nesse item serão prestados com base no volume de processos de negócio, conforme previsto na neste termo de referência.

6.63.2 Realizar a avaliação dos processos de negócio para identificação da finalidade e definição da base legal para o tratamento de dados pessoais. A atividade inclui a coleta de informações, entrevistas junto às áreas de negócio e demais etapas necessárias, de forma a realizar a avaliação completa dos processos que tratam dados pessoais;

6.63.3 Quando aplicável, realizar a avaliação da aplicação da base legal do legítimo interesse (LIA), gerando a documentação para comprovação junto à ANPD;

6.63.4 Quando aplicável, elaborar o relatório de impacto de proteção de dados pessoais (RIPD/DPIA), gerando a documentação necessária para comprovação junto à ANPD;

6.63.5 Avaliação de riscos e necessidades de adequação dos processos de negócio que tratam dados pessoais, gerando as informações necessárias para inclusão na plataforma de gestão;

6.63.6 Elaboração da documentação pertinente às atividades realizadas.

6.64 SERVIÇOS DE REVISÃO DOS PROCESSOS DE NEGÓCIO QUE TRATAM DADOS PESSOAIS E/OU SENSÍVEIS.

6.64.1 Os serviços previstos nesse item destinam-se à revisão das atividades de avaliação dos processos de negócio que tratam dados pessoais, já realizadas pela CONTRATANTE.

6.64.2 Realizar a revisão das finalidades e bases legais para o tratamento de dados pessoais definidas pela contratante. A atividade será realizada através da documentação e entrevistas com a equipe da contratante responsável por sua elaboração, de forma a complementar com informações necessárias à inclusão na plataforma;

6.64.3 Quando aplicável, revisar a avaliação da aplicação da base legal do legítimo interesse (LIA), bem como a documentação gerada pela CONTRATANTE;

6.64.4 Quando aplicável, revisar o relatório de impacto de proteção de dados pessoais (RIPD/DPIA), bem como a documentação gerada pela CONTRATANTE;

6.64.5 Avaliação de riscos e necessidades de adequação dos processos de negócio que tratam dados pessoais, gerando as informações necessárias para inclusão na plataforma de gestão;

6.64.6 Elaboração da documentação pertinente às atividades realizadas.

6.65 REQUISITOS DO MÓDULO DE CONSCIENTIZAÇÃO

6.65.1 O módulo de treinamento online deve fornecer treinamentos em proteção de dados pessoais e segurança cibernética, além de conceitos de segurança da informação para os colaboradores da organização. O treinamento deverá ser disponibilizado em EAD;

6.65.2 Deve possuir recurso elaborar e gerir planos de treinamento, incluindo a geração de relatórios;

6.65.3 A solução deve possuir a capacidade de mensurar o desempenho dos colaboradores nos treinamentos realizados através de avaliações nos próprios módulos de treinamento (vídeo aulas, testes, etc.) e coletar o desempenho de cada treinando por curso.

6.66 PLANEJAMENTO E GERÊNCIA DOS SERVIÇOS CONTRATADOS

6.66.1 Definir em conjunto com o CONTRATANTE a metodologia formal de trabalho, a gestão e o cronograma que serão adotados durante o desenvolvimento dos trabalhos, de forma a atender o prazo necessário para a conformidade com as Normas de Privacidade;

6.66.2 Definir o plano de comunicação e divulgação do projeto, incluindo o engajamento inicial de todas as áreas do CONTRATANTE .

6.66.3 Realizar a gestão do projeto, apresentando e acompanhando os indicadores de gestão dos serviços sob a responsabilidade do CONTRATADO.

6.66.4 Elaborar e implementar planos de ação para correção de desvios.

6.66.5 Documentar todo e qualquer plano de ação, procedimento ou conhecimento estruturado necessário para a execução dos serviços.

6.66.6 Todas as atividades que envolvam usuários e profissionais do CONTRATANTE deverão ser realizadas em língua portuguesa, incluindo todos os níveis de atendimento, material fornecido, sites e conteúdos disponibilizados, mensagens, entre outros.

6.66.7 Profissionais do CONTRATANTE acompanharão as atividades desenvolvidas a fim de absorver a transferência dos conhecimentos gerados pela CONTRATADA.

6.66.8 As reuniões de trabalho deverão ocorrer por videoconferência ou audioconferência.

6.66.9 O CONTRATADO deverá designar um representante para o gerenciamento do CONTRATO durante sua vigência.

6.66.10 O CONTRATADO deverá designar um representante para o gerenciamento do projeto;

6.66.11 O CONTRATANTE deverá prover aos profissionais designados os recursos necessários à execução das atividades.

6.66.12 A CONTRATADA deverá identificar a necessidade de capacitação dos profissionais do CONTRATANTE das áreas de Governança, Riscos e Compliance (GRC) e de TI (GTSI), propondo cursos e certificações para o desempenho adequado de suas funções, com vistas às Normas de Privacidade.

6.66.13 Entrega: ao término da etapa, disponibilizar o plano de trabalho detalhado, o plano de comunicação com o cronograma das atividades e a atribuição dos responsáveis.

6.66.14 Entrega: ao término da etapa, disponibilizar a descrição da metodologia, a descrição dos procedimentos, os locais de armazenamento dos documentos gerados e os modelos de documentos que serão utilizados para evidenciar e formalizar a execução de todas as atividades descritas nos itens anteriores.

6.66.15 As entregas deverão ser disponibilizadas até a conclusão de cada etapa de trabalho.

6.67 SERVIÇOS DE ATENDIMENTO TÉCNICO

6.67.1 A CONTRATADA deverá prover atendimento técnico à Solução no regime de 8 horas x por 5 dias, das 8h - 18h, da solução para a CONTRATANTE . O atendimento deverá incluir resposta a chamados críticos e permitir a comunicação por meio de e-mail, chat e telefone (devendo a CONTRATADA fornecer um número telefônico para chamada local ou gratuita). No momento do aceite de cada ordem de serviço, a CONTRATADA deverá comprovar estar em operação descrita neste item.

6.67.2 Os serviços de atendimento técnico compreendem todos os chamadas relativas a um

serviço previamente planejado e executado pela CONTRATADA, bem como todos os chamados que objetivem esclarecer dúvidas na utilização dos serviços prestados diretamente pelo provedor, independentemente de esses serviços terem sido provisionados pela CONTRATADA ou pela CONTRATANTE .

6.67.3 Os serviços de atendimento técnico deverão ser prestados pela CONTRATADA sem qualquer ônus adicional para a CONTRATANTE.

6.67.4 Os atendimento técnico serão classificados por severidade, de acordo com o impacto no ambiente computacional da CONTRATANTE . Os possíveis níveis de severidade são:

6.67.5 Severidade 1 – A solução em produção está parado ou fora de funcionamento e não há meios de contornar a falha. Número significativo de usuários foi afetado ou impacto operacional significativo foi causado.

6.67.6 Severidade 2 - A solução em produção está apresentando falhas de funcionamento, sem causar interrupção do serviço, mas afetando significativamente seu desempenho. Impacto crítico aos usuários.

6.67.7 Para fins de verificação do atendimento, os chamados serão agrupados por nível de severidade e seus prazos de atendimento serão contabilizados mensalmente, conforme tabela de Nível de Serviço.

Tabela de Nível de Serviço – Prazo para atendimento dos serviços de suporte técnico.

Tabela de níveis de serviços - Tabela 3

Descrição do Nível de Serviço	Tempo máximo para início do atendimento	Prazo máximo (em horas úteis) para solução. Horário comercial (das 8h as 18h)
Chamados com severidade 1	2 horas úteis	4 horas úteis
Chamados com severidade 2	4 horas úteis	8 horas úteis

6.67.8 A CONTRATADA não será responsabilizada pelo prazo máximo estabelecido na Tabela de Nível de Serviço, quando o chamado for originado por falha, interrupção ou qualquer outra ocorrência nos serviços de telecomunicações ou energia elétrica que atendem à infraestrutura interna da CONTRATANTE ; indisponibilidade de dados, inconsistência de dados e informações geradas pela CONTRATANTE , não se caracterizando, nesses casos, a indisponibilidade dos serviços ou inadimplemento da CONTRATADA.

6.67.9 Toda e qualquer intervenção no ambiente produtivo resultante de serviços de atendimento técnico deve ser executada somente mediante prévia autorização da CONTRATANTE , a partir de informações claras dos procedimentos que serão adotados/executados pela CONTRATADA.

6.67.10 No final do atendimento e resolução da ocorrência, o técnico da CONTRATADA realizará, em conjunto com representantes da CONTRATANTE , testes para verificação dos resultados obtidos, certificando-se do restabelecimento à normalidade e/ou resolução do problema.

6.67.11 Ao término dos testes e do atendimento (fechamento do chamado), a CONTRATADA deverá registrar, detalhadamente, por e-mail, as causas do problema e a resolução adotada.

6.67.12 Nos casos em que o atendimento não se mostrar satisfatório, a CONTRATANTE fará reabertura do chamado, mantendo-se as condições e prazos do primeiro chamado.

6.67.13 O atendimento técnico poderá ser atendido em três níveis, sendo:

6.67.13.1 Primeiro nível: Atendimento pela plataforma da CONTRATADA, em portal web na internet, ou através de e-mail ou contato telefônico, onde a CONTRATADA orientará o funcionário da CONTRATANTE na solução do problema;

6.67.13.2 Segundo nível: Atendimento remoto por parte da CONTRATADA com acompanhamento de funcionário da CONTRATANTE ;

6.67.13.3 Terceiro nível: Atendimento presencial por parte da CONTRATADA com acompanhamento de funcionário da CONTRATANTE .

6.67.14 O serviço de atendimento técnico deverá ser disponibilizado pela CONTRATADA durante 08 (oito) horas por dia, 5 (cinco) dias por semana.

6.67.15 A solicitação será efetuada através de abertura de chamado na Central de Serviços da CONTRATADA disponível preferencialmente por portal web, e podendo ser contingenciado através de correio eletrônico ou telefone. A CONTRATADA deverá fornecer o nome do site, o endereço eletrônico e número do telefone, na assinatura do contrato.

6.67.16 A cada abertura de chamado, o Central de Serviços da CONTRATADA deverá fornecer ao CONTRATANTE um código identificador para acompanhamento da ocorrência.

6.67.17 Caberá exclusivamente à CONTRATANTE a definição de criticidade/impacto no ato da abertura do chamado.

6.67.18 A CONTRATADA deverá providenciar o início do atendimento dentro do prazo definido no Tempo Máximo para Início do Atendimento contido neste documento.

6.67.19 Os diagnósticos das ocorrências serão realizados pelo(s) técnico(s) da CONTRATADA, com acompanhamento do responsável(is) da CONTRATANTE , respeitando os prazos estabelecidos e sem custos adicionais para o CONTRATANTE .

6.67.20 As despesas relativas a eventuais deslocamentos dos técnicos que se fizerem necessárias para a correção de problemas técnicos, correrão por conta da CONTRATADA e sob sua exclusiva responsabilidade.

6.67.21 O planejamento de atividades de implantação e/ou atualização na solução deverá ser realizado pelo CONTRATANTE , com o acompanhamento de técnicos da CONTRATADA, utilizando as recomendações do fabricante para minimizar o risco de instabilidade no ambiente.

6.67.22 O serviço de otimização (tunning) da Plataforma será realizado periodicamente, em data a ser informada pelo CONTRATANTE, a fim de avaliar as necessidades de melhorias relacionadas ao desempenho e nível de segurança.

6.67.23 Melhoria na Solução e novos serviços técnicos especializados deverão ser remunerados por meio de Unidades de Serviço Técnico (UST).

6.67.24 A unidade de medida adotada (UST) corresponde ao esforço padronizado para determinada complexidade, independentemente da quantidade de recursos humanos alocados. O seu pagamento é condicionado à prestação dos serviços e atendimento dos níveis de serviços especificados.

6.67.25 A CONTRATADA é responsável pela prestação dos serviços caracterizados nas ordens de serviço, devendo utilizar pessoal técnico qualificado para prestar o serviço técnico, nos quantitativos adequados, para garantir a plena qualidade dos serviços entregues, ficando sob sua definição qualquer composição de recursos, otimização de rotinas ou procedimentos.

6.67.26 A CONTRATANTE fará uso e efetuará o pagamento apenas das USTs necessárias à implementação e manutenção dos serviços que solicitar à CONTRATADA, até o limite máximo das USTs estimadas. A CONTRATANTE não realizará pagamento prévio de USTs sob qualquer hipótese

6.67.27 A quantidade de USTs por novos serviços técnicos especializados não poderá ser superior à quantidade de USTs definidas neste Termo de Referência.

6.67.28 As tarefas de Planejamento/Criação/Diagnóstico e Execução/Alteração/Implantação e Exclusão referentes aos novos serviços técnicos especializados serão cobradas com base em cada solicitação atendida;

6.67.29 Os valores de referência UST especificados terão seu cômputo ajustado de acordo com a natureza da solicitação da CONTRATANTE , conforme detalhado na tabela abaixo.

6.67.30 A relação dos serviços técnicos especializados do objeto da presente contratação consta das Tabela 4 e 7. Esses serviços serão prestados pela CONTRATADA.

6.67.31 Com vistas a mitigar o risco de sobrepreço e superfaturamento de preços dos serviços baseadas em UST, a LICITANTE vencedora do certame deverá apresentar juntamente com sua proposta comercial, Planilha de Composição de Custos e Formação de Preços referente os serviços baseados em UST, conforme Tabela 4, baseado no modelo constante no Anexo VII-D da Instrução Normativa nº 5, de 26 de maio de 2017, da Secretaria de Gestão, do Ministério do Planejamento, Desenvolvimento e Gestão.

6.67.32 Natureza da solicitação de novos serviços técnicos especializados:

Tabela 4

Natureza da tarefa	Complexidade	Ajuste no valor de referência (fator multiplicador)
Planejamento, criação ou diagnóstico	Alta	1
Execução, alteração ou implantação	Média	0,5
Exclusão	Baixa	0,25

2.1.1 Todas as demandas devem ser validadas pela CONTRATANTE e serão critério de aceitação/aprovação da solução proposta pela CONTRATADA;

2.1.2 Na tabela abaixo, novos Serviços técnicos especializados sob demanda:

Tabela 5

Item	Descrição de novos Serviços	Periodicidade	Complexidade	Totais(em UST)
1	**Operação assistida** - Gerenciamento da plataforma, monitoramento 8x5, implementação de demandas e emissão de relatórios e Suporte mensal	Rotineira/Mensal	Média	160
2	Elaborar relatório Jurídico de **Impacto e Riscos**	Periódico	Alta	80
3	Elaborar e implantar pacote de políticas, normas e termos em conformidade com as Normas de Privacidade	Periódico	Alta	160
4	Elaborar **Auditoria trimestral** de itens de Privacidade	Rotineira/Trimestral	Alta	40
5	Elaborar **Discovery e Data Mapping** de Sistemas Estruturados	Rotineira	Alta	160
6	Criar e manter o **Portal do Titular** em conformidade com as Normas de Privacidade e as normas internas	Rotineira/Mensal	Média	80
7	Elaborar **Diagnostico Maturidade TI**	Periódico	Alta	160
8	Manter o Monitoramento **Compliance on-line**	Rotineira/Mensal	Baixa	10
9	Realizar o **Discovery e Data Mapping** dos Dados não Estruturados	Periódico	Média	80
10	Mapeamento e **catalogação de dados** pessoais	Periódico	Média	160
11	Mapeamento do **ciclo de vida dos dados** pessoais identificados	Periódico	Média	80
12	Elaborar Planejamento **Estratégico de Governança de Dados**	Periódico	Alta	160
13	Criar documento de estrutura da área responsável pela gestão da **proteção de dados**	Periódico	Alta	40
14	Elaborar regras de negócio do módulo de gestão de tratamento de dados - Módulo de **proteção e rastreabilidade de tratamento dos dados** pessoais	Periódico	Alta	160

15	Especificação das regras de negócio para o módulo de gestão de notificações - **Módulo de Mensageria** e notificações	Periódico	Alta	40
16	Elaborar e implantar **Plano de Capacitação**	Periódico	Média	80
17	Elaborar e implantar **Plano de Métricas**	Periódico	Média	80
18	Definir o **plano de comunicação e divulgação** do projeto.	Periódico	Alta	40
19	Realizar a gestão do projeto, apresentando e acompanhando os **indicadores de gestão dos serviços**.	Periódico	Média	150
20	Elaborar e implementar **planos de ação para correção de desvios**.	Periódico	Média	150
21	Elaborar **relatório de Identificação do cenário atual** do CONTRATANTE em relação a processos, tecnologias, governança, políticas e normas e realizar a avaliação em relação às exigências da Lei nº 13.709/18	Periódico	Média	60
22	Elaborar **inventário de todos os processos de negócios** que envolvem dados pessoais, nos termos da lei.	Periódico	Média	60
23	Elaborar inventário de todos os processos de negócios que envolvem dados sensíveis, nos termos da lei.	Periódico	Média	60
24	Elaborar análise para identificar os processos nos quais o **consentimento do titular dos dados pessoais** utilizados deverá ser solicitado e formalizado.	Periódico	Média	60
25	Realizar a **busca de dados pessoais não estruturados em pastas de arquivos**, utilizando ferramenta para Descoberta de Dados (Data Discovery).	Rotineira/Mensal	Média	80
26	Prover serviços de **consultoria de Monitoramento e Suporte à Privacidade e jurídica especializada em ÀS NORMAS DE PRIVACIDADE** de acordo com a demanda para esclarecimento e orientações específicas.	Rotineira/Mensal	Média	150
27	**Identificar os controladores e processadores de dados** envolvidos nos processos de negócios.	Rotineira/Mensal	Média	60
28	Estruturar o relatório de "***Data Protection Impact Assessment***" (DPIA) e fornecer modelo de preenchimento, bem como suportar a equipe do	Periódico	Média	40

	CONTRATANTE no desenvolvimento de novos RIPDs/DPIAs.			
29	Revisar e propor as alterações necessárias nas **políticas de privacidade**	Periódico	Média	150
30	Elaborar e implementar **método de análise de impacto à privacidade** em conformidade com as Normas de Privacidade.	Periódico	Alta	160
31	Preparar o material para **divulgação da política de governança.**	Periódico	Média	80
32	Elaborar o processo de **gerenciamento de violações e notificações** necessárias.	Periódico	Média	80
33	Elaborar plano de **gestão de crise** em caso de incidente/ violação de dados.	Periódico	Média	20
34	Avaliação das **exigências adicionais em relação à Lei de Acesso à Informação** presentes na Lei Federal Nº 12.527/11 para identificação de lacunas no cenário atual.	Periódico	Média	20
35	**Revisar as políticas e os procedimentos existentes** que tratem da segurança de informação, privacidade, acesso à informação, classificação de informação, entre outros.	Periódico	Baixa	40

6.68 TREINAMENTO

6.68.1 O treinamento será destinado aos colaboradores técnicos da CONTRATANTE, visando a capacitá-los no gerenciamento e no uso da plataforma, conforme requisitos estabelecidos neste documento;

6.68.2 O treinamento será ministrado nas dependências da CONTRATANTE, em data e horário por ela definido. Poderá, a critério dela, ser ministrado o treinamento à distância;

6.68.3 Os eventos de treinamento serão solicitados com no mínimo vinte dias úteis de antecedência, salvo entendimento diverso entre as partes;

6.68.4 O treinamento deverá ser presencial (salvo exceções a critério da CONTRATANTE) e dividido em etapas. O treinamento não poderá ser meramente expositivo. Deve contemplar também o uso prático da solução e o desenvolvimento de estudos de caso. No caso de o treinamento ser realizado nas dependências da CONTRATANTE, as instalações e recursos audiovisuais serão providos por ela;

6.68.5 O treinamento fornecido pela CONTRATADA deve ser apresentado em língua portuguesa. O material didático deve ser fornecido em formato digital e/ou impresso para todos os participantes com o conteúdo abordado durante o treinamento em língua portuguesa. Não serão aceitos materiais e treinamentos ministrados em língua estrangeira;

6.68.6 A CONTRATADA deverá emitir, ao final do treinamento, o certificado de conclusão para

cada participante, no qual deverão constar a identificação do treinando, o período de realização, o conteúdo e a carga horária do treinamento.

6.68.7 O instrutor responsável pela execução do treinamento deverá possuir experiência comprovada como instrutor da solução e pleno conhecimento da solução alvo do treinamento. A comprovação da capacitação do instrutor dar-se-á com base na apresentação de certificados dos treinamentos.

6.68.8 Caso a qualidade do treinamento em alguma turma seja considerada insatisfatória pela maioria simples dos alunos, a CONTRATANTE poderá exigir que o treinamento seja refeito, sem onerá-la de modo algum, no prazo a ser estipulado entre as partes.

6.68.9 O treinamento deverá ser ministrado em duas turmas;

6.68.10 Limite máximo de até 20 participantes cada turma;

6.68.11 A carga horária do curso deverá ser de, no mínimo, 24 horas;

6.68.12 A contratada deverá produzir o relatório final de cada entrega em duas vias impressas, encadernadas e assinadas pelos responsáveis, com sumário, resumo executivo e índice remissivo, mantendo a coerência e organização entre os volumes, além de disponibilizar todo o material em meio digital;

6.68.13 O idioma oficial de todo trabalho desenvolvido é o português (Brasil).

7. CATÁLOGO DE SERVIÇOS

Tabela 7

CATEGORIA	ATIVIDADE	DESCRIÇÃO ATIVIDADE	ENTREGÁVEL	COMPLEXIDADE
Pré-projeto e Levantamento de requisitos	Reunião Inicial	Reunião inicial do projeto com o cliente e parte técnica para alinhar expectativas do produto a ser entregue e macro-cronograma. Nessa reunião será definido o levantamento de requisitos.	Ata de Reunião, Relatório de Requisitos e Cronograma	Baixa

	Reunião para mapeamento das bases de dados	Reunião com cliente do projeto e área técnica com objetivo de identificar a origem dos dados necessários para desenvolvimento do projeto (banco de dados, planilhas, txt, xml, etc.) e qual relação entre elas.	Ata de Reunião, Relatório de Requisitos e Cronograma	Média
	Reunião para levantamento de áreas para mapeamento de processos e dados de fundação	Reunião com cliente do projeto e área técnica com objetivo de identificar organograma, sistemas, pessoas que participarão do mapeamento e e-mails.	Ata de Reunião, Relatório de Requisitos e Cronograma	Baixa
	Criação do documento de projeto	Criação de documento detalhando todas as origens de dados que serão utilizadas, portais, ambientes de instalação dos produtos on-primisses, URLS e contagem de HST	Documento de Projeto	Baixa
	Definir o plano de comunicação e divulgação do projeto.	Criação do conteúdo, canais de comunicação e processos de divulgação do projeto	Plano de Comunicação	Alta
	Criação de conexão a diretórios de usuário, LDAP, Ac ve Directory, SQL, etc.	Criação de conexão a diretórios de usuário, LDAP, Ac ve Directory, SQL, etc.	Relatório Técnico Descritivo	Média
Serviços Especializados	Elaborar relatório Jurídico de Impacto e Riscos	Elaborar relatório Jurídico de Impacto e Riscos	Relatório Técnico Descritivo	Alta
	Elaborar Discovery e Data Mapping de Sistemas Estruturados	Elaborar Discovery e Data Mapping de Sistemas Estruturados	Relatório Técnico Descritivo	Alta
	Criar e manter o Portal do Titular em conformidade com as	Criar e manter o Portal do Titular em conformidade com as	Relatório Técnico Descritivo	Média

	Normas de Privacidade e as normas internas	Normas de Privacidade e as normas internas		
	Elaborar Diagnóstico de Maturidade TI	Elaborar Diagnóstico de Maturidade TI	Relatório Técnico Descritivo	Alta
	Realizar o Discovery e Data Mapping dos Dados não Estruturados	Realizar o Discovery e Data Mapping dos Dados não Estruturados	Relatório Técnico Descritivo	Média
	Mapeamento e catalogação de dados pessoais	Mapeamento e catalogação de dados pessoais	Relatório Técnico Descritivo	Média
	Mapeamento do ciclo de vida dos dados pessoais idenficados	Mapeamento do ciclo de vida dos dados pessoais idenficados	Relatório Técnico Descritivo	Média
	Elaborar Planejamento Estratégico de Governança de Dados	Elaborar Planejamento Estratégico de Governança de Dados	Relatório Técnico Descritivo	Alta
	Criar documento de estrutura da área responsável pela gestão da proteção de dados	Criar documento de estrutura da área responsável pela gestão da proteção de dados	Relatório Técnico Descritivo	alta
	Elaborar regras de negocio do modulo de gestão de tratamento de dados - Modulo de proteção e rastreabilidade de tratamento dos dados pessoais	Elaborar regras de negocio do modulo de gestão de tratamento de dados - Modulo de proteção e rastreabilidade de tratamento dos dados pessoais	Relatório Técnico Descritivo	Alta
	Especificação das regras de negocio para o modulo de gestão de noficações - Modulo de Mensageria e noficações	Especificação das regras de negocio para o modulo de gestão de noficações - Modulo de Mensageria e noficações	Relatório Técnico Descritivo	Alta
	Elaborar e implantar Plano de Métricas	Elaborar e implantar Plano de Métricas	Relatório Técnico Descritivo	Média
	Elaborar inventario de todos os processos de negócios que envolvem dados pessoais, nos termos da lei.	Elaborar inventario de todos os processos de negócios que envolvem dados pessoais, nos termos da lei.	Relatório Técnico Descritivo	Média

	Elaborar inventario de todos os processos de negócios que envolvem dados sensíveis, nos termos da lei.	Elaborar inventario de todos os processos de negócios que envolvem dados sensíveis, nos termos da lei.	Relatório Técnico Descritivo	Média
	Elaborar análise para identificar os processos nos quais o consentimento do titular dos dados pessoais utilizados deverá ser solicitado e formalizado.	Elaborar análise para identificar os processos nos quais o consentimento do titular dos dados pessoais utilizados deverá ser solicitado e formalizado.	Relatório Técnico Descritivo	Média
	Identificar os controladores e processadores de dados envolvidos nos processos de negócios.	Identificar os controladores e processadores de dados envolvidos nos processos de negócios.	Relatório Técnico Descritivo	Média
	Estruturar o relatório de "*Data Protection Impact Assessment*" (DPIA) e fornecer modelo de preenchimento, bem como suportar a equipe do CONTRATANTE no desenvolvimento de novos RIPDs/DPIAs.	Estruturar o relatório de "*Data Protection Impact Assessment*" (DPIA) e fornecer modelo de preenchimento, bem como suportar a equipe do CONTRATANTE no desenvolvimento de novos RIPDs/DPIAs.	Relatório Técnico Descritivo	Média
	Revisar e propor as alterações necessárias nas politicas de privacidade	Revisar e propor as alterações necessárias nas politicas de privacidade	Relatório Técnico Descritivo	Média
	Elaborar e implementar método de análise de impacto à privacidade em conformidade com as Normas de Privacidade.	Elaborar e implementar método de análise de impacto à privacidade em conformidade com as Normas de Privacidade.	Relatório Técnico Descritivo	Alta
	Preparar o material para divulgação da politica de governança.	Preparar o material para divulgação da politica de governança.	Relatório Técnico Descritivo	Média

	Elaborar o processo de gerenciamento de violações e noficações necessárias.	Elaborar o processo de gerenciamento de violações e noficações necessárias.	Relatório Técnico Descritivo	Média
	Elaborar plano de gestão de crise em caso de incidente/ violação de dados.	Elaborar plano de gestão de crise em caso de incidente/ violação de dados.	Relatório Técnico Descritivo	Média
	Avaliação das exigências adicionais em relação à Lei de Acesso à Informação presentes na Lei Federal No 12.527/11 para identificação de lacunas no cenário atual.	Avaliação das exigências adicionais em relação à Lei de Acesso à Informação presentes na Lei Federal No 12.527/11 para identificação de lacunas no cenário atual.	Relatório Técnico Descritivo	Média
	Revisar as politicas e os procedimentos existentes que tratem da segurança de informação, privacidade, acesso à informação, classificação de informação, entre outros.	Revisar as politicas e os procedimentos existentes que tratem da segurança de informação, privacidade, acesso à informação, classificação de informação, entre outros.	Relatório Técnico Descritivo	Baixa
Desenvolvimento do Projeto	Elaborar e implantar pacote de politicas, normas e termos em conformidade com as Normas de Privacidade	Mapear políticas, termos e normas existentes e criar os documentos necessários	Políticas, Termos e Normas de Privacidade	Alta
	Elaborar relatório de Identificação do cenário atual do CONTRATANTE em relação a processos, tecnologias, governança, politicas e normas e realizar a avaliação em relação as exigências da Lei no 13.709/18	Mapear processos, políticas, ferramentas, sistemas e nível de conscientização em relação às Normas de Privacidade	Relatório de Gaps	Média
	Criação de conexão a fonte de dados e	Criação de conexão a fontes de dados que	Relatório Técnico Descritivo	Alta

	configuração dos ambientes	serão utilizadas na plataforma.		
	Publicação em Produção dos Portais	Publicação dos portais em produção e liberação de acessos.		
Mentoria	Elaborar e implantar Plano de Capacitação	Análise das Bases de Conhecimento, Treinamentos e melhores práticas	Relatório de Atividades de Mentoria e Capacitação na plataforma	Média
	Processo contínuo de Data Discovery/ Data Mapping	Apoio na criação e manutenção de processos de carga; criação de novos painéis e manutenção de existente; performance, otimização e melhores práticas; verificação de logs de carga; sustentação de aplicação legada; monitoramento do ambiente	Relatório de Atividades	Baixa
Operação e Manutenção da Plataforma	Operação assistida	Gerenciamento da plataforma, monitoramento 8x5, implementação de demandas e emissão de relatórios e Suporte mensal	Rotineira/Mensal	Média
	Elaborar Auditoria trimestral de itens de Privacidade	Auditoria das dimensões jurídicas, de proteção de dados, das políticas e cultura	Rotineira/Trimestral	Alta
	Manter o Monitoramento Compliance on-line	Rodar scan dos sites para verificação das coletas de cookies	Relatório de Scan de Compliance on-line	Baixa
	Elaborar e implementar planos de ação para correção de desvios.	Análise dos riscos, tarefas, prazos e responsáveis	Relatório de Atividades	Média

	Realizar a busca de dados pessoais não estruturados em pastas de arquivos, utilizando ferramenta para Descoberta de Dados (Data Discovery).	Rodar discovery trimestral das fontes de dados não estruturados	Relatório de Discovery de Dados não estruturados	Média
	Prover serviços de consultoria de Monitoramento e Suporte à Privacidade e assessoria especializada de acordo com a demanda para esclarecimento e orientações especificas.	Suporte consultivo à Equipe de Privacidade, tanto nas questões legais quanto da Plataforma	Relatório de Atividades	Média
	Realizar a gestão do projeto, apresentando e acompanhando os indicadores de gestão dos serviços.	Suporte do PMO ao Gestor do Projeto	Relatório de Atividades	Média

8. REQUISITOS DE NEGÓCIO

8.1. Os serviços serão executados remotamente. Em casos específicos, caso seja de interesse da CONTRATADA e da CONTRATANTE, algumas atividades inerentes a estes serviços poderão ser realizadas localmente nas instalações da CONTRATANTE;

8.2. Quando a prestação dos serviços ocorrer nas instalações do CONTRATANTE, será de responsabilidade do CONTRATANTE a disponibilização de todos os insumos necessários para prestação de serviços, dentre eles: espaço físico, mobiliário, estação de trabalho, rede elétrica e acesso à rede corporativa do CONTRATANTE;

8.3. Os serviços serão prestados em horário normal de trabalho, ou seja, dias úteis entre às 08h e às 18h. O período diário de trabalho é de 08 (oito) horas com intervalo para almoço;

8.4. A equipe de colaboradores designada pelo CONTRATANTE prestará apoio na comunicação interna, bem como no entendimento de processos e normas internas, de forma a auxiliar a consultoria.

8.5. A prestação do serviço deverá ser executada por profissionais com conhecimentos e experiências em proteção de dados pessoais;

8.6. Os profissionais da CONTRATADA, que executarão os trabalhos, deverão possuir formações em temas correlacionados e sempre exercer suas atribuições com acompanhamento e orientação do PREPOSTO, responsável pela condução e realização dos serviços contratados.

9. DA PLANILHA DE COTAÇÃO

9.1. O valor total estimado total da contratação por 12 meses será de R$ X (X milhões de reais) , conforme a tabela a seguir:

Tabela 8

Item	Descrição	Unidade	Quantidade máxima	Valor Unt	Valor total
01	Portal Centralizado de Governança, incluindo suporte técnico, manutenção e atualização tecnológica, implantação, diagnósticos e melhorias nos processos aderentes	Mensal	60		
02	Módulo de Governança	Bancos de dados – blocos de 50	750		
03	Módulo de Privacidade	Bancos de dados – blocos de 50	750		
04	Módulo de Segurança	Bancos de dados – blocos de 50	750		
05	Módulo de Gerenciamento Integrado de Riscos	Usuários – blocos de 25	250		
06	Módulo de Automação	Usuários – blocos de 25	250		
07	Módulo de Gestão de Serviços	Usuários – blocos de 25	250		
08	Módulo de Gestão de Atendimento	Usuários – blocos de 25	250		
09	Módulo de Gestão de Demandas, Projetos e Novos Desenvolvimentos	Usuários – blocos de 25	250		
10	Módulo de Gestão de Operações	Usuários – blocos de 25	250		
11	Módulo de Gestão de Ativos	Usuários – blocos de 25	250		
12	Módulo de Gestão de Segurança e Incidentes	Usuários – blocos de 25	250		
13	Serviço de hospedagem em cloud	Banco de dados – Blocos de 50 (mensal)	1.000		
14	Solução de monitoramento contínuo para detecção de possíveis impactos corporativos	Por ativos – blocos de 10	300		
15	Solução de monitoramento, detecção e resposta a incidentes de segurança da informação - 1.500 Eventos por segundo (EPS)	Aferição mensal de eventos por segundo	Máximo 6000 mês		
16	Serviços de customização e desenvolvimento de integrações com os sistemas da Contratante.	blocos de 100 UST	5.000		
17	Serviço especializado para mapeamento e análise dos processos de negócio, serviços de customização e desenvolvimento de integrações com os sistemas da contratante.	blocos de 100 UST	1.000		
18	Solução para testes de penetração em acordo com o OWASP (Plataforma WEB aberta para segurança de aplicativos)	500 endpoints 10 domínios	Máximo 5000 endpoints Máximo 1000 domínios		

19	Solução de compliance e anti-fraude em ambientes de inteligência artificial com deploy ilimitados	Blocos de 10 usuários	50 usuários		
20	Transferência de conhecimento de instalação, configuração e administração da plataforma e componentes	Por turma com 20 alunos	40		
21	Serviços de operação assistida (sustentação da plataforma)	blocos de 100 UST	2.000		
22	Serviços de monitoramento e suporte à privacidade	blocos de 100 UST	2.000		
23	Licença para uso de plataforma de treinamento em Conceitos de Segurança da Informação em formado EAD	Por Aluno – mínimo 50	5.000		

10. DO NÃO PARCELAMENTO DO OBJETO

10.1. O § 1º do artigo 23 da Lei Federal nº 8.666/93 exige o parcelamento do objeto da licitação, desde que haja viabilidade técnica e econômica para tal. O objeto deste Termo de Referência é a contratação de empresa especializada para prestação de serviços técnicos de Adequação e Governança de Dados Corporativos visando melhorias nos processos aderentes às Normas de Privacidade do CONTRATANTE , compreendendo desenvolvimento, implantação, treinamento e serviços de Técnico Especializado .

10.2. Trata-se de prestação de serviço específico de TI, com objetivo de adequar bases de dados corporativa e serviços e tecnologias do CONTRATANTE às Normas de Privacidade . A interação entre os profissionais de TI e os servidores conhecedores do negócio é fundamental para garantir pleno funcionamento dos serviços contratados.

10.3. As Normas de Privacidade vem para estabelecer regras de segurança da informação do cidadão, não importa se a sede da Organização ou o Centro de Dados estejam localizado no Brasil ou no exterior. Portanto, se há o processamento de conteúdo de pessoas, brasileiras ou não, que estão no território nacional, as Normas de Privacidade devem ser cumpridas, portanto não é recomendável parcelar uma solução tão complexa entre vários fornecedores.

10.3.1. Uma maior divisão da contratação, poderia acarretar riscos de não integração entre as partes contratadas, gerando alto tempo de resposta a incidentes e prejuízos às atividades do CONTRATANTE , além de conflito de responsabilidade entre os diversos envolvidos, dificultando a gestão dos contratos e serviços.

10.3.2. Frente ao exposto, o objeto deste Termo de Referência não é parcelável.

10.3.3. Convém destacar que a presente propositura não se constitui inovação na Administração Pública. Há registros de inúmeros contratos que guardam semelhança com os serviços ora propostos, demonstrando-se haver um mercado estabelecido, com capacidade de absorver e suprir as necessidades da presente contratação.

11. DO CONSÓRCIO E SUBCONTRATAÇÃO

11.1. É admitida a subcontratação deste termo de referência por se tratar de serviços especializados, que constituem etapa preparatória à implantação da solução;

11.1.1. Todas as soluções dessa especificação poderão ser subcontratada até 30%.

11.1.2. A participação de consórcios não será admitida, uma vez que o objeto a ser adquirido é amplamente comercializado por diversas empresas no mercado. Tal permissibilidade poderia causar dano à administração por frustrar o próprio caráter competitivo da disputa pelo menor preço.

12 DA VIGÊNCIA DO CONTRATO

12.1 Os prazos de vigência e de execução contratual serão de 12 (doze) meses, podendo ser prorrogado, a critério da Contratante, com concordância da contratada, por períodos iguais ou inferiores, conforme art. 71 da Lei Federal 13.303/2016 e do art. 148 do Regulamento de Licitações e Contratos da ETICE.

12.2 Referido contrato poderá ser alterado nos casos previstos no art. 81 da Lei Federal n°13.303/2016 e no art. 149 do Regulamento de Licitações e Contratos da ETICE.

13 DO MODELO DE PROPOSTA

13.1 O modelo de proposta encontra-se no Anexo A.

14 CONFIDENCIALIDADE DOS TRABALHOS

14.1 A Contratada, seu preposto e qualquer profissional da mesma, envolvidos na realização dos trabalhos, obrigam-se a tratar todas as informações obtidas junto a ETICE e seu cliente final como **informação sigilosa ou confidencial**, devendo neste sentido mantê-las sob estrito sigilo, comprometendo-se ainda em não comunicar, divulgar ou revelar as informações confidenciais a terceiros, **mesmo após a finalização dos trabalhos a confidencialidade das informações permanece.**

14.2 Para tal, serão consideradas como informações confidenciais todas e quaisquer informações ou dados, independentemente de estarem expressamente classificados como confidenciais, fornecidas verbalmente ou por escrito, ou de qualquer outra forma, corpórea ou não, cuja divulgação possa provocar prejuízos de qualquer natureza, abrangendo, mas não se limitando a, pormenores, estratégias de negócios, pesquisas, dados financeiros e estatísticos, informações sobre negociações em andamento, informações sobre softwares, informações cadastrais, documentos que venha a ter conhecimento ou acesso, ou que venha a receber da contratante, sejam de caráter técnico ou não.

14.3 Tais informações confidenciais deverão ser usadas **exclusivamente** para a condução dos trabalhos objeto da relação de serviços entre a ETICE, cliente final e a contratante, não podendo, sob nenhuma forma ou pretexto, serem divulgadas, reveladas, reproduzidas,

utilizadas ou ser dado conhecimento a terceiros estranhos a esta contratação, exceto quando o dever de divulgar tais informações seja estritamente por força de exigência legal, devendo a parte obrigada a fornecer tais informações, avisar imediatamente a outra parte sobre tal exigência legal para, se for o caso, tomar as providências que achar necessárias.

14.4 A Contratada deverá apresentar "Termo de Responsabilidade e Sigilo", contendo a declaração de manutenção de sigilo e ciência das normas de segurança da Etice, assinado por cada empregado seu que estiver diretamente envolvido na contratação, quando o serviço exigir.

14.5 A contratada deverá entregar a ETICE, no momento da rescisão do contrato, todo o material físico ou digital de propriedade da contratante e destruir qualquer cópia em posse da contratada.

15 DA FRAUDE E DA CORRUPÇÃO

15.1 As Pré-Qualificadas devem observar e a contratada deve observar e fazer observar, por seus fornecedores e subcontratados, se admitida subcontratação, o mais alto padrão de ética durante todo o processo de licitação, de contratação e de execução do objeto contratual.

15.1.1 Para os propósitos deste item, definem-se as seguintes práticas:

a) "**prática corrupta**": oferecer, dar, receber ou solicitar, direta ou indiretamente, qualquer vantagem com o objetivo de influenciar a ação de servidor público no processo de licitação ou na execução de contrato;

b) "**prática fraudulenta**": a falsificação ou omissão dos fatos, com o objetivo de influenciar o processo de licitação ou de execução de contrato;

c) "**prática conluiada**": esquematizar ou estabelecer um acordo entre duas ou mais licitantes, com ou sem o conhecimento de representantes ou prepostos do órgão licitador, visando estabelecer preços em níveis artificiais e não-competitivos;

d) "**prática coercitiva**": causar dano ou ameaçar causar dano, direta ou indiretamente, às pessoas ou sua propriedade, visando a influenciar sua participação em um processo licitatório ou afetar a execução do contrato.

e) "**prática obstrutiva**":

(1) destruir, falsificar, alterar ou ocultar provas em inspeções ou fazer declarações falsas aos representantes do organismo financeiro multilateral, com o objetivo de impedir materialmente a apuração de alegações de prática prevista neste subitem;

(2) atos cuja intenção seja impedir materialmente o exercício do direito de o organismo financeiro multilateral promover inspeção.

15.2 Na hipótese de financiamento, parcial ou integral, por organismo financeiro multilateral, mediante adiantamento ou reembolso, este organismo imporá sanção sobre uma empresa ou pessoa física, para a outorga de contratos financiados pelo organismo se, em qualquer momento, constatar o envolvimento da empresa, diretamente ou por meio de um agente, em práticas corruptas, fraudulentas, conluiadas, coercitivas ou obstrutivas ao participar da licitação ou da execução um contrato financiado pelo organismo.

15.3 Considerando os propósitos dos itens acima, a licitante vencedora como condição para a contratação, deverá concordar e autorizar que, na hipótese de o contrato vir a ser financiado, em parte ou integralmente, por organismo financeiro multilateral, mediante adiantamento ou reembolso, permitirá que o organismo financeiro e/ou pessoas por ele formalmente indicadas possam inspecionar o local de execução do contrato e todos os documentos e registros relacionados à licitação e à execução do contrato.

15.4 A contratante, garantida a prévia defesa, aplicará as sanções administrativas pertinentes, previstas na Lei, se comprovar o envolvimento de representante da empresa ou da pessoa física contratada em práticas corruptas, fraudulentas, conluiadas ou coercitivas, no decorrer da licitação ou na execução do contrato financiado por organismo financeiro multilateral, sem prejuízo das demais medidas administrativas, criminais e cíveis.

16 DA SUBCONTRATAÇÃO

16.1 Será admitida a subcontratação no limite de até 30% (trinta por cento) do objeto, conforme disposto no art. 78 da Lei nº 13.303/2016 e nos arts. 143 a 147 do Regulamento de Licitações e Contratos da ETICE, desde que não constitua o escopo principal da contratação, e, se previamente aprovada pela ETICE.

16.2 A subcontratação de que trata esta cláusula, **não exclui a responsabilidade da contratada perante a ETICE** quanto à qualidade do objeto contratado, **não constituindo, portanto, qualquer vínculo contratual ou legal da ETICE com a subcontratada.**

16.3 A empresa subcontratada deverá atender, em relação ao objeto da subcontratação, as exigências de qualificação técnica impostas a licitante vencedora.

16.4 É **vedada** a subcontratação de empresa ou consórcio que tenha participado:

16.4.1 Do procedimento licitatório do qual se originou a contratação.

16.4.2 Direta ou indiretamente, da elaboração de projeto básico ou executivo.

17 DAS DISPOSIÇÕES GERAIS

17.1 **Esta chamada de oportunidade não importa necessariamente em contratação**, nos moldes já dispostos Edital de Pré-Qualificação 001/2019, podendo a autoridade competente revogá-la por razões de interesse público, anulá-la por ilegalidade de ofício ou por provocação de terceiros, mediante decisão devidamente fundamentada, sem quaisquer reclamações ou direitos à indenização ou reembolso.

17.2 É facultada à Comissão de Avaliação ou à autoridade competente, em qualquer fase da licitação, **a promoção de diligência** destinada a esclarecer ou a complementar a instrução do processo licitatório, vedada a inclusão posterior de documentos que deveriam constar originariamente na proposta e na documentação.

17.3 Toda a documentação fará parte dos autos e **não será devolvida a licitante**, ainda que se trate de originais.

17.4 Na contagem dos prazos estabelecidos nesta Chamanda de Oportunidade, excluir-se-ão os dias de início e incluir-se-ão os dias de vencimento. **Os prazos estabelecidos neste edital para a fase externa se iniciam e se vencem somente em dias úteis de expediente da ETICE**.

17.5 Os representantes legais das Pré-Qualificadas são responsáveis pela fidelidade e legitimidade das informações e dos documentos apresentados em qualquer fase da licitação.

17.6 O desatendimento de exigências meramente formais, não essenciais, não implicará no afastamento da Pré-Qualificada, desde que seja possível a aferição da sua qualificação e a exata compreensão da sua proposta.

17.7 **A Comissão de Avaliação poderá sanar erros formais que NÃO acarretem prejuízos para o objeto da Chamada de Oportunidade**, à Administração e às Pré-Qualificadas, dentre estes, os decorrentes de operações aritméticas.

17.8 Desde já fica estabelecido que caso a Pré-Qualificada **NÃO APRESENTE PROPOSTA** para a presente Chamada de Oportunidade, já está renunciando, assim, expressamente ao direito de recurso e respectiva contrarrazões, concordando com o curso desta Chamada de Oportunidade de Serviços de Nuvem Pública, aderente ao Edital de Pré-Qualificação Permanente de Serviços em Nuvem Nº 001/ 2019 – ETICE

17.9 Os casos omissos serão resolvidos pela Comissão de Avaliação, nos termos da legislação pertinente.

17.10 As normas que disciplinam esta Chamada de Oportunidade serão sempre interpretadas em favor da ampliação da disputa.

17.11 Os documentos referentes aos orçamentos, bem como o valor estimado da contratação, **possuem caráter sigiloso e serão disponibilizados exclusivamente aos órgãos de controle interno e externo.**

17.12 As Pré-Qualificadas deverão atender ao disposto no Código de Conduta, Ética e Integridade da ETICE, o qual encontra-se disponível no nosso sítio eletrônico para download.

17.13 O **foro** designado para julgamento de quaisquer questões judiciais resultantes deste edital será o da **Comarca de Fortaleza**, Capital do Estado do Ceará.

Fortaleza, 01 de agosto de 2022.

José Lassance de Castro Silva
Presidente ETICE

Marco Antônio Marinho Russo
Diretor DITEC

ROL DE ANEXOS:

ANEXO A - MODELO DE PROPOSTA

ANEXO A
Modelo de Proposta

TABELA 01

Item	Descrição	Unidade	Quantidade máxima (a)	Valor Unitário Mensal (b)	Valor Anual (c)
01	Portal Centralizado de Governança, incluindo suporte técnico, manutenção e atualização tecnológica, implantação, diagnósticos e melhorias nos processos aderentes	Mensal	60		
02	Módulo de Governança	Bancos de dados – blocos de 50	750		
03	Módulo de Privacidade	Bancos de dados – blocos de 50	750		
04	Módulo de Segurança	Bancos de dados – blocos de 50	750		
05	Módulo de Gerenciamento Integrado de Riscos	Usuários – blocos de 25	250		
06	Módulo de Automação	Usuários – blocos de 25	250		
07	Módulo de Gestão de Serviços	Usuários – blocos de 25	250		
08	Módulo de Gestão de Atendimento	Usuários – blocos de 25	250		
09	Módulo de Gestão de Demandas, Projetos e Novos Desenvolvimentos	Usuários – blocos de 25	250		
10	Módulo de Gestão de Operações	Usuários – blocos de 25	250		
11	Módulo de Gestão de Ativos	Usuários – blocos de 25	250		
12	Módulo de Gestão de Segurança e Incidentes	Usuários – blocos de 25	250		
13	Serviço de hospedagem em cloud	Banco de dados – Blocos de 50 (mensal)	1.000		
14	Solução de monitoramento contínuo para detecção de possíveis impactos corporativos	Por ativos – blocos de 10	300		
15	Solução de monitoramento, detecção e resposta a incidentes de segurança da informação - 1.500 Eventos por segundo (EPS)	Aferição mensal de eventos por segundo	Máximo 6000 mês		
16	Serviços de customização e desenvolvimento de integrações com os sistemas da Contratante.	blocos de 100 UST	5.000		
17	Serviço especializado para	blocos de 100 UST	1.000		

	mapeamento e análise dos processos de negócio, serviços de customização e desenvolvimento de integrações com os sistemas da contratante.				
18	Solução para testes de penetração em acordo com o OWASP (Plataforma WEB aberta para segurança de aplicativos)	500 endpoints 10 domínios	Máximo 5000 endpoints Máximo 1000 domínios		
19	Solução de compliance e anti-fraude em ambientes de inteligência artificial com deploy ilimitados	Blocos de 10 usuários	50 usuários		
20	Transferência de conhecimento de instalação, configuração e administração da plataforma e componentes	Por turma com 20 alunos	40		
21	Serviços de operação assistida (sustentação da plataforma)	blocos de 100 UST	2.000		
22	Serviços de monitoramento e suporte à privacidade	blocos de 100 UST	2.000		
23	Licença para uso de plataforma de treinamento em Conceitos de Segurança da Informação em formado EAD	Por Aluno – mínimo 50	5.000		
				Soma (d)	

(t1) Valor Total em R$ (igual a "d")

_____

Valor Total da Proposta (t1)

_____