

ANEXO A – ESPECIFICAÇÕES E REQUISITOS

1.	DETALHAMENTO DO OBJETO	3
2.	INFORMAÇÕES GERAIS	3
3.	DETALHAMENTO DOS SERVIÇOS	6
3.1.	Considerações Iniciais.....	6
3.2.	Modelo de atuação.....	7
3.3.	Ambiente da CONTRATADA	10
3.4.	Gerência de Serviços	11
3.5.	Canais de Comunicação.....	13
3.6.	Horário de atendimento.....	15
3.7.	Acompanhamento do Contrato	16
3.8.	Gerente Técnico de Conta (TAM)	17
3.9.	Níveis mínimos de serviço (NMS)	18
3.10.	Equipe técnica e Capacitação dos Profissionais	23
3.11.	Implantação, mudanças e adoção tecnológica	24
3.12.	Requisitos de Segurança da CONTRATADA	28
3.13.	Soluções Informatizadas e Ferramentas fornecidas.....	28
4.	GOVERNANÇA, GESTÃO DE RISCOS E CONFORMIDADE	30
4.1.	Características Gerais	30
4.2.	Gestão de políticas e procedimentos de segurança.....	31
4.3.	Conscientização dos colaboradores	31
4.4.	Gestão de riscos e conformidade	41
4.5.	Gestão de Vulnerabilidades.....	52
4.6.	Simulação de ataques.....	88
4.7.	Gestão de risco de terceiros.....	93
5.	CONTROLES DE SEGURANÇA	109
5.1.	Serviço gerenciado de segurança:.....	109
5.2.	Proteção de Perímetros.....	111
6.	PROTEÇÃO DAS INFORMAÇÕES, PRIVACIDADE e PROTEÇÃO DE DADOS PESSOAIS.....	149
6.1.	Características Gerais	149
6.2.	Módulo de Gerenciamento de Cookies e Portais e Websites	151

6.3. Gerenciamento de Políticas.....	152
6.4. Gestão de Atendimento de Titulares	153
6.5. Gerenciamento de Consentimentos	156
6.6. Portal da Privacidade.....	157
6.7. Gerenciamento de Auditoria.....	158
6.8. Mapeamento de Dados Pessoais	159
6.9. Gestão de Avaliações e Gestão de Fornecedores	163
6.10. Due Diligence.....	165
6.11. Gestão de Riscos.....	166
6.12. Gestão de Incidentes	168
6.13. Descoberta de Dados.....	169
6.14. Anonimização de Dados Pessoais.....	171
6.15. Gerenciamento de ESG.....	172
6.16. Workflow	173
6.17. Gráficos e Painéis.....	175
6.18. Governança em IA	175
7. Proteção das Aplicações.....	176
8. GESTÃO DE INCIDENTES	193
8.1. Proteção Contra Riscos Digitais.....	193
8.2. Detecção e Resposta aos Incidentes	201
9. CONTINUIDADE DO NEGÓCIO	222
9.1. Plano de continuidade do negócio	222
10. TREINAMENTO NA COMPREENSÃO E CAPACITAÇÃO TÉCNICA	223
10.1. Características Gerais	223
11. PROFISSIONAL DEDICADO	226
11.1. Características Gerais	226
12. SERVIÇOS TÉCNICOS ESPECIALIZADOS	228
12.1. Características Gerais	228

1. DETALHAMENTO DO OBJETO

- 1.1. Este processo tem como objetivo a contratação de uma solução para o planejamento, proteção, detecção e resposta aos incidentes relacionados à segurança das informações da CONTRATANTE, contemplando as diversas etapas evolutivas para uma correta e eficiente gestão dos processos de segurança da informação.
- 1.2. Está orientado à prestação de serviços, incluindo os softwares e hardwares necessários para sua execução, através de centros de monitoramento e resposta a incidentes (ambiente integrado de monitoramento e resposta a incidentes de segurança da informação - serviço gerenciado de segurança da informação), que objetivam assegurar os mais altos níveis de serviço quanto a predição, identificação, contenção e resposta aos incidentes, reduzindo ou mesmo evitando os impactos aos serviços da CONTRATANTE.
- 1.3. Para tal, o objeto a ser contratado abrangerá os seguintes processos:
 - 1.3.1. Governança, gestão de riscos e conformidade;
 - 1.3.2. Controles de segurança;
 - 1.3.3. Proteção das informações, privacidade e proteção de dados pessoais;
 - 1.3.4. Gestão de incidentes;
 - 1.3.5. Continuidade do negócio;
 - 1.3.6. Treinamento na compreensão e capacitação técnica;
 - 1.3.7. Profissional dedicado;
 - 1.3.8. Serviços técnicos especializados.

2. INFORMAÇÕES GERAIS

- 2.1. Todos os itens exigidos e especificados neste Termo de Referência constituem requisitos obrigatórios, devendo ser considerados nas diferentes fases de implementação e, por conseguinte, na execução dos serviços;
- 2.2. Em caso de eventuais ocorrências que demonstrem que os serviços não estejam sendo prestados a contento, a CONTRATANTE exigirá a imediata regularização de quaisquer desconformidades observadas, de modo que sejam preservados e mantidos os níveis de serviço contratados;

2.3. Considerando que a precificação da presente contratação depende de informações acerca do ambiente tecnológico da CONTRATANTE, e que o sigilo de tais informações é primordial para a manutenção da segurança institucional, os dados e informações de caráter sigiloso necessários ao entendimento do ambiente e ao adequado balizamento das propostas serão disponibilizados às interessadas **mediante solicitação formal e assinatura prévia do Termo de Confidencialidade e Não Divulgação;**

2.3.1. Para fins do disposto no subitem anterior, a CONTRATANTE disponibilizará, em caráter restrito e controlado, o documento denominado **“Infraestrutura de Tecnologia da Informação do MPRJ”**, o qual conterá informações sensíveis sobre o ambiente tecnológico, sendo **vedada sua juntada pública ao processo** e/ou sua divulgação a terceiros;

2.3.2. O documento referido no subitem 2.3.1 deverá ser solicitado por meio do endereço eletrônico **go.vistoria@mprj.mp.br**, observadas as orientações e os procedimentos de controle definidos pela CONTRATANTE;

2.3.3. Sem o fornecimento dessas informações de caráter sigiloso, devidamente controladas, a licitante poderá não dispor de elementos suficientes para balizar seus cálculos e estabelecer proposta compatível com a realidade do ambiente, motivo pelo qual a disponibilização controlada de tais dados visa assegurar maior precisão na formação dos preços e maior aderência técnica das propostas;

2.3.4. Considera-se, ainda, que diferentes soluções podem demandar formas de execução e ferramentas informatizadas distintas, razão pela qual a divulgação dessas métricas e informações sensíveis diretamente neste Termo de Referência tende a ser insuficiente, além de potencialmente comprometer a segurança institucional;

2.3.5. A realização de **visita técnica** às instalações da CONTRATANTE, **presencial ou virtual (Microsoft Teams)**, será **facultada** às licitantes interessadas, exclusivamente para fins de melhor compreensão do ambiente e esclarecimento de dúvidas relacionadas à execução do objeto, desde que preservado o sigilo das informações institucionais;

2.3.6. Caso a licitante opte pela realização da visita técnica, o agendamento deverá ser solicitado por e-mail ao endereço **go.vistoria@mprj.mp.br**,

contendo no assunto a expressão “**Visita Técnica – <número da licitação>**” e, no corpo da mensagem, as seguintes informações:

- 2.3.6.1. Empresa: Nome e CNPJ;
- 2.3.6.2. Contato: nome, telefone e endereço eletrônico;
- 2.3.6.3. Visitantes (profissionais técnicos designados pela empresa): Nome, identificação civil, endereço eletrônico;
- 2.3.6.4. Envio do Termo de Confidencialidade e Não Divulgação preenchido e assinado.
- 2.3.7. O agendamento somente será efetivado após o recebimento do Termo de Confidencialidade e Não Divulgação devidamente assinado, quando houver compartilhamento de informações sensíveis ou acesso ao documento “Infraestrutura de Tecnologia da Informação do MPRJ”;
- 2.3.8. A eventual realização de visita técnica **não constituirá requisito de habilitação**, nem condição obrigatória para participação no certame, servindo apenas como instrumento de apoio ao correto dimensionamento e elaboração da proposta;
- 2.3.9. As informações sensíveis disponibilizadas, seja por meio do documento “Infraestrutura de Tecnologia da Informação do MPRJ”, seja em visita técnica, deverão ser mantidas sob sigilo e utilizadas exclusivamente para elaboração da proposta e para os fins relacionados à presente contratação, sendo vedada qualquer forma de divulgação, reprodução ou compartilhamento não autorizado.
- 2.4. É vedada a subcontratação total ou parcial do objeto, a associação da CONTRATADA com outrem, a cessão ou transferência total ou parcial, bem como a fusão, cisão ou incorporação, salvo se expressamente admitido neste Termo de Referência e no instrumento convocatório;
 - 2.4.1. A CONTRATADA deverá dimensionar as soluções de segurança para suportar, sem perda de performance, **8.600 (oito mil e seiscentos) usuários e 10.000 (dez mil) ativos**, incluindo, entre outros, desktops, servidores, impressoras, switches, roteadores, pontos de acesso (APs), VoIP, TVs corporativas e demais equipamentos que possuam endereço IP atribuído;

- 2.4.2. Demais informações sobre o ambiente tecnológico da CONTRATANTE deverão ser mantidas em sigilo e somente poderão ser disponibilizadas às licitantes mediante a assinatura prévia do Termo de Confidencialidade e Não Divulgação, na forma prevista nos subitens 2.3 e seguintes.

3. DETALHAMENTO DOS SERVIÇOS

3.1. Considerações Iniciais

- 3.1.1. A presente contratação deverá ser entregue na modalidade de prestação de serviços.
- 3.1.2. A CONTRATADA é responsável por prover todos os softwares, hardwares e infraestrutura necessária para o funcionamento das soluções exigidas neste processo, salvo os equipamentos descritos explicitamente, que serão disponibilizados pela CONTRATANTE para hospedar os serviços inerentes ao atendimento do contrato;
- 3.1.3. A CONTRATADA deverá se beneficiar das soluções e equipamentos já em uso no ambiente do MPRJ, para coletar informações e apoiar a estratégia de defesa cibernética, bem como aumentar a quantidade e qualidade das informações para uma melhor postura de segurança;
- 3.1.4. Quaisquer informações coletadas durante a execução desse contrato, somente poderão ser divulgadas à terceiros após a aprovação formal da CONTRATANTE;
- 3.1.5. Todos os equipamentos e softwares utilizados pela CONTRATADA para a entrega deste serviço, quando for o caso e se necessário à execução das atividades de segurança, devem atender às especificações técnicas do objeto durante o prazo de vigência do contrato, incluindo garantia, manutenção, atualização dos produtos e monitoramento de segurança em regime 24x7 (vinte e quatro horas por dia, sete dias por semana);
- 3.1.6. Todos os **equipamentos e softwares** utilizados pela CONTRATADA para a entrega deste serviço, devem ser declarados de forma clara e objetiva, com a documentação técnica em PDF ou URL válida para verificação das especificações técnicas, na proposta cadastrada para a fase de lances deste processo, incluindo, minimamente, **fabricante, modelo, versão, forma de licenciamento, licenças estimadas, configuração e capacidades estimados**,

tamanho da solução em U's (no caso de equipamento a ser instalado no datacenter do MPRJ);

3.1.7. Todos os equipamentos e softwares utilizados pela CONTRATADA para fornecer este serviço devem ser acompanhados de documentações técnicas e de treinamento para a utilização das soluções pelas equipes técnicas da CONTRATANTE, conforme necessário e para o número de participantes conforme descrito no item 9;

3.1.8. A proposta apresentada deve ser complementada por planilha “ponto a ponto” de comprovação do atendimento da especificação das soluções informatizadas, indicando a documentação técnica (manual técnico, catálogo técnico, datasheet, folha de dados ou folha de especificações, artigo de conhecimento de suporte técnico e similares do fabricante), a página e/ou tópico onde se encontra cada informação, ou, alternativamente, imagens da console das soluções que comprovem o atendimento do requisito;

3.1.9. Durante a execução dos serviços, a CONTRATADA deverá disponibilizar o quantitativo de profissionais necessários para atender todos os perfis, buscando o normal desenvolvimento dos Serviços Gerenciados de Segurança;

3.1.10. A CONTRATADA deverá monitorar permanentemente e avaliar criticamente os serviços, traçando curvas de comportamento, definindo a volumetria média de acessos e identificando comportamentos não usuais, visando antecipar a identificação de incidentes de segurança, antes mesmo de impactarem nos serviços.

3.2. Modelo de atuação

3.2.1. O serviço deve ser prestado majoritariamente de forma remota;

3.2.2. As seguintes atividades deverão ser realizadas mediante atendimento presencial, nas instalações da CONTRATANTE:

3.2.2.1. Migração de versionamento ou modernização dos equipamentos gerenciados da CONTRATADA;

3.2.2.2. Atuação em incidentes massivos ou desastres;

3.2.2.3. Atuação em casos de inacessibilidade dos equipamentos gerenciados da CONTRATADA;

- 3.2.2.4. O local é especificado no documento Infraestrutura de Tecnologia da Informação do MPRJ.
- 3.2.3. O serviço deve ser provido através de uma infraestrutura de um **Centro de Operação de Segurança** da informação (**Security Operation Center**), também denominado **ambiente integrado de monitoramento e resposta a incidentes de segurança da informação**, incluindo minimamente dois ambientes na CONTRATADA, redundantes entre si e distantes, com pelo menos, 50 km (cinquenta quilômetros) de distância geodésica um do outro, localizados no Brasil, de modo que a indisponibilidade de um deles não afete a prestação dos SERVIÇOS GERENCIADOS DE SEGURANÇA;
- 3.2.4. Estes ambientes já devem estar em pleno funcionamento na data da diligência, de modo que a indisponibilidade de um deles não afete nenhum aspecto dos serviços prestados;
- 3.2.5. Os Centros de Operação de Segurança utilizados para a prestação do serviço deverão possuir obrigatoriamente as certificações ISO/IEC 27001 e ISO/IEC 27701 e, adicionalmente, uma das seguintes certificações: ISO/IEC 27000 ou ISO/IEC 9000 ou ISO/IEC 37001;
- 3.2.6. As certificações devem estar vigentes, serem emitidas em nome da CONTRATADA por organização independente acreditada pelo Inmetro ou por autoridade equivalente globalmente reconhecida;
- 3.2.7. Todos os ambientes utilizados para a prestação dos serviços deverão observar os requisitos de segurança e soberania de dados, devendo as informações do MPRJ permanecer armazenadas e processadas em território nacional;
- 3.2.7.1. Os Centros de Operação de Segurança (SOC) deverão estar fisicamente instalados no Brasil;
- 3.2.7.2. Será admitida a utilização de soluções baseadas em nuvem (SaaS), desde que:
- 3.2.7.2.1. garantam a proteção, confidencialidade e integridade das informações do MPRJ;
- 3.2.7.2.2. assegurem a residência dos dados em território nacional;

- 3.2.7.2.3. atendam integralmente aos requisitos de segurança estabelecidos neste documento.
- 3.2.7.3. Não serão aceitos Centros de Operação de Segurança (SOC) exclusivamente virtuais, integralmente baseados em nuvem ou sem estrutura física instalada no Brasil.
- 3.2.8. Além do **ambiente integrado de monitoramento e resposta a incidentes de segurança da informação**, a CONTRATADA deverá fazer uso de uma ferramenta de monitoramento que contemple uma console em nuvem, com a finalidade de que a mesma possa ser acessada, também, a partir do ambiente da CONTRATANTE e que seja possível se fazer o controle do serviço de monitoramento da operação de segurança a partir do ambiente da CONTRATADA e da CONTRATANTE;
- 3.2.9. Cada um dos **ambientes integrados de monitoramento e resposta a incidentes de segurança da informação** devem atender aos seguintes requisitos mínimos:
 - 3.2.9.1. Funcionar em regime de 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, e 365 (trezentos e sessenta e cinco) dias por ano;
 - 3.2.9.2. Possuir um profissional dedicado à operação das soluções de detecção e resposta aos incidentes com ao menos uma certificação do fabricante do produto que será adotado, não sendo necessário a presença física no ambiente da CONTRATANTE;
 - 3.2.9.3. Estar conectado aos Data Centers que hospedam os sistemas de suporte técnico, monitoramento, administração e gerenciamento através de múltiplas conexões de rede local ou WAN, de forma que a falha de uma conexão isoladamente não afete o acesso aos mesmos;
 - 3.2.9.4. Possuir estrutura central para visualização dos painéis dos sistemas de suporte técnico, monitoramento, administração e gerenciamento que permita que todos os profissionais visualizem eventos relevantes simultaneamente;
 - 3.2.9.5. Possuir UPS que suporte todos os equipamentos essenciais ao funcionamento, por, pelo menos, 30 minutos;

- 3.2.9.6. Utilizar sistema de gerenciamento por câmera, tipo CFTV, que viabiliza o rastreamento de pessoas dentro do ambiente da CONTRATADA e cujas imagens possam ser recuperadas por no mínimo 30 (trinta) dias;
- 3.2.9.7. Ter o acesso de entrada e saída dos visitantes registrado, com identificação individual, e constituído por pelo menos 02 (dois) fatores de autenticação;
- 3.2.9.8. O perímetro físico dos Centros de Operações de Segurança deve ser equipado com sensor de intrusão e alarmes contra acesso indevido;
- 3.2.9.9. Ser vigiado de forma ininterrupta por segurança física especializada em regime de 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, e 365 (trezentos e sessenta e cinco) dias por ano;
- 3.2.9.10. Ter componentes de segurança necessários para garantir a preservação dos dados em casos de incêndio e execução de plano de recuperação de catástrofes;
- 3.2.9.11. Não possuir campo físico visual externo das suas instalações, a fim de garantir que as informações exibidas em monitores estejam inacessíveis a leituras e a capturas externas, desautorizadas.

3.3. Ambiente da CONTRATADA

- 3.3.1. Os recursos físicos da CONTRATADA (prédio, salas, mesas e outros) poderão ser compartilhados com outros clientes, desde que:
 - 3.3.1.1. Toda a infraestrutura lógica que atende a CONTRATANTE seja separada dos demais clientes;
 - 3.3.1.2. Garantir que todos os profissionais alocados na execução dos serviços tenham firmado, previamente ao início de suas atividades, Termo de Ciência e Compromisso de Manutenção de Sigilo, no qual assumam expressamente as responsabilidades quanto à confidencialidade, ao uso adequado das informações institucionais e ao cumprimento das normas de segurança da informação aplicáveis;

- 3.3.1.3. O acesso ao ambiente da CONTRATANTE, pelos profissionais da CONTRATADA, deve ser realizado estritamente a partir das Centrais de Serviços certificadas da CONTRATADA;
 - 3.3.1.4. É vedado aos profissionais da CONTRATADA estabelecer um canal de comunicação, mesmo que através de VPN, ou acessar diretamente o ambiente da CONTRATANTE utilizando equipamentos que não estejam no ambiente certificado ou não tenham sido verificados e autorizados pela CONTRATADA;
 - 3.3.1.5. Em caso emergencial, desde que autorizado pela CONTRATANTE, o profissional poderá fazer uso de equipamento fora do ambiente da CONTRATADA, que tenham sido verificados e autorizados e sob a total responsabilidade da CONTRATADA, e com o devido acompanhamento da CONTRATANTE.
- 3.3.2. Conexão entre o **ambiente integrado de monitoramento e resposta a incidentes de segurança da informação** e a CONTRATANTE;
- 3.3.2.1. A CONTRATADA deverá disponibilizar, às suas expensas, links dedicados e redundantes para comunicação com seus Centros de Operação de Segurança (SOCs) e o ambiente do MPRJ, destinados à transmissão de logs, telemetria e atividades de gerenciamento, sendo vedada a utilização dos links de internet da CONTRATANTE para essa finalidade;
 - 3.3.2.2. O acesso aos painéis de monitoramento, consoles de controle e configuração dos serviços da CONTRATADA deverão utilizar esses links de comunicação dedicados.

3.4. Gerência de Serviços

- 3.4.1. A gestão deve conhecer os padrões internacionais do HDI (Help Desk Institute) seguindo todos os processos definidos pela CONTRATANTE, com comprovação desta aptidão;
- 3.4.2. Diariamente, no primeiro horário útil, a CONTRATADA deverá disponibilizar informações através de painel ou portal, sobre a saúde do ambiente, contemplando, no mínimo:
 - 3.4.2.1. Análise de risco;

- 3.4.2.2. Quantidade de vulnerabilidade identificadas;
 - 3.4.2.3. Total de vulnerabilidades no parque (categorizadas por risco);
 - 3.4.2.4. Novas vulnerabilidades identificadas;
 - 3.4.2.5. Indicador de compliance;
 - 3.4.2.6. Ameaças na Darkweb;
 - 3.4.2.7. Análise de incidentes;
 - 3.4.2.8. Alerta de incidentes globais;
 - 3.4.2.9. Total de incidentes identificados;
 - 3.4.2.10. Total de incidentes bloqueados;
 - 3.4.2.11. Eventuais impactos observados.
- 3.4.3. Entregar mensalmente relatórios gerenciais, incluindo níveis de serviço, atualizações de versões, principais incidentes e vulnerabilidade, estatísticas sobre desempenho e melhorias propostas, e demais recomendações, conforme as melhores práticas;
- 3.4.4. Entregar relatórios mensais dos resultados dos serviços prestados, com análise crítica clara elaborada pelos times técnicos da CONTRATADA;
- 3.4.4.1. Tais relatórios deverão ser confeccionados por equipes independentes, utilizando dupla validação das áreas de Cibersegurança e ambiente integrado de monitoramento e resposta a incidentes de segurança da informação, devendo conter minimamente:
 - 3.4.4.1.1. Análise de vulnerabilidades, incluindo categorização, severidade e recomendações dos controles de segurança necessários para correção;
 - 3.4.4.1.2. Descrição das ações realizadas;
 - 3.4.4.1.3. Contatos da CONTRATANTE acionados;
 - 3.4.4.1.4. Possíveis problemas aplicáveis;
 - 3.4.4.1.5. Apresentação das evidências apuradas;
 - 3.4.4.1.6. Fontes de pesquisa;
 - 3.4.4.1.7. Pontos positivos encontrados;
 - 3.4.4.1.8. Referências;
 - 3.4.4.1.9. Ferramentas utilizadas;

- 3.4.4.1.10. Apresentação da evolução de, no mínimo, 12 (doze) meses anteriores e do mês atual por meio de um gráfico.
- 3.4.5. Agendar reunião mensal presencial, ou remota, a critério e disponibilidade da CONTRATANTE, para apresentação dos resultados dos serviços prestados;
- 3.4.6. Realizar pesquisa de qualidade operacional trimestralmente, documentando e disponibilizando os resultados para a CONTRATANTE em reunião presencial, ou remota;
- 3.4.7. Rever periodicamente as políticas e processos do ambiente integrado de monitoramento e resposta a incidentes de segurança da informação a fim de contribuir com a melhoria contínua da operação, de forma documentada e em conformidade com as melhores práticas do ITIL;
- 3.4.8. Disponibilizar dashboards de acompanhamento da operação do ambiente integrado de monitoramento e resposta a incidentes de segurança da informação que permitam a validação dos indicadores acordados;
- 3.4.9. Apoiar de forma consultiva para a melhoria contínua da segurança do ambiente;
- 3.4.10. Confeccionar relatórios técnicos pontuais sob demanda da CONTRATANTE.

3.5. Canais de Comunicação

- 3.5.1. Para abertura de solicitações, a CONTRATADA deverá disponibilizar 03 (três) tipos de canais de comunicação, a saber:

Grupo de Tecnologia	Classificação
Linha de telefonia gratuita (0800) de cobertura nacional	Tipo 1
E-mail com domínio registrado e de propriedade da CONTRATADA.	Tipo 2
Ferramenta de Service Desk ou Sistema de ITSM (<i>Information Technology Service Management</i> - Gerenciamento de Serviços de TI).	Tipo 3

Tabela 1 - TIPOS DE CANAIS DE COMUNICAÇÃO

- 3.5.1.1. Independente do canal de comunicação utilizado pela CONTRATANTE, as solicitações devem ser convergidas, atualizadas, resolvidas e concentradas em um único sistema de ITSM do inglês

Information Technology Service Management (Gerenciamento de Serviços de TI). Ou seja, caso a CONTRATANTE realize a abertura de uma nova solicitação de serviço via linha telefônica gratuita, por exemplo, em seguida a mesma deve constar no sistema de ITSM;

3.5.1.2. Sobre o canal de comunicação do tipo 1: via linha telefonia gratuita (0800), tais ligações obrigatoriamente devem ser atendidas e/ou recepcionadas por uma interface humana, não sendo permitida a utilização de URA (Unidade de Resposta Audível), e/ou qualquer uso de atendimento eletrônico;

3.5.1.3. Para um eventual cenário de crise, ou seja, onde o negócio fim da CONTRATANTE estiver sendo fortemente afetado por um problema envolvendo a segurança da informação, a CONTRATADA deverá disponibilizar uma sala de videoconferência virtual de sua propriedade, onde a qualquer tempo poderá ser utilizada para reuniões emergenciais para tratamento de crises;

3.5.1.3.1. Tal sala deve estar disponível via internet e seu acesso deve obrigatoriamente ser criptografado, utilizando protocolo SSL (Secure Socket Layer).

3.5.2. Ferramenta de Service Desk

3.5.2.1. Disponibilizar uma Ferramenta de Service Desk para o registro das demandas e tickets que devem ser tratados pelo ambiente integrado de monitoramento e resposta a incidentes de segurança da informação;

3.5.2.2. Todas as solicitações deverão ocorrer, por meio da interface web do portal do cliente, segura, através de sistema próprio e que contenha as seguintes características:

3.5.2.2.1. Módulos de incidente/solicitação, requisição de mudança, eventos, problemas, itens de configuração (IC), Contratos, Clientes, Fornecedores, Empresas, acordos de nível de serviço (SLA), Criticidades, Analistas, Base de conhecimento, Usuários e Avisos;

3.5.2.2.2. Realizar notificações por e-mail;

3.5.2.2.3. Gerenciamento de Catálogo de Serviços;

3.5.2.2.4. Integração com a ferramenta de monitoramento.

- 3.5.2.3. A ferramenta de Service Desk da CONTRATADA deve permitir o acompanhamento dos chamados em aberto bem como a consulta dos chamados já finalizados (BASE HISTÓRICA DE INCIDENTES) e validação do chamado antes do encerramento do mesmo;
- 3.5.2.4. Os serviços, tanto de suporte quanto de consultoria, requerem solicitação exclusiva através dos contatos cadastrados, utilizando os métodos delineados abaixo, acessíveis em qualquer momento;
- 3.5.2.5. A CONTRATADA deverá comunicar o usuário final, ou seu superior imediato, conforme orientado no plano de comunicação enviado pela CONTRATANTE, nos casos em que seja necessário realizar o bloqueio de suas credenciais e acessos, em ações punitivas ou de resposta aos incidentes;
- 3.5.2.6. As requisições de serviços relacionadas a atividades sensíveis, tais como desbloqueio de contas, troca de senhas ou registro de autenticação de múltiplo fator no Active Directory, deverão ser registradas na ferramenta de Service Desk e permanecerão sob a gestão exclusiva da CONTRATANTE;
- 3.5.2.6.1. A atuação da CONTRATADA, quando necessária, limitar-se-á ao suporte técnico especializado, à análise e à recomendação de ações corretivas ou preventivas, bem como à execução pontual de procedimentos, desde que previamente autorizados pela CONTRATANTE, não se caracterizando, em qualquer hipótese, a transferência da administração, governança ou controle do serviço de diretório institucional.

3.6. Horário de atendimento

- 3.6.1. Os SERVIÇOS GERENCIADOS DE SEGURANÇA, devem, obrigatoriamente, serem executados, ofertados, e estarem acessíveis à CONTRATANTE em regime de 24 (vinte quatro) horas por dia, 07 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano, durante todo o período de vigência do contrato;

- 3.6.2. Todo o atendimento deve ser iniciado por profissionais da CONTRATADA, que estejam em horário de trabalho no momento do atendimento. Não sendo permitido o uso de funcionários no chamado “Regime de Plantão”, “Sobreaviso” e/ou sistemas similares, onde o funcionário apenas passa a trabalhar no momento do incidente.).

3.7. Acompanhamento do Contrato

- 3.7.1. Os serviços executados pela CONTRATADA estarão sujeitos à aceitação pela CONTRATANTE, mediante aferição dos correspondentes entregáveis, visando garantir que os mesmos satisfizeram os prazos e condições o padrão de qualidade exigido, considerando as disposições contidas neste documento;
- 3.7.2. Na ocasião da apresentação do prestador de serviço, os Fiscais designados para acompanhar o contrato deverão prover a verificação da conformidade da documentação apresentada às normas do CONTRATANTE e às exigências do Termo de Referência;
- 3.7.3. Na ocasião do recebimento dos entregáveis, os seguintes procedimentos serão realizados pelos Fiscais designados para acompanhar o contrato:
- 3.7.3.1. Recebimento dos entregáveis através do preenchimento do Termo de Recebimento Provisório e entrega ao preposto da CONTRATADA;
 - 3.7.3.2. Verificação do cumprimento da qualidade esperada na prestação dos serviços no período de referência, em conformidade com os Níveis Mínimos de Serviço (NMS) definido neste documento;
 - 3.7.3.3. Preenchimento do Termo de Recebimento Definitivo e da Autorização para Emissão de Nota Fiscal/Fatura e entrega a CONTRATADA.
- 3.7.4. O Relatório Mensal de Execução de Serviços, emitido pela CONTRATADA, deverá conter informações completas sobre os serviços prestados, incluindo no mínimo:
- 3.7.4.1. A situação atualizada do projeto de implantação;
 - 3.7.4.2. As atividades realizadas no período de referência juntamente com o acumulado de atividades já realizadas;

- 3.7.4.3. As atividades previstas, mas não realizadas no período de referência juntamente com a descrição detalhada sobre as causas do não cumprimento do cronograma previsto;
 - 3.7.4.4. Dificuldades encontradas e o plano de ação utilizado para solução;
 - 3.7.4.5. Cronograma atualizado contendo prazos estimados e realizados para cada uma das atividades;
 - 3.7.4.6. A avaliação do nível mínimo de serviço atingido e plano de ação para melhoria da qualidade;
 - 3.7.4.7. Informações detalhadas sobre o desempenho e os serviços executados para análise gerencial;
 - 3.7.4.8. Informações dos projetos e contratações em que houve o seu apoio técnico.
- 3.7.5. A Equipe de Gestão da Contratação elaborará documento interno obrigatório de acompanhamento mensal do contrato para registro de ocorrências durante a execução de um contrato, onde será avaliado o desempenho da CONTRATADA no que tange aos serviços prestados;
- 3.7.6. O documento interno obrigatório de acompanhamento mensal do contrato deverá fazer parte do correspondente processo de pagamento das faturas;
- 3.7.7. A Equipe de Gestão da Contratação exercerá a fiscalização permanente sobre a qualidade dos serviços prestados e atuação da CONTRATADA, inclusive quanto ao cumprimento da legislação, apontando todas as irregularidades verificadas, sem prejuízo da obrigação da CONTRATADA de gerenciar, por meio de seu preposto, a execução prestada por seus subordinados, dentro do critério de periodicidade que entender como necessário ao cumprimento de suas responsabilidades.

3.8. Gerente Técnico de Conta (TAM)

- 3.8.1. A CONTRATADA deverá contar com Gerente Técnico de Conta (TAM), para realizar o acompanhamento das entregas através de reuniões e servir como ponto focal da CONTRATANTE;

3.8.2. Deverá estabelecer contato de forma quinzenal através de reuniões presenciais ou remotas, à critério da CONTRATANTE;

3.8.2.1. Entregável: Ata de reunião.

3.8.3. Deverá ser feito o acompanhamento periódico dos indicadores listados no contrato para antecipar desvios e corrigi-los antes que saiam das conformidades exigidas;

3.8.3.1. Entregável: Acompanhamento periódico a partir das ferramentas de registro de chamado ou medição.

3.8.4. Todos os entregáveis do contrato são acompanhados pelo TAM – desde o SLA de atendimento à relatórios, a fim de garantir a conformidade e cadência correta estabelecida;

3.8.4.1. Entregável: Checklist periódico dos entregáveis do projeto, conforme RFP, TR, proposta técnica e afins.

3.8.5. Deverá manter a Matriz de Comunicação atualizada: quem a CONTRATADA deve acionar e quem a CONTRATANTE deve acionar em casos específicos ou de escalação conforme matriz de acionamento;

3.8.5.1. Entregável: Documento formal de Matriz de Acionamento conforme formato pré-estabelecido.

3.8.6. Deve acompanhar o cumprimento das obrigações legais da CONTRATADA;

3.8.6.1. Entregável: relatórios de ponto, execução de obrigações trabalhistas de todos os funcionários com dedicação exclusiva à execução do contrato.

3.9. Níveis mínimos de serviço (NMS)

3.9.1. Características Gerais:

3.9.1.1. Os níveis mínimos de serviços são critérios objetivos e mensuráveis que visam aferir e avaliar diversos fatores relacionados com os serviços contratados, como a qualidade, desempenho, disponibilidade, abrangência/cobertura e segurança;

- 3.9.1.2. Os serviços serão medidos e apurados mensalmente, de modo a alcançar as respectivas metas exigidas, conforme tabela do item 3.9.3;
- 3.9.1.3. Serão aplicadas glosas, sob forma de desconto, à CONTRATADA referentes a falhas nos serviços executados ou em sua infraestrutura, que afetem a qualidade, desempenho, disponibilidade, abrangência/cobertura e segurança dos serviços, quando a responsabilidade for da CONTRATADA;
- 3.9.1.4. A aplicação de glosa pelo não atendimento aos Índices de Mediação de Resultado (IMR), onde se aplicar, poderá ser objeto de contestação, por meio do oferecimento de elementos que visem comprovar a não responsabilidade, por parte da CONTRATADA;
- 3.9.1.5. O valor do desconto, decorrente das glosas descritas nesta seção, e detectadas, conforme disposto neste documento, deverá ser concedido na fatura do mês de referência da prestação do serviço, em que foi identificado o não atendimento aos níveis de qualidade de serviço determinados neste documento;
- 3.9.1.6. O faturamento somente poderá ser emitido pela CONTRATADA e atestado pelo fiscal do contrato, após a aferição dos descontos a serem concedidos, decorrentes das glosas aplicadas, os quais deverão ser lançados na fatura do mês de prestação do serviço onde foram detectadas as ocorrências que ensejaram o não atendimento aos níveis de qualidade de serviço determinados neste documento;
- 3.9.1.7. A qualidade da execução do objeto contratado será avaliada por de Níveis Mínimos de Serviço (NMS), que indicarão a faixa de ajuste no pagamento, de modo que o CONTRATANTE pague apenas pelo que efetivamente lhe foi entregue;
- 3.9.1.8. O NMS é composto de indicadores objetivos indicados no item 3.9.2;
- 3.9.1.9. As glosas decorrentes das faixas de ajustes oriundas dos indicadores aferidos que compõem Índice de Medição de Resultado (IMR) não configuram sanção;

3.9.1.10. As glosas não ultrapassarão 10% (dez por cento) do valor mensal do serviço;

3.9.1.11. Independentemente da glosa aplicada, poderá ser aberto procedimento apuratório para aplicação de sanção mediante justificativa fundada em prejuízos ou transtornos causados em decorrência da entrega imperfeita do objeto contratado.

3.9.2. Nível Mínimo de Serviço para início do atendimento

3.9.2.1. Criticidade Alta: Início de atendimento em até 0,5 (meia) hora;

3.9.2.2. Criticidade Média: Início de atendimento em até 04 (quatro) horas;

3.9.2.3. Criticidade Baixa: Início de atendimento em até 08 (oito) horas.

3.9.3. Instrumento de Medição de Resultado

INSTRUMENTO DE MEDIÇÃO DE RESULTADO			
INDICADOR	MÉTRICAS	META MENSAL	GLOSA POR DESCUMPRIMENTO DA META
Índice de disponibilidade do ambiente de segurança entregue pela CONTRATADA.	(Total de tempo com disponibilidade no mês) / (Total de tempo no mês) * 100.	>= 99,7 %	0,40%
Triagem de incidentes de segurança.	Tempo = Hora da triagem – Hora de entrada do evento de segurança <= 15 minutos.	>= 99,5 %	0,25%
Resposta para os incidentes de segurança com gravidade considerada ALTA pela CONTRATANTE.	Tempo = Hora do início da resposta – hora da triagem <= 0,5 hora.	>= 99,5 %	0,25%
Resposta para os incidentes de segurança com gravidade considerada MÉDIA pela CONTRATANTE.	Tempo = Hora do início da resposta - hora da triagem <= 4 horas.	>= 99,5 %	0,25%
Resposta para os incidentes de segurança com gravidade considerada BAIXA pela CONTRATANTE.	Tempo = Hora do início da resposta – hora da triagem <= 8 horas.	>= 99,5 %	0,25%

Correção de incidentes nos serviços de segurança, que façam parte do escopo deste projeto, em caso de Indisponibilidade.	Tempo = Hora do restabelecimento – Hora do início da indisponibilidade ≤ 2 horas	≥ 99,5 %	0,25%
Indicação de solução de controle para tratamento de grave vulnerabilidade ou ameaça emergente, nos equipamentos e softwares utilizados pela CONTRATADA para entrega dos Serviços. Disponibilizados pelos fabricantes.	Tempo = Hora de conclusão do planejamento da requisição de mudança – hora de disponibilização dos patches e hot- fixes ou divulgação de grave vulnerabilidade ou ameaça emergente ≤ 72 horas.	≥ 99,5 %	0,25%
Aplicação de patches e hotfixes ou atualização dos firmwares e/ou softwares das soluções entregues. Sem gravidade.	Tempo = Hora de conclusão do planejamento da requisição de mudança – hora de disponibilização dos patches e hot- fixes ou atualização de firmware ≤ 96 horas.	≥ 99,5 %	0,25%
Resposta a incidentes- tempo para responder a um incidente de phishing relatado pelo cliente no portal - Incidentes desconhecidos.	Iniciar análise em até 30 minutos.	≥ 99,7 %	0,20%
Identificação de Vulnerabilidades de Severidade Alta – Entrega e apresentação do Plano de Remediação.	Em até 48 horas após o fim da varredura.	≥ 99,7 %	0,20%
Simulação de ataque phishing – Entrega do Relatório.	Em até 5 dias após o fim do teste.	≥ 99,7 %	0,20%
Alerta de Todas as Vulnerabilidades Encontradas – Entrega do Relatório semanal.	Entrega todas às terças-feiras.	≥ 99,7 %	0,20%
Alerta de Vulnerabilidades – Vulnerabilidades críticas.	Em até 24 horas após publicação.	≥ 99,7 %	0,20%
Tratamento de Incidentes Críticos Detectados.	Em até 20 Minutos para iniciar o tratamento.	≥ 99,7 %	0,20%

Abertura de chamados de suporte.	Tempo = Hora de abertura do chamado – hora da triagem ≤ 15 minutos.	≥ 99,7 %	0,20%
Finalizar a requisição de serviço ou incidente sem a devida resolução ou sem realizar os testes necessários para aferir a efetiva resolução.	Quantidade de requisições finaliza- das com resolução/ quantidade de requisições finalizadas * 100.	≥ 99,7 %	0,20%
Finalizar uma requisição de serviço sem documentar os procedi- mentos executados para atendimento da solicitação.	Quantidade de requisições finaliza- das com documentação / quantidade de requisições finalizadas * 100.	≥ 99,0%	0,20%
Relatório de Investigação e Remediação do Incidente.	8 Horas (a partir da detecção do incidente).	≥ 99,7 %	0,20%
Comunicação de incidentes aos gestores de TI do CONTRATANTE.	Tempo = Hora da comunicação – hora da triagem ≤ 1 hora	≥ 99,7 %	0,20%
Finalizar um incidente sem documentar a causa, a solução de contorno (se houver) ou os procedimentos adotados para solução.	Quantidade de incidentes finaliza- dos sem documentar a causa, a solução de contorno (se houver) ou os procedimentos adotados para solução / Quantidade de incidentes finalizados * 100.	≥ 99,5 %	0,20%
Finalizar um problema sem documentar a investigação realizada, a causa-raiz ou a solução aplicada.	Quantidade de problemas finaliza- dos sem documentar a investigação realizada, a causa- raiz ou a solução aplicada / Quantidade de problemas finalizados * 100.	≥ 99,5 %	0,20%
Apresentar mensalmente relatório do plano de tratamento de vulnerabilidades, indicando as ações mais efetivas para redução dos riscos.	Unidade.	100%	0,20%

3.10. Equipe técnica e Capacitação dos Profissionais

- 3.10.1. A CONTRATADA é responsável por dimensionar e manter equipe técnica em quantitativo e capacitação compatíveis com a prestação de serviço, a fim de garantir que as atividades sejam executadas dentro dos NMS e sem qualquer interrupção, independentemente de ocorrências de férias, descansos semanais, licenças, greves, paralisações do transporte público, faltas ao serviço e desligamentos de empregados;
- 3.10.2. A equipe deve contar com profissionais com habilidade de comunicação na língua inglesa, para leitura, escrita e conversação, tendo em vista frequentemente ser o idioma padrão em manuais, fóruns de dúvidas, bases de conhecimento e canais de atendimento de fabricantes;
- 3.10.3. A CONTRATADA deve prever e substituir imediatamente qualquer profissional por outro de mesmo perfil no caso de falta, impedimentos, férias e outras questões trabalhistas;
- 3.10.4. A CONTRATADA deve retirar dos serviços qualquer colaborador que, a critério da CONTRATANTE, seja julgado inconveniente ao bom andamento dos trabalhos;
- 3.10.5. A fim de garantir a prestação do serviço em conformidade com o framework ITIL, a CONTRATADA deve possuir ao menos um profissional com a certificação ITIL Foundation;
- 3.10.6. A fim de garantir a condução do projeto de acordo com as melhores práticas do mercado, a CONTRATADA deve possuir ao menos um profissional pós-graduado em Gerência de Projetos ou com a certificação PMI PMP;
- 3.10.7. A fim de garantir o conhecimento em Segurança da Informação, a CONTRATADA deve possuir ao menos um profissional com a certificação CISSP (Certified Information Systems Security Professional) ou CISM (Certified Information Security Manager);
- 3.10.8. A fim de garantir o conhecimento técnico em Segurança da Informação, a CONTRATADA deve possuir ao menos um profissional com a certificação Security+;

- 3.10.9. A fim de garantir a existência de profissional com experiência de hacker ético, fundamental em momentos de crise de segurança, a CONTRATADA deve possuir ao menos um profissional com a certificação CEH, OSCP ou equivalente;
- 3.10.10. A CONTRATADA deverá, para fins de execução contratual, manter equipe técnica compatível com os requisitos estabelecidos neste Termo de Referência, devendo apresentar à CONTRATANTE, sempre que solicitado ou no início da execução contratual, a comprovação da qualificação dos profissionais, mediante apresentação de currículos e certificações exigidas, todas com validade vigente;
 - 3.10.10.1. A CONTRATADA deverá indicar, de forma clara, as atribuições técnicas de cada profissional em relação às principais atividades do objeto, tais como monitoramento, análise de eventos, resposta a incidentes, gestão de vulnerabilidades e demais funções correlatas, conforme aplicável;
 - 3.10.10.2. A comprovação do vínculo dos profissionais com a CONTRATADA poderá ser exigida no momento da assinatura do contrato ou durante a execução contratual, nos termos da legislação aplicável.
- 3.11. **Implantação, mudanças e adoção tecnológica**
 - 3.11.1. A CONTRATADA deve executar no prazo máximo de **60 dias corridos**, a contar da data da Ordem de Serviço, as atividades de planejamento, instalação/adoção tecnológica, implantação do serviço, configuração e elaboração de documentação técnica, em conformidade com este Termo de Referência;
 - 3.11.2. A CONTRATADA deverá apresentar um Gerente de Projetos que ficará responsável por:
 - 3.11.2.1. Planejar as atividades;
 - 3.11.2.2. Elaborar cronograma para as atividades que deverá ser aprovado pela CONTRATANTE;
 - 3.11.2.3. Acompanhar a execução das atividades;
 - 3.11.2.4. Deverá atuar em conjunto com o Gerente Técnico da Conta (TAM);

- 3.11.2.5. Deverá realizar reuniões periódicas de acompanhamento das atividades, apresentando a ata da reunião em até 1 (um) dia útil.
- 3.11.3. Todas as atividades e documentação apresentadas deverão ser previamente aprovadas pela CONTRATANTE;
- 3.11.4. É responsabilidade da CONTRATADA o levantamento, junto à CONTRATANTE, de todas as informações necessárias para implantação/adoção dos itens de serviço, incluindo topologia e configuração atual, processos de trabalho em execução e locais de execução dos serviços;
- 3.11.5. **A implantação, configuração e manutenção das soluções e serviços é responsabilidade da CONTRATADA**, com anuência, orientação e acompanhamento da CONTRATANTE e deverá ser executada por profissional certificado na solução ou serviço;
- 3.11.6. Durante todo o período do Contrato a empresa deverá possuir pelo menos um profissional certificado pelo fabricante e responsável em cada solução deste documento;
- 3.11.7. É de responsabilidade da CONTRATANTE fornecer todas as informações necessárias do seu ambiente tecnológico;
- 3.11.8. Após a ativação dos serviços, deve ser entregue à CONTRATANTE documentação de “as-built” de cada serviço, contendo, no mínimo, as seguintes informações:
- 3.11.8.1. Descrição dos serviços implantados;
 - 3.11.8.2. Descrição da topologia física, após a ativação dos serviços, dos ambientes onde estão hospedados os equipamentos, softwares e soluções entregues pela CONTRATADA;
 - 3.11.8.3. Dados dos equipamentos e softwares, incluindo configurações, números de série, versões e licenças;
 - 3.11.8.4. Parâmetros de configuração, operação, instalação, manutenção, atualização e correto funcionamento dos equipamentos e softwares;

- 3.11.8.5. Definição de responsabilidades e matriz de acionamento, deixando explícito que a manutenção e gerência do hardware e softwares e administração da solução, são de responsabilidade da CONTRATADA;
- 3.11.8.6. Recursos de alta disponibilidade;
- 3.11.8.7. Procedimentos para abertura e atendimento a chamados;
- 3.11.8.8. Procedimentos de recuperação de equipamentos;
- 3.11.8.9. Rotinas de backup e restore dos equipamentos, softwares e configurações implantadas, deixando explícito que a manutenção e gerência do hardware e softwares e administração da solução, são de responsabilidade da CONTRATADA;
- 3.11.8.10. Rotinas periódicas configuradas;
- 3.11.8.11. Documentação dos processos de trabalho associados ao item;
- 3.11.8.12. Desenho dos racks onde estão instalados os equipamentos;
- 3.11.8.13. Definição de padrões porventura existentes na solução (ex. padrão de nome de objetos).
- 3.11.9. A CONTRATADA, como parte da execução do Serviço de Operação e Atendimento de Requisições, deverá realizar, nos **primeiros 40 (quarenta) dias** de execução deste serviço, uma avaliação completa do ambiente da CONTRATANTE (Assessment de Segurança), com o objetivo identificar lacunas ou oportunidades de melhoria (Gap Analysis) e determinar a maturidade dos controles de segurança da CONTRATANTE;
- 3.11.10. O Assessment de Segurança e o GAP Analysis deverá ser realizado utilizando como base um dos seguintes frameworks de segurança: NIST ou CIS, devendo o planejamento ser antecipadamente aprovado pela CONTRATANTE;
- 3.11.11. A CONTRATADA, após o levantamento inicial das lacunas ou falhas de segurança da informação no ambiente da CONTRATANTE, deverá elaborar, coordenar e supervisionar um plano de ação em conjunto com a CONTRATANTE, priorizando as falhas consideradas mais críticas;

- 3.11.12. A CONTRATADA deverá seguir o processo de mudança estabelecido pela CONTRATANTE;
- 3.11.13. Todos os serviços previstos neste processo deverão ser implantados, documentados e revisados pela CONTRATADA, seguindo a metodologia ITIL4;
- 3.11.14. A CONTRATADA, sempre que solicitada, deverá estar disponível para participar das reuniões internas da CONTRATANTE para prestar informações sobre os ambientes e serviços por ela executados;
- 3.11.15. Mudanças que envolvam procedimentos complexos, englobando diversas equipes ou empresas contratadas e acarretando riscos de interrupção dos serviços considerados prioritários, devem ser tratadas como projetos a serem elaborados e supervisionados pelo Gerente de Projetos designado pela CONTRATADA;
- 3.11.16. A CONTRATADA deverá apresentar ao CONTRATANTE o planejamento de quaisquer mudanças no ambiente, conforme níveis de controle estabelecidos, para todas as mudanças apresentadas;
- 3.11.17. Todos os serviços de manutenção corretiva e preventiva são considerados de natureza contínua e deverão minimizar a necessidade de parada do ambiente em produção;
- 3.11.18. Se alguma solução proposta envolver o uso de SGBD – Sistema Gerenciador de Bancos de Dados, este deve ser descrito em detalhes e fornecido como parte integrante da solução, incluído no custo total, e não pode depender da infraestrutura de servidores virtuais da CONTRATANTE;
- 3.11.19. Se alguma solução proposta exigir servidores virtuais ou appliances virtuais, esses devem ser especificados em detalhes e fornecidos como parte integrante incluído no custo total da solução, sem depender da infraestrutura de servidores virtuais da CONTRATANTE;
- 3.11.20. Se alguma solução proposta exigir armazenamento de informações geradas pela solução implantada, esses devem ser especificados em detalhes e fornecidos como parte integrante incluído no custo total da

solução, sem depender da infraestrutura de servidores virtuais ou dispositivos de armazenamento da CONTRATANTE;

- 3.11.21. Os serviços deverão ser executados por profissionais habilitados, com base em programas de formação e/ ou certificações oficiais, conforme os requisitos específicos para o perfil profissional.

3.12. Requisitos de Segurança da CONTRATADA

- 3.12.1. Respeitar os critérios de sigilo, aplicáveis aos dados, informações e às regras de negócios relacionados com a prestação do serviço contratado;
- 3.12.2. Todas as informações transmitidas pela CONTRATANTE para a CONTRATADA e aos seus funcionários são de caráter confidencial e não poderão ser transmitidas ou facilitadas a quem quer que seja, sem expressa autorização do CONTRATANTE;
- 3.12.3. Deverá ser mantida a confidencialidade das informações obtidas em razão da execução do contrato.

3.13. Soluções Informatizadas e Ferramentas fornecidas

- 3.13.1. Não serão aceitas ferramentas gratuitas, desenvolvidas pela, ou para, própria LICITANTE e/ou baseadas em softwares projetados para uso genérico, devendo estas serem providas por fabricantes amplamente consolidados no mercado;
- 3.13.2. Todas as ferramentas fornecidas como parte das soluções informatizadas devem contar com serviços plenos de sustentação, conforme a seguir;
- 3.13.2.1. A sustentação, administração, operação, suporte técnico e atualização das soluções informatizadas fornecidas pela CONTRATADA, bem como qualquer outra que se faça necessária para o pleno e adequado atendimento ao escopo e requisitos, serão serviços de natureza continuada de responsabilidade da CONTRATADA;
- 3.13.2.2. Todas as soluções Informatizadas devem possuir os serviços de licenciamento ou subscrição, garantia, suporte técnico e atualização oficiais do fabricante, com níveis de serviço adequados e compatíveis com os dos serviços envolvidos, que

devem estar contratados e disponíveis a partir da implantação da respectiva solução e durante toda a vigência do contrato;

- 3.13.2.3. As soluções informatizadas devem atender às especificações técnicas do objeto durante o prazo de vigência do contrato;
- 3.13.2.4. As soluções informatizadas não podem constar, no momento da apresentação da proposta comercial, em listas de end-of-sale, end-of-support, end-of-life ou similares do fabricante, e não podem ter previsão de descontinuidade de fornecimento, suporte ou vida pelo menos até o fim da vigência prevista para o contrato;
- 3.13.2.5. Em caso de descontinuação inesperada das tecnologias específicas implementadas para este contrato e caso seja cessado o suporte e a garantia do fabricante, a CONTRATADA é responsável por assegurar a evolução da solução, mesmo que isso envolva a substituição do fabricante, sem custo adicional para a CONTRATANTE. Tal medida deve ser acompanhada pela elaboração de um projeto de migração, sujeito à aprovação da CONTRATANTE;
- 3.13.2.6. As soluções informatizadas devem ser instaladas em sua versão mais estável e atualizada;
- 3.13.2.7. A CONTRATADA deverá cumprir todos os termos e condições do contrato de licenciamento dos respectivos fabricantes das soluções informatizadas, cuidando do adequado dimensionamento quantitativo e qualitativo das licenças necessárias para a prestação dos serviços e aderência ao ambiente da CONTRATANTE, mantendo a conformidade com os direitos de propriedade intelectual;
- 3.13.2.8. A CONTRATADA deve comprovar, na contratação e durante toda a vigência do contrato, que tenha, junto ao fabricante de cada ferramenta das soluções informatizadas, amplo e irrestrito acesso aos recursos e serviços de suporte técnico bem como à plenitude de capacidades e efetividade da ferramenta, prestados diretamente pelo fabricante, como centros e laboratórios de inteligência, investigação, diagnóstico, análise e automação, dentre outros aplicáveis;

- 3.13.2.9. A CONTRATADA assegurará garantia integral e perfeito funcionamento das soluções informatizadas pelo período de vigência do contrato.

4. GOVERNANÇA, GESTÃO DE RISCOS E CONFORMIDADE

4.1. Características Gerais

- 4.1.1. A CONTRATADA deverá prestar serviços de Governança, Risco e Conformidade (GRC), com amplo apoio e suporte técnico e metodológico ao CONTRATANTE, em segurança da informação, visando apoiar na melhoria e atingimento das metas estratégicas e objetivos da CONTRATANTE, incluindo:

- 4.1.1.1. Conformidade com a legislação, normativos e melhores práticas da CONTRATANTE;
- 4.1.1.2. Elevação da maturidade e melhoria contínua posicionando a CONTRATANTE em um nível de excelência na Governança, Gestão de Risco e Conformidade;
- 4.1.1.3. Estruturar, planejar, implementar, controlar, monitorar e evoluir arcabouços e instrumentos do sistema de gestão de segurança da informação (SGSI) e do sistema de gestão de continuidade de negócios (SGCN) com foco em Tecnologia da Informação;
 - 4.1.1.3.1. Alinhado ao ISO/IEC 27014, buscando garantir que a governança da segurança esteja bem integrada e alinhada com os objetivos estratégicos;
 - 4.1.1.3.2. Alinhado aos ISO/IEC 27001, 27005 e 31000, buscando fornecer uma abordagem para identificar e mitigar riscos em toda a organização;
 - 4.1.1.3.3. Alinhado ao ISO/IEC 37301, buscando a conformidade com leis e regulamentos e ajudando a estabelecer um sistema robusto de gestão de conformidade.
- 4.1.1.4. Estabelecer segurança da informação abrangente e integrada em toda a organização;

- 4.1.1.5. Tomar decisões usando uma abordagem baseada em risco;
- 4.1.1.6. Definir o direcionamento de iniciativas e aquisições;
- 4.1.1.7. Assegurar a conformidade com os requisitos internos e externos;
- 4.1.1.8. Promover uma cultura positiva de segurança;
- 4.1.1.9. Assegurar que o desempenho da segurança atenda aos requisitos atuais e futuros da entidade.

4.2. Gestão de políticas e procedimentos de segurança

- 4.2.1. A CONTRATADA deverá propor, elaborar, analisar, revisar e melhorar continuamente as políticas, estratégias, planos, processos e procedimentos de segurança da informação da CONTRATANTE, com base nas necessidades, na legislação e nos normativos vigentes aplicáveis, bem como nas melhores práticas de mercado, visando orientar e sustentar, em termos normativos e regulatórios, a efetividade e eficácia das operações e práticas de segurança cibernética e consolidar um sistema de gestão de segurança da informação (SGSI);
 - 4.2.1.1. Deve haver um ciclo de revisão e melhoria contínua de periodicidade máxima semestral para todas as políticas, processos, planos, métricas e indicadores.

4.3. Conscientização dos colaboradores

- 4.3.1. Deverá ser desenvolvido um projeto com o intuito de ajustar e/ou aprimorar a cultura de segurança da informação dentro da CONTRATANTE, abordando conceitos de boas práticas e a política e normas de segurança em vigor. Tal projeto deve contemplar:
 - 4.3.1.1. Planejamento:
 - 4.3.1.1.1. A fim de garantir que o Plano de Conscientização esteja adequado ao contexto corporativo, antes do início das ações, a Política de Segurança da Informação (PSI) da CONTRATANTE deverá ser analisada, sendo então selecionados seus pontos chave;

- 4.3.1.1.2. Adicionalmente, deverão ser consideradas no planejamento questões como o modelo corporativo de comunicação, o histórico de incidentes de segurança, eventuais exigências de clientes e/ou parceiros de negócio, as leis e regulamentações aplicáveis, entre outros;
- 4.3.1.1.3. Todas estas questões deverão ser direcionadoras para a seleção dos temas e a forma de comunicação.
- 4.3.1.2. Cumprindo o objetivo de fortalecer a cultura de segurança da informação na CONTRATANTE, a CONTRATADA deverá, mensalmente:
 - 4.3.1.2.1. Enviar e-mail para todos os colaboradores, contendo dicas de segurança baseadas na PSI, conforme características listadas abaixo:
 - 4.3.1.2.1.1. Envio através de plataforma especializada, possibilitando a obtenção de indicadores como total de mensagens enviadas, recebidas, descartadas, lidas e clicadas;
 - 4.3.1.2.1.2. Layout personalizado, obedecendo o manual de marca da CONTRATANTE;
 - 4.3.1.2.1.3. Texto curto, para rápida leitura e compreensão do tema, com link para material externo, atingindo aqueles colaboradores que desejam se aprofundar no assunto.
- 4.3.2. Campanhas trimestrais:
 - 4.3.2.1. A CONTRATADA deverá elaborar, trimestralmente, campanha de conscientização, contemplando:
 - 4.3.2.1.1. Lâmina A4 para “Jornal mural”;
 - 4.3.2.1.2. Papel de parede para estações de trabalho e servidores Windows;

- 4.3.2.1.3. Material impresso para ser entregue aos colaboradores, tais como folhetos, adesivos, entre outros;
- 4.3.2.1.4. Os materiais deverão ser confeccionados obedecendo o manual de marca da CONTRATANTE e entregues a um ponto único de contato central, que se encarregará de distribuí-los aos equipamentos e colaboradores da CONTRATANTE;
- 4.3.2.1.5. As provas e aprovação dos materiais produzidos ficam a critério da CONTRATANTE e serão realizadas conforme reunião de preparação do material;
- 4.3.2.1.6. A CONTRATADA será responsável pela equipe de marketing e produção dos materiais, bem como do custo de elaboração das campanhas;
- 4.3.2.1.7. A quantidade de material produzido deverá atender os quantitativos de usuários ou equipamentos, conforme o tipo de material a ser criado.

4.3.3. Avaliação semestral:

- 4.3.3.1. Semestralmente a CONTRATADA deverá executar uma avaliação do conhecimento de segurança para todos os colaboradores da CONTRATANTE, conforme características listadas abaixo;
 - 4.3.3.1.1. Formulário contendo 10 perguntas, com resposta do tipo múltipla escolha;
 - 4.3.3.1.2. Layout personalizado, obedecendo o manual de marca do cliente;
 - 4.3.3.1.3. Envio através de plataforma especializada, possibilitando a obtenção de indicadores como total de formulários enviados, respondidos, média de acertos, entre outros.

4.3.4. Simulação de Phishing:

- 4.3.4.1. A CONTRATADA deverá executar testes de phishing trimestralmente com o objetivo de conscientizar os usuários

quanto à identificação de e-mails maliciosos que buscam extrair dados sigilosos ou fazer a proliferação de artefatos maliciosos;

4.3.4.2. A CONTRATADA deverá possuir um vasto repositório de e-mails para que os usuários não identifiquem que está sendo alvo de uma simulação;

4.3.4.3. Para que seja entregue um serviço adequado as exigências deste processo, a CONTRATADA deverá fazer uso de uma ferramenta de automação dos testes de phishing e conscientização;

4.3.4.3.1. Deve ser capaz de lançar e gerenciar campanhas simuladas de phishing;

4.3.4.3.2. Deve ser baseado em nuvem e não deve exigir servidores locais;

4.3.4.3.3. Deve prover os seguintes tipos de campanhas pré-definidas:

4.3.4.3.3.1. Campanhas de phishing – Induzir os usuários alvo a clicarem em um link dentro de um e-mail;

4.3.4.3.3.2. Campanha de coleta de credenciais - Tentar fazer com que os usuários alvo insiram suas credenciais em um site de aparência legítima, mas falso, sem a coleta das senhas;

4.3.4.3.3.3. Campanha de anexo - Tente fazer com que os usuários alvo abram um anexo dentro de um e-mail;

4.3.4.3.3.4. Campanha de treinamento - Inscreve os usuários alvo em treinamento obrigatório com base nos módulos de treinamento selecionados. E-mails devem poder serem enviados usando configurações personalizadas do servidor SMTP, se configurado.

4.3.4.3.4. Deve prover opção de seleção do tipo de treinamento:

4.3.4.3.4.1. Todos os treinamentos;

4.3.4.3.4.2. HTML interativo;

4.3.4.3.4.3. Vídeos fornecidos pela CONTRATADA.

- 4.3.4.3.5. Deve fornecer diferentes níveis de sofisticação de ataque, do tipo voltado a usuário iniciante, com conhecimento intermediário e avançado;
- 4.3.4.3.6. Deve suportar, entre outros, os seguintes tipos de simulação de ataque phishing:
 - 4.3.4.3.6.1. Clicar em link de vídeo;
 - 4.3.4.3.6.2. Clicar em link para fazer login em conta de site conhecido;
 - 4.3.4.3.6.3. Clicar em link oferecendo teste gratuito de 1 ano em serviço online conhecido;
 - 4.3.4.3.6.4. Clicar em link de proposta de plano de renda pessoal;
 - 4.3.4.3.6.5. Clicar em link para remover seu endereço de e-mail de site que teve dados vazados;
 - 4.3.4.3.6.6. Clicar em link de proposta de crédito de banco conhecido;
 - 4.3.4.3.6.7. Clicar em link para verificar transação financeira realizada em seu nome;
 - 4.3.4.3.6.8. Clicar em link para verificar falha no envio de mensagem;
 - 4.3.4.3.6.9. Clicar em link para verificar restituição do imposto de renda;
 - 4.3.4.3.6.10. Clicar em link para ver foto de carro enviada;
 - 4.3.4.3.6.11. Clicar no link para ver foto engraçada enviada;
 - 4.3.4.3.6.12. Clicar no link para visualizar arquivo confidencial criptografado anexado;
 - 4.3.4.3.6.13. Clicar no link para visualizar e-mail do RH sobre episódio de Cyber-Bullying;

- 4.3.4.3.6.14. Clicar no link para verificar se sua conta está envolvida em evento de vazamento de dados;
- 4.3.4.3.6.15. Clicar no link para visualizar arquivo compartilhado no Dropbox;
- 4.3.4.3.6.16. Clicar no link para trocar senha da conta de e-mail;
- 4.3.4.3.6.17. Clicar no link para aumentar a cota da conta de e-mail com armazenamento excedido;
- 4.3.4.3.6.18. Clicar no link para realizar ações em Facebook pessoal;
- 4.3.4.3.6.19. Clicar no link para visualizar documento do Google Docs;
- 4.3.4.3.6.20. Clicar no link para verificar armazenamento do Google Drive;
- 4.3.4.3.6.21. Clicar no link para mudar usuário e senha de acesso a banco;
- 4.3.4.3.6.22. Clicar no link para visualizar Nota Fiscal;
- 4.3.4.3.6.23. Clicar no link para realizar ações em seu LinkedIn;
- 4.3.4.3.6.24. Clicar no link para visitar site sugerido;
- 4.3.4.3.6.25. Clicar no link para verificar ou mudar credenciais da Microsoft/Office 365;
- 4.3.4.3.6.26. Clicar no link para desbloquear sua conta do Netflix;
- 4.3.4.3.6.27. Clicar no link para verificar pagamento que realizou pela sua conta no PayPal;
- 4.3.4.3.6.28. Clicar no link para verificar a agenda de manutenção de servidores;
- 4.3.4.3.6.29. Clicar no link para liberar e-mail com suspeita de spam para sua caixa postal;

- 4.3.4.3.6.30. Clicar no link para verificar sua conta ou mudar/cancelar corrida do Uber;
- 4.3.4.3.6.31. Clicar no link para acessar correio de voz;
- 4.3.4.3.6.32. Clicar no link para verificar alertas meteorológicos;
- 4.3.4.3.6.33. Clicar no link para visualizar o status de seu perfil ou suas violações de acesso a conteúdo na internet;
- 4.3.4.3.6.34. Clicar no link para visualizar detalhes de transferência internacional.
- 4.3.4.3.7. Deve ser capaz de executar campanha de coleta de credenciais;
- 4.3.4.3.8. Deve suportar esses tipos de simulação de ataques de coleta de credenciais;
 - 4.3.4.3.8.1. Clicar no link para login na Amazon utilizando suas credenciais;
 - 4.3.4.3.8.2. Abrir documento criptografado utilizando credenciais;
 - 4.3.4.3.8.3. Abrir documento que redireciona a site falso;
 - 4.3.4.3.8.4. Revisar documento e assinar digitalmente;
 - 4.3.4.3.8.5. Realizar login na conta de e-mail utilizando suas credenciais, inclusive Office 365 e Google;
 - 4.3.4.3.8.6. Realizar login no LinkedIn utilizando suas credenciais;
 - 4.3.4.3.8.7. Realizar login no Netflix utilizando suas credenciais.
- 4.3.4.3.9. Deve ser capaz de executar Campanhas de Anexo;
- 4.3.4.3.10. Deve suportar esses tipos de simulação de ataques de anexo;

- 4.3.4.3.10.1. Clicar em documento anexado citando Bônus de Fim de Ano e permitir conteúdo e macro;
- 4.3.4.3.10.2. Clicar em documento do Word anexado que faz parte do treinamento obrigatório sobre conscientização sobre assédio;
- 4.3.4.3.10.3. Clicar em documento com lista de vagas abertas para contratação;
- 4.3.4.3.10.4. Clicar em documento relacionado a despesas e sobre como elas podem ser reembolsadas;
- 4.3.4.3.10.5. Clicar em documentos relacionados a possibilidades de promoção;
- 4.3.4.3.10.6. Clicar em documento criptografado como parte das instruções sobre como descriptografá-lo.
- 4.3.4.3.11. Deve oferecer ao menos as seguintes opções de campanha:
 - 4.3.4.3.11.1. Nome da campanha;
 - 4.3.4.3.11.2. Data de início;
 - 4.3.4.3.11.3. Coleção de dados finais;
 - 4.3.4.3.11.4. Escalonar/incrementar envio de e-mail de campanha;
 - 4.3.4.3.11.5. Enviar automaticamente lembretes de treinamento aos usuários;
 - 4.3.4.3.11.6. Pontuação mínima para aprovação;
 - 4.3.4.3.11.7. Enviar e-mail de teste.
- 4.3.4.3.12. Deve ser capaz de educar os usuários sobre ameaças de phishing utilizando comunicação do tipo newsletter;

4.3.4.3.13. Deve ser capaz de mostrar o histórico de comunicações enviadas, incluindo quantos e-mails enviados e e-mails abertos;

4.3.4.3.14. Deve prover os seguintes modelos de newsletter:

4.3.4.3.14.1. Newsletter de formato aberto;

4.3.4.3.14.2. Newsletter pré-formatada em branco;

4.3.4.3.14.3. Modelo sobre os perigos do WiFi público;

4.3.4.3.14.4. Modelo alertando sobre phishing relacionado a impostos;

4.3.4.3.14.5. Modelo para educar usuários sobre o Phish Threat;

4.3.4.3.14.6. Modelo para educar usuários sobre o Whaling;

4.3.4.3.14.7. Modelo para educar os usuários sobre tendências de segurança e como lidar com isso;

4.3.4.3.14.8. Modelo para educar usuários sobre o que eles compartilham nas mídias sociais;

4.3.4.3.14.9. Modelo para educar usuários sobre Ransomware e Cryptolocker;

4.3.4.3.14.10. Modelo para educar usuários sobre Engenharia Social.

4.3.4.3.14.11. Deve ser capaz de:

4.3.4.3.14.11.1. Adicionar usuários manualmente;

4.3.4.3.14.11.2. Carregar usuários em massa através de arquivo CSV;

4.3.4.3.14.11.3. Atribuir usuários a grupo ou grupos para a simulação de phishing.

4.3.4.3.15. Deve ser capaz de gerar relatórios personalizados;

- 4.3.4.3.15.1. Executar relatórios customizados;
- 4.3.4.3.15.2. Executar relatórios predefinidos.
- 4.3.4.3.16. Deve ser capaz de fornecer os seguintes relatórios predefinidos:
 - 4.3.4.3.16.1. Usuários que clicaram;
 - 4.3.4.3.16.2. Usuários que clicaram, por Departamento;
 - 4.3.4.3.16.3. Treinamentos fracassados;
 - 4.3.4.3.16.4. Treinamentos incompletos;
 - 4.3.4.3.16.5. Plugins desatualizados;
 - 4.3.4.3.16.6. Infrator reincidente;
 - 4.3.4.3.16.7. Usuários que não clicaram;
 - 4.3.4.3.16.8. Anexos abertos;
 - 4.3.4.3.16.9. Macros habilitadas;
 - 4.3.4.3.16.10. Usuários que entraram com credenciais.
- 4.3.4.3.17. Capaz de falsificar o domínio da empresa, retransmitir e-mails simulados de Phish Threat através de seus próprios servidores de e-mail para o servidor de e-mails da empresa;
- 4.3.4.3.18. Capaz de inscrever automaticamente novos funcionários para uma campanha;
- 4.3.4.3.19. Capaz de inscrever automaticamente campanha ao atribuir novos funcionários quando eles são adicionados ao Phish Threat;
- 4.3.4.3.20. Capaz de inscrever automaticamente funcionários para uma campanha quando eles responderem a ataques de phishing;
- 4.3.4.3.21. Deve ser capaz de personalizar o conteúdo;

- 4.3.4.3.21.1. Inscrição de treinamento;
- 4.3.4.3.21.2. E-mails de lembrete.
- 4.3.4.3.22. Deve ser capaz de agendar campanhas e lançá-las imediatamente;
- 4.3.4.3.23. Deve ser capaz de encerrar uma campanha em progresso;
 - 4.3.4.3.23.1. Parar de enviar e-mails;
 - 4.3.4.3.23.2. Parar de coletar resultados.

4.4. Gestão de riscos e conformidade

- 4.4.1. A CONTRATADA deverá executar serviços para estabelecer uma gestão de riscos de segurança da informação que permitam identificar, analisar e avaliar riscos, criar uma matriz de riscos e possibilitar o tratamento adequado, através da evitação, da aceitação, da mitigação, da eliminação ou da transferência.
- 4.4.2. Das atividades:
 - 4.4.2.1. Deverá realizar, nos primeiros **90 (noventa) dias** de execução deste serviço, uma avaliação completa do ambiente do CONTRATANTE com o objetivo de identificar lacunas ou oportunidades de melhoria (Gap Analysis) com o objetivo de avaliar a maturidade dos controles de segurança na CONTRATANTE, contendo no mínimo:
 - 4.4.2.1.1. Avaliação de maturidade do ambiente da CONTRATANTE;
 - 4.4.2.1.2. Levantamento de Cloud Access Security Broker (CASB) – Agente de Segurança de Acesso à Nuvem;
 - 4.4.2.1.3. Scan de vulnerabilidade.
 - 4.4.2.2. A CONTRATADA deverá capacitar o CONTRATANTE para lidar com os riscos. Além da estrutura de decisão, quatro tipos de risco que requerem diferentes planos de gerenciamento de risco: Riscos de rotina, Riscos complexos, Riscos incertos e Riscos ambíguos;

- 4.4.2.3. A CONTRATADA deverá manter uma rotina mensal de avaliação dos processos e práticas em todas as áreas de atuação do escopo do contrato com o objetivo de avaliar a eficácia, propor melhorias e auxiliar na implementação desses ajustes;
- 4.4.2.4. Estabelecer o processo de gerenciamento de risco envolvendo a revisão das informações coletadas como parte das avaliações de risco, passando pelas etapas de identificação, análise e avaliação dos riscos. Essas informações devem constituir a base das decisões que levam ao resultado para cada risco percebido, que será estabelecido em conjunto com o CONTRATANTE;
- 4.4.2.5. Operacionalizar a Gestão de Riscos de Segurança da Informação, tornando o ambiente mais seguro, possuindo um grau de garantia de que continuará a funcionar adequadamente conforme suas características estabelecidas, mesmo na presença de eventos negativos decorrentes da interação com agentes maliciosos ou na ocorrência de eventos decorrentes de acidentes ou desastres de origem natural ou ambiental, continuando a cumprir seus objetivos, mesmo em face do sinistro;
- 4.4.2.6. Quanto ao gerenciamento de riscos a CONTRATADA deverá:
 - 4.4.2.6.1. Estabelecer uma matriz de riscos juntamente com a CONTRATANTE e propor ações de tratamento desses riscos (evitar, aceitar, mitigar, eliminar ou transferir);
 - 4.4.2.6.2. Realizar ações de análise de riscos, visando a criação de uma matriz em conformidade com as diretrizes CONTRATANTE;
 - 4.4.2.6.3. Elaborar um documento para que seja avaliado e homologado pela CONTRATANTE, contendo minimamente a matriz de riscos, e os processos de tratamento dos riscos reportados;
 - 4.4.2.6.4. Realizar análises de risco de segurança para cada contratação tecnológica a ser realizada pela CONTRATANTE;

4.4.2.6.5. Acompanhar e realizar ações de cobrança junto aos responsáveis para cada ação definida nos processos de mitigação e tratamento.

4.4.3. Avaliação de Riscos:

4.4.3.1. Entendimento da probabilidade que um desastre ou outra interrupção no serviço poderá de fato ocorrer. Falhas na avaliação de todos os riscos relevantes deixam a organização vulnerável a possíveis interrupções;

4.4.3.2. A CONTRATADA deverá fazer a avaliação de riscos identificando:

4.4.3.2.1. Os riscos a processos ou serviço em particular;

4.4.3.2.2. Níveis de ameaças e vulnerabilidades;

4.4.3.2.3. Níveis de risco;

4.4.3.2.4. Medidas iniciais de redução de riscos.

4.4.3.3. Para que seja possível o adequado gerenciamento de riscos deve ser utilizado uma ferramenta no ambiente da CONTRATANTE com as seguintes características:

4.4.3.3.1. Quanto à administração, a solução deverá:

4.4.3.3.1.1. Possuir módulo único e central de administração do ambiente, com possibilidade de definição de perfis de acesso e permissões para usuários e grupos de usuários, permitindo que o administrador parametrize quais funções do sistema cada usuário terá acesso;

4.4.3.3.1.2. Registrar atividades em trilhas de auditoria;

4.4.3.3.1.3. Possuir interface para gestão e monitoramento da fila de serviços de execução;

4.4.3.3.1.4. Possuir interface para monitoramento de notificações enviadas por e-mail.

4.4.3.3.2. Quanto à usabilidade, a solução deverá:

- 4.4.3.3.2.1. Ser compatível com os navegadores internet: Google Chrome, Microsoft Internet Explorer, Edge e Firefox;
- 4.4.3.3.2.2. Permitir a conversão de conteúdo para o formato PDF;
- 4.4.3.3.2.3. Suportar idiomas padrão UTF8;
- 4.4.3.3.2.4. Possuir visualizador nativo HTML 5 para PDF sem a necessidade de instalação de softwares adicionais para visualização nas estações clientes.

4.4.3.3.3. Quanto à segurança, a solução deverá:

- 4.4.3.3.3.1. Realizar comunicação segura entre os diferentes componentes da solução e com a estação de trabalho usando padrões de criptografia e protocolos;
- 4.4.3.3.3.2. Registrar os acessos efetuados por todos os usuários em um arquivo de log, para fins de auditoria e elaboração de relatórios gerenciais. Esses dados serão acessíveis apenas por um grupo determinado de usuários autorizados, contendo no mínimo os seguintes dados: usuário, data, hora, transação realizada;
- 4.4.3.3.3.3. Prover mecanismos de segregação de usuários através de nível de atuação (usuários, gerentes de projeto, consultor do escritório de projetos, suporte, administração);
- 4.4.3.3.3.4. Armazenar as senhas de usuários utilizando algoritmos de criptografia salted hash;
- 4.4.3.3.3.5. Permitir a configuração e autenticação em mais de um domínio para a mesma instância, de forma que em um mesmo ambiente seja possível se autenticar através de Single Sign-On (SSO) em diferentes domínios, não necessitando que os mesmos estejam

integrados entre si, sem qualquer necessidade de parametrização via arquivo de configuração ou customização do produto.

4.4.3.3.4. Quanto à gestão de riscos, a solução deverá:

- 4.4.3.3.4.1. Permitir a definição da metodologia de avaliação de pontuação do risco em qualquer nível da organização;
- 4.4.3.3.4.2. Permitir diversos métodos para a avaliação de risco, tais como: matriz; critérios quantitativos; mais de um critério quantitativos para gerar os eixos da matriz, e; critérios qualitativos;
- 4.4.3.3.4.3. Classificar os riscos de acordo com a severidade para a organização e com a probabilidade da ocorrência no processo;
- 4.4.3.3.4.4. Permitir a avaliação periódica do risco, monitorando a sua evolução analítica e graficamente;
- 4.4.3.3.4.5. Permitir a criação de modelos (template) de plano de riscos, para facilitar a replicação de estruturas similares nas organizações;
- 4.4.3.3.4.6. Permitir uma abordagem estratégica na identificação dos principais objetivos da organização e dos riscos existentes para o alcance desses objetivos;
- 4.4.3.3.4.7. Permitir que os riscos possam ser facilmente identificados e associados a um processo;
- 4.4.3.3.4.8. Permitir a criação de bibliotecas de riscos, ou seja, que os nomes dos riscos e tipos de riscos sejam armazenados em um repositório único, garantindo um conjunto de riscos padronizados para a organização;

- 4.4.3.3.4.9. Permitir a definição de equipes responsáveis pela avaliação;
- 4.4.3.3.4.10. Manter o cadastro e acompanhamento das alterações (revisões) dos objetos e dos planos de riscos;
- 4.4.3.3.4.11. Permitir a definição do custo dos controles e o valor do impacto ou ganho do risco, possibilitando a realização de análises quantitativas do risco;
- 4.4.3.3.4.12. Permitir a abertura de eventos (incidentes, problemas, workflows), caso as consequências do risco superem o esperado, possibilitando a identificação das causas, análise da causa, criação de planos de ação e verificação da eficácia. Estes registros devem ser mantidos para histórico e entrada da nova avaliação do risco futuramente;
- 4.4.3.3.4.13. Possibilitar a abertura de um workflow específico, caso a avaliação do risco esteja acima do esperado;
- 4.4.3.3.4.14. Possibilitar a aprovação do plano de riscos ao final do planejamento e a revalidação dentro de frequência pré-estabelecida;
- 4.4.3.3.4.15. Permitir que os riscos possam ser associados a mais de um processo, porém que sejam analisados e documentados individualmente para cada processo;
- 4.4.3.3.4.16. Permitir a avaliação considerando o risco potencial, o risco inerente e o risco residual;
- 4.4.3.3.4.17. Permitir o cálculo automático do risco residual;
- 4.4.3.3.4.18. Permitir a associação de anexos e documentos controlados ao Risco;
- 4.4.3.3.4.19. Executar as avaliações de maneira on-line;

- 4.4.3.3.4.20. Permitir a análise de risco dos processos mapeados;
- 4.4.3.3.4.21. Apresentar graficamente, no fluxograma do processo, as atividades que possuem riscos associados;
- 4.4.3.3.4.22. Mapear os processos e modelar todas as atividades relacionadas;
- 4.4.3.3.4.23. Permitir a análise de risco dos ativos e dos projetos;
- 4.4.3.3.4.24. Permitir o planejamento do projeto com a definição de atividades, responsabilidades, recursos, prazos e custos;
- 4.4.3.3.4.25. Mapear os riscos operacionais de acordo com o framework COSO;
- 4.4.3.3.4.26. Permitir o preenchimento da árvore de decisão na gestão dos riscos de segurança da Informação e comunicação;
- 4.4.3.3.4.27. Permitir a habilidade de desenvolver ou adotar um framework para a gestão de riscos;
- 4.4.3.3.4.28. Permitir a associação de tratamentos e planos de ação no momento da criação da análise de risco;
- 4.4.3.3.4.29. Permitir a associação de controles aos riscos durante o cadastro, facilitando a utilização posterior;
- 4.4.3.3.4.30. Apresentar o histórico das avaliações do risco atualizado conforme última versão do método de avaliação;
- 4.4.3.3.4.31. Oferecer método de avaliação para a definição do nível do risco. Critérios quantitativos podem ser informados para a obtenção do resultado;

- 4.4.3.3.4.32. Personalizar as colunas para serem visualizadas na estrutura do plano de risco e controle;
 - 4.4.3.3.4.33. Permitir a visualização da Matriz de Risco e controle de riscos contidos no Plano de Gerenciamento de Riscos;
 - 4.4.3.3.4.34. Permitir a visualização da Matriz de Risco agrupando quantitativamente as avaliações dos riscos;
 - 4.4.3.3.4.35. Permitir a associações do risco no momento que está cadastrando um evento, ou seja, um incidente, problema ou workflow;
 - 4.4.3.3.4.36. Permitir registrar uma justificativa, anexo ou documento para cada resultado da avaliação do risco;
 - 4.4.3.3.4.37. Permitir associar causas, consequências, fontes de risco e melhores práticas ao risco;
 - 4.4.3.3.4.38. Permitir criar e gerenciar Indicadores chave de risco (KRI), com geração de eventos caso o KRI esteja fora dos valores aceitáveis;
 - 4.4.3.3.4.39. Permitir enviar e-mail a aprovação da avaliação do risco;
 - 4.4.3.3.4.40. Permitir solicitar a avaliação de risco para o responsável no momento da Auditoria;
 - 4.4.3.3.4.41. Supervisionar a implantação do plano de ação de risco e realizar a revisão periodicamente.
- 4.4.3.3.5. Quanto aos problemas e tratamento, a solução deverá:
- 4.4.3.3.5.1. Permitir a identificação de problemas nas atividades de controle e na avaliação do risco;
 - 4.4.3.3.5.2. Permitir a associação de prioridade aos problemas;

- 4.4.3.3.5.3. Permitir a definição de responsáveis aos problemas;
- 4.4.3.3.5.4. Permitir o monitoramento de prazos de planejamento e de execução;
- 4.4.3.3.5.5. Permitir o envio de e-mail automaticamente para o responsável assim que uma ocorrência for registrada;
- 4.4.3.3.5.6. Permitir a criação e o monitoramento de múltiplos planos de ação para cada problema;
- 4.4.3.3.5.7. Permitir que os responsáveis pelos planos de ação possam ser diferentes dos responsáveis pelo problema;
- 4.4.3.3.5.8. Permitir que os planos de ação sejam revisados e aprovados por um usuário específico ou pelo responsável pelo problema;
- 4.4.3.3.5.9. Permitir que a situação de execução dos planos de ação seja monitorada;
- 4.4.3.3.5.10. Permitir que as notificações por e-mail possam ser definidas pelos usuários;
- 4.4.3.3.5.11. Permitir que o gestor tenha fácil acesso a todos os problemas e planos de ação de sua área de responsabilidade;
- 4.4.3.3.5.12. Permitir a análise de causa e de tendência;
- 4.4.3.3.5.13. Permitir a personalização da resposta ao risco;
- 4.4.3.3.5.14. Permitir a criação ou a associação de um ou mais planos de ação para cada tratamento do risco;
- 4.4.3.3.5.15. Permitir a gestão de iniciativas de acordo com o PMBOK;

4.4.3.3.5.16. Permitir definir um tratamento para uma avaliação de risco e associar um plano de ação para este tratamento.

4.4.3.3.6. Consultas e relatórios:

4.4.3.3.6.1. Permitir que o sistema agrupe e gere consultas da avaliação de riscos em todos os níveis da base de dados, incluindo a estrutura organizacional, processos e riscos;

4.4.3.3.6.2. Apresentar a listagem de problemas e planos de ação com possibilidade de desdobramentos;

4.4.3.3.6.3. Permitir salvar relatórios no formato PDF;

4.4.3.3.6.4. Permitir que os responsáveis pelos controles e auditores independentes possam acessar facilmente sua informação no sistema;

4.4.3.3.6.5. Permitir que os responsáveis pelos processos possam acessar facilmente sua informação no sistema;

4.4.3.3.6.6. Apresentar listagens ou relatórios da avaliação de riscos, visando a fácil identificação de pontos críticos na organização;

4.4.3.3.6.7. Apresentar os objetivos estratégicos e da avaliação dos riscos de maneira gráfica e visual;

4.4.3.3.6.8. Apresentar a matriz de riscos para a fácil identificação dos riscos dentro dos quadrantes do método de avaliação;

4.4.3.3.6.9. Garantir o acompanhamento do plano de riscos permitindo uma fácil visualização do fluxograma do processo, riscos por etapa, controles e tratamentos, matriz de riscos x etapa e demais elementos;

- 4.4.3.3.6.10. Apresentar a matriz de riscos para a fácil identificação da relação entre riscos e atividades;
- 4.4.3.3.6.11. Apresentar o cálculo do risco médio gerado automaticamente e agrupado por Unidade Organizacional, Processo, Risco e Tipo de Risco, com visões gráficas da matriz de risco em um portal interativo;
- 4.4.3.3.6.12. Permitir comparar os resultados entre as revisões do plano de risco e controle;
- 4.4.3.3.6.13. Permitir a definição de indicadores de desempenho associados aos processos e acompanhamento do cumprimento das metas estabelecidas;
- 4.4.3.3.6.14. Possibilitar a geração de diversos tipos de relatórios e gráficos contendo informações detalhadas ou resumidas sobre os processos e atividades;
- 4.4.3.3.6.15. Possuir semáforos que sinalizam visualmente o nível de cumprimento dos resultados;
- 4.4.3.3.6.16. Possuir indicador de tendência sobre possíveis problemas futuros;
- 4.4.3.3.6.17. Permitir a formatação dos resultados em planilhas e gráficos configuráveis pelo usuário;
- 4.4.3.3.6.18. Permitir a visualização dos recursos e custos requeridos para a execução dos processos.

4.4.4. Análise de impacto no negócio (AIN):

- 4.4.4.1. A CONTRATADA deverá elaborar a Análise de Impacto no Negócio - AIN, para quantificar o impacto que a perda do serviço de SI impactará no negócio da CONTRATANTE;
- 4.4.4.2. A CONTRATADA através de análise de Risco deverá identificar potenciais ameaças para a continuidade e a probabilidade que

porventura acontecer, bem como, precisará incluir medidas para gerenciar as ameaças identificadas, quando o custo se justificar;

4.4.4.3. A CONTRATADA efetuará análise contendo:

4.4.4.3.1. A identificação dos serviços críticos ao negócio da CONTRATANTE;

4.4.4.3.2. Determinar os efeitos da indisponibilidade;

4.4.4.3.3. Avaliação do cenário que será impactado;

4.4.4.3.4. Análise das obrigações legais junto ao cumprimento pela CONTRATADA e CONTRATANTE;

4.4.4.3.5. Análise do tempo que a CONTRATANTE se manterá em caso de indisponibilidade total da TI;

4.4.4.3.6. Avaliação dos requisitos mínimos de restabelecimento (pessoal, infraestrutura e serviços) para assegurar os processos críticos para a CONTRATANTE.

4.4.4.4. Determinar o tempo mínimo e máximo dos níveis de serviços a serem recuperados;

4.4.4.5. Determinar quais processos da CONTRATANTE devem ser recuperados por completo.

4.5. Gestão de Vulnerabilidades

4.5.1. Considerações gerais:

4.5.1.1. A atividade de Gestão de Vulnerabilidades poderá ser realizada remotamente e terá como objetivo principal a análise geral do ambiente da CONTRATANTE quanto a segurança da informação para identificar, mapear, documentar, controlar e reportar possíveis vulnerabilidades em seus sistemas, serviços e ativos de infraestrutura tecnológica, bem como apresentar recomendações de melhorias e/ou correções das vulnerabilidades identificadas durante os testes.

4.5.1.2. Fazem parte do processo de gestão de vulnerabilidades as fases de Varredura de Vulnerabilidades, Alerta de Vulnerabilidades, Priorização

da Vulnerabilidades e Controle das Vulnerabilidades (nos equipamentos fornecidos pela CONTRATADA, automatização do processo de patches e fornecimento do plano de remediação nos demais equipamentos do ambiente). Estas fases devem atuar de forma integrada com o objetivo de proverem informações suficientes para uma proteção mais eficaz do ambiente da contratada.

4.5.1.3. A empresa CONTRATADA deverá entregar à CONTRATANTE todo detalhamento dos testes, sejam manuais ou automatizados, realizados, desde os ativos a serem testados, qual procedimento adotado, ferramentas utilizadas, entre outras informações que possam ser solicitadas.

4.5.1.4. Os testes só poderão acontecer mediante autorização da CONTRATANTE, com anuência da área técnica responsável pela sustentação em produção do sistema escopo.

4.5.1.5. Todos os testes realizados deverão ser precedidos de caderno de testes, contendo todo o detalhamento das ações a serem executadas, possíveis comprometimentos, possíveis ações de contorno, dentre outras informações que se julguem necessárias para garantia da segurança e do sigilo das informações da CONTRATANTE.

4.5.1.6. Quaisquer atividades que possam comprometer ou prejudicar algum ambiente ou ativo deverão ser reportadas, antes de sua execução, haja vista a necessidade de manter a disponibilidade dos ambientes e serviços ativos.

4.5.1.7. Deverá ser realizada, com periodicidade mínima semanal, uma varredura interna de vulnerabilidades no escopo descrito abaixo;

4.5.1.8. As varreduras de vulnerabilidades deverão considerar até 10.000 (dez mil) endereços IPs, 400 URLs, e 8.300(oito mil e trezentos) usuários definidos pela CONTRATANTE, devendo considerar as seguintes etapas:

4.5.1.8.1. Levantamento de todos os ativos da infraestrutura de TIC que deverão ser alvo da varredura. Para cada ativo, deverão ser levantados além das informações básicas, as informações de criticidade do ativo no ambiente, a matriz de responsáveis e as informações das janelas de manutenção e mudanças;

- 4.5.1.8.2. Execução da varredura de vulnerabilidades;
- 4.5.1.8.3. Análise dos resultados e priorização das vulnerabilidades;
- 4.5.1.8.4. Elaboração e entrega de um Plano de Remediação considerando a criticidade da vulnerabilidade identificada e, também, os critérios definidos na fase de Levantamento de Ativos.
- 4.5.1.8.5. Para toda vulnerabilidade encontrada, a CONTRATADA deverá descrever as ações para correção. Caso precise ter acesso as configurações dos ativos de tecnologia, a CONTRATADA deverá justificar a necessidade, ficando a cargo do CONTRATANTE decidir pela liberação;
- 4.5.1.8.6. A CONTRATADA será responsável por automatizar todo o processo de aplicação dos patches e atualizações, nos sistemas em que for possível;
- 4.5.1.8.7. A CONTRATANTE será responsável por todo o processo de homologação dos patches e atualizações, caberá a CONTRATADA executar, de forma automatizada a aplicação destes patches nos sistemas em que for possível;
- 4.5.1.8.8. Será de reponsabilidade da CONTRATANTE a aprovação dos patches antes que estes sejam aplicados, seguindo o processo disponibilizado pela CONTRATADA;
- 4.5.1.8.9. Será de reponsabilidade da CONTRATANTE informar a CONTRATADA os horário em que os patches poderão ser aplicados, bem como executar qualquer remediação no ambiente que possa ser causado por um patch aprovado.
- 4.5.1.8.10. A liberação de novos patches somente será realizada após a homologação destes;
- 4.5.1.8.11. Caberá a CONTRATANTE disponibilizar um ambiente para que os patches possam ser homologados;
- 4.5.1.8.12. A homologação dos patches será realizada de acordo com o processo de gestão de mudanças da CONTRATANTE;

- 4.5.1.8.13. Será de responsabilidade da CONTRATANTE a aprovação dos patches antes que estes sejam aplicados, seguindo o processo disponibilizado pela CONTRATADA.
- 4.5.1.8.14. Uma vez homologados, os patches serão liberados para a implantação automática no ambiente da CONTRATANTE;
- 4.5.1.8.15. Caso haja necessidade, a CONTRATANTE poderá solicitar a CONTRATADA que seja iniciado um processo de rollback de um determinado patch. Porém, caso o processo de rollback, realizado através da solução de Patch, não seja bem-sucedido e entendendo que a administração e a operação dos softwares e sistemas operacionais, nos quais serão executadas as remediações através de patches, não estão sob a gestão e a administração da CONTRATADA, caberá a equipe de TI da CONTRATANTE atuar nestes casos e executar, caso necessário, estratégias de recuperação dos softwares e/ou sistemas operacionais.
- 4.5.1.9. Para realização das varreduras de vulnerabilidades e gestão de patches deve ser entregue, pela CONTRATADA, uma ferramenta com as seguintes características:
 - 4.5.1.9.1. Quanto às suas características gerais, a solução deverá:
 - 4.5.1.9.1.1. Realizar a gestão de todos os módulos considerados neste termo através de uma console única;
 - 4.5.1.9.1.2. Permitir descobrir, avaliar, priorizar e auxiliar na correção de vulnerabilidades / configurações em toda a infraestrutura de rede, incluindo estações de trabalho, servidores, dispositivos de rede, dispositivos de telecomunicações e dispositivos de segurança, hypervisors, máquinas virtuais, orquestradores de contêineres, contêineres e nuvens (Azure, GCP, AWS), proporcionando através de única interface para o administrador via um portal web para gerenciamento de todos os ativos, permitindo o gerenciamento centralizado de todos os componentes da solução a partir de um único ponto, sem a necessidade de incorrer em consoles -

componentes adicionais fora dele para a administração dos serviços oferecidos;

4.5.1.9.1.3. Possuir no mínimo, duas das seguintes certificações de privacidade e segurança:

4.5.1.9.1.4. EU-U.S. Privacy Shield Framework;

- Swiss-U.S. Privacy Shield Framework;
- Cloud Security Alliance;
- (CSA) STAR.

4.5.1.9.1.5. Todos os serviços da plataforma devem estar disponíveis sob o mesmo padrão de qualidade de serviço 24x7x365 e garantir 99% de disponibilidade;

4.5.1.9.1.6. Oferecer manutenção e atualização constante da plataforma durante todo o período de vigência do contrato de serviço;

4.5.1.9.1.7. Prover atualizações de serviço de forma transparente para o administrador da solução, sem afetar nenhum dos dados armazenados e serviços fornecidos;

4.5.1.9.1.8. Garantir que todas as comunicações entre componentes, transferência de dados e sincronização da solução sejam criptografadas de ponta a ponta, fazendo uso de no mínimo TLS 1.2, certificados assinados com RSA 2048 bits e algoritmo de assinatura SHA256;

4.5.1.9.1.9. Permitir a criação de usuários distintos;

4.5.1.9.1.10. Permitir a separação de funções e permissões na console;

4.5.1.9.1.11. Permitir a integração através de SSO com, pelo menos, Azure Active Directory;

- 4.5.1.9.1.12. Possuir console acessível a partir de, pelo menos, um dos seguintes navegadores:
- 4.5.1.9.1.13. Google Chrome;
- 4.5.1.9.1.14. Microsoft Edge;
- 4.5.1.9.1.15. Firefox.
- 4.5.1.9.2. Quanto aos seus agentes, a solução deverá:
 - 4.5.1.9.2.1. Oferecer um agente de baixo impacto nos sistemas operacionais onde está instalado e no consumo de largura de banda que utilizará na rede;
 - 4.5.1.9.2.2. Atualizar automaticamente seus agentes e gerir as suas atualizações também de forma automática;
 - 4.5.1.9.2.3. Suportar plataformas de nuvem AWS, GCP, Azure;
 - 4.5.1.9.2.4. Ser capaz de coletar informações sobre o inventário de ativos;
 - 4.5.1.9.2.5. Prover nativamente um dispositivo capaz de concentrar requisições dos agentes para encaminhamento a console de gerenciamento de forma a evitar a conexão direta de agentes com a plataforma;
 - 4.5.1.9.2.6. Suportar o uso de proxy;
 - 4.5.1.9.2.7. Permitir a definição do intervalo de comunicação entre o agente e a console de gerenciamento;
 - 4.5.1.9.2.8. Possibilitar limitar o consumo de CPU e memória do agente;
 - 4.5.1.9.2.9. Permitir a definição de um período global de inatividade dos agentes.
- 4.5.1.9.3. Quanto à categorização e inventário de ativos, a solução deverá:

- 4.5.1.9.3.1. Permitir a coleta de informações detalhadas sobre o ativo gerenciado, deve detalhar pelo menos os seguintes dados para cada ativo:
 - 4.5.1.9.3.1.1. Serviços em execução;
 - 4.5.1.9.3.1.2. Software instalado;
 - 4.5.1.9.3.1.3. Usuários;
 - 4.5.1.9.3.1.4. Portas abertas;
 - 4.5.1.9.3.1.5. Nome do host;
 - 4.5.1.9.3.1.6. FQDN;
 - 4.5.1.9.3.1.7. IP v4 / v6;
 - 4.5.1.9.3.1.8. Endereço MAC.
- 4.5.1.9.3.2. Classificar automaticamente os ativos por famílias de tecnologia, tipo de dispositivo, tipo de plataforma e fabricante;
- 4.5.1.9.3.3. Normalizar automaticamente os nomes dos fabricantes de HW e SW com seus dados relevantes, como o nome dos aplicativos e versões, para facilitar sua posterior busca na solução;
- 4.5.1.9.3.4. Possuir a habilidade de etiquetagem (Tags) de ativos para facilitar a identificação, deve permitir a geração de Tags, pelo menos, usando os seguintes parâmetros:
 - 4.5.1.9.3.4.1. Palavras-chave;
 - 4.5.1.9.3.4.2. Endereço IP e intervalos de IP;
 - 4.5.1.9.3.4.3. Segmento de rede;
 - 4.5.1.9.3.4.4. Portas abertas;

4.5.1.9.3.4.5. Informações de inventário considerando, no mínimo:

4.5.1.9.3.4.5.1. Sistema operacional;

4.5.1.9.3.4.5.2. Presença ou ausência de determinado software instalado ou serviço em execução.

4.5.1.9.3.5. Permitir o agrupamento manual a critério do administrador da solução;

4.5.1.9.3.6. Permitir atribuir criticidade ao ativo para priorizá-lo durante o processo de gerenciamento;

4.5.1.9.3.7. Permitir criação de Dashboards personalizados que sejam capazes de trazer as seguintes informações sobre os ativos:

4.5.1.9.3.7.1. Categorias de softwares instalados nos ativos;

4.5.1.9.3.7.2. Hosts que executam máquinas virtuais;

4.5.1.9.3.7.3. Sistemas operacionais utilizados;

4.5.1.9.3.7.4. Serviços e portas TCP ou UDP abertas;

4.5.1.9.3.7.5. Softwares de segurança instalados;

4.5.1.9.3.7.6. Memória total utilizada;

4.5.1.9.3.7.7. Quantidade de processadores;

4.5.1.9.3.7.8. Quantidade de armazenamento disponível.

4.5.1.9.3.8. Permitir a visualização de quantidade de máquinas com um determinado software instalado;

4.5.1.9.3.9. Permitir visibilidade a respeito de hosts que executam containers e containers em execução.

4.5.1.9.4. Quanto à gestão de configuração, a solução deverá:

- 4.5.1.9.4.1. Permitir a avaliação, o relatório e o relatório de problemas de configuração, com base nas referências do padrão da indústria do Centro de Segurança da Internet (CIS);
- 4.5.1.9.4.2. Ter seu fabricante oficialmente certificado pelo CIS para fornecer este nível de controle;
- 4.5.1.9.4.3. Oferecer avaliação de configuração com base no benchmark CIS padrão da indústria, cobrindo esta funcionalidade nas seguintes categorias:
 - 4.5.1.9.4.3.1. Sistemas operacionais;
 - 4.5.1.9.4.3.2. Software de servidor;
 - 4.5.1.9.4.3.3. Provedores de nuvem;
 - 4.5.1.9.4.3.4. Dispositivos de rede;
 - 4.5.1.9.4.3.5. Software de desktop.
- 4.5.1.9.4.4. Suportar detecção de falhas de conformidades através de varreduras autenticadas ou através de agente instalado diretamente no ativo monitorado;
- 4.5.1.9.4.5. Permitir que os administradores recebam informação de conformidade de sistemas operacionais Windows e Linux, mesmo que não estejam conectados à rede corporativa;
- 4.5.1.9.4.6. Permitir a avaliação de certificados digitais (internos e externos) e configurações de TLS em busca de problemas e vulnerabilidades de certificados, resultando em diferentes graus de conformidade de acordo com os resultados da avaliação de seu emissor, prazo de validade, tipo de certificado, robustez do algoritmo e o conjunto de criptografia usados.
- 4.5.1.9.5. Quanto à gestão de vulnerabilidades de infraestrutura, a solução deverá:

4.5.1.9.5.1. Permitir varreduras de vulnerabilidade com base em:

4.5.1.9.5.1.1. Sistemas Operacionais;

4.5.1.9.5.1.2. Serviços WEB;

4.5.1.9.5.1.3. Portas TCP e UDP;

4.5.1.9.5.1.4. Serviços;

4.5.1.9.5.1.5. Aplicações;

4.5.1.9.5.1.6. Bancos de dados;

4.5.1.9.5.1.7. Dispositivos de rede como switches, roteadores e balanceadores de carga.

4.5.1.9.5.2. Abranger os seguintes sistemas operacionais, bancos de dados e aplicativos:

4.5.1.9.5.2.1. Microsoft Windows;

4.5.1.9.5.2.2. UNIX;

4.5.1.9.5.2.3. LINUX;

4.5.1.9.5.2.4. MacOS;

4.5.1.9.5.2.5. Mac OS X;

4.5.1.9.5.2.6. Cisco;

4.5.1.9.5.2.7. Alcatel;

4.5.1.9.5.2.8. VMware.

4.5.1.9.5.3. Detectar e analisar vulnerabilidades nas principais versões de Bancos de Dados, pelo menos:

4.5.1.9.5.3.1. Microsoft SQL Server;

4.5.1.9.5.3.2. MySQL;

4.5.1.9.5.3.3. Oracle;

4.5.1.9.5.3.4. MongoDB;

4.5.1.9.5.3.5. Postgres.

4.5.1.9.5.4. Detectar e analisar vulnerabilidades em plataformas WEB, pelo menos:

4.5.1.9.5.4.1. IIS;

4.5.1.9.5.4.2. Apache Tomcat;

4.5.1.9.5.4.3. RedHat JBoss;

4.5.1.9.5.4.4. RedHat Openshift.

4.5.1.9.5.5. Detectar e analisar vulnerabilidades em portas e serviços TCP e UDP;

4.5.1.9.5.6. Detectar vulnerabilidades em pelo menos os seguintes aplicativos ou plataformas:

4.5.1.9.5.6.1. Adobe;

4.5.1.9.5.6.2. Apple;

4.5.1.9.5.6.3. McAfee;

4.5.1.9.5.6.4. Microsoft (Office, IIS, Exchange);

4.5.1.9.5.6.5. Oracle;

4.5.1.9.5.6.6. Oracle Java;

4.5.1.9.5.6.7. VMware.

4.5.1.9.5.7. Permitir a descoberta de vulnerabilidades na rede, oferecendo as seguintes alternativas de varredura:

4.5.1.9.5.7.1. Varredura ativa de rede não autenticada;

4.5.1.9.5.7.2. Varredura ativa de rede autenticada;

4.5.1.9.5.7.3. Agente;

4.5.1.9.5.7.4. Varreduras externas;

4.5.1.9.5.7.5. Varredura Passiva.

- 4.5.1.9.5.8. Atualizar semanalmente a base de conhecimento de vulnerabilidades, garantindo a incorporação de, pelo menos 20 CVEs, e possuir uma base de conhecimento com, pelo menos, 35.000 CVEs relacionados, incluindo tecnologias legadas e atuais;
- 4.5.1.9.5.9. Oferecer suporte ao padrão da indústria para pontuação de vulnerabilidade do Common Vulnerability Scoring System (CVSS);
- 4.5.1.9.5.10. Oferecer suporte ao padrão da indústria para adicionar detecções personalizadas usando Open Vulnerability Assessment Language (OVAL);
- 4.5.1.9.5.11. Permitir vincular as vulnerabilidades detectadas e indicar sua relação com ameaças como Vírus, Trojan e Malware;
- 4.5.1.9.5.12. Ser capaz de indicar explorações disponíveis e códigos disponíveis para uma vulnerabilidade, quando aplicável;
- 4.5.1.9.5.13. Possuir banco de dados capaz de relacionar a maioria das vulnerabilidades ao CVE e Bugtraq;
- 4.5.1.9.5.14. Oferecer suporte à integração para autenticação por ferramentas de cofres de senha com ao menos duas dos seguintes fabricantes, Thycotic/Centrify, CyberArk, BeyondTrust;
- 4.5.1.9.5.15. Permitir buscas interativas de vulnerabilidade utilizando filtros como severidade, categoria, sistema operacional, status, classificação do CVSS, CVE ou KB;

- 4.5.1.9.5.16. Permitir a utilização de operadores lógicos na busca de vulnerabilidades para que seja possível encontrar, no mínimo, as seguintes informações:
 - 4.5.1.9.5.16.1. Vulnerabilidades associadas a ransomware e que possuem patches disponíveis;
 - 4.5.1.9.5.16.2. Vulnerabilidades detectadas em um segmento de rede;
 - 4.5.1.9.5.16.3. Vulnerabilidades detectadas em serviços específicos;
 - 4.5.1.9.5.16.4. Vulnerabilidades detectadas por um usuário específico;
 - 4.5.1.9.5.16.5. Vulnerabilidades detectadas por tag AWS ou Azure específicas;
 - 4.5.1.9.5.16.6. Vulnerabilidades detectadas em hardware específico.
- 4.5.1.9.5.17. Permitir, na busca de vulnerabilidades, o agrupamento para mostrar, no mínimo, as seguintes visualizações:
 - 4.5.1.9.5.17.1. Quantidade de ocorrências de uma mesma vulnerabilidade;
 - 4.5.1.9.5.17.2. Quantidade de vulnerabilidades por sistema operacional;
 - 4.5.1.9.5.17.3. Quantidade de vulnerabilidades por host;
 - 4.5.1.9.5.17.4. Quantidade de vulnerabilidades por Exploit disponível;
 - 4.5.1.9.5.17.5. Quantidade de vulnerabilidades por produto/software vulnerável.
- 4.5.1.9.5.18. Permitir exportar buscas e filtros criados para um dashboard;

- 4.5.1.9.5.19. Permitir salvar filtros criados em buscas para reutilização;
 - 4.5.1.9.5.20. Mostrar dashboards que consigam mostrar variação histórica de vulnerabilidades novas, corrigidas, reabertas;
 - 4.5.1.9.5.21. Permitir mostrar dashboards que contenham quantidades de vulnerabilidades associadas a ramsonware, que contém exploits públicos e que permitem exploração sem autenticação;
 - 4.5.1.9.5.22. Mostrar dashboards que mostrem o racional de vulnerabilidades que podem ser corrigidas através de patches;
 - 4.5.1.9.5.23. Mostrar patches faltantes em sistemas operacionais independente da relação com uma vulnerabilidade existente;
 - 4.5.1.9.5.24. Oferecer a possibilidade de monitorar dispositivos móveis Android ou IOS.
- 4.5.1.9.6. Quanto à gestão de vulnerabilidades de aplicações, a solução deverá:
- 4.5.1.9.6.1. Habilitar varreduras profundas dinâmicas para descobrir e catalogar todos os aplicativos da web e APIs na rede corporativa externa, redes corporativas internas e instâncias de nuvem;
 - 4.5.1.9.6.2. Permitir varreduras autenticadas, complexas e progressivas;
 - 4.5.1.9.6.3. Suportar varreduras programadas de serviços SOAP e REST API;
 - 4.5.1.9.6.4. Contar com uma API e integração com Jenkins para automação em um ambiente de CI / CD;

- 4.5.1.9.6.5. Detectar, identificar, avaliar, rastrear os 10 principais riscos OWASP (Top 10), como injeção de SQL, Cross-site script (XSS), XML External Entity (XXE), autenticação interrompida e configurações incorretas, também ameaças de WASC, vulnerabilidades CWE e CVEs associados em aplicações da web;
- 4.5.1.9.6.6. Suportar a capacidade de retestar uma vulnerabilidade específica que foi detectada anteriormente na aplicação web;
- 4.5.1.9.6.7. Ter capacidade de encontrar aplicações web aprovadas e não aprovadas em sua rede, gerando um processo contínuo de catalogação e descoberta de aplicações web;
- 4.5.1.9.6.8. Gerar tags para facilitar a localização e o uso de ativos de aplicações web encontrados;
- 4.5.1.9.6.9. Permitir que se faça a varredura de grandes aplicações da web usando um mecanismo de varredura progressiva, que deve permitir a varredura em estágios incrementais e evitar quaisquer restrições que possam surgir ao tentar fazer a varredura de um aplicativo de uma vez;
- 4.5.1.9.6.10. Definir a hora exata de início e duração das verificações;
- 4.5.1.9.6.11. Permitir gerenciar várias varreduras de aplicações web, combinando vários scanners para acelerar o processo e obter resultados mais rapidamente;
- 4.5.1.9.6.12. Fornecer relatórios resumidos e de varredura do site que podem ser exportados para os formatos HTML e PDF;

4.5.1.9.6.13. Oferecer suporte à criação de escopos e funções definidos pelo usuário e permitir que as permissões apropriadas sejam atribuídas a cada função.

4.5.1.9.7. Quanto ao mecanismo de varredura (scanner), a solução deverá:

4.5.1.9.7.1. Permitir o uso de scanners capazes de identificar vulnerabilidades através de varreduras em ranges de IP definidos pelo administrador;

4.5.1.9.7.2. Fornecer os scanners em formato de appliance virtual, ou seja, com software e sistema operacional próprios, não sendo aceito o uso de softwares de terceiros ou componentes open-source;

4.5.1.9.7.3. Permitir a instalação de uma quantidade ilimitada de scanners virtuais no ambiente;

4.5.1.9.7.4. Permitir o uso de scanners externos, sem a necessidade de instalação e em nuvem própria do fabricante, para varreduras de ativos publicados na internet;

4.5.1.9.7.5. Suportar pelo menos um dos seguintes hypervisors:

4.5.1.9.7.5.1. Hyper-V;

4.5.1.9.7.5.2. VMWare.

4.5.1.9.7.6. Suportar a varredura de ambientes em nuvem para pelo menos os seguintes provedores:

4.5.1.9.7.6.1. Azure;

4.5.1.9.7.6.2. AWS;

4.5.1.9.7.6.3. Google Cloud Platform;

4.5.1.9.7.6.4. Oracle.

- 4.5.1.9.7.7. Reportar vulnerabilidades para console em nuvem, permitindo uma visão consolidada das vulnerabilidades;
- 4.5.1.9.7.8. Permitir o agendamento de varreduras para máquinas que possuam uma determinada versão de banco de dados em execução;
- 4.5.1.9.7.9. Permitir a varredura sob demanda para um ou mais ativos de rede;
- 4.5.1.9.7.10. Permitir que o mesmo scanner varra por falhas de conformidade e por vulnerabilidades;
- 4.5.1.9.7.11. Consolidar vulnerabilidades encontradas em um ativo que possua agente instalado;
- 4.5.1.9.7.12. Permitir a configuração do tipo de varredura a ser realizada, permitindo pelo menos definir as seguintes configurações ao defini-la:
 - 4.5.1.9.7.12.1. Configuração de quantidades de portas TCP/UDP a serem validadas;
 - 4.5.1.9.7.12.2. Consumo de largura de banda e recursos (alto, médio, baixo);
 - 4.5.1.9.7.12.3. Digitalize para dispositivos que não suportam ping e/ou traceroute;
 - 4.5.1.9.7.12.4. Detecção de balanceadores de carga;
 - 4.5.1.9.7.12.5. Configuração de força bruta para usar em senhas;
 - 4.5.1.9.7.12.6. Uso de um cabeçalho HTTP personalizado;
 - 4.5.1.9.7.12.7. Ignorar pacotes;
 - 4.5.1.9.7.12.8. Instalação de agente temporário para validação de registro local.

4.5.1.9.8. Quanto à detecção e priorização de ameaças, a solução deverá:

4.5.1.9.8.1. Permitir enviar alertas em tempo real sobre irregularidades na rede, identificar ameaças e monitorar mudanças inesperadas que ocorram na mesma;

4.5.1.9.8.2. Permitir a atribuição de destinatários diferentes para cada alerta;

4.5.1.9.8.3. Enviar alertas de monitoramento sobre vulnerabilidades, configurações incorretas e outros parâmetros definidos pelo administrador da solução, para, no mínimo:

4.5.1.9.8.4. Ativos com sistemas operacionais não aprovados;

4.5.1.9.8.4.1. Certificados expirados e/ou expirando;

4.5.1.9.8.4.2. Portas abertas;

4.5.1.9.8.4.3. Vulnerabilidades graves;

4.5.1.9.8.4.4. Tickets de correção abertos, resolvidos e fechados;

4.5.1.9.8.4.5. Software não aprovado.

4.5.1.9.8.5. Fornecer fontes de inteligência de ameaças em tempo real e técnicas de aprendizado de máquina para fornecer controle de administrador sobre a evolução das ameaças relacionadas a vulnerabilidades encontradas nos ativos da organização e identificar quais corrigir primeiro;

4.5.1.9.8.6. Permitir consultas ad-hoc com múltiplas variáveis e critérios, como classe de ativo, tipo de vulnerabilidade, indicadores de ameaça em tempo real, etiqueta de ativo e sistema operacional, de modo que, por exemplo, seja possível pesquisar todas as vulnerabilidades que tenham um alta

classificação de gravidade, são fáceis de explorar e foram lançados na semana passada;

4.5.1.9.8.7. Permitir que se faça uma correlação em tempo real das ameaças ativas contra as vulnerabilidades detectadas nos ativos corporativos;

4.5.1.9.8.8. Incluir indicadores de ameaças em tempo real que ajudam a avaliar e priorizar as vulnerabilidades detectadas, categorizados da seguinte forma:

4.5.1.9.8.8.1. Dia Zero;

4.5.1.9.8.8.2. Exploração pública;

4.5.1.9.8.8.3. Ataques ativos;

4.5.1.9.8.8.4. Movimento lateral;

4.5.1.9.8.8.5. Fácil exploração;

4.5.1.9.8.8.6. Perda de dados;

4.5.1.9.8.8.7. Negação de serviço;

4.5.1.9.8.8.8. Vulnerabilidade sem patch disponível;

4.5.1.9.8.8.9. Malware;

4.5.1.9.8.8.10. Kit de exploração.

4.5.1.9.8.9. Atribuir uma pontuação a cada vulnerabilidade de forma contextual de forma a quantificar o risco associado a esta vulnerabilidade;

4.5.1.9.8.10. Considerar, quanto aos fatores de risco, pelo menos 3 dos fatores abaixo:

4.5.1.9.8.10.1. Malwares associados;

4.5.1.9.8.10.2. Atores maliciosos associados;

4.5.1.9.8.10.3. Possibilidade de remediação.

4.5.1.9.8.11. Permitir a criação de tickets de correção manualmente por um administrador de solução e automaticamente, a partir do resultado de uma varredura de vulnerabilidade, com base nas informações de um host específico.

4.5.1.9.9. Quanto ao gerenciamento de patches de segurança, a solução deverá:

4.5.1.9.9.1. Permitir aplicação de patches de segurança para, no mínimo, as plataformas abaixo:

4.5.1.9.9.1.1. Windows Embedded 7;

4.5.1.9.9.1.2. Windows 7;

4.5.1.9.9.1.3. Windows 8 e 8.1;

4.5.1.9.9.1.4. Windows 10;

4.5.1.9.9.1.5. Windows 11;

4.5.1.9.9.1.6. Windows Server 2022;

4.5.1.9.9.1.7. Red Hat Enterprise Linux 6;

4.5.1.9.9.1.8. Red Hat Enterprise Linux 7 até 7.9;

4.5.1.9.9.1.9. Red Hat Enterprise Linux 8 até 8.5;

4.5.1.9.9.1.10. CentOS 6 até 6.7;

4.5.1.9.9.1.11. CentOS 7 até 7.8;

4.5.1.9.9.1.12. Oracle Enterprise Linux

4.5.1.9.9.2. Possuir um catálogo com no mínimo 35.000 patches e permitir aplicação de patches para, no mínimo, os produtos abaixo:

4.5.1.9.9.2.1. 7-Zip;

4.5.1.9.9.2.2. Adobe Acrobat;

- 4.5.1.9.9.2.3. Adobe Flash;
- 4.5.1.9.9.2.4. Adobe Reader;
- 4.5.1.9.9.2.5. Adobe Shockwave;
- 4.5.1.9.9.2.6. Apache Software Foundation Tomcat;
- 4.5.1.9.9.2.7. Apple iCloud;
- 4.5.1.9.9.2.8. Apple iTunes;
- 4.5.1.9.9.2.9. Apple Mobile Device Support;
- 4.5.1.9.9.2.10. Apple Software Update;
- 4.5.1.9.9.2.11. Cisco Jabber;
- 4.5.1.9.9.2.12. Cisco WebEx Teams;
- 4.5.1.9.9.2.13. Citrix GoToMeeting;
- 4.5.1.9.9.2.14. Dropbox;
- 4.5.1.9.9.2.15. Evernote;
- 4.5.1.9.9.2.16. FileZilla;
- 4.5.1.9.9.2.17. Chrome;
- 4.5.1.9.9.2.18. Google Drive;
- 4.5.1.9.9.2.19. Google Desktop;
- 4.5.1.9.9.2.20. Google Drive File Stream;
- 4.5.1.9.9.2.21. Google Earth Pro;
- 4.5.1.9.9.2.22. Microsoft .Net;
- 4.5.1.9.9.2.23. Microsoft .Net Core;
- 4.5.1.9.9.2.24. Azure Site Recovery Provider;

- 4.5.1.9.9.2.25. Azure Information Protection Client;
- 4.5.1.9.9.2.26. Microsoft Content Management Server;
- 4.5.1.9.9.2.27. Windows Defender;
- 4.5.1.9.9.2.28. Microsoft Digital Image;
- 4.5.1.9.9.2.29. DirectX;
- 4.5.1.9.9.2.30. Microsoft Dynamics;
- 4.5.1.9.9.2.31. Microsoft Edge;
- 4.5.1.9.9.2.32. Microsoft Enhanced Mitigation Experience Toolkit;
- 4.5.1.9.9.2.33. Exchange Server;
- 4.5.1.9.9.2.34. Exchange System Manager;
- 4.5.1.9.9.2.35. Forefront Server;
- 4.5.1.9.9.2.36. Front Page Server;
- 4.5.1.9.9.2.37. Host Integration Server;
- 4.5.1.9.9.2.38. Microsoft Identity Manager;
- 4.5.1.9.9.2.39. Internet Explorer;
- 4.5.1.9.9.2.40. Internet Information Server;
- 4.5.1.9.9.2.41. ISA Server;
- 4.5.1.9.9.2.42. Microsoft Journal Viewer;
- 4.5.1.9.9.2.43. Live Meeting;
- 4.5.1.9.9.2.44. Live Messenger;
- 4.5.1.9.9.2.45. Lync;
- 4.5.1.9.9.2.46. Lync Server;

4.5.1.9.9.2.47. Skype for Business Server;

4.5.1.9.9.2.48. MSN Messenger;

4.5.1.9.9.2.49. Office Web Components XP;

4.5.1.9.9.2.50. Suíte Office nas versões 2000, 2002, 2003, 2007, 2010, 2013 e 2016;

4.5.1.9.9.2.51. System Center Operations Manager;

4.5.1.9.9.2.52. Microsoft SQL Server nas versões 2005, 2008, 2008 R2, 2012, 2014, 2016, 2017 e 2019;

4.5.1.9.9.2.53. SQL Management Studio;

4.5.1.9.9.2.54. Microsoft Visual Studio;

4.5.1.9.9.2.55. Windows Server 2012, 2016 e 2019;

4.5.1.9.9.2.56. Windows 7, 8, 8.1, 10 e 11.

4.5.1.9.9.3. Permitir a criação de dashboards para acompanhamento de aplicação de patches;

4.5.1.9.9.4. Permitir a inclusão de filtros personalizados nos dashboards para incluir, no mínimo, os requisitos abaixo:

4.5.1.9.9.4.1. Ativos que não possuem patches de segurança instalados;

4.5.1.9.9.4.2. Ativos pendente de boot para aplicação de patches;

4.5.1.9.9.4.3. Patches faltantes por fabricante;

4.5.1.9.9.4.4. Status de aplicação de patches;

4.5.1.9.9.4.5. Patches faltantes por severidade.

4.5.1.9.9.5. Permitir mostrar em um mesmo dashboard a quantidade de ativos que possuem um software

instalado e quantidade de patches relevantes a esse mesmo software;

- 4.5.1.9.9.6. Conter uma lista de produtos e softwares priorizados, permitindo visualizar patches relevantes a esses produtos;
- 4.5.1.9.9.7. Permitir a criação de tarefas de instalação a partir de produtos e softwares priorizados;
- 4.5.1.9.9.8. Oferecer uma interface que permita buscas com uma sintaxe lógica para visualizar detalhes de um patch específico. As buscas devem considerar, no mínimo, os filtros abaixo:
 - 4.5.1.9.9.8.1. Fabricante da aplicação ou software;
 - 4.5.1.9.9.8.2. Patches que corrigem falhas de segurança;
 - 4.5.1.9.9.8.3. Patches de sistema operacional ou aplicações;
 - 4.5.1.9.9.8.4. Severidade do fabricante;
 - 4.5.1.9.9.8.5. Número do KB ou boletim;
 - 4.5.1.9.9.8.6. CVE associado.
- 4.5.1.9.9.9. Ser capaz de apresentar informações de patches que já consideram e resolvem correções anteriores;
- 4.5.1.9.9.10. Apontar vulnerabilidades resolvidas por um determinado patch;
- 4.5.1.9.9.11. Apontar todas as versões da aplicação que são afetadas e precisam de correção;
- 4.5.1.9.9.12. Conter referências do fabricante do software ou sistema operacional contendo descrição dos patches disponíveis;

- 4.5.1.9.9.13. Possibilitar a visualização de agentes e o último status de comunicação, a quantidade de patches aplicados e faltantes;
- 4.5.1.9.9.14. Possibilitar definir o intervalo em horas para verificação de patches e reporte à console;
- 4.5.1.9.9.15. Suportar tarefas de instalação e remoção dos patches;
- 4.5.1.9.9.16. Permitir a execução de scripts personalizados durante a tarefa de instalação de patches;
- 4.5.1.9.9.17. Possibilitar a execução de scripts Powershell antes e depois da instalação de correções;
- 4.5.1.9.9.18. Permitir a instalação de softwares através de scripts;
- 4.5.1.9.9.19. Permitir a alteração de chaves de registro na tarefa de aplicação de patches;
- 4.5.1.9.9.20. Permitir, na tarefa de aplicação de correções, selecionar manualmente os patches a serem aplicados ou através de um filtro de seleção que considere, no mínimo:
 - 4.5.1.9.9.20.1. Severidade do patch;
 - 4.5.1.9.9.20.2. Fabricante;
 - 4.5.1.9.9.20.3. Associação a uma vulnerabilidade;
 - 4.5.1.9.9.20.4. Associação a riscos de segurança.
- 4.5.1.9.9.21. Possibilitar restringir a aplicação de patches à um grupo de máquinas baseados em ranges de IP, software instalado, portas abertas, serviços em execução;
- 4.5.1.9.9.22. Possibilitar o agendamento de execução de tarefas de patch de forma imediata;

- 4.5.1.9.9.23. Possibilitar agendar a execução de tarefas de patch em um horário específico com recorrência diária, semanal ou mensal;
- 4.5.1.9.9.24. Possibilitar agendar a execução de tarefas de patch com agendamento a partir do Patch Tuesday, da Microsoft, de forma automática;
- 4.5.1.9.9.25. Possibilitar configurar uma janela de tempo máximo para execução de patches em intervalo de horas ou minutos;
- 4.5.1.9.9.26. Permitir customização de mensagens para o usuário antes, durante e após a aplicação de patches;
- 4.5.1.9.9.27. Permitir o download de patches antes do início da tarefa, de forma a otimizar o processo de instalação;
- 4.5.1.9.9.28. Permitir a supressão do reinício do sistema operacional, forçá-la ou permitir que o usuário reinicie o sistema, caso o patch aplicado exija o reinício;
- 4.5.1.9.9.29. Possibilitar restringir o licenciamento a um determinado grupo de máquinas baseado em critérios como sistema operacional, presença de softwares instalados e ranges de IPs;
- 4.5.1.9.9.30. Conter a inteligência de filtrar automaticamente, sem intervenção, quais ativos receberão os patches selecionados na tarefa de patch considerando a arquitetura do sistema operacional e também a pré-existência de determinada aplicação, evitando assim instalações indesejadas;
- 4.5.1.9.9.31. Possibilitar gerar relatórios a partir do catálogo de patches a serem aplicados considerando filtros dos patches e dos ativos;
- 4.5.1.9.9.32. Filtrar no catálogo de patches a serem aplicados, de forma simples, quais são os patches que precisam

ser instalados e exibir somente as últimas versões disponíveis de cada um deles, considerando a obsolescência de versões antigas;

4.5.1.9.9.33. Possibilitar visualizar, pela interface, o status de instalação de cada uma das tarefas de patch criadas;

4.5.1.9.9.34. No status individual de cada tarefa de patch, mostrar quais patches foram instalados com sucesso, quais falharam e quais não foram instalados por não serem necessários;

4.5.1.9.9.35. Exibir, para os patches que não foram instalados com sucesso, qual o motivo do erro;

4.5.1.9.9.36. Possibilitar gerar um relatório CSV para uma tarefa de patch específica, com a finalidade de validar seu progresso e situação final de execução;

4.5.1.9.9.37. Possuir controle de acesso no modelo Role Based Access Control (RBAC), para que sejam definidos no mínimo dois perfis de usuários caso seja necessário, sendo um deles, necessariamente, incapaz de iniciar uma tarefa de execução de patch.

4.5.1.9.10. Quanto aos relatórios e dashboards, a solução deverá:

4.5.1.9.10.1. Permitir administração centralizada via interface gráfica WEB usando HTTPS;

4.5.1.9.10.2. Permitir a definição de diferentes perfis de usuários e funções para administração;

4.5.1.9.10.3. Fornecer controles de acesso de usuário hierárquicos e baseados em funções que permitem a delegação de responsabilidades para refletir a estrutura organizacional;

4.5.1.9.10.4. Permitir o acesso de um usuário autorizado de qualquer local;

- 4.5.1.9.10.5. Suportar integração com uma biblioteca API XML extensível;
- 4.5.1.9.10.6. Suportar autenticação de dois fatores para usuários e login;
- 4.5.1.9.10.7. Suportar configurações de segurança de senha;
- 4.5.1.9.10.8. Suportar a capacidade de rastrear a atividade do usuário por nome da conta do usuário, data, ação e informações sobre a ação;
- 4.5.1.9.10.9. Suportar a capacidade de distribuir relatórios em PDF com segurança por meio de uma senha e um número restrito de download de relatórios por meio do link;
- 4.5.1.9.10.10. Suportar acesso por SSO (Single Sign-on) usando SAML 2.0;
- 4.5.1.9.10.11. Permitir o controle de alterações com trilhas de auditoria à prova de violação;
- 4.5.1.9.10.12. Gerar relatórios por IPs, Grupo e Tags;
- 4.5.1.9.10.13. Permitir a geração de relatórios de qualquer IP - Host previamente verificado;
- 4.5.1.9.10.14. Permitir agendar relatórios diários, semanais, mensais e sob demanda;
- 4.5.1.9.10.15. Permitir o envio de notificações por e-mail sempre que um relatório estiver disponível para o administrador da solução, usuários específicos e perfis diferentes criados na ferramenta;
- 4.5.1.9.10.16. Permitir pelo menos os seguintes tipos de relatórios:
 - 4.5.1.9.10.16.1. Relatório de correção;
 - 4.5.1.9.10.16.2. Relatório de vulnerabilidades altamente críticas;

- 4.5.1.9.10.16.3. Relatório Executivo;
- 4.5.1.9.10.16.4. Relatório de autenticação;
- 4.5.1.9.10.16.5. Relatório de conformidade normativa e regulatória;
- 4.5.1.9.10.16.6. Relatório de remediação.
- 4.5.1.9.10.17. Fornecer relatórios de correção por grupo de ativos, usuário e vulnerabilidade;
- 4.5.1.9.10.18. Permitir a criação de relatórios baseados em IPv4, endereços IPv6, nome do host, grupo de ativos e rótulos personalizados pelo administrador;
- 4.5.1.9.10.19. Permitir relatórios com cálculo de risco de segurança, permitindo um cálculo de risco global para todos os ativos incluídos no relatório;
- 4.5.1.9.10.20. Permitir relatórios que possibilitem o cálculo do risco do negócio, utilizando como base para o cálculo do risco de impacto ao negócio e do risco de segurança dos ativos incluídos no relatório;
- 4.5.1.9.10.21. Permitir relatar as descobertas com base no status das vulnerabilidades detectadas e seu status, conforme lista abaixo:
 - 4.5.1.9.10.21.1. Novo;
 - 4.5.1.9.10.21.2. Resolvido;
 - 4.5.1.9.10.21.3. Reaberto;
 - 4.5.1.9.10.21.4. Ativo.
- 4.5.1.9.10.22. Permitir relatórios que incluam vulnerabilidades com base na data de publicação;

- 4.5.1.9.10.23. Permitir incluir ou excluir kernels Linux detectados na varredura de vulnerabilidade e que não estão em execução;
- 4.5.1.9.10.24. Permitir a exclusão de vulnerabilidades que você encontrará em uma porta ou serviço que não está em execução;
- 4.5.1.9.10.25. Permitir excluir vulnerabilidades que não são exploráveis devido à configuração do sistema / plataforma onde foi detectada;
- 4.5.1.9.10.26. Permitir a exclusão de patches da Microsoft que foram substituídos por um novo patch ou um patch cumulativo do mesmo fabricante;
- 4.5.1.9.10.27. Fornecer relatórios automatizados de tendências e diferenciais;
- 4.5.1.9.10.28. Fornecer várias opções de distribuição de relatórios, incluindo PDF criptografado;
- 4.5.1.9.10.29. Suporte à personalização do modelo de relatório conforme necessário;
- 4.5.1.9.10.30. Permitir a exportação de relatórios para os formatos HTML, MHT, PDF, DOC, CSV e XML;
- 4.5.1.9.10.31. Permitir que relatórios sejam apresentados em tabelas e gráficos com as ocorrências ocorridas, permitindo a customização detalhada de cada relatório;
- 4.5.1.9.10.32. Permitir em seus relatórios comparar o nível de conformidade entre políticas, tecnologias e ativos;
- 4.5.1.9.10.33. Possuir um painel (dashboard) que, por padrão, permite que você veja as tendências de vulnerabilidades por gravidade, plataforma, idade e status de remediação;

- 4.5.1.9.10.34. Permitir a customização dos painéis fazendo uso de qualquer um dos dados disponíveis associados aos ativos varridos para selecionar diferentes tipos de gráficos, tabelas e visualizações sobre a priorização de vulnerabilidades;
- 4.5.1.9.10.35. Fornecer painéis executivos personalizáveis com uma visão unificada de todos os componentes da solução;
- 4.5.1.9.10.36. Criar dashboards que mostrem a pontuação de risco global de ativos e sua variação ao longo do tempo.

4.5.1.10. Solução de análise em ambiente Microsoft Active Directory

- 4.5.1.10.1. A solução deve identificar fraquezas ocultas em configurações dedicadas ao Active Directory;
- 4.5.1.10.2. A solução deve possuir ações preventivas de hardening para o Active Directory;
- 4.5.1.10.3. A solução deve identificar ataque específicos para a estrutura do Active Directory;
- 4.5.1.10.4. A solução deve possuir funcionalidade para analisar em detalhes cada configuração incorreta que acarreta riscos de segurança – com uma linguagem simples, contextualizando tal risco para os times envolvidos;
- 4.5.1.10.5. A solução deve possuir recomendações de correção para cada configuração incorreta no Active Directory;
- 4.5.1.10.6. A solução deve avaliar relações de confiança perigosas entre florestas e domínios;
- 4.5.1.10.7. A solução deve capturar as mudanças que ocorrem no AD e demonstrar na console de administração;
- 4.5.1.10.8. A solução deve possuir dashboard com os principais ataques e vulnerabilidades por domínio;

- 4.5.1.10.9. A solução deve permitir a correlação de mudanças no Active Directory e desvios de segurança;
- 4.5.1.10.10. A solução deve analisar em detalhes um ataque explorando as descrições através do framework MITRE ATT&CK;
- 4.5.1.10.11. A solução deve prover interface web para gerenciamento de todas as funcionalidades;
- 4.5.1.10.12. A solução deve possuir capacidade nativa de criação de dashboards customizados;
- 4.5.1.10.13. A solução deve suportar um modelo de controle de acesso baseado em funções (RBAC) flexível;
- 4.5.1.10.14. A solução deve realizar alterações no Active Directory, seus objetos e atributos;
- 4.5.1.10.15. A solução deve armazenar ou sincronizar nenhuma credencial de objetos do Active Directory;
- 4.5.1.10.16. A solução deve suportar ambientes com múltiplas florestas e domínios;
- 4.5.1.10.17. A solução deve suportar monitoramento contínuo de ambientes com Active Directory com o nível funcional de floresta e domínio a partir do 2003;
- 4.5.1.10.18. A solução deve suportar reter os eventos coletados por no mínimo um ano;
- 4.5.1.10.19. A solução deve descobrir e mapear a superfície de ataque do Active Directory e seus domínios monitorados com os seguintes padrões:
 - 4.5.1.10.19.1. Não depender de agentes ou sensores para coleta de informações do AD;
 - 4.5.1.10.19.2. A solução deve seguir as boas práticas de menor privilégio, a conta de serviço utilizada para conexão com o Active Directory, sendo o menor nível de

acesso esperado para a conta de serviço como parte do grupo Domain User;

4.5.1.10.19.3. Interface web que consolida e apresenta de maneira unificada os domínios monitorados e as possíveis relações de confiança estabelecidas entre eles;

4.5.1.10.20. A solução deve analisar continuamente a postura de segurança do AD, minimamente avaliando:

4.5.1.10.20.1. Validação de GPOs desvinculadas, desabilitadas ou órfãs;

4.5.1.10.20.2. Validação de contas desativadas em grupos privilegiados;

4.5.1.10.20.3. Domínio usando uma configuração perigosa de compatibilidade com versões anteriores por meio de alterações no atributo dSHeuristics;

4.5.1.10.20.4. Validação de atributos relacionados a roaming de credenciais vulneráveis (ms-PKI-DPAPIMasterKeys) gerenciados por um usuário sem privilégios;

4.5.1.10.20.5. Validação de domínio sem GPOs de proteção de computador, desativando protocolos vulneráveis antigos, como NTLMv1;

4.5.1.10.20.6. Validação de contas com senhas que nunca expiram;

4.5.1.10.20.7. Validação de senhas reversíveis em GPOs;

4.5.1.10.20.8. Validação de uso de senhas reversíveis em contas de usuário;

4.5.1.10.20.9. Validação de utilização de protocolo criptográfico fraco (Ex. DES) em contas de usuário;

4.5.1.10.20.10. Validação de uso do LAPS (Solução de senha de administrador local) para gerenciar senhas de contas locais com privilégios;

- 4.5.1.10.20.11. Validação se o domínio possui um nível funcional desatualizado;
- 4.5.1.10.20.12. Validação de contas de usuário utilizando senha antiga;
- 4.5.1.10.20.13. Validação se o atributo AdminCount está definido em usuários padrão;
- 4.5.1.10.20.14. Validação do uso recente da conta de administrador padrão;
- 4.5.1.10.21. Validação de usuários com permissão para ingressar computadores no domínio;
- 4.5.1.10.22. Validação de contas dormentes;
- 4.5.1.10.23. Validação de computadores executando um sistema operacional obsoleto;
- 4.5.1.10.24. Validação de restrições de logon para usuários privilegiados em ambiente com múltiplos tiers (1, 2 e 3) de segregação de ativos;
- 4.5.1.10.25. Validação de direitos perigosos configurados no Schema do AD;
- 4.5.1.10.26. Validação de relação de confiança perigosa com outras Florestas e Domínios;
- 4.5.1.10.27. Validação de contas que possuem um atributo perigoso de histórico SID (SID History);
- 4.5.1.10.28. Validação de contas utilizando controle de acesso compatível com versões anteriores ao Windows 2000;
- 4.5.1.10.29. Validação da última alteração de senha do KDC;
- 4.5.1.10.30. Validação da última alteração da senha da conta SSO do Azure AD;
- 4.5.1.10.31. Validação de contas que podem ter senha em branco/vazia;

- 4.5.1.10.32. Validação de utilização do grupo nativo Protected Users;
- 4.5.1.10.33. Validação de privilégios sensíveis (Ex. Debug a program, Replace a process level token, etc.) perigosos atribuídos aos usuários;
- 4.5.1.10.34. Validação de possível senha em clear-text;
- 4.5.1.10.35. Validação de sanidade das GPOs e componentes CSEs (Client-Side Extension);
- 4.5.1.10.36. Validação de uso de algoritmos de criptografia fracos na PKI do Active Directory;
- 4.5.1.10.37. Validação de contas de serviço com SPN (Service Principal Name) que fazem parte de grupos privilegiados;
- 4.5.1.10.38. Validação de contas anormais nos grupos administrativos padrão do AD;
- 4.5.1.10.39. Validação de consistência no container adminSDHolder;
- 4.5.1.10.40. Validação de delegação Kerberos perigosa;
- 4.5.1.10.41. Validação em permissões de objetos raiz que permitem ataques do tipo DCSync;
- 4.5.1.10.42. Validação de políticas de senha fracas aplicadas aos usuários;
- 4.5.1.10.43. Validação das permissões relacionadas às contas do Azure AD Connect;
- 4.5.1.10.44. Validação do ID do grupo primário do usuário (Primary Group ID);
- 4.5.1.10.45. Validação de permissões em GPOs sensíveis associadas aos Containers Configuration, Sites, Root Partition e OUs sensíveis como Domain Controllers;
- 4.5.1.10.46. Controladores de domínio gerenciados por usuários ilegítimos;

- 4.5.1.10.47. Validação de certificado mapeado através de atributo altSecurityIdentities em contas privilegiadas;
- 4.5.1.10.48. Validação de uso de protocolo Netlogon inseguro (ZeroLogon/CVE-2020-1472);
- 4.5.1.10.49. A solução deve identificar vulnerabilidades e configurações incorretas do AD à medida que são introduzidas sendo:
 - 4.5.1.10.49.1. Identificar todas as vulnerabilidades e configurações incorretas no AD;
 - 4.5.1.10.49.2. Monitorar relações de confiança perigosas em toda a estrutura AD;
 - 4.5.1.10.49.3. Apresentar ameaças e alterações sem a necessidade de scans estáticos e programados no Active Directory e sua infraestrutura;
 - 4.5.1.10.49.4. Apresentar as ameaças e alterações em tempo real ou em menos de cinco minutos;
- 4.5.1.10.50. Detecção e resposta a ataques:
 - 4.5.1.10.50.1. Monitorar continuamente os indicadores de possíveis ataques como DCSync, DCShadow, Password Spraying, Password Guessing/Brute Force, Lsaas Injecton nos controladores de domínio, Golden Ticket, NTLM Relay, entre outros;
 - 4.5.1.10.50.2. Detecção de ataques ao AD em tempo real ou em menos de um minuto;
 - 4.5.1.10.50.3. Análise detalhada do ataque, apresentando ativo de origem, vetor de ataque, controlador de domínio afetado, técnica aplicada;
 - 4.5.1.10.50.4. Apresentação de ataques em uma linha do tempo;
 - 4.5.1.10.50.5. Investigar ameaças, reproduzir ataques e procurar por backdoors;

- 4.5.1.10.50.6. Permitir busca ágil de eventos específicos na base da solução através de queries customizadas;
- 4.5.1.10.51. A solução deve ser capaz de enviar alertas por e-mail;
- 4.5.1.10.52. A solução nativamente deve ser capaz de se integrar com SIEM através de protocolo SYSLOG;
- 4.5.1.10.53. A solução deve ser capaz de filtrar e enriquecer os eventos que serão enviados para o SIEM;
- 4.5.1.10.54. A solução deve possuir conjunto de APIs REST, todas as chamadas disponíveis devem estar contidas na documentação;
- 4.5.1.10.55. A solução deve permitir a criação de listas de exclusões, suportando minimamente Exclusão por domínios do AD monitorados e por itens analisados;
- 4.5.1.10.56. A solução deve ser licenciada pelo número de usuários habilitados.

4.6. Simulação de ataques

- 4.6.1. Prestação de serviço de simulação de ameaças e análise de postura dos controles de segurança, com o objetivo de simular a exploração das vulnerabilidades reportadas de modo a priorizá-las e que seja testado a efetividade do plano de remediação proposto.
 - 4.6.1.1. Implantação, planejamento, execução, análise e relatório de testes automatizados, repetíveis e continuados de segurança com ferramenta de simulação de violações e ataques (breach and attack simulation – BAS), visando:
 - 4.6.1.1.1. Avaliar e validar a eficácia operacional dos controles de segurança e identificar as lacunas na cadeia e postura de segurança;
 - 4.6.1.1.2. Avaliar e validar se as fontes de registros e telemetria e as regras de monitoramento, detecção e resposta estão sendo

capturadas pela ferramenta de monitoramento, buscando também reduzir falsos positivos e negativos;

4.6.1.1.3. Executar simulações de ataque que compõem hipóteses a serem validadas no processo de caçada contínua de ameaças e gerar registros (logs) e evidências para a busca nas ferramentas envolvidas no processo;

4.6.1.1.4. A CONTRATADA deve, de forma continuada e periódica:

4.6.1.1.4.1. Identificar e entender os ativos-alvo mais críticos e representativos para aplicação dos testes de segurança automatizados;

4.6.1.1.4.2. Criar e configurar os casos de uso, processos, ciclos e cobertura de testes;

4.6.1.1.4.3. Administrar e monitorar a execução dos testes, analisar e reportar os resultados e recomendações decorrentes;

4.6.1.1.4.4. Configurar e calibrar a Solução de testes de segurança de forma a otimizar a eficácia das detecções e alertas e reduzir o tempo médio para detecção (MTTD) e o tempo médio de reparo (MTTR) das falhas de segurança;

4.6.1.1.4.5. O licenciamento da solução ofertada deverá abranger todo o parque da CONTRATANTE, possibilitando a instalação de seus agentes em todas as máquinas, ainda que sejam realizadas simulações em apenas 200 (duzentos) ativos por mês;

4.6.1.1.4.6. Criar e melhorar painéis (dashboards) e relatórios personalizados para apresentar resultados objetivos e abrangentes.

4.6.1.2. Para realização das simulações de ataque deve ser entregue uma ferramenta com as seguintes características:

- 4.6.1.2.1. Os itens que compõem a Solução de Simulação de Ameaças e seu sistema de gerenciamento devem ser produzidos pelo mesmo fabricante;
- 4.6.1.2.2. Não serão aceitos componentes baseados em software projetados para uso genérico, devendo estes serem providos por fabricantes amplamente consolidados no mercado. Como referência de mercado serão adotados estudos de institutos de análise independente e imparcial, como Gartner, Forrester, IDC, ISG Group;
- 4.6.1.2.3. A solução deve contemplar a versão de software e/ou firmware mais estável e recomendado pelo fabricante;
- 4.6.1.2.4. O fabricante deve possuir rede de inteligência (threat intelligence) própria da solução para atualização constante de ameaças (threat feed) de forma automática;
- 4.6.1.2.5. Permitir o gerenciamento centralizado da ferramenta, por meio de interface gráfica (GUI), nos formatos web segura (https) ou em formato de aplicativo cliente compatível com Windows 11 e superior, podendo ser em nuvem (cloud), appliance virtual ou por meio da própria solução;
- 4.6.1.2.6. Sendo a gerência em cloud (nuvem), o encaminhamento de dados deve ser criptografado e protegido, sem enviar dados dos usuários e armazenados de forma criptografada;
- 4.6.1.2.7. Quanto à arquitetura, a solução deverá:
 - 4.6.1.2.7.1. Possuir agentes (softwares que possam ser instalados em máquinas, ou em ambientes virtuais (servidores), confeccionadas para simulação de ataques ou apresentar atores simuladores) virtuais, podendo ser arquivos *.OVA , com a capacidade de criar um local próprio capaz de permitir a reprodução de ataques;
 - 4.6.1.2.7.2. Possuir agentes compatíveis com sistemas operacionais Linux e Windows (Server e 11);

4.6.1.2.7.3. Possibilitar a instalação de agentes, ou máquinas OVA/ ISO em ambientes de cloud (nuvem).

4.6.1.2.8. Quanto as suas principais características, a solução deverá:

4.6.1.2.8.1. Ser capaz de simular ataques em gateways de web e e-mail, web application firewall (WAF), em endpoints (EDR, Antivírus), simular ataques em toda a cadeia de destruição cibernética (Cyber Kill Chain), incluindo infiltração, movimento lateral e exfiltração de dados, phishing, ransomwares, violações de segurança e ataques persistentes avançados (APTs);

4.6.1.2.8.2. Não trazer qualquer risco real de infectar a rede do cliente em suas atividades;

4.6.1.2.8.3. Ter seu portfólio de ataques baseado em frameworks de segurança cibernética, no mínimo MITRE ATT&CK e OWASP;

4.6.1.2.8.4. Possuir portfólio de ataques, templates ou cenários que deverá ser atualizado continuamente, de forma manual e automática, com a opção de agendar a atualização em determinado período;

4.6.1.2.8.5. Possibilitar a configuração de cenários de ataque, permitindo a seleção de quais ataques executar no teste;

4.6.1.2.8.6. Permitir o agendamento de simulações com a opção de execução contínua e automatizada;

4.6.1.2.8.7. Possibilitar a execução ilimitada de todos os vetores de simulação disponíveis pela plataforma durante a vigência do mesmo;

4.6.1.2.8.8. Possuir base ampla de recomendação de remediação possibilitando visualizar ações de correção, redução do impacto da vulnerabilidade/ataque e prevenção alinhados com

as recomendações específicas dos fabricantes de elementos de segurança;

4.6.1.2.8.9. Possuir atualização diária da base de malwares;

4.6.1.2.8.10. Possuir a instrumentação de IoCs (Indicators of Compromise) provenientes de provedores de Threat Intelligence e/ou laboratório de inteligência de ameaça do fabricante da solução;

4.6.1.2.8.11. Possuir simulações de campanhas de ameaças, com link para o relatório da identificação e descrição da ameaça em campo, descrevendo seus impactos e identificando as regiões do mundo afetadas pela campanha;

4.6.1.2.8.12. Disponibilizar APIs (Application Programming Interfaces) que permitam sua integração com demais soluções de segurança;

4.6.1.2.8.13. Possuir integração nativa com soluções de SIEM;

4.6.1.2.8.14. Possuir integração nativa com soluções de EDRs.

4.6.1.2.9. Quanto aos dashboards, a solução deverá:

4.6.1.2.9.1. Possuir dashboard com visualização dos resultados das simulações que retratem o nível de risco para cada fase do Cyber Kill Chain ou do MITRE ATT&CK com a possibilidade de customizar as visões apresentadas;

4.6.1.2.9.2. Apresentar dados históricos de diferentes ataques simulados, bem como a visão de rastreamento;

4.6.1.2.9.3. Detalhar:

4.6.1.2.9.3.1. Tipo de ataque simulado;

4.6.1.2.9.3.2. O que o artefato executou;

4.6.1.2.9.3.3. Data em que a simulação do ataque aconteceu;

4.6.1.2.9.3.4. Taxa de penetração.

4.6.1.2.9.4. Quanto aos relatórios e logs a solução deverá:

4.6.1.2.9.4.1. Apresentar relatórios e registros de auditoria detalhados, que identifiquem o histórico completo de acessos (logins) e ações, por cada usuário ou grupo de usuários;

4.6.1.2.9.4.2. Ter a opção de gerar relatórios após cada avaliação comparando com o resultado de testes anteriores, mostrando as vulnerabilidades mais críticas;

4.6.1.2.9.4.3. Permitir exportar relatórios para no mínimo no formato PDF ou CSV (Comma-separated values);

4.6.1.2.9.4.4. Apresentar relatório detalhando a ação do ataque simulado;

4.6.1.2.9.4.5. Permitir exportar os logs da solução via API ou conectores compatíveis com o SIEM;

4.6.1.2.9.4.6. Ser capaz de criar incidentes de forma manual e automática por meio de integrações com o SIEM.

4.7. Gestão de risco de terceiros

4.7.1. A plataforma/serviço deve identificar falhas/vulnerabilidades nos principais domínios de segurança, incluindo: segurança de rede, segurança de aplicativos, integridade do DNS, segurança de terminais, reputação de IP, cadência de patches, canais hackers, informações vazadas e phishing.

4.7.2. As descobertas devem ser detectadas por meio de fonte de dados ativa, passiva e de terceiros. Os métodos ativos de coleta de dados devem incluir sensores que rastreiam a Internet em busca de vulnerabilidades e fraquezas de segurança que podem ser exploradas por atores mal-intencionados. Os métodos de dados passivos, como buracos (Sinkhole), honeypots e coleta de dados de trocas de publicidade, bem como fontes de terceiros devem completar a coleta para fornecer uma imagem abrangente dos controles de segurança das empresas que estão sendo monitoradas.

- 4.7.3. A plataforma/serviço deve incluir no mínimo os principais fornecedores selecionados por empresa e poder catalogar rapidamente novos fornecedores que podem ou não ser monitorados no momento. Descrevendo a cobertura atual (empresas / domínios / IPs) do serviço e quanto tempo leva para avaliar uma nova empresa.
- 4.7.4. Deve suportar a evidência da fonte das descobertas na plataforma de terceiros utilizados, usando fontes como WHOIS, certificados SSL, pesquisa de DNS, dados publicados, fontes de dados de terceiros para dar suporte ao processo de avaliação.
- 4.7.5. Este serviço/plataforma também deve fornecer uma maneira de visualizar possíveis violações existentes, possíveis sistemas comprometidos e dados que podem indicar transferência de arquivos ponto a ponto.
- 4.7.6. As informações devem ser compartilhadas em um nível detalhado para qualquer terceiro a ser monitorado, informações como endereço IP, fonte de dados, descrição da vulnerabilidade, risco, recomendação de correção, links para fontes de informações de correção, além de informações sobre a data da detecção, data da última observação e bem como o impacto na pontuação.
- 4.7.7. Deve também permitir a identificação de possíveis vulnerabilidades que possam ser observadas externamente bem como o tempo durante o qual estão ativas.
- 4.7.8. A plataforma/serviço deve oferecer a possibilidade de ajustar os ativos digitais identificados pelas empresas (impressão digital). Mesmo após uma fusão / aquisição para obter resultados precisos atualizados.
- 4.7.9. A solução deve fornecer recursos analíticos profundos, incluindo a capacidade de entender nosso desempenho relativo da organização no contexto de pares. Esta solução também deve fornecer uma profunda visão forense para analisar possíveis problemas tanto na própria infraestrutura como na monitorização de terceiros, bem como uma ferramenta para prever modificações e simulações de alteração do Rating.
- 4.7.10. O Rating Risco Cibernético deve ter, no mínimo, as seguintes características:
 - 4.7.10.1. Atualizações diárias, para cada entidade monitorada.

- 4.7.10.2. Dados de histórico diário até 12 meses, desde que a empresa esteja monitorada na solução.
- 4.7.10.3. O escaneio automático das vulnerabilidades deve ir até ao máximo de 31 dias.
- 4.7.10.4. Cada vetor de risco que compõem a classificação deve ser avaliado individualmente.
- 4.7.10.5. A correlação entre Data Breaches e o Rating de Risco Cibernético deve ter sido validado independentemente por meio de uma terceira parte independente.
- 4.7.10.6. Todos os eventos que impactam o Rating devem ser apoiados com evidência objetiva, verificável e que também permita uma ação nos mesmos e a pontuação do impacto no score visível.
- 4.7.10.7. Visualização total da pegada digital (Digital Footprint composta por IP's, Domínios e Subdomínios) para todos os vendedores monitorados sem necessidade de autorização para o vendedor, com a evidência para cada.
- 4.7.10.8. Escaneio de todos os IP's quer da própria entidade, quer de todos os terceiros/fornecedores, no máximo a cada 45 dias com data de validação na solução.
- 4.7.10.9. Solução nativa de envio e recepção de questionários de segurança customizados em português do Brasil é totalmente customizável sobre qualquer questionamento de segurança ou não
- 4.7.10.10. Possibilidade de criação de scores customizados pela digital footprint e/ou localização dos IP's quer para a própria organização, bem como para qualquer terceiro a monitorar.
- 4.7.10.11. Ferramenta nativa de plano de ações a tomar refletindo o melhoramento do score.
- 4.7.10.12. Relatórios resumidos e detalhados traduzidos na solução para português do Brasil, espanhol, alemão português de Portugal, francês, japonês, chinês e coreano.

- 4.7.10.13. As vulnerabilidades ou eventos detectados na solução e identificadas como remediadas pelo usuário e aceites pela solução como tal (com exceção da cadência de patches) o impacto das mesmas não pode mais afetar o score em mais de 48 horas.
- 4.7.10.14. A possibilidade de estabelecer ações automáticas de alguma nova vulnerabilidade, evento ou incidente afeta alguma entidade/score como envio automático de relatórios resumidos e detalhados para usuários do cliente no portal, copiar as entidades afetadas para portfolios a eleger, enviar alertas para qualquer usuário do cliente eleito pelo mesmo.
- 4.7.10.15. A metodologia, cálculo e algoritmo têm de ser públicos e publicados na internet, bem como dados a conhecer a qualquer usuário ou empresa que o solicite.
- 4.7.10.16. A solução deve ter publicada em portal da transparência o detalhe de sua metodologia acessível de forma pública.
- 4.7.10.17. Possuir um sistema de marcação (tags) para cada entidade monitorada.
- 4.7.10.18. Deve possuir a funcionalidade de visualização das entidades monitoradas em nível geral (watchlist) com informações sobre seu score e a variação desse nos últimos 30 dias sem que isso impacte a quantidade de entidades monitoradas em nível profundo.
- 4.7.11. A solução/serviço deve possuir os seguintes vetores de risco:
- 4.7.11.1. A solução deverá coletar dados no SPF Records, e mencionar em separado o que é de SPF Record Missing; SPF Record Contains a Softfail; SPF Record Contains Wildcard; Malformed SPF Record;
- 4.7.11.2. A solução tem de coletar dados em certificados TLS / SSL, incluindo se usa Weak Cypher;
- 4.7.11.3. A solução tem de coletar dados em certificados SSL / TLS expirados;
- 4.7.11.4. A solução tem de coletar dados sobre vulnerabilidades SSL / TLS;

- 4.7.11.5. A solução tem de coletar dados nos cabeçalhos de aplicativos da Web;
- 4.7.11.6. A solução tem de incluir dados sobre redirecionamento entre HTTP e HTTPS e vice-versa.
- 4.7.11.7. A solução deve levar em conta os sinais de vulnerabilidades da própria superfície de ataque e de terceiros que podem gerar possíveis conflitos com normas como CISv8, CSA-CCM, ISO/IEC 27001:2022, ISO/IEC 27001:2013, NIST CSF, NIST SP 800-53 rev5, SOC2 e MITRE. Os conflitos devem ser sinalizados e relacionados com os respectivos controles das normas.
- 4.7.11.8. A solução tem de identificar serviços em execução em portas abertas (independentemente do número de porta, que permita a ligação não ser o padrão para o serviço)
- 4.7.11.9. A solução tem de coletar dados nos registros DNSSEC
- 4.7.11.10. A solução tem de coletar dados de Software de Servidores
- 4.7.11.11. A solução tem de coletar dados sobre a existência de vulnerabilidades detectadas em serviços expostos à Internet, que já tenham sido alvo de correções por parte do fabricante
- 4.7.11.12. A solução tem de coletar dados sobre se as organizações estão executando Sistemas Operacionais de desktop e navegadores (browsers) não mais suportados
- 4.7.11.13. A solução tem de coletar dados sobre se as organizações estão com Bitcoin Server exposto
- 4.7.11.14. A plataforma deve permitir que a EMPRESA demarque e identifique vários elementos da sua digital footprint, como Wi-Fi ou Redes Guest ou domínios de segurança que podem incluir laboratórios ou outros tipos de serviço, através de envio que existe um controle de compensação ativo, esta opção tem de figurar na interface do usuário.
- 4.7.11.15. Deve fornecer acesso à plataforma a um fornecedor por tempo ilimitado.

- 4.7.11.16. A solução deve ser capaz de mostrar rapidamente quais fornecedores têm infecções.
- 4.7.11.17. A solução deve ser capaz de mostrar rapidamente quais fornecedores têm vulnerabilidades, e quais.
- 4.7.11.18. A solução deve oferecer aos fornecedores-alvo a capacidade de ver seu rating gratuitamente.
- 4.7.11.19. A solução deve permitir que os fornecedores-alvo possam acessar à plataforma a convite da EMPRESA, gratuitamente, tenham apoio durante esse acesso por parte do fabricante, e se o entenderem, possam contestar as descobertas facilmente, bem como, se o pretenderem, possam criar uma visão da sua infraestrutura com maior contexto interno – como por exemplo uma estrutura sem os IPs correspondentes a redes usadas para serviços Wi-Fi ou de Hospedagem de clientes.
- 4.7.11.20. A solução tem de demonstrar com transparência a percentagem de impacto que determinada vulnerabilidade tem no score tanto da EMPRESA como de qualquer terceiro que a EMPRESA esteja a monitorar.
- 4.7.11.21. Incluir algum tipo de previsão de correção (remediação) para indicar melhorias no rating se forem tomadas ações específicas
- 4.7.11.22. Permite baixar todos os dados de descobertas com os IPs mostrados, para que se possa corrigir esses itens off-line, tanto da infra da EMPRESA como de qualquer terceiro que a EMPRESA esteja monitorando.
- 4.7.11.23. Oferecer a possibilidade de customizar um scorecard por IPs, Domínios, ou localização geográfica, tanto para a EMPRESA como para qualquer terceiro que a EMPRESA esteja a monitorar, essa opção deve ser realizada pela EMPRESA sem a necessidade de suporte.
- 4.7.11.24. A digital footprint de todas as empresas mapeadas no portal/solução têm de ser atualizadas automaticamente no mínimo a cada 45 dias, para validação da pegada digital (digital footprint).

- 4.7.11.25. A solução/portal tem de ter um mínimo de 12.000.000 de empresas/entidades/organizações já mapeadas no portal e disponível para monitorização imediata pelo usuário
- 4.7.11.26. A solução para mapeamento de uma nova empresa/organização/entidade não pode levar mais de 10 minutos para que essa nova empresa/organização/entidade fique disponível no portal.
- 4.7.11.27. A EMPRESA tem de ter acesso à visualização de toda a digital footprint, entenda-se por IPs e Domínios/subdomínios de qualquer terceiro que a EMPRESA deseje monitorar, sem que seja necessária a autorização desse terceiro para tal.
- 4.7.11.28. Os usuários deverão ver dados forenses detalhados dos eventos detectados de qualquer terceiro que a EMPRESA necessite de monitorizar.
- 4.7.11.29. Toda e qualquer vulnerabilidade presente deve ter visível qual o impacto que essa vulnerabilidade afetou ou afeta o score/rating.
- 4.7.11.30. Evitar a exclusão de endereços IP dos dados do fornecedor (sem documentação suficiente) para garantir que eles não estão manipulando o rating.
- 4.7.11.31. O comparativo em análise para cada vulnerabilidade deve ser tomado em base de comparação com empresas com o mesmo número de IPs, exemplo EMPRESA em certificados expirados é comparada com empresas/organização/entidade com um número de IPs semelhante.
- 4.7.11.32. A solução deve oferecer um processo totalmente interativo para ajustar as coletas digitais das empresas na plataforma, com a possibilidade de remover endereços IP que podem não ser necessários e adicionar endereços IP. Também deve permitir ao usuário gerar scorecards personalizados tanto para a EMPRESA como para qualquer terceiro, com base em linhas de negócios, linhas de serviço, subsidiárias etc. O usuário também deve ter a possibilidade de fornecer informações sobre subsidiárias e fusões que podem ser agrupadas em um único scorecard.

- 4.7.11.33. Deve oferecer métodos de suporte à correção para seus clientes, primeiro, na própria plataforma, com as orientações de correção para o problema. A EMPRESA também pode gerar seus próprios scorecards e planos de correção, mostrando o risco dos problemas identificados e o impacto na pontuação, se o problema for corrigido.
- 4.7.11.34. A solução/plataforma deve permitir usuários ilimitados para acesso à plataforma.
- 4.7.11.35. Deve ser considerado líder por pelo menos uma empresa de análise ou independente como Forrester ou Gartner.
- 4.7.11.36. Deve ter um processo independente para esclarecer qualquer disputa envolvendo o Rating.
- 4.7.11.37. Deverá ter a possibilidade de configurar alertas por usuário para portfólios, direcionados também em relação à modificação de qualquer família de risco.
- 4.7.11.38. Deverá ter a possibilidade de exibir fornecedores em um quadrante de risco, a fim de priorizar o envolvimento do fornecedor e analisar o risco.
- 4.7.11.39. Os relatórios da solução/serviço devem fornecer:
 - 4.7.11.39.1. Relatório resumido em português do Brasil.
 - 4.7.11.39.2. Relatório dos eventos encontrados
 - 4.7.11.39.3. Relatório detalhado com detalhe forense visível ao nível do IP afetado, seja nos relatórios gerados para a infra da EMPRESA como nos relatórios gerados para a infraestrutura de qualquer terceiro monitorado em português do Brasil.
- 4.7.11.40. Deve incluir relatórios de tendências históricas e classificações de segurança de terceiros. Descrever o nível de detalhes que seu serviço fornece para entender e analisar o progresso histórico ou declínio de uma empresa ao longo do tempo.
- 4.7.11.41. Deve fornecer relatórios em vários níveis, incluindo para cada empresa: relatórios resumidos, relatórios de nível de problemas, vulnerabilidades, relatórios detalhados e relatórios de parceria. Os relatórios de resumo em alto nível (Diretores e C-Level), relatórios de comparação da empresa, etc. Por meio da API, o cliente também deve ter a flexibilidade de se envolver em relatórios ad-hoc, conforme desejado.
- 4.7.11.42. A plataforma/ serviço deve incluir análise de ameaças.

- 4.7.11.43. O detalhe dos eventos deve ter, no mínimo, as seguintes características:
- 4.7.11.43.1. Visão sobre eventos de infecção para a própria empresa e para qualquer terceiro, que deve incluir detalhes forenses.
 - 4.7.11.43.2. Deverá possuir infraestrutura própria de Sinkhole.
 - 4.7.11.43.3. Deverá ser capaz de fazer referência cruzada das descobertas dos sinkholes próprios com outros para minimizar falsos positivos
- 4.7.11.44. A solução/serviço deve:
- 4.7.11.44.1. Coletar dados sobre infecções por botnet
 - 4.7.11.44.2. Coletar dados sobre propagação de spam
 - 4.7.11.44.3. Coletar dados em servidores de malware
 - 4.7.11.44.4. Identificar comunicações não solicitadas externamente, como por exemplo, port-scan originários da infraestrutura da empresa.
 - 4.7.11.44.5. Coletar dados em sistemas executando aplicativos potencialmente indesejados, como por exemplo, adware.
 - 4.7.11.44.6. Identificar malware específico por nome, fornece detalhes e instruções de correção
- 4.7.11.45. O modelo de pontuação deve ser determinístico, ou seja, um fornecedor ou EMPRESA pode ver no nível do problema como sua pontuação é impactada positiva ou negativamente por um problema específico.
- 4.7.11.46. Deve possuir processo de colaboração que permite que terceiros corrijam seus problemas e melhorem sua pontuação (processo de convite, correção e validação)
- 4.7.11.47. Deve oferecer suporte especializado à análise de ameaças identificadas pela plataforma.
- 4.7.11.48. O SLA referente à resposta do suporte, correção de problemas ou correção de dados após o envio deve ser de no máximo 24 horas úteis.
- 4.7.11.49. Um evento/vulnerabilidade remediada na infra da EMPRESA ou de qualquer terceiro e informada essa resolução através do portal o impacto deve ser resolvido para zero em máximo de 72 horas, após certificação e confirmação pelo portal de que a vulnerabilidade já não é existente, com exceção de atualização da cadência de patches que no máximo deverá tomar 120 dias.
- 4.7.11.50. Processo de mapeamento de empresas:

- 4.7.11.50.1. Os mapeamentos da empresa devem incluir IPs, domínios e subdomínios, com a visibilidade desses em qualquer empresa monitorada.
- 4.7.11.51. Alertas devem ser fornecidos imediatamente após a detecção da regra de acionamento. Esses alertas podem ser enviados na forma de um e-mail ou podem ser capturados diretamente através de uma API (Application Programming Interface) para serem capturados em uma fonte central na EMPRESA.
- 4.7.11.52. A solução deve fornecer uma API REST completa. A API deve estar totalmente acessível na plataforma e incluída nas taxas de assinatura. Além disso, possuir integrações prontas para uso com todas as principais ferramentas de GRC, Ticket Management, SIEM, IDM (ex: Service Now - VRM; Service Now - IT SM; RSA Archer GRC; Splunk; SAI Global; IBM QRadar; LockPath; ProcessUnity; Rsam; Venminder; ORACLE CASB; Glavaníze; Egan-Jones; Aravo; RMS; Third Party Trust; Proactive Risk; NRI Secure – Secure SketCH; One Trust Vendorpedia; DFLabs; SecurityGate IO/OT RM ; Crowdstrike; Palo Alto Cortex XSOAR; Teams, Slack e Jira).
- 4.7.11.53. A Solução deverá fornecer um painel de alertas para TODOS os alertas
- 4.7.11.54. Os alertas deverão ser configurados por alterações percentuais no rating
- 4.7.11.55. Os alertas podem ser configurados por alterações nas notas dos vetores de risco
- 4.7.11.56. Os alertas podem ser configurados pelos portfólios de terceiros.
- 4.7.11.57. Os alertas podem ser enviados por e-mail se solicitado
- 4.7.11.58. A solução tem de possibilitar automatização de processos, exemplo:
 - 4.7.11.58.1. Vulnerabilidade(s) detectada (s) = envio automático de relatório resumido e/ou detalhado.
 - 4.7.11.58.2. Vulnerabilidade(s) detectada (s) = envio automático de alerta(s) para o usuário e/ou usuários que se configurem no portal.
 - 4.7.11.58.3. Vulnerabilidade(s) detectada (s) = envio automático de questionário ou questionários, customizados ou não.
 - 4.7.11.58.4. Vulnerabilidade(s) detectada (s) = envio automático de notificação para a plataforma SLACK
 - 4.7.11.58.5. Vulnerabilidade(s) detectada (s) = envio automático de notificação para a plataforma TEAMS.

- 4.7.11.58.6. Vulnerabilidade(s) detectada (s) = envio automático de ticket para a plataforma JIRA
- 4.7.11.58.7. Vulnerabilidade(s) detectada (s) = envio automático de ticket para a plataforma ZENDESK.
- 4.7.11.58.8. Vulnerabilidade(s) detectada(s) = anexação automática da empresa afetada em determinado portfolio.
- 4.7.11.59. A solução deve possuir a opção de criar regras que abarcam o envio de relatórios automatizados, automatização do fluxo de alertas e ações secundárias, baseadas em um calendário configurável e/ou gatilhos. Ademais, as regras devem ser capazes de acionar um fluxo de trabalho que possa derivar ações em ferramentas ITSM integradas, como abertura de chamados em ex.: Jira, Slack, Teams, Zendesk.
- 4.7.12. Gestão de Questionários (Questionnaires)
 - 4.7.12.1. A solução deve ter uma solução nativa para envio e recepção de questionários baseados em frameworks como GDPR, ISO, NIST, HIPAA, TISAX, CSA, PCI bem como a possibilidade de o usuário poder customizar os seus próprios questionários em português do Brasil para a LGPD e BACEN 4658, ou em Português Europeu como por exemplo sobre o quadro de ciber segurança Nacional.
 - 4.7.12.2. Os questionários têm de possibilitar perguntas relacionadas com controles detectados no portal de ratings e de forma resumida mostrar evidência do portal de ratings para a validação da resposta de forma parametrizável e automática, também não sendo necessário estar a monitorar essa empresa/entidade/organização no momento da revisão do questionário.
 - 4.7.12.3. Deve ser possível customizar um questionário em português sobre LGPD (Lei Geral de Proteção de Dados do Brasil) e BACEN 4658.
 - 4.7.12.4. A solução deve incluir gerenciamento de questionário do fornecedor
 - 4.7.12.5. A solução deve ter a capacidade de mapear os dados de pontuação de segurança no questionário
 - 4.7.12.6. A solução deve ter a capacidade de enviar questionários personalizados e questionários pré-existent
 - 4.7.12.7. A solução deve ter a capacidade de adicionar ponderações personalizadas às respostas do questionário
 - 4.7.12.8. A solução deve proporcionar a possibilidade de automatizar o envio de um determinado questionário anualmente, semestralmente ou trimestralmente

- 4.7.12.9. A solução deve permitir determinar uma data limite para a conclusão de resposta do questionário enviado.
- 4.7.12.10. A solução deve proporcionar a possibilidade de enviar o questionário utilizando o email do destinatário ou apenas o domínio da organização entrevistada.
- 4.7.12.11. A solução deve possibilitar que o destinatário possa determinar colaboradores para a resposta do questionário mediante o compartilhamento do link que dá acesso ao mesmo.
- 4.7.12.12. Deve ser possível adicionar templates de questionários através da UI utilizando um arquivo Excel.
- 4.7.12.13. Deve ser possível acompanhar o progresso em porcentagem da resposta de cada questionário enviado
- 4.7.12.14. A solução deve permitir baixar os questionários respondidos em um formato legível por outras ferramentas (ex .CSV)
- 4.7.12.15. A solução deve permitir a configuração do questionário que possibilite recolectar respostas em formato de arquivos (upload .jpg, .ppt, .jpeg, .csv. etc)
- 4.7.12.16. A solução deve possuir um histórico para cada questionário que permite visualizar as atividades relacionados ao mesmo (ex.: usuário, data, hora e evento)
- 4.7.13. Análisis de Risco Financeiro (CRQ)
 - 4.7.13.1. A solução pode fornecer relatórios de quantificação de risco financeiro. Isso deve incluir uma metodologia que se vincule à pontuação de risco cibernético e mostre um valor correspondente às melhorias nessas pontuações. Também deve incluir um intervalo de moedas, incluindo USD, AUD, BRL, CAD, EUR, GBP, HKD, IDR, INR, JPY, SGD, THB e TWD.
 - 4.7.13.2. A solução deve permitir gerar relatórios sobre a quantificação de risco financeiros da propria organização e de terceiros.
- 4.7.14. Detecção Automática de Fornecedores (AVD)
 - 4.7.14.1. A solução tem de coletar quais são as terceiras e quartas partes de uma organização de maneira automática.
 - 4.7.14.2. Deve mostrar a relação entre as quartas partes e a organização
 - 4.7.14.3. Deve mostrar a relação e a porcentagem de concentração entre as quartas partes e os terceiros
 - 4.7.14.4. A solução deve ser capaz de mostrar a média da classificação de segurança tanto para os terceiros detectados de maneira automática como a média das quartas partes (terceiros dos terceiros)

- 4.7.14.5. Deve permitir aplicar filtros por grau da classificação de segurança dos terceiros e quartas partes detectadas automaticamente.
- 4.7.14.6. A informação das terceiras e quartas partes detectadas automaticamente deve possuir o método utilizado para estabelecer a relação entre as partes.
- 4.7.14.7. A solução deve ser capaz de identificar produtos usados pelas terceiras e quartas partes detectadas.
- 4.7.14.8. A solução deve oferecer mecanismos para identificar domínios ou produtos rapidamente entre as terceiras e quartas partes detectadas (ex.: barra de pesquisa)
- 4.7.14.9. A solução deve permitir adicionar as terceiras e quartas partes detectadas a portfólios para monitoramento contínuo, seja em um portfólio existente ou a partir de um novo portfólio.
- 4.7.14.10. A solução deve possibilitar exportar as entidades detectadas em um formato legível por outras ferramentas (ex.: .csv).
- 4.7.15. Ambiental, Social & Governança (ESG Data)
 - 4.7.15.1. A solução deve permitir o monitoramento contínuo dos riscos ambientais, sociais e de governança corporativa (ESG) para a própria organização.
 - 4.7.15.2. A solução deve permitir o monitoramento contínuo dos riscos ambientais, sociais e de governança corporativa (ESG) para terceiros.
 - 4.7.15.3. Deve possuir uma API para que possa exportar as informações armazenadas sobre ESG relacionadas a própria organização e de terceiros.
 - 4.7.15.4. A solução deve atualizar as informações diariamente.
 - 4.7.15.5. Deve utilizar múltiplas fontes como mídia adversa e agências governamentais.
 - 4.7.15.6. A solução deve ser capaz de fornecer informações sobre: Roubos, Conspiração, Crime Contra a Humanidade, Crime cibernético, Crimes Ambientais, Espionagem, Operações de jogos de azar, Abuso dos Direitos Humanos, Sequestro, Violações Trabalhistas, Pirataria, Poluição, Pornografia, Crimes de guerra, Lavagem de dinheiro, etc
- 4.7.16. Ambiental, Social & Governança (ESG Data)
 - 4.7.16.1. A solução deve permitir o monitoramento contínuo dos riscos ambientais, sociais e de governança corporativa (ESG) para a própria organização.
 - 4.7.16.2. A solução deve permitir o monitoramento contínuo dos riscos ambientais, sociais e de governança corporativa (ESG) para terceiros.

- 4.7.16.3. Deve possuir uma API para que possa exportar as informações armazenadas sobre ESG relacionadas a própria organização e de terceiros.
- 4.7.16.4. A solução deve atualizar as informações diariamente.
- 4.7.16.5. Deve utilizar múltiplas fontes como mídia adversa e agencias governamentais.
- 4.7.16.6. A solução deve ser capaz de fornecer informações sobre: Roubos, Conspiração, Crime Contra a Humanidade, Crime cibernético, Crimes Ambientais, Espionagem, Operações de jogos de azar, Abuso dos Direitos Humanos, Sequestro, Violações Trabalhistas, Pirataria, Poluição, Pornografia, Crimes de guerra, Lavagem de dinheiro, etc
- 4.7.17. Inteligencia de Ameaças (ASI)
 - 4.7.17.1. A solução deve permitir a investigação profunda da superfície de ataque de qualquer organização a nível global. Isso deve incluir a investigação baseada em endereço IP, Hostname, tipo de dispositivo, tipo de sistema operacional, ator malicioso, fornecedor de nuvem, CVE, CVE Score, portas, etc
 - 4.7.17.2. A solução deve proporcionar o IP resultante da investigação e relacionar informações como domínios atribuídos, portas abertas, Serviços, biblioteca da aplicação, dispositivos, sistema operacional, histórico de vulnerações (breaches), Infecções ativas, vulnerabilidades, ransomware groups, atores maliciosos, técnicas MITRE, etc)
 - 4.7.17.3. Deve possibilitar exportar os dados em um formato legível por outras ferramentas como .CSV e .JSON
 - 4.7.17.4. Deve possuir uma API para coleta de informações.
 - 4.7.17.5. O modelo de licenciamento deve ser baseado no número de queries mensais e não em usuários.
- 4.7.18. Inteligencia de Ameaças na Cadeia de Abastecimento (SCRI)
 - 4.7.18.1. A solução deve proporcionar informações relevantes sobre a própria organização e os terceiros monitorados continuamente como:
 - 4.7.18.1.1. Infecções
 - 4.7.18.1.2. Produtos de alto risco
 - 4.7.18.1.3. Vulnerabilidades
 - 4.7.18.1.4. Vulnerações (Breaches)
 - 4.7.18.2. Deve ser capaz de indicar o detalhe das infecções detectadas em cada terceiro como quantidade de IPs infectados, total de infecções, categoria da infecção (ex.: Malware, Aplicação Potencialmente não Desejada, Aplicação Potencialmente Vulnerável, etc)

- 4.7.18.3. Deve ser capaz de informar a quantidade de infecções severas para cada terceiro.
- 4.7.18.4. Deve ser capaz de indicar o detalhe das vulnerabilidades detectadas na própria organização e em cada terceiro como vulnerabilidades já exploradas (exploited vulnerabilities), total de vulnerabilidades, Atores Maliciosos com potencial de explorar as vulnerabilidades detectadas, indicar o CVE de cada vulnerabilidade e seu CVSS score e a quantidade de IPs infectados.
- 4.7.18.5. A solução deve mostrar informações históricas sobre vulnerações para cada terceiro e a própria organização, a informação deve conter a data da ultima vulneração, o total de vulnerações e a fonte da informação
- 4.7.18.6. Deve fornecer informações sobre os produtos identificados na própria organização e de terceiros monitorados continuamente e suas vulnerabilidades (CVEs), a quantidade de IPs afetados, a quantidade de softwares vulneráveis e última vez que foi observado.
- 4.7.18.7. A solução deve ser capaz de criar planos de ação
- 4.7.19. Gestão de Vulnerabilidades (CVEDetails)
 - 4.7.19.1. A solução deve agrupar multiplas fontes de informações de vulnerabilidades, conter informações históricas de pelos menos os últimos 10 anos (2014) e proporcionar conteúdo técnico para a gestão de vulnerabilidades.
 - 4.7.19.2. A solução deve ter as seguintes capacidades sobre informações e vulnerabilidades:
 - 4.7.19.2.1. Ser capaz de mostrar os CVEs publicados em cada mês e em cada ano desde 2014 com não menos de 5 mil CVEs por ano.
 - 4.7.19.2.2. Mostrar a quantidade de vulnerabilidades por tipo/categoria como Overflow, Memory Corruption, SQL Injection, XSS, Directory Transversal, File Inclusion, CSRF, XXE, SSRF, Open Redirect, Input Validation, etc
 - 4.7.19.2.3. Mostrar a quantidade de vulnerabilidades por tipo de impacto como Code Excution, Bypass, Privilege Escalation, Denial of Service, Information leak, etc
 - 4.7.19.2.4. Mostrar as vulnerabilidades já exploradas presentes no CISA KEV Catalog, además de indicar os detalhes de cada CVE e os produtos afetados.
 - 4.7.19.3. Oferecer informações relevantes para cada CVE já explorado como a probabilidade de atividade exploratória nos próximos 30 dias, CVSS

Score, Data de publicação, Categoria da vulnerabilidade e patches se já disponíveis.

- 4.7.19.4. A solução deve fornecer informações sobre Softwares Vulneráveis por fornecedor (vendedor), por produto e pesquisa por versão
- 4.7.19.5. Ter capacidade de fornecer informações através de notícias (newsfeed)
- 4.7.19.6. Fornecer informações sobre vulnerabilidades de código aberto para ecossistemas de código aberto.
- 4.7.19.7. Deve ter a capacidade de conter informações atualizadas sobre CVEs emergentes (Emerging CVEs), com informações de IDs de CVEs que ainda não foram publicados.
- 4.7.19.8. A solução deve ter informações gerais sobre Exploits
- 4.7.19.9. Conter dados monitorados de alterações de código em repositórios de código aberto e marcar alterações de código relevantes e correlacionar alterações de código com CVEs
- 4.7.19.10. A solução deve ser capaz de mostrar informações gerais sobre a própria superfície de ataque como domínios, quantidade de IPs, ISPs, Serviços, etc
- 4.7.19.11. A solução deve ser capaz de criar alertas, RSS Feed, aplicar etiquetas e notas.
- 4.7.19.12. A solução deve ter a capacidade de fornecer módulos uteis de Metasploit.
- 4.7.19.13. A solução deve permitir adicionar produtos ou versões à pilha de tecnologia para facilitar acesso, relatórios, feeds RSS e alertas.
- 4.7.20. Lista de Alto Nível
 - 4.7.20.1. A solução deve fornecer visibilidade de alto nível na pontuação geral de um número ilimitado de terceiros.
 - 4.7.20.2. A lista de alto nível de terceiros deve incluir as seguintes informações:
 - 4.7.20.2.1. Nome da empresa
 - 4.7.20.2.2. Pontuação geral da empresa
 - 4.7.20.2.3. Impacto no negócio
 - 4.7.20.2.4. Etiquetas ("Tags")
 - 4.7.20.2.5. Ciclo de Vida do Fornecedor
 - 4.7.20.2.6. Tipo de dados Compartilhado
 - 4.7.20.2.7. Unidade de Negócio
 - 4.7.20.2.8. Nível de Risco
 - 4.7.20.2.9. Data de término do contrato

- 4.7.20.2.10. Violações nos últimos 30 dias ("Breach - 30 dias")
- 4.7.20.2.11. Status
- 4.7.20.2.12. Data em que a empresa foi adicionada à lista
- 4.7.20.2.13. Contatos na empresa
- 4.7.20.2.14. Identificador de Fornecedor ou Terceiro
- 4.7.20.3. A solução em sua listagem de alto nível deve fornecer informações sobre se o terceiro está sendo monitorado nas pastas de monitoramento profundo e de baixo nível.
- 4.7.20.4. A solução na sua listagem de alto nível deve permitir que você adicione notas para cada empresa.
- 4.7.20.5. A lista de alto nível deve permitir filtros com base em informações da empresa, como: Pontuação geral, Impacto no Negócio, Risco, Intervalo de datas de término do contrato, E-mail de contato interno, Empresas com ou sem um contato atribuído, Etiquetas, Sinais de vulnerabilidade presentes na empresa e Tipo de informação compartilhada.
- 4.7.20.6. A solução deve permitir que empresas ou terceiros sejam convidados através da lista de alto nível para aqueles com contatos atribuídos.
- 4.7.20.7. A listagem de alto nível deve permitir a edição em massa de informações da empresa, bem como permitir a adição em massa de etiquetas às empresas listadas.
- 4.7.20.8. A listagem de alto nível deve permitir quais colunas devem ser visíveis e quais não.

5. CONTROLES DE SEGURANÇA

5.1. Serviço gerenciado de segurança:

5.1.1. Monitoramento das Soluções Gerenciadas

- 5.1.1.1. Monitorar o ambiente 24x7x365, quanto à disponibilidade e desempenho dos equipamentos que compõe a solução a ser gerenciada;
- 5.1.1.2. Fazer a gestão dos incidentes (criação de alertas, detecção e abertura de chamados);
- 5.1.1.3. Acompanhamento completo dos incidentes de segurança, performance e disponibilidade;

- 5.1.1.4. Realizar a monitoração de performance e disponibilidade dos ativos;
- 5.1.1.5. Realizar o acionamento por matriz de escalação hierárquica e funcional, para eventos de segurança, performance e disponibilidade.
- 5.1.2. Quanto ao suporte especializado a CONTRATADA deve:
 - 5.1.2.1. Permitir a abertura, acompanhamento e validação de chamados através de e-mail, web site (portal do cliente) e telefone (0800) no regime 24x7x365, com atendimento bilíngue (português e inglês);
 - 5.1.2.2. Possuir processo de escalação funcional, mapeamento e documentado, com os seguintes níveis de atendimento: N1, N2 e N3, conforme melhores práticas descritas pelo ITIL;
 - 5.1.2.3. Possuir canal com os fabricantes envolvidos na solução dos incidentes, bem como ser responsável pela abertura e acompanhamento dos chamados junto aos mesmos;
 - 5.1.2.4. Possuir análise técnica documentada pelo N3 do ambiente integrado de monitoramento e resposta a incidentes de segurança da informação antes do envolvimento dos fabricantes, a fim de garantir o processo de escalação funcional;
 - 5.1.2.5. Possuir os processos de gerenciamento de incidente, requisição, eventos, problemas, mudanças, incidentes críticos e atendimento aos usuários VIPs mapeados e documentados de acordo com as melhores práticas descritas pelo ITIL;
 - 5.1.2.6. Os administradores de tecnologia do CONTRATANTE terão total acesso à plataforma para fins de auditoria, porém a responsabilidade pela operação diária da solução será da CONTRATADA.
- 5.1.3. Atuação preventiva:
- 5.1.4. A CONTRATADA deve realizar de forma proativa as ações necessárias para manter o ambiente de segurança da CONTRATANTE adequado às melhores práticas do mercado, devendo:
 - 5.1.4.1. Atualizar os firmwares e/ou softwares das soluções que compõe a solução e das respectivas consoles de gerenciamento;
 - 5.1.4.2. Propor ajustes e melhorias constantes, de acordo com as melhores práticas dos fabricantes, mantendo-as sempre documentadas;
 - 5.1.4.3. Após aprovação da CONTRATANTE, executar tais ajustes e melhorias nas soluções entregues como parte do objeto deste edital, mantendo-as documentadas e acessíveis no portal do cliente;
 - 5.1.4.4. Sugerir tais ajustes e melhorias nas tecnologias de segurança sob operação da CONTRATANTE.

- 5.1.5. A CONTRATADA deverá manter uma rotina mensal de avaliação dos processos e práticas em todos as áreas de atuação do escopo deste contrato com o objetivo de avaliar a eficácia, propor melhorias e auxiliar na implementação desses ajustes;
- 5.1.6. A CONTRATADA deverá manter uma rotina mensal de análise de indicadores internos e pesquisa de mercado com o objetivo de apresentar à contratante um relatório com as inovações tecnológicas e solução que possam aumentar a qualidade e o grau de maturidade da segurança da informação do ambiente tecnológico;
- 5.1.7. Atuar quando ocorrer a falha dos controles de segurança ou situação previamente desconhecida e que tenha probabilidade de comprometer os sistemas e serviços de TI;
- 5.1.8. Monitorar permanentemente e avaliar criticamente os produtos e serviços de segurança da CONTRATANTE;
- 5.1.9. Consolidar em manuais de procedimentos e em base de conhecimento todas as soluções adotadas na execução das atividades;
- 5.1.10. Elaborar mensalmente relatórios de desempenho, auditoria e operação dos ativos sob sua administração;
- 5.1.11. Atuar proativamente na antecipação e identificação de incidentes de segurança, antes mesmo do impacto nos serviços;
- 5.1.12. Sugerir novas tecnologias para modernizar o ambiente tecnológico, buscando subsidiar a equipe do CONTRATANTE na gestão de segurança da informação;
- 5.1.13. Monitorar e propor soluções aos projetos/atividades em andamento otimizando-os quanto aos requisitos de Segurança da Informação;
- 5.1.14. Participar, quando solicitado, de reunião com os gerentes e participantes dos projetos de desenvolvimento e manutenção de sistemas e administração de dados, a fim de prover soluções para projetos/atividades em andamento;
- 5.1.15. Participar da implantação de projetos/soluções, substituição e atualização de soluções destinadas à Segurança da Infraestrutura de rede;
- 5.1.16. Elaborar relatório detalhado das funcionalidades necessárias de equipamentos e softwares a serem adquiridos, destinados à Segurança da Informação.

5.2. Proteção de Perímetros

- 5.2.1. Solução de Microsegmentação:

- 5.2.1.1. Com o objetivo de aprimorar as estratégias de proteção e defesa cibernética no MPRJ, a CONTRATADA deverá fazer a entrega de uma solução que possa microsegmentar os acessos e permissões no ambiente tecnológico;
- 5.2.1.2. Para tal, a CONTRATADA deverá fornecer uma ferramenta e implementá-la no ambiente do MPRJ, licenciada para 10000 (dez mil) ativos, sendo elas divididas em até 1000 (mil) servidores, 8500 (oito mil e quinhentos) estações de trabalho, 200 (duzentos) Nodes de Containers/Kubernetes;
- 5.2.1.3. Características Gerais:
 - 5.2.1.3.1. O licenciamento da plataforma deverá ser por ativo protegido, sendo este um dos abaixo:
 - 5.2.1.3.1.1. Servidores Físicos (Bare Metal), Virtuais, Cloud (Workloads);
 - 5.2.1.3.1.2. Estações de trabalho ou Notebooks;
 - 5.2.1.3.1.3. Nós (Nodes) de Containeres / Kubernetes;
 - 5.2.1.3.1.4. O licenciamento deverá ser flexível, ou seja, não limitado por tipo de ativo.
 - 5.2.1.3.2. Cada licença deverá possibilitar a utilização para qualquer um dos ativos do item anterior, devendo atender uma proporção de no mínimo:
 - 5.2.1.3.2.1. Uma (1) licença de servidor poderá possibilitar o uso de no mínimo cinco (5) licenças de estações de trabalho;
 - 5.2.1.3.2.2. Cinco (5) licenças de servidores poderão possibilitar o uso de uma (1) uma licença para nós (Nodes) de Contêineres / Kubernetes;
 - 5.2.1.3.2.3. Deverá ser possível alterar o uso da licença entre os ativos acima;
 - 5.2.1.3.2.4. Caso haja algum prazo mínimo para esta mudança de uso de licenciamento, está deverá ser de no máximo 30 dias;
 - 5.2.1.3.3. Toda a solução deverá ser do mesmo fabricante;
 - 5.2.1.3.4. O gerenciamento da solução deve ser 100% em nuvem e totalmente dedicado para este órgão;
 - 5.2.1.3.5. A solução deve prover no mínimo 99.5% de disponibilidade no nível de serviço;

- 5.2.1.3.6. A solução SaaS deverá estar hospedada primariamente em Datacenter localizado em território brasileiro.
- 5.2.1.3.7. Toda a solução deverá ser gerenciada por uma console única de gerência centralizada, para todos os tipos de ativos especificados anteriormente.
- 5.2.1.3.8. Serão aceitas exceções em casos de integrações com soluções de terceiros, quando especificado e autorizado pela CONTRATANTE;
- 5.2.1.3.9. Deverá ser oferecido retenção mínima de 30 dias para todos os dados enviados para a console, incluindo os Fluxos de Dados;
- 5.2.1.3.10. Não deverá ser necessário qualquer parada (downtime) dos servidores ou aplicações;
- 5.2.1.3.11. A solução deverá prover, sem custo adicional e de forma nativa, Feeds de Ameaça (Threat Feeds) possuindo, no mínimo, IPs, Domínios e HASHs maliciosos.
- 5.2.1.3.12. Os Feeds deverão ser do próprio fabricante, podendo utilizar também listas de terceiros;
- 5.2.1.3.13. A solução deverá suportar IPv4 e IPv6;
- 5.2.1.3.14. Deve ser capaz de monitorar TODOS os fluxos de tráfego do Datacenter: Leste-Oeste (servidor-servidor) e Norte-Sul (rede cliente-servidor ou servidor-externa, ou seja, internet);
- 5.2.1.3.15. A solução deve monitorar os fluxos de tráfego de todos os ativos que possuem agentes instalado, incluindo também entre máquinas virtuais em execução no mesmo hypervisor, ativos de tipos diferentes, comunicação entre nuvem pública com datacenter privado, entre outros.
- 5.2.1.3.16. A solução também deverá permitir a criação de regras de filtragem de comunicação entre distintos tipos de ativos, bem como entre distintos tipos de ambientes;
- 5.2.1.3.17. A solução deverá manter registro de todos os Fluxos de Ativos, incluindo os que não foram bloqueados bem como aqueles que falharam;
- 5.2.1.3.18. Toda a comunicação interna entre os componentes da solução deve ser completamente criptografada e autenticada;
- 5.2.1.3.19. Se a solução necessitar, deverão ser entregues todos os componentes de hardware necessários para o seu correto funcionamento;

5.2.1.4. Arquitetura da Solução:

5.2.1.4.1. A solução deverá ser entregue em modelo SaaS, podendo ser utilizada sem qualquer componente on-premises, com exceção dos agentes instalados nos ativos protegidos;

5.2.1.4.2. A Console de Gerenciamento deverá ser única e centralizada para toda a solução;

5.2.1.4.3. Para garantir a segurança dos dados desta organização, o ambiente em nuvem deverá ser dedicado para este órgão. Nenhuma informação deverá ser compartilhada, incluindo os IPs e FQDNs de acesso da Console de Gerenciamento, bem como de todos os outros componentes na nuvem do fabricante da solução;

5.2.1.4.4. Deverá ser possível implementar canais (relays) de comunicação internos, para centralizar a comunicação dos agentes. Esse canal será responsável por receber a comunicação dos agentes e somente ele enviar para a Console Centralizada em nuvem;

5.2.1.4.5. Os canais (relays) poderão ser instalados também em nuvem pública ou privada;

5.2.1.4.6. Caso seja necessário, deverão ser licenciados no mínimo 50 canais (relays) Internos;

5.2.1.4.7. Os canais deverão trabalhar tanto em Alta Disponibilidade (HA), quando balanceamento (Load Balance) entre eles. Não deverá ser necessário nenhuma solução de terceiros para estas funcionalidades;

5.2.1.4.8. Os canais (relays) deverão ser em modelo de Virtual Appliance, compatível no mínimo com:

5.2.1.4.8.1. VMware;

5.2.1.4.8.2. Hyper-V;

5.2.1.4.8.3. AWS;

5.2.1.4.8.4. Azure;

5.2.1.4.8.5. GCP;

5.2.1.4.8.6. OCI.

5.2.1.4.9. A solução deverá utilizar agentes instalados nos ativos protegidos, responsável por coletar os fluxos de dados e garantir a aplicabilidade das regras configuradas;

5.2.1.4.10. Os agentes da solução deverão ser uma implementação de Firewall do próprio fabricante, não utilizando o Firewall nativo do Sistema Operacional;

5.2.1.4.11. Caso os agentes dependam do Firewall do Sistema Operacional, deverão atender os seguintes requerimentos mínimos:

5.2.1.4.11.1. Deverá estender as capacidades técnicas do Firewall do Sistema Operacional, não se limitando somente a versão nativamente existente, devendo atender aos itens técnicos deste documento;

5.2.1.4.11.2. Deverá possuir controles nativos da solução que evitem alteração nas políticas definidas pelo administrador da solução de micro segmentação;

5.2.1.4.11.3. Deverá possuir controles nativos que impeçam a parada do Firewall do Sistema Operacional;

5.2.1.4.11.4. Bloquear caso o administrador da rede, ou do sistema operacional, tente efetuar alterações manuais nas regras de firewall diretamente no próprio Sistema Operacional;

5.2.1.4.11.5. Bloquear caso outra solução, como um Antivírus ou EDR, tente efetuar a parada ou desinstalação do Firewall nativo do sistema operacional;

5.2.1.4.11.6. Bloquear a tentativa de parada, desinstalação ou comprometimento do Firewall nativo do Sistema Operacional em casos de ataques;

- 5.2.1.4.11.7. O Fabricante da solução de Microsegmentação deverá garantir a atualização, ou mecanismos de contorno/proteção, em caso de conhecidas e/ou publicação de novas vulnerabilidades existente no Firewall nativo do Sistema Operacional.
- 5.2.1.4.12. Os agentes deverão possuir nativamente controle de consumo de CPU e Memória RAM, podendo ser configurável, mas não consumindo mais que 5% nos ativos instalados;
- 5.2.1.4.13. Possuir coletores com a capacidade de receber flow de rede através de dispositivos físicos, como Switches e Roteadores, sendo compatível no mínimo com os protocolos: Netflow 5 and 9, IPFI, and sFlow;
- 5.2.1.4.14. Possuir coletor dedicado com a capacidade de receber flows de VMware ESX, através de dados enviados de um Span Port de um switch do tipo VSS (Virtual Standard Switch) ou VDS (vSphere Distributed Switch);
- 5.2.1.4.15. Possuir coletor dedicado com a capacidade de receber flows de um Span Port de um Switch Físico, ou um Network TAP;
- 5.2.1.4.16. Todos os coletores deverão ser em modelo de Virtual Appliance;
- 5.2.1.4.17. As informações recebidas pelos Coletores deverão ser representadas em forma gráfica na Console de Gerenciamento;
- 5.2.1.4.18. A solução deverá possuir de forma nativa Feed de Ameaças (Threat Feeds), do próprio fabricante, possuindo no mínimo informações sobre Domínios, IPs e HASHs maliciosos;
- 5.2.1.4.19. A solução deverá possuir APIs abertas e documentadas;
- 5.2.1.4.20. A solução deve possuir, no mínimo, conectores para a seguintes nuvens públicas:
- 5.2.1.4.20.1. Amazon Web Services (AWS);
 - 5.2.1.4.20.2. Microsoft Azure;
 - 5.2.1.4.20.3. Google Cloud Platform (GCP);

5.2.1.4.20.4. Oracle Cloud (OCI).

5.2.1.4.21. A solução deve possuir, no mínimo, conectores para a seguintes soluções:

5.2.1.4.21.1. VMware VSphere;

5.2.1.4.21.2. MS Active Directory;

5.2.1.4.21.3. F5;

5.2.1.4.22. Deve ser capaz de ser implantado em vários segmentos de rede (VLANs), independente do equipamento utilizado para controlar a VLAN;

5.2.1.4.23. A solução deverá possuir a capacidade de etiquetamento de todos os ativos, incluindo os que possuem agentes ou outros ativos sem agente mas que se comunicaram ou receberam comunicação de um ativo protegido pela solução;

5.2.1.4.24. Deve ser capaz de detectar e rotear conexões com falha para um servidor dedicado de "Honeypot, podendo ser do mesmo fabricante ou de terceiros, desde que entregue em conjunto com a solução;

5.2.1.4.25. Os agentes deverão ser compatíveis com Microsoft Windows, Linux e Unix, bem como em ambiente Kubernetes;

5.2.1.5. Console de Gerenciamento:

5.2.1.5.1. A console de gerenciamento deverá ser única para toda a solução de micro segmentação;

5.2.1.5.2. Ter a capacidade de gerenciar todos os tipos de ativos (servidores, cloud, estações de trabalho e Kubernetes) em uma única console;

5.2.1.5.3. Ter a capacidade de visualizar os fluxos de dados e configurar as políticas de segurança em uma única console;

5.2.1.5.4. Possuir um Dashboard com as principais informações referentes ao ambiente;

- 5.2.1.5.5. Ter a capacidade de visualizar em modo gráfico, através de mapas, os fluxos de dados do ambiente;
- 5.2.1.5.6. Ser possível visualizar de forma agregada o fluxo de dados, de forma gráfica, de um período de tempo, como 30 dias por exemplo;
- 5.2.1.5.7. Visualizar todos os ativos protegidos, incluindo informações como Nome, Sistema Operacional, Número de CPUs, IP e MAC Address;
- 5.2.1.5.8. Ter a capacidade de visualizar todas as etiquetas associadas a um único dispositivo;
- 5.2.1.5.9. Ter a capacidade de visualizar todos os ativos para uma única etiqueta;
- 5.2.1.5.10. Deve possuir uma área específica para visualizar todos os fluxos de comunicação de rede coletados no ambiente;
- 5.2.1.5.11. Deve ser possível filtrar os fluxos de comunicação de dados, no mínimo em:
 - 5.2.1.5.11.1. Bloqueado, Permitido, não foi possível o bloqueio;
 - 5.2.1.5.11.2. Origem: por etiqueta e nome do ativo;
 - 5.2.1.5.11.3. Destino: por etiqueta e nome do ativo;
 - 5.2.1.5.11.4. Comunicações com Origem ou Destino para a Internet;
 - 5.2.1.5.11.5. Pelo nome do conjunto de regras de proteção aplicado no ambiente;
 - 5.2.1.5.11.6. Porta e Protocolo;
 - 5.2.1.5.11.7. Período de tempo;
 - 5.2.1.5.11.8. Por processo utilizado da comunicação.

- 5.2.1.5.12. Ser possível criar novas etiquetas e gerenciar etiquetas existentes;
- 5.2.1.5.13. Exportar as etiquetas, no mínimo em CSV ou XLS;
- 5.2.1.5.14. Ter a capacidade, através de interface gráfica na própria console, de monitorar a saúde de todos os componentes da solução, no mínimo para os agentes, coletores e servidores de Relay e Clusters Kubernetes
- 5.2.1.5.15. Ter a capacidade, através de interface gráfica na própria console, de parar e reiniciar os componentes da solução, no mínimo para os agentes, coletores e servidores de Relay;
- 5.2.1.5.16. Deve possuir Logs de Auditoria, para no mínimo:
 - 5.2.1.5.16.1. Autenticação do usuário: com sucesso e falha de autenticação
 - 5.2.1.5.16.2. Política de Segmentação: criação e alteração de políticas, bem como a ação de desabilitar a política;
 - 5.2.1.5.16.3. Etiquetas: criação e alteração;
 - 5.2.1.5.16.4. Logs: quem consultou os logs;
 - 5.2.1.5.16.5. Os Logs de Auditoria devem conter, no mínimo: o dia, hora, Ação Executada, Nome do usuário, IP de Origem e Descrição;
 - 5.2.1.5.16.6. Deve ser possível gerenciar os usuários com acesso a solução, não havendo limites para o número de usuários existentes;
 - 5.2.1.5.16.7. Deve possuir integração com sistemas de diretório para integração de autenticação. Deve ser compatível com mínimo com LDAP e SAML 2.0;
 - 5.2.1.5.16.8. Deve suportar autenticação Kerberos;
 - 5.2.1.5.16.9. Deve ser possível criar usuários locais, e gerenciar os usuários existentes. Deve permitir alterar a senha do usuário

utilizando uma nova senha Temporária de alteração obrigatória no primeiro login;

- 5.2.1.5.16.10. Deve suportar segundo fator de autenticação;
- 5.2.1.5.16.11. Possuir níveis de permissões diferentes para os usuários, no mínimo com as seguintes características:
 - 5.2.1.5.16.11.1. Administrador da solução;
 - 5.2.1.5.16.11.2. Somente Leitura;
 - 5.2.1.5.16.11.3. Somente visualização dos Incidentes;
 - 5.2.1.5.16.11.4. Administração das Políticas.
- 5.2.1.5.16.12. Deve ser possível configurar quais etiquetas o usuário possui permissão;
- 5.2.1.5.16.13. Ser possível verificar todos os incidentes gerados pela solução diretamente na própria console de administração;
- 5.2.1.5.16.14. Ser possível filtrar os incidentes no mínimo por Severidade, Tipo, Etiquetas, Nome do Ativo e período de tempo;
- 5.2.1.5.16.15. Deve possuir mecanismo de busca dos incidentes;
- 5.2.1.5.16.16. Deve ser possível customizar o nível de criticidade dos incidentes;
- 5.2.1.5.16.17. Deve ser possível desabilitar o uso de dados de reputação, bem como habilitar ou desabilitar o envio de informações de IoC (indicadores de comprometimento) para o fabricante da solução;
- 5.2.1.5.16.18. Deve ser possível trabalhar com múltiplos sites, em console única e que permitam aos usuários aplicar seletivamente políticas e regras a um conjunto de ativos nessa localização;

5.2.1.5.16.19. Deve ser possível gerenciar a administração de políticas em vários sites/divisões gerenciando os escopos dos usuários por site;

5.2.1.5.16.20. Deve ser possível ao administrador total autonomia para criar, modificar e excluir regras, além de visualizar todos os logs para Ativos atribuídos aos seus sites.

5.2.1.6. Agentes:

5.2.1.6.1. A solução deverá possuir agentes instalados nos ativos protegidos;

5.2.1.6.1.1. Os agentes deverão ser compatíveis com as seguintes plataformas, no mínimo:

5.2.1.6.1.1.1. Windows Server: 2003 SP2 (32 e 64 bits), 2008 (32 bits), 2008 R2, 2012, 2016, 2016 Core, 2019 e 2022;

5.2.1.6.1.1.2. Windows Desktop: 7 (32 e 64 bits), 8 (32 e 64 bits), 8.1 (32 e 64 bits), 10 (32 e 64 bits) e 11;

5.2.1.6.1.1.3. MacOS Catalina, Big Sur, Monterey, Ventura e mais atuais;

5.2.1.6.1.1.4. Red Hat Linux: 4, 5, 5.1, 5.2 até 5.11, 6, 7 e 8 (todos 64 bits);

5.2.1.6.1.1.5. CentOS Linux: 5.2 (32 bits), 5.2 até 5.11 (64 bits), 6 até 9 (64 bits);

5.2.1.6.1.1.6. Oracle Linux: 5.2 até 5.11, 6 até 9 (todos 64 bits);

5.2.1.6.1.1.7. Ubuntu Linux: 12.04 até 22.04 LTS (todos 64 bits);

5.2.1.6.1.1.8. Debian Linux: 7.5 até 12 (todos 64 bits);

5.2.1.6.1.1.9. Rocky 8 e 9 (64bits).

5.2.1.6.1.2. Para Containers e Kubernetes, a solução deverá atuar como um DaemonSet em todos os nós do cluster;

5.2.1.6.1.3. Os agentes deverão consumir no máximo 5% de CPU e memória do ativo instalado, podendo este valor ser

configurado nativamente na própria console de Gerenciamento;

- 5.2.1.6.1.4. Os agentes deverão ser capazes de coletar informações do ativo, como flows de rede, e executar as políticas de proteção;
- 5.2.1.6.1.5. As políticas de proteção deverão permanecer em execução mesmo que o ativo não tenha acesso ao Relay ou a Console de Gerenciamento;
- 5.2.1.6.1.6. Os agentes deverão armazenar os Logs de Fluxo de Dados e Incidentes mesmo que o ativo não tenha acesso ao Relay ou a Console de Gerenciamento;
- 5.2.1.6.1.7. Os agentes da solução deverão ser uma implementação de Firewall do próprio fabricante, não utilizando o Firewall nativo do Sistema Operacional;
- 5.2.1.6.1.8. Caso os agentes não sejam uma implementação nativa de Firewall e dependam do Firewall do Sistema Operacional, deverão atender os seguintes requerimentos mínimos:
 - 5.2.1.6.1.8.1. Deverá estender as capacidades técnicas do Firewall do Sistema Operacional, não se limitando somente a versão nativamente existente, devendo atender aos itens técnicos deste documento;
 - 5.2.1.6.1.8.2. Deverá possuir controles nativos da solução que evitem alteração nas políticas definidas pelo administrador da solução de micro segmentação;
 - 5.2.1.6.1.8.3. Deverá possuir controles nativos que impeçam a parada do Firewall do Sistema Operacional;
 - 5.2.1.6.1.8.4. Bloquear caso o administrador da rede, ou do sistema operacional, tente efetuar alterações manuais nas regras de firewall diretamente no próprio Sistema Operacional;

- 5.2.1.6.1.8.5. Bloquear caso outra solução, como um Antivírus ou EDR, tente efetuar a parada ou desinstalação do Firewall nativo do sistema operacional;
- 5.2.1.6.1.8.6. Bloquear a tentativa de parada, desinstalação ou comprometimento do Firewall nativo do Sistema Operacional em casos de ataques;
- 5.2.1.6.1.9. O Fabricante da solução de Micro Segmentação deverá garantir a atualização, ou mecanismos de contorno/proteção, em caso de conhecidas e/ou publicação de novas vulnerabilidades existente no Firewall nativo do Sistema Operacional;
- 5.2.1.6.1.10. Deverá suportar o uso do agente da solução em conjunto com o Firewall Nativo do Sistema Operacional, ou de terceiros, exceto em casos de Limitação do Sistema Operacional;
- 5.2.1.6.1.11. Os agentes deverão capturar todos os Fluxos de Dados nos ativos instalados e enviar para a console de gerenciamento.
- 5.2.1.6.1.12. As informações capturadas pelo agente deverão conter no mínimo:
 - 5.2.1.6.1.12.1. IP de Origem e Destino;
 - 5.2.1.6.1.12.2. Hostname de Origem e Destino;
 - 5.2.1.6.1.12.3. Porta e Protocolo;
 - 5.2.1.6.1.12.4. Quantidade de conexões;
 - 5.2.1.6.1.12.5. Hora e Data;
 - 5.2.1.6.1.12.6. Informações do processo/binário responsável pela comunicação, na origem e destino;
 - 5.2.1.6.1.12.7. Caminho do binário no ativo;
 - 5.2.1.6.1.12.8. Nome do Serviço do Windows (Ex.: BITS) responsável pela comunicação, quando este for executado em um processo padrão (Ex.: SVCHost.exe);
 - 5.2.1.6.1.12.9. Usuário que executou o processo;

- 5.2.1.6.1.12.10. FQDN ou IP, quando for um acesso com origem ou destino para Internet.
- 5.2.1.6.1.13. A instalação do agente não deverá requer qualquer tipo de parada no Sistema Operacional, incluindo reiniciar (Reboot);
- 5.2.1.6.1.14. A instalação do agente não deverá requerer qualquer tipo alteração no ativo, como mudança de IP, Hostname, ou instalação de software que possam comprometer o funcionamento normal da aplicação;
- 5.2.1.6.1.15. Serão aceitas soluções que não se utilizem somente de agentes para efetuar todos os controles requeridos.
- 5.2.1.6.1.16. Serão aceitas soluções complementares para atender os requerimentos deste documento, desde que suportadas pelos mesmos SLAs e pelo único vencedor desta licitação;
- 5.2.1.6.1.17. Caso a solução não utilize somente agentes para efetuar todos os controles requeridos, deverão ser entregues todos os hardware e/ou softwares necessários, com o mesmo quantitativo de licenças, para atendimento dos itens;
- 5.2.1.6.1.18. Os agentes deverão ter a capacidade de coletar informações dos ativos que estão instalados, como exemplo, mas não se limitando: Número de CPUs, processos em execução, usuários pertencentes ao grupo de administrador local, softwares instalados, uptime do sistema, ativos com um determinado software instalado, entre outros;
- 5.2.1.7. Características de visibilidade:
- 5.2.1.7.1. A solução deverá prover visibilidade de toda a comunicação de rede de forma gráfica, através de um mapa de rede;
- 5.2.1.7.2. Deve permitir navegar facilmente pelo mapa e focar em parte específica do data center ou aplicativos específicos;

- 5.2.1.7.3. Deve possuir, no mapa de rede, filtros de inclusão e exclusão, permitindo filtrar no mínimo:
- 5.2.1.7.3.1. IP;
 - 5.2.1.7.3.2. Porta;
 - 5.2.1.7.3.3. Aplicação, Binário e Serviço;
 - 5.2.1.7.3.4. Nome do Ativo;
 - 5.2.1.7.3.5. Tipo de Conexão - Estabelecida, falhada (time out), bloqueada e as que violaram uma política;
 - 5.2.1.7.3.6. Internet - Com Origem e Destino da Internet;
 - 5.2.1.7.3.7. Usuário que iniciou o processo.
- 5.2.1.7.4. Deve ser possível criar diferentes mapas de rede, determinando o período de tempo e aplicando filtros conforme item anterior;
- 5.2.1.7.5. Deve reter os fluxos de dados por um mínimo de 30 (trinta) dias, sendo possível criar ou visualizar os mapas utilizando períodos históricos;
- 5.2.1.7.6. A tela do Mapa de Dados deve possuir mecanismo de busca;
- 5.2.1.7.7. Deverá ser possível aplicar Etiquetas, de forma pontual (único ativo) ou para vários ativos ao mesmo tempo;
- 5.2.1.7.8. Deverá ser possível verificar as Etiquetas aplicadas a um ativo diretamente da tela do Mapa de Dados;
- 5.2.1.7.9. Ser possível identificar a quantidade de vezes que uma determinada comunicação aconteceu em um período de tempo;
- 5.2.1.7.10. Ser possível, no mapa de dados, obter informações detalhadas do processo que efetuou uma determinada comunicação;
- 5.2.1.7.11. Deve ser possível, no mapa de dados, visualizar as comunicações de todos os ativos do ambiente, máquina a máquina;
- 5.2.1.7.12. Deve ser possível, no mapa de dados, agrupar os ativos através das etiquetas existentes no ambiente;

- 5.2.1.7.13. Deve registrar e apresentar todos os fluxos de comunicação do datacenter, em formato de tabela, juntamente com informações contextuais e detalhadas sobre as cargas de trabalho e aplicativos (processos) de comunicação;
- 5.2.1.7.14. Deve fornecer recursos de filtragem que permita identificar se a comunicação foi estabelecida/bloqueada ou falhou (time-out);
- 5.2.1.7.15. Deve descobrir automaticamente qualquer novo fluxo de comunicação em tempo real;
- 5.2.1.7.16. Deve ser possível filtrar os fluxos de dados por um conjunto de regras aplicados no ambiente;
- 5.2.1.7.17. Deve ser possível exportar os fluxos de dados no mínimo em CSV;
- 5.2.1.7.18. Deve ser possível visualizar todos os ativos, através da console, obtendo informações da primeira vez que foi visto e a última vez que o ativo se comunicou com a console;
- 5.2.1.7.19. Deverá ser possível etiquetar ou aplicar TAGs nos ativos do ambiente, ativos com agentes e sem agentes, para utilizar tanto na visualização, em políticas bem como em filtros;
- 5.2.1.7.20. A etiquetas deverão seguir um modelo de Categoria e Valores, por exemplo Ambiente / Produção, ou de forma similar onde é possível incluir valores diferentes para uma mesma categoria;
- 5.2.1.7.21. As etiquetas deverão ser criadas através da própria console de gerenciamento, no mínimo com duas das seguintes formas:
 - 5.2.1.7.21.1. De forma manual, adicionando diretamente ao dispositivo, podendo inclusive ser através do mapa de fluxo de dados;
 - 5.2.1.7.21.2. Através de Inteligência Artificial - A solução deverá sugerir Etiquetas baseadas nas aplicações existentes no dispositivo;
 - 5.2.1.7.21.3. Através de Integração com sistemas que já possuem TAGs - Como VMWare VCenter, Nuvens públicas (AWS, GCP, Azure, OCI), Kubernetes (Metadados dos clusters) e CSV;

5.2.1.7.21.4. Através de APIs públicas.

5.2.1.7.22. Não deve existir um limite no tipo e/ou nome de Etiquetas a serem criadas na solução, para as categorias e para os valores;

5.2.1.7.23. Deverá ser possível agrupar etiquetas em Grupos de Etiquetas, para uso nas políticas e outras partes da solução;

5.2.1.7.24. Deverá ser registrado em Log toda a criação, remoção ou modificação das etiquetas, informando no mínimo o usuário responsável, hora e data e a etiqueta alterada. Esses logs deverão ser acessíveis através da própria console de gerenciamento;

5.2.1.7.25. Deverá ser possível aplicar uma Etiqueta a um único dispositivo, e a um conjunto de dispositivos;

5.2.1.7.26. A console de gerenciamento deverá possuir uma área específica de informações dos ativos que devem apresentar todas as Etiquetas aplicadas ao ativo;

5.2.1.7.27. As etiquetas poderão ser utilizadas no Mapa de Visualizações de Fluxo de Dados e nas criações de políticas;

5.2.1.7.28. Deverá ser possível hierarquizar as etiquetas, sem restrições, para visualização agrupada com subníveis no mapa de fluxo de dados.

5.2.1.7.29. A hierarquização de etiquetas poderá utilizar qualquer etiqueta do ambiente, e não ter limitador do número de níveis

5.2.1.7.30. Deverá apresentar no mapa de fluxo de dados os dispositivos gerenciados e não-gerenciados pela solução;

5.2.2. Microsegmentação e Segurança do Ambiente:

5.2.2.1. Deve fornecer a capacidade de criar, gerenciar e monitorar políticas de tráfego Leste-Oeste e Norte-Sul flexíveis até o nível de uma única carga de trabalho e aplicativo (processo ou serviço do MS Windows);

5.2.2.2. Deve permitir criar e monitorar políticas de comunicação de aplicativo a partir do mapa de visualização;

5.2.2.3. Deve suportar regras definidas sobre grupos de ativos de acordo com sua função ou Etiqueta;

- 5.2.2.4. Deve possuir no mínimo 3 (três) tipos de regras: Bloqueio, Permissão e Alerta;
- 5.2.2.5. Deve permitir trabalhar tanto com Whitelist como Blacklist, de forma independente;
- 5.2.2.6. Deve permitir criar regras de micro segmentação utilizando os seguintes parâmetros como Origem e Destino:
 - 5.2.2.6.1. Etiquetas e Grupo de Etiquetas
 - 5.2.2.6.2. Ativo (nome do ativo)
 - 5.2.2.6.3. IP/Subrede
 - 5.2.2.6.4. Aplicação / Processo do Windows (Ex.: BITS)
 - 5.2.2.6.5. Grupo de usuários
 - 5.2.2.6.6. FQDN
 - 5.2.2.6.7. Internet (Comunicação vindo da Internet / Rede Interna)
 - 5.2.2.6.8. Qualquer (Any).
- 5.2.2.7. Deve permitir criar regras de Bloqueio, Permissão e Alerta utilizando a Porta e Protocolo (TCP/UDP), incluindo ICMP;
- 5.2.2.8. Deve ser possível criar regras de bloqueio, permissão e alerta, de forma independente;
- 5.2.2.9. Deve ser possível criar regras somente de bloqueio, sem precisar fazer uma Whitelist da aplicação. Por exemplo, com uma única regra bloquear todos os servidores de Banco de Dados de receber comunicação da Internet;
- 5.2.2.10. Deve ser possível agrupar ou nomear um conjunto de regras com a mesma finalidade, para facilitar o gerenciamento, visualização e filtros por esse agrupamento;
- 5.2.2.11. Ser possível desabilitar uma regra, ou um conjunto de regras, sem a necessidade de excluir da console;
- 5.2.2.12. Possuir filtros de informações no gerenciamento das regras do ambiente;
- 5.2.2.13. Ser possível identificar e filtrar as regras pelo usuário que a criou;

- 5.2.2.14. As regras devem ser publicadas manualmente para os ativos, podendo inclusive escolher se serão aplicadas todas as regras ou um conjunto específico baseado no nome do agrupamento;
- 5.2.2.15. Deve salvar as revisões de política e permitir a reversão para versões anteriores;
- 5.2.2.16. A solução deve possuir nativamente modelos (templates) pré-definidos para aplicações conhecidas de mercado, como o Active Directory, tendo o catálogo disponibilizado na própria console de gerenciamento;
- 5.2.2.17. Deve possuir nativamente modelos (templates) pré-definidos para políticas de Prevenção de Ransomware;
- 5.2.2.18. A solução deve sugerir automaticamente aplicação de políticas de microssegmentação para as aplicações existentes no ambiente;
- 5.2.2.19. Deve sugerir a criação de regras de forma automática com base no fluxo histórico de comunicação das aplicações (mínimo de 30 dias como base de pesquisa);
- 5.2.2.20. Deve poder sugerir políticas automaticamente de acordo com os dados coletados;
- 5.2.2.21. A solução deve utilizar Inteligência Artificial para analisar fluxos de dados históricos (mínimo de 30 dias) e sugerir políticas de segmentação para qualquer aplicação do ambiente;
- 5.2.2.22. Deve permitir incluir na política a identidade do usuário autenticado no ativo. Será aceito para esta funcionalidade a integração com outra solução do mesmo fabricante, desde que seja entregue o quantitativo de licenças necessário para o correto funcionamento;
- 5.2.2.23. Deve ser possível criar políticas com Lógicas de E e OU;
- 5.2.2.24. Durante a criação de políticas, ao ser selecionado a categoria de Aplicação / Processo do Windows, deverão aparecer automaticamente todos os processos já identificados no ambiente pelo agente ou pelo Relay. Ainda deverá ser possível adicionar manualmente um novo processo, que ainda não se comunicou no datacenter;
- 5.2.2.25. A solução deverá permitir a inclusão de listas de FQDNs, através de importação de arquivo, para serem utilizadas durante a consulta DNS em bloqueio ou liberação de acesso a sites específicos;

- 5.2.2.26. Deve ter a capacidade de isolar uma máquina da rede, ou um grupo de máquinas, com uma única regra;
- 5.2.2.27. Deve ser possível bloquear e permitir uma comunicação efetuada pela mesma porta e protocolo utilizando binários diferentes.
- 5.2.2.28. Deve permitir a criação de regras com usuários em ambientes VDI de forma a garantir que apenas determinados grupos do Active Directory possam chegar a um determinado endereços e/ou aplicações na rede;
- 5.2.2.29. Deve permitir a combinação de regras utilizando máquina/usuário/processo de origem e serviço no destino;
- 5.2.2.30. Deve informar ao usuário o impacto das regras criadas no fluxo de comunicação de forma visual, simulando o impacto das regras no fluxo de comunicações;
- 5.2.2.31. Em sistemas operacionais Windows, deve permitir criar regras utilizando não somente o processo como também o serviço;
- 5.2.2.32. Deve detectar, analisar e relatar suspeitas de tentativas de movimento lateral;
- 5.2.2.33. Deve permitir tipos de eventos personalizáveis, prioridade e gravidade para tipos de eventos individuais;
- 5.2.2.34. Deve permitir editar listas de indicadores confiáveis;
- 5.2.2.35. Deve alertar sobre a violação da política e fornecer informações detalhadas sobre a violação da conexão, indicando inclusive qual processo iniciou a comunicação;
- 5.2.2.36. Deve possuir mecanismo de reputação de hash para todo e qualquer processo que tente se comunicar com a rede;
- 5.2.2.37. Deve permitir a integração com fontes externas de informação para aumentar a base de detecção de hashes;
- 5.2.2.38. Deve possuir mecanismo de reputação de DNS e validar toda e qualquer tentativa de resolução de nomes nos ativos protegidos pela solução
- 5.2.2.39. Deve possuir mecanismo de reputação de IP, para evitar comunicações de IP's sabidos como maliciosos da internet;

5.2.2.40. É necessário oferecer a opção de verificar todos os processos de comunicação como parte de malware conhecido por um serviço de reputação incluído.

5.2.3. Detecção Avançada de Ameaças para o ambiente microssegmentado;

5.2.3.1. Deve detectar, analisar e relatar suspeitas de tentativas de movimento lateral;

5.2.3.2. Deve detectar e rotear conexões que infringiram uma política para um servidor de interceptação, acionado por qualquer tentativa de acessar portas fechadas / filtradas em máquinas reais;

5.2.3.3. A solução deverá provisionar dinamicamente um servidor de que faça a função de isca, do próprio fabricante ou através de integração com terceiros. Caso a solução seja de terceiros, deverá ser incluída nesta contratação;

5.2.3.4. É necessário usar máquinas reais (e não emulações) como base do servidor de interceptação ("servidor isca de alta interação"), e os invasores devem poder interagir com o servidor de fraude em todos os níveis.

5.2.3.5. Deve ser capaz de apresentar servidores de armadilhas baseados em Windows e Linux e bancos de dados;

5.2.3.6. Deve fornecer isolamento completo do servidor de interceptação e impedir que o invasor use o mesmo como plataforma de lançamento para atacar ainda mais os ativos da rede;

5.2.3.7. Deve possuir a capacidade de efetuar download de todos os arquivos criados e modificados para análise local do servidor de interceptação;

5.2.3.8. Deve possuir a capacidade de baixar capturas de tela do servidor de interceptação do Windows capturadas durante a interação com um invasor;

5.2.3.9. É necessário registrar todas as credenciais tentadas em um servidor de interceptação;

5.2.3.10. Deve oferecer suporte a uma lista configurável de credenciais que concederia ao invasor acesso ao serviço solicitado no servidor de interceptação;

- 5.2.3.11. Deve suportar um número configurável de tentativas de login antes de conceder ao invasor de força bruta o acesso ao serviço solicitado no servidor de interceptação;
 - 5.2.3.12. Deve ser capaz de detectar todas as chamadas do sistema no nível do sistema operacional, bem como a atividade no nível do aplicativo e usuário executando o aplicativo, no servidor de interceptação;
 - 5.2.3.13. Deve ser capaz de detectar a atividade do invasor no servidor de interceptação sem uma maneira razoável de o invasor perceber que está envolvido em um sistema altamente monitorado
 - 5.2.3.14. Deve ser capaz de apresentar a gravação da sessão completa de todas as atividades do invasor no nível do sistema e do aplicativo
 - 5.2.3.15. Deve ser capaz de detectar automaticamente a atividade humana versus ataques automatizados
 - 5.2.3.16. A solução deve possuir mecanismo de consulta instantânea nos dispositivos gerenciados compatível com padrão OSQUERY;
 - 5.2.3.17. Deverá ter a capacidade de coletar informações dos ativos com o agente da solução, como exemplo, mas não se limitando: Número de CPUs, processos em execução, usuários pertencentes ao grupo de administrador local, softwares instalados, uptime do sistema, ativos com um determinado software instalado, entre outros;
 - 5.2.3.18. Ser capaz de aplicar Etiquetas no ambiente através do resultado de uma consulta e/ou coleta de informações;
 - 5.2.3.19. Deverá ser possível agendar estas consultas para execuções contínuas, podendo inclusive adicionar uma etiqueta automaticamente aos ativos encontrados;
 - 5.2.3.20. Deverá ser possível consultar vulnerabilidades nos ativos, e aplicar etiquetas dedicadas aos ativos vulneráveis. Estas etiquetas de vulnerabilidade poderão ser utilizadas no mapa de fluxo de dados e também para criação de políticas;
- 5.2.4. Kubernetes;
- 5.2.4.1. Os agentes da solução deverão operar como um DaemonSet diretamente no Nó do Cluster;

- 5.2.4.2. Deve coletar todos os fluxos de dados de comunicação, entre PODs, bem como com origem e/ou destino de infraestrutura não baseada em micro serviço;
- 5.2.4.3. Deverá ser compatível com, no mínimo as seguintes Plataformas de Containers:
 - 5.2.4.3.1. OpenShift 3.x/4.x;
 - 5.2.4.3.2. Kubernetes nativo;
- 5.2.4.4. Ser capaz de visualizar todo o fluxo de dados dos PODs no mesmo mapa de fluxo de dados, ou seja, o mapa de fluxo de dados deverá ser único para Servidores, Desktops, Cloud Workload e PODs;
- 5.2.4.5. Ser possível configurar regras de permissão, alerta e bloqueio para comunicações no ambiente. Estas regras deverão também ser baseadas em etiquetas;
- 5.2.4.6. Deverá possuir integração nativa com as plataformas acima para coletar metadados e labels e transformar estes em etiquetas na solução, de forma automática e sem necessidade de ajustes ou customizações na plataforma de Kubernetes e/ou PODs. Deverá ser obrigatoriamente utilizado o objeto "Labels", não sendo necessário o uso ou criação de qualquer outro objeto no YAML e/ou Kubernetes;
- 5.2.4.7. Deverá também refletir de forma automática, qualquer alteração de metadados e labels do cluster, ajustando as regras de segmentação já criadas;
- 5.2.4.8. Ser capaz de visualizar todo o fluxo de dados dos PODs no mesmo mapa de fluxo de dados, ou seja, o mapa de fluxo de dados deverá ser único para Servidores, Desktops, Cloud Workload e PODs;
- 5.2.4.9. Deverá apresentar informações de comunicação entre os PODs, incluindo qual o processo (container) que originou ou recebeu a comunicação, a porta e o protocolo utilizado, além da imagem e linha de comando utilizada, suportando a identificação de uso indevido dentro da plataforma de kubernetes;
- 5.2.4.10. Deverá apresentar o fluxo de dados leste-oeste e norte-sul (comunicação de e para a internet);

5.2.4.11. A solução não deve limitar a quantidade de PODs utilizados por nó de cluster, estando este limitado apenas ao suporte oficial da plataforma de kubernetes

5.2.4.12. A solução não deve gerar nenhum tipo de impacto ou atraso na subida de recursos do ambiente de kubernetes (PODs, Serviços e Etc)

5.2.4.13. A solução deve permitir de forma simples criar regras de proteção (bloqueio) e com apenas uma regra bloquear um acesso externo ao cluster acessar uma aplicação interna ao cluster, reduzindo esforço administrativo e dificuldade no entendimento final da regra (Ex.: Block VM Externa -> K8s App)

5.2.5. Integrações:

5.2.5.1. Deve fornecer alertas em tempo real contendo relatórios completos de eventos de segurança;

5.2.5.2. Deve suportar a personalização de alertas por gravidade, conteúdo etc.

5.2.5.3. Deve enviar alertas por e-mail

5.2.5.4. Deve oferecer suporte ao mascaramento de informações confidenciais de alertas por e-mail (ou seja, senhas)

5.2.5.5. É necessário integrar-se ao SIEM;

5.2.5.6. Deve exportar IOCs para o formato STIX

5.2.5.7. Deve suportar uma API para integração com serviços externos

5.2.5.8. Deve possuir integração com ferramenta de análise de vulnerabilidade para coletar metadados e criar etiquetas baseada em Vulnerabilidades existentes;

5.2.5.9. Possuir integração com ferramenta de gerência centralizada de Firewalls;

5.2.6. Acesso remoto seguro:

5.2.6.1. A CONTRATADA deverá oferecer uma solução de acesso remoto seguro baseada no conceito de ZTNA (Zero Trust Network Access). O objetivo é aumentar a maturidade de segurança nas atividades de acesso seguro aos recursos de rede com base em políticas de confiança mínima, independente se o usuário estiver dentro ou fora da sede no

MPRJ. A solução deve incluir, minimamente, autenticação multifatorial, criptografia do tráfego de dados e monitoramento contínuo do comportamento do usuário e do dispositivo. Essa solução proporcionará uma abordagem eficaz para proteger os recursos de rede do MPRJ contra ameaças internas e externas, aumentando a segurança e a privacidade dos dados.

5.2.6.2. Características Gerais e Arquitetura:

5.2.6.2.1. A solução deverá permitir somente comunicação mTLS/TLS entre seus usuários e seu ambiente de aplicações;

5.2.6.2.2. A solução deverá oferecer uma arquitetura de nuvem dupla, fechando as conexões de entrada de firewall (inbound);

5.2.6.2.3. A solução deverá possuir uma máquina virtual que será responsável por realizar o acesso as aplicações, realizando apenas uma liberação de saída (outbound) para a nuvem da solução;

5.2.6.2.4. A imagem da máquina virtual deverá ser compatível com no mínimo as seguintes plataformas:

5.2.6.2.4.1. VMware

5.2.6.2.4.2. OpenStack/KVM

5.2.6.2.4.3. Microsoft Hyper-V

5.2.6.2.4.4. Docker

5.2.6.2.5. A solução deverá permitir a utilização de uma ou mais máquinas virtuais (sem custo adicional) para alta disponibilidade;

5.2.6.2.6. A solução deverá liberar acesso apenas a usuários autenticados e apenas as suas próprias aplicações;

5.2.6.2.7. A solução deve prover imagem virtual para instalação local de elemento para orquestrar autenticação de usuários em base local, sem a necessidade de comunicação com internet;

5.2.6.2.8. A solução deve suportar integração com Identity Providers (IdPs) com no mínimo dois dos seguintes formatos: Active Directory (AD), Lightweight Directory Access Protocol (LDAP), Active Directory Lightweight Directory Services (AD

LDS), System for Cross-domain Identity Management (SCIM);

- 5.2.6.2.9. A solução deverá oferecer acesso, sem a necessidade de instalar um agente, a aplicações baseadas em navegador (HTTP) e permitir que proteja também sem agente o acesso a aplicações/Aplicativos que utilizam (RDP e SSH);
- 5.2.6.2.10. O acesso a aplicações TCP/UDP, deve ser realizado através de um túnel seguro para nuvem da solução e não para o ambiente da CONTRATANTE, e deve estabelecer conexão apenas a aplicações autorizadas;
- 5.2.6.2.11. O agente utilizado pela solução deverá fornecer recursos de controle de postura dos dispositivos que estão realizando o acesso;
- 5.2.6.2.12. A solução deve permitir a configuração e uso de provedores de identidade (IdPs), sendo possível utilizar a própria solução com seu IdP;
- 5.2.6.2.13. A solução deve ser capaz de se integrar com ao menos os seguintes provedores:
 - 5.2.6.2.13.1. Google
 - 5.2.6.2.13.2. Microsoft Azure AD
 - 5.2.6.2.13.3. Outras soluções baseadas em SAML
- 5.2.6.2.14. A solução deverá possuir Ponto de Presença (POP) no Brasil;
- 5.2.6.2.15. A solução deve possuir estrutura de diretório e provedor de identidade (IdP) próprio, não dependendo da integração com terceiros para acesso as aplicações;
- 5.2.6.2.16. A solução deve utilizar protocolo seguro (TLS) para integração com provedores de identidade
- 5.2.6.2.17. A estrutura de diretório e IdP próprio deve prover no mínimo os seguintes recursos:
 - 5.2.6.2.17.1. Envio de link por e-mail para ingresso no diretório;

- 5.2.6.2.17.2. Política de senhas (mínimo de caracteres, complexidade, não pode ser armazenada em texto claro etc.);
- 5.2.6.2.17.3. Operações em massa (exclusão, convite e adição em grupo) por meio de API ou agente;
- 5.2.6.2.17.4. Criação de atributos adicionais para mapeamento com outros diretórios;
- 5.2.6.2.17.5. Possibilitar SSO e autenticação de múltiplo fator nativos;
- 5.2.6.2.17.6. Suporte à integração via SAML;
- 5.2.6.2.17.7. Suporte a uso de estrutura de nome de domínio própria;
- 5.2.6.2.18. A solução deve ter SLA mínimo de 99%;
- 5.2.6.2.19. Acesso e Gerenciamento;
 - 5.2.6.2.19.1. O acesso a solução deve possuir controles baseados no método RBAC;
 - 5.2.6.2.19.2. O controle de acesso a solução deve permitir no mínimo os seguintes perfis de acesso:
 - 5.2.6.2.19.3. Administrador (Acesso completo);
 - 5.2.6.2.19.4. Visualizador (Apenas leitura);
 - 5.2.6.2.19.5. Administrador de aplicações;
 - 5.2.6.2.19.6. Administrador de conetores;
- 5.2.6.2.20. A solução deve permitir a combinação de um ou mais perfis de acesso;
- 5.2.6.2.21. A solução deve utilizar protocolo seguro (TLS) para integração com provedores de identidade;
- 5.2.6.2.22. A solução deve permitir a configuração e uso de provedores de identidade (IdPs), sendo possível utilizar a própria solução com seu IdP;

- 5.2.6.2.23. A solução deve permitir a configuração das cifras utilizadas pelo protocolo de integração com os provedores de identidade, para autenticação das mensagens, suportando, no mínimo, os seguintes protocolos:
- 5.2.6.2.23.1. SHA256
 - 5.2.6.2.23.2. SHA384
 - 5.2.6.2.23.3. MD5
 - 5.2.6.2.23.4. 3DES
- 5.2.6.2.24. A solução deve permitir a configuração de tempo de sessão do provedor de identidade, possibilitando que sessões sem uso (idle) sejam expiradas para segurança;
- 5.2.6.2.25. A solução deve permitir um limite máximo para sessões ativas, sendo possível configurar valores até no máximo 5 dias;
- 5.2.6.2.26. Suporte a identidade SAML nativa para aplicações na nuvem, na Web e no local, para permitir SSO fácil para os usuários;
- 5.2.6.2.27. A solução deve permitir o uso de outros provedores de identidades baseados em SAML, e permitir também ela mesma o provedor de identidades SAML;
- 5.2.6.2.28. A solução deve permitir o uso de provedor de identidade SAML com Microsoft Enhanced Client ou Proxy (ECP);
- 5.2.6.2.29. A solução deve ser compatível com Open ID Connect (OIDC) suportando processo de autenticação através deste protocolo
- 5.2.6.2.30. A solução deve ser compatível com Web Service Federation, suportando a integração com aplicações legadas que utilizam este formato;
- 5.2.6.2.31. A solução deve permitir o bloqueio e desbloqueio de usuários ao acesso as aplicações;

- 5.2.6.2.32. Caso seja realizado o bloqueio e desbloqueio de um usuário que esteja acessando uma aplicação através do agente, seu bloqueio deve refletir de forma imediata forçando o logout do usuário assim que aplicado o bloqueio;
- 5.2.6.2.33. A solução deve permitir single sing-on (SSO) para desktops, suportando autenticação integrada do windows baseada em Kerberos, ajudando a fornecer uma experiência de acesso unificada ao usuário final sem gerar fricção;
- 5.2.6.2.34. A solução deve permitir a utilização de duplo fator de autenticação para os acessos;
- 5.2.6.2.35. A solução deve permitir a configuração do acesso utilizando duplo fator para no mínimo os seguintes cenários:
 - 5.2.6.2.35.1. Global
 - 5.2.6.2.35.2. Aplicação
 - 5.2.6.2.35.3. Diretório
 - 5.2.6.2.35.4. Grupo
- 5.2.6.2.36. A solução deve permitir a configuração de mais de uma opção de duplo fator, tendo nos mínimos as seguintes opções:
 - 5.2.6.2.36.1. E-mail;
 - 5.2.6.2.36.2. Authentication Token (TOTP)
 - 5.2.6.2.36.3. MFA nativo da solução
- 5.2.6.2.37. A solução, no que diz respeito a acesso multifatorial deve ser compatível com os padrões do PCI DSS;
- 5.2.6.2.38. A solução deve possuir solução de duplo fator nativa, fornecendo suporte também nativo a FIDO2;

- 5.2.6.2.38.1. Caso não possua, deve ser disponibilizada outra forma de autenticação via FIDO2, seguindo no mínimo os requerimentos:
 - 5.2.6.2.38.1.1. Através de software comercial (não podendo ser opensource, free, ou semelhantes), suportado pelo fabricante e pela Contratada;
 - 5.2.6.2.38.1.2. Através de hardware token, seguindo o mesmo prazo de suporte, com toda a estrutura de hardware, software e serviço necessária para o seu correto funcionamento e integração;
 - 5.2.6.2.38.1.3. No caso de Hardware Token, deverá ser levado em consideração uma quantidade de 30% adicional do número total de usuários especificados, para eventuais trocar referentes a falhas e perdas do dispositivo;
 - 5.2.6.2.38.1.4. Em ambos os casos, deverá ser entregue uma licença para cada usuário deste órgão, ou seja, não poderá ser considerado pools de licença, licenças concorrentes e licenças e hardware tokens.
- 5.2.6.2.39. A solução deve permitir ao administrador a configuração de bypass do duplo fator de autenticação, caso algumas situações sejam atendidas:
 - 5.2.6.2.39.1. Quando o acesso estiver sendo realizado da rede corporativa;
 - 5.2.6.2.39.2. Quando o acesso estiver sendo feito através de um dispositivo gerenciado e contendo um certificado válido;
 - 5.2.6.2.39.3. Utilizando uma combinação das opções acima.
- 5.2.6.2.40. A solução deve permitir o uso de certificados para autenticação e acesso as aplicações, mesmo para cenários sem agente;

- 5.2.6.2.41. A solução deve permitir o uso e configuração de autenticação mútua para conexão entre os dispositivos dos usuários e a nuvem da solução
- 5.2.6.2.42. Em caso de uso de certificados para autenticação, se ele não for válido, o acesso deve ser negado
- 5.2.6.2.43. A solução deve suportar o uso do protocolo de validação online de certificados (OCSP), facilitando a gestão da solução e certificados utilizados pela companhia
- 5.2.6.2.44. A solução deve permitir a criação de zonas de acesso que serão utilizadas como critérios nas políticas de acesso. Suportando ao menos 900 IPs e 10 zonas distintas
- 5.2.6.2.45. A solução deve possuir um dashboard para acompanhamento geral do status da solução, fornecendo informações mínimas como:
 - 5.2.6.2.45.1. Aplicações mais utilizadas
 - 5.2.6.2.45.2. Localidade dos usuários
 - 5.2.6.2.45.3. Principais Usuários
 - 5.2.6.2.45.4. Sistemas Operacionais e Browsers utilizados
 - 5.2.6.2.45.5. Falhas de login (Senha inválida ou Usuário inválido)
 - 5.2.6.2.45.6. Aplicações por cliente
 - 5.2.6.2.45.7. Atividade geral dos usuários
 - 5.2.6.2.45.8. Saúde geral do ambiente (Aplicações, Diretórios, e etc)
- 5.2.6.2.46. A solução deve permitir a criação de relatórios customizados e que possam ajudar na identificação de problemas e também uso geral das aplicações
- 5.2.6.2.47. Os relatórios devem possuir no mínimo as seguintes opções:

- 5.2.6.2.47.1. Dados de acesso a aplicações;
- 5.2.6.2.47.2. Auditoria SSH (com toda a interação via teclado), para as sessões de acesso via protocolo SSH;
- 5.2.6.2.47.3. Dados de acesso dos usuários;
- 5.2.6.2.47.4. Dados de acesso em geral (sessões ativas, duração da sessão, falhas de login);
- 5.2.6.2.47.5. Dados de Sistema.
- 5.2.6.2.48. A solução deve suportar integração com SIEM através de API ou através do envio de syslog, facilitando a integração com este tipo de solução
- 5.2.6.2.49. A solução deve possuir uma API completa que permita realizar as operações de configuração, segurança e entrega de aplicações
- 5.2.6.3. Criação, Acesso e Gerenciamento de Aplicações:
 - 5.2.6.3.1. Deve ser possível realizar o acesso a aplicações de diversos tipos como, RDP, HTTP, SSH, VNC, entre outras, sejam on-premises ou em nuvem;
 - 5.2.6.3.2. A solução deverá possuir recursos para aplicações não baseada em navegador, utilizar um agente para realizar a comunicação através de protocolos TCP e UDP;
 - 5.2.6.3.3. O acesso a aplicações TCP/UDP, devem ser realizadas através de um túnel seguro, estabelecendo conexão apenas a aplicações autorizadas;
 - 5.2.6.3.4. O agente utilizado pela solução deverá fornecer recursos de controle de postura dos dispositivos que estão realizando o acesso;
 - 5.2.6.3.5. Deve ser possível prover acesso e controlar aplicações de diversas categorias, no mínimo para:
 - 5.2.6.3.5.1. HTTP/HTTPS ou Aplicação Web;

- 5.2.6.3.5.2. Sharepoint;
- 5.2.6.3.5.3. RDP;
- 5.2.6.3.5.4. VNC;
- 5.2.6.3.5.5. SSH;
- 5.2.6.3.5.6. SAML;
- 5.2.6.3.5.7. GitHub;
- 5.2.6.3.5.8. O365.

- 5.2.6.3.6. Deve ser possível verificar o status da aplicação diretamente na console de gerência, mostrando se a mesma está online ou offline;
- 5.2.6.3.7. Caso a aplicação esteja com o status de offline, deve ser mostrado o motivo exato no mesmo local;
- 5.2.6.3.8. A solução deverá permitir associar cada aplicação a uma máquina virtual específica a desejo do administrador e que será responsável por realizar o acesso a aplicação;
- 5.2.6.3.9. A solução deve permitir associar de forma individual, qual provedor de identidades será utilizado para o seu acesso;
- 5.2.6.3.10. A solução deve permitir associar um ou mais diretórios para autenticação dos usuários;
- 5.2.6.3.11. A solução deve permitir criar listas de controle de acesso para cada aplicação;
- 5.2.6.3.12. A solução deve permitir elencar as aplicações que possuem mais uso para que sejam facilmente identificadas;
- 5.2.6.3.13. A solução deve permitir a publicação de uma aplicação utilizando diferentes zonas globais, possibilitando a escolha de uma zona mais próxima da aplicação, reduzindo a latência de acesso.

- 5.2.6.3.14. Deve ser possível publicar uma aplicação utilizando o domínio da própria empresa ou da solução contratada;
- 5.2.6.3.15. A solução deve possuir controle de versionamento das aplicações publicadas, permitindo realizar rollback para configurações mais antigas;
- 5.2.6.3.16. Deve ser possível realizar o acesso as aplicações através de um portal único provido pela solução;
- 5.2.6.3.17. A solução deve permitir além do acesso baseado em FQDN, acesso também baseado em URL path, com o objetivo de diminuir o impacto gerado na migração para o modelo zero trust;
- 5.2.6.3.18. A solução deve permitir a reescrita de URLs, facilitando o acesso a aplicações internas e externas, com ou sem a utilização de proxy;
- 5.2.6.3.19. A solução deve permitir a migração das aplicações entre zonas de forma única ou diversas ao mesmo tempo;
- 5.2.6.3.20. No caso de uso de aplicações do tipo RDP, deve ser possível especificar diferentes operações permitidas, minimamente:
 - 5.2.6.3.20.1. Quais programas devem ser inicializados junto com a sessão;
 - 5.2.6.3.20.2. Especificar qual aplicação remota pode ser acessada;
 - 5.2.6.3.20.3. Possibilidade de copiar e colar conteúdo;
 - 5.2.6.3.20.4. Possibilidade de uso de áudio;
 - 5.2.6.3.20.5. Possibilidade e utilizar recursos de impressão;
 - 5.2.6.3.20.6. Possibilidade de utilizar compartilhamento de arquivos.
- 5.2.6.3.21. A solução também deve possuir recursos para aplicações tipo RDP o uso de SSO;

- 5.2.6.3.22. No caso de uso de aplicações do tipo SSH, a solução deve permitir a configuração via chave pública/privada ou usuário e senha. No caso de chave privada, a mesma não deve ser armazenada na nuvem e sim na máquina virtual responsável por realizar o acesso a aplicação de destino;
- 5.2.6.3.23. A solução deve permitir o controle de acesso as aplicações, aplicando regras de bloqueio/negação, para no mínimo os seguintes critérios:
 - 5.2.6.3.23.1. URL solicitada pelo usuário;
 - 5.2.6.3.23.2. Grupo do usuário;
 - 5.2.6.3.23.3. Usuário;
 - 5.2.6.3.23.4. IP do cliente;
 - 5.2.6.3.23.5. País;
 - 5.2.6.3.23.6. Hora do acesso;
 - 5.2.6.3.23.7. Hostname, Porta e Protocolo da aplicação;
 - 5.2.6.3.23.8. Risco do dispositivo.
- 5.2.6.3.24. A solução deve possuir recursos de compressão de tráfego, reduzindo o consumo de recursos e latência;
- 5.2.6.3.25. A solução deve permitir a configuração de balanceamento de carga, distribuindo o tráfego do acesso entre 2 ou mais servidores, aumentando a concorrência de usuários acessando uma aplicação e confiabilidade geral da aplicação.
- 5.2.6.3.26. A solução deve suportar a customização de cabeçalhos a serem enviados a aplicação configurada.
- 5.2.6.4. Agente e postura dos dispositivos
 - 5.2.6.4.1. O agente utilizado pela solução deve realizar o acesso as aplicações sem a necessidade de estabelecer um túnel VPN;

5.2.6.4.2. O agente utilizado deve permitir a coexistência com outros túneis VPN caso existam;

5.2.6.4.3. O agente utilizado deve possuir capacidades de SSO e múltiplo fator de autenticação;

5.2.6.4.4. A comunicação do agente deve suportar comunicação via protocolos TCP e UDP;

5.2.6.4.5. A comunicação do agente deve suportar aplicações, no mínimo para:

5.2.6.4.5.1. SSH;

5.2.6.4.5.2. RDP;

5.2.6.4.5.3. SFTP;

5.2.6.4.5.4. SCP;

5.2.6.4.5.5. TFTP.

5.2.6.4.6. O agente deve suportar máquinas físicas e virtuais;

5.2.6.4.7. O agente deve suportar no mínimo os seguintes sistemas operacionais:

5.2.6.4.7.1. Windows 10;

5.2.6.4.7.2. Windows 11;

5.2.6.4.7.3. Apple MacOS;

5.2.6.4.7.4. Ubuntu 20.04 ou 22.04;

5.2.6.4.7.5. iOS 11 ou superior;

5.2.6.4.7.6. Android 6 ou superior.

5.2.6.4.8. Deve ser permitido realizar a atualização do agente de forma centralizada;

- 5.2.6.4.9. Deve ser possível extrair e enviar logs para fins de diagnostico e troubleshooting;
- 5.2.6.4.10. O agente deve permitir realizar algumas operações básicas como:
 - 5.2.6.4.10.1. Coletar diagnostico;
 - 5.2.6.4.10.2. Copiar informações do dispositivo (ID, Nome do Usuário, Provedor de Identidade e versão do agente);
 - 5.2.6.4.10.3. Salvar e enviar logs de debug;
 - 5.2.6.4.10.4. Sincronizar com a camada de gerenciamento da solução;
 - 5.2.6.4.10.5. Resetar o agente;
 - 5.2.6.4.10.6. Verificar alertas;
 - 5.2.6.4.10.7. Verificar a postura e remediações necessárias.
- 5.2.6.4.11. O agente deve suportar captive portal.
- 5.2.6.4.12. A solução deve possuir recurso que identifique se o endpoint está dentro da rede corporativa ou remoto e permitir a aplicação de políticas distintas para cada tipo de acesso;
- 5.2.6.4.13. A solução ZTNA deve permitir o controle de acesso as aplicações, aplicando regras de bloqueio/negação, para no mínimo os seguintes critérios:
 - 5.2.6.4.13.1. URL solicitada pelo usuário;
 - 5.2.6.4.13.2. Grupo do usuário;
 - 5.2.6.4.13.3. Usuário;
 - 5.2.6.4.13.4. IP do cliente;
 - 5.2.6.4.13.5. País;

- 5.2.6.4.13.6. Hora do acesso;
- 5.2.6.4.13.7. Hostname, Porta e Protocolo da aplicação.
- 5.2.6.4.14. O agente deve suportar ambientes que possuem forward proxy;
- 5.2.6.4.15. O agente deve possuir capacidade de analisar a postura do dispositivo, tanto para desktops quanto dispositivos móveis;
- 5.2.6.4.16. O agente deve fornecer dados que ajudem a definir o risco de acesso do dispositivo;
- 5.2.6.4.17. O agente deve conseguir capturar ao menos os seguintes dados para uso:
 - 5.2.6.4.17.1. Anti-malware;
 - 5.2.6.4.17.2. Certificados;
 - 5.2.6.4.17.3. Nome e ID do dispositivo;
 - 5.2.6.4.17.4. Última atualização;
 - 5.2.6.4.17.5. Status da criptografia de disco;
 - 5.2.6.4.17.6. Versão do agente instalado;
 - 5.2.6.4.17.7. Versão do Browser e SO utilizados;
 - 5.2.6.4.17.8. Status do firewall do sistema;
 - 5.2.6.4.17.9. Status biometria (mobile);
 - 5.2.6.4.17.10. Status Jailbreak (mobile);
 - 5.2.6.4.17.11. Status do bloqueio de tela.
- 5.2.6.4.18. A solução deve permitir a criação de perfis de risco baseado nos dados coletados;

5.2.6.4.19. A solução deve permitir definir regras de acesso específicas baseadas nas seguintes categorias de riscos:

5.2.6.4.19.1. Baixo;

5.2.6.4.19.2. Médio;

5.2.6.4.19.3. Alto.

5.2.6.4.20. O agente deve permitir a integração com outras soluções para coletas adicionais de dados, como CrowdStrike e VMWare Carbon Black;

5.2.6.4.21. A solução deve permitir a atribuição de Etiquetas para o risco dos dispositivos independente do risco associado baseado nos dados coletados;

5.2.6.4.22. A solução deve permitir o bloqueio de um dispositivo baseado nas categorias de risco ou Etiquetas criadas.

6. PROTEÇÃO DAS INFORMAÇÕES, PRIVACIDADE e PROTEÇÃO DE DADOS PESSOAIS

6.1. Características Gerais

6.1.1. O sistema deve ser acessível através dos navegadores de internet mais populares, sem limitações ou exigência de plugins ou complementos para sua plena execução, utilizando HTTPS em todas as suas requisições;

6.1.2. O sistema deverá funcionar, sem limitações, no idioma Português do Brasil, com exceção termos como "download" e similares;

6.1.3. O sistema deverá permitir a criação de usuários/acessos adicionais e sua inativação a qualquer momento;

6.1.4. O sistema deverá permitir definir a data de expiração de acesso deste usuário, sendo que caso ultrapassada a data prevista, o usuário será inativado;

6.1.5. O sistema deverá disponibilizar perfis de acesso pré-configurados, considerando limitações de acesso para cada perfil, permitindo a criação de novos perfis personalizados;

- 6.1.6. O sistema não deverá possuir limitação de quantidade de usuários e perfis a serem adicionados;
- 6.1.7. O sistema deve permitir integração com mecanismos de autenticação interna como LDAP, AD e SSO (Single sign-on);
- 6.1.8. O sistema deve permitir autenticação através do protocolo SAML e também OpenID;
- 6.1.9. O sistema deve permitir indicar o usuário que será o Encarregado pelo Tratamento de Dados Pessoais ou Data Protection Officer (DPO);
- 6.1.10. As API's de integração devem poder ser acessadas por chaves seguras através do protocolo OAuth2.0;
- 6.1.11. O sistema deverá permitir criar usuários específicos para acesso às API's e chaves de API;
- 6.1.12. O sistema deverá possuir uma política de criação de senhas fortes;
- 6.1.13. O sistema deverá possuir mecanismo de 2FA de forma nativa;
- 6.1.14. O sistema deverá possuir mecanismo que permita personalizar o tempo para expiração da senha criada pelos usuários;
- 6.1.15. O sistema deverá possuir mecanismo que permita personalizar a quantidade de dias que o usuário poderá ficar sem acessar o sistema, sendo que caso seja excedido, o usuário deverá ter seu acesso expirado;
- 6.1.16. O sistema deverá permitir a personalização do tempo máximo de inatividade da sessão dos usuários;
- 6.1.17. O sistema deverá permitir personalizar a quantidade máxima de tentativas de login, sendo que caso seja excedido, o usuário deverá ser bloqueado;
- 6.1.18. O usuário deverá permitir a configuração de SMTP próprio, para que as comunicações feitas através do sistema com o titular de dados usem o domínio da organização;
- 6.1.19. O sistema deverá permitir o cadastro da logomarca da organização, para utilização em comunicações com titulares de dados;
- 6.1.20. O sistema deve possuir toda a documentação técnica e/ou manuais em idioma Português do Brasil, com exceção de termos como "download" e similares;
- 6.1.21. O sistema deverá possuir todos os treinamentos acerca do uso do sistema em idioma Português do Brasil;
- 6.1.22. O sistema deve enviar notificações de expiração de acesso para usuários do sistema que tiverem a data de expiração excedida;
- 6.1.23. O sistema deve ter um local com notícias, atualizações regulatórias, documentos de autoridades e demais informações com atualização diária

quanto ao mercado de privacidade e proteção de dados, boas práticas na área e amplo material com vídeo, guias e recomendações de especialistas.

6.2. Módulo de Gerenciamento de Cookies e Portais e Websites

- 6.2.1. O sistema deverá permitir o cadastro de um ou mais websites para gerenciamento e execução de varreduras;
- 6.2.2. O sistema deverá permitir a configuração e agendamento de uma periodicidade de varreduras, apresentando relatório sobre cada varredura realizada;
- 6.2.3. O sistema deverá identificar os cookies utilizados nos domínios cadastrados sem quaisquer limitações acerca da composição do domínio (.com, .com.br, .gov e outros);
- 6.2.4. O sistema deverá permitir a configuração de notificações acerca das varreduras realizadas;
- 6.2.5. O sistema deve classificar automaticamente os cookies encontrados na varredura em diferentes idiomas;
- 6.2.6. O sistema deverá permitir a edição de um cookie, seus atributos e informar o nome do fornecedor (third-party) responsável pelo cookie;
- 6.2.7. O sistema deverá permitir o agrupamento de cookies por categoria, possibilitando adicionar, alterar e remover grupos de cookies;
- 6.2.8. O sistema deverá permitir a exclusão de cookies mapeados de forma granular ou a partir de ação em massa de exclusão do mapeamento;
- 6.2.9. O sistema deverá permitir a personalização do aviso de cookies (cores, textos, formato);
- 6.2.10. O sistema deverá permitir gerar o aviso de cookies em diferentes idiomas;
- 6.2.11. O banner de cookies deve possuir a capacidade de ser multi-idioma, detectando automaticamente o idioma do navegador para apresentar a melhor experiência do titular, com ao menos Português Brasileiro, Inglês e Espanhol;
- 6.2.12. O sistema deverá permitir a integração do aviso de cookies através de script gerado em sua interface;
- 6.2.13. O sistema deverá, através do script disponibilizado, bloquear todos os cookies gerados no websites, com exceção dos obrigatórios ou essenciais;
- 6.2.14. O sistema deverá manter o registro dos registros de aceite e rejeição de cookies;
- 6.2.15. Deve existir plugin para integração nativa com Google Tag Manager;

- 6.2.16. O sistema deverá permitir a identificação e busca de um registro com base no IP utilizado e país de origem do usuário visitante que concedeu ou rejeitou um determinado consentimento;
- 6.2.17. O sistema deverá permitir que os cookies mapeados pelo monitoramento sejam automaticamente inseridos na política de cookies.

6.3. Gerenciamento de Políticas

- 6.3.1. O sistema deverá permitir adicionar novas políticas e editar os conteúdos dentro da sua interface;
- 6.3.2. O sistema deverá permitir classificar o tipo da política, atribuir responsáveis pelo seu gerenciamento e revisão;
- 6.3.3. O sistema deverá permitir a atribuição de prazos de validade e revisão da política;
- 6.3.4. O sistema deverá permitir a criação de políticas em diferentes idiomas;
- 6.3.5. O sistema deverá gerar um link público (URL) para acesso ao conteúdo da política, possibilitando a sua publicação e despublicação;
- 6.3.6. O sistema deverá permitir a configuração da interface visual (design) da política permitindo a edição de logomarca e cores a serem utilizadas;
- 6.3.7. O sistema deverá possuir mecanismo próprio que inibam a cópia do conteúdo da política no link público (URL) gerado;
- 6.3.8. O sistema deverá possuir mecanismo de versionamento das políticas, permitindo adicionar novas versões de uma política existente;
- 6.3.9. O sistema deverá permitir a consulta de versões anteriores das políticas;
- 6.3.10. O sistema deverá permitir no link público (URL) gerado acompanhar as alterações realizadas em cada versão;
- 6.3.11. O sistema deverá possuir mecanismos de integridade da política;
- 6.3.12. Deve ser possível inserir em uma política de cookies uma tabela de todos os cookies tratados pela empresa com atualização automática, ou seja, quando surgir um novo cookie a política deve ser atualizada;
- 6.3.13. Deve ser possível inserir em uma política uma tabela com todos os dados pessoais sendo tratados pela empresa e suas finalidades com atualização automática, ou seja, quando surgir um novo dado pessoal a política deve ser atualizada;
- 6.3.14. O sistema deverá possuir uma API REST para consulta e exibição de políticas de modo que o conteúdo das políticas possam ser inseridos em qualquer portal ou aplicativo;

- 6.3.15. A ferramenta de gestão de políticas deve possuir histórico de versões e fornecer notificações por email para usuários do sistema quando são feitas alterações nas políticas;
- 6.3.16. O sistema deverá permitir a integração com o módulo de Gestão de Consentimentos para a criação de mecanismos de coleta de anuências e consentimentos sobre termos e políticas;
- 6.3.17. O sistema deverá armazenar os logs de consentimentos vinculados a cada versão de política e/ou termo.

6.4. Gestão de Atendimento de Titulares

- 6.4.1. O sistema deverá possuir um link público (URL) de um formulário para receber solicitações que serão realizadas pelos titulares de dados;
- 6.4.2. O formulário automaticamente deverá ser apresentado em múltiplos idiomas, conforme as configurações do navegador do usuário;
- 6.4.3. O sistema deverá permitir a configuração das categorias de solicitações que estarão disponíveis, assim como a definição do prazo de atendimento para cada uma das categorias definidas;
- 6.4.4. O sistema deverá permitir a configuração de templates de respostas para cada categoria de solicitação;
- 6.4.5. O sistema deverá permitir a configuração de quais tipos de direitos poderão ser respondidos através de automação do procedimento de modo que pedidos que dependam de aprovação do DPO não sejam automatizados e pedidos que não dependam de aprovação possam ser atendidos sem intervenção humana;
- 6.4.6. O sistema deverá permitir a configuração de um ou mais responsáveis por uma categoria de solicitação;
- 6.4.7. O sistema deverá possuir um workflow próprio com todas as etapas de uma solicitação sendo no mínimo necessário as etapas de autenticação, confirmação de identidade, tratamento do pedido, pedido respondido, pedido rejeitado e pedido finalizado;
- 6.4.8. O sistema deverá permitir a customização das etapas de solicitação, possibilitando a definição de responsáveis e tempo máximo de permanência em cada etapa;
- 6.4.9. O sistema deverá permitir a configuração dos tipos de titulares que aparecerão no formulário;
- 6.4.10. O sistema deverá permitir a customização de texto/mensagem antes dos campos do formulário, assim como dos campos do formulário;

- 6.4.11. O sistema deverá disponibilizar no formulário, minimamente a coleta dos seguintes dados dos usuários: Nome, E-mail e CPF;
- 6.4.12. O sistema deverá possuir a possibilidade de adição de novos campos dos seguintes tipos, com minimamente: Texto, Número, Checkbox, Seleção, Upload de Arquivo;
- 6.4.13. O sistema deverá permitir a customização de expressão regular (regex) sobre os campos adicionais para que eles sejam validados;
- 6.4.14. O sistema deverá permitir vincular políticas cadastradas ao formulário de solicitações;
- 6.4.15. O sistema deverá gerar um protocolo, ID, registro único para identificar cada solicitação feita no formulário;
- 6.4.16. O sistema deverá enviar um e-mail de confirmação para o usuário solicitante;
- 6.4.17. O e-mail de confirmação deverá ser personalizado, com a possibilidade de inclusão de anexos para confirmação de identidade do solicitante;
- 6.4.18. O sistema deverá permitir a configuração da rejeição automática da solicitação caso o usuário não faça a confirmação do e-mail enviado;
- 6.4.19. O sistema deverá possuir um painel de visualização das solicitações contendo filtros de busca que permitam localizar uma ou mais solicitações;
- 6.4.20. O sistema deverá permitir a exportação da lista de solicitações, possibilitando a aplicação de filtros para o download em CSV dos pedidos selecionados;
- 6.4.21. O sistema deverá permitir acessar os detalhes de uma solicitação;
- 6.4.22. O sistema deverá permitir responder, encerrar e rejeitar uma solicitação;
- 6.4.23. O sistema deverá permitir anexar um arquivo na resposta da solicitação;
- 6.4.24. O sistema deverá salvar o histórico de respostas e o registro de todas as ações realizadas em uma solicitação (logs de auditoria) com a possibilidade de exportar os logs para CSV;
- 6.4.25. O sistema deverá permitir cadastrar tarefas/atividades para outros usuários do sistema acerca de uma solicitação;
- 6.4.26. O sistema deverá permitir registrar um incidente a partir de uma solicitação;
- 6.4.27. O sistema deverá permitir relacionar uma solicitação com outra;
- 6.4.28. O sistema deverá permitir atribuir motivos e causas a uma solicitação;
- 6.4.29. O sistema deverá permitir configurar e-mails da organização que irão receber notificações de novas solicitações;
- 6.4.30. O sistema deverá permitir configurar se o titular poderá responder os e-mails advindos do sistema;

- 6.4.31. O sistema deverá permitir personalizar os templates de e-mails enviados pelo sistema;
- 6.4.32. O sistema deverá permitir a integração o módulo de Data Discovery para realizar a busca de dados do titular;
- 6.4.33. O sistema deverá permitir a realização de respostas automáticas a partir do módulo de Data Discovery;
- 6.4.34. O sistema deverá possuir mecanismo para calcular o custo real de cada solicitação para organização apresentando em relatórios os custos em reais (R\$);
- 6.4.35. O sistema deverá possuir diferentes API's de integração com o módulo em formato REST;
- 6.4.36. O sistema deverá permitir buscar um usuário e visualizar as solicitações vinculadas à ele;
- 6.4.37. Deve ser possível que o administrador solicite o reprocessamento de um pedido de titular que buscou dados no Data Discovery, mas que precisa de atualização;
- 6.4.38. Refinamento de respostas: deve ser possível que diferentes pessoas da equipe trabalhem de forma colaborativa no pedido do titular, cada um com sua contribuição de modo que o DPO possa reunir facilmente todas as informações encontradas pelo time e responder ao titular;
- 6.4.39. O sistema deverá permitir importar titulares de dados em formato TXT ou CSV;
- 6.4.40. O sistema deverá permitir o registro de motivos e sub-motivos para a rejeição de solicitações de atendimento aos titulares;
- 6.4.41. O sistema deverá permitir a criação de tarefas automatizadas de busca de dados, vinculadas as solicitações recebidas, possibilitando a definição de responsáveis e prazos de execução da tarefa;
- 6.4.42. O sistema deverá permitir a exportação do histórico de atendimento vinculado a solicitação do titular, contendo as datas e responsáveis por cada ação realizada relacionada ao pedido (envio de resposta, inserção de anotação, etc.);
- 6.4.43. O sistema deverá permitir que pedidos em aberto sejam reprocessados, desta forma realizando novamente buscas de dados e demais ações vinculadas a cada tipo de solicitação;
- 6.4.44. O sistema deverá possuir recurso de inteligência artificial para apoio as demandas de atendimento às requisições de titulares de dados;
- 6.4.45. O sistema deverá realizar a análise de cada requisição de forma automatizada, sugerindo possíveis respostas a serem dadas ao solicitante;

6.4.46. Na análise de contexto, o sistema deverá levar em consideração o titular de dados requisitante, o tipo de direito solicitado e histórico de respostas enviadas;

6.4.47. O sistema deverá sugerir as respostas com base no contexto analisado para apoiar tomadas de decisão do encarregado de proteção de dados.

6.5. Gerenciamento de Consentimentos

6.5.1. O sistema deverá permitir a criação de finalidades de coleta de consentimento, autorizações e anuências, com a descrição detalhada de cada finalidade;

6.5.2. O sistema deverá permitir o agrupamento de finalidades;

6.5.3. O sistema deverá permitir personalizar o prazo de retenção de validade do consentimento do usuário;

6.5.4. O sistema deverá permitir cadastrar os dados pessoais que são vinculados a este consentimento e finalidade;

6.5.5. O sistema deverá permitir importar consentimentos do mapeamento de dados (ROPA);

6.5.6. O sistema deverá permitir visualizar os registros de aceite e rejeição de uma determinada finalidade;

6.5.7. O sistema deverá permitir gerar, em sua interface, um link público (URL) com conteúdo personalizável para coleta de consentimento de usuários;

6.5.8. O sistema deverá gerar um QR Code para acesso ao link público (URL) para coleta de consentimentos;

6.5.9. O sistema deverá permitir a customização de campos e do layout/design do formulário do link público (URL) de coleta de consentimento;

6.5.10. O sistema deverá permitir a customização do layout/design do link público (URL) de coleta de consentimento;

6.5.11. O sistema deverá permitir o envio de campanhas por e-mail para coleta de consentimento, autorização ou anuência dos usuários;

6.5.12. O sistema deverá permitir a customização do template de e-mail das campanhas;

6.5.13. O sistema deverá disponibilizar API's para integração e coleta de consentimentos em websites e aplicativos;

6.5.14. O sistema deverá possuir mecanismo para buscar um titular de dados e identificar os consentimentos, autorizações e anuências deste;

6.5.15. O sistema deverá possuir mecanismos de buscas e filtros que permitam ao menos filtrar por: finalidades, origem, status, nome, documento e e-mail;

- 6.5.16. O sistema deverá permitir a exportação do resultado da busca com os filtros aplicados;
- 6.5.17. O sistema deverá permitir a importação de titulares por upload de arquivos XLS e com o uso de API REST;
- 6.5.18. O sistema deverá permitir a realização de consulta assíncrona dos consentimentos, a partir de inserção de planilha para validação dos dados e dos consentimentos registrados;
- 6.5.19. O sistema deverá permitir vincular finalidades e status do consentimento, autorização e anuência aos titulares adicionados via importação;
- 6.5.20. A plataforma deve possuir um SDK em Javascript e para integração e pedido de consentimentos em portais web;
- 6.5.21. Exige-se que o SDK para aplicativos seja entregue para no mínimo as plataformas IOS (Apple) e Android (Google) em linguagem nativa, compatível com Android (Java/Kotlin) e IOS (Swift/Objective-C);
- 6.5.22. Deve permitir que o operador do sistema faça a revogação ou aceite de consentimentos em nome de um titular para casos em que o titular não tenha como fazer a ação livre de consentimento;
- 6.5.23. No caso de registros feitos por operadores do sistema, a plataforma deve guardar todos os logs para auditoria dessa ação realizada;
- 6.5.24. O sistema deverá ter um plugin pronto para Wordpress para que possa ser coletado consentimentos em formulários.

6.6. Portal da Privacidade

- 6.6.1. O sistema deverá disponibilizar uma interface logada para que o titular de dados possa gerenciar seus consentimentos e as solicitações;
- 6.6.2. O sistema deverá permitir que diferentes portais sejam criados, internos e externos, para interação com os titulares de dados e recebimento de alimentações do sistema;
- 6.6.3. O sistema deverá permitir que sejam realizadas no portal ações de criação e alimentação de novas atividades de tratamento, reporte de incidentes e respostas de avaliações;
- 6.6.4. A interface do portal deverá ser customizável, permitindo a alteração de elementos, textos, imagens, cores, logomarca;
- 6.6.5. O sistema deverá permitir a integração do portal através de link público (URL) e por QR Code;
- 6.6.6. O sistema deverá permitir escolher se o portal aceitará novos cadastros de titulares;

- 6.6.7. O sistema deverá permitir escolher se o portal terá ou não uma tela pública inicial (capa) onde podemos expor mais detalhes sobre nosso programa de adequação;
- 6.6.8. O sistema deverá permitir quais finalidades serão exibidas no portal para que o titular gerencie seus consentimentos;
- 6.6.9. O sistema deverá permitir a autenticação via token ou cadastro para integração com sistemas existentes;
- 6.6.10. Na autenticação via token, o usuário informará seu e-mail e então receberá um código de autenticação para realizar o login;
- 6.6.11. Na autenticação via cadastro, o usuário irá realizar o seu cadastro e realizará o login utilizando o e-mail e senha cadastrados;
- 6.6.12. O sistema deverá possuir mecanismo de autenticação de acesso ao portal integrado a provedores como GOV.BR, LinkedIn e Facebook, permitindo também integração com demais sistemas utilizados pela empresa;
- 6.6.13. O sistema deverá permitir aos usuários realizarem solicitações (pedidos de titular) através do portal;
- 6.6.14. O sistema deverá permitir aos usuários gerenciarem as condições de consentimento no portal, com opções de opt-in e opt-out;
- 6.6.15. O sistema deverá permitir que o titular de dados visualize as datas de concessão e expiração dos consentimentos fornecidos;
- 6.6.16. O sistema deverá permitir ao titular de dados solicitante a exportação, via portal, de respostas e dados encontrados na empresa.

6.7. Gerenciamento de Auditoria

- 6.7.1. O sistema deverá permitir a criação de um procedimento de auditoria;
- 6.7.2. O sistema deverá permitir configurar um identificador para auditoria;
- 6.7.3. O sistema deverá permitir definir o objetivo de cada auditoria;
- 6.7.4. O sistema deverá permitir definir o período de realização da auditoria;
- 6.7.5. O sistema deverá permitir indicar os auditores responsáveis pela auditoria;
- 6.7.6. O sistema deverá permitir a vinculação de normas e controles;
- 6.7.7. O sistema deverá permitir minimamente as seguintes normas: AICPA TSC 2017(SOC 2), ISO/IEC 27005, NIST (CSF) Core v1.1, NIST SP 800-171 rev2, NIST Privacy, ISO/IEC 27017:2015, ISO/IEC 27018:2019, ISO/IEC 29151:2017, ISO 20000-1:2018, OCEG Capability Model v3, Shared Assessments 2021, ISO/IEC;
- 6.7.8. O sistema deverá permitir a adição de anexos na auditoria;
- 6.7.9. O sistema deverá permitir a criação e atribuição de tarefas para outros usuários dentro da auditoria;

- 6.7.10. O sistema deverá permitir que os auditores forneçam pareceres acerca controles e objetivos da auditoria;
- 6.7.11. O sistema deverá manter o registro das alterações realizadas na auditoria.
- 6.7.12. O sistema deverá permitir que o auditor defina o parecer acerca da conformidade ou não de um determinado controle;
- 6.7.13. O sistema deverá possuir um dashboard para visualização das auditorias em andamento e anteriores;
- 6.7.14. O sistema deverá possuir um dashboard com as auditorias concluídas, indicando o seu resultado.

6.8. Mapeamento de Dados Pessoais

- 6.8.1. O sistema deverá permitir a gestão de diferentes pontos de coleta/origem de dados pessoais, tais como: API, Formulário Web, Whatsapp, entre outros meios analógicos ou digitais;
- 6.8.2. O sistema deverá permitir o registro de operações de tratamento de dados pessoais (ROPA), sem limitações;
- 6.8.3. O sistema deve permitir agrupar operações de tratamento (ROPA) para facilitar a organização;
- 6.8.4. O sistema deverá possibilitar o cadastramento de entidades para que seja feita uma análise dos setores da empresa, profissionais ou qualquer outra entidade que venha a processar dados pessoais;
- 6.8.5. O sistema deve permitir vincular uma entidade de tratamento de dados pessoais com um fornecedor previamente cadastrado;
- 6.8.6. O sistema deve permitir vincular um usuário do sistema com uma entidade responsável pelo tratamento de dados;
- 6.8.7. O sistema deve permitir vincular uma entidade com qualquer país para que seja controlado a transferência internacional de dados;
- 6.8.8. O sistema deverá permitir a gestão de ativos de tecnologia, sistemas e demais operações de negócio da organização;
- 6.8.9. O sistema deverá permitir a indicação de prazos de retenção de dados vinculados aos ativos de tecnologia;
- 6.8.10. O sistema deverá possuir integração entre a gestão de ativos e o módulo de descoberta de dados, objetivando a atualização automática dos ativos com base nos dados localizados em varreduras;
- 6.8.11. O sistema deve permitir o cadastro de dados pessoais dentro de uma atividade de tratamento de dados;
- 6.8.12. O sistema deverá permitir vincular os pontos de coleta/origem dos dados pessoais com as operações de tratamento;

- 6.8.13. O sistema deverá permitir o cadastro de atributos adicionais às operações de tratamento com ao menos categoria, questão e resposta;
- 6.8.14. O sistema deverá permitir a criação de campos customizados para o cadastro de ativos e atividades de tratamento de dados pessoais;
- 6.8.15. O sistema deverá permitir a criação e validação do inventário de atividades de tratamento, ativos, fornecedores a partir de requisições de preenchimento de questionários para os responsáveis;
- 6.8.16. O sistema deverá registrar as alterações realizadas no inventário de atividades de tratamento, possibilitando versionamento das operações;
- 6.8.17. Deve permitir a gestão de riscos relacionados a cada atividade de Tratamento e Ativos com no mínimo as seguintes propriedades de controle:
 - 6.8.17.1. Nível do risco;
 - 6.8.17.2. Categoria de risco (reputação, financeiro, operacional, etc.);
 - 6.8.17.3. Ameaça;
 - 6.8.17.4. Vulnerabilidade;
 - 6.8.17.5. Controles e Normas;
 - 6.8.17.6. Informações sobre a ameaça e vulnerabilidades;
 - 6.8.17.7. Plano de tratamento do risco;
 - 6.8.17.8. Datas de criação e prazos;
 - 6.8.17.9. Usuário responsável pela mitigação e tratamento do risco.
- 6.8.18. O administrador deve poder personalizar novas ameaças, vulnerabilidades, controles e categorias.
- 6.8.19. O sistema deve permitir que o administrador crie modelos de riscos prontos e reutilize estes modelos quando for atribuir um novo risco;
- 6.8.20. O sistema deve sugerir automaticamente possíveis riscos no ROPA conforme o preenchimento do mesmo vai acontecendo;
- 6.8.21. Deve permitir cadastrar tipos de dados pessoais vinculados ao ROPA;
- 6.8.22. O sistema deverá permitir a classificação dos dados vinculados ao ROPA, com base no limite de acesso ao dado, tipo de dado, auditoria e forma de gravação do dado;
- 6.8.23. Deve permitir importar tipos de dados pessoais de websites cadastrados no sistema (campos de formulários).
- 6.8.24. Deve permitir informar se um dado pessoal é relacionado a criança ou adolescente;
- 6.8.25. Deve permitir cadastrar transações e fluxos de dados com no mínimo as seguintes propriedades:
 - 6.8.25.1. Direção da transação (saída de dados ou entrada de dados);
 - 6.8.25.2. Entidade de tratamento de dados de origem;

- 6.8.25.3. Entidade de tratamento de dados de destino;
- 6.8.25.4. Quantidade média de dados afetados pela transação;
- 6.8.25.5. Volume de dados transacionados;
- 6.8.25.6. Seguranças empregadas na transação.
- 6.8.26. Deve permitir um trabalho de classificação e mapeamento de tratamento de dados pessoais para cada dado pessoal de cada ROPA registrado;
- 6.8.27. Deve permitir informar para cada tipo de dado pessoal no mínimo as seguintes informações relacionadas com o fluxo de tratamento de dados pessoais:
 - 6.8.27.1. Validação se é um dado que torna um titular de dados identificado ou identificável (um dado que pode potencialmente se relacionar com outros e identificar o titular);
 - 6.8.27.2. Validação se é um dado sensível e um dado obrigatório;
 - 6.8.27.3. Aspectos de criptografia e segurança do dado;
 - 6.8.27.4. Aspectos de auditoria e logs do tratamento do dado.
- 6.8.28. Deve permitir o registro das finalidades de processamento para cada dado pessoal e para cada operação de tratamento;
- 6.8.29. Deve permitir cadastrar categorias de dados pessoais para melhor classificá-los;
- 6.8.30. O controle de finalidades de processamento deve prever todas as hipóteses de tratamento de dados pessoais da LGPD e GDPR;
- 6.8.31. No caso da hipótese de tratamento “Legítimo interesse” deve ser viável realizar um teste de balanceamento de interesses seguindo as boas práticas do mercado;
- 6.8.32. No caso da hipótese de tratamento “Consentimento” deve ser viável realizar um controle adicional para justificar o uso dessa hipótese;
- 6.8.33. Deve possuir ferramentas de controle de transferência internacional de dados para orientar o controlador quanto aos riscos dessa ação;
- 6.8.34. Deve possuir ferramentas de controle quanto à remoção de dados pessoais para orientar o controlador quanto aos riscos dessa ação;
- 6.8.35. Deve ser possível visualizar de modo gráfico o ciclo de vida dos dados pessoais dentro da organização;
- 6.8.36. Devem ser exibidos relatórios e gráficos de controle do mapeamento de dados tais como:
 - 6.8.36.1. Relatório de dados pessoais sendo processados;
 - 6.8.36.2. Relatório com matriz de riscos;
 - 6.8.36.3. Relatório de transferência internacional de dados.

- 6.8.37. Deve possuir um cadastro de regulamentações para uso no mapeamento de dados quanto aos aspectos regulatórios.
- 6.8.38. Deve ser possível criar modelos de classificação de dados pessoais para poder reutilizar um modelo em um novo dado pessoal
- 6.8.39. Deve possuir API REST para integração do sistema com outros sistemas.
- 6.8.40. O Sistema deve gerar automaticamente o DPIA (RIPD) - Relatório de Impacto de Proteção de Dados para uma ou mais atividades de processamento conforme escolha do usuário.
- 6.8.41. O sistema deve permitir a impressão do relatório de impacto gerado.
- 6.8.42. Deve ser possível vincular tarefas relacionadas a uma operação de tratamento de modo que outras pessoas do time possam trabalhar na adequação.
- 6.8.43. O sistema deve ter um relatório de temporalidade de modo a exibir em uma única tela todos os dados pessoais e seu prazo de retenção para o devido controle do prazo de processamento do dado.
- 6.8.44. O sistema deve ter um relatório sintético de bases legais que mostre a quantidade de operações de tratamento, quantidade de dados pessoais e quantidade de dados pessoais sensíveis para cada base legal da LGPD.
- 6.8.45. O sistema deve possuir uma representação visual/gráfica de todo o ciclo de vida dos dados pessoais de uma determinada operação de tratamento evidenciando a coleta, tratamento, distribuição e remoção de dados.
- 6.8.46. O sistema deve permitir a exportação do ROPA em XLS ou XLSX e PDF de um ou vários processos.
- 6.8.47. O sistema deve permitir a importação do ROPA que tenha sido feito em planilha XLS ou XLSX.
- 6.8.48. O sistema deverá possuir um modelo XLS ou XLSX proposto para importação, como planilha padrão para importação.
- 6.8.49. O sistema deverá permitir a conversão de qualquer modelo XLS ou XLSX para o modelo proposto, através de recurso de conversão que permita ao administrador correlacionar as colunas da planilha não-padrão e gere automaticamente a planilha padrão.
- 6.8.50. O sistema deverá permitir a exportação do ROPA em modelo XLS ou XLSX próprio do sistema ou personalizável.
- 6.8.51. Deve ser possível vincular políticas com uma determinada atividade de tratamento.
- 6.8.52. O sistema deverá permitir minimamente as seguintes normas: AICPA TSC 2017 (SOC 2), ISO/IEC 27005, NIST (CSF) Core v1.1, NIST SP 800-171 rev2, NIST Privacy, ISO/IEC 27017:2015, ISO/IEC 27018:2019, ISO/IEC 29151:2017,

ISO 20000-1:2018, OCEG Capability Model v3, Shared Assessments 2021, ISO/IEC21434:2021, NIST- SP800, Secure Controls Framework (SCF) 2021.1, LGPD, ISO/IEC 29100:20

6.9. Gestão de Avaliações e Gestão de Fornecedores

- 6.9.1. O sistema deve permitir a gestão de fornecedores, para que seja feita uma análise de risco de processamento de dados pessoais.
- 6.9.2. O sistema deve permitir vincular um fornecedor com qualquer país, para que seja controlado a ocorrência de transferência internacional de dados.
- 6.9.3. O sistema deve permitir informar os contatos do encarregado pelo tratamento de dados pessoais do fornecedor.
- 6.9.4. O sistema deve possuir uma base de fornecedores comuns de mercado já populada para utilização no sistema.
- 6.9.5. O sistema deve permitir a importação de fornecedores através de planilha, em formato XLS ou XLSX.
- 6.9.6. O sistema deve permitir que avaliações realizadas para aquele fornecedor sejam vinculadas ao seu cadastro.
- 6.9.7. O sistema deverá permitir que as Due Dilligences realizadas com o fornecedor sejam vinculadas ao seu cadastro.
- 6.9.8. O sistema deverá permitir atrelar ao cadastro do fornecedor, os documentos ou endereços web a seguir: Data Processing Agreement (DPA), Política de Privacidade e Canal de Solicitações de Titulares de Dados do fornecedor.
- 6.9.9. O sistema deve permitir o gerenciamento de modelos de diagnósticos de maturidade a serem realizados com interessados.
- 6.9.10. Cada modelo de diagnóstico deve permitir o cadastramento de uma ou várias categorias de questionários que fazem parte da entrevista de diagnóstico.
- 6.9.11. As questões devem ser dinâmicas. O administrador do sistema deve poder criar questões com diversos tipos e formatos com no mínimo: arquivo de upload, texto, checkbox, combo, múltipla escolha, data e "sim ou não"
- 6.9.12. O sistema deve permitir a aplicação de lógica condicional nas questões com perguntas sensíveis ao contexto, dependentes das respostas anteriores.
- 6.9.13. Deve ser possível criar uma instância do modelo e gerar um formulário de entrevista.
- 6.9.14. O sistema deve permitir o envio do formulário de entrevista para usuários internos e usuários externos através de e-mail.

- 6.9.15. O sistema deve permitir o envio de formulário de entrevista para fornecedores, inclusive enviando para todos os fornecedores da base.
- 6.9.16. O sistema deve armazenar todas as respostas coletadas para posterior análise.
- 6.9.17. O sistema deve permitir o arquivamento de respostas já concedidas.
- 6.9.18. O sistema deve possibilitar a geração de formulários dinâmicos sem limitação de perguntas para que áreas da empresa possam responder questões a respeito do tratamento de dados pessoais.
- 6.9.19. O sistema deve possibilitar a geração de formulários prontos para atividades comuns no fluxo de tratamento de dados pessoais e procedimentos de segurança, sendo no mínimo formulários prontos para:
 - 6.9.19.1. Relatório de impacto para processamento de dados pessoais (DPIA);
 - 6.9.19.2. Relatório de impacto para uso do legítimo interesse (LIA);
 - 6.9.19.3. ISO 27.001.
- 6.9.20. O sistema deve permitir a configuração de normas e controles de conformidade.
- 6.9.21. Deve exibir dashboards e relatórios de maturidade para cada dimensão e para cada critério de conformidade.
- 6.9.22. Deve permitir vincular um diagnóstico com um fornecedor para poder avaliar a maturidade dele.
- 6.9.23. O sistema deve permitir configurar níveis de maturidade conforme metodologias conhecidas de mercado como por exemplo CMMI.
- 6.9.24. O sistema deve permitir a criação de medidas de conformidade sugeridas para que a empresa possa saber quais são as medidas recomendadas para cada diagnóstico realizado.
- 6.9.25. O sistema deve permitir a importação de planilhas com questões já existentes.
- 6.9.26. O sistema deve oferecer um controle de planos de ação com atividades utilizando a metodologia Kanban.
- 6.9.27. O sistema deve poder relacionar atividades do plano de ação com responsáveis, prazo de conclusão e percentual de andamento.
- 6.9.28. O sistema deverá permitir vincular riscos de negócio com um determinado fornecedor.
- 6.9.29. O sistema deverá permitir exibir relatórios e dashboard com matriz de risco para fornecedores.
- 6.9.30. O sistema deve permitir que o operador do sistema registre comentários internos sobre as respostas feitas pelo fornecedor.

- 6.9.31. Deve ser possível que o administrador gerencie campos customizáveis do cadastro do fornecedor de modo que novos campos do cadastro possam ser criados e gerenciados sem a necessidade de programação.
- 6.9.32. Deve existir uma gestão de arquivos com possibilidade de controle de pastas e upload de arquivos para o sistema.
- 6.9.33. Todos os arquivos enviados para o sistema devem aparecer na gestão centralizada de arquivos.
- 6.9.34. Deve ser possível renomear, mover e baixar arquivos através da gestão centralizada de arquivos.
- 6.9.35. Deve ser possível exportar os fornecedores em planilha.
- 6.9.36. O administrador deve poder vincular tarefas relacionadas ao fornecedor com seus responsáveis e controle de prazos.
- 6.9.37. O administrador deve poder anexar arquivos e registrar contratos do fornecedor com no mínimo os seguintes campos: nome do contrato, data da assinatura, valor e data de vencimento do contrato.
- 6.9.38. O conteúdo dos e-mails que serão enviados pela plataforma deve poder ser customizados pelo administrador na própria plataforma.
- 6.9.39. Deve ser possível versionar (criar e gerenciar versões) de modelos de diagnóstico de modo que o administrador possa controlar e ver o histórico de versões dos modelos gerenciados.
- 6.9.40. O sistema deverá possuir chat em tempo real para troca de mensagens entre o avaliador e respondente do questionário, para facilitar as interações durante o preenchimento da avaliação.
- 6.9.41. O sistema deve permitir a inclusão ou remoção de atributos do fornecedor, sem a necessidade de desenvolvimento, bastando clicar para gerar a ação de adição/exclusão de novos campos.

6.10. **Due Diligence**

- 6.10.1. O sistema deverá permitir criar processos de diligência prévia.
- 6.10.2. O sistema deverá permitir a atribuição de um protocolo para cada diligência.
- 6.10.3. O sistema deverá permitir a indicação do fornecedor que receberá a diligência prévia.
- 6.10.4. O sistema deverá permitir a atribuição de um solicitante relacionado à diligência prévia.
- 6.10.5. O sistema deverá permitir a atribuição de uma área responsável pela diligência prévia.

6.10.6. O sistema deverá permitir atrelar mais de uma avaliação ao processo da Due Dilligence.

6.10.7. O sistema deverá permitir anexar evidências relacionadas à Due Dilligence.

6.10.8. O sistema deverá permitir relacionar riscos identificados no processo de Due Dilligence.

6.10.9. O sistema deverá permitir o cadastro de pareceres da Due Dilligence.

6.10.10. O sistema deverá apresentar o resultado de cada avaliação da Due Dilligence.

6.10.11. O sistema deverá permitir, na identificação do parecer, qual o resultado da diligência prévia realizada com o fornecedor.

6.11. Gestão de Riscos

6.11.1. O sistema deverá permitir integrações com soluções de descoberta de dados.

6.11.2. O sistema deverá permitir integração com provedores de identidade (IdP).

6.11.3. O sistema deverá permitir integração com soluções CMDB para integração de riscos em ativos de informação.

6.11.4. O sistema deverá permitir integração com soluções de BI (exemplo: Tableau ou Power BI).

6.11.5. O sistema deverá possuir Frameworks de APIs para integrações customizadas para coleta de riscos de outras fontes de dados

6.11.6. O sistema deverá permitir a importação de riscos em massa.

6.11.7. O sistema deverá ter a capacidade de gerar gráficos tipo “mapas de calor” para visualização e reporte de riscos.

6.11.8. O sistema deverá possuir funcionalidade de multi-aprovador para os fluxos de trabalho de tratamento dos riscos.

6.11.9. O sistema deverá permitir realizar uma avaliação quantitativa de risco, suportando no mínimo o processo de Análise de Fator de Risco da Informação (sigla FAIR, em inglês).

- 6.11.10. O sistema deverá permitir a gestão de uma matriz de risco possibilitando a sua personalização, com no mínimo os seguintes níveis: 3x3, 4x4 e 5x5.
- 6.11.11. O sistema deverá permitir parametrizar e personalizar os itens da matriz, renomeando os indicadores de impacto e probabilidade.
- 6.11.12. O sistema deverá gerar um score a partir da ligação entre impacto e probabilidade.
- 6.11.13. O sistema deverá permitir minimamente as seguintes normas: AICPA TSC 2017 (SOC 2), ISO/IEC 27005, NIST (CSF) Core v1.1, NIST SP 800-171 rev2, NIST Privacy, ISO/IEC 27017:2015, ISO/IEC 27018:2019, ISO/IEC 29151:2017, ISO 20000-1:2018, OCEG Capability Model v3, Shared Assessments 2021, ISO/IEC21434:2021, NIST- SP800, Secure Controls Framework (SCF) 2021.1, LGPD, ISO/IEC 29100:2011, ISO/IEC 27701:2013
- 6.11.14. O sistema deverá possuir um catálogo de ameaças, vulnerabilidades e controles conforme a norma ISO/IEC 27001:2013, HIPPA, GDPR, CIS Controls V8, COSO e ISO22301.
- 6.11.15. O sistema deverá permitir a importação de ameaças, vulnerabilidade e controles das normas disponíveis no sistema.
- 6.11.16. O sistema deverá permitir a criação de modelos de riscos no sistema com no mínimo os seguintes atributos:
- 6.11.16.1. Título do risco;
 - 6.11.16.2. Impacto;
 - 6.11.16.3. Probabilidade;
 - 6.11.16.4. Nível do Risco;
 - 6.11.16.5. Categoria do Risco;
 - 6.11.16.6. Ameaça;
 - 6.11.16.7. Vulnerabilidade;
 - 6.11.16.8. Controles;

6.11.16.9. Descrição de Riscos;

6.11.16.10. Plano de Contingência;

6.11.16.11. Ações Mitigatória;

6.11.17. Deve ser possível que o administrador gerencie campos customizáveis do cadastro do risco de modo que novos campos do cadastro possam ser criados e gerenciados sem a necessidade de programação.

6.11.18. O sistema deverá permitir importar os modelos de riscos cadastrados nas soluções de mapeamento de dados, gestão de incidentes, gestão e avaliação de fornecedores e outros locais que possam ser aplicadas.

6.11.19. O sistema deverá permitir a configuração de regras para a geração de tarefas automáticas conforme criticidade do risco.

6.11.20. O sistema deverá registrar o histórico de tratamento do risco, com a visualização do risco residual resultante das ações estabelecidas para controle.

6.12. Gestão de Incidentes

6.12.1. O sistema deverá prover de uma biblioteca de tipos de incidente.

6.12.2. O sistema deverá permitir customizar e inserir e excluir tipos de incidentes da biblioteca.

6.12.3. O sistema deverá permitir o registro de novos incidentes.

6.12.4. O sistema deverá permitir identificar a forma pela qual o incidente foi reportado.

6.12.5. O sistema deverá permitir definir um responsável por um incidente.

6.12.6. O sistema deverá possuir fases de gerenciamento de um incidente, permitindo o acompanhamento e avanço do incidente.

6.12.7. O sistema deverá permitir gerar análises de um incidente.

6.12.8. O sistema deverá apresentar uma linha do tempo de andamento do incidente.

6.12.9. O sistema deverá permitir relacionar riscos à um incidente.

6.12.10. O sistema deverá permitir inserir anexos nos registros de incidentes.

- 6.12.11. O sistema deverá permitir realizar o relacionamento entre o incidente e outras funcionalidades e itens do sistema, tais como: Atividades de Tratamento de Dados, Usuários, Ativos e outros.
 - 6.12.12. O sistema deverá permitir o cadastro do número de titulares impactados pelo incidente, dados pessoais e o impacto do incidente.
 - 6.12.13. O sistema deverá permitir a vinculação de uma tarefa a um incidente, indicando o responsável pela tarefa.
 - 6.12.14. O sistema deverá permitir elencar as informações vinculadas ao incidente, bem como a quantidade de titulares envolvidos, localização dos titulares e tipos de dados afetados.
 - 6.12.15. O sistema deverá permitir a comunicação de um incidente para o titular de dados e/ou para a ANPD.
 - 6.12.16. O sistema deverá possuir o template de comunicação de incidentes disponibilizado pela ANPD (Autoridade Nacional de Proteção de Dados).
 - 6.12.17. O sistema deverá permitir enviar o template de comunicação por e-mail, ou disponibilizar mecanismos de download do arquivo para compartilhamento em DOC ou DOCX e PDF.
 - 6.12.18. Deve ser possível que o administrador gerencie campos customizáveis do cadastro do incidente de modo que novos campos do cadastro possam ser criados e gerenciados sem a necessidade de programação.
 - 6.12.19. O sistema deverá permitir a criação de uma base de conhecimento.
 - 6.12.20. O sistema deverá permitir a atribuição de problemas e descrição de problemas.
- 6.13. Descoberta de Dados**
- 6.13.1. O sistema deverá possuir integração nativa para automação dos pedidos dos titulares a partir da busca de dados pessoais encontrados.
 - 6.13.2. O sistema deverá possuir um relatório que indique o volume de dados e quais as bases que possuem dados pessoais, permitindo ainda a exportação em XLS ou XLSX.
 - 6.13.3. O sistema deve permitir o monitoramento de no mínimo os seguintes ambientes:
 - 6.13.3.1. Arquivos (via upload manual no sistema);
 - 6.13.3.2. PostgreSQL 9.2 e superiores;
 - 6.13.3.3. Oracle 9, 10, 11 e superiores;
 - 6.13.3.4. MySQL e MariaDB;
 - 6.13.3.5. IBM DB/2;

- 6.13.3.6. IBM DB/2 - AS/400;
- 6.13.3.7. SAP HANA;
- 6.13.3.8. Databricks (Datalake)
- 6.13.3.9. MongoDB versões 4.4 e inferiores até 3.7;
- 6.13.3.10. Ambientes de FTP/FTPS;
- 6.13.3.11. Ambientes através de SSH (SFTP);
- 6.13.3.12. Sistema de arquivos (storage/NFS);
- 6.13.3.13. Amazon AWS
- 6.13.3.14. Azure Blobs
- 6.13.3.15. Alfresco
- 6.13.3.16. Microsoft 365 (OneDrive, Exchange e SharePoint);
- 6.13.3.17. Google Drive;
- 6.13.3.18. Computadores de uma rede através do download de agentes locais para os sistemas operacionais Windows, Linux e Mac.
- 6.13.4. O sistema deverá permitir o agendamento de execução do fluxo de descoberta de dados.
- 6.13.5. O sistema deverá permitir, por livre escolha da contratante, que a instalação do módulo seja feita em infraestrutura de propriedade da contratante, sem prejuízo dos recursos oferecidos e sem mudança em preço.
- 6.13.6. O sistema deverá permitir a customização de busca de dados pessoais a partir do uso de expressões regulares ou inteligência artificial.
- 6.13.7. O sistema deverá possuir controle de tipos de dados (categoria) e severidade de cada tipo, podendo no mínimo ativar e desativar tipos de dados pessoais e suas expressões regulares.
- 6.13.8. O sistema deverá permitir percorrer todos os resultados da busca e saber onde estão os dados pessoais.
- 6.13.9. O sistema deverá permitir integração com o módulo de atendimento de pedidos para acelerar a automação do pedido.
- 6.13.10. O sistema deve possuir conexão nativa com o módulo de data mapping (mapeamento de dados) de modo que uma varredura já faça o trabalho inicial de mapeamento de dados com as operações de tratamento encontradas e seus dados pessoais.
- 6.13.11. Deve permitir a remoção de dados pessoais indexados no sistema de descoberta de dados e inseri-los em uma 'blacklist' de dados para não serem novamente indexados.
- 6.13.12. O sistema deve permitir limpar os resultados de uma varredura anterior quando for executar uma nova varredura.

- 6.13.13. O sistema deve ter componentes para Windows, Linux e Mac para que possa ser feito uma varredura de arquivos no computador em busca de dados pessoais armazenados.
- 6.13.14. O sistema deverá permitir agrupar os dados de titulares automaticamente com base em um banco de dados estruturado.
- 6.13.15. O sistema deverá permitir realizar a busca de titulares agrupados através da chave de identificação.
- 6.13.16. O sistema deverá gerar relatório em PDF com a quantidade de dados encontrados nas varreduras e sua classificação.

6.14. Anonimização de Dados Pessoais

- 6.14.1. O sistema deve realizar a identificação e classificação de dados pessoais dentro de um documento e exportá-lo com estes dados anonimizados;
- 6.14.2. O sistema deve possuir uma tela para buscar o arquivo no computador do usuário e possibilidade arrastar e soltar o arquivo (drag and drop) para upload.
- 6.14.3. O sistema deve possuir tela de consulta contendo:
 - 6.14.3.1. Histórico dos arquivos que foram submetidos a verificação e anonimização.
 - 6.14.3.2. Nome do arquivo
 - 6.14.3.3. Tamanho do arquivo
 - 6.14.3.4. Situação do processamento
 - 6.14.3.5. Data de inserção do arquivo para análise
 - 6.14.3.6. Data da última revisão do arquivos
 - 6.14.3.7. Opção para realizar uma revisão no arquivo referente aos dados classificados para anonimização
 - 6.14.3.8. Opção para Imprimir/exportar o arquivo revisado com os dados anonimizados
 - 6.14.3.9. Opção para exclusão do arquivo/análise de dados
- 6.14.4. O sistema deve possuir no mínimo os campos de busca e filtros abaixo listados:
 - 6.14.4.1. Campo para buscar arquivos pelo nome
 - 6.14.4.2. Filtro para buscar de um determinado formato de arquivo
 - 6.14.4.3. Filtro para buscar arquivos em um determinado status
- 6.14.5. Deve possuir a classificação mínima de arquivos:
 - 6.14.5.1. Processando.
 - 6.14.5.2. Aguardando Revisão.
 - 6.14.5.3. Revisado.

- 6.14.6. O sistema deve exibir o documento processado, com os dados sensíveis identificados, grifados e devidamente classificados.
- 6.14.7. O sistema deve possibilitar a marcação de um dado a ser anonimizado.
- 6.14.8. O sistema deve possibilitar a classificação de dados marcado para anonimização.
- 6.14.9. O sistema deve identificar automaticamente o dado marcado.
- 6.14.10. O sistema deve possuir a tabela exibindo, no mínimo, os dados sensíveis encontrados ou marcados pelo operador e a classificação do dado.
- 6.14.11. O sistema deve possuir biblioteca nativa de dados pessoais para classificação com no mínimo, mas não limitado à, CPF, Nome, Endereço, Cidade, CEP, Telefone, Cartão de Crédito, PIS.
- 6.14.12. O sistema deve possibilitar o cadastro de novas expressões e regras para reconhecimento de dados sensíveis;
- 6.14.13. O sistema deve ser possível gerar/exportar este em PDF ou JPG, com os dados anonimizados.
- 6.14.14. O sistema deve guardar o documento original, com os dados classificados para eventual consulta.

6.15. Gerenciamento de ESG

- 6.15.1. O sistema deverá permitir cadastrar os projetos de ESG da organização.
- 6.15.2. O sistema deverá permitir o cadastro de iniciativas vinculados aos projetos de ESG da organização.
- 6.15.3. O sistema deverá permitir o cadastro de iniciativas baseadas em padrões e frameworks globais de ESG, como SASB, GRI e WEF.
- 6.15.4. O sistema deverá permitir atribuir a uma iniciativa uma das categorias de ESG: Ambiental, Social ou Governança.
- 6.15.5. O sistema deverá permitir a atribuição de um prazo para cada iniciativa.
- 6.15.6. O sistema deverá permitir a atribuição de áreas e usuários responsáveis por cada iniciativa.
- 6.15.7. O sistema deverá permitir a atribuição de tarefas aos usuários para cada iniciativa prevista
- 6.15.8. O sistema deverá considerar a conclusão do objetivo a partir do avanço das tarefas relacionadas as iniciativas
- 6.15.9. O sistema deverá permitir a inserção de anexos em cada objetivo.
- 6.15.10. O sistema deverá permitir a inserção de observações adicionais a iniciativa.
- 6.15.11. O sistema deverá possuir um dashboard que exiba todas as tarefas de ESG.

- 6.15.12. O sistema deverá possuir dashboards e gráficos para acompanhamento do ESG na organização, contendo indicadores dos avanços.
 - 6.15.13. O sistema deverá disponibilizar a geração de um selo de empresa em processo de adequação à ESG para publicação em portais e websites.
 - 6.15.14. O sistema deverá disponibilizar perfis de usuários para o cadastro de interessados em cada projeto de ESG.
 - 6.15.15. O sistema deverá permitir o cadastro de usuários vinculados a três tipos de interessados: patrocinadores, propositores e fornecedores.
 - 6.15.16. O sistema deverá permitir elencar os interessados de cada tipo de projeto de ESG, possibilitando sua classificação por tipo: patrocinador, propositor ou fornecedor.
 - 6.15.17. O sistema deverá possuir base de informações alimentada com ODS (Objetivo de Desenvolvimento Sustentável), possibilitando edição dos conteúdos e criação de objetivos adicionais.
 - 6.15.18. O sistema deverá permitir a vinculação de ODS (Objetivo de Desenvolvimento Sustentável) com as iniciativas propostas.
 - 6.15.19. O sistema deverá permitir o cadastro de métricas vinculadas as iniciativas.
 - 6.15.20. O sistema deverá permitir a criação de métricas e sua vinculação com normas e controles.
 - 6.15.21. O sistema deverá permitir a vinculação de métricas com uma das categorias de ESG: Ambiental, Social ou Governança.
 - 6.15.22. O sistema deverá permitir a classificação da métrica por tipo: texto, percentual ou número.
 - 6.15.23. O sistema deverá permitir a definição de meta esperada vinculada a métrica proposta e o seu acompanhamento a partir de lançamentos periódicos para a visualização do status atual x meta esperada
 - 6.15.24. O sistema deverá permitir a definição de prazo para a conclusão da métrica vinculada a iniciativa.
 - 6.15.25. O sistema deverá disponibilizar dashboards para o acompanhamento de métricas, permitindo aplicar filtros por projeto ou visualizar de forma geral as métricas de todos os projetos.
- 6.16. **Workflow**
- 6.16.1. Deve existir um módulo de workflow para criação de fluxos customizáveis a partir de ações e eventos que ocorram no sistema, com no mínimo os

seguintes eventos: Criações ou Alterações em políticas, ativos, titulares, atividades de tratamento, incidentes e fornecedores, consentimentos

6.16.2. O sistema deve ter a capacidade de criação de workflows customizados, através de módulo nativo e integrado da própria ferramenta é compatível com todos os demais módulos ofertados.

6.16.3. O sistema deve ter a capacidade de criar workflows de forma visual, com gatilhos e ações interligáveis suportando lógica condicional entre eles.

6.16.4. A solução de workflow deve permitir iniciar ações automaticamente quando:

- 6.16.4.1. Requisições DSAR são criadas, alteradas e fechadas;
- 6.16.4.2. Consentimentos são registrados, aceitos e revogados;
- 6.16.4.3. Dados são detectados pelo Data Discovery;
- 6.16.4.4. Objetos catalogados no Data Mapping são criados e alterados;
- 6.16.4.5. Incidentes são registrados;
- 6.16.4.6. Questionários são recebidos e dependendo do risco associado;
- 6.16.4.7. Determinado dia/hora, periodicidade e intervalo de tempo;
- 6.16.4.8. Acionamento externo por API;
- 6.16.4.9. Fornecedores são criados ou modificados no sistema;
- 6.16.4.10. Contratos de fornecedores são registrados ou modificados no sistema;
- 6.16.4.11. O sistema deve permitir criação de múltiplos fluxos de automação independentes.

6.16.5. Deve permitir que um fluxo acione outro fluxo da ferramenta, para reaproveitamento e cascadeamento de ações.

6.16.6. O sistema deve oferecer diversas ações de workflow, incluindo:

- 6.16.6.1. Criar tarefas e subtarefas nas requisições de titular (DSAR);
- 6.16.6.2. Alterar proprietários de tarefas e subtarefas das requisições de titular;
- 6.16.6.3. Anexar arquivos às requisições de titular;
- 6.16.6.4. Criar e alterar itens do catálogo de Data Mapping, incluindo Ativos de TI e Processos;
- 6.16.6.5. Iniciar avaliações/questionários;
- 6.16.6.6. Gerenciar fornecedores cadastrados na ferramenta;
- 6.16.6.7. Criar incidentes no módulo de gestão de incidentes;
- 6.16.6.8. Executar queries, inserts e updates nos bancos de dados do Contratante;
- 6.16.6.9. Ler e extrair conteúdo de arquivos no formato PDF;
- 6.16.6.10. Consumir APIs externas.

6.17. Gráficos e Painéis

- 6.17.1. O sistema deverá permitir a consulta de informações que estão armazenadas nos demais módulos, possibilitando visualização para a geração de indicadores e gráficos personalizados.
- 6.17.2. O sistema deverá possuir recurso para a criação e personalização de gráficos e painéis, possibilitando a apresentação de dashboards vinculados às seguintes informações constantes no sistema:
 - 6.17.2.1. Atividades de Tratamento
 - 6.17.2.2. Ativos de Tecnologia
 - 6.17.2.3. Riscos
 - 6.17.2.4. Avaliações
 - 6.17.2.5. Fornecedores
- 6.17.3. O sistema deverá permitir o cruzamento de informações de fontes distintas para a geração de gráficos personalizados.
- 6.17.4. O sistema deverá automaticamente atualizar os gráficos e painéis criados quando ocorrerem atualizações e alterações nas informações constantes nas fontes do sistema.
- 6.17.5. O sistema deverá permitir a criação de painéis contendo os gráficos personalizados para apresentações e demonstrações de resultados obtidos no programa de privacidade da empresa.
- 6.17.6. O sistema deverá permitir a criação de coleções de painéis, organizando as estruturas conforme a necessidade de cada projeto (por área, usuário ou assunto).

6.18. Governança em IA

- 6.18.1. O sistema deverá permitir cadastrar os projetos que utilizam IA da organização.
- 6.18.2. O sistema deve ter a capacidade de vincular as seguintes informações aos projetos:
 - 6.18.2.1. Controles
 - 6.18.2.2. Atividades de Tratamento
 - 6.18.2.3. Planos de ação
 - 6.18.2.4. Fornecedores
 - 6.18.2.5. Riscos
 - 6.18.2.6. Avaliações
 - 6.18.2.7. Arquivos (via upload manual no sistema);

- 6.18.3. O sistema deverá permitir o cadastro de iniciativas vinculados aos projetos de IA da organização.
- 6.18.4. O sistema deverá permitir a atribuição de um prazo para cada projeto.
- 6.18.5. O sistema deverá permitir a atribuição de usuários responsáveis por cada projeto.
- 6.18.6. O sistema deverá permitir a atribuição do status de cada projeto.
- 6.18.7. O sistema deverá permitir cadastrar um ou mais modelo em cada projeto.
- 6.18.8. O sistema deverá permitir a criação de um dataset.
- 6.18.9. O sistema deverá possuir recurso para a criação e personalização para vincular as seguintes informações constantes no sistema:
 - 6.18.9.1. Tipos de IA
 - 6.18.9.2. Níveis de autonomia
 - 6.18.9.3. Frameworks
 - 6.18.9.4. Fornecedores de IA
 - 6.18.9.5. Linguagem de programação
 - 6.18.9.6. Tipo de aprendizado do modelo de IA
 - 6.18.9.7. Tipo de tarefas que a IA está executando
 - 6.18.9.8. Licença de software
 - 6.18.9.9. Tipos de conjunto de dados
 - 6.18.9.10. Função de conjunto de dados
- 6.18.10. O sistema deverá apresentar dashboards para gerenciamento dos projetos.
- 6.18.11. O sistema deverá apresentar uma biblioteca pronta que preenche as informações de forma automática
- 6.18.12. O sistema deverá apresentar modelos de IA

7. Proteção das Aplicações

- 7.1.1. A CONTRATADA deverá fazer a entrega de um conjunto de soluções com objetivo de prover uma plataforma de segurança e performance para as aplicações da CONTRATANTE contemplando, minimamente:
 - 7.1.1.1. WAF;
 - 7.1.1.2. CDN (para aprimoramento das estratégias de defesa distribuída de aplicações);
 - 7.1.1.3. Proteção de API;
 - 7.1.1.4. Anti-BOT.

- 7.1.2. A solução deverá combater ameaças como injeção SQL e XSS através de robustos mecanismos de segurança que identificam e bloqueiam acessos não autorizados.
 - 7.1.3. Adicionalmente, deve oferecer proteção das aplicações, incluindo o bloqueio geográfico e listas de IPs, identificando e diferenciando entre requisições legítimas e automatizadas, empregando análises detalhadas de assinaturas, comportamentos para reforçar a proteção contra ameaças mecânicas.
- 7.2. Solução de rede dinâmica de distribuição e aceleração de conteúdo – CDN;
- 7.2.1. Considerando a abrangência territorial do CONTRATANTE, a solução deverá ser descentralizada e sem ponto único de falha, para entrega de conteúdo estático ou dinâmico de forma criptografada (TLS/SSL) em todos os pontos da rede;
 - 7.2.2. No caso de dados pessoais, deverão ser observadas as orientações previstas na Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais - LGPD, e demais legislações sobre o assunto;
 - 7.2.3. Para atendimento as necessidades da CONTRATANTE a solução de rede dinâmica de distribuição e aceleração de conteúdo – CDN, deverá:
 - 7.2.3.1. Possuir um algoritmo de roteamento dinâmico que caso algum datacenter fique indisponível o tráfego seja redirecionado sem afetar o desempenho dos serviços;
 - 7.2.3.2. Possuir um ambiente de testes de configurações, onde seja possível aplicar todas as funcionalidades de distribuição de conteúdo e segurança, a fim de validar todas as configurações do website ou aplicação antes de publicar em produção;
 - 7.2.3.3. Possuir endereços IPs ou hostnames específicos que devem ser usados nos testes, possibilitando que sejam testadas todas as funcionalidades dos websites ou aplicações protegidas, apenas realizando o direcionamento do navegador do cliente para este ambiente;
 - 7.2.3.4. Possui melhores condições de entrega, utilizando métodos para o redirecionamento do usuário, desde servidores de aplicações, até o

redirecionamento no nível de Servidor de Domínio de Nomes (Domain Name Servers, DNS);

7.2.3.5. Fornecer o serviço de balanceamento de carga entre datacenters para entrega de aplicações híbridas ou multinuvem;

7.2.3.6. O balanceamento de carga deve ser capaz de identificar falhas de camada 3 e camada 7 do modelo OSI mantendo a disponibilidade do sistema e redirecionando as solicitações quando uma origem não está mais operacional para continuar transmissão e entrega do conteúdo;

7.2.3.6.1. O PROVEDOR deve realizar o balanceamento de tráfego, assim como suportar a configuração de uma origem principal e outra backup (standby), que só será utilizada em caso de falha da primeira;

7.2.3.6.2. O balanceamento deve possuir controle granular para rotear o tráfego com base em atributos HTTP;

7.2.3.6.3. O balanceamento deve possuir afinidade de sessão, sendo capaz de vincular os usuários a origem selecionada durante a operação normal de tempo de execução, oferecendo suporte a experiências ininterruptas;

7.2.3.6.4. Tratar os erros e exceções na comunicação a nível de rede ou de aplicação com as origens, buscando conexão nas demais origens em caso de timeout ou em caso da resposta HTTP com erro 404 (Not Found);

7.2.3.6.5. Deverá ser configurada para habilitar todos os seus servidores a reconhecer o site de origem, seus conteúdos estáticos e dinâmicos;

7.2.3.6.6. A contratada deverá prover aceleração e proteção, com capacidade de expansão para a quantidade de URLs informada no documento “Infraestrutura de Tecnologia da Informação do MPRJ”, pertencentes ao CONTRATANTE;

7.2.3.6.7. Prover disponibilidade dos sites e tempo de carregamento das páginas inferior ao de carregamento sem o uso da CDN,

independentemente da quantidade de usuários e dados acessados simultaneamente;

- 7.2.3.6.8. Garantir o desempenho dos acessos por meio da determinação, em tempo real, de qual servidor de rede dinâmica possui melhores condições de entrega para cada usuário do conteúdo da aplicação acessada;

Propagar as mudanças nas listas de liberação e bloqueio em até 15 minutos, permitindo assim a resposta a incidentes de segurança na infraestrutura do CONTRATANTE;

- 7.2.3.6.9. Realizar a expiração de conteúdo (purge) por URL, com suporte a wildcard ou similar, em toda a rede, em um prazo máximo de 05 (cinco) minutos;

- 7.2.3.6.10. Possuir caminhos redundantes de acesso e distribuição de conteúdo, a fim de garantir o acesso a seus serviços bem como ao serviço de origem;

- 7.2.3.6.11. Acelerar e distribuir indistintamente quaisquer aplicações baseadas em Protocolo de Transferência de Hipertexto (Hypertext Transfer Protocol, HTTP e HTTPS), balanceando entre seus POPs, a carga das páginas de modo a garantir melhor performance;

- 7.2.3.6.12. Para a aceleração e distribuição de aplicações HTTPS, o proponente deverá utilizar um padrão de encriptação seguro, conforme padrão internacional reconhecidamente aceito, que possa ser implementado com chaves de encriptação geradas e armazenadas pelo CONTRATANTE;

- 7.2.3.6.13. O compartilhamento de chaves entre a CONTRATADA e a CONTRATANTE deve ser feito de acordo com processos e tecnologias de gerenciamento de chaves que sigam um padrão internacional reconhecidamente aceito e que não exponham as chaves em texto-claro;

- 7.2.3.6.13.1. Após a instalação dos certificados, deverão ser realizados testes utilizando a ferramenta Qualys SSL Labs <https://www.ssllabs.com/ssltest>, na qual deverá ser obtida a qualificação "A" para todas as URLs;

- 7.2.3.6.13.2. Os Certificados Digitais A1 SSL/TLS para Servidor Web poderão ser individualizados para cada URL implantada ou do tipo SAN (Subject Alternative Name), onde um único certificado pode conter várias URL conforme definição da CONTRATANTE.
- 7.2.3.6.13.3. A CONTRATANTE poderá definir a Autoridade Certificadora a ser utilizada, desde que compatíveis com as Autoridades Certificadoras suportadas pela solução;
- 7.2.3.6.13.4. A CONTRATANTE controlará o prazo de expiração dos certificados fornecidos à CONTRATADA;
- 7.2.3.6.13.5. A CONTRATADA deverá possuir a capacidade de configuração das cifras criptográficas e da versão de TLS 1.2 ou superior utilizadas pelo CONTRATANTE, suportando, no mínimo, as cifras a seguir:
- 7.2.3.6.13.5.1. `tls_ecdhe_ecdsa_with_aes_128_gcm_sha256`;
- 7.2.3.6.13.5.2. `tls_ecdhe_ecdsa_with_aes_256_gcm_sha384`;
- 7.2.3.6.13.5.3. `tls_ecdhe_rsa_with_aes_128_gcm_sha256`;
- 7.2.3.6.13.5.4. `tls_ecdhe_rsa_with_aes_256_gcm_sha384`.
- 7.2.3.6.13.6. A configuração das cifras suportadas em cada URL será definida pela CONTRATANTE;
- 7.2.3.6.13.7. Quando da necessidade de validação do cliente por meio de certificado digital – numa conexão mTLS, por exemplo – a CONTRATADA deverá fazer todas as validações previstas no método `X509_verify_cert`, existente na estrutura do Openssl;
- 7.2.3.6.13.8. O certificado de cliente só deve ser aceito se o método `X509_verify_cert` retornar “OK” para todas as validações previstas;

- 7.2.3.6.13.9. As chaves privadas dos certificados utilizados nas URL da CONTRATANTE devem ser armazenadas e processadas de forma segura;
- 7.2.3.6.13.10. A CONTRATADA deverá instalar todos os certificados com a cadeia de certificação completa;
- 7.2.3.6.13.11. A CONTRATADA deverá permitir a desativação dos parâmetros TLS Renegotiation e TLS Resumption, conforme solicitado pela CONTRATANTE;
- 7.2.3.6.14. Ser sensível à existência de letras maiúsculas e minúsculas para armazenamento de objetos em cache;
- 7.2.3.6.15. Deverá permitir o serviço de cache dinâmico;
- 7.2.3.6.16. A CDN deverá possuir os seguintes recursos para a gestão de cache:
 - 7.2.3.6.16.1. Não armazenagem;
 - 7.2.3.6.16.2. Bypass cache.
- 7.2.3.6.17. Deverá responder a diferentes métodos HTTP, considerando, pelo menos: GET, HEAD, POST, PUT, PATCH, DELETE e OPTIONS;
- 7.2.3.6.18. Deverá restringir para determinado site, métodos HTTP específicos, bloqueando outros métodos que não forem habilitados;
- 7.2.3.6.19. Deverá modificar, adicionar ou remover informações do cabeçalho HTTP durante a comunicação com os datacenters de origem;
- 7.2.3.6.20. A CDN deverá permitir a implementação de redirecionamento HTTP otimizando a comunicação com o datacenter de origem;
- 7.2.3.6.21. Fornecer o serviço de geolocalização a nível de país, que permitirá o gerenciamento de listas de permissão e negação de acessos;

- 7.2.3.6.22. A CDN deverá realizar a entrega de qualquer formato e tipo de conteúdo para no mínimo os protocolos HTTP 1.1 e 2;
- 7.2.3.6.23. Realizar a entrega do conteúdo em cache, mesmo que já expirado, caso a origem do Datacenter esteja inacessível;
- 7.2.3.6.24. Prover aceleração por meio da compressão de dados desde que suportado pelo navegador ou dispositivo utilizado pelo usuário;
- 7.2.3.6.25. Detectar as características dos dispositivos por meio das informações de navegador de Internet;
- 7.2.3.6.26. Permitir a obtenção de objetos cacheados a partir de outros servidores da rede, evitando assim conexão com o datacenter de origem;
- 7.2.3.6.27. Permitir a utilização de métodos de validação de usuário;
- 7.2.3.6.28. Deverá disponibilizar forma de consulta e alteração das configurações de cache e regras de segurança com reflexo em todos os servidores de borda da plataforma;
- 7.2.3.6.29. Verificar que a requisição está sendo feita por um site autorizado a ter acesso ao conteúdo armazenado;
- 7.2.3.6.30. Deverá prover a infraestrutura necessária para a adequada prestação dos serviços indicados anteriormente, de forma escalável, automaticamente e em tempo real, independentemente da quantidade de acessos simultâneos;
- 7.2.3.6.31. Por meio do painel de monitoramento deverá subdividir e permitir a consulta de dados referente a tráfego, requisições HTTP e HTTPS, hits, exclusivamente para cada site WEB configurado, permitindo a geração de relatórios específicos para cada site presente na CDN para até 30 dias de histórico.
 - 7.2.3.6.31.1. Para dados além de 30 dias, deverá ser fornecido “logs” para consultas.

- 7.2.3.6.32. O painel de monitoramento deverá possuir opções para geração de filtros, possibilitando a criação de relatórios customizados por site e data;
- 7.2.3.6.33. O painel de monitoramento deverá permitir acompanhar, o quantitativo de requisições realizadas para cada site WEB na CDN;
- 7.2.3.6.34. O painel de monitoramento deverá disponibilizar informações como: país, endereço IP, descrição da ameaça/regra que está sendo processada, método HTTP utilizado, data e hora da ocorrência da CDN;
- 7.2.3.6.35. Conter informações acerca das atividades maliciosas processadas, apresentando:
- 7.2.3.6.35.1. Quais sites WEB estão sendo atacados;
 - 7.2.3.6.35.2. O que está sendo explorado no ataque e;
 - 7.2.3.6.35.3. Qual a origem do ataque.
 - 7.2.3.6.35.4. O painel de monitoramento deverá apresentar as informações e permitir a consulta da CDN, com delay máximo de 15 minutos e de no mínimo 30 dias de dados processados.
- 7.2.3.6.36. O painel de monitoramento deverá apresentar e contabilizar, por meio de gráficos, todas as requisições de conteúdo realizadas pelo usuário final para todo e qualquer código de status HTTP/HTTPS, gerando relatórios por período, permitindo a identificação dos picos de acesso a CDN;
- 7.2.3.6.37. O painel de monitoramento deverá apresentar e contabilizar, por meio de gráficos e API, o volume de dados trafegados e requisições entre a CDN e o usuário final para todo e qualquer código de status HTTP/HTTPS gerados na CDN;
- 7.2.3.6.38. O painel de monitoramento deverá apresentar e contabilizar, por meio de gráficos e API, o volume de dados trafegado, e requisições buscadas a partir da origem ou entregues a partir dos servidores de borda da plataforma da CDN;

- 7.2.3.6.39. Possibilitar a integração com SIEM (Security Information and Event Management), permitindo o gerenciamento de eventos e informações de segurança, incluindo serviço de WAF, proteção contra robôs e reputação de IP, sendo necessário a integração com no mínimo a ferramenta QRadar;
- 7.2.3.6.40. Para a análise das atividades das aplicações como desempenho, erros e eventos, deverá fornecer visibilidade próxima ao tempo real aos dados em pelo menos 30 segundos, possibilitando monitorar e visualizar a integridade das aplicações disponíveis na CDN e seus impactos nos usuários finais;
- 7.2.3.6.41. O serviço de entrega de log deverá fornecer controle sobre os fluxos de entrega de dados de registro ao vivo e em baixa latência a cada 30 segundos ou agregados frequentemente a cada minuto, permitindo:
 - 7.2.3.6.41.1. Criar, editar, visualizar e excluir configurações de fluxo de dados;
 - 7.2.3.6.41.2. Coletar, agrupar e transmitir registros de log brutos para um destino escolhido em janelas de tempo selecionadas;
- 7.2.3.6.42. Parar as entregas de logs conforme necessário;
- 7.2.3.6.43. Possibilitar a proteção e aceleração de qualquer aplicação http ou https que esteja hospedada, no mínimo, nos provedores de nuvem pública abaixo:
 - 7.2.3.6.43.1. Amazon AWS;
 - 7.2.3.6.43.2. Microsoft Azure;
 - 7.2.3.6.43.3. Google Cloud Plataform;
 - 7.2.3.6.43.4. IBM cloud.
- 7.2.3.6.44. Emitir alertas de notificação em caso de falhas no envio dos logs ajudando a resolver problemas quando os arquivos não forem

carregados para o destino por vários motivos, como configurações de destino inválidas ou tempos limite.

7.2.4. Solução de segurança de firewall de aplicação web – WAF:

7.2.4.1. A solução deverá disponibilizar em todos os pontos de presença o serviço de WAF, incluindo pelo menos as seguintes funcionalidades, além de outros tipos de ataques comuns e vulnerabilidades conhecidas a serem bloqueadas.

- 7.2.4.1.1. Bloqueio por rede e IP;
- 7.2.4.1.2. Geolocalização;
- 7.2.4.1.3. Secure token;
- 7.2.4.1.4. Cross site scripting (XSS);
- 7.2.4.1.5. Remote file inclusion (RFI);
- 7.2.4.1.6. Directory traversal;
- 7.2.4.1.7. Directory Climbing;
- 7.2.4.1.8. SQL injection;
- 7.2.4.1.9. Cookie e Command Injection;
- 7.2.4.1.10. Cross-Site Request Forgery;
- 7.2.4.1.11. Violações do protocolo HTTP;
- 7.2.4.1.12. Web Parameter Tampering;
- 7.2.4.1.13. Cookie Tampering;
- 7.2.4.1.14. Code Injection.

7.2.4.2. Possuir proteção contra as principais vulnerabilidades WEB listadas no OWASP, descritos em <https://owasp.org/Top10/>, além de proteção para a lista de vulnerabilidades para APIs, inclusive das novas vulnerabilidades que vierem a ser incluídos no OWASP durante a vigência do contrato;

- 7.2.4.3. Possuir proteção contra exploração de vulnerabilidade (exploit) por meio de inspeções de regras WAF;
- 7.2.4.4. Permitir a atribuição de políticas de segurança para segmentos configuráveis e altamente granulares da camada de aplicação WEB;
- 7.2.4.5. Permitir a configuração de regras de forma agrupada ou individual;
- 7.2.4.6. Fornecer o serviço de Geolocalização para permitir o bloqueio por país e redes indesejadas;
- 7.2.4.7. Tratar de maneira individualizada as requisições maliciosas direcionadas aos sites WEB da origem e bloqueá-las;
- 7.2.4.8. Fornecer o serviço de controle de camada IP para bloqueio ou liberação de endereços IP. Tais listas devem ser propagadas por toda a infraestrutura da Rede de Distribuição de Conteúdo;
- 7.2.4.9. Suportar a criação de listas de bloqueio ou liberação de sub-redes;
- 7.2.4.10. Permitir a detecção e bloqueio de crawlers e scanners de vulnerabilidade Web;
- 7.2.4.11. Permitir a detecção e bloqueio da resposta de determinada aplicação Web;
- 7.2.4.12. Permitir o bloqueio de ataques no modo blacklisting (bloqueio de ataques conhecidos por assinatura) e whitelisting (permitir apenas requisições e respostas conhecidas);
- 7.2.4.13. Possuir funcionalidade de aprendizagem automática do funcionamento de uma aplicação Web, suas URLs, parâmetros, campos de formulário, cookies, dentre outras, para a configuração do bloqueio por whitelisting;
- 7.2.4.14. Permitir a inclusão do IP do cliente no campo X-Forwarded-For;
- 7.2.4.15. Permitir a customização, pelo administrador, dos parâmetros aprendidos, de forma a criar regras baseadas no tamanho do parâmetro, tipo de conteúdo, e expressões regulares;

- 7.2.4.16. Possuir capacidade de ocultar os websites e aplicações, restringindo o acesso dos usuários diretamente na origem, fornecendo uma camada adicional de proteção, por meio de uma lista definida de endereços IPs que têm permissão para se comunicar com a origem da aplicação;
- 7.2.4.17. Deverá realizar inspeção completa de corpo de requisições HTML por segundo;
- 7.2.4.18. Permitir a inclusão de parâmetros customizados nos cabeçalhos (headers) HTTP, além da alteração dos existentes, para envio à aplicação de destino;
- 7.2.4.19. Para evitar falso positivos, a solução deverá implementar análise e inspeção de corpo de requisições, não limitando-se apenas a assinaturas;
- 7.2.4.20. Permitir a utilização de lista dinâmica, atualizada automaticamente, para detectar e bloquear endereços IP de má reputação, botnets, remetentes de phishing, dentre outras atividades maliciosas, sem custo adicional;
- 7.2.4.21. Permitir a geração de relatórios específicos do módulo de Web Application Firewall, disponibilizando no mínimo os relatórios abaixo:
 - 7.2.4.21.1. Top Ataques (geral ou por aplicação/servidor);
 - 7.2.4.21.2. Top IPs de origem dos ataques.
- 7.2.4.22. Implementar serviços de Serviço de Firewall IP/Geo, de bloqueio de Autonomous System, de regras nativas de filtragem de tráfego da solução e de regras customizáveis de filtragem de tráfego da solução;
- 7.2.4.23. Mitigação de ataques distribuídos de negação de serviço – DDoS;
 - 7.2.4.23.1. Prover serviço de defesa visando mitigar os efeitos de ataques de Distributed Denial-Of-Service (DDoS), sobre o conteúdo distribuído por meio dos servidores de borda, evitando que estes ataques alcancem a origem dos dados;

- 7.2.4.23.2. Deverá mitigar ataques de forma transparente, absorvendo e bloqueando ataques de TCP/IP SYN flood nos seus endereços IP mantendo a disponibilidade do serviço e entrega das aplicações;
- 7.2.4.23.3. Deverá fornecer o serviço de detecção e mitigação de ameaças para tráfego HTTP e HTTPS. O serviço deve continuar escalável instantaneamente e manter alta performance;
- 7.2.4.23.4. Deverá absorver e tratar as ameaças WEB na origem do ataque, absorvendo o tráfego malicioso e criando proteção de perímetro dentro da Internet;
- 7.2.4.23.5. Possuir proteção automática de APIs;
- 7.2.4.23.6. Possuir proteção da camada de rede por meio de bloqueio geográfico e listas negras de IP;
- 7.2.4.23.7. Possuir proteção DDoS por meio de controles de taxa (rate limit);
- 7.2.4.23.8. Possuir detecção e geração de alertas por taxas excessivas de tráfegos que excedam parâmetros configurados para pelo menos: solicitação de visualização de página, erro de origem e solicitação de página POST.
- 7.2.4.23.9. Implementar mecanismos capazes de mitigar quaisquer ataques que façam o uso não autorizado de recursos de rede, automaticamente, tanto para IPv4 e IPv6, para no mínimo:
 - 7.2.4.23.9.1. Ataques de inundação ou volumétricos, incluindo: SYN Flood, UDP Flood, TCP Flood e ICMP Flood;
 - 7.2.4.23.9.2. Ataques à pilha TCP;
 - 7.2.4.23.9.3. Ataques de botnets e Worms;
 - 7.2.4.23.9.4. Ataques que utilizam falsificação de endereços IP de origem (IP spoofing);
 - 7.2.4.23.9.5. Ataques à camada de aplicação, incluindo os protocolos HTTP e DNS, para no mínimo: HTTP URLGet/Post Flood, DNS Flood e Slowloris.

- 7.2.4.23.10. Possuir detecção e mitigação automática de ataques, utilizando múltiplas técnicas para mitigação e contramedidas, para no mínimo: whitelists, blacklists, limitação de taxa, técnicas desafio-resposta e descarte de pacotes malformados;
- 7.2.4.23.11. Possuir análise e inspeção automaticamente o tráfego XML e JSON em busca de ataques de aplicações;
- 7.2.4.23.12. Possuir inspeção de filtrar todo o tráfego da API;
- 7.2.4.23.13. Possuir análise e inspeção tráfego de API predefinido;
- 7.2.4.23.14. Possuir proteger as APIs contra chamadas mal-intencionadas;
- 7.2.4.23.15. Proteção contra robôs (botnets).
 - 7.2.4.23.15.1. Detectar o acesso de robôs nos sites do CONTRATANTE;
 - 7.2.4.23.15.2. Identificar bots com base em reputação e realizar a mitigação;
 - 7.2.4.23.15.3. Banir botnets automaticamente com base na reputação, heurísticas e métricas de identificação de sua nocividade;
 - 7.2.4.23.15.4. Realizar o tratamento de bots por meio de testes com Javascript injection e demais métricas que possibilitem seu tratamento e proteção do sítio;
 - 7.2.4.23.15.5. Ser capaz de diferenciar entre as requisições legítimas realizadas por usuários humanos das requisições realizadas por bots, web scraping e ataques automatizados;
 - 7.2.4.23.15.6. Prover defesa proativa contra bots, por meio da injeção de um desafio JavaScript para detectar se é um usuário legítimo ou robô.
- 7.2.4.23.16. Gerenciar de forma ativa as ameaças de bot realizando seu tratamento com base em assinaturas, comportamento, origem, possibilitando a criação de controles e regras padrão e

customizadas de forma automática e manual, que garantam o tratamento de no mínimo os seguintes ataques:

- 7.2.4.23.16.1. Rate limit para consumos identificados como anormais;
- 7.2.4.23.16.2. Ataques de DoS e DDoS;
- 7.2.4.23.16.3. Ataques de preenchimento de credenciais (Credential stuffing);
- 7.2.4.23.16.4. Ataques de força bruta (Brute force attack e password cracking);
- 7.2.4.23.16.5. Extração de dados (Web Scraping);
- 7.2.4.23.16.6. Roubo de identidade (Account Takeover).
- 7.2.4.23.17. Categorizar os robôs com base em suas ações e no impacto na infraestrutura de serviços do CONTRATANTE;
- 7.2.4.23.18. O software de configuração deverá permitir aplicar ações de segurança para os robôs, permitindo, no mínimo, as seguintes opções:
 - 7.2.4.23.18.1. Permitir o acesso;
 - 7.2.4.23.18.2. Bloquear o acesso e retornar código de erro HTTP 403 (acesso negado);
 - 7.2.4.23.18.3. Bloquear o acesso e retornar com mensagem customizada;
 - 7.2.4.23.18.4. Retardar a resposta às solicitações de forma customizada;
 - 7.2.4.23.18.5. Realizar a proteção de aplicações WEB, APIs e aplicativos móveis nativos.
- 7.2.4.23.19. Para aplicações WEB e APIs, deverá possuir detecção de anomalias comportamentais para páginas transacionais

importantes, protegendo-as como terminais de recursos da API, por meio de injeção de JavaScript para essas páginas;

7.2.4.23.20. Para aplicativos móveis nativos (Android e iOS), deverá coletar dados comportamentais, incluindo as características do dispositivo, eventos de toque de tela e dados do acelerômetro durante a interação do usuário;

7.2.4.23.21. Detectar em camadas diferentes atividades de bots para proteção do ambiente;

7.2.4.23.22. Possuir diretórios de bots conhecidos com base atualizada frequentemente;

7.2.4.23.23. Permitir a parametrização de regras de prevenção à bots;

7.2.4.23.24. Usar modelos que permitam aprendizagem de máquina para aprimoramento do serviço;

7.2.4.23.25. Incluir análise de comportamento do usuário, impressões digitais do navegador, detecção automática de navegadores, detecção de anomalias em HTTP e alta taxa de solicitação do serviço;

7.2.4.23.26. Possuir interface única de acesso, com relatórios próximos ao tempo real, de histórico e de tendências gerais e análises detalhadas de bots individuais ou outros segmentos do tráfego de bots, com intervalo de no máximo 60 segundos;

7.2.4.23.27. Permitir compartilhamento de informações sobre bots com SIEM.

7.2.5. Solução de sistema de nomes de domínio autoritativo em nuvem:

7.2.5.1. Deverá prover solução em nuvem para os serviços de DNS autoritativo.

7.2.5.2. Os serviços fornecidos deverão ser do tipo DNSSEc (Domain Name System Security Extensions).

7.2.5.3. Possuir ao menos 05 (CINCO) pontos de presença para resolução de DNS no Brasil.

- 7.2.5.4. A Plataforma deverá prover mecanismos para eventual aceleração de resolução de nomes DNS.
- 7.2.5.5. Implementar o serviço como DNS primário ou secundário, substituindo ou aumentando a infraestrutura DNS do CONTRATANTE.
- 7.2.5.6. A plataforma de DNS em nuvem deve prover:
 - 7.2.5.6.1. Aceleração de resolução DNS;
 - 7.2.5.6.2. Proteção contra os ataques DNS;
 - 7.2.5.6.3. Mecanismos que possibilitem ao alta disponibilidade do serviço DNS;
 - 7.2.5.6.4. Mecanismos para manutenção da configuração de DNS para os sítios a serem protegidos.
- 7.2.5.7. Prover interface de gerenciamento dos serviços de DNS por meio de portal em nuvem e por meio de interfaces de programação de aplicação (APIs), permitindo integrações com ferramentas do CONTRATANTE, no mínimo para as operações de:
 - 7.2.5.7.1. Criação, alteração e exclusão de zonas;
 - 7.2.5.7.2. Operações DNSSEC (assinatura, manual key rollover, etc.);
 - 7.2.5.7.3. Criação, alteração e exclusão de registros A, AAAA, MX, TXT, CNAME, DNAME, ALIAS e NS;
 - 7.2.5.7.4. A CDN deve disponibilizar serviço de reputação de IPs, com o objetivo de aumentar a precisão das decisões de segurança na identificação de IPs mal-intencionados, permitindo sua detecção e bloqueio, inclusive por meio de integração com mecanismo de WAF.

8. GESTÃO DE INCIDENTES

8.1. Proteção Contra Riscos Digitais

8.1.1. Para melhor compreensão deste tópico, devem ser consideradas as seguintes definições:

8.1.1.1. Proteção Proativa: Identifica e mitiga ameaças antes que se materializem em ataques.

8.1.1.2. Visibilidade Ampliada: Oferece uma visão abrangente do perfil de risco digital da organização.

8.1.1.3. Conformidade Regulatória: Auxilia no cumprimento de normas de segurança e privacidade de dados.

8.1.1.4. Economia de Recursos: Automatiza processos de monitoramento, reduzindo a carga sobre equipes internas.

8.1.1.5. Inteligência Acionável: Fornece informações relevantes para tomada de decisões estratégicas de segurança.

8.1.2. Requisitos gerais

8.1.2.1. A solução de cibervigilância se aplica aos domínios: mp.br, mprj.mp.br, mp.rj.gov.br, consumidorvencedor.mp.br, rap.gov.br, cnpg.org.br e todos os seus subdomínios, perfis institucionais oficiais em redes sociais: X(antigo twitter), tiktok, linkedin, facebook, flickr, instagram e youtube, bem como 50 (Cinquenta) usuários VIPs;

8.1.2.2. A Solução deverá ser ofertada em modo SaaS, sem a necessidade de instalação de componentes no ambiente da CONTRATANTE ou nos ambientes monitorados;

8.1.2.3. Licenciamento deverá ser efetivado pela quantidade de domínios principal, sem cobrança adicional por subdomínios, quantidade de endereços IP e quantidade de usuários;

8.1.2.4. Deverá possuir as seguintes funcionalidades:

8.1.2.4.1. EASM (External Attack Surface Management)

8.1.2.4.2. DRPS (Digital Risk Protection Services)

- 8.1.2.4.3. SRS (Scoring Risk Services)
- 8.1.2.4.4. BRM (Branding Monitoring)
- 8.1.2.4.5. TPRA (Third Parties Risk Management) integradas;
- 8.1.2.5. A solução de cibervigilância e ciberinteligência, deverá possuir recursos de inteligência artificial e automação, permitindo uma detecção mais rápida e precisa de ameaças em tempo real sem necessidade de intervenção humana;
- 8.1.2.6. A solução deverá monitorar menções e usos indevidos da marca da CONTRATANTE em redes sociais, detectando perfis falsos, páginas fraudulentas ou usos não autorizados.
- 8.1.2.7. Deverá dispor de mapeamento dinâmico do perímetro de ataque digital, monitoramento e detecção automática de informações expostas, através de robôs de busca automatizados;
- 8.1.2.8. Análise não intrusiva e monitoramento contínuo 24/7;
- 8.1.2.9. Monitoramento abrangente para uma visão mais completa dos riscos cibernéticos, através da obtenção de dados de diversas fontes, tais como Internet superficial, Deep Web, Dark Web e Redes sociais;
- 8.1.2.10. A solução deverá identificar credenciais corporativas obtidas a partir de sistemas comprometidos e integrados em botnets.
- 8.1.2.11. A solução deve aprender e obter informações de forma autônoma, sem a necessidade de fornecimento de informações como palavras-chave, ativos, fontes, datas ou outros dados específicos;
- 8.1.2.12. A curva de aprendizado da ferramenta deve ser simples e não exigir informações ou configurações específicas;
- 8.1.2.13. A solução deve possuir uma metodologia específica para controle de falsos positivos, estabelecendo contextos de busca configuráveis pelo usuário;
- 8.1.2.14. Avaliação de riscos e pontuação de segurança cibernética em tempo real;

- 8.1.2.15. Identificação proativa de riscos;
- 8.1.2.16. Análise de riscos de terceiros e fornecedores;
- 8.1.2.17. A solução deverá dispor de equipe especializada em inteligência e ameaças cibernéticas para gerenciamento de remoção de conteúdo e melhoria contínua da plataforma.

8.1.3. Interface do usuário

- 8.1.3.1. Deve fornecer uma avaliação geral de risco o mais próximo possível do aparecimento da ameaça;
- 8.1.3.2. Deve fornecer uma descrição e recomendação de correção para cada vulnerabilidade;
- 8.1.3.3. Deve exibir graficamente cada vulnerabilidade identificada por gravidade;
- 8.1.3.4. Deve rastrear o histórico e exibir graficamente categorias associadas à análise de vulnerabilidade externa;
- 8.1.3.5. Exibir uma lista com as três principais vulnerabilidades graves.

8.1.4. Monitoramento de dados de usuários VIPs:

- 8.1.4.1. Licenciamento baseado no número de usuários VIPs monitorados;
- 8.1.4.2. Capacidade de monitorar dados pessoais sensíveis de usuários VIPs, tais como documentos de identificação, informações bancárias, cartões de crédito e Wallets Bitcoin, mediante autorização e entrada dessas informações pelo próprio usuário VIP na plataforma;
- 8.1.4.3. Os dados pessoais sensíveis dos usuários VIP devem ser protegidos por criptografia, mascaramento e controle de acesso, impedindo que qualquer pessoa além do proprietário dos dados, mesmo os administradores da plataforma, venham a ter acesso a esses dados;
- 8.1.4.4. Monitoramento contínuo das informações pessoais quanto ao vazamento de informações ou atividades suspeitas que possam representar ameaça à integridade pessoal ou patrimonial da pessoa protegida;

8.1.4.5. Capacidade de análise de postagens e interações em redes sociais que possam ameaçar a integridade da pessoa protegida.

8.1.5. Monitoramento e Análise Avançados

8.1.5.1. Monitoramento contínuo 24/7/365 da Internet superficial, Deep Web e Dark Web;

8.1.5.2. Análise de redes sociais, fóruns, marketplaces ilegais e canais de mensagens;

8.1.5.3. Capacidade de monitorar pelo menos 100 milhões de fontes de dados diferentes;

8.1.5.4. Monitoramento não intrusivo, totalmente autônomo e automatizado, sem a necessidade de intervenção humana;

8.1.5.5. Identificação automática de vazamentos de dados, credenciais comprometidas e informações sensíveis expostas;

8.1.5.6. Detecção de menções à marca, executivos e ativos digitais da organização em contextos maliciosos;

8.1.5.7. Alertas em tempo real para ameaças emergentes, com priorização baseada em gravidade e relevância.

8.1.6. Monitoramento da Superfície de Ataque.

8.1.6.1. Descoberta e inventário automático de ativos digitais expostos (domínios, subdomínios, endereços IP, etc.);

8.1.6.2. Identificação de vulnerabilidades em sistemas e aplicações expostos à internet;

8.1.6.3. Monitoramento contínuo de alterações na superfície de ataque digital, incluindo:

8.1.6.4. Rede: exposição e possível nível de risco representado pela rede da organização;

- 8.1.6.5. Integridade do DNS: Subdomínios públicos e análise de domínios maliciosos ou suspeitos de phishing: Detecção de páginas falsas para fraude, phishing ou roubo de dados;
- 8.1.6.6. Vazamento de Dados: Vazamento de dados pessoais ou informações corporativas confidenciais, sensíveis e protegidas;
- 8.1.6.7. Credenciais vazadas: detecção em tempo real de credenciais que representam a possibilidade de acesso privilegiado;
- 8.1.6.8. Análise Web: status de proteção do CMS, patches, plug-ins e suas configurações e atualizações;
- 8.1.6.9. Reputação de IP: Comportamento anômalo dos IPs do domínio, indicativo de elementos infectados;
- 8.1.6.10. Gerenciamento de Patches: Informações obtidas a partir da análise de CVEs em tempo real conforme definido na norma;
- 8.1.6.11. Segurança de Email: Verificação e validação de configuração e detecção de informações ou e-mails vazados;
- 8.1.6.12. Inteligência em Redes Sociais: Detecção de ameaças e riscos através da análise de conversas em redes sociais (Hacktivismo, Fraude, Fake News, Impersonation, discurso de ódio).
- 8.1.6.13. As fontes de monitoramento devem considerar, no mínimo:
 - 8.1.6.13.1. Internet, Deep Web e Dark Web: A análise da Dark Web não se limitará apenas à conhecida rede Tor. Outras redes que também fazem parte da Dark Web deverão ser incluídas no monitoramento:
 - 8.1.6.13.1.1. Sites Git: onde os programadores compartilham código, como GitHub e similares;
 - 8.1.6.13.1.2. “Paste” sites: onde são compartilhados fragmentos de texto que podem ser códigos ou informações não estruturadas, como PasteBin e similares;

8.1.6.13.1.3. Fóruns: onde os usuários compartilham informações de vários tipos, como Reddit, Breached.vc ou similares;

8.1.6.13.1.4. Sites de informação: repositórios genéricos de informações compartilhadas, como Discord ou IRC.

8.1.7. Avaliação de Riscos e Inteligência de Ameaças

8.1.7.1. Pontuação de Risco Cibernético

8.1.7.2. Cálculo dinâmico de score de risco baseado em múltiplos fatores (exposição, ameaças, vulnerabilidades);

8.1.7.3. Benchmarking de risco em relação a pares da indústria e melhores práticas de segurança;

8.1.7.4. Recomendações acionáveis para melhoria do perfil de risco.

8.1.7.5. Avaliação de Terceiros

8.1.7.5.1. Monitoramento contínuo de riscos associados a fornecedores, parceiros e clientes;

8.1.7.5.2. Avaliação automatizada de postura de segurança de terceiros;

8.1.7.5.3. Alertas sobre mudanças significativas no perfil de risco de entidades relacionadas;

8.1.7.5.4. Possibilidade de conhecer em detalhe as vulnerabilidades caso desejado.

8.1.7.6. Inteligência de Ameaças Contextualizada

8.1.7.6.1. Coleta e análise de indicadores de comprometimento (IoCs) relevantes para a organização;

8.1.7.6.2. Correlação de dados de ameaças com o ambiente específico da organização;

8.1.7.6.3. Geração de relatórios de inteligência personalizados e acionáveis.

8.1.7.6.4. Proteção de Dados e Propriedade Intelectual

8.1.7.6.5. Detecção de vazamentos de dados sensíveis, incluindo dados pessoais, dados pessoais sensíveis e dados financeiros;

8.1.7.6.6. Monitoramento de exposição de propriedade intelectual (código-fonte, segredos comerciais, patentes).

8.1.7.7. Gestão de Reputação Digital

8.1.7.7.1. Monitoramento de sentimento e menções à marca em mídias sociais e fóruns online;

8.1.7.7.2. Detecção de campanhas de desinformação ou ataques coordenados à reputação;

8.1.7.7.3. Alertas sobre uso não autorizado de marcas registradas ou propriedade intelectual.

8.1.8. Requisitos Técnicos e de Implementação

8.1.8.1. Tecnologia e Arquitetura

8.1.8.1.1. Utilização de Inteligência Artificial e Machine Learning

8.1.8.1.2. Utilização de modelos de IA para detecção de anomalias e padrões de ameaças;

8.1.8.1.3. Algoritmos de aprendizado de máquina para redução de falsos positivos e priorização de alertas;

8.1.8.1.4. Capacidade de processamento de linguagem natural para análise de conteúdo em múltiplos idiomas.

8.1.8.2. Automação Avançada

8.1.8.2.1. Crawlers e scrapers automatizados para coleta contínua de dados da web;

8.1.8.2.2. Workflows automatizados para resposta a incidentes e mitigação de riscos.

8.1.8.2.3. Escalabilidade e Desempenho

8.1.8.2.4. Arquitetura distribuída capaz de processar e analisar petabytes de dados;

8.1.8.2.5. Tempo de alerta inferior a 5 minutos para alertas críticos;

8.1.8.2.6. Capacidade de escalar horizontalmente para acomodar crescimento de dados e usuários.

8.1.8.3. Integração e Interoperabilidade

8.1.8.3.1. APIs RESTful documentadas para integração com sistemas de segurança existentes (SIEM, SOAR, etc.);

8.1.8.3.2. APIs para plataformas populares de segurança e gerenciamento de riscos.

8.1.8.4. Segurança e Conformidade

8.1.8.4.1. Proteção de ponta a ponta para todos os dados em trânsito e em repouso;

8.1.8.4.2. Autenticação multifator e controle de acesso baseado em funções (RBAC);

8.1.8.4.3. Conformidade com padrões de segurança (ISO 27001, SOC 2) ou equivalente e regulações de privacidade (GDPR, CCPA).

8.1.8.5. Experiência do Usuário

8.1.8.5.1. Dashboard personalizável com visualizações interativas de dados e riscos;

8.1.8.5.2. Interface responsiva otimizada para desktop e dispositivos móveis;

8.1.8.5.3. Suporte multilíngue.

8.1.9. Capacidades de IA e Automação Essenciais

8.1.9.1. Análise Preditiva de Ameaças

8.1.9.1.1. Utilização de modelos de machine learning para prever tendências de ameaças e ataques potenciais;

8.1.9.1.2. Capacidade de identificar padrões sutis que indicam preparação para ataques cibernéticos.

8.1.9.2. Detecção de Anomalias Baseada em IA

8.1.9.2.1. Algoritmos de aprendizado não supervisionado para identificar comportamentos anômalos em redes e sistemas;

8.1.9.2.2. Adaptação contínua a padrões de tráfego e atividade normais para reduzir falsos positivos.

8.1.9.3. Processamento de Linguagem Natural Avançado

8.1.9.3.1. Análise semântica de conteúdo em múltiplos idiomas para identificar ameaças e intenções maliciosas;

8.1.9.3.2. Capacidade de entender contexto e nuances em comunicações relacionadas a ameaças.

8.1.9.4. Enriquecimento e Correlação de Dados Automatizados

8.1.9.4.1. Agregação e correlação automática de dados de múltiplas fontes para criar inteligência acionável.

8.2. Detecção e Resposta aos Incidentes

8.2.1. Monitoração de Incidentes:

8.2.1.1. Das atividades da CONTRATADA:

8.2.1.1.1. Monitorar o ambiente quanto à disponibilidade e desempenho dos equipamentos que compõe a solução a ser gerenciada, bem como todo o escopo contratado quanto aos incidentes relacionados à segurança da informação;

8.2.1.1.2. O ambiente a ser monitorado possui até 10.000 (dez mil) ativos, incluindo servidores, roteadores, switches, entre outros.

8.2.1.1.3. Gerir os incidentes (criação de alertas, detecção e abertura de chamados);

8.2.1.1.4. Acompanhar do início ao fim os incidentes;

8.2.1.1.5. Realizar o acionamento por matriz de escalação hierárquica e funcional, para os incidentes;

8.2.1.1.6. Correlacionar o processo de eventos (gerenciar eventos durante todo o seu ciclo de vida) e o processo de incidentes de forma automatizada entre as ferramentas de ITSM e monitoramento;

8.2.1.1.7. Acompanhar os processos através de indicadores de desempenho.

8.2.2. Detecção e resposta:

8.2.2.1. A CONTRATADA deve apoiar a CONTRATANTE na elaboração e/ou revisão do Plano de Resposta aos Incidentes. Tal plano deve conter, minimamente:

8.2.2.1.1. Tipo de incidente;

8.2.2.1.2. Ações a serem realizadas;

8.2.2.1.3. Responsáveis pela execução das ações, incluindo nome, telefone e e-mail.

8.2.2.2. A solução ofertada deve contemplar, de forma integrada e nativa, minimamente os seguintes mecanismos de detecção de incidentes

8.2.2.2.1. Correlacionamento de eventos (SIEM);

8.2.2.2.2. Análise comportamental de usuários (UEBA);

8.2.2.2.3. Detecção e Reposta de Rede (NDR);

8.2.2.2.4. Detecção de intrusão (IDS);

8.2.2.2.5. Malware Sandbox.

- 8.2.2.3. A solução ofertada deve permitir o Gerenciamento, análise, orquestração e automação de políticas, posturas, casos de uso, playbooks e integrações, com capacidade de resposta autônoma e aplicação próxima a tempo real, com componente de Orquestração, Automação e Resposta de Segurança (SOAR), totalmente e nativamente integrado à solução, com o objetivo de automatizar os processos e fluxos de trabalho, a execução de atividades repetitivas ou de difícil execução e a orquestração das diversas ferramentas de segurança, sem necessidade de atuação humana;
- 8.2.2.4. A CONTRATADA deverá reagir aos eventos de Segurança da Informação que possam afetar a disponibilidade, integridade ou confidencialidade das informações existentes nos sistemas ou serviços de TI do CONTRATANTE;
- 8.2.2.5. A CONTRATADA deve prover a proposta de contenção, erradicação e recuperação, articulação com as equipes do CONTRATANTE, controle de ações, notificações e escalonamento dos incidentes;
- 8.2.2.6. Em caso de ataque, devem ser elaborados alertas e estratégias de prevenção para todos os ambientes da CONTRATANTE;
- 8.2.2.7. A CONTRATADA deve criar, revisar e manter artigos de conhecimento (playbooks) de segurança com objetivo de simplificar e dar agilidade ao processo de resposta a incidentes;
- 8.2.2.8. Os referidos artigos de conhecimento devem ser transferidos para a CONTRATANTE;
- 8.2.2.9. A CONTRATADA deverá fazer uso de uma plataforma unificada para Detecção e Resposta a Incidentes com as seguintes características e especificações:
- 8.2.2.9.1. Quanto às suas características gerais, a solução ofertada deverá:
- 8.2.2.9.1.1. Possuir diversas funcionalidades de segurança que irão prover a capacidade de detecção e resposta aos

incidentes de segurança, através do modelo da Cadeia de Ataque (Kill Chain) automaticamente, contando com, pelo menos, os seguintes componentes:

- 8.2.2.9.1.1.1. Gerenciamento e correlação de eventos (SIEM);
 - 8.2.2.9.1.1.2. Orquestração e automação de respostas aos incidentes (SOAR);
 - 8.2.2.9.1.1.3. Análise do comportamento do usuário (UEBA);
 - 8.2.2.9.1.1.4. Detecção e Resposta na Rede (NDR);
 - 8.2.2.9.1.1.5. Sistema de detecção de intrusão (IDS);
 - 8.2.2.9.1.1.6. Malware Sandbox;
 - 8.2.2.9.1.1.7. Inteligência de Ameaças (Theat Intelligence).
-
- 8.2.2.9.1.2. Gerenciar todos os componentes solicitados através de uma única interface gráfica Web, permitindo o gerenciamento centralizado de toda a solução;
 - 8.2.2.9.1.3. Podendo ser hospedada na nuvem do fabricante com leitura de dados próprios para correlação de eventos de atividades maliciosas;
 - 8.2.2.9.1.4. Ser implantada de forma transparente através de sensores para fazer a coleta de informações, logs e telemetria;
 - 8.2.2.9.1.5. Rastrear e detectar ameaças em qualquer fonte ou local dentro da CONTRATANTE, incluindo, no mínimo, redes, servidores (físicos e virtuais), aplicações e nuvens públicas e privadas;
 - 8.2.2.9.1.6. Permitir o inventário dos ativos presentes na rede, por endereços IP e o nível de risco desses ativos, contando com detalhes e evidências disso sem a necessidade de executar varreduras de rede para este fim;

- 8.2.2.9.1.7. Possuir nativamente a capacidade de correlacionar vulnerabilidades relatadas por ferramentas de terceiros, com assinaturas de ataque identificadas e exibi-las em um painel de controle a partir dos quais os relatórios são gerados;
- 8.2.2.9.1.8. Possuir mecanismos de controle de acesso e autenticação, baseado em função, para que apenas as pessoas autorizadas pela CONTRATANTE tenham acesso às informações;
- 8.2.2.9.1.9. Deve ser capaz de se integrar com métodos de autenticação via Active Directory e LDAP.
- 8.2.2.9.1.10. Priorizar o risco e as atividades de operação de segurança no contexto da superfície de ataque e do negócio da organização;
- 8.2.2.9.1.11. Prover toda a comunicação entre os componentes de forma criptografada;
- 8.2.2.9.1.12. Incluir mecanismos de sincronização, como NTP (Network Time Protocol) e, assim, garantir a sincronização correta das informações;
- 8.2.2.9.1.13. Possibilitar a auditoria sobre o status das ações tomadas ou pendentes.
- 8.2.2.9.2. Quanto ao modelo de licenciamento, a solução ofertada:
 - 8.2.2.9.2.1. Deverá estar dimensionada pelo número total de ativos e não poderá estar limitada pela quantidade de eventos, tendo a capacidade de operar acima do estimado inicialmente sem perder qualquer funcionalidade/capacidade de indexação;
 - 8.2.2.9.2.2. Permitir a análise do tráfego de rede completo da CONTRATADA.
- 8.2.2.9.3. Quanto ao armazenamento de logs e eventos, a solução ofertada deverá:

- 8.2.2.9.3.1. Armazenar, na própria solução, as informações do tráfego de rede e dos Logs durante o período, mínimo, de 30 dias, bem como o registro dos incidentes gerados pela plataforma durante o período de 365 dias;
- 8.2.2.9.4. Permitir a retenção do histórico de segurança da CONTRATADA, contemplando, minimamente, os seguintes dados:
 - 8.2.2.9.4.1. Dados de eventos de segurança;
 - 8.2.2.9.4.2. Dados das aplicações;
 - 8.2.2.9.4.3. Dados dos sistemas operacionais;
 - 8.2.2.9.4.4. Dados das nuvens públicas e privadas;
 - 8.2.2.9.4.5. Dados do tráfego de rede;
 - 8.2.2.9.4.6. Tráfego de registro (syslog).
- 8.2.2.9.5. Quanto à compatibilidade e integrações, a solução ofertada deverá:
 - 8.2.2.9.5.1. Ser capaz de integrar-se às soluções de segurança terceiras presentes na rede, a fim de enriquecer a análise das informações coletadas e permitir ações adicionais de bloqueio contra-ataques cibernéticos;
 - 8.2.2.9.5.2. Possuir uma API restful para integração com vários serviços para ingestão de logs, telemetria e tráfego para detecção e resposta a eventos de segurança;
 - 8.2.2.9.5.3. Ser compatível com plataformas Windows e Linux;
 - 8.2.2.9.5.4. Permitir a análise de plataformas como:
 - 8.2.2.9.5.4.1. Amazon AWS;
 - 8.2.2.9.5.4.2. Microsoft Azure;
 - 8.2.2.9.5.4.3. Google G-Suite;

8.2.2.9.5.4.4. Microsoft Office 365;

8.2.2.9.5.4.5. Componentes virtuais (máquinas virtuais);

8.2.2.9.6. Quanto ao mecanismo de gerenciamento e correlação de eventos (SIEM), a solução ofertada deverá:

8.2.2.9.6.1. Possuir a capacidade de realizar a coleta e a ingestão de logs de todos os componentes do ambiente tecnológico da CONTRATANTE, através do padrão syslog ou similar;

8.2.2.9.6.2. Poderá se beneficiar das informações disponibilizadas pelo SIEM da CONTRATANTE;

8.2.2.9.6.3. Correlacionar eventos, com o objetivo de identificar anomalias e incidentes automaticamente;

8.2.2.9.6.4. Deverá ser uma solução reconhecida no mercado e deverá se integrar aos equipamentos e soluções em uso pela CONTRATANTE, sem que causem perda de desempenho ou consumam recursos dos ativos que monitorar;

8.2.2.9.7. Quanto ao mecanismo de detecção e resposta na rede (NDR), a solução deverá:

8.2.2.9.7.1. Analisar o tráfego TCP/UDP na rede da CONTRATANTE para detectar comportamentos e possíveis ameaças, gerando eventos de alerta de acordo com o tipo de tráfego;

8.2.2.9.7.2. Ter a capacidade de identificar ameaças no tráfego de rede e realizar o monitoramento proativo de forma automatizada do tráfego passante na rede da CONTRATANTE, contemplando os seguintes critérios:

8.2.2.9.7.2.1. Utilização da largura de banda;

8.2.2.9.7.2.2. Tentativas de penetração e varreduras de IPs e portas;

8.2.2.9.7.2.3. Autenticações recusadas ou com falhas;

- 8.2.2.9.7.2.4. Ataques bem-sucedidos de autenticação de força bruta;
- 8.2.2.9.7.2.5. Presença de tráfego malicioso, como ransomware, movimentação lateral, cryptojacking, mirmekatz, etc;
- 8.2.2.9.7.2.6. Análise de arquivos benignos e maliciosos e suas respectivas categorias;
- 8.2.2.9.7.2.7. Ataques de negação de serviço;
- 8.2.2.9.7.2.8. Conexões de comando e controle presentes, internamente ou de/para a Internet;
- 8.2.2.9.7.2.9. Dispositivos que representam o maior risco;
- 8.2.2.9.7.2.10. Aplicações que consomem mais recursos de rede;
- 8.2.2.9.7.2.11. Identificação das conexões e seu risco associado;
- 8.2.2.9.7.2.12. Identificação de aplicações da Camada 7;
- 8.2.2.9.7.2.13. Principais eventos críticos de segurança;
- 8.2.2.9.7.2.14. Nos ambientes de virtualização cujo tráfego passa pela rede física monitorada, pelo menos as seguintes métricas devem ser obtidas:
 - 8.2.2.9.7.2.14.1. Eventos críticos de segurança identificados nos servidores virtualizados;
 - 8.2.2.9.7.2.14.2. As aplicações que são mais utilizados;
 - 8.2.2.9.7.2.14.3. Principais eventos de segurança entre máquinas virtuais.
- 8.2.2.9.7.3. Deve permitir que a organização implemente um processo de investigação, threat hunting e forense de rede com base em metadados da solução utilizando funcionalidades de detecção e investigação;

- 8.2.2.9.7.4. Deve ser aderente ao framework de segurança cibernética ATT&CK do Mitre;
- 8.2.2.9.7.5. Pode possuir sensores que serão instalados na rede da organização para coletar, processar e gerar metadados a partir do tráfego de rede;
- 8.2.2.9.7.6. A solução deverá ser fornecida inicialmente com capacidade de inspeção agregada de, no mínimo, 1 Gbps ou caso a solução seja baseada em ativos deverá estar licenciada para 10000 (dez mil) ativos;
- 8.2.2.9.7.7. A solução de NDR deve ser constantemente alimentada por assinaturas de detecção de ameaças construídas por um time de pesquisa de ameaças avançadas do fornecedor;
- 8.2.2.9.7.8. Deve suportar a retenção dos metadados para fins de investigação e busca retroativa por no mínimo 365 dias;
- 8.2.2.9.7.9. A solução deverá processar o tráfego e armazenar os metadados das comunicações realizadas na plataforma de dados da solução.
- 8.2.2.9.8. Quanto a detecção dos incidentes, a solução ofertada deverá:
 - 8.2.2.9.8.1. Ser capaz de detectar padrões de ataques sem a utilização de assinaturas, através da elaboração automatizada de um baseline comportamental dos usuários e entidades;
 - 8.2.2.9.8.2. Possuir a capacidade de, via técnicas de Machine Learning, para o escopo de 10000 (dez mil) ativos, identificar anomalias nos comportamentos individuais dos usuários e entidades e de gerar alertas com relação, ao menos, aos seguintes casos de uso:
 - 8.2.2.9.8.3. Horário atípico do acesso;

- 8.2.2.9.8.4. Número atípico de sessões de uso nos sistemas operacionais;
- 8.2.2.9.8.5. Volume de conexões atípico;
 - 8.2.2.9.8.5.1. Volume de transferências de dados atípico;
 - 8.2.2.9.8.5.2. Localização geográfica atípica da origem do acesso;
 - 8.2.2.9.8.5.3. Endereço IP de origem atípico do acesso;
 - 8.2.2.9.8.5.4. Acesso atípico a dados armazenados;
 - 8.2.2.9.8.5.5. Criação e uso de processos (executáveis em memória) atípicos pelo usuário/entidade;
 - 8.2.2.9.8.5.6. Mudança na postura do usuário ou entidade.
- 8.2.2.9.8.6. Possuir mais de 150 modelos de detecção para casos de uso, como, no mínimo, Ransomware, Command & Control, DGA, Cryptojacking, phishing, scripts de power shell maliciosos, UBA e ataques de zero-day;
- 8.2.2.9.8.7. Permitir a criação de novas regras de detecção e alteração das regras existentes;
- 8.2.2.9.8.8. Emitir alertas quando eventos críticos de segurança forem detectados na rede e estes se desviarem de padrões estabelecidos (anomalias), por meio de análises detalhada de cada aplicativo em execução na rede de modo nativo, gerando chamados para a equipe do ambiente integrado de monitoramento e resposta a incidentes de segurança da informação (SOC), automaticamente, para a sua atenção, atuação e documentação;
- 8.2.2.9.8.9. Permitir a geração de diagramas de comunicação, mostrando como as ameaças estão associadas, bem como se movem no ambiente, baseado em capturas de tráfego, classificados e normalizadas automaticamente.
- 8.2.2.9.9. Quanto a resposta aos incidentes, a solução ofertada deverá:

- 8.2.2.9.9.1. Incluir uma solução integrada de gerenciamento de casos e incidentes;
- 8.2.2.9.9.2. Ter a capacidade de associar vários alertas recebidos a um único incidente que tem a capacidade de ser atribuído, ter uma linha do tempo, objetos associados, bem como as principais métricas MTTD e MTTR;
- 8.2.2.9.9.3. Ter a capacidade de enviar instruções de resposta através dos mesmos sensores de coleta;
- 8.2.2.9.9.4. Ter a capacidade de responder a todos os eventos de forma orquestrada e automatizada, integrando-se ao ambiente tecnológico da CONTRATANTE. As ações possíveis de resposta devem ser, pelo menos, as seguintes:
 - 8.2.2.9.9.4.1. Enviar um e-mail;
 - 8.2.2.9.9.4.2. Enviar mensagens para meios de comunicação do tipo SLACK
 - 8.2.2.9.9.4.3. Fazer um POST, GET ou um PUT para um servidor;
 - 8.2.2.9.9.4.4. Criar regras de bloqueio no firewall;
 - 8.2.2.9.9.4.5. Desabilitar usuários no Active Directory;
 - 8.2.2.9.9.4.6. Executar scripts.
- 8.2.2.9.9.5. Contemplar uma ferramenta que permita a investigação e busca de ameaças, com o objetivo de identificar as ameaças presentes na rede e automatizar os eventos de segurança para responder a elas;
- 8.2.2.9.9.6. Ser capaz de realizar análise retrospectiva com base nos dados ingeridos e armazenados do tráfego TCP/UDP, apoiando uma análise forense.
- 8.2.2.9.10. Quanto aos relatórios e dashboards, a solução ofertada deverá:

- 8.2.2.9.10.1. Ter a capacidade de gerar relatórios executivo e operacionais, com base em modelos pré-configurados, personalizáveis, baseados em dashboards, incluindo, pelo menos, relatórios sobre o status atual dos dispositivos, seu risco associado e tendências;
- 8.2.2.9.10.2. Gerar informações detalhadas sobre os eventos detectados, incluindo ameaças, anomalias, comportamentos e tendências de rede associadas ao risco de rede;
- 8.2.2.9.10.3. Detalhar os gráficos para aprofundar as informações apresentadas (mecanismo conhecido como Drill Down);
- 8.2.2.9.10.4. Gerar KRI (Principais Indicadores de Risco), como o número de eventos gerados em um dia, semana ou meses e compará-los com um período semelhante, o mesmo com a criticidade média dos eventos;
- 8.2.2.9.10.5. Permitir ao pessoal designado a geração de relatórios explorando todas as variáveis e funcionalidades da ferramenta, com a opção de parametrizar esses relatórios e consultá-los via Web, bem como a criação de filtros personalizados para pesquisas de eventos específicos;
- 8.2.2.9.10.6. Fornecer painéis configuráveis que possam conter diferentes gráficos com informações de, pelo menos:
 - 8.2.2.9.10.6.1. Eventos anômalos e críticos, incluindo:
 - 8.2.2.9.10.6.2. Detecções de segurança;
 - 8.2.2.9.10.6.3. IPs de Origem e Destino;
 - 8.2.2.9.10.6.4. Visão geral da atividade dos dispositivos (servidores e infraestrutura, física e virtualizada);
 - 8.2.2.9.10.6.5. Táticas e técnicas do MITRE ATT&CK;
 - 8.2.2.9.10.6.6. Fases do Kill Chain e os alertas associados.
 - 8.2.2.9.10.6.7. Aplicações utilizadas e seus dados históricos, discriminada por:

8.2.2.9.10.6.7.1. Risco associado;

8.2.2.9.10.6.7.2. IP de Origem e Destino;

8.2.2.9.10.6.7.3. Anomalias detectadas;

8.2.2.9.10.6.7.4. Classificação de risco;

8.2.2.9.10.6.7.5. Tráfego entre hosts.

8.2.2.9.10.6.7.6. Informações de em um Host:

8.2.2.9.10.6.7.7. Aplicações utilizadas;

8.2.2.9.10.6.7.8. Tráfego 'de' e 'para' o Host com base em detecções de segurança e anomalias.

8.2.2.9.10.7. Informações e o status das aplicações e serviços que estão sendo executados no data center, tais como:

8.2.2.9.10.7.1. Quantidade e a gravidade das anomalias;

8.2.2.9.10.7.2. Possíveis problemas de segurança no data center.

8.2.2.9.10.7.3. Permitir a criação de relatórios por período (hora, dia, semana, mês, ano, e personalizado por datas específicas);

8.2.2.9.10.7.4. Possuir filtros pós-captura, pelo menos para:

8.2.2.9.10.7.5. Filtro de erro;

8.2.2.9.10.7.6. Filtros por tráfego entre duas estações através da seleção do nome ou endereço IP;

8.2.2.9.10.7.7. Filtros por protocolos;

8.2.2.9.10.7.8. Geolocalização;

8.2.2.9.10.7.9. Gravidade;

8.2.2.9.10.7.10. Endereço IP.

8.2.2.9.10.8. Ser capaz de gerar um gráfico das anomalias das aplicações dentro da rede, fornecendo resultados com pelo menos as seguintes variáveis:

8.2.2.9.10.8.1. Movimentos laterais;

8.2.2.9.10.8.2. Histórico de eventos;

8.2.2.9.10.8.3. Anomalias de tráfego maliciosos;

8.2.2.9.10.8.4. Anomalias de políticas e negações de firewalls de infraestrutura;

8.2.2.9.10.8.5. Principais Aplicações;

8.2.2.9.10.8.6. Top Servidores;

8.2.2.9.10.8.7. Top Clientes;

8.2.2.9.10.8.8. Status das sessões atuais;

8.2.2.9.10.8.9. Origens e destinos de países com má reputação.

8.2.2.9.10.9. Exportar as informações dos pacotes capturados em metadados para análise posterior.

8.2.2.10. A fim de prover visibilidade aos mecanismos de detecção de incidentes, a CONTRATADA deverá fornecer uma ferramenta com as seguintes características:

8.2.2.10.1. Possuir funcionalidades e hardware específicos para agregação, regeneração, filtragem, descriptografia SSL/TLS e modificação/transformação do tráfego, não sendo aceitas soluções similares, como switches, roteadores, firewalls, balanceadores, servidores e soluções híbridas;

8.2.2.10.2. A solução é definida como um Network Packet Broker, ou seja, realiza características de um broker a nível de pacotes de rede e das funções competentes, como inspeção e descriptografia SSL. Trata-se de um equipamento exclusivo para esta função e, desta forma, não serão aceitas soluções como Firewalls UTM, Next-Generation Firewall (NGFW), Load Balancers com

funcionalidade de SSL Offloading para atendimento desta solicitação.

8.2.2.10.2.1. A solução deverá ser composta por único fabricante, incluindo os itens de Agregador, módulos e GBICs, com vista ao não desperdício de recursos técnicos e facilidade de integração.

8.2.2.10.3. Operar em taxa de linha completa sem perda de pacotes;

8.2.2.10.4. Quanto as suas características básicas, a solução deverá:

8.2.2.10.4.1. Possuir fonte de alimentação interna que trabalhe em 100V-240V, 50/60 Hz, com detecção automática de tensão e frequência, hot-swappable;

8.2.2.10.4.2. As fontes de alimentação devem permitir utilização de circuitos elétricos distintos;

8.2.2.10.4.3. As fontes de alimentação devem ser do tipo substituível (hot-swap), permitindo instalação e/ou substituição sem a necessidade de remoção do equipamento.

8.2.2.10.5. Possuir interfaces de 1 Gbps e 10 Gbps através da adição ou substituição de módulos ou licenças, sem impactar o desempenho dos equipamentos ofertados;

8.2.2.10.5.1. Permitir a conexão de interfaces Port Mirroring para receber fluxos de pacotes, de forma que as duas origens de captura possam coexistir simultaneamente conectadas à solução;

8.2.2.10.5.2. Todas as interfaces deverão vir com os transceivers necessários para interligação de equipamentos de acordo com as especificações do objeto;

8.2.2.10.5.3. Possibilitar o recebimento e encaminhamento do tráfego para soluções do tipo appliance e virtual machine;

- 8.2.2.10.5.4. Permitir a inclusão e remoção de regras ou filtros sem necessidade de reinicialização dos equipamentos;
- 8.2.2.10.5.5. Possuir capacidade de processamento line rate (non-blocking/wirespeed) para a aplicação dos filtros (regras) e encaminhamento de tráfego, em todas as portas suportadas pelo equipamento (pode ser comprovado documentalmente);
- 8.2.2.10.5.6. Implantar as seguintes configurações para agregação e encaminhamento de pacotes das portas de Rede para as portas de Ferramentas, tanto para os fluxos Out-of-Band (cópia de tráfego) respectivamente:
 - 8.2.2.10.5.6.1. Uma para uma;
 - 8.2.2.10.5.6.2. Uma para várias, possibilitando o balanceamento para as ferramentas;
 - 8.2.2.10.5.6.3. Várias para uma;
 - 8.2.2.10.5.6.4. Várias para várias, possibilitando o balanceamento para as ferramentas.
- 8.2.2.10.5.7. Permitir a criação filtros (regras) baseados em, no mínimo, os seguintes campos:
 - 8.2.2.10.5.7.1. Endereços MAC de origem e destino;
 - 8.2.2.10.5.7.2. Endereço IPv4 e IPv6 de origem/destino;
 - 8.2.2.10.5.7.3. Portas TCP de origem e destino;
 - 8.2.2.10.5.7.4. VLAN ID;
 - 8.2.2.10.5.7.5. Ethertype;
 - 8.2.2.10.5.7.6. IPFrag;
 - 8.2.2.10.5.7.7. TOS;

8.2.2.10.5.7.8. Protocol;

8.2.2.10.5.7.9. TCP Control Flags;

8.2.2.10.5.7.10. DSCP.

8.2.2.10.5.8. Implantar load-balancing dos pacotes utilizando os parâmetros abaixo como critérios para distribuição dos pacotes:

8.2.2.10.5.8.1. Endereços MAC de origem e destino;

8.2.2.10.5.8.2. Endereços IPv4 de origem e destino;

8.2.2.10.5.8.3. Endereços IPv6 de origem e destino;

8.2.2.10.5.8.4. Portas L4 (TCP e UDP) de origem e destino. Todos os acessos administrativos devem ser autenticados e criptografados.

8.2.2.10.5.9. Permitir a integração com servidores RADIUS, TACACS+ e LDAP para tarefa de autenticação e autorização;

8.2.2.10.5.10. Permitir accounting (AAA) dos usuários com TACACS+;

8.2.2.10.5.11. Possuir interfaces gráficas em formato web para administração, não sendo aceitos aplicativos cliente e/ou solução de administração executado em Java Virtual Machine;

8.2.2.10.5.12. Adotar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps;

8.2.2.10.5.13. Possuir MIB II, conforme RFC 1213;

8.2.2.10.5.14. Gerar e armazenar trilhas de auditoria que permitam o rastreamento de ações efetuadas em todos os seus componentes;

8.2.2.10.5.15. Os registros de logs devem conter a identificação do evento, data e hora, identificação do usuário.

8.2.2.10.6. Implantar funcionalidade que permita registrar eventos de logs;

8.2.2.10.7. Implantar funcionalidade para exportar os logs para servidores de log externo (syslog).

8.2.2.11. Quanto a deduplicação de pacotes, a solução deverá:

8.2.2.11.1. Implantar recurso de deduplicação de forma a remover pacotes duplicados antes de enviar para as interfaces da ferramenta;

8.2.2.11.2. Não impactar o desempenho das interfaces de entrada, nem as demais funcionalidades da solução

8.2.2.11.3. Implantar deduplicação de pacotes IPv4, IPv6 e pacotes sem IP, devendo levar em consideração o payload e os cabeçalhos ethernet;

8.2.2.11.3.1. Detectar pacotes duplicados recebidos em diferentes portas ou módulos do(s) equipamento(s);

8.2.2.11.3.2. Ser implementada sem necessitar reiniciar o equipamento.

8.2.2.11.4. Quanto a descryptografia, a solução deverá:

8.2.2.11.4.1. Implantar a criptografia/descryptografia tanto para o tráfego inbound (de entrada) quanto outbound (de saída);

8.2.2.11.4.2. Permitir carregar as chaves privadas (certificados) diretamente no equipamento, permitindo assim abrir todo o tráfego criptografado para as ferramentas que não possuem esta funcionalidade, centralizando a função de descryptografia;

8.2.2.11.4.3. Possuir capacidade de integração com dispositivos HSM (Hardware Security Module) externos, de forma a

verificar as chaves e certificados armazenados de forma centralizada nesses dispositivos;

8.2.2.11.4.4. Suportar, no mínimo, 2Gbps de throughput para tráfego SSL/TLS com abertura do tráfego criptografado, envio aberto para cadeia de inspeção e recriptografia para o destino original;

8.2.2.11.4.5. Suportar, no mínimo 15.000 (quinze mil) transações SSL por segundo, utilizando a cifra RSA-AES128, considerando toda a orquestração do tráfego SSL (abertura, direcionamento e recriptografia de tráfego);

8.2.2.11.4.6. Processar, no mínimo, 200.000 (duzentas mil) sessões concorrentes SSL, considerando toda a orquestração do tráfego SSL (abertura, direcionamento e recriptografia de tráfego);

8.2.2.11.4.7. Deve considerar como uma sessão a comunicação bidirecional fim-a-fim (cliente - servidor / servidor - cliente).

8.2.2.11.4.8. Permitir a importação de, no mínimo, 1.000 (mil) certificados em formato PKCS#12 ou PEM;

8.2.2.11.4.9. Implantar a abertura do tráfego de saída, através da reassinatura do certificado;

8.2.2.11.4.10. Implantar mecanismo que permita selecionar o tráfego que não será decryptografado, através de endereço IP, URL e domínio exemplo;

8.2.2.11.4.11. Ser capaz de operar de modo transparente, sem demandar alterações na topologia de rede;

8.2.2.11.4.12. Suportar, no mínimo, os seguintes protocolos:

8.2.2.11.4.12.1. SSL 3;

8.2.2.11.4.12.2. TLS 1.0;

8.2.2.11.4.12.3. TLS 1.1;

8.2.2.11.4.12.4. TLS 1.2;

8.2.2.11.4.12.5. TLS 1.3.

8.2.2.11.4.13. Implantar, no mínimo, 35 cifras distintas, distribuídas entre os protocolos SSLv3, TLS1.0, TLS.1.1, TLS 1.2 e TLS1.3.

8.2.2.11.4.14. Implantar, no mínimo, os seguintes algoritmos de criptografias para cifras e digest e mensagens de autenticação:

8.2.2.11.4.14.1. AES 128 GCM;

8.2.2.11.4.14.2. AES 256 GCM;

8.2.2.11.4.14.3. CHACHA20_POLY1305;

8.2.2.11.4.14.4. SHA-1;

8.2.2.11.4.14.5. SHA256;

8.2.2.11.4.14.6. SHA384.

8.2.2.11.4.15. Implantar, no mínimo, a troca de chaves RSA, DHE RSA, ECDHE, ECC e ECDHE ECDSA;

8.2.2.11.4.16. Implantar, no mínimo, os seguintes tamanhos de chaves:

8.2.2.11.4.16.1. 512;

8.2.2.11.4.16.2. 1024;

8.2.2.11.4.16.3. 2048;

8.2.2.11.4.16.4. 4096.

8.2.2.12. Quanto ao mecanismo de proteção, deverá ser provida solução de bypass, que deverá:

8.2.2.12.1. Ser instalada externa e independente ao equipamento de visibilidade, de forma que cada segmento interceptado pelo

bypass deverá possuir conexões de mesma velocidade para a plataforma de visibilidade, funcionando de forma non-blocking e com velocidade line-rate, devendo;

8.2.2.12.2. Prover interfaces de 1 Gbps ou 10 Gbps em fibra ótica monomodo ou multimodo;

8.2.2.12.3. Implantar fontes de alimentação internas, com plugues de energia separados, operando de forma redundante entre si, atuando na faixa de tensão 127V-240V;

8.2.2.12.4. Implantar proteção para que em caso de falhas das fontes de alimentação, as portas de rede mantenham o fluxo de dados sem interrupção;

8.2.2.12.5. Implantar interface dedicada para gerenciamento e configuração das políticas de direcionamento, sendo acessível via SSH (linha de comando) e Web;

8.2.2.12.6. Possuir portas físicas independentes para conexão aos dispositivos de rede e das interfaces de ferramenta;

8.2.2.12.7. Implantar nas portas de ferramentas que operem em velocidades iguais ou distintas das interfaces de rede;

8.2.2.12.8. Implantar recurso de detecção de falha de link tanto simétrico (LFD), permitindo que o status da porta de uma interface de rede do bypass seja espelhada para outra porta em caso de queda do dispositivo de rede;

8.2.2.12.9. Implantar atuação com múltiplas ferramentas nos cenários ativo ou redundante;

8.2.2.12.10. Implantar os seguintes protocolos para administração e gerenciamento:

8.2.2.12.10.1. SNMP v2C e v3;

8.2.2.12.10.2. Syslog;

8.2.2.12.10.3. SCP (Secure Copy) ou SFTP;

8.2.2.12.10.4. Poder ser atualizado via SCP ou SFTP.

9. CONTINUIDADE DO NEGÓCIO

9.1. Plano de continuidade do negócio

9.1.1. A CONTRATADA deve elaborar, implantar, testar e melhorar continuamente um Plano de Continuidade de Negócios (PCN), contemplando:

9.1.1.1. elaboração completa de Análise de Impacto de Negócio (business impact analysis – BIA) incluindo:

9.1.1.1.1. entrevistas aos principais setores envolvidos na área judiciária, identificação dos processos de trabalho e/ou atividades envolvidas,

9.1.1.1.2. avaliação dos impactos de interrupção,

9.1.1.1.3. identificação e estabelecimento de período máximo tolerável de interrupção (maximum tolerable period of disruption – MTPD ou maximum acceptable outage – MAO),

9.1.1.1.4. ponto de recuperação objetivado (recovery point objective – RPO);

9.1.1.1.5. tempo de recuperação objetivado (recovery time objective – RTO);

9.1.1.2. identificação, mapeamento e correlação dos ativos, recursos, dependências e atividades de apoio que suportam o serviço de negócio;

9.1.1.3. elaboração de Plano de administração de crise (PAC),

9.1.1.4. elaboração de Plano de continuidade operacional (PCO),

9.1.1.5. elaboração de Plano de recuperação de desastres (PRD) como componentes do PCN;

9.1.2. planejamento, elaboração e execução de testes, exercícios e revisão com periodicidade mínima anual, visando estabelecer e consolidar um sistema de gestão de continuidade de negócios (SGCN) com foco em TIC;

9.1.3. Deve adotar como referência a experiência e a metodologia da CONTRATADA e as seguintes normas:

9.1.3.1. ABNT NBR ISO 22301:2020 – Sistema de gestão de continuidade de negócios — Requisitos;

9.1.3.2. ABNT NBR ISO 22313:2020 – Orientações para o uso da ABNT NBR ISO 22301;

9.1.3.3. ABNT ISO/TS 22317:2023 – Diretrizes para análise de impacto nos negócios (BIA);

9.1.3.4. ISO/TS 22332:2021 – Guidelines for developing business continuity plans and procedures;

9.1.3.5. ISO 22398:2013 – Societal security — Guidelines for exercises.

10. TREINAMENTO NA COMPREENSÃO E CAPACITAÇÃO TÉCNICA

10.1. Características Gerais

10.1.1. Desenvolver um programa de treinamento customizado e estruturado para capacitar os profissionais de Segurança Cibernética do MPRJ, concentrando-se nas tecnologias e práticas cruciais para a compreensão técnica e participação efetiva no serviço contratado. O objetivo é capacitar os participantes a entenderem e contribuírem de forma eficaz em fóruns relacionados à execução do serviço, especialmente quando houver necessidade de tomada de decisão por parte da CONTRATANTE.

10.1.2. O propósito deste treinamento é habilitar os participantes a compreenderem os princípios fundamentais da segurança cibernética, reconhecer ameaças comuns, sugerir implementações de medidas de proteção e supervisionar o processo de resposta a incidentes de segurança da CONTRATADA.

- 10.1.3. O treinamento terá uma duração total de 96 horas, divididas em 12 sessões, sendo cada sessão com duração de 8 horas. Se houver dificuldade de agendamento, a CONTRATANTE poderá sugerir horários alternativos, desde que estejam dentro do horário comercial em conjunto com a disponibilidade do instrutor da CONTRATADA.
- 10.1.4. Este treinamento é direcionado a profissionais de tecnologia da informação, gestores de segurança, analistas de segurança, administradores de sistemas e a qualquer indivíduo integrante da força de trabalho do MPRJ que queiram aprimorar seus conhecimentos em segurança cibernética.
- 10.1.5. O treinamento deverá abranger, no mínimo, os seguintes tópicos, sem prejuízo de outros conteúdos pertinentes ao objeto contratado:
- 10.1.5.1. Melhores práticas e padrões de segurança cibernética;
 - 10.1.5.2. Instalação, configuração e operação da solução implantada, quando a CONTRATADA julgar necessário;
 - 10.1.5.3. Análise de desempenho e melhores práticas no uso da solução;
 - 10.1.5.4. Análise de problemas e drill-down para diagnóstico de eventos;
 - 10.1.5.5. Outros assuntos relacionados ao tema de Segurança da Informação, Governança e Risco.
- 10.1.6. O público-alvo poderá variar de acordo com o contexto e os objetivos específicos de cada turma, sendo a definição dos participantes de responsabilidade da CONTRATANTE, por intermédio do gestor administrativo do contrato.
- 10.1.7. O treinamento será ministrado de forma teórica e prática, com utilização de recursos audiovisuais, estudos de caso, exercícios orientados, demonstrações guiadas e simulações aplicadas ao contexto institucional do MPRJ, visando assegurar a adequada assimilação e aplicação dos conceitos apresentados.
- 10.1.8. Ao final de cada turma, será concedido aos participantes certificado de conclusão, contendo, no mínimo, o nome do participante, a carga horária cumprida, a data de realização e a identificação do instrutor responsável, devidamente assinado pela CONTRATADA.

- 10.1.9. O treinamento será realizado de forma remota, sendo cada sessão estruturada em 2 (duas) turmas independentes, com 4 (quatro) horas-aula por turma, limitadas a até 6 (seis) participantes por turma, podendo ser executado ao longo da vigência contratual de 36 (trinta e seis) meses, conforme a necessidade da CONTRATANTE.
- 10.1.10. O programa de treinamento será ofertado sob demanda, mediante solicitação formal da CONTRATANTE, podendo ser programado em datas distintas ao longo da vigência contratual, de acordo com a evolução das necessidades institucionais e a disponibilidade do instrutor da CONTRATADA.
- 10.1.11. O início das atividades de capacitação deverá ocorrer em até 10 (dez) dias corridos, contados a partir da emissão da Ordem de Serviço específica, facultando-se à CONTRATANTE a proposição de ajustes no cronograma, desde que compatíveis com o horário comercial e previamente acordados com a CONTRATADA.
- 10.1.12. Todo o material didático utilizado deverá ser disponibilizado em formato digital, sem ônus para a CONTRATANTE. As sessões deverão ser gravadas e disponibilizadas posteriormente, com a finalidade de permitir consultas futuras e apoiar processos de integração e capacitação continuada.
- 10.1.13. Ao término de cada turma, os participantes deverão avaliar o treinamento e o instrutor, por meio de formulário próprio indicado pela CONTRATANTE. Caso 30% (trinta por cento) ou mais dos participantes atribuam avaliação global insatisfatória à turma, o treinamento deverá ser reaplicado, sem ônus adicional para a CONTRATANTE, no prazo máximo de 10 (dez) dias úteis.
- 10.1.14. O recebimento definitivo do treinamento ficará condicionado ao atendimento cumulativo dos seguintes requisitos:
- 10.1.14.1. cumprimento integral da carga horária prevista;
 - 10.1.14.2. cumprimento integral da carga horária prevista;
 - 10.1.14.3. disponibilização do material didático e das gravações das sessões;
 - 10.1.14.4. resultado satisfatório da avaliação dos participantes.

10.1.15. Somente após o pleno atendimento desses requisitos será emitido o **Termo de Recebimento Definitivo** referente à etapa de capacitação.

11. PROFISSIONAL DEDICADO

11.1. Características Gerais

11.1.1. Deve ser disponibilizado 01 (um) profissional, alocado em regime de dedicação exclusiva de mão de obra, em regime presencial, nas dependências da CONTRATANTE na cidade do Rio de Janeiro;

11.1.2. A atuação deste profissional se dará em horário comercial, considerando os feriados nacionais, estaduais do estado do Rio de Janeiro e municipais do município do Rio de Janeiro, bem como os pontos facultativos decretados pela CONTRATANTE;

11.1.3. Tal profissional deverá possuir habilidades pessoais necessárias para o exercício da função, tais como:

11.1.3.1. Facilidade de comunicação e fluência verbal;

11.1.3.2. Bom relacionamento interpessoal e cortesia;

11.1.3.3. Equilíbrio emocional;

11.1.3.4. Proatividade, criatividade e iniciativa;

11.1.3.5. Clareza e objetividade;

11.1.3.6. Organização;

11.1.3.7. Comprometimento com prazos e com qualidade;

11.1.3.8. Espírito de equipe;

11.1.3.9. Discrição;

11.1.3.10. Boa redação.

11.1.4. Durante o afastamento de um profissional por motivo de férias, quaisquer licenças, ou ainda na impossibilidade de execução de suas atividades

profissionais, a CONTRATADA deverá garantir a execução dos serviços sem interrupção, mantendo a qualidade da prestação;

11.1.5. Caso a ausência exceda o prazo de 5 (cinco) dias úteis, um novo profissional com as mesmas qualificações, ou superior, deverá ser interinamente apontado para a função, desde que autorizado pela CONTRATANTE;

11.1.6. O profissional dedicado deverá possuir, no mínimo, o perfil profissional descrito na tabela listada no Anexo III, atendendo, na íntegra, as qualificações e dedicação exigidas no Contrato;

11.1.7. A substituição de um profissional, sempre que necessária, deverá se dar por outro profissional que atenda as qualificações técnicas descritas neste edital, relativas ao perfil que atuará.

11.1.8. A CONTRATANTE disponibilizará o espaço físico, mobiliário, ponto de rede e energia, necessários para a perfeita execução das atividades deste profissional;

11.1.9. A CONTRATADA deverá disponibilizar todos os demais recursos necessários, incluindo recursos de informática, tais como computadores, notebooks, softwares e insumos correlatos à prestação dos serviços, sem ônus para a CONTRATANTE;

11.1.10. O profissional dedicado terá a função de Gerente Técnico do Contrato, voltado principalmente para o acompanhamento, suporte e apoio geral à execução contratual e dos serviços, nos aspectos administrativos e técnico-operacionais, incluindo o cumprimento dos níveis mínimos de serviço, o cumprimento de prazos e de qualidade na execução e nos entregáveis dos serviços, andamentos e esclarecimentos relacionados ao faturamento dos serviços, dentre outros.

11.1.11. O profissional deverá apresentar mensalmente um relatório com as atividades realizadas no período, e cronograma das atividades programadas para o mês subsequente. O relatório deverá também apontar problemas críticos e prioritários, com uma estimativa de impactos e riscos, caso existam.

12. SERVIÇOS TÉCNICOS ESPECIALIZADOS

12.1. Características Gerais

- 12.1.1. A CONTRATADA deve disponibilizar um banco de horas técnicas para execução de serviços técnicos especializados, relativos às atividades correlatas não previstas no escopo original, a serem demandadas, aprovadas e executadas sob demanda, mediante ordem de serviço (OS), contemplando 300 (trezentas) horas ao longo do contrato.